Enhanced communications in data collection multihop Wireless Sensor Networks

Gérard Chalhoub

Habilitation à Diriger des Recherches

Université d'Auvergne

Spécialité : Informatique

Enhanced communications in data collection multihop Wireless Sensor Networks

Présentée par Gérard Chalhoub le 22 juin 2016

Rapporteurs :

André-Luc Beylot, Professeur, Université de Toulouse
Kaveh Pahlavan, Professeur, Worcester Polytechnic Institute
Fabrice Valois, Professeur, Insa de Lyon

Examinateurs :

Pascal Lafourcade, MCF HDR, Université Clermont Auvergne
Pascale Minet, CR HDR, Inria
Thierry Val, Professeur, Université de Toulouse

Tuteur :

Michel Misson, Professeur, Université Clermont Auvergne

Contents

French summary

Les réseaux de capteurs sans fil ont été développés depuis le début des années 2000 pour répondre à des besoins de beaucoup de domaines d'application. La facilité de déploiement, l'auto-configuration et l'autonomie énergétique constituent les atouts principaux de cette nouvelle technologie. L'amélioration des communications dans un réseau de capteurs multi-saut présente des défis à chaque niveau de la pile protocolaire. Plusieurs méthodes dans la littérature ont été proposées pour rendre le réseau plus fiable et plus performant. Mes contributions concernent essentiellement les techniques d'accès au médium, de routage et de sécurité pour les applications industrielles de collecte de données. Dans ce contexte, la qualité de service en termes de taux de délivrance, délai de bout-en-bout, et robustesse du réseau sont les besoins principaux. Des améliorations complémentaires doivent être étudiées au niveau des différents niveaux de la pile protocolaire pour aboutir à une solution performante. Au niveau de la méthode d'accès au médium, j'ai exploité le multi-canal avec des nœuds puits multi-interfaces pour augmenter le débit du réseau et éviter les interférences. Cette contribution est baptisée HMC-MAC (Hybrid Multi-Channel Medium Access Control). Au niveau du routage, j'ai travaillé sur la répartition équitable du trafic afin d'éviter les congestions dans le réseau. Ce travail a donné lieu à CoLBA (Collaborative Load Balancing Algorithm). Pour garantir des communications sécurisées au sein du réseau, j'ai travaillé sur la gestion des clés cryptographiques et l'authentification des nœuds et des échanges pour aboutir à des solutions prouvées sûres et qui passent à l'échelle. Enfin, avec la congestion de technologies exploitant la même bande de fréquences ISM, j'ai étudié l'effet du WiFi sur les solutions qui exploitent le CSMA/CA de la norme IEEE 802.15.4. Ce travail donne des guides de précautions à prendre en compte pour que ces deux technologies cohabitent sans perturber l'activité du réseau de capteurs. Toutes ces contributions ont été évaluées par simulation en utilisant NS2 ou Cooja, ou bien par maquettage sur des cartes spécifiques ou des modules TelosB.

To my family...

Acknowledgements

This work would not have been made possible without the help and support of the people that I have worked with since 2006.

I would like to thank my all time advisor Michel Misson for all the years that we have shared and all the projects on which we have worked. His trust and support have helped me reach where I am today.

I would sincerely like to thank the expert evaluators, André-Luc Beylot, Kaveh Pahlavan, and Fabrice Valois, who evaluated my Habilitation for their valuable comments and encouragements. I would also like to thank Pascal Lafourcade, Pascale Minet, and Thierry Val for their examination of the Habilitation and their support throughout our years of collaboration.

An important part of the work presented in this document was made possible with the help of the PhD students I co-supervised, Rana Diab, Ismail Mansour, and Hamadoun Tall, many thanks go to them. Without forgetting all the co-authors with whom I collaborated.

I would also like to thank the Networks and Protocols research team of LIMOS and the department of Networking and Telecommunications of IUT of University of Auvergne for their support during the past 10 years.

Chapter 1

Introduction

Wireless Sensor Networks (WSNs) technology has emerged in the early twenty first century as a new promising solution for many applications. From smart homes, elderly health care, intrusion detection, environmental monitoring, military and medical applications, to industrial automation. Ease and low cost of deployment made this technology very popular. The first IEEE low power and low rate wireless network standard appeared in 2003 [1]. In the early stages, the main concern for network protocols used for WSNs was energy efficiency and extending network lifetime was the primary objective.

In order for network protocols to be energy efficient, they compromised performance efficiency. Thus, the first available solutions were only suitable for non-critical applications. Nevertheless, WSNs started to be considered for more critical applications. Hence, optimizations for network protocols were needed to ensure acceptable performances from the application perspective. Network performance expectations differ depending on the application constraints and needs. A compromise is to be found according to what is more important to guarantee. For example, if energy efficiency is the main priority, protocols should be able to put nodes into sleep mode for as long as possible. Some needs might be antagonist, such as guaranteeing small delays and high data delivery rate on one hand, and optimizing energy consumption on the other hand. Thereby, a generic protocol stack solution cannot meet the wide variety of application needs.

Wireless sensor networks became an essential part of the Internet of Things (IoT) domain. They constitute an important part of the lower level of the architecture. In a typical deployment scenario, sensors and devices that are part of the wireless network should exchange data, report information and execute commands in an Ad-Hoc manner. Many communication protocols that have been proposed for Ad-Hoc networks were adapted for wireless sensor networks and many more have been specifically proposed to better cope with the particularities of this new technology.

This document presents my contributions in the wireless sensor network domain. I have mainly worked on optimizing communication protocols for in-

dustrial data collection applications. In such contexts, quality of service in terms of data packet delivery, end-to-end delay and network robustness are the main priorities. An overview on my main contributions that followed my PhD work is presented in chapters 2, 3, 4, and 5. My contributions are four-fold. One of my essential contributions is optimizing MAC (Medium Access Control) protocols for wireless sensor networks. Protocols such such as MaCARI [2] and HMC-MAC [3] are the products of my work on MAC protocols that enhance the network performance in terms of throughput efficiency and aggregate throughput. Enhancing MAC performance without taking into considerations routing issues might lead to congestion and performance degradation in the network. Hence, my second contribution is on traffic management using a congestion aware routing protocol called CoLBA [4]. Combining MAC and routing optimizations might optimize network reliability and robustness but this does not protect the network against malicious behavior and attacks. My third contribution is thus on securing communications in wireless sensor networks using energy efficient and scalable key distribution and key establishment protocols based on standard cryptographic algorithms [5]. In a shared frequency band such as the ISM (Industrial Scientific and Medical) band, a special care should be given to co-existence between technologies using the same communication channels in order to better understand its consequences. Therefore, my forth contribution focuses on the co-existence between overlapping technologies, namely the study concentrates on the effect of IEEE 802.11 [6] on IEEE 802.15.4 [7] based protocols.

I started working on wireless networking during my Master's degree. I have studied interference and coverage issues in mobile Ad-Hoc communications using Wi-Fi and emulated information propagation that mimics a bio-contamination process, results of this work showed the importance of understanding mobility scenarios and signal propagation models in network simulators [8]. My PhD thesis was part of the OCARI (Optimization of Communication for Ad hoc Reliable Industrial networks) project [9]. During my PhD thesis, I have designed and evaluated a deterministic, energy efficient and synchronized MAC protocol called MaCARI [2, 10, 11, 12, 13, 14]. Results showed the important compromise between energy efficiency and guaranteeing end-to-end delay. Following performance evaluation by simulation and prototype [15, 16] and I have worked after my PhD on enhancing the performance of MaCARI [17], and integrated node coloring optimizations in order to allow simultaneous communications without interference [18, 19]. The latter work is a joint work with Hypercom team of Inria Rocquencourt.

I have co-supervised a PhD thesis that aimed at securing communications in WSNs [20, 5]. This thesis lead to interesting results in ensuring scalable key establishment and authentication protocols that will be discuss in 4 [21, 22, 23, 24, 25, 26]. I have also co-supervised a thesis on optimizing throughput in WSNs using a multi-channel MAC protocol that we called HMC-MAC (Hybrid Multi-Channel MAC) [27, 3, 28]. This thesis was funded by the FUI (Unique Inter-ministerial Funds) project SAHARA2 (Solution for ArcHitecture and Applications of wireless netwoRks in Aircraft). Results of this thesis, that are discussed in 2, showed the enhancements in the network performance in

terms of MAC efficiency using multiple channels and multiple radio interfaces on the sink node [29, 30]. I am currently co-supervising a thesis that started on November 2014 on load balancing routing techniques in order to optimize traffic flow in WSNs. The first results of this thesis, that are discussed in 3, are encouraging and show the gain obtained by avoiding overloaded nodes [4]. In this thesis we are working on making network simulation tools more realistic and more reliable [31]. I am also co-supervising a thesis that started on December 2015 on mobility and instability consequences on WSNs protocols.

The remainder of the document is organized as follows. Chapter 2 briefly describes my main contributions on MAC layer protocols. Chapter 3 presents my contributions on load balancing. Chapter 4 presents a quick overview on my contributions on security for wireless sensor networks. Chapter 5 describes measurements and analysis I have supervised on wireless technologies coexistence. Chapter 6 discusses the open issues in MAC and load balancing protocols and highlight my ongoing and future works. Chapter 7 summarizes my teachings contributions, whereas Chapter 8 sums up my collaborations with other researchers, Institutes and Universities. In addition, an extended french resume is added in A.

Chapter 2

Multichannel MAC

In this chapter, I will go through a quick overview on the literature concerning multichannel MAC protocols. My PhD thesis was centred on MAC optimization for industrial WSNs. It was part of the national ANR (National Research Agency of France) project OCARI [9]. OCARI aimed at optimizing ad-hoc communications in industrial networks. When we deal with industrial networks, we deal with critical SCADA (Supervisory Control And Data Acquisition) applications with quality of service requirements such as guaranteed end-to-end delay and low packet loss ratio. In that context, my PhD thesis focused on optimizing the MAC performance in order to guarantee access to the medium from the source to the destination in an energy efficient manner. OCARI aimed at guaranteeing energy efficient behavior in order to extend network lifetime for applications such as nuclear plant employees monitoring.

The main contribution of my thesis was a deterministic and energy efficient TDMA and CSMA/CA based MAC protocol called MaCARI [2]. MaCARI is based on a multi-hop synchronization that is initiated by the sink of the network [11]. This synchronization ensures that all nodes of the network share the same schedule and are able to reduce interference and collisions using a time segmentation approach for data collection [16]. The challenge was to find the right compromise between energy efficiency and network performance. For in order to reduce energy consumption nodes should turn off their radio as long as possible, and in order to reduce end-to-end delay nodes should remain active. Enhancements were made on MaCARI in order to reduce the synchronization period [32] and optimize the data collection process [17].

What follows highlights joint contributions on multi-channel MAC protocols with my PhD student Rana Diab and co-supervisor Michel Misson. This work is part of the national FUI project SAHARA2. This project main objective is to be able to replace part of the wired networks deployed on aircraft by wireless networks based on IEEE 802.15.4 physical layer without compromising performance. In order to do so, wireless protocols should be able to achieve high reliability and high throughput. In that context, we worked on MAC protocols that offer high throughput efficiency, that is, achieving high data rate delivery

with minimal data loss. The highest IEEE 802.15.4 data rate is limited to 250 Kbps, which is not enough for some of the applications requirements of SAHARA2. Most of these applications are data collection applications with only one sink. Hence, one radio interface at 250 Kbps rate will not be able to cope with the applications needs. In order to enhance the sink reception rate, we proposed a multi-interface sink node equipped with multiple IEEE 802.15.4 radio interfaces. For these radio interfaces to work simultaneously they would need to operate on orthogonal communication channels. In addition, a single hop is not enough to cover the extend of the network on the aircraft, a multi-hop deployment is thus a must. With these requirements, we studied and proposed a MAC protocol that exploits multiple channels in a multi-hop topology and allows the sink node to receive simultaneously on all its radio interfaces. The remainder of this section describes the proposed solution.

2.1 Quick overview on multichannel MAC protocols

Multi-channel MAC protocols have obtained considerable attention in WSNs because they help increase the network performance. Operating on multiple channels can ensure robustness against internal and external interference and allows collision free parallel communications. Most existing MAC protocols proposed for WSNs use a single channel for data transmission. This is essentially due to the fact that energy efficiency is considered to be the most important issue in WSNs. On the other hand, in dense deployment of sensor networks, a single channel utilization generates high level of interference and limits the use of the bandwidth.

In a multi-hop topology, packets must be transmitted several times over multiple hops in order to reach the final destination. This overloads the radio channel and induces interference. It also increases the risk of collision due to the hidden terminal problem [1] for example [33], which results in degrading the medium access protocol performance. The use of multiple channels helps mitigate the effect of interference and enhances the network performance under high traffic load. The availability of multiple channels increases the number of simultaneous transmissions between nodes which leads to an increase in the global network throughput.

The hardware of most popular platforms and those compliant with the IEEE 802.15.4 [7] and Zigbee [34] standards provides a radio chip capable of switching its communication channel, and is therefore not limited to a single channel operation. In the literature, several surveys on multi-channel MAC protocols with different objectives have been proposed for WSNs [35, 36, 27]. These surveys classify multi-channel MAC protocols according to several criteria: periodicity

1. The hidden terminal problem occurs when more than one senders are not in range and access the medium at the same time to communicate with the same node causing interference and collisions at the receiver.

of channel switching, centralized or distributed manner for channel assignment, schedule-based or contention based MAC protocols. In what follows, a quick summary is presented of the main characteristics of each type of channel assignment protocols based on the periodicity of channel switching. We distinguish static, semi-dynamic and dynamic channel assignment protocols.

Static channel assignment approaches group nodes into clusters and allocate different channels for each cluster avoiding using the same channel in clusters which may cause interferences. The channel assignment is done once, at the network initialization phase. The protocols presented in [37, 38, 39] adopt a static channel assignment approach. The main advantage of static channel assignment approaches is the ease of implementation since the dynamics due to channel switching and variations in the network topology are not taken into account and do not affect the channel assignment process. On the other hand, the drawback of static channel assignment is that it is not suitable to dynamic network conditions such as topology changes due to unstable links or traffic requirements. In addition to that, if two nearby nodes are assigned to different channels, they cannot communicate with each other. This will generate traffic overload because messages should be sent to intermediate nodes, generally the sink node, in order to reach nodes using a different channel.

Semi-dynamic approaches assign fixed channels but nodes can switch between channels in order to communicate with neighboring nodes. This approach includes many protocols such as in [40, 41, 42, 43, 44]. The main advantage of semi-dynamic approaches over the static channel assignment is that nodes can switch channels to communicate with neighbors which helps eliminating network partitions and reduces traffic overload. However, with semi-dynamic channel assignment approaches coordination of channel switching is required between senders and receivers in order to be on the same channel at the same time. The problems that arise due to channel switching are multi-channel hidden terminal problem, deafness problem [2] and broadcast support problem [3], which are mainly caused by the lack of synchronization between nodes.

In dynamic channel assignment approaches such as in [45, 46, 47, 48], nodes switch channels before every transmission. The channel selection can be measurement based or status based. In measurement based approaches, nodes measure the SINR (Signal to Interference plus Noise Ratio) value on a channel before transmitting. In status based approaches nodes keep track of the status of channels, such as busy or idle, using received control packets. Although dynamic channel assignment protocols can reduce interference to some degree, they all have to frequently exchange information globally or in a large neighborhood to perform channel usage negotiations and synchronization coordination. Therefore, they cause considerable communication overhead to WSNs.

2. Deafness problem occurs when a sender tries to communicate with a node that is busy on an other channel.

3. When nodes use multiple channels, it is not possible to achieve a broadcast on the network level without a global synchronization.

2.2 Main contribution: HMC-MAC

This section describes the main contribution in multi-channel MAC protocols which is HMC-MAC (Hybrid Multi-Channel MAC) protocol. HMC-MAC is a semi-dynamic multi-channel MAC protocol that uses a TDMA multihop beacon synchronization method in order to achieve a network segmentation and channel assignment.

2.2.1 Network Creation and Beacon Propagation

The first node to be activated in the network is the node that will create the network and start broadcasting periodical beacons. When a new node is activated and wants to join the network, it starts by scanning for beacons. A node will consider that it is the first node in the network and creates a new network if it does not detect beacons. This node is known as the Network Coordinator (NC) and is on depth 0 [4]. In case the new node receives at least one beacon, it chooses the most suitable one and sends an association request to the node that is broadcasting it. The choice of the beacon can be based on different criteria such as the RSSI (Received Signal Strength Indicator) and the LQI (Link Quality Indicator) for robust links, or the number of hops separating the source of the beacon from the destination node for minimum end-to-end delay, or a combination of both depending on the application needs. In our case, we consider the current number of children of the source in order to achieve load balancing at the association phase.

Time is divided into cycles as shown in Figure 2.1. Each cycle is divided into intervals during which communications are organized in a specific manner. Each cycle begins with a TDMA beacon propagation period $[T_0; T_1]$ that is followed by a data exchange period $[T_1; T_2]$ and an inactive period $[T_2; T_0]$. Depending on the application needs, the duration of these intervals can be adjusted to suit the generated traffic size.

During $[T_0; T_1]$ the NC broadcasts a beacon that is propagated in a multi-hop manner to reach all the nodes of the network based on the MaCARI protocol [16]. Each node in the network has a unique beacon transmission slot during which it broadcasts its beacon. The beacon contains information that enables each node to know in which slot it should propagate its beacon. When a new node joins the network, its ID is sent to the NC in order to update the propagation order. The NC will then include this ID in the beacon for m consecutive cycles. Similarly, in case of node departure, a leave request is sent to the NC (it can be sent by the node that is willing to leave the network, or sent by neighboring nodes that detected that a node has failed. The latter aspect has not been studied). This allows nodes to update their local propagation order. The propagation order is maintained by each node and updated using the beacon. The order of the IDs defines the order in which the beacon is propagated. If the ID of a node has

4. In case two nodes create new networks at the same time and are able to detect each other, the NC with the bigger ID quits its own network and joins the network of the NC with the smaller ID. The process of switching networks is not considered in this study.

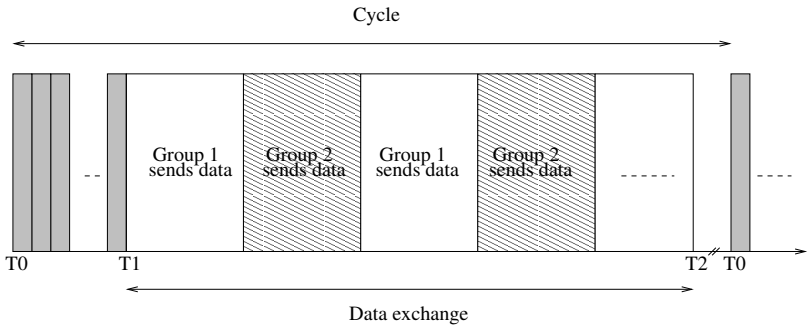


Figure 2.1: Global cycle. $[T_0; T_1]$ is a synchronization period, $[T_1; T_2]$ is dedicated for data exchange. Section 2.2.3 describes how groups are created.

the index 3 in the propagation order, it means that it is the third node to send the beacon during $[T_0; T_1]$ (more details on this aspect can be found in [11]). This guarantees that beacons are not sent at the same time and thus avoids collisions. The beacon is propagated using a known common channel. This way new nodes scan only one channel to discover the network.

2.2.2 Neighbor discovery

Neighbor discovery enables each node to know which nodes are prone to interfere. In order to avoid overloading the network with long control messages to exchange neighborhood information, we use bitmaps to define neighbors. Using the local propagation order (which is a list of all the node IDs), every node is able to build and manage a bitmap that represents all the nodes in the network. Each index of the bitmap corresponds to the node ID with the same index in the propagation order. This way, when the network is dense, neighborhood information will not overload the network with control traffic.

In order to avoid interference when acknowledgements are used, 3-hop neighborhood needs to be discovered. In [19], we discussed why the reuse of channels should be considered up to 3-hop neighborhood to avoid collisions and interference when immediate MAC layer acknowledgments are used. Figure 2.2 shows an example of how the use of the same frequency channel by 3-hop neighbors might cause collisions. Nodes A and D are 3-hop neighbors using the same channel. A collision can occur on C when B is sending data to A and D is sending an acknowledgement to C. Thus, the same channel cannot be used in a 3-hop neighborhood.

One hop neighbor list is built using the source address of received beacons. When a node receives a beacon from another node, it considers that this node is a neighbor. This does not guarantee that the link is bi-directional, but we assume that it is an interfering node. In order to build 2-hop neighbor lists, each node includes the bitmap of its 1-hop neighbors in the beacon. Hence, when a node receives all the beacons from its neighbors, it is able to build the

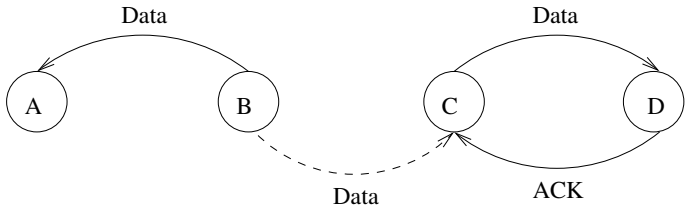


Figure 2.2: 3-hop neighborhood interference in channel allocation with acknowledgements. A and D are 3-hop away nodes, if they are allowed to receive data during the same time slots, the ACK sent from D to C will collide with the data sent from B to A.

list of its 2-hop neighbors. When a node figures in the bitmap of a neighbor, it can consider that a bi-directional link exists with that neighbor. In order to build 3-hop neighbor lists, each node should include the bitmap of its 1-hop neighbors and the bitmap of its 2-hop neighbors in the beacon it sends.

By using the beacon and the propagation order to build 1-hop, 2-hop and 3-hop interference neighborhood, we avoid using additional control traffic such as HELLO messages that are traditionally used by routing protocols. By using bitmap codification and sending beacons in a TDMA manner, neighboring information are exchanged efficiently between nodes without collision and with light overhead. It should be noted that only new arriving nodes are included in the propagation order to avoid sending the complete list in the beacon and overload the frame payload.

2.2.3 Channel Allocation Scheme and Node Activity

The role of the NC is to divide time into intervals and inform all nodes of this time segmentation using the beacon frame. We assume that each node has only one radio interface (nodes should be low cost and use energy efficient hardware components), the sink can have several radio interfaces. We consider the availability of 16 orthogonal communication channels as specified by IEEE 802.15.4 standard [7].

All nodes willing to communicate with the same node compete on the same channel in order to access the medium and send information using slotted CSMA/CA algorithm. Topology is organized into several depths based on ZigBee Custer-Tree topology [34]. We consider that all traffic is destined to the NC, for that, exchanges can be sequenced according to the depth of the nodes in the topology and channels can be allocated taking into account the traffic flow orientation.

In order to increase throughput, the NC should remain in reception mode and nodes in depth 1 should alternate between sending mode and reception mode but keep part of them in transmission mode. Thus, we divided the network into two groups as it is shown in Figure 2.3), *Group* 1 includes odd depth nodes that are descendants of an even child of NC interface (B, D, F are even children of

an interface), and also includes even depth nodes that are descendants of an odd child of NC interface. All other nodes are included in *Group* 2. For example, in Figure 2.3 *Group* 1 includes nodes G, H, B, M, D, O, P, F. All other nodes are part of the second group. When nodes of *Group* 1 are in transmission mode, nodes of *Group* 2 are in reception mode, and vice versa. This insures that interfaces of the NC always have nodes in transmission mode forwarding them traffic (this can also be ensured using methods of topology control [49], but it is out of the scope of this paper).

Figure 2.4 depicts the algorithm that is executed by each node in order to calculate the index of the branch to which it is affiliated. The index of the branch allows the node to know to which group it belongs. We use hierarchical addresses of ZigBee based on the Cskip formula as explained in the standard [34].

For channel allocation, each node has a 3-hop neighborhood bitmap which enables it to choose dynamically its own channel. The node with the highest priority in a 3-hop neighborhood chooses its channel first. Priorities are assigned according to the network addresses. The node with the smallest network address has the highest priority. A node proceeds to its channel allocation as soon as it becomes the node with the smallest address among its 3 hop-neighborhood that is not yet assigned a channel. A bitmap that represents all nodes is also used to announce which nodes have completed the channel allocation process in order for each node to know if it is its turn to choose a channel. When a node chooses its channel, it broadcasts it in the beacon frame.

Each node then builds a 16-bit bitmap for nodes that belong to *Group* 1. It also builds 16-bit bitmap for nodes that belong to group *Group* 2. Where each bit in the bitmaps indicates the occupancy of the equivalent channel in 1-hop neighborhood. These bitmaps are then included to the beacon which allows nodes to build a 2-hop channel allocation bitmaps. All four bitmaps are then included in the beacon to build a 3-hop channel allocation view for each group of nodes.

16 channels are not enough in order to allow all nodes to communicate at the same time without interference when the network is dense. Hence, the channel allocation process should exploit spatial reuse or allow interfering nodes to use same channels using CSMA/CA. In our channel allocation process, we will try to decrease the interference as much as possible. A node first tries to find a free channel in the 3-hop neighborhood of its group, if it does not find one, it tries to find a free channel in the 2-hop neighborhood of its group. In case there are no available channels in its 2-hop neighborhood, a node tries to find a free channel in the 1-hop neighborhood of its group. Finally, if it does not find a free channel, it randomly chooses a channel among the least used channels in its 1-hop neighborhood that are part of its group. Indeed, because each node indicates its channel in the beacon, each node can manage the number of neighboring nodes using the same channel. Note that whenever multiple channels are available, nodes randomly choose one of the available channels. Figure 2.5 depicts the steps executed by each node before choosing a channel.

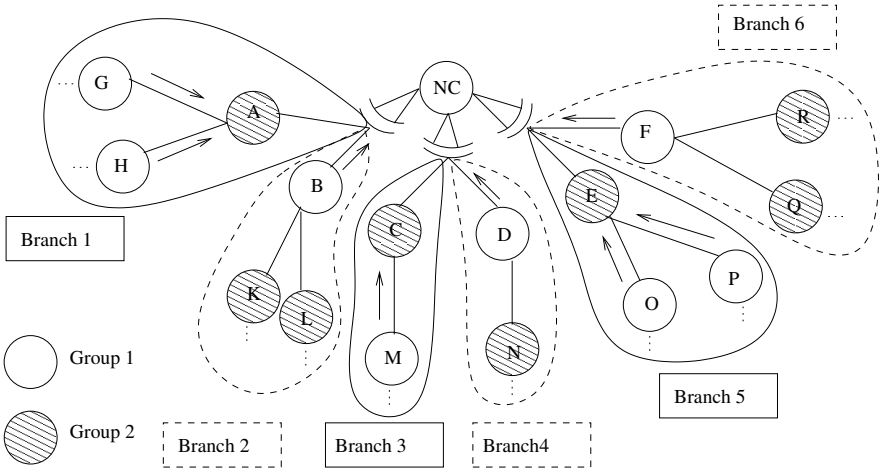


Figure 2.3: Network segmentation. Each interface divides its descendants into two branches. In the first branch, even depth nodes belong to *Group* 1, odd depth nodes belong to *Group* 2. In the second branch, odd depth nodes belong to *Group* 1, even depth nodes belong to *Group* 2.

These operations run only during the setup phase or if changes in the topology occur. The setup phase ends when all nodes have chosen frequencies. Then, data exchange phase can start. $[T_1; T_2]$ is divided into intervals, each interval is divided into two time slots. During the first time slot, *Group* 1 are senders and *Group* 2 are receivers. During the following time slot nodes exchange roles, receivers become senders and senders become receivers. Each node knows its own depth. Thus, it is able to alternate between sending and receiving states. Nodes receive data frames from lower depth neighbors and transmit frames to one of their higher depth neighbors using slotted CSMA/CA algorithm.

2.3 Evaluation results

In this section, part of the evaluation results of the overall performance of HMC-MAC is presented. The chosen metrics are the aggregate throughput (which is the number of received packets per second at the sink), packet delivery ratio, and number of frame repetitions. Indeed, these results show the enhancements that HMC-MAC offers under high data rate scenarios that emulate periodic traffic and burst traffic profiles. Also, the weakness of HMC-MAC is shown in the results in terms of queue overflow.

We used NS-2 simulator [50]. We have implemented a physical layer that is compliant with IEEE 802.15.4 physical layer in terms of data rate, bandwidth and communication channels. We also take into account physical phenomena such as capture effect, near far effect, ambient noise, collisions, and interference. The MAC layer is implemented according to the description of each evaluated

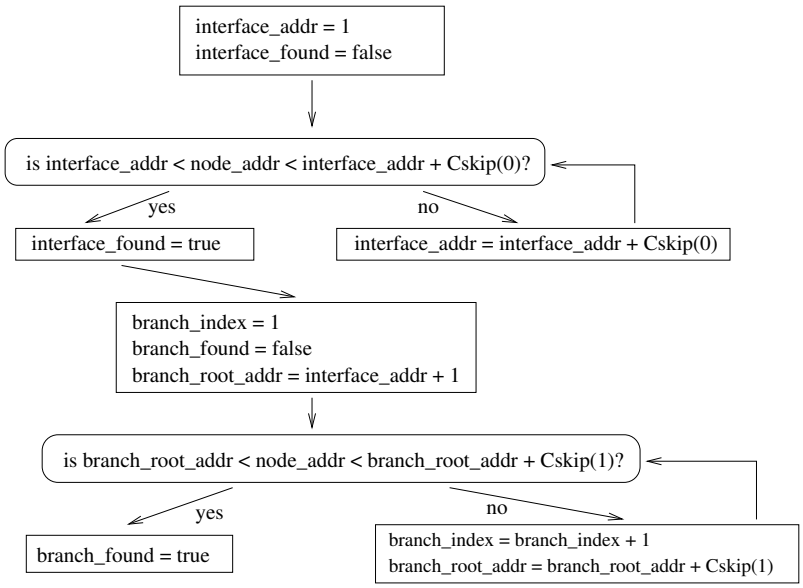


Figure 2.4: Algorithm for calculating the index of the branch to which a node is affiliated.

protocol. Namely for HMC-MAC, we have implemented the protocol as a new MAC protocol in the simulator. We have also implemented slotted CSMA/CA of IEEE 802.15.4 and used it for data exchange.

The network dimensions are $100 \times 100\ m^2$ with a communication range of $20\ m$. Our topologies correspond to hierarchical topologies of 50 nodes with a maximum depth of 7 ($Lm = 7$), and 3 maximum children by coordinator ($Cm = 3$). We used the ZigBee hierarchical routing protocol in all simulations [34]. We also assumed that number of available channels is 16. We fixed the packet queue size to 200. Each point in the following graphs is the mean over 50 iterations. These parameters are the same for all the evaluated methods.

All presented results are obtained from a 20-second observation window during $[T_1; T_2]$ activity period. During this window, we have 80 alternations between group intervals (each interval being $125\ ms$ long). This evaluation is done after the network has reached a stable state and all nodes have joined in. We considered only 3 radio interfaces for the sink and two children for each interface. There is no rational for the number of interfaces, 3 is just a case study. We limited the number of children per interface to 2 in order to avoid competition between these nodes and thus avoid collisions on the sink on each interface. The simulation is carried out by varying the number of packets generated by each node, the topologies and the type of traffic production. Also note that we do not do any packet or frame aggregation in the network.

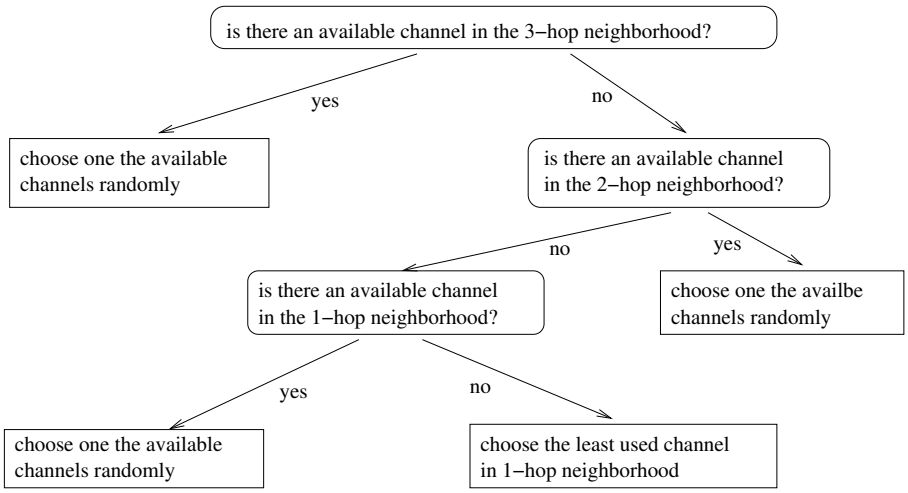


Figure 2.5: Algorithm for choosing a channel.

2.3.1 Traffic Production

We defined two types of traffic generation profiles: periodic generation and burst generation. In the periodic traffic generation, nodes generate data in a periodic manner similar to a CBR (Constant Bit Rate) traffic. In the burst traffic generation, nodes generate packets by doubling the rate of periodic generation in the first second and then refrain from generating traffic in the following second. This type of traffic generation emulates sudden data bursts. With both traffic generation profiles we reach the same number of generated packets. But, in the burst generation, nodes compete much more to access to the medium for 50% of the time compared to the periodic generation and spend the other 50% forwarding packets accumulated in the packet queues. This results in higher offered load during the first 50% compared with the periodic traffic. Figure 2.6 shows how traffic is generated in both modes.

2.3.2 Comparison with other methods

Most protocols in the literature use 2-hop information to allocate channels and some of them use random allocation. Others divide the network into clusters. Accordingly, we chose to compare our protocol with four different allocation methods: HMC without segmentation method, 2-hop method, random method and cluster method. These are variants of HMC-MAC but inspired by protocols from the literature.

In the HMC without segmentation method, a node applies the same channel allocation scheme as HMC-MAC but without taking into account the group segmentation. This method is evaluated in order to show the importance of network segmentation. In the 2-hop method, a node chooses an available channel

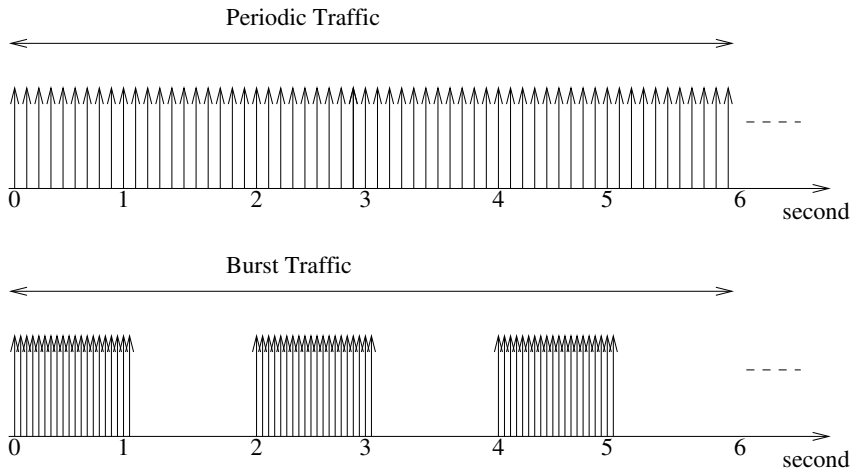


Figure 2.6: Traffic generation in periodic and burst modes.

in its 2-hop neighborhood. In case all channels are used, it randomly chooses a channel. This method is used to evaluate the effect of doing an allocation based on 3-hop information and not only 2-hop information. In the random method, a node randomly chooses a channel from the list of authorized channels without checking the availability of this channel. This method is simply a default method used for comparison sake only. In the cluster method, the network is divided into 3 clusters. Each interface with its descendants represent a cluster. We allocate a different channel for each cluster. All nodes belonging to the same cluster use CSMA/CA to compete for channel access on the same channel. This method is the equivalent of 3 sub-networks using CSMA/CA without channel switching.

2.3.3 Aggregate Throughput

Figures 2.7 and 2.8 present the results in terms of aggregate throughput. For HMC-MAC protocol, it shows that when the number of generated packets increases the aggregate throughput increases. All other protocols reach saturation (Figure 2.7) or rise slowly (Figure 2.8) when the number of generated packets becomes greater than 8 pkts/sec/node due to the high number of collisions and frame repetitions. As for the cluster method, the number of packets collected by the NC does not exceed 100 packets/sec and reaches saturation when the number of generated packets exceeds 4 pkts/sec/node.

The performances of HMC-MAC are close to those obtained with HMC without segmentation, for low traffic rates (under 6 pkts/sec/node for periodic traffic scenario and under 3 pkts/sec/node for burst traffic scenario). On the other hand, for higher traffic rates HMC-MAC copes much better than the other protocols. This is due to the fact that HMC-MAC divides the network into two groups. It always takes into consideration the channel usage in the groups before choosing a channel. This means, with HMC-MAC we have 16

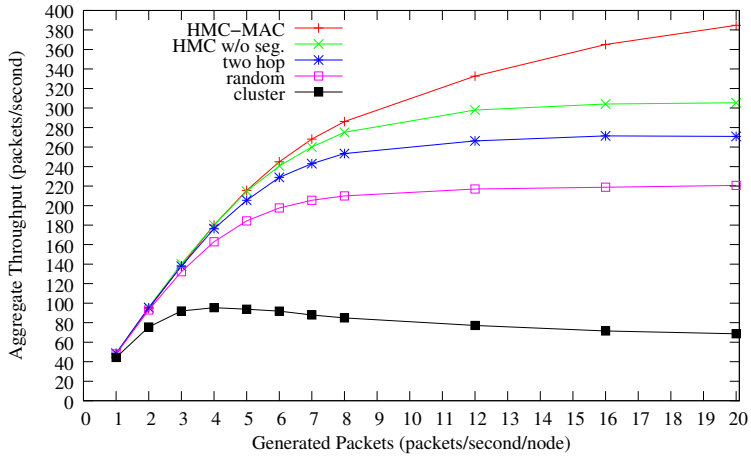


Figure 2.7: Aggregate throughput for periodic traffic.

channels for each group, whereas in HMC without segmentation and the other methods we have 16 channels for all the nodes. In addition, segmenting the network and defining the receivers during each interval help HMC-MAC avoid sending frames for nodes that are not in reception mode on the right channel. This leads to higher packet delivery rate with HMC-MAC.

Note that HMC-MAC outperforms other protocols even more in burst traffic generation. For example, with 12 pkts/sec/node, when we use a periodic traffic generation, HMC-MAC increases the received packets at the sink by around 76.8%, 34.7%, 20% and 10.4% compared to cluster method, random method, 2-hop method and HMC without segmentation method, respectively. When we use a burst traffic generation, the number of packets received by the sink is increased by almost 77%, 45.7%, 39.4% and 32.5% respectively. This is due to the same reasons stated earlier and shows that HMC-MAC is able to better manage the access to the medium under high burst traffic than other protocols that suffer more from packet loss due to lack of rendez-vous between senders and receivers.

We can also notice that HMC without segmentation outperforms the 2-hop method and that 2-hop method is more efficient than the random method. This is due to the fact that 2-hop does not take into consideration the channel usage in its 3-hop neighborhood. It is also important to note that we are using a slotted CSMA/CA algorithm in all the evaluated methods. Slotted CSMA/CA is a variant of non-persistent CSMA/CA, and this is why we reach a saturation point and not a decrease point.

2.3.4 Packet Delivery Ratio

Figures 2.9 and 2.10 show the results in terms of delivery ratios at the sink node. Similarly, HMC-MAC achieves better delivery ratios than other protocols

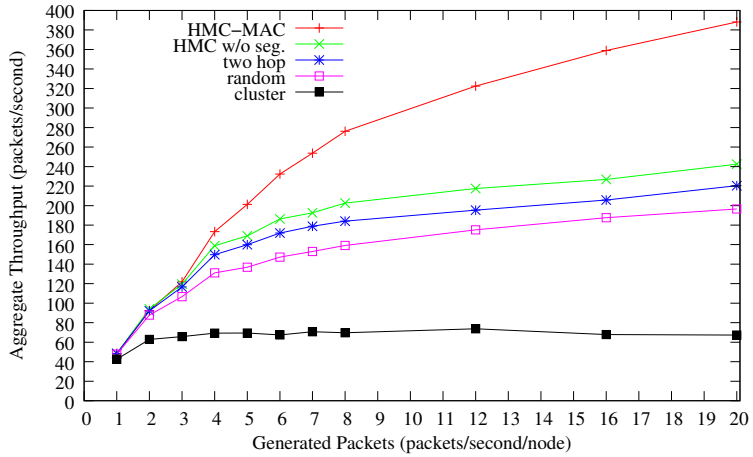


Figure 2.8: Aggregate throughput for burst traffic.

during high data rate and burst traffic.

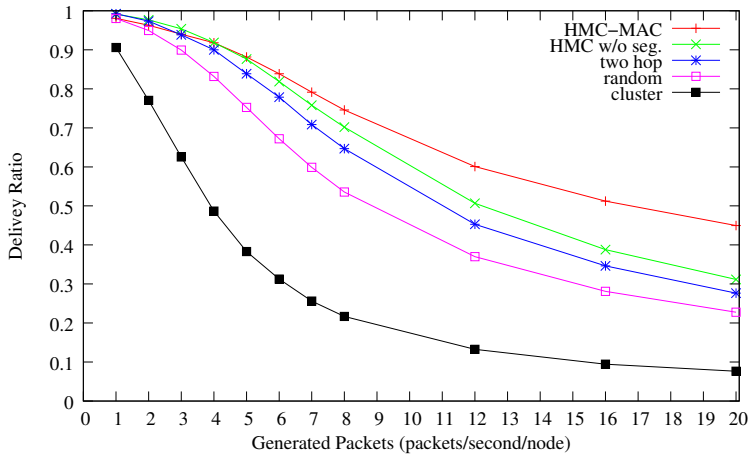


Figure 2.9: Delivery ratio at the sink for periodic traffic.

2.3.5 Number of Repetitions

Figure 2.11 shows the results in terms of number of repetitions (including collisions and lost packets). Results show that when the number of generated packets increases the number of collisions increases as well.

These results show, as stated earlier, high repetition rate for the protocols that do not apply a rendez-vous mechanism. Indeed, when a node sends a packet to a node which is trying to send a packet to another node on a different channel,

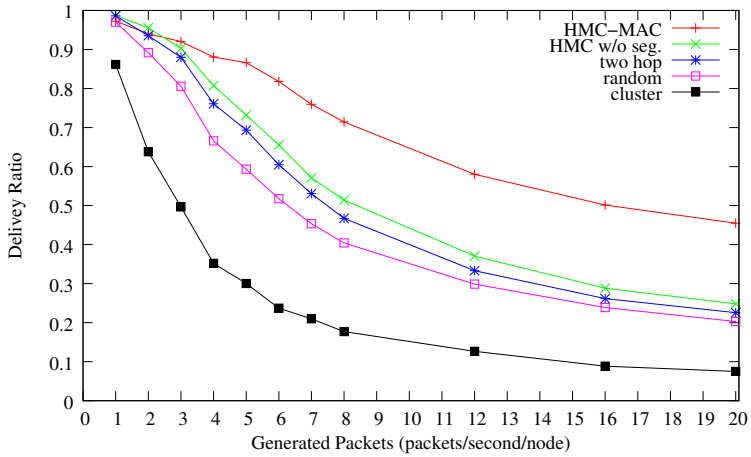


Figure 2.10: Delivery ratio at the sink for burst traffic.

this packet will be lost because the receiver is currently busy on a different channel. HMC-MAC protocol does not suffer from that problem, and thus, reduces the number of frame repetitions compared to the other methods. Consequently, HMC-MAC avoids wasting energy by reducing the number of repetitions.

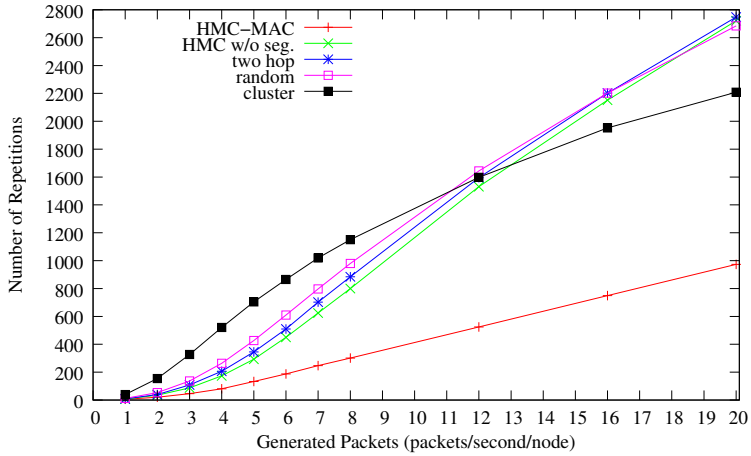


Figure 2.11: Number of repetitions for periodic traffic.

2.3.6 Queue Overflow

Figure 2.12 shows the results in terms of packet loss due to the queue overflow in all the nodes of the network. We observe high rate of queue overflow in HMC-MAC protocol because of the limited capacity of the packet queues especially on

nodes situated near the sink. Indeed, HMC-MAC is able to route packets with much less loss on the medium than other protocols. This leads to accumulation of packets in nodes that are situated near the sink and that have a high number of descendants. These nodes are thus unable to transmit these accumulated traffic and suffer from high rates of queue overflow. This phenomena is also known as the funnelling effect [51].

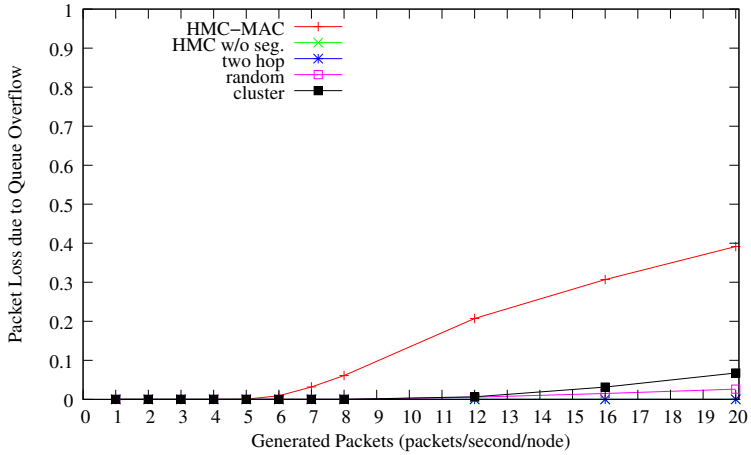


Figure 2.12: Packet loss due to queue overflow (periodic traffic).

Next section discusses techniques that allow nodes to avoid congested routes and reduce packet loss due packet overflow. These techniques use the end-to-end delay in order as routing metric.

Chapter 3

Load balancing

In the previous chapter, results showed that enhancing MAC performance might generate congestion and data loss due to queue overflow. This chapter starts with presenting the importance of load balancing in WSNs in order to avoid data loss caused by congestion and queue overflow, followed by a quick overview on existing techniques for achieving that goal. Part 3.2 presents a joint contribution, CoLBA (Collaborative Load Balancing Algorithm), with my PhD student Hamadoun Tall and co-supervisor Michel Misson. CoLBA is a routing protocol that we proposed in [4], it avoids queue overflow by dispatching traffic on underloaded nodes and employs a defence mechanism against data loss. Part 3.3 includes some of the main performance evaluation results of CoLBA.

3.1 Quick overview on load balancing routing protocols

In wireless sensor networks, each sensor node transmits its own sensing data and plays the role of a router to relay data coming from neighboring sensor nodes. In data collection applications, data is mostly destined to the sink node. In some cases and due to heavy traffic, this generates congestion and the queue storage capacity of sensor nodes cannot meet the increased traffic. This creates queue overflow and data loss. This phenomena often occurs in nodes close to the sink. Thus, the sink node is unable to process data that has made multiple hops and consumed time, bandwidth and energy. Consequently, it degrades the reliability of the network.

In a multi-hop data collection WSN, data is collected by sensor nodes and sent to the sink node via multiple intermediate nodes. In case of heavy traffic situation, depending on routing metrics and positions of nodes, some nodes might be part of the routing path more often than others. Thus, these nodes will suffer from congestion which leads to packet queue overflow and data loss. Congestion control is an important issue in data collection oriented applications. WSNs have limited bandwidth and nodes have reduced storage capacity which leads

to very limited buffer size to store data packets. Indeed, the limited bandwidth prevents nodes from transmitting at a rate that enables them to send all the accumulated traffic that they received. This leads to queue overflow especially in case of high traffic load once the amount of collected traffic is bigger than that buffer size of nodes.

Congestion avoidance approaches can be grouped into three categories: proactive, reactive and hybrid. In proactive approaches, such as [52, 53, 54], routing protocols integrate congestion avoidance in their normal process during route formations. In [52] transmission rates of nodes are regulated according to their popularity which is based on their position in the topology and their implication in monitored events, but this does not give an accurate estimation of the real accumulated traffic. In [53], disjoint multipath routes are formed in order to achieve load balancing, but this is not always possible in data collection scenarios. In [54], the proposed solution is based on MAC layer estimation and queueing delay in order to build less congested paths, but the estimation is not regulated according to current situation of the traffic flow. The main drawback of the proactive approach is that it does not include an additional mechanism that reacts to queue overflow when it eventually occurs.

In reactive approaches, such as [55, 56, 57, 58, 59], special mechanisms are applied only when congestion is detected. In [55] and [57], nodes monitor their input and output ratios and in case it exceeds a given threshold the sink node is alerted and orders certain nodes to reduce their sensing rate. By doing so, the network is not pushed to its limits and some underloaded nodes are not exploited. In [56], nodes exchange their incoming traffic rates up to 2 hops. When congestion appears, congested nodes have to ask their neighbors to change their routes. The difficulty of this method resides in the fact that the congested node is the one that should find a solution for other nodes. In [58], nodes that suffer from congestion alert their neighbors by using the ACK messages so that they change their routes. Neighbors choose alternative paths based on number of hops, residual energy and queue occupancy. The main drawback of this protocol is that it only takes local information into account without considering the end-to-end path, in addition ACK messages are modified and thus might be difficult to implement as proposed because it would not be IEEE 802.15.4 compliant. In [59], congestion is only avoided for high priority data which can only be useful in networks with multiple priorities. The main difficulty of reactive approaches is their capability of reacting fast enough to congestion appearance in order to find a solution before data loss becomes critical.

Hybrid approaches prevent congestion from happening and handle it in case it occurs, such as proposed in [60, 61]. In [60], the proposed solution uses a traffic regulation approach based on the application needs by asking part of the nodes to stop generating data in case of congestion. Nevertheless, this method cannot be applied for applications where every node has a different role in the network. In [61], nodes monitor their buffers occupancy and in case a threshold is reached their alert neighbors in order to change routes. The choice of an alternative route does not take into account buffer occupancy and thus might not always give a better solution. Hybrid approaches combine congestion monitoring with

congestion mitigation. This approach inspired our proposition CoLBA that I will describe it in the next section.

3.2 Collaborative Load Balancing Algorithm

The aim of CoLBA protocol is to avoid congestion and packet loss due to queue overflow. CoLBA balances the traffic load among underloaded next hop neighbors in the network. A node executing CoLBA algorithm has two main functionalities, the first one is monitoring the packet queue occupancy rate and alerting transmitting neighbors when the critical threshold is reached. The second one is finding a path towards the sink with the minimum queuing delay along the path. It is a collaborative protocol because nodes should cooperate to disseminate delay information to avoid congested nodes and also when a node receives an alert it should immediately change its next hop. In what follows, I will explain how the routing metric of CoLBA is computed and how queue overflow is avoided.

3.2.1 CoLBA metric computation

CoLBA uses a node based attribute metric for routing purposes that we call node delay. It considers the average time spent by packets in the queue. Each node is then able, according to its position in the topology, to estimate the time needed to reach the sink.

In order to compute the node delay, a node computes the difference between the queuing time and the dequeuing time of a received or created packet. This time represents the delay spent in the queue. In order to have an uptodate and representative delay, the average delay of the last ten packets is computed. In case the total number of dequeued packets is less than 10, the average is computed over the dequeued packets. Different nodes will have different node delays depending on the node position in the network topology.

1-hop neighbors of the sink transmit their data to the sink first, then compute their node delays. The delay of the 1-hop neighbors of the sink is equal to the path delay for these nodes. 1-hop neighbors broadcast the path delay to their neighbors. When 2-hop neighbors of the sink receive the broadcast messages, they choose the neighbor with the minimum path delay as their next hop towards the sink.

When a node sends its data packet, it can update its own node delay and add it to the minimum path delay. Then, it broadcasts the path delay from it towards the sink. Indeed, the path delay is broadcast each time it is updated. This process is repeated until all nodes in the network obtain a path delay towards the sink. Each node manages a list of its neighbors and the path delays from each neighbor to the sink node.

3.2.2 CoLBA approach to avoid queue overflow

Choosing the next hop towards the sink with the minimum path delay does not help to balance load nor to reduce queues overflow. In order to avoid queue overflow, CoLBA uses queue occupancy rate monitoring approach and random best next hop selection in a short list. Indeed, each node monitors its queue occupancy rate, when a certain critical threshold is reached, it means that the queue is close to be full, a broadcast message with a null path delay value is sent in order to react to queue overflow. When neighboring nodes receive this notification, this node will no longer be considered as a potential next hop by its neighbors. Once its queue occupancy rate drops, it sends a new broadcast message with a new not null path value allowing its neighbors to reconsider it as a potential next hop.

Choosing the neighbor with the minimum path delay as the next hope will make all nodes in the same communication range choose the same next hop. Thus, the neighbor with the best path delay will quickly reach the critical situation and all transmitting neighors have to change the path. In order to avoid this from happening, CoLBA uses a short list of neighbors with best path delays towards the sink. This list contains the neighbor with the smallest path delay, and all the neighbors having a path delay that is at most 2 milliseconds bigger. Thus, the short list might contain two, three, or more neighbors depending on the depth and the differences in the path delay. At any time a node has a packet to send, it should randomly choose a neighbor in the short list. This random mechanism helps avoid all nodes choosing at the same time the same next hop.

3.3 Performance evaluation

We evaluated the performance of CoLBA by means of simulation using Cooja simulator [62]. Cooja is a flexible Java-based simulator designed for simulating sensor networks running the Contiki operating system [63].

We compared CoLBA to a standard routing protocol that takes into account the shortest path in terms of number of hops (HopCount). We also compared 2 versions of CoLBA one that applies the random choice of next hop (CoLBA_withRandom) and one that only takes as a next hop the node with the smallest path delay (CoLBA_withOutRandom). Also note that the HopCount routing algorithm is used as a default routing protocol with CoLBA until enough data is exchanged in the network to have delay information.

To analyze the general behavior of CoLBA under different conditions, we have considered the following simulation settings. Sensor nodes are randomly scattered in an area of 200 x $200m^2$ with a transmission range of $35m$. We have evaluated scenarios with a single sink node, with a number of nodes N that varies in $\{10, 20, 30, 40\}$. The MAC method used is unslotted CSMA/CA of IEEE 802.15.4. We fixed the queue capacity to 8 packets. We have implemented unslotted CSMA/CA because the available version is not compliant with the IEEE 802.15.4 standard. Details about this implementation are given

in [31]. The radio propagation model is Unit Graph Disc Medium. As in previous sections, only part of the results will be presented, please refer to [4] for more results. The following results show the enhancements offered by CoLBA in terms of packet reception rate and packet queue overflow. Also, results of the overhead of CoLBA are presented.

3.3.1 Packet reception rate

In what follows, I will only present results for $1pkt/s$ and $10pkt/s$. $1pkt/s$ represents an underloaded network, whereas $10pkt/s$ represents an overloaded network.

Figure 3.1 shows that CoLBA gives comparable results to HopCount when the network is underloaded.

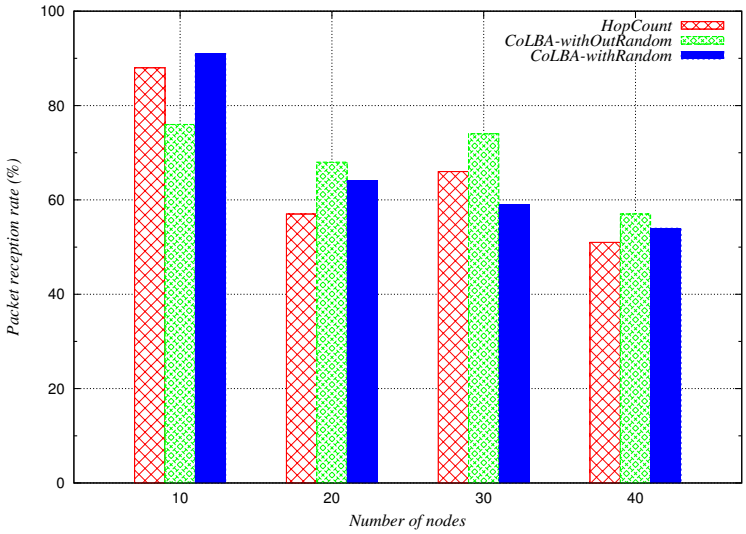


Figure 3.1: Packet reception rate for a traffic load of 1 packet per second.

Figure 3.2 shows that both CoLBA variants outperform HopCount and this is essentially due to the fact that sticking to the same route based on the hop count creates congestion. Results also show that CoLBA_withRandom is outperformed by CoLBA_withOutRandom for 20, 30 and 40 nodes with low traffic load. This is mainly due to the fact that choosing the next hop randomly have an overhead in term of number of hops and packets will travel more hops to reach the sink and thus are more likely to be lost due to collisions. With high traffic load CoLBA_withRandom outperforms CoLBA_withOutRandom and this is due to the fact that the random choice of next hop avoids congestion and allows a better load balancing.

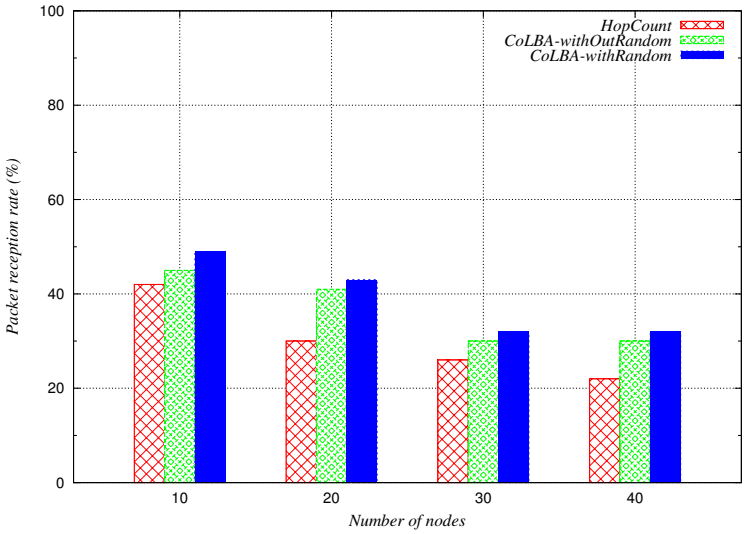


Figure 3.2: Packet reception rate for a traffic load of 10 packets per second.

3.3.2 Packet loss due to queue overflow

In order to ensure the effectiveness of CoLBA in avoiding queue overflow, we counted the number of packets that were dropped due to queue overflow for all 3 protocols. With 1 packet per second, we did not observe any packet dropped for all four network topology sizes with all three protocols. With $10pkt/s$ Figure 3.3 shows that the number of packets that were dropped using the HopCount protocol is much bigger compared to that of both variants of CoLBA. In addition, CoLBA with random choice of next hop gives better performance due to the fact that it ensures a better load balancing. With very high traffic load, 30 and 40 nodes at $10pkt/s$, CoLBA is unable to avoid queue overflows and this is due to the fact that the beacons that are sent with a null value for the path delay are lost due to collisions and thus neighboring nodes continue to send packets towards the node that is suffering from queue overflow.

3.3.3 Number of beacons

In this section we evaluate the overhead of each method in terms of number of generated beacons [1]. Figure 3.4 shows that HopCount outperforms both CoLBA variants which is an expected result because HopCount generates beacons in a periodical manner regardless of the path delay changes. On the other hand, CoLBA variants send much more beacons in order to announce path delay changes and thus overload the network with control traffic. This overhead

1. Only results for 5 packets per second are presented, 1 packet per second and 10 packets per second give comparable results.

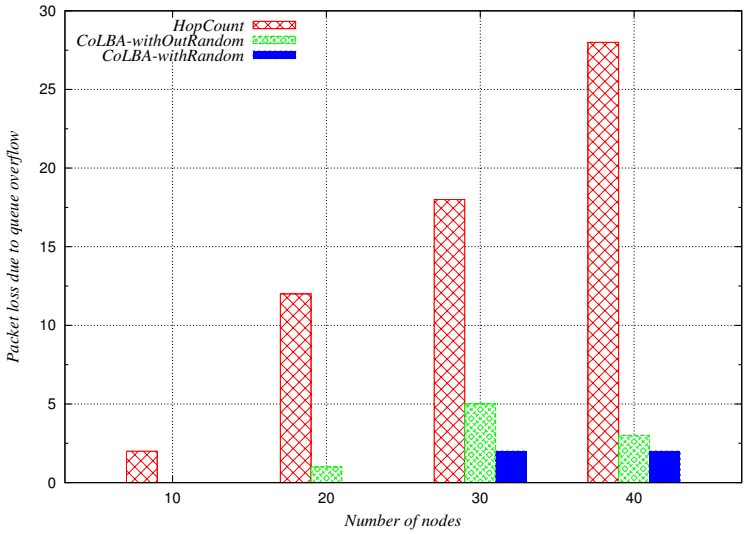


Figure 3.3: Number of dropped packets due to queue overflow with a traffic load of 10 packets per second.

contributes to collisions with data packets as well.

We are currently working on a prediction function that takes into account the traffic flow arriving in the packet queue and leaving the packet queue. This prediction function will help nodes better estimate critical queue occupancy and reduce beacon broadcasts.

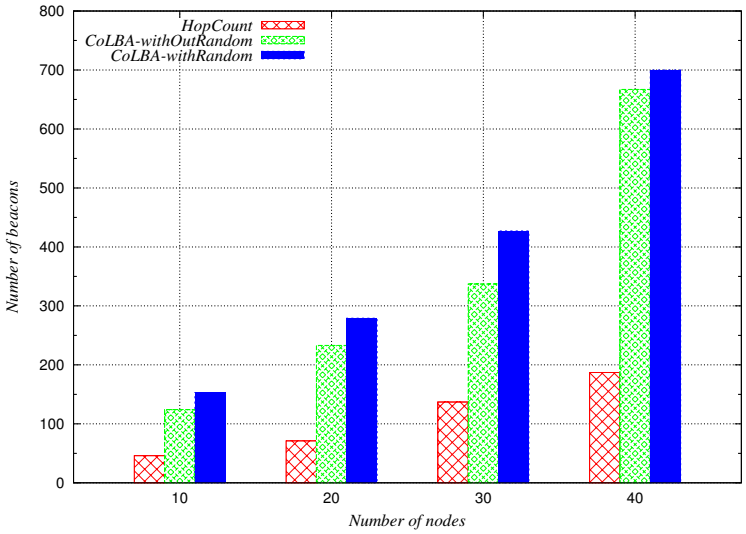


Figure 3.4: Number of generated beacons with a traffic load of 5 packets per second.

Chapter 4

Security in WSNs

Optimizing MAC and routing performance might not be enough for ensuring an operational network. Guaranteeing secure communications in wireless sensor networks is a must for critical applications in order to avoid malicious attacks. In what follows, I will present a quick overview on security management in WSNs followed by a description of the contribution and the main evaluation results. This work is mainly a joint work with my PhD student Ismail Mansour and colleague Psacal Lafourcade.

4.1 Quick overview on key management in WSNs

Key management in WSNs covers key establishment, key revocation and key renewal. In what follows I will briefly summarize the main contributions in this domain.

Internet of Things (IoT) has become a reality, more and more devices are deployed to monitor our environment and to interconnect embedded objects. IoT relies on Wireless Sensor Networks (WSNs) for ensuring connectivity between nodes on the lower level of the network architecture. In such context, sensitive applications often require cryptographic mechanisms in order to ensure security [64]. Hence, it is crucial to design secure communication mechanisms between nodes of the network. These mechanisms can be achieved based on modern cryptographic primitives.

Designing secure protocols is an error-prone task. A well known example is the famous flaw found on the Needham Schroeder protocol seventeen years after its publication [65]. During the last decades, several automatic tools for verifying security of cryptographic protocols have been elaborated by several authors, like for instance Proverif [66], Avispa [67] or Scyther [68]. These symbolic tools use the Dolev-Yao intruder model [69], that considers that the intruder is controlling the network and makes the perfect encryption hypothesis, meaning that it is possible to obtain the plain text of an encrypted message only if the secret key is known. The state of the art [70] shows that automatic checking methods are

now mature and efficient enough to be used in the design of security protocol in order to avoid such logical flaws.

Table 4.1 summarizes the main key establishment protocols in WSNs. The summary gives the type of cryptographic algorithms used, the type of cryptographic technique and the evaluation and verification methods.

Proposed scheme	Standard algorithms	Cryptographic technique	Simulation	Implementation	Verification
Perrig et al., 2002 [71]	yes	symmetric	none	Smart dust[72]	manual
Chan et al., 2005 [73]	not specified	symmetric	yes	none	none
Yu et al., 2009 [74]	not specified	symmetric	none	TelosB	manual
Munivel et al., 2010 [75]	yes	symmetric/ asymmetric	none	none	none
Yeh et al., 2011 [76]	yes	symmetric/ asymmetric	none	none	none
Zhang et al., 2012 [77]	not specified	symmetric	none	none	none
Al-mahmud et al., 2012 [78]	yes	symmetric/ asymmetric	none	none	none
Han et al., 2012 [79]	not specified	symmetric/ asymmetric	none	none	none
Manjusha et al., 2013 [80]	yes	symmetric/ asymmetric	Matlab	none	none

Table 4.1: Comparison with existing key establishment schemes.

Once secure communication channels are established in the network, several situations might occur ; a node can run out of battery, it can get destroyed or just leave the network, it can be captured, a new node can join the network, etc. When an intruder captures a node he can get all its secret data (including secret cryptographic keys). An attacker could also try to join the network and be part of the authenticated nodes of the network. Several Intrusion Detection Systems (IDS) have been proposed in the literature [81, 82] in order to detect such malicious behaviour. In general, an IDS either searches for signs of malicious activity in the network, or monitor the internal behaviour of nodes. Several works use signature-based or anomaly-based detection techniques. Based on the detections of an IDS, the next step is to revoke identified malicious nodes and to renew the cryptographic keys used by nodes of the network.

In this context, it is crucial to have efficient key revocation and renewal mechanisms in WSNs. In the literature, many key revocation protocols have been proposed for WSNs. In [83], authors made a survey and a taxonomy of the most relevant key management protocols proposed for WSNs. Key revocation is closely related to key distribution. Key revocation protocols can be classified into centralized and distributed protocols. In centralized mode, a central entity decides to revoke certain keys or nodes in the network. In distributed mode, a local voting procedure takes place to revoke keys or nodes. The latter might be faster and requires less control traffic, but it is generally more complex to implement.

Table 4.2 summarizes the comparison between the existing key revocation schemes and our proposition. The complexity of the protocols is not included in the table. As the table shows, and according to our knowledge, similarly to authentication and key establishment protocols, none of the existing revocation and key renewal protocols were verified using an automatic formal verification tool. In addition, most of the results in the state of the art are obtained through simulations or complexity estimation when evaluating the cost of the cryptographic scheme. Most of the existing schemes do not specify the cryptographic algorithms of encryption/decryption, leaving the choice of these algorithms to the application.

Proposed Schemes	Standard Algorithms	Cryptographic Technique	Simulation	Implementation	Verification
Chan *et al.* 2003 [84]	not specified	symmetric	none	none	none
Chan *et al.* 2005 [85]	not specified	symmetric	none	none	none
Chattopadhyay *et al.* 2012 [86]	not specified	symmetric	none	none	none
Chuang *et al.* 2010 [87]	yes	asymmetric	none	none	none
Dini *et al.* 2006 [88]	not specified	symmetric	none	none	none
Jiang *et al.* 2008 [89]	not specified	symmetric	none	none	none
Jolly *et al.* 2003 [90]	not specified	symmetric	yes	none	none
Purohit *et al.* 2011 [91]	not specified	symmetric	none	none	none
Wang *et al.* 2006 [92]	none	symmetric	none	none	none
Wang *et al.* 2010 [93]	not specified	symmetric	yes	none	none
Wang *et al.* 2007 [94]	not specified	symmetric	yes	none	none

Table 4.2: Comparison with existing key revocation schemes.

4.2 Description of the contribution

The originality of this contribution resides in the fact that it suites large scale multihop wireless sensor networks. Indeed, regardless of the number of hops separating the communicating nodes, the number of cryptographic operations is limited. We have implemented our protocols on TelosB motes in order to obtain the execution time and communication. Note that we used TelosB motes as a means for comparing the different protocols. The main objective is to present secure solutions using standard cryptographic algorithms and primitives publicly available on the Internet [1]. The chosen primitives can be replaced by more optimized primitives for better performance. Lightweight cryptographic primitives [95, 96] guarantee only a low level of security. Thus, they cannot be used in critical deployments. For instance, authors in [97] proved that they can break a lightweight block cipher for WSNs called *LBlock* using a personal computer within one hour [2].

In what follows, I will present some of the main protocols we have proposed for key establishment. For more details please refer to [5] for join protocols, [25] for multihop ad hoc key establishments and node authentication, [20] for evaluation of cryptographic primitives, [26] for revocation and renewal of keys.

4.2.1 Cryptographic Primitives and Notations

It is widely admitted that asymmetric encryption primitives based on exponentiation, such as RSA [99] or Elgamal [100], should not be used because sensor nodes have limited resources (battery and computation power). We use public key Elliptic Curve Cryptography (ECC), using parameters secp160r1 given by the Standards for Efficient Cryptography Group [101]. Our implementation of ECC on TelosB is based on optimized TinyECC library [102]. More precisely we use Elliptic Curve Integrated Encryption Scheme (ECIES 160 bits), the public key encryption system proposed by Victor Shoup in 2001 [103]. For all symmetric encryptions we use an optimized implementation of AES [104] with a key of 128 bits proposed by [105].

In what follows, we also use the following notations to describe exchanged messages in our protocols:

- I: a new node that initiates the protocol,
- R: a neighbor of node I,
- S: the sink of the network (also called *base station*),
- n_A: a nonce generated by node A,
- $\{x\}_k$: the encryption of message x with the symmetric or asymmetric key k,
- $pk(A)$: the public key of node A,

1. The evaluation is essentially a proof of concept and shows that the steps of each protocol can be implemented on low cost motes such as TelosB motes that are known for their low capacities in computation speed.

2. Recently a promising work [98] provided a solution to avoid such attacks by using code polymorphism. This method improves security at several levels in electronic devices.

– $sk(A)$: the secret (private) key of node A,
– $K(I, S)$ or $K(S, I)$: the symmetric session key between I and S,
– NK: the symmetric network key between all nodes of the network,
– $K_{DH}(N, S)$ or $K_{DH}(S, N)$: the shared symmetric key between N and S using the Diffie-Hellman key exchange without interaction described below.

Before deployment, each node N knows the public key $pk(S)$ of the sink and also its own pair of public and private keys, denoted $pk(N)$ and $sk(N)$ respectively. Based on ECC, we have that $pk(N) = sk(N) \times G$, where G is a public generator point of the elliptic curve. From $pk(N)$ and G it is difficult to find $sk(N)$, this problem is called *elliptic curve discrete logarithm problem* (ECDLP) [106, 107].

Using this material, each node N can compute a shared key with the sink S using a variation of the Diffie-Hellman key exchange without interaction, denoted $K_{DH}(N, S) = K_{DH}(S, N)$.

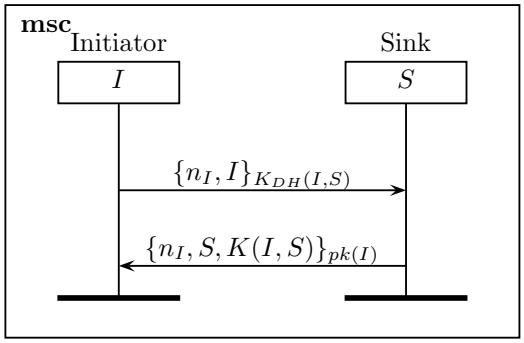
– The sink knows its own secret key $sk(S)$ and the public key $pk(N)$ of any node N. The sink computes $K_{DH}(N, S) = sk(S) \times pk(N)$.
– Node N multiplies its secret key $sk(N)$ by the public key of the sink $pk(S)$ to get $K_{DH}(N, S)$.

Both computations give the same shared key since: $K_{DH}(N, S) = sk(N) \times pk(S) = sk(N) \times (sk(S) \times G) = (sk(N) \times G) \times sk(S) = pk(N) \times sk(S)$.

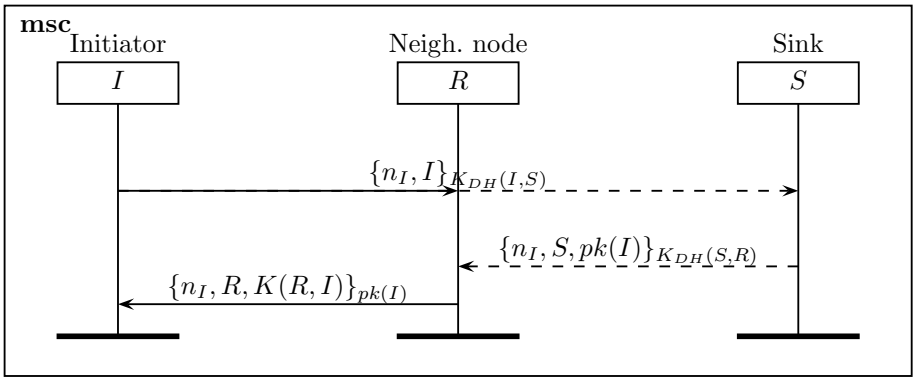
4.2.2 Key establishment

Figure 4.1 presents two key establishment protocols [5]. The first protocol, called *Direct Join to the Sink* (DJS), allows a node to join directly through the sink and is described in Figure 4.1a. In DJS, a new node I sends a direct request to S in order to establish a session key with it. Node I begins the join process by computing the symmetric key $K_{DH}(I, S)$ with the sink S. Then, node I generates a nonce n_I and adds its identity then encrypts it with $K_{DH}(I, S)$ and sends it to S. Upon reception, S computes $K_{DH}(I, S)$ to decrypt the request. Then, S verifies the identity of I and generates a new session key $K(I, S)$. The join response contains n_I, the identity of S and the new symmetric session key $K(I, S)$. The response is encrypted using $pk(I)$ and is sent to I. Only I is able to decrypt the response with its secret key $sk(I)$. Note that n_I helps I to authenticate S.

The second protocol, called *Indirect Join to the Sink* (IJS), allows a new node I to join the network through a neighbor node R that is already authenticated in the network. Node I sends an indirect request to S in order to establish a session key with R. Node R forwards without any modification the request to S through intermediate nodes that are trusted to route the request towards S. Only nodes I and S are able to decrypt the messages encrypted with $K_{DH}(I, S)$, and only R and S are able to decrypt the messages encrypted with $K_{DH}(S, R)$.



(a) DJS: Direct Join to the Sink. Node I joins directly the network by communicating directly with the sink S.



(b) IJS: Indirect Join to the Sink. Intermediate nodes between R and S forward messages without any encryption or decryption.

Figure 4.1: Key establishment protocols executed during the join process.

4.2.3 Multihop key establishment protocols

In this section I will present the protocols we proposed for establishing a shared key between any two authenticated nodes I and R of the network (not necessary in range). Protocol MSK_a, depicted in Figure 4.2a, uses the secure channels created between the sink and each node to communicate the public key of I and R. Notice that in our context the sink knows all the public keys of all nodes and a node only knows its public key and the public of the sink. The initiator node I builds a request containing the identity of node R and a nonce n_I. This request is encrypted with $K_{DH}(I, S)$ and is sent to S. The sink S sends:

- to I, the identity of R, a nonce n_S, the public key of R encrypted with the shared symmetric key $K_{DH}(I, S)$,
- to R, the identity of I, the same nonce n_S, the nonce n_I received from I and the public key of I encrypted with the shared symmetric key $K_{DH}(S, R)$.

Once these messages received, the two nodes are able to compute $K_{DH}(I, R)$ as follows:

- Node I computes $sk(I) \times pk(R) = sk(I) \times sk(R) \times G = K_{DH}(I, R)$.
- Node R computes $sk(R) \times pk(I) = sk(R) \times sk(I) \times G = K_{DH}(I, R)$.

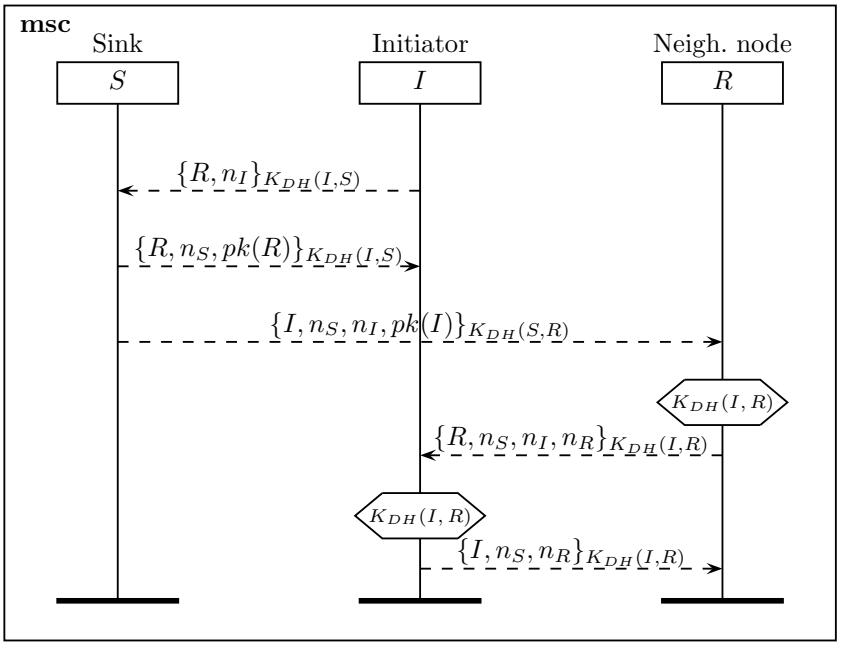
To ensure mutual authentication of R and I, node R generates a nonce n_R, then uses $K_{DH}(I, R)$ to encrypt its own identity, the two received nonces from S plus its own nonce n_R. This cipher is sent to I, without necessary passing by S. Node I verifies that the received nonce from R is the same as the one sent by the sink. Then it confirms that it correctly received the message by sending to R its own identity and the two nonces n_S and n_R, encrypted with $K_{DH}(I, R)$.

Notice that the computation of the new keys can be done by the sink in order to save some computations on nodes R and I. This version called MSK_b is depicted in Figure 4.2b.

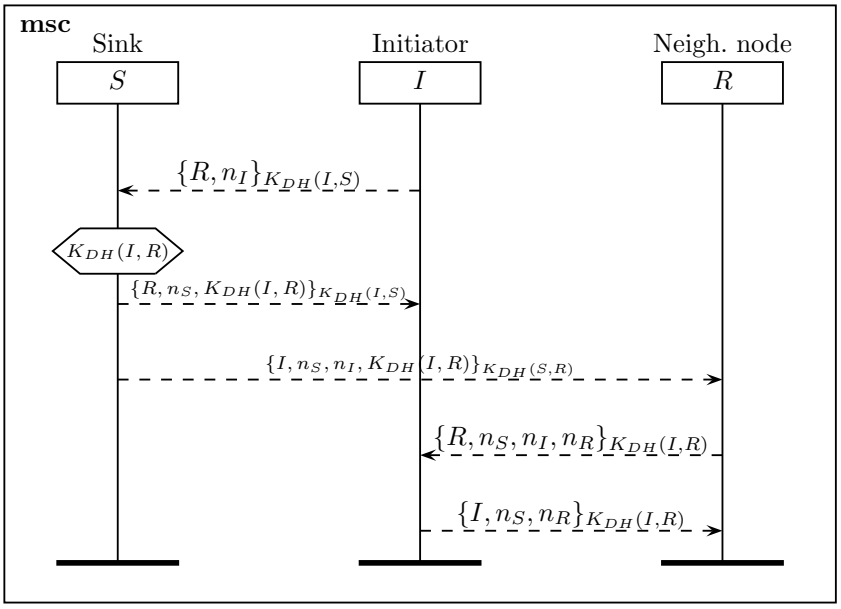
We also proposed protocols that do not use the sink but use instead a trusted intermediate node T to establish a new key. The main idea is to allow other nodes to authenticate new key establishment. This way we avoid exhausting the sink and we preserve energy of its neighbors that are relaying all the requests towards it. Doing so also helps to avoid traffic congestion around the sink. When other nodes share this role, traffic for key establishment will be distributed in the network.

A node T is considered as trusted by a node I if nodes I and T have at least one secret key in common. This secret key is previously established either during the join process or using protocol MSK. Node T might have the public key of nodes I and R, one of them or none of them according to the protocol that has served for the secret key establishment. In order to establish a secret key, an initiator node I tries first to find a common trusted node T with the responder R. In what follows, I will only describe the case where node T only has $pk(I)$ but not $pk(R)$, which we call protocol MSK_T.

According to protocol MSK_T (Figure 4.3), node I starts the process by sending a message to T encrypted with the secret key between I and T. Node T sends $pk(I)$ to R, then R sends its own public key to T in order to send it



(a) Protocol MSK_a.



(b) Protocol MSK_b.

Figure 4.2: Protocols for multihop shared key.

to I. Once I has $pk(R)$, both nodes I and T can execute the Diffie-Hellmen protocol and establish a secret key. Note that the last two messages are used to verify nonces and confirm the establishment of the shared key $K_{DH}(I, R)$. In addition, in order for node R to know if it needs to include its public key in the reply to T or not, it can keep a record of how it obtained the shared key with T and react accordingly, or we can add in the header of the message sent from T to R the identifier of the protocol used for the key establishment.

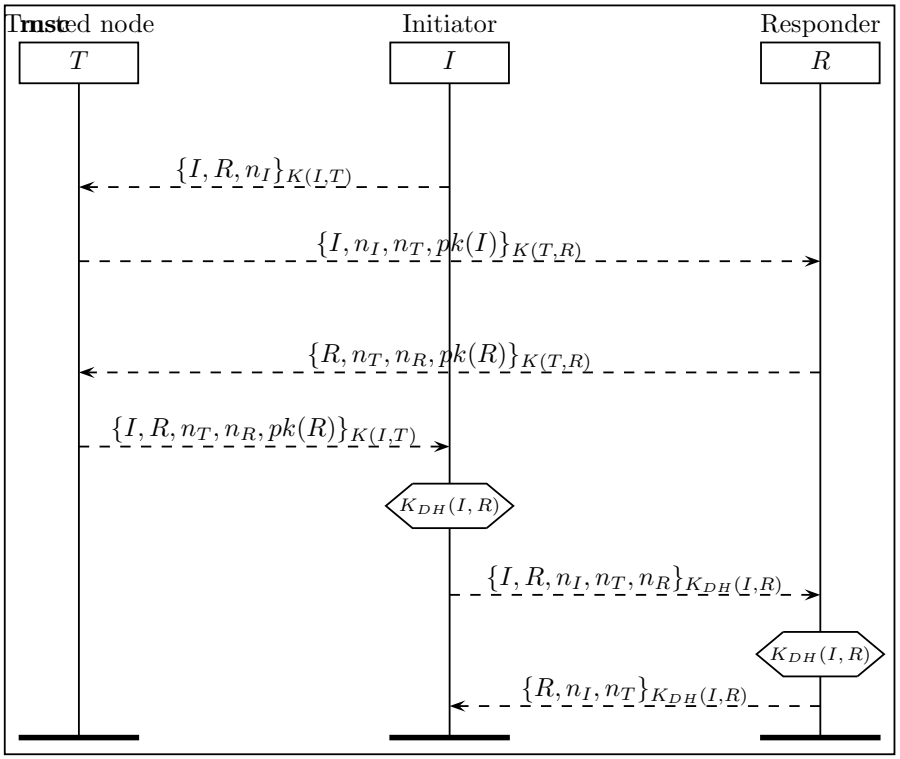


Figure 4.3: MSK_T: Multihop Key Establishment using a trusted node T to deliver public keys. T has $pk(I)$ but not $pk(R)$. $K_{DH}(I, R)$ is computed by the initiator I and the responder R.

4.2.4 Renewing Asymmetric Keys (RAK)

Each node N has several keys that should be renewed: a symmetric shared key between N and S ($K_{DH}(N, S)$), symmetric keys shared with neighbors and other nodes in the network, a pair of public/secret keys $(pk(N), sk(N))$, the public key of the sink ($pk(S)$) and a symmetric network key (NK). In what follows, I will only present protocols for renewing asymmetric keys (for other renewal protocols please refer to [26].).

In what follows, I present four protocols to renew asymmetric keys of the network. These protocols use the existing key infrastructure to securely replace the asymmetric keys between the sink and all nodes of the network. For this, the sink creates its own new public/private keys $(pk'(S), sk'(S))$ and a new pair of public/private keys $(pk'(I), sk'(I))$ for each node I in the network. Our four protocols (RAKnk$_a$, RAKnk$_b$, RAKdh$_a$ and RAKdh$_b$) are based on the same idea: First S securely sends $pk'(S)$ and the new pair of keys for node I; then node I replies by sending back its identity with the new shared key $K'_{DH}(S, I)$.

In Figure 4.4, protocols RAKnk$_a$ and RAKnk$_b$ are presented. The new public key of the sink $pk'(S)$ is broadcast to all nodes using the network key (NK). In the first protocol RAKnk$_a$, depicted in Figure 4.4a, the sink only sends to each node I the new pair of keys using $K_{DH}(S, I)$. Then I computes the new shared key $K'_{DH}(S, I) = sk'(I) \times pk'(S)$. In order to save computation time for node I, we proposed a second version RAKnk$_b$ described in Figure 4.4b, where the sink pre-computes $K'_{DH}(S, I) = sk'(S) \times pk'(I)$ without using the secret key of I.

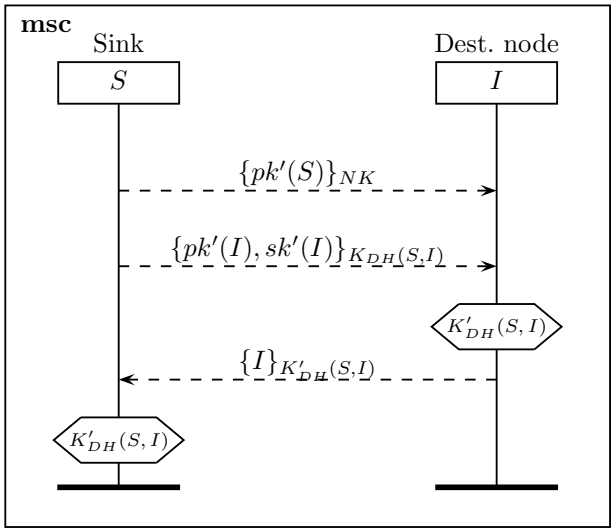
An alternative is to use the pre-shared key $K_{DH}(S, I)$ instead of NK in the distribution of $pk'(S)$. Using symmetric shared keys on each hop prevents an intruder that has the network key from learning the new key of the sink. Nevertheless this solution creates more traffic on the network since the transmission of the public key of the sink is not a broadcast using the network key but a unicast using a symmetric shared key between two nodes. For more details about this version please refer to [25].

4.3 Security Analysis

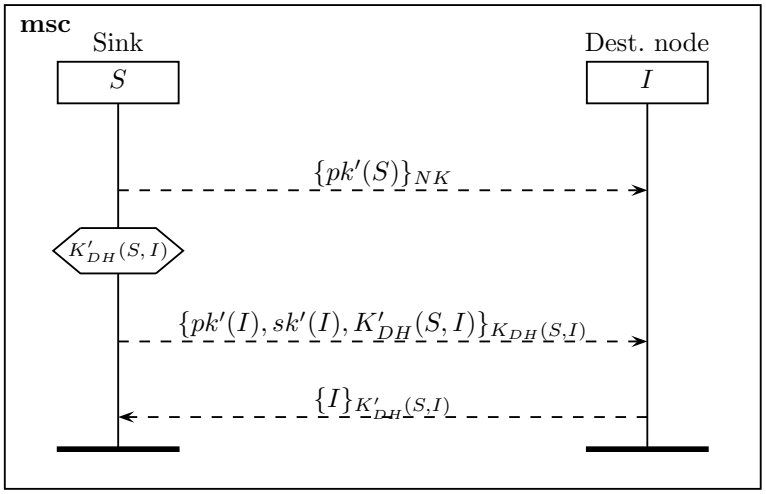
We verified automatically all our protocols using Scyther. Scyther concludes that all our protocols are secure. More precisely, we proved the secrecy of all sensitive data exchanged (keys and nonces) and also the authenticity of the communication. Our Scyther codes are available here [108]. The advantage of using an automatic verification tool, that considers a powerful intruder, is that we are sure that there exists no attack, including replay or man-in-the-middle attacks. In all our protocols, the authentication is ensured by using nonces in an appropriate manner, it also ensures the freshness of the messages to avoid for instance replay attacks. Moreover the tool guarantees that our protocols preserve the confidentiality of the sensitive data and the different participants communicate in an authenticated manner.

4.4 Experimentation results

In order to provide a proof of concept, we implemented each protocol on TelosB motes. These motes have a 8 MHz microcontroller with 10 Kb of RAM, 48 Kb of ROM and a CC2420 radio using the IEEE 802.15.4 standard. Our implementation of ECC is based on TinyECC library [102], on Elliptic Curve Integrated Encryption Scheme (ECIES) with a key of 160 bits, and on an op-



(a) Protocol RAKnk$_a$: S and I compute $K'_{DH}(S,I)$.



(b) Protocol RAKnk$_b$: S computes $K'_{DH}(S,I)$ and sends it to I.

Figure 4.4: Two protocols for renewing asymmetric keys of a node I, where S uses the network key NK to broadcast $pk'(S)$.

timized implementation of symmetric encryption AES [109] in CTR mode with a key of 128 bits. In order to explain why we choose AES with CTR mode and the 128-bit key k, we recall the mechanism of this scheme: let us consider a message m composed of k blocks $m_1||m_2||\ldots||m_p$, and an initial counter value IV randomly chosen. The cipher of the block m_i is $c_i = \{IV + i\}_k \oplus m_i$, where $\oplus$ denotes the bitwise exclusive-or operator. If you know IV and the key k, then you can easily recover from c_i the message $m_i = \{IV + i\}_k \oplus c_i$. When the size of the last block m_p is smaller than 128 bits it is usual to pad it with 0 up to 128 bits in order to have both operands with the same length to perform the bitwise exclusive-or. In this case, the size of the transmitted encrypted packets are always a multiple of 128 bits. But in CTR mode, we can just cut the $\{IV + p\}_k$ message to the size of m_p. Hence we can transmit an encrypted message that has exactly the same size as the original message, and therefore avoid any overhead in terms of transmission time. For example in protocol KR, if the list of revoked nodes and the nonce is l-bit long that is smaller than 128 bits (AES block size), it is sufficient to only transmit l bits.

Protocol	Name	Figure	Time with S (ms)	Time without S (ms)	Gain	Standard deviation (ms)
Join Protocols	DJS	4.1a	10112.62	4082.05	59%	78.09
	IJS	4.1b	10180.81	10049.45	1%	111.94
Multihop Shared Key	MSK_a	4.2a	6893.76	6631.91	4%	5.76
	MSK_b	4.2b	3682.53	301.42	91%	5.25
	MSK_T	4.3	-	7324.88	-	7.77
Renewing AsymKey	RAKnk_a	4.4a	6797.75	3436.24	49%	4.26
	RAKnk_b	4.4b	3646.05	254.62	93%	3.95

Table 4.3: Execution time the presented protocols.

For each protocol, we presented the results with and without the execution time of the sink, since in many applications the base station is a special node with extra resources. All results are the averages of 100 experiments of each protocol. We also provided the standard deviations for execution time including time of S. Notice that these values are small compared to the execution time of the protocol. These variations are normal according to the motes used, physical

parameters like 2.4 GHz interference, battery level, humidity, temperature etc. Moreover, the cause of the high standard deviation of join protocols is essentially related to the random number (that is of course different at each generation) that is used in multiplication operations in the asymmetric encryption. In fact, when the random number is small, the multiplication operations take much less time than what they take for a large random number.

Note the gain obtained by pre-computing keys by the sink. By generating the key on the sink we avoid consuming additional time and energy on the sensor nodes. In some cases it helps obtain a gain of around 90% if we consider that the sink is not time nor energy constraint.

Chapter 5

Coexistence

Optimizing protocols and securing communications might not be enough if the frequency bands are not available for establishing operational links. In this chapter, an in-depth analysis is presented on co-existence issues between IEEE 802.11 and IEEE 802.15.4 networks. This is joint work with my undergraduate student Kevin Verny, Eric Perrier from Electricity of France, and Michel Misson.

Wireless networks are more and more deployed in different areas of applications and in our everyday life. The WiFi standard, which is based on IEEE 802.11 standard [6], has been widely deployed in the past 25 years. The most used version of this standard uses the 2.4 GHz unlicensed ISM (Industrial Scientific and Medical) band and is based on a random medium access control that allows different WiFi networks to coexist even when they are working on the same channel or overlapping channels. Nevertheless, it is highly recommended to use 5-channel separation to avoid interference because WiFi channels are overlapping as it is shown in Figure 5.1. For example, channels 1, 6 and 11 in Figure 5.1 are highlighted as possible 3 non-overlapping channels.

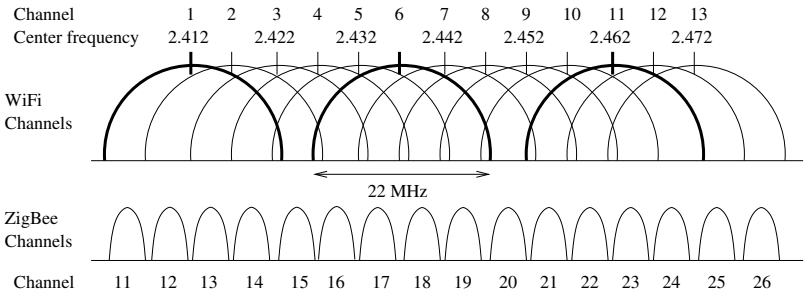


Figure 5.1: The overlap between WiFi channels from 1 to 13 and the ZigBee channels from 11 to 26 in the 2.4 GHz spectrum.

Another standard which has recently gained in popularity is ZigBee [34]. It is based on IEEE 802.15.4 standard [7]. ZigBee also uses the 2.4 GHz ISM band

and is often deployed in areas where WiFi is already installed. Other more recently approved wireless standards such as WirelessHART [110] and ISA100.11a [111], that are proposed for industrial wireless sensor networks, are also based on the the physical layer of IEEE 802.15.4 and work in the 2.4 GHz ISM band. Figure 5.1 also shows how IEEE 802.15.4 channels overlap with those of the IEEE 802.11. WirelessHART and ISA100.11a are supposed to be deployed in more controlled environments such as indoor industrial monitoring and control applications and they are mostly based on TDMA (Time Division Multiple Access) and frequency hopping. Unlike ZigBee which is essentially based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) for accessing the medium.

In most cases, these networks need to coexist in the same physical space and share the same bandwidth in the 2.4 GHz ISM band. The increasing number of applications using wireless technology is creating congestion in the 2.4 GHz frequency band and making the coexistence issue even more critical.

5.1 Quick overview on similar coexistence work

Many studies have been done to evaluate the effect of the coexistence such as [112, 113, 114, 115, 116]. They were limited to the Received Signal Strength Indicator (RSSI), the Packet Error Rate (PER), and the Link Quality Indicator (LQI).

Our study presents an analysis in great details of the behaviour of slotted CSMA/CA of IEEE 802.15.4 in the presence on a WiFi network. We investigate how WiFi affects the performance of IEEE 802.15.4 when it uses slotted CSMA/CA algorithm. An in-depth analysis of the behaviour of CSMA/CA is given according to the relative positions of IEEE 802.15.4 transmitters and receivers and WiFi nodes. We show that the effect of WiFi on the transmitters is not the same as on the receivers. In addition, we showed how the effect of WiFi on IEEE 802.15.4 depends on the traffic load of WiFi. We also measured the interference in overlapping channels and non-overlapping channels. We also proposed a new overhead estimation caused by the coexistence. [1]

5.2 Evaluation methodology

We conducted different experiments in order to measure the effect of WiFi on ZigBee [117]. All the experiments were done using Cisco Aironet access points and Texas Instruments (TI) sensor nodes that implement IEEE 802.15.4 slotted CSMA/CA with CC2420 transceiver [118]. WiFi traffic was generated without nearby IEEE 802.11b stations, RTS/CTS were not used, application layer acknowledgements were not used, and ERP-OFDM modulation with a short

1. This work has been done with the collaboration of EDF R&D. We would like to thank Kevin Verny for his important contribution to the realization of the experiments and Andre Misson for providing the experimental site.

preamble was used. We made modifications on the TI code in order to obtain the different timing elements. TI nodes were connected to a computer using a serial cable and timing indicators for the node activity were logged on the computer.

We concentrated results on aspects that were not studied in previously published. We studied the overhead of the coexistence in terms of additional delay that the ZigBee packets undergo before accessing the medium. We calculated the average delay for accessing the medium without the presence of interference and we considered that all additional average delays when a WiFi interference is present is an overhead generated by the coexistence. Thus, we computed the overhead according to the following formula:

$Overhead =$
$(ADwP - ADwoP) + AAF * (NbF/NbS) + AAS * ((NbS - NbR)/NbS)$, where

- ADwP (Average Delay with Perturbation) is the average medium access delay with the presence of WiFi interference,
- ADwoP (Average Delay without Perturbation) is the average medium access delay without WiFi interference,
- AAF (Average Access Failure) is the average time for an access failure to occur,
- NbF (Number of Failures) is the number of frames that were not transmitted due to failure to access the medium,
- NbS (Number of Successes) is the number of frames that were successfully transmitted,
- AAS (Average Access Success) is the average time for accessing the medium without errors,
- NbR (Number of Received) is the number of received frames.

Therefore,

- (ADwP - ADwoP) will give us the average additional delay due to interference from WiFi.
- AAF*(NbF/NbS) will give us the additional average time spent on trying to send frames that were not sent due to interference.
- AAS*((NbS-NbR)/NbS) will give us the additional average time spent on repeating frames due to interference.

In these scenarios, the ZigBee node that is being the object of interference will be suffering from an interference level at -65 dBm and the other node at -80 dBm in the first case. We have made the tests with 2 ZigBee traffic profiles. On one hand, a relatively low ZigBee traffic with one message of 30 bytes every second, each message is acknowledged and repeated 3 times in case the acknowledgement is not received. This traffic profile represents typical notification messages sent by sensors to a control center. And on the other hand, a very high traffic rate with one message of 30 bytes every 9 ms, messages are not repeated, but acknowledgements are kept for calculating the statistics. This profile represents the maximum transmission data rate with acknowledgements that we were able to generate using our motes without causing synchronization errors.

5.3 Experimentation results

Results in Figure 5.2 show that with the presence of WiFi interference, each ZigBee packet suffers between 30 ms and 55 ms of additional delay due to access delay, repetitions and packet loss. In addition, it is clear to notice that the overhead is higher when the interference is more significant on the transmitter. This is essentially due to the fact that when the transmitter is under high interference, it will struggle to send a frame and will keep waiting for an idle channel to be able to send it. This will cause significant delay before accessing the medium.

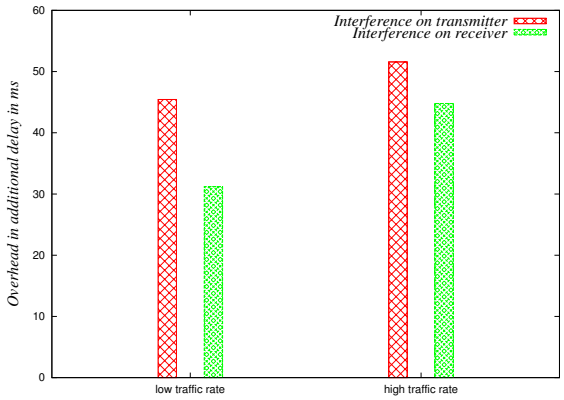


Figure 5.2: Overhead: average additional delay due to interference with TCP traffic.

In addition, a high rate ZigBee traffic is more likely to suffer from interference because it is more likely to find the medium idle to receive or send packets when the number of packets is very high.

We also tested the high data rate profile with UDP WiFi traffic with 1 Mbps and 5 Mbps over a 6 Mbps modulation. As Figure 5.3 shows, UDP generates less interference than TCP and the 1 Mbps generates less interference than the 5 Mbps. The overhead in additional delay reflects the consequences of these interferences.

In Figure 5.4 we show the overhead on the ZigBee activity when we use channels 20 to 26 while WiFi is active on channel 6 with an interference level at around -30 dBm.

We did a similar experiment with WiFi on channel 11 and ZigBee on channels 25 and 26. We started with an interference level at -55 dBm and then -65 dBm. Results show significant overhead on channel 25 and very little overhead on channel 26 when the interference level is at -55 dBm as shown in Figure 5.5. On the other hand, with interference level at -65 dBm there was no overhead on neither channels.

Overall, results showed that using ZigBee and WiFi in the same environment is possible if special precautions are taken into account. For example, placing

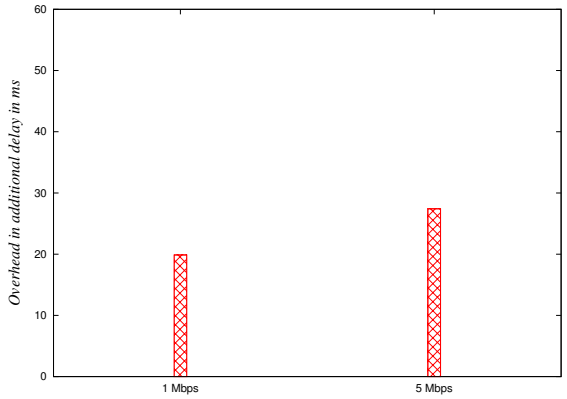


Figure 5.3: Overhead: average additional delay due to interference with UDP traffic.

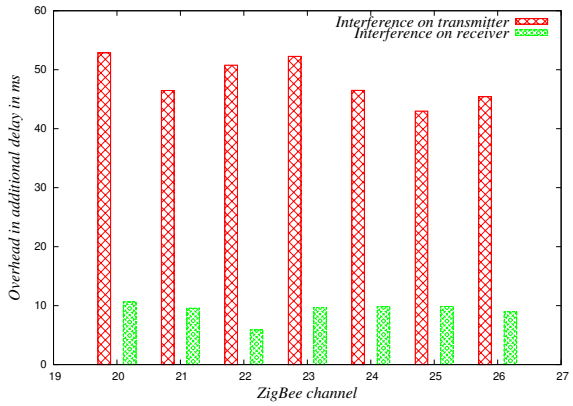


Figure 5.4: Overhead with very high interference and non-overlapping channels.

the ZigBee nodes in places where the RSSI level of WiFi is below -65 dBm when possible will significantly protect ZigBee traffic from interference. Choosing non-overlapping channels is always encouraged. And if possible, reduce WiFi activity in such a way to avoid occupying the channel with very high duty cycles; duty cycles below 33% are very much encouraged.

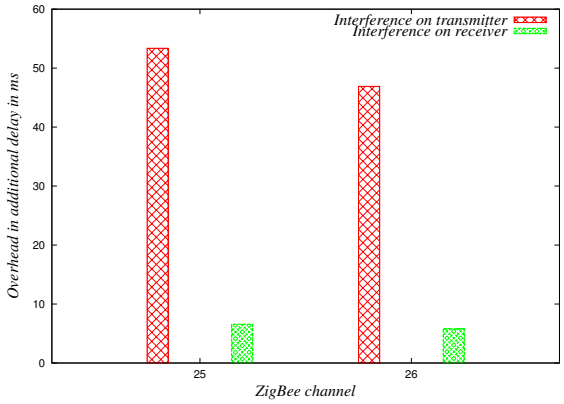


Figure 5.5: Overhead on non-overlapping channels 25 and 26 with -55 dBm WiFi interference.

Chapter 6

Ongoing research and perspectives

In this chapter, I will discuss open issues in multi-channel WSNs, describe my ongoing and conclude with perspectives.

6.1 Open issues in multichannel WSNs

Multi-channel WSNs are attracting more attention and standards have appeared proposing full protocol stacks based on multi-channel operations such as WirelessHART [110], ISA100.11a [111] and IEEE 802.15.4e [119]. The IEEE 802.15.4e standard based its Time Slotted Channel Hopping (TSCH) MAC protocol on TSMP [120] (which is a dynamic multi-channel MAC protocol) as well as both wireless industrial standards WirelessHART and ISA100.11a. In addition, ISA100.11a adopts a variation of TSMP which is a hybrid MAC for asynchronous medium access where timeslots of 250 ms are allocated for groups of nodes that contend using CSMA/CA to access the channel.

Although standards propose solutions based on multi-channel MAC protocols, networks still need to face major challenges in order to optimize channel usage and network performance. In what follows, I will discuss some of the open issues in multi-channel WSNs domain.

6.1.1 Wireless networks co-existence

Wireless networks are prone to interference. Interference could be generated from the other nodes from the same network, in this case we talk about internal network interference. In case interference are generated by nodes that are not part of the same network, we talk about external network interference [121]. The 2.4 GHz ISM band is used by other technologies like WiFi, Bluetooth and IEEE 802.15.4 based radio modules. An efficient MAC protocol should be able to avoid

external interference caused by nearby networks or equipment. Hence, multi-channel protocols should be environment aware. Channels used in the ISM bands may at any time be prone to external interference. MAC protocols that only consider internal interference will only perform well in protected environment where all nodes of the network are out of range of other external active elements. Techniques based on CSMA/CA approach might cope better in case of external interference. Using CSMA/CA has its drawbacks especially in energy and time wasting as discussed in [122]. On the other hand, special adaptation to TDMA approaches can be made in order to take into account external intermittent interference [123] but this will induce additional energy and time wasting as well.

6.1.2 Interfering channels

The goal of an efficient multi-channel protocol is to avoid intra-network interference. All sixteen channels offered by the IEEE 802.15.4 are theoretically orthogonal. Nevertheless, in practice, interference may be observed when adjacent channels are simultaneously used in very close range [124]. Hence, multi-channel MAC protocols must take this aspect into account during the channel allocation process which would have an impact on the channel distribution especially when dealing with a very dense network and multi-radio nodes [121].

6.1.3 Multi-hop synchronization

Most of the TDMA-based protocols suffer from unrealistic considerations for timeslot synchronization over a multi-hop network. For most cases, nodes that are used in WSNs must be low cost and energy efficient. This objective has several consequences on the design of a node on the hardware architecture and the choice of the components as well. This is why the existing solutions based on IEEE 802.15.4 are equipped with a relatively slow clock that provides a low capacity to manage time in a fine-grained way. Hence, the precision of both the transceiver and the processor is not enough to establish a synchronization using the time of arrival of the frames (such as the Start of Frame Delimiter (SFD) interruption offered by most of the IEEE 802.15.4 compliant transceivers). Some efforts have been made in order to enhance the precision of synchronisation [125]. One of the solutions to overcome this problem is to include guard time intervals as suggested by many standards such as [119] when considering synchronization over a multi-hop network which causes a loss of bandwidth and energy when frequently applied.

6.1.4 Diffusion support

The particularity of multi-channel environment makes broadcast a challenging task as discussed in [126]. One of the main approaches adopted for diffusion is to use a dedicated channel, as in [127], for that purpose and adopt a scheduling-based approach to make all nodes listen on this dedicated channel at the same

time. This approach has many challenges to tackle such as the periodicity of switching to the broadcast channel, the duration of broadcast intervals, the number of nodes participating to the broadcast (1-hop, 2-hop, 3-hop, network wide), etc.. Routing protocols, especially those that offer multiple routes to destinations, broadcast control information in order to keep an uptodate vision of the topology. Ensuring the reception of diffused information in a multi-channel network requires efficient coordination between nodes as discussed in the proposal of [128].

6.1.5 Compromise between overhead and optimization

Most deterministic multi-channel MAC protocols require high control traffic exchange between nodes in order to establish an appropriate slot/channel allocation which induces bandwidth and energy consumption overhead as shown in [129]. It is often based on neighborhood discovery and on the offered load of each node (data transmission rate). Adding to that, dynamic routing protocols might change the amount of packets one node is asked to route when routes are changed and topology changes as discussed in [130]. Hence, in order to adopt a fair timeslot allocation, these information must be accurate and updated when needed to avoid overloading nodes that do not have enough timeslots or underloading nodes with available unused allocated timeslots. Evaluating the overhead caused by a network protocol is often not measured but remains an important aspect that should be taken into account as shown in [131].

6.1.6 Mitigating control traffic

Each protocol has its own control traffic. For example, control messages are usually generated by the MAC layer for channel allocation purposes and by the network layer for routing information exchange. Indeed, when changes in the network topology occur, the channel allocation and the routing information should be updated. Generating two types of control messages for maintaining channels and routes can produce an important overhead and overload the network. Finding a way to mitigate control traffic by exploiting the same control traffic by different protocols should help reduce overloading the network and thus enhance its performance. This aspect is not investigated enough in the current literature and is one of the key optimizations of CoLBA [4] where a single control message is in charge of maintaining routes and allocating channels.

6.1.7 Application effect on the protocol design

Designing a generic MAC protocol that suits all application profiles demands a great compromise between performance and suitability. This was the case of the famous CSMA/CA of IEEE 802.11 standard [6] (that has evolved ever since essentially thanks to enhanced capacities on the physical layer [132] and [133]). When dealing with a data collection application profile, it is clear that slot reservation and allocation can be easily established to route data towards the

sink in an optimal way. On the other hand, when dealing with applications where any node can be a destination, slot allocation would be more complex as traffic might travel in all directions or to more than one destination [134]. The cross-layer design between the application profile and multi-channel slot allocation algorithm is an open research topic that helps adapt the mechanism to better suit traffic flows.

6.1.8 Security related issues

Wireless communications facilitate enormous opportunities to modern computing world where not only humans but also objects and sensing devices can communicate and collaborate with each other. Billions of connected objects, what is now known as Internet Of Things, will create a business of hundred billion of euros. Wireless sensor networks are part of this new technology with its own well known energy efficiency constraints.

In order for these communications to be exploited, security should be provided on all levels. Application level by protecting the exchanged data from eavesdropping and manipulation for example, and protocol level by preventing malicious nodes from penetrating the network and executing ad hoc attacks. Issues such as node capturing [135], intrusion detection [136] and fault tolerance [137] are still facing challenges in order to ensure malicious free networking.

6.2 Short term perspectives

In what follows I will highlight my current research topics.

6.2.1 Load balancing for multichannel protocols

When dealing with high data rate wireless sensor networks, load balancing becomes a major issue. Nodes have inherently low storage capacities, thus they need to empty their buffers in order to avoid queue overflow. When a multi-channel MAC protocol is enhanced with a TDMA approach it is usually based on time segmentation which forces nodes to wait for predefine intervals in order to send their traffic. This mechanism, although it avoids collisions, generates traffic accumulation on nodes that are close to sink in a typical data collection network.

In order to avoid this phenomena, load balancing techniques that were proved efficient in section 3 can be used in a multi-channel network. Most of the existing protocols including CoLBA are evaluated in single channel WSNs where traffic load is not very high and all nodes are communicating on the same channel. In multi-channel WSNs, traffic load will be higher than single channel networks. Hence, results will most certainly be different. Moreover, the context of multi-channel is different than that of the single channel. We need to adapt or to propose efficient load balancing approaches that take into account multi-channel communications.

6.2.2 Mobility management

Mobility and dynamic topologies make routing and resource management in a wireless sensor network a complicated issue [138, 139]. When links are broken due to nodes changing positions or environment changes, nodes might become temporarily unreachable. This issue has been studied in [140, 141] where we worked on an extension of MaCARI that supports mobility for part of the network. We are currently working on extending this work in order to support mobility in a multi-channel network.

6.3 Long term perspectives

With the emergence of the Internet of Things era, wireless protocols will require more enhancements and optimization in order to cope with the limited available bandwidth [142]. New protocols and new technologies are appearing every year such as the new versions of WiFi that support IEEE 802.11ac [132] and WiGig with IEEE 802.11ad [133]. In what follows, I will describe research aspects that I will be investigating and that should also occupy the community for the coming years.

6.3.1 Dynamic and adaptive wireless protocols

Most wireless network standards operate in the unlicensed ISM bands. New frequency bands are made available and standards are coping in order to exploit these new frequencies. It is predicted that communicating objects will exceed 50 billion devices by 2020 [142]. This excessive number of communicating devices will make issues such as coexistence and robustness much more challenging.

Communicating protocols should be able to adapt to unexpected congestion and to intelligently choose convenient frequencies in terms of quality of service. MAC protocols based on CSMA/CA will be more suitable for such environment where networks cannot predict traffic generated from neighboring nodes when communications share the same frequency band. In addition, IEEE 802.11ac [132], for example, uses MIMO technology and beamforming in order to achieve gigabits per second throughputs. Beamforming is very suitable for reducing interference by controlling the beam of signals when sending unicast traffic.

6.3.2 Secure protocol stack

Wireless networks are known to be more vulnerable to attacks because of the fact that devices share the same public medium especially in the unlicensed ISM bands. This vulnerability concerns applications as much as networking protocols. There has been many contributions for securing routing protocols in wireless sensor networks [143] and new protocols are proposed every year [144, 145, 146]. Security issues can be dealt with on the MAC layer as well [147], some concentrated on security aspects related to nodes exhaustion [148].

Securing the entire network protocol stack by securing each protocol independently is inefficient. In my future work I will concentrate on means that ensure security on all levels of the stack with minimum cryptographic operations.

Chapter 7

Teachings

I started my teaching career in 2007 at the department of Networking and Telecommunications of the University Institute of Technology (IUT for *Institut Universitaire de Technologie*) of University of Auvergne. I started as an assistant temporary teacher and became an Assistant Professor in 2011 at the same department. Since 2014, I started giving a course on wireless local networks for Master's student at ISIMA engineering school. Since 2015, I started teaching network services security and WiFi configuration at ISIMA as well. In what follows, I will highlight my contributions and the administrative responsibilities that I have had throughout my career.

7.1 Contributions

I have meanly taught courses on networking and security. From introduction to networking, network services, WiFi deployment, socket programming, wireless sensor networks, security of network services and network security. I have published two academic papers on wireless sensor networks [149] and DNSSEC [150] in the proceedings of Networking and Telecommunications workshops of 2010 and 2014.

7.1.1 DNSSEC

Domain Name Service is currently being upgraded to its secure version DNSSEC [151]. DNSSEC uses public key cryptography to ensure integrity and authenticity of DNS Resource Records. I took the initiative to include DNSSEC in the Networking and Telecommunication program at the bachelor level. After explaining the fundamentals of DNS architecture, operations and resources, I explain in details the cache poisoning attack and the Kaminsky exploit in order to give credit to DNSSEC and the solution that was found to protect DNS servers. During the lab sessions, I have put in place a detailed subject during which students spend about 9 hours in order to install, configure and secure a

DNSSEC server.

7.1.2 Firewalls

I have put in place 21 hours of laboratory sessions around firewall configurations. Students use Cisco ASA5505 firewalls and Stormshield firewalls, which are the most used firewalls in France. During these sessions, students explore and configure all types of Network Address Translation (static, dynamic, PAT), filtering policies and secure tunnel configuration.

7.1.3 Access Points

I have put in place 21 hours of WiFi network configuration including basic wireless local area network creation, wireless VLAN management, wireless network expansion, authentication and client management. Students use Cisco Aironet access points during these sessions, which is one of the most popular professional access points around the world [152].

7.2 Responsibilities

7.2.1 Networking head teacher

I was appointed head teacher of networking modules at the department of Networking and Telecommunications. My role is to make sure that networking courses respect the national program committee recommendations, find external teachers primarily from the industry, intervene when necessary for helping new teachers in the networking courses.

7.2.2 Member of department council

I am an elected member of the department council since 2009. As a member of the council I take part in all the decisions concerning the policy of the department concerning the evolution of the courses, internal organisation, recruitment policy, etc.

7.2.3 International Relations correspondent

In 2012 I have initiated and helped in establishing a collaborative agreement between Université d'Auvergne and University of Balamand of Lebanon. This effort in addition to my communication skills in English has earned me the position of International Relations correspondent of the IUT at the University d'Auvergne in the start of 2015. Since then, I have been helping colleagues in establishing and maintaining international relations with academic and industrial partners for students and teachers exchange programs in addition to research collaborations.

Chapter 8

Collaborations

In this chapter, I will briefly describe the collaboration that I was involved with. I have collaborated with members of our research team, as well as other research teams and Universities in France, Lebanon, Canada and Germany.

8.1 Joint work with members of LIMOS

I have been member of Networks and Protocols team of LIMOS since 2006 where I did my Master's degree internship. Throughout the years I collaborated with members of Networks and Protocols on specific topics such as detailed evaluation of the deference mechanism of slotted CSMA/CA of IEEE 802.15.4 standard with Nassima Hadid [153], simulation and evaluation of packet exchange between priority queues in a multi-stack architecture with Alexandre Guitton [154].

I have also collaborated with Pascal Lafourcade on security issues related to Wireless Sensor Networks [23, 22, 21, 23, 26]. Pascal is specialized in security verification and our collaboration is expending.

8.2 French collaborators

8.2.1 French industrials

Thanks to my participation in OCARI and SAHARA projects, I have had the opportunity to establish collaborations with industrial partners.

After the end of OCARI project we have worked on extensions of OCARI with EDF R&D. This work lead to a prototype of the OCARI protocol stack which was presented at EDF in December 2011. This event was highly promoted by EDF and partners of EDF were invited to assist to the demo.

I have also been contacted during 2011 by EXERA group to provide an analysis of industrial wireless sensor networks solutions, mainly ISA100.11a and

WirelessHART. This was done under a contract between the EXERA group and University of Auvergne.

SAHARA project aimed at defining and developing a WSN protocol stack that takes into account high data rate in a multihop network topology. The proposed solution was a compromise that covers all the needs of industrial partners. As a partner, the CNES wanted a more specific protocol stack that suites better their needs. This resulted in joint project funded by the CNES. This project is ongoing.

8.2.2 French research teams

I have had the opportunity to collaborate with the research team of Pascal Minet from Inria Requencourt on issues related to joint projects (OCARI and SAHARA) [19, 155]. Pascal's team is specialized in routing and network optimization in wireless networks.

I have also collaborated with the research team of Thierry Val of IRIT on issues related to MAC protocol optimizations as we were partners in the OCARI project [10, 13, 14].

8.3 International partners

Throughout my career, I have established and participated to international collaborations on academic and research levels. In what follows, I will briefly describe each collaboration.

8.3.1 University of Balamand

I have put in place in 2012 a cooperation between University of Auvergne and University of Balamand of Lebanon. This cooperation was put in place with the collaboration of Dr. Joel Toussaint of University of Auvergne. The main objective of this cooperation was to exchange students and expertise in the domain of networking with the Faculty of Technology of the University of Balamand.

In 2013, we were invited, Joel Toussaint and myself, to form the teachers and technical staff of the Faculty of Technology on Telephony over IP and Wireless LAN technologies. During the same year, we have invited Dr. Gilbert Habib for 2 weeks during which we collaborated on Wireless Sensor Networks issues. This collaboration gave birth to a publication [141]. Since the start of the cooperation, the University of Auvergne has received 3 second year level students for internships on subjects related to wireless communications.

8.3.2 Lebanese University

I was invited by the Lebanese University in 2010 to give a course on Wireless Networking with Michel Misson to Master's students of Technologies of Medical

and Industrial Systems (TSMI). This invitation was the initiative of Dr. Bassem Bakhache with whom we collaborated later on in the organisation of ICWCUCA 2012 in Clermont-Ferrand.

Following the course, we have offered 2 Master level internships in Clermont-Ferrand for students of TSMI. One of the internships gave place to a publication [140].

8.3.3 Lebanese American University

I started collaborating with the Lebanese American University (LAU) in 2013. We are working together on issues related to VANETs and security in wireless communications. Azzam Mourad was a visiting professor at University of Auvergne during June 2014.

We are partners in an international project funded by the Lebanese CNRS, the LAU University and the Natural Sciences and Engineering Research Council of Canada (NSERC). The project is entitled Intelligent Transport and Vehicular Technologies [156]. It addresses the problems pertaining to intelligent transport and vehicular technologies within limited and basic infrastructure environments.

8.3.4 University of Quebec in Abitibi-Temiscamingue

Our research team has been collaborating with the University of Quebec in Abitibi-Temiscamingue (UQAT) since the 1990s. In this context, I have been involved on several occasions in collaborations with UQAT. In 2012, we closely collaborated in organizing the third edition of the International Conference on Wireless Communications in Unusual and Confined Areas (ICWCUCA). In 2015, Hamadoun Tall, a PhD student under my supervision, had obtained a budget to spend one month in Quebec to collaborate with Nadir Hakem on issues related to traffic congestion management in WSNs. This budget had been obtained thanks to Samuel de Champlain project managed by Alexandre Guitton and Nadir Hakem.

8.3.5 Marie Curie-Skłodowska University of Lublin

Bogdan KSIEZOPOLSKI is a research at Marie Curie-Skłodowska University of Lublin that visited LIMOS in September 2013. He works on security issues in wireless networks. We have collaborated on evaluating the cost of security protocols in large scale wireless sensor networks [24].

8.3.6 Technical University of Dresden

My cooperation with the Technical University of Dresden has started with the invitation of Dr. Waltenegus Dargie by our research team in 2011. Following several meetings between 2011 and 2014. We submitted a proposal to the 2015 H2020 European program entitled ASQUAL (Adaptive and Scalable Water Quality Monitoring System). The project included partners from Germany

(Technical University of Dresden), Finland (University of Turun Yliopisto), Ethiopia (Ethiopian Institute of Water Resources, Addis Ababa University), Tanzania (University of Dodoma), and Nigeria (University of Lagos-Unilag).

8.3.7 Dhurubhai Ambani Institute of India

This is a recent collaboration that will start in 2016 in the context of DST-INRIA-CNRS research project program between LIMOS and Dhurubhai Ambani Institute of Information and Communication Technology (DA-IICT). The project is entitled Study of privacy, accountability and ownership in Internet of Things. Its aim is to investigate the design of new primitives, protocols and formal methods for establishing the security and privacy of IOT. It is a 3-year project that funds the involved students and researchers accommodation and travel expenses between India and France.

Appendices

Annexe A

Long French Resume

Nom : Chalhoub
Prénom : Gérard
Année de naissance : 1982
Courriel : gerard.chalhoub@udamail.fr
Etablissement d'affectation : Université d'Auvergne
Grade : Maître de Conférences
Section CNU : 27
Domaine scientifique : Sciences et technologies de l'information et de la communication

A.1 Thèmes de recherche développés

- Protocoles MAC et Routage pour les réseaux de capteurs sans fil
- Amélioration de la robustesse dans un réseau de capteurs sans fil
- Prise en compte de la mobilité dans un réseau de capteurs sans fil
- Interférences et cohabitation de différentes technologies sans fil
- Simulation et maquettage de protocoles réseaux pour les réseaux de capteurs sans fil
- Sécurisation des communications dans un réseau de capteurs sans fil

A.2 Responsabilités Programmes (ANR, Europe, FUI, Région)

- Participation au projet ANR OCARI 2007-2010 (partenaires : EDF, DCNS, INRIA, LRI, LATTIS, Télit), contribution : proposition et étude d'un protocole MAC économe et déterministe pour les réseaux de capteurs sans fil industriels, responsable de la réalisation d'un démonstrateur OCARI.
- Participation au projet FUI SAHARA2 2011-2015 (partenaires : EADS, Astrium, BeanAir, Eurocopter, Oktal SE, Reflex CES, Safran Engineer-

ing Systems, CNES, ECE, EPMI), contribution : proposition et étude d'un protocole MAC économe en énergie, robuste et répondant aux applications à haut débit pour les réseaux de capteurs sans fil installés dans des aéronefs, réalisation d'une maquette de faisabilité des protocoles MAC et routage proposés.

A.3 Responsabilité de Contrats ou Partenariats Industriels

- Avec EXERA 2012 : suite à une sollicitation du groupe EXERA, j'ai été responsable d'une étude comparative entre les deux standards sans fil industriel WirelessHART et ISA100.11a.
- Avec EDF et Beanair 2011-2012 : responsable d'une étude et évaluation de la cohabitation des normes IEEE 802.11 et IEEE 802.15.4.
- Avec EDF 2010-2011 : suite au projet OCARI, j'ai été responsable des contrats d'amélioration du réseau OCARI et de la réalisation d'un démonstrateur OCARI.
- Avec le CNES 2016-2017 : responsable d'une étude par simulation d'un réseau sans fil réactif et robuste répondant aux contraintes de déploiement dans les lanceurs.

A.4 Responsabilités de Partenariats Internationaux

- Partenaire et membre de l'unité de recherche ARU-ITVT "Associated Research Unit on Intelligent Transport and Vehicular Technonolgies" (membres : CNRS libanais, LAU, Ministère libanais des affaires intérieures, l'Université Libanaise, l'Université Américaine de Beyrouth, Khalifa University des Emirats Arabes Unis, ETS de Quebec Canada, Concordia University de Canada, Team International Lebanon) : unité de recherche portée par l'Université Américaine de Liban et financée par le CNRS libanaise, NSERC du Canada et l'Université Américaine de Liban. Rôle : exploitation des données réelles issues des véhicules pour simuler des protocoles de communication permettant une meilleure gestion de trafic routier
- Etablissement de convention de collaboration entre l'Université d'Auvergne et l'Université de Balamand de Liban : échanges d'étudiants et d'expertise dans le domaine des réseaux.
- Collaboration en cours de mise en place avec l'Université Américaine de Liban (LAU) : rapprochement pédagogique pour la création d'une formation de technologie à l'Université LAU. Ce rapprochement permettrait de consolider les collaborations initiées avec cette université dans le cadre de l'unité de recherche ARU-ITVT.

A.5 Encadrements

Stage de master

– Stage de fin d'étude de Antoinette Mouawad 2010 : Prise en compte de la mobilité dans un réseau de capteurs sans fil. Co-encadrée avec Michel Misson. Taux d'encadrement 90

Thèses soutenues

– Thèse de Ismail Mansour 2010-2013 (financement Région/FEDER) (qualifié CNU 27) : Contribution à la sécurité des communications des réseaux de capteurs sans fil. Encadrement mixte. Taux d'encadrement 50
– Thèse de Rana Diab 2011-2015 (Financement projet FUI SAHARA2) : HMC-MAC : un protocole MAC hybride et multi-canal pour les réseaux de capteurs sans fil. Co-encadrée avec Michel Misson. Taux d'encadrement 80

Thèses en cours

– Thèse de Hamadoun Tall 2014- (Financement Région/FEDER) : Répartition de trafic équitable dans un réseau de capteurs sans fil multi-canal. Co-encadrée avec Michel Misson. Taux d'encadrement 80
– Thèse de Jinpeng Wang 2015- (Financement Région/FEDER) : Impact de la mobilité et du déploiement en espaces confinés sur les réseaux de capteurs sans fil. Co-encadrée avec Michel Misson. Taux d'encadrement 80

A.6 Activités diverses liées à la recherche

– Co-chair du TPC de la conférence internationale ICWCUCA 2012.
– Membre du TPC des conférences suivantes : WiSEE16, PEMWN16, NTMS-16, WINSYS16, ICETE15, WCCS15, WINSYS15, CSDI15, SDTA14, WCC-S14, WINSYS14, PIMRC12, ICWCUCA12, ICCS12, JNCTT11.
– Relecteurs pour différents conférences et journaux scientifiques.
– Rapporteur en tant qu'expert international sur la thèse de doctorat de Leovigildo Sanchez Casado intitulée "Anomaly-based multi-layer intrusion detection for MANET environments" de l'Université de Granada, Espagne

A.7 Production scientifique

Revues Internationales

– Hamadoun Tall, Gerard Chalhoub, Michel Misson, Implementation and performance evaluation of IEEE 802.15.4 unslotted CSMA/CA protocol on Contiki OS, Annals of Telecommunications, juin 2016
– Gerard Chalhoub, Eric Perrier de La Bâthie, Michel Misson, Overhead caused by WiFi on ZigBee networks using slotted CSMA/CA, Journal of Networks, 2016, volume 11, numéro 2

– Ismail Mansour, Gerard Chalhoub, Pascal Lafourcade, Key Management in Wireless Sensor Networks, Journal of Sensor and Actuator Networks, septembre 2015, volume 4, numéro 3
– Gerard Chalhoub, Rana Diab, Michel Misson, HMC-MAC Protocol for High Data Rate Wireless Sensor Networks, International Journal on Electronics, juin 2015, volume 4 numéro 3
– Ismail Mansour, Gerard Chalhoub, Pascal Lafourcade, Evaluation of Secure Multi-Hop Node Authentication and Key Establishment Mechanisms for Wireless Sensor Networks, Journal of Sensor and Actuator Networks, septembre 2014, volume 3, numéro 3
– Rana Diab, Gerard Chalhoub, Michel Misson, Overview on Multi-Channel Communications in Wireless Sensor Networks, the International Journal Network Protocols and Algorithms, 2013, volume 5, numéro 3
– Saoucene Mahfoudh, Gerard Chalhoub, Pascale Minet, Michel Misson, Ichrak Amdouni, Node Coloring and Color Conflict Detection in Wireless Sensor Networks, Future Internet Journal, oct 2010, volume 2, numéro 4
– Gerard Chalhoub, François Delobel, Michel Misson, Time Segmentation Approach Allowing QoS and Energy Saving for Wireless Sensor Networks, Journal of Telecommunications, mai 2010, volume 2, numéro 2
– Khaldoun Al Agha, Gerard Chalhoub, Alexandre Guitton, Erwan Livolant, Saoucène Mahfoudh, Pascale Minet, Michel Misson, Joseph Rahmé, Thierry Val, Adrien Van Den Bossche, Cross-layering in an industrial wireless sensor network : case study of OCARI, JNW (Journal of Networks), aout 2009, volume 4, numéro 6
– Gerard Chalhoub, Erwan Livolant, Alexandre Guitton, Adrien van den Bossche, Michel Misson, Thierry Val, Specifications and evaluation of a MAC protocol for a LP-WPAN, AHSWN (Ad Hoc & Sensor Wireless Networks), 2009, volume 7, numéro 1-2

Chapitres de livres

– Pascale Minet, Gerard Chalhoub, Erwan Livolant, Michel Misson, Ridha Soua, Rana Diab, Badr Rmili, Jean-Francois Perelgritz, Multichannel Wireless Sensor Networks for Structural Health Monitoring of Aircraft and Launchers, Wiley, à paraitre
– Ismail Mansour, Gerard Chalhoub, Michel Misson, Security architecture for multi-hop wireless sensor networks, Chapitre de livre, CRC Press Book, avril 2014

Conférences internationales

– Pascale Minet, Gerard Chalhoub, Erwan Livolant, Michel Misson, Badr Rmili, Jean-Francois Perelgritz, Adaptive wireless sensor networks for aircraft, IEEE International Conference on Wireless for Space and Extreme Environments, decembre 2015
– Hamadoun Tall, Gerard Chalhoub, Michel Misson, CoLBA : a Collaborative Load Balancing Algorithm to avoid queue overflow in WSNs, IEEE International Conference on Internet of Things, decembre 2015
– Hamadoun Tall, Gérard Chalhoub, Michel Misson, Implementation of IEEE 802.15.4 unslotted CSMA/CA protocol on Contiki OS, PEMWN15, novem-

bre 2015

- Rana Diab, Gérard Chalhoub, Michel Misson, Enhanced Multi-Channel MAC Protocol for Multi-Hop Wireless Sensor Networks, Wireless Days, novembre 2014
- Rana Diab, Gérard Chalhoub, Michel Misson, Evaluation of a Hybrid Multi-Channel MAC Protocol for Periodic and Burst Traffic, IEEE Conference on Local Computer Networks (LCN), septembre 2014
- Ismail Mansour, Gerard Chalhoub, Pascal Lafourcade, François Delobel, Secure Key Renewal and Revocation for Wireless Sensor Networks, IEEE Conference on Local Computer Networks (LCN), septembre 2014
- Ismail Mansour, Gerard Chalhoub, Pascal Lafourcade, Secure Multihop Key Establishment Protocols for Wireless Sensor Networks, International Conference on Cryptography and Security Systems (CSS), septembre 2014
- Rana Diab, Gerard Chalhoub, Michel Misson, Channel Allocation Evaluation for a multi-channel MAC protocol, IEEE PIMRC (International Symposium on Personal, Indoor and Mobile Radio Communications), septembre 2013
- Ismail Mansour, Damian Rusinek, Gerard Chalhoub, Pascal Lafourcade, Bogdan Ksiezopolski, Multihop Node Authentication Mechanisms for Wireless Sensor Networks, International Conference on Ad-Hoc Networks and Wireless (ADHOC-NOW), juin 2014
- Rana Diab, Gerard Chalhoub, Michel Misson, Hybrid Multi-Channel MAC Protocol for Wireless Sensor Networks : Interference Rate Evaluation, IEEE VTC (Vehicular Technology Conference), septembre 2013
- Antoinette Mouawad, Gerard Chalhoub, Gilbert Habib, Michel Misson, A performance study of mobile nodes in a Wireless Sensor Network, ICCIT (International Conference on Communications and Information Technology), juin 2013
- Ismail Mansour, Gerard Chalhoub, Evaluation of different cryptographic algorithms on wireless sensor network nodes, ICWCUCA (International Conference on Wireless Communications in Unusual and Confined Areas), aout 2012
- Antoinette Mouawad, Gerard Chalhoub, Michel Misson, Data Management in a Wireless Sensor Network with Mobile Nodes : A Case Study, ICWCUCA (International Conference on Wireless Communications in Unusual and Confined Areas), aout 2012
- Ismail Mansour, Gerard Chalhoub, Bassem Bakhache, Evaluation of a fast symmetric cryptographic algorithm based on the chaos theory for wireless sensor networks, MWNS (International Symposium on Mobile Wireless Network Security), juin 2012
- Nancy El Rachkidy, Gerard Chalhoub, Alexandre Guitton, Michel Misson, Queue-exchange mechanism to improve the QoS in a multi-stack architecture, ACM PE-WASUN (ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks), octobre 2011
- Ismail Mansour, Gerard Chalhoub, Alain Quilliot, Security architecture

for wireless sensor networks using frequency hopping and public key management, IEEE ICNSC (IEEE International Conference on Networking, Sensing and Control), avril 2011
- Ismail Mansour, Gerard Chalhoub, Michel Misson, Energy-Efficent Security Protocol for Wireless Sensor Networks Using Frequency Hopping and Permutation Cyphering, PECCS (International Conference on Pervasive and Embedded Computing and Communication Systems), mars 2011
- Gerard Chalhoub, Michel Misson, Cluster-tree based energy efficient protocol for wireless sensor networks, IEEE ICNSC (IEEE International Conference on Networking, Sensing and Control), avril 2010
- Pascale Minet, Saoucene Mahfoudh, Gerard Chalhoub, Alexandre Guitton, Node coloring in a wireless sensor network with unidirectional links and topology changes, IEEE WCNC (IEEE Wireless Communications & Networking Conference), avril 2010
- Gerard Chalhoub, Nassima Haddid, Alexandre Guitton, Michel Misson, Deference mechanisms significantly increase the MAC delay of slotted CSMA/CA, IEEE ICC (IEEE International Conference on Communications), juin 2009
- Marc-Henry Bertin, Adrien van den Bossche, Gerard Chalhoub, Tuan Dang, Saoucène Mahfoudh, Joseph Rahmé, Jean-Baptiste Viollet, OCARI for industrial wireless sensor networks, IFIP Wireless Daysk, novembre 2008, papier invité
- Gerard Chalhoub, Alexandre Guitton, Frédérique Jacquet, Antonio Freitas, Michel Misson, Medium Access Control for a Tree-Based Wireless Sensor Network : Synchronization Management, IFIP Wireless Days, novembre 2008
- Gerard Chalhoub, Alexandre Guitton, Michel Misson, MAC specifications for a WPAN allowing both energy saving and guaranteed delay - Part A : MaCARI : a synchronized tree-based MAC protocol, IFIP WSAN (IFIP Conference on Wireless Sensor and Actor Networks), juillet 2008
- papier collaboratif, OCARI : Optimization of Communication for Ad hoc Reliable Industrial networks, IEEE INDIN (IEEE International Conference on Industrial Informatics), juillet 2008, prix de la meilleure présentation
- Gerard Chalhoub, Antonio Freitas, Michel Misson, A Novel Approach for Simulating a Bio-Contamination Process, BIODEVICES (International Conference on Biomedical Electronics and Devices), janvier 2008

Conférences Nationales

- Ismail Mansour, Pascal Lafourcade et Gérard Chalhoub, Mécanismes d'authentification pour des réseaux de capteurs sans fil multi-sauts, 16emes Rencontres Francophones pour les Aspects Algorithmiques des Télécommunications, juin, 2014.

A.8 Activités relevant des missions autres que la recherche

- Référent Relations Internationales à l'IUT de Clermont-Ferrand
- Responsable des modules réseaux au département R&T de l'IUT de Clermont-Ferrand
- Publication de papiers pédagogiques au workshop des départements réseaux et télécommunications :
  - Gerard Chalhoub, Du DNS au DNSSEC, Workshop R&T de l'IUT, novembre 2014
  - Gerard Chalhoub, Réseaux de capteurs sans fil, Workshop R&T de l'IUT, novembre 2010
- Membre du conseil de département R&T de l'IUT de Clermont-Ferrand
- Formateur sur les points d'accès Cisco dans le cadre d'une mission en tant que formateur invité à l'Université de Balamand au Liban
- Responsable de l'organisation et de la mise en place de la WAN Party (évènement annuel de jeux en réseau au niveau national entre les différents départements R&T de France)

A.9 Perspectives à moyen et court termes

Mes travaux de recherche à court et moyen termes portent sur la fiabilité, la sureté de fonctionnement et la sécurité des communications sans fil dans des enviremments perturbés et confinés.

A.9.1 Protocoles de communication

Les réseaux de capteurs sans fil (RCSF) constituent une brique essentielle des Internet des Objets (IdO). Ce dernier domaine étant devenu la préoccupation majeur de ces dernières années et le sera encore pour les quelques années avenir. En effet, d'après Siemens, l'une des sociétés majeurs du domaine de télécommunications, il est prévu qu'en 2020 le nombre d'objets autonomes connecté atteindra les 13 milliards et dépassera le nombre cumulé de téléphones mobiles, de tablettes et d'ordinateurs.

Cette émergence de l'IdO requerra une allocation intelligente des ressources fréquentielles disponibles. Ces objets communicants utilisent des bandes ISM. Ces fréquences sont donc partagées avec les autres objets faisant partie d'autres réseaux, les autres technologies WLAN, Bluetooth, etc. Ainsi, les protocoles de partage du médium sans fil devraient utiliser d'une façon optimisée les fréquences disponibles en prenant en compte la coexistence et le partage des ressources. Des techniques classiques permettent de gérer cette utilisation comme le TDMA, le FDMA et le CDMA. D'autres techniques plus récentes comme le Beamforming commencent à être adoptées par les nouvelles versions des standards comme le WiFi avec la norme IEEE 802.11ac.

Ainsi, au niveau de la conception des protocoles de communication, ces techniques devraient être adaptées et employées selon les besoins des applications exploitant ces objets. En effet, une norme est le résultat de compromis qui permettent de couvrir un large panel de besoins applicatifs sans que ce soit optimisé pour répondre aux besoins d'une application en particulier. Une conception prenant en compte les besoins de l'application donnera de meilleurs résultats. Se rajoutent à ce challenge les contraintes classiques de ressources et capacités limitées de certains types des objets, surtout ceux des RCSF.

Parmi les problématiques à résoudre, nous pouvons identifier les suivantes :

- Gestion de la répartition des ressources (temporelles et fréquentielles) dans un réseau multi-saut : une telle gestion devrait reposer sur une connaissance de voisinage et une répartition équitable qui permet au réseau de fonctionner selon les contraintes de l'application. Souvent, trouver la solution optimale de répartition revient à résoudre un problème NP-complet. Ainsi, la solution envisagée devrait se rapprocher le plus possible d'une solution optimale.
- Prise en compte des interférences extérieures : une répartition des ressources entre les noeuds d'un réseau sans fil doit prendre en compte l'utilisation de ces ressources par les objets communicants voisins pouvant affecter les communications du réseau. Cette prise en compte pose une difficulté majeure du fait de l'imprédictibilité de l'utilisation des ressources par des entités ne faisant pas partie du réseau.
- Prise en compte des changements de topologie : avoir des protocoles dynamiques capables de s'adapter aux changements de topologie constitue une difficulté au niveau de la complexité même des protocoles. En effet, afin de s'adapter aux changements il faudrait les détecter au plus vite. Ceci engendre une surveillance de la topologie à travers un trafic de contrôle qui surcharge le réseau et consomme une partie des ressources disponibles.
- Précision temporelle : maintenir une synchronisation à plusieurs sauts dans un réseau constitué de noeuds est un challenge technologique. Ceci devient davantage plus difficile du fait de l'utilisation de composants à basse consommation ; les contraintes énergétiques imposent aux noeuds d'un RCSF d'être équipés de composants à faible consommation ce qui induit un fonctionnement non optimal.
- Compromis entre un fonctionnement optimal et la surcharge : un fonctionnement idéal est difficilement atteignable et demande des échanges fréquents afin de s'adapter aux changements de l'état du réseau. Il est nécessaire de trouver un compromis capable de fournir des performances acceptable selon les besoins de l'application. Par exemple, au niveau de la méthode d'accès, l'utilisation du CSMA/CA risque de créer des pertes mais permet de s'adapter aux changements sans générer un trafic de contrôle, alors qu'une méthode purement basée sur du TDMA garantit un fonctionnement sans perte mais requière plus de trafic de contrôle.

A.9.2 Travaux en cours sur les protocoles de communication :

Je co-encadre avec Michel Misson depuis novembre 2014 une thèse menée par Hamadoun Tall sur la répartition de trafic équitable dans un réseau de capteurs sans fil à haut débit exploitant plusieurs canaux de communication. Cette thèse s'inscrit dans le contexte des RCSF déployer faire la collecte d'information. Son objectif principal est de trouver un moyen d'éviter de créer des goulots d'étranglement autour des noeuds proches du puits de collecte. Nous sommes en train d'évaluer une méthode qui repose sur la surveillance des délais d'attente dans les files d'attente afin de faire passer les données à travers des chemins non surchargés. Une meilleure répartition du trafic permet aussi d'exploiter d'une façon plus efficace la réutilisation spatiale des fréquences de communication. Ainsi, cette répartition contribuera à la diminution des interférences dans un réseau utilisant plusieurs canaux.

Les points durs à améliorer sont les suivants :

- L'identification des prochains sauts qui mènent vers des routes non surchargées.
- L'utilisation simultanée de prochains sauts différents.
- La réactivité face à l'apparition des congestions et des débordements des files d'attente.

Aussi, je co-encadre avec Michel Misson une thèse à partir de novembre 2015 menée par Jinpeng Wang sur la prise en compte de la mobilité dans un réseau de capteurs sans fil. Cette thèse s'inscrit dans un contexte de déploiement sur site industriel qui impose des changements fréquents de topologie. Le réseau devrait appliquer une méthode d'accès au médium qui permet une agilité fréquentielle afin de supporter une charge importante tout en évitant les perturbations extérieures. La méthode employée devrait permettre une adaptation rapide aux changements de topologie afin de garantir un fonctionnement répondant aux contraintes de l'application. Une des pistes serait de garantir une couverture cellulaire permettant d'avoir tous les noeuds du réseau à portée d'un noeud fixe se trouvant à au plus 3 sauts. Une méthode s'appuyant sur un découpage TDMA centralisé serait difficile à maintenir. Nous explorons une méthode répartie permettant une flexibilité et une gestion localisée des ressources.

Les points durs à investiguer sont les suivants :

- Création de clusters à trois sauts de façon à couvrir tous les noeuds et distribuer la gestion des ressources aux chefs de cluster.
- Définir des scénarios de mobilité réalistes et basés sur des applications existantes (un rapprochement des problématiques de communications au sein d'un hôpital est prévu).
- La réutilisation des ressources devrait prendre en compte l'imperfection de la connaissance de la topologie.

A.9.3 Sécurisation des communications

Avec la parution d'applications critiques basées sur les objets communicants comme la surveillance des états des patients, la détection d'intrusion, etc. les problématiques liées à la sécurisation des communications deviennent aussi importantes que les protocoles de communication. La nature des architectures multi-saut des réseaux des objets, différentes des topologies en étoile des réseaux classique WiFi, et la limitation des capacités des noeuds, beaucoup moins puissants que les ordinateurs et les téléphones portables, requière une adaptation des protocoles de sécurité pour répondre à ces contraintes.

Beaucoup de protocoles de sécurité ont été proposés pour résoudre cette problématique. Les solutions basées sur des algorithmes de chiffrement normalisés sont souvent celles qui sont adoptées par les standards de communication. D'autres solutions concurrentes basées sur des calculs plus légers sont aussi proposées mais manquent de crédibilité comparées à celles qui bénéficient de l'approbation des organismes de normalisation.

D'un côté, la gestion des clés de chiffrement dans un environnement tel que celui des réseaux des objets pose des difficultés à cause de la difficulté de centraliser cette gestion dans un contexte multi-saut. D'un autre côté, il important de limiter le coût des opérations cryptographiques. Ceci peut se faire en utilisant des opérations moins couteuses que d'autres (typiquement les opérations symétriques) et en limitant globalement le nombre d'opérations nécessaire pour effectuer une tâche donnée.

Parmi les problématiques à résoudre, nous pouvons identifier les suivantes :

- Limiter le nombre d'opérations cryptographiques : le but est de concevoir un protocole de sécurité avec un nombre d'opérations limité afin de limiter son surcoût. Néanmoins, le protocole doit être sûr, c'est-à-dire, ne présente pas de faille de sécurité.
- Le choix des types d'opérations : il est connu que les opérations asymétriques sont plus couteuses que les opérations symétriques. Mais ce que permet d'assurer les opérations asymétriques au niveau de l'authentification et de partage de clé est difficilement réalisable avec les opérations symétriques. Ainsi, un compromis est à trouver entre les différentes utilisations d'opérations afin de couvrir les besoins.
- Gestion répartie de confiance : l'établissement de liens sécurisés repose sur l'établissement de clé secrètes communes. Ainsi, une répartition au niveau des noeuds pourrait simplifier et accélérer l'établissement de liens sécurisé sans passer par une entité centrale.
- Mutualisation des ressources : dans le monde des objets connectés il est tout à fait possible qu'un fasse partie de plusieurs réseaux. Nous pouvons considérer qu'on capteur de présence pourrait être utilisé par une application de détection d'intrusion et une application de gestion d'air conditionné centralisée. Ainsi, les données de différentes applications devraient transiter à travers des noeuds qui ne font pas partie d'un seul réseau et peuvent être utilisé par d'autres applications. Ceci nous incite à considérer

un modèle de sécurité capable de se protéger face à des applications qui exploitent les mêmes ressources de communication.

Travaux en cours sur la sécurisation des échanges :

Suite à la thèse d'Ismail Mansour que j'ai co-encadrée et qui a été soutenue en 2013, je travaille en collaboration avec Pascal Lafourcade dans le cadre de la chaire industrielle sur la suite des travaux de cette thèse qui ont donné lieu à plusieurs publications entre 2014 et 2015. L'objectif principal de ces travaux est de proposer et d'évaluer des protocoles de gestion de clés de chiffrement dans les réseaux de capteurs sans fil.

Des pistes de collaboration sont en cours de consolidation :

- Projet de collaboration avec l'Inde sur les problématiques liées à la sécurité de l'internet des objets : dans le cadre du programme DST-INRIA-CNRS, nous avons eu un budget sur 3 ans à partir de 2016 qui permet de financer des invitations mutuelle.
- Positionnement sur des projets H2020 : avec Pascal Lafourcade, nous avons été sollicités par la société BelHard de la Belarus. L'objectif de ce rapprochement est d'identifier des projets internationaux autour de la sécurité et la sureté de fonctionnement des protocoles de communication.

Bibliographie

[1] IEEE 802.15, "Part 15.4 : Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs)," ANSI/IEEE, Standard 802.15.4 R2003, 2003.

[2] G. Chalhoub, A. Guitton, and M. Misson, "MAC specifications for a WPAN allowing both energy saving and guaranteed delay - Part A : MaCARI : a synchronized tree-based mac protocol," in *IFIP WSAN*, 2008.

[3] R. Diab, G. Chalhoub, and M. Misson, "Hybrid multi-channel MAC protocol for wireless sensor networks : Interference rate evaluation," in *IEEE 78th Vehicular Technology Conference : VTC2013-Fall, Las Vegas, USA*, September 2013.

[4] H. Tall, Gerard Chalhoub, and M. Misson, "Colba : a collaborative load balancing algorithm to avoid queue overflow in wsns," in *IEEE International Conference on Internet of Things*, December 2015.

[5] I. Mansour, G. Chalhoub, and M. Misson, *Security architecture for multihop wireless sensor networks.* CRC Press Book, 2014, pp. 157–178.

[6] IEEE 802.11, "Part 11 : Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," ANSI/IEEE, Standard 802.11 R2003, 1999.

[7] IEEE 802.15, "Part 15.4 : Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs)," ANSI/IEEE, Standard 802.15.4 R2006, 2006.

[8] G. Chalhoub, A. Freitas, and M. Misson, "A novel approach for simulating a bio-contamination process," in *BIODEVICES (International Conference on Biomedical Electronics and Devices)*, January 2008.

[9] The OCARI project, "The ocari project web site," https ://ocari.org/.

[10] OCARI-Consortium, "OCARI : Optimization of communication for ad hoc reliable industrial networks," in *IEEE International Conference on Industrial Informatics*, July 2008.

[11] G. Chalhoub, A. Guitton, F. Jacquet, A. Freitas, and M. Misson, "Medium access control for a tree-based wireless sensor network : Synchronization management," in *IFIP Wireless Days*, 2008.

[12] M.-H. Bertin, G. Chalhoub, T. Dang, S. Mahfoudh, J. Rahmé, A. van den Bossche, and J.-B. Viollet, "OCARI for industrial wireless sensor networks," in *IFIP Wireless Days*, 2008.

[13] G. Chalhoub, E. Livolant, A. Guitton, A. van den Bossche, M. Misson, and T. Val, "Specifications and evaluation of a MAC protocol for a LP-WPAN," *Ad Hoc & Sensor Wireless Networks*, vol. 7, no. 1-2, 2009.

[14] K. A. Agha, G. Chalhoub, A. Guitton, E. Livolant, S. Mahfoudh, P. Minet, M. Misson, J. Rahmé, T. Val, and A. V. D. Bossche, "Cross-layering in an industrial wireless sensor network : case study of OCARI," *Journal of Networks*, vol. 4, no. 6, 2009.

[15] G. Chalhoub, F. Delobel, and M. Misson, "Time segmentation approach allowing QoS and energy saving for wireless sensor networks," *Journal of Telecommunications*, vol. 2, no. 2, 2010.

[16] G. Chalhoub and M. Misson, "Cluster-tree based energy efficient protocol for wireless sensor networks," in *IEEE International Conference on Networking, Sensing and Control*, April 2010.

[17] N. Rachkidy, G. Chalhoub, A. Guitton, and M. Misson, "Queue-exchange mechanism to improve the QoS in a multi-stack architecture," in *ACM PE-WASUN, (ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks)*, October 2011.

[18] P. Minet, S. Mahfoudh, G. Chalhoub, and A. Guitton, "Node coloring in a wireless sensor network with unidirectional links and topology changes," in *IEEE Wireless Communications and Networking Conference*, April 2010.

[19] S. Mahfoudh, G. Chalhoub, P. Minet, M. Misson, and I. Amdouni, "Node coloring and color conflict detection in wireless sensor networks," *Future Internet*, vol. 2, no. 4, pp. 469–504, 2010.

[20] I. Mansour and G. Chalhoub, "Evaluation of different cryptographic algorithms on wireless sensor network nodes," in *International Conference on Wireless Communications in Unusual and Confined Areas*, 2012.

[21] I. Mansour, P. Lafourcade, and G. Chalhoub, "Mécanismes d'authentification pour des reseaux de capteurs sans fil multi-sauts," in *Rencontres Francophones pour les Aspects Algorithmiques des Telecommunications*, June 2014.

[22] I. Mansour, G. Chalhoub, P. Lafourcade, and F. Delobel, "Secure key renewal and revocation for wireless sensor networks," in *IEEE Conference on Local Computer Networks*, September 2014.

[23] I. Mansour, G. Chalhoub, and P. Lafourcade, "Secure multihop key establishment protocols for wireless sensor networks," in *International Conference on Cryptography and Security Systems*, September 2014.

[24] I. Mansour, D. Rusinek, G. Chalhoub, P. Lafourcade, and B. Ksiezopolski, "Multihop node authentication mechanisms for wireless sensor networks," in *13th International Conference, ADHOC-NOW 2014*, ser. Lecture Notes in Computer Science. Springer, 2014.

[25] I. Mansour, G. Chalhoub, and P. Lafourcade, "Evaluation of secure multi-hop node authentication and key establishment mechanisms for wireless sensor networks," *Journal of Sensors and Actuator Networks*, vol. 3, pp. 224–244, 2014.

[26] I. Mansour, G. Chalhoub, and P. Lafourcade, "Key management in wireless sensor networks," *Journal of Sensor and Actuator Networks*, vol. 4, no. 3, p. 251, 2015. [Online]. Available : http://www.mdpi.com/2224-2708/4/3/251

[27] R. Diab, G. Chalhoub, and M. Misson, "Overview on multi-channel communications in wireless sensor networks," *Network Protocols and Algorithms Surveys and Tutorials*, vol. 5, no. 3, pp. 1943–3581, 2013.

[28] R. Diab, G. Chalhoub, and M. Misson, "Channel allocation evaluation for a multi-channel MAC protocol," in *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC, London, UK.*, September 2013.

[29] R. Diab, G. Chalhoub, and M. Misson, "Evaluation of a hybrid multi-channel mac protocol for periodic and burst traffic," in *IEEE 39th Local Computer Networks : LCN2014, Edmonton, Canada*, September 2014.

[30] G. Chalhoub, R. Diab, and M. Misson, "Hmc-mac protocol for high data rate wireless sensor networks," *Electronics*, vol. 4, no. 2, p. 359, 2015. [Online]. Available : http://www.mdpi.com/2079-9292/4/2/359

[31] H. Tall, G. Chalhoub, and M. Misson, "Implementation of IEEE 802.15.4 unslotted csma/ca protocol on contiki os," in *International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks*, I. J. of Engineering Research & Technology, Ed., November 2015.

[32] F. Delobel, A. Guitton, M. Misson, and W. Dargie, "Minimization of the diffusion delay of a tree-based wireless sensor network," in *Proceedings of the Global Communications Conference, GLOBECOM*, 2011.

[33] A. Jayasuriya, S. Perreau, A. Dadej, and S. Gordon, "Hidden vs. exposed terminal problem in ad hoc networks," in *Proceedings of the Australian Telecommunication Networks and Applications Conference*, 2004.

[34] Zigbee, "Zigbee Specification," ZigBee Standards Organization, Standard Zigbee 053474r13, 2006.

[35] G. EkbataniFard and R. Monsefi, "A detailed review of multi-channel medium access control protocols for wireless sensor networks," *International Journal of Wireless Information Networks*, vol. 19, no. 1, pp. 1–21, 2012.

[36] O. D. Incel, "A survey on multi-channel communication in wireless sensor networks," *Computer Networks*, vol. 55, no. 13, pp. 3081–3099, 2011.

[37] A. Gupta, C. Gui, and P. Mohapatra, "Exploiting multi-channel clustering for power efficiency in sensor networks," in *Comsware : First International Conference on Communication System Software and Middleware*, 2006, pp. 1–10.

[38] Y. Wu, J. A. Stankovic, T. He, and S. Lin, "Realistic and efficient multi-channel communications in wireless sensor networks," in *INFOCOM : the 27th Conference on Computer Communications*, 2008.

[39] X. Wang, X. Wang, X. Fu, G. Xing, and N. Jha, *Flow-based real-time communication in multi-channel wireless sensor networks.* Springer Berlin Heidelberg, 2009, pp. 33–52.

[40] G. Zhou, C. Huang, T. Yan, T. He, J. Stankovic, and T. Abdelzaher, "MMSN : Multi-frequency media access control for wireless sensor networks," in *Infocom*, 2006, pp. 1–13.

[41] Z. Yuanyuan, N. Xiong, J. Park, and L. Yang, "An interference-aware multichannel media access control protocol for wireless sensor networks," *The Journal of Supercomputing*, vol. 60, no. 3, pp. 437–460, 2008.

[42] O. Incel, L. van Hoesel, P. Jansen, and P. Havinga, "MC-LMAC : a multi-channel mac protocol for wireless sensor networks," *Ad Hoc Networks*, vol. 9, no. 1, pp. 73–94, 2011.

[43] M. Ramakrishnan and V. R., "Multi-channel mac for wireless sensor networks," *International Journal of Computer Networks & Communications*, vol. 1, no. 2, 2009.

[44] S. Lohier, A. Rachedi, I. Salhi, and E. Livolant, "Multichannel access for bandwidth improvement in ieee s02.15.4 wireless sensor network," in *Wireless Days*, 2012.

[45] Y. Kim, H. Shin, and H. Cha, "Y-MAC : An energy-efficient multi-channel mac protocol for dense wireless sensor networks," in *IPSN*, 2008, pp. 53–63.

[46] J. Borms, K. Steenhaut, and B. Lemmens, "Low-overhead dynamic multichannel mac for wireless sensor networks," in *EWSN*, 2010, pp. 81–96.

[47] J. Chen, Q. Yu, B. Chai, Y. Sun, and Y. Fan, "Dynamic channel assignment for wireless sensor networks : a regret matching based approach," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 1, pp. 95–106, 2015.

[48] R. E. Irwin, A. B. MacKenzie, and L. A. DaSilva, "Resource-minimized channel assignment for multi-transceiver cognitive radio networks," *Journal of Selected Areas in Communications*, vol. 31, no. 3, pp. 442–450, 2013.

[49] T. Neves and J. Bordim, "Topology control in cooperative ad hoc wireless networks," *Electronic Notes in Theoretical Computer Science*, vol. 302, pp. 29 – 51, 2014, proceedings of the {XXXIX} Latin American Computing Conference (CLEI 2013).

[50] "The Network Simulator NS-2," http://www.isi.edu/nsnam/ns/.

[51] G.-S. Ahn, E. Miluzzo, and A. T. Campbell, "A funneling-mac for high performance data collection in sensor networks," in *SenSys*, 2006, pp. 345–346.

[52] D. Kandris, D. J. Vergados, D. D. Vergados, and A. Tzes, "A routing scheme for congestion avoidance in wireless sensor networks," in *IEEE Conference on Automation Science and Engineering*, August 2010.

[53] M. Xie and Y. Gu, "Multipath routing algorithm for wireless multimedia sensor networks within expected network lifetime," in *International Conference on Communication and Mobile Computing*, April 2010.

[54] H. Li, Y. Cheng, C. Zhou, and W. Zhuang, "Minimizing end-to-end delay : A novel routing metric for multi-radio wireless mesh networks," in *IEEE INFOCOM*, April 2009.

[55] C. Wan, S. Eisenman, and A. Campbell, "CODA : congestion detection and avoidance in sensor networks," in *ACM Conference on Embedded Networked Sensor Systems*, November 2003.

[56] F. Ren, T. He, S. Das, and C. Lin, "Traffic-aware dynamic routing to alleviate congestion in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 9, pp. 1585–1599, 2011.

[57] Y. Sankarasubramaniam, O. Akan, and I. Akyildiz, "ESRT : event to-sink reliable transport for wireless sensor networks," in *ACM International Symposium on Mobile Ad Hoc Networking and Computing*, June 2003.

[58] C. Sergiou and V. Vassiliou, "DAlPaS : A performance aware congestion control algorithm in Wireless Sensor Networks," in *International Conference on Telecommunications*, May 2011.

[59] R. Kumar, H. Rowaihy, G. Cao, F. Anjum, A. Yener, and T. L. Porta, "Congestion aware routing in sensor networks," Tech. Rep., June 2006.

[60] W. wei Fang, J. ming Chen, L. Shu, T. shu Chu, and D. pei Qian, "Congestion avoidance, detection and alleviation in wireless sensor networks," *Journal of Zhejiang University SCIENCE*, vol. 11, no. 1, pp. 63–73, 2010.

[61] O. Banimelhem and S. Khasawneh, "GMCAR grid-based multipath with congestion avoidance routing protocol in wireless sensor networks," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1346–1361, 2012.

[62] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-level sensor network simulation with cooja," in *IEEE Conference on Local Computer Networks*, November 2006.

[63] A. Dunkels, B. Gronvall, and T. Voigt, "Contiki a lightweight and flexible operating system for tiny networked sensors," in *IEEE International Conference on Local Computer Networks*, November 2004.

[64] M. A. Hussain, P. Khan, and K. K. Sup, "Wsn research activities for military application," in *Proceedings of the 11th international conference on Advanced Communication Technology-Volume 1*. IEEE Press, 2009, pp. 271–274.

[65] G. Lowe, "Breaking and fixing the needham-schroeder public-key protocol using fdr," *Software - Concepts and Tools*, vol. 17, no. 3, pp. 93–102, 1996.

[66] B. Blanchet, "Automatic proof of strong secrecy for security protocols," in *IEEE Symposium on Security and Privacy*, Oakland, California, May 2004, pp. 86–100.

[67] V. B. Pérez, P. González, J. C. Cabaleiro, D. B. Heras, T. F. Pena, J. J. Pombo, and F. F. Rivera, "Avispa : visualizing the performance prediction of parallel iterative solvers." *Future Generation Comp. Syst.*, vol. 19, no. 5, pp. 721–733, 2003.

[68] C. Cremers, "The Scyther Tool : Verification, falsification, and analysis of security protocols," in *Computer Aided Verification, 20th International Conference, CAV 2008, Proc.*, ser. Lecture Notes in Computer Science, vol. 5123/2008. Springer, 2008, pp. 414–418.

[69] D. Dolev and A. C. Yao, "On the security of public key protocols," in *Proceedings of the 22Nd Annual Symposium on Foundations of Computer Science*, ser. SFCS '81, 1981, pp. 350–357.

[70] D. Basin, C. Cremers, and C. Meadows, *Model Checking Security Protocols*. Springer, 2014, ch. 24, to appear.

[71] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. Culler, "SPINS : Security protocols for sensor networks," *Wireless Networks*, 2002.

[72] K. S. Pister, J. M. Kahn, B. E. Boser *et al.*, "Smart dust : Wireless networks of millimeter-scale sensor nodes," *Highlight Article in 1999 Electronics Research Laboratory Research Summary*, p. 2, 1999.

[73] H. Chan and A. Perrig, "Pike : Peer intermediaries for key establishment in sensor networks," in *INFOCOM*. IEEE Computer Society, 2005, pp. 524–535.

[74] C. Yu, C. Lu, and S. Kuo, "A simple non-interactive pairwise key establishment scheme in sensor networks," in *IEEE International Conference on Sensing, Communication, and Networking, SECON*, 2009.

[75] E. Munivel and G. Ajit, "Efficient public key infrastructure implementation in wireless sensor networks," in *International Conference on Wireless Communication and Sensor Computing*, 2010, pp. 1–6.

[76] H.-L. Yeh, T.-H. Chen, P.-C. Liu, T.-H. Kim, and H.-W. Wei, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 11, no. 5, 2011.

[77] J. Zhang, R. Shankaran, M. A. Orgun, A. Sattar, and V. Varadharajan, "A dynamic authentication scheme for hierarchical wireless sensor networks." in *MobiQuitous*, vol. 73. Springer, 2012, pp. 186–197.

[78] A. Al-mahmud and R. Akhtar, "Secure sensor node authentication in wireless sensor networks," *International Journal of Computer Applications*, vol. 46, no. 4, pp. 10–17, May 2012, published by Foundation of Computer Science, New York, USA.

[79] K. Han and T. Shon, "Sensor authentication in dynamic wireless sensor network environments," *International Journal of RFID Security and Cryptography*, 2012.

[80] Manjusha and L. B. Rananavare, "A robust message authentication scheme in multihop wsn using elliptical curve cryptography and elgamal signature," *International Journal of Engineering Research & Technology (IJERT)*, July 2013.

[81] H. Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of intrusion-detection systems," *Computer Networks*, vol. 31, no. 8, 1999.

[82] B. Sun, L. Osborne, Y. Xiao, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," *Wireless Communications, IEEE*, vol. 14, no. 5, pp. 56–63, 2007.

[83] J. Zhang and V. Varadharajan, "Wireless sensor network key management survey and taxonomy," *Journal of Network and Computer Applications*, vol. 33, pp. 63–75, 2010.

[84] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *IEEE Symposium on Security and Privacy*, 2003.

[85] H. Chan, V. Gligor, A. Perrig, and G. Muralidharan, "On the distribution and revocation of cryptographic keys in sensor networks," *IEEE Transaction on Dependable and Secure Computing*, vol. 2, 2005.

[86] S. Chattopadhyay and A. K. Turuk, "A scheme for key revocation in wireless sensor networks," *International Journal on Advanced Computer Engineering and Communication Technology*, vol. 1, pp. 16–20, 2012.

[87] P. Chuang, S. Chang, and C. Lin, "A node revocation scheme using public-key cryptography in wireless sensor networks," *Journal of Information Sience and Enfineering*, pp. 1859–1873, 2010.

[88] G. Dini and I. Savino, "An efficient key revocation protocol for wireless sensor networks," in *International Symposium on a World of Wireless, Mobile and Multimedia Networks*, 2006.

[89] Y. Jiang and H. Shi, "A cluster-based random key revocation protocol for wireless sensor networks," *Journal of Electronic Science and Technology of China*, vol. 6, pp. 10–15, 2008.

[90] G. Jolly, M. Kusçu, P. Kokate, and M. Younis, "A low-energy key management protocol for wireless sensor networks," in *Proceedings of the Eighth IEEE International Symposium on Computers and Communications*. IEEE Computer Society, 2003.

[91] G. N. Purohit and A. S. Rawat, "Revocation and self-healing of keys in hierarchical wireless sensor network," *International Journal of Computer Science and Information Technologies*, vol. 2, 2011.

[92] C. Wang, T. Hong, G. Horng, and W. Wang, "A key renewal scheme under the power consumption for wireless sensor networks," *Journal of Colloid and Interface Science*, 2006.

[93] G. Wang, S. Kim, D. Kang, D. Choi, and G. Cho, "Lightweight key renewals for clustered sensor networks," *Journal of Networks*, vol. 5, 2010.

[94] Y. Wang, B. Ramamurthy, and X. Zou, "Keyrev : An efficient key revocation scheme for wireless sensor networks," in *International Conference on Communications*, 2007, pp. 1260–1265.

[95] T. Eisenbarth, S. Kumar, L. Uhsadel, C. Paar, and A. Poschmann, "A Survey of Lightweight-Cryptography Implementations," in *A Survey of Lightweight-Cryptography Implementations.* IEEE Design & Test of Computers, 2007.

[96] M. Cazorla, K. Marquet, and M. Minier, "Survey and benchmark of lightweight block ciphers for wireless sensor networks," in *SECRYPT 2013 - Proceedings of the 10th International Conference on Security and Cryptography, 29-31 July, 2013*, P. Samarati, Ed. Reykjavík, Iceland : SciTePress, 2013, pp. 543–548.

[97] K. Jeong, C. Lee, and J. Lim, "Improved differential fault analysis on lightweight block cipher lblock for wireless sensor networks," *EURASIP J. Wireless Comm. and Networking*, vol. 2013, p. 151, 2013.

[98] D. Couroussé, B. Robisson, J. Lanet, T. Barry, H. Noura, P. Jaillon, and P. Lalevée, "COGITO : code polymorphism to secure devices," in *SECRYPT 2014 - Proceedings of the 11th International Conference on Security and Cryptography, Vienna, Austria, 28-30 August, 2014*, 2014, pp. 451–456. [Online]. Available : http://dx.doi.org/10.5220/0005113704510456

[99] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[100] T. El Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Proceedings of CRYPTO 84 on Advances in Cryptology.* New York, NY, USA : Springer, 1984, pp. 10–18.

[101] C. Research, "Standards for efficient cryptography, sec 1 : Elliptic curve cryptography," September 2000.

[102] A. Liu and N. Ning, "Tinyecc : A configurable library for elliptic curve cryptography in wireless sensor networks," in *7th International Conference on Information Processing in Sensor Networks*, April 2008, pp. 245–256.

[103] V. Shoup, "A proposal for an ISO standard for public key encryption," *IACR Cryptology ePrint Archive*, vol. 2001, p. 112, 2001, (accessed on 20th Dec 2001). [Online]. Available : http://eprint.iacr.org/2001/112

[104] J. Daemen and V. Rijmen, *The Design of Rijndael : AES - The Advanced Encryption Standard.* Heidelberg, Germany : Springer Verlag, 2002.

[105] N. Manica, M. Saloni, and P. Toldo, "WSN - secure comunications with AES algoritms," University of Trento - Faculty of Computer Science, Trento, Italy, 2008.

[106] I. F. Blake, G. Seroussi, and N. P. Smart, *Elliptic Curves in Cryptography.* New York, NY, USA : Cambridge University Press, 1999.

[107] V. S. Miller, "Use of elliptic curves in cryptography," in *Lecture Notes in Computer Sciences ; 218 on Advances in cryptology—CRYPTO 85.* New York, NY, USA : Springer-Verlag New York, Inc., 1986, pp. 417–426. [Online]. Available : http://dl.acm.org/citation.cfm?id=18262.25413

[108] I. Mansour, P. Lafourcade, and G. Chalhoub, "Scyther code of our authentication protocols," (accessed on December 2013), http://sancy.univ-bpclermont.fr/~lafourcade/scyther-jsan-code.tar.

[109] J. Daemen and V. Rijmen, *The Design of Rijndael : AES - The Advanced Encryption Standard*. Heidelberg, Germany : Springer-Verlag, 2002.

[110] HART Communication Foundation Std., "HART field communication protocol specifications," Tech. Rep., 2008.

[111] International Society of Automation Std., "ISA100.11a : 2009 wireless systems for industrial automation : Process control and related applications," Draft standard, in preparation, 2009.

[112] D. Yang, Y. Xu, and M. Gidlund, "Wireless coexistence between ieee 802.11- and ieee 802.15.4-based networks : A survey," *International Journal of Distributed Sensor Networks*, vol. 2011, p. 17, 2011.

[113] M. Rihan, M. El-Khamy, and M. El-Sharkawy, "On zigbee coexistence in the ism band : Measurements and simulations," in *ICWCUCA*, August 2012.

[114] S. Shin, S. Choi, H. Park, and W. Kwon, "Packet error rate analysis of ieee 802.15.4 under ieee 802.11b interference," in *WWIC*, May 2005.

[115] A. Sikora and V. Groza, "Coexistence of ieee 802.15.4 with other systems in the 2.4 ghz-ism-band," in *IEEE Instrumentation and Measurement Technology Conference*, August 2005.

[116] L. Angrisani, M. Bertocco, D. Fortin, and A. Sona, "Experimental Study of Coexistence Issues Between IEEE 802.11b and IEEE 802.15.4 Wireless Networks," *IEEE Transactions on Instrumentation and Measurement*, vol. 57, no. 8, 2008.

[117] G. Chalhoub, E. Perrier de La Bâthie, and M. Misson, "Overhead caused by wifi on zigbee networks using slotted CSMA/CA," *Journal of Networks*, vol. 11, no. 2, 2016.

[118] Chipcon company, "CC2420 coexistence," Tech. Rep., June 2006.

[119] IEEE Task Group 4e, "TG4e contributions," last accessed on October 2015, http ://www.ieee802.org/15/pub/TG4e.html.

[120] K. S. J. Pister and L. Doherty, "Tsmp : Time synchronized mesh protocol," in *Parallel and Distributed Computing and Systems (PDCS), Orlando, Florida, USA*, 2008.

[121] V. Raman and N. H. Vaidya, "Adjacent channel interference reduction in multichannel wireless networks using intelligent channel allocation," Tech. Rep., 2009.

[122] M. Bertocco, G. Gamba, and A. Sona, "Is csma/ca really efficient against interference in a wireless control system ? an experimental answer," in *2008 IEEE International Conference on Emerging Technologies and Factory Automation*, Sept 2008, pp. 885–892.

[123] B. Raman and R. Jain, "Sir-based interference-maps for tdma-based outdoor mesh networks," in *Local and Metropolitan Area Networks (LANMAN), 2010 17th IEEE Workshop on*, May 2010, pp. 1–6.

[124] E. Toscano and L. L. Bello, "Cross-channel interference in ieee 802.15.4 networks," in *Factory Communication Systems, 2008. WFCS 2008. IEEE International Workshop on*, May 2008, pp. 139–148.

[125] R. Leidenfrost and W. Elmenreich, "Firefly clock synchronization in an 802.15.4 wireless network," *EURASIP J. Embedded Syst.*, vol. 2009, pp. 7 :1–7 :17, Jan. 2009. [Online]. Available : http://dx.doi.org/10.1155/2009/186406

[126] S. Qin and D. Chen, *Advances in Wireless Sensor Networks : 6th China Conference, CWSN 2012, Huangshan, China, October 25-27, 2012, Revised Selected Papers.* Berlin, Heidelberg : Springer Berlin Heidelberg, 2013, ch. A Distributed Broadcast Protocol of Wireless Sensor Networks Based on Dynamic Multi-channel MAC Protocol, pp. 363–370. [Online]. Available : http://dx.doi.org/10.1007/978-3-642-36252-1_34

[127] Y. Wan, X. Chen, and J. Lu, "Broadcast enhanced cooperative asynchronous multichannel mac for wireless ad hoc network," in *Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on*, Sept 2011, pp. 1–5.

[128] M. Wang, Q. Liu, J. Zuo, and Y. Xu, "Rsm : A broadcast available multichannel mac protocol for wireless sensor networks," in *Computational and Information Sciences (ICCIS), 2012 Fourth International Conference on*, Aug 2012, pp. 1076–1079.

[129] Bhupendra and V. Sharma, "Energy efficient communication overhead algorithm in wireless sensor networks," in *Advance Computing Conference (IACC), 2013 IEEE 3rd International*, Feb 2013, pp. 427–430.

[130] B. Djamaa and M. Richardson, "The Trickle Algorithm : Issues and Solutions," research report, 2015.

[131] P. Goswami and A. D. Jadhav, "Evaluating the performance of routing protocols in wireless sensor networks," in *Computing Communication Networking Technologies (ICCCNT), 2012 Third International Conference on*, July 2012, pp. 1–4.

[132] IEEE 802.11ac, "Part 11 : Wireless lan medium access control (mac) and physical layer (phy) specifications–amendment 4 : Enhancements for very high throughput for operation in bands below 6 ghz," ANSI/IEEE, Standard 802.11, 2013.

[133] IEEE 802.11ad, "Part 11 : Wireless lan medium access control (mac) and physical layer (phy) specifications - amendment 3 : Enhancements for very high throughput in the 60 ghz band," ANSI/IEEE, Standard 802.11, 2012.

[134] R. Soua, E. Livolant, and P. Minet, "Musika : A multichannel multi-sink data gathering algorithm in wireless sensor networks," in *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, July 2013, pp. 1370–1375.

[135] M. Bharathi, R. Tanguturi, C. Jayakumar, and K. Selvamani, "Node capture attack in wireless sensor network : A survey," in *Computational Intelligence & Computing Research*, December 2012.

[136] N. Alrajeh, K. A., and B. Shams, "Intrusion detection systems in wireless sensor networks : A review," *International Journal of Distributed Sensor Networks*, vol. 2013, p. 7, 2013.

[137] R. V. Kshirsagar and A. B. A. B. Jirapure, "A survey on fault detection and fault tolerance in wireless sensor networks," *IJCA Proceedings on International Conference on Benchmarks in Engineering Science and Technology 2012*, vol. ICBEST, no. 1, pp. 6–9, October 2012.

[138] D. Djenouri, A. Derhab, and N. Badache, *Ad hoc networks routing protocols and mobility*, vol. 3, April 2006.

[139] H. F., M. Z., M. A., A. K., and P. M., *Smart-HOP : A Reliable Handoff Mechanism for Mobile Wireless Sensor Networks*. Lecture Notes in Computer Science, 2012, vol. 7158, pp. 131–146.

[140] A. Mouawad, G. Chalhoub, and M. Misson, "Data management in a wireless sensor network with mobile nodes : A case study," in *Third International Conference on Wireless Communications in Unusual and Confined Areas (ICWCUCA)*, August 2012.

[141] A. Mouawad, G. Chalhoub, G. Habib, and M. Misson, "A performance study of mobile nodes in a wireless sensor network," in *Third International Conference on Communications and Information Technology (ICCIT)*, June 2013.

[142] D. Evans, "The internet of things - how the next evolution of the internet is changing everything," Cisco Internet Business Solutions Group, White paper, 2011.

[143] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks : Attacks and countermeasures," 2003.

[144] S. Ganesh and R. Amutha, "Efficient and secure routing protocol for wireless sensor networks through snr based dynamic clustering mechanisms," *Communications and Networks, Journal of*, vol. 15, no. 4, pp. 422–429, Aug 2013.

[145] T. M. Rahayu, S.-G. Lee, and H.-J. Lee, "A secure routing protocol for wireless sensor networks considering secure data aggregation," *Sensors*, vol. 15, no. 7, p. 15127, 2015.

[146] D. Tang, T. Li, J. Ren, and J. Wu, "Cost-aware secure routing (caser) protocol design for wireless sensor networks," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 26, no. 4, pp. 960–973, April 2015.

[147] S. E., K. M., and S. M., "Mac protocols security in wireless sensor networks : A survey," *International Journal of Computer and Information Technology*, vol. 3, no. 1, January 2014.

[148] C.-T. Hsueh, C.-Y. Wen, and Y.-C. Ouyang, "A secure scheme against power exhausting attacks in hierarchical wireless sensor networks," *Sensors Journal, IEEE*, vol. 15, no. 6, pp. 3590–3602, June 2015.

[149] G. Chalhoub, "Réseaux de capteurs sans fil," in *Workshop Réseaux et élécommunication de l'IUT*, November 2010.

[150] G. Chalhoub, "Du DNS au DNSSEC," in *Workshop Réseaux et élécommunication de l'IUT*, November 2014.

[151] D. D. W. Group, "Dnssec deployment initiative https ://www.dnssec-deployment.org," October 2015, last visited on October 2015.

[152] K. Bent, "http ://www.crn.com/slide-shows/networking/300071855/the-top-10-best-selling-access-points-by-brand.htm/," February 2014, last visited on October 2015.

[153] G. Chalhoub, N. Haddid, A. Guitton, and M. Misson, "Deference mechanisms significantly increase the MAC delay of slotted CSMA/CA," in *IEEE International Conference on Communications*, June 2009.

[154] N. E. Rachkidy, G. Chalhoub, A. Guitton, and M. Misson, "Queue-exchange mechanism to improve the QoS in a multi-stack architecture," in *ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks*, October 2011.

[155] P. Minet, G. Chalhoub, E. Livolant, M. Misson, B. Rmili, and J.-F. Perelgritz, "Adaptive wireless sensor networks for aircraft," in *IEEE International Conference on Wireless for Space and Extreme Environments*, December 2015.

[156] LAU, "www.aru-itvt.com," February 2015, last visited on September 2015.