POLITECNICO DI TORINO

SCUOLA DI DOTTORATO
Dottorato in Ingegneria Informatica e dei Sistemi – XXVI ciclo

Tesi di Dottorato

Reliable Communication in Wireless Networks

Zhang Linchao, 178728

Tutore
Prof. M. Rebaudengo

Coordinatore del corso di dottorato
Prof. P. Laface

2014

Acknowledgements

This thesis has been done in the research group inside the Department of Control and Computer Engineering (DAUIN) of Politecnico di Torino, Italy.

Firstly, I want to thank my family and friends for their long-term support during my study.

Then, I would like to express my sincere gratitude to my advisor, Prof.Maurizio Rebaudengo, for the profound advices and great helps in my PhD life. I also want to thank to my colleagues Filippo Gandino and Renato Ferrero, the discussion with them shows me the way to proceed in my scientific research and teaches me the methods to overcome difficulties. I have benefited enormously from working with them over the last three years.

Finally, thanks for the 5 years' life in Turin. I miss my homeland now, but I believe I will miss Turin in the future.

Contents

Summary

Wireless communication systems are increasingly being used in industries and infrastructures since they offer significant advantages such as cost effectiveness and scalability with respect to wired communication system. However, the broadcast feature and the unreliable links in the wireless communication system may cause more communication collisions and redundant transmissions. Consequently, guaranteeing reliable and efficient transmission in wireless communication systems has become a big challenging issue. In particular, analysis and evaluation of reliable transmission protocols in wireless sensor networks (WSNs) and radio frequency identification system (RFID) are strongly required.

This thesis proposes to model, analyze and evaluate self-configuration algorithms in wireless communication systems. The objective is to propose innovative solutions for communication protocols in WSNs and RFID systems, aiming at optimizing the performance of the algorithms in terms of throughput, reliability and power consumption. The first activity focuses on communication protocols in WSNs, which have been investigated, evaluated and optimized, in order to ensure fast and reliable data transmission between sensor nodes. The second research topic addresses the interference problem in RFID systems. The target is to evaluate and develop precise models for accurately describing the interference among readers. Based on these models, new solutions for reducing collision in RFID systems have been investigated.

The reliable transmission mechanisms from one node to another can be categorized into *non-acknowledgement (NoACK) based mechanism* and *acknowledgement (ACK) based mechanism.* In the NoACK-based mechanism, the sender schedules the transmission multiple times without knowing whether the transmission is successful or not. On the other hand, in the ACK-based mechanism, the sender expects an acknowledgement from the receiver for each transmission. The two end-to-end transmission mechanisms differ in the number of transmissions and in the number of collisions, consequently they may have different performance. The choice of the most appropriate transmission mechanism is crucial in many applications and a precise evaluation is highly dependent on the communication characteristics. In traditional networks, the end-to-end communication is usually modeled by a *point-to-point model.* Although it can also be applied to duty-cycle and sparse WSNs, it

does not take into account the broadcast characteristic of general WSNs in which one transmission may be listened by several neighbors. The one-to-many data transmission is typical in WSNs due to the broadcast characteristic and it can be modeled by the *point-to-multipoint model*. Furthermore, as the majority of energy consumption is spent while the node is waiting without action (*idle listening* state), a duty cycle mechanism is introduced in which each node shuts off the radio transceiver when no data are coming from its higher layers or other nodes. This mechanism requires further optimization to be combined with the reliable transmission mechanism in WSNs. In Chapter. 2, the performance of the NoACK- and ACK-based transmissions is analyzed and compared considering both the point-to-point model and the point-to-multipoint model. In particular, the point-to-multipoint model is evaluated considering the effect of the proposed selective acknowledgement mechanism. The theoretical analysis has been included in [1].

Despite of the theoretical analysis, it is worth to see the effects of the two reliable mechanisms on specific routing protocols. Opportunistic flooding [2] is the first research on a flooding method that is especially tailored for low-duty-cycle networks with unreliable wireless links and predetermined working schedules. It first predefines the flooding path along an energy optimal tree and then it adds "opportunistic" links outside the pre-computed tree in real time. Each sender makes probabilistic forwarding decisions by comparing the delay of the individual transmissions with the static delay distributions of the destination nodes. Chapter. 3 implements and evaluates the opportunistic flooding algorithm considering the NoACK- and ACK-based transmissions. Based on the evaluation results, the performance of the two transmission methods is presented and analyzed, providing a solid framework to decide which mechanism should be used according to the network requirements. The evaluation framework and partial results have been presented in [3] and [4].

Although the communication between RFID readers can be viewed as a particular case in WSN, it requires special anti-collision mechanisms to resolve three special types of interferences: tag-to-tag interference, reader-to-tag interference and reader-to-reader interference. Tag-to-tag interference can be avoided by tree-based algorithm, ALOHA and beam forming algorithm. Reader-to-tag can be solved by separating reader interrogating ranges. Instead, the reader-to-reader interference is still requiring more studies to address efficient solution. Although a number of researches related to analyzing reader-to-reader interference have been conducted so far, there is not a commonly agreed interference model that analyze the reader-to-reader interference in a mathematical way. The models adopted for describing the reader-to-reader interference can be categorized into two groups. The first group called *single interference model*, it assumes that each reader has a fixed interference range and it can collide only with other readers located within this distance. Under this hypothesis, the most popular one is the unit disk graph model. The second called *additive interference model*, which takes into account the power of all the exchanged signals. It assumes that all the interference power from multiple interfering readers to the target reader is additive and determines the collision with respect to the signal to interference plus noise (SINR) ratio. Both the propagation models have their own advantages and disadvantages, and the main models of the two families have been investigated in Chapter. 4. Based on that survey, a particular model for the reader-to-reader interference is proposed. Furthermore, a theoretical comparison between single interference model and additive interference model is presented based on the experimental results under three different evaluation scenarios. The results have been partially presented in [5] and [6].

Based on the comparison between single interference model and additive interference model, it is shown that the additive interference model is more accurate because it predicts more readers' interference. However, it is important to decide how many concurrent readers' interferences have to be considered for an additive interference model. That value determines a trade-off between the reliability and the efficiency of interference models for the RFID system. In Chapter. 5, the additive interference model with different values of n is evaluated. The evaluation is based on a proposed branch and bound algorithm that collects the numbers of minimal *collision-set-n*. A minimal collision-set-n is defined as the collision set with n members in which only the sum interference of all the member readers are larger than the threshold interference that can hamper the target readers interrogation activity, but the sum interference of any subset will have no influence. Based on the collected results, analysis of the throughput and the accuracy is further conducted. The analysis and evaluation are described in [7] and [8].

Although the researches in Chapter. 4 and Chapter. 5 have shown that the single interference model cannot detect a relevant part of the possible collisions detected by the additive model, the anti-collision protocols in the state-of-art are mainly based on the single interference model. As a result, a more complete evaluation based on an discrete event simulator is necessary. Chapter. 6 investigates on the general purposed simulators that are available for the simulation of reader-to-reader collisions. The design of an RFID system should carefully consider the reader-to-reader interference. Simulations can dramatically speed up the design and testing phase, by deferring the implementation of a prototype to the last phase of the development. Unfortunately, no specific simulators of interference in RFID networks are currently available. The state-of-the-art works exploit either general purpose network simulators, which often do not provide the required features for simulating an RFID network, or self deployed tools, which are not publicly available and therefore do not allow the validation and reproducibility of the results. Therefore, it is worthy to identify the requirements that a simulator of reader-to-reader interference should satisfy and propose a specifically designed simulator to evaluate the performance of reader-to-reader anti-collision protocols. Considering the defects of the existing

simulators, a novel simulator for reader-to-reader collisions in RFID system is presented, which is modular and easy to build the specific protocols or application behaviors. To test the simulator and simulate the performance of the additive interference model, several evaluation scenarios are assumed and the simulation results are presented.

Chapter 1

Introduction

1.1 Wireless Sensor Networks

A wireless sensor network (WSN) is a network in which each node is an embedded system equipped with multiple sensors that collect, process and exchange the information of the environment to perform various tasks [9] [10]. A typical sensor node, as shown in Figure 1.1, usually consists of one or more *autonomous sensors* to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, a *radio transceiver* or other wireless communications device responsible for communication with its neighbors, a *micro controller unit* that controls all activities of the node and executes communication protocols and an *energy source*, usually a battery. Besides, the sensor nodes can configure by themselves the communication with their neighbors and select data to transmit by means of their data processing component. Figure 1.2 shows a sensor device developed by Libelium company[1], which includes available connections to more than 60 sensors, 8 different wireless interfaces, supports for over the air programming and three sleep modes for low power consumption. The characteristics and constraints of WSNs include:

- *limited energy*, due to the power supply by batteries;
- *overlapping communication areas*, because of the broadcast feature of the antennas.
- *unreliable links* due to limited bandwidth and interferences in the environment;
- *dynamic network topology* because of the limited lifetime and node mobility;

[1] http://www.libelium.com/

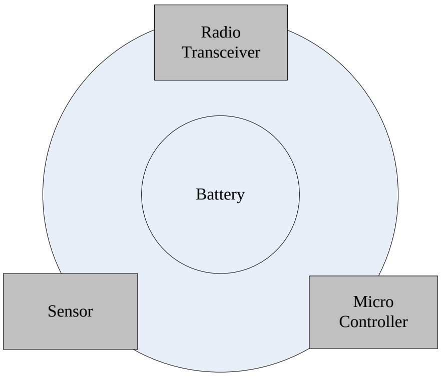


Figure 1.1. A typical sensor node structure

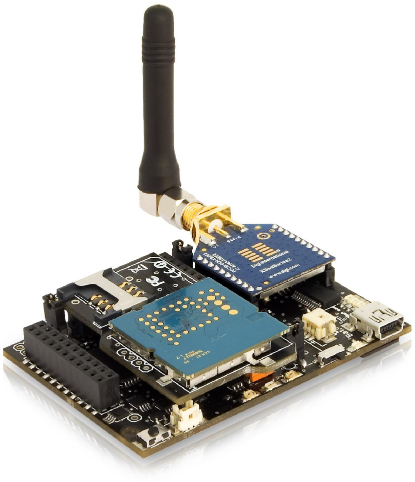


Figure 1.2. An example of the current sensor node: Waspmote

- *application oriented*, since different self-configuration algorithms are required with respect to the specific application.

Due to the *energy limitation*, an efficient power management [11] is essential for each sensor node in order to achieve a tradeoff between the lifetime and the performance. In particular, previous researches [12] have shown that the majority of energy consumption is spent when the node is waiting without performing any action (*idle listening* state). Sending each node to sleep in the idle listening state is proposed as an energy optimization solution. The percentage of time that a node is active is called *duty cycle*. A *duty cycle WSN* is defined as a network in which each node shuts down the radio transceiver when no data comes from its higher layer or from other nodes, in order to extend its lifetime. In a duty-cycle WSN, transmitted packets can not be received by all the neighbors simultaneously as in an always-awake network. In order to deliver a packet, a sender may have to wait until the destination node becomes active.

Due to the *overlapping communication areas*, the sensing activities and communications of sensor nodes should be scheduled according to anti-collision algorithms. Duty cycle mechanism can also alleviate the collision problem. Besides, an analysis of the optimal sensor node deployment [13] is also required in order to improve the coverage and minimize power requirements.

Due to the *unreliable links*, a packet can be completely lost even if it is reported by multiple sensor nodes. Consequently, special communication mechanisms has to be implemented in order to insure the reliable transmissions.

Finally, the *dynamic network topology* and the *application oriented* [14] characteristic of WSNs require appropriate routing protocols [15] at node level to minimize the power consumption and the transmission delay when forwarding the sensed information. In particular, many applications and network operations rely on the flooding technique [16] [17] for network-wide information dissemination from the source to all the other nodes. The main problems involved in flooding include two aspects: to avoid collisions in the MAC layer [18] and to minimize the transmission redundancy.

In the last years, the developments in micro-electro-mechanical systems and wireless communication technology have made WSNs increasingly applied in various areas including military, environment [19], infrastructure [20], indoor applications and industry monitoring [21]. The applications for WSNs are varied and typically involving some kind of monitoring, tracking, or controlling. A typical classification of the WSN-based applications is as follows:

- ***Military applications***: The wireless sensor networks were initially designed for the military applications. The features of robustness, self-organizing and fault tolerance make sensor networks appropriate for military use. Examples of the military applications of sensor networks are monitoring army, equipment and ammunition and enemy surveillance [22].

- ***Environment applications***: A number of WSNs have also been deployed for environment monitoring [19] since WSNs make it possible to realistically monitor the natural environment. For example, the real-time information captured by sensor nodes can be used for forest fire detection and flood detection. The Envisense Glacs Web project [23] has developed a monitoring system for a glacial environment. Monitoring the ice caps and glaciers provides valuable information about the global warming and climate change.

- ***Infrastructure applications***: Infrastructure is the basic physical and organizational structures needed for the operation of a society or enterprise, or the services and facilities necessary for an economy to function. WSNs have been widely used in this area like fleet monitoring and traffic control. For example, in fleet monitoring, it is possible to put a mote with a GPS module on-board of each ship. The mote gathers it's position via the GPS module, and reports its coordinates so that the location is tracked in real-time. The motes can be equipped with temperature sensors to avoid any disruption of the cold chain, helping to ensure the safety of food, pharmaceutical and chemical shipments. In situations where there is not reliable GPS coverage, like inside buildings, garages and tunnels, using information from GSM cells is an alternative for to GPS localization.

- ***Indoor applications***: Home automation [24] is a promising example of indoor applications. As for home automation, tiny sensor nodes could be attached to the electrical appliances such as air-conditioner, computer, refrigerator etc. These sensor nodes can communicate with each other or with the users who live outside this network. The users can control these appliances via the internet or satellite network.

- ***Industry monitoring applications***: WSNs are also applied to various industrial monitoring areas like agriculture, retail business, products manufacturing, medical and infrastructure industries. For example, reference [21] illustrated the role of wireless sensor network in data gathering and emergence rescue navigation.

1.2 Radio Frequency Identification System

Radio Frequency IDentification (RFID) is a leading technology in Automatic Identification and Data Capture (AIDC). With the growing interest of end users in different applications, RFID technology is increasingly used in various areas such as identification, tracking, monitoring and electronic payment [25, 26, 27] because of its ubiquitous features such as location-aware, widespread and transparent to users. Other advantages in RFID adoption also include an increase in process efficiency, a complete item traceability and a better quality control. To some extent, RFID system can be viewed as a special case of wireless sensor networks with the only difference that the information is stored in the RFID tags instead of sensor node in WSNs.

A basic RFID system is composed of several *tags*, one or more *readers* and a central *server*. The tag contains data which can be read by the readers located in the field. A unique Electronic Product Code (EPC) is stored in each tag. The range within which a reader can communicate with a tag is referred to as the *interrogation range* of the reader. The central server receives, processes and stores the data sent by the reader. According to [28], the entry of new players, the technological advancements and the growing government support will make the global RFID market grow at a compound annual growth rate of around 18% to a value of approximately $19.3 billion in the period of 2011-2014.

The readers in the RFID system operate in a specific frequency. The adopted frequency bands can be classified as

- low frequency (LF), between 125 and 134 KHz;
- high frequency (HF), at 13.56 MHz;
- ultra high frequency (UHF), between 866 and 868 MHz in EU, between 902 and 928 MHz in USA;
- microwave at 2.45 GHz in EU, between 2.4 and 2.4835 GHz and between 5.725 and 5.85 GHz in USA.

Most of the RFID systems work at UHF [29] and many large installations deploy *dense reader environments* [30] where there are multiple readers in mutual range.

Tags are categorized into *passive*, *semi-passive* and *active*. UHF passive tags only respond to a reader's interrogation, since they use back scatter modulation to reflect the reader's signal right back. The microchip of the tag is powered by the electromagnetic field emitted by the reader. This energy requirement restricts the operating range of a passive tag to a maximum of 10 meters. UHF semi-passive tags include a battery to operate the microchip, but they exploit passive tag's backscatter mechanism for uplink communication. With self-sufficient power supply, the constraining factor in the operating range of semi-passive tags becomes the weakness of their generating signal and, thereby, the sensitivity of the reader's receiver. The theoretical operating range of a UHF semi-passive tag is more than 20 m. Active tags are supplied by a more powerful battery cell, so they can generate a radio frequency signal to reply to a reader interrogation and they can also initiate a communication. The interrogation range of active tags is considerably longer, up to some hundreds of meters. However, passive RFID applications are by far the most adopted for their best trade-off between cost and performance.

1.3 Reliable Communication in WSNs and RFID Systems

In wireless networks, it is necessary to consider the *Quality of service* (QoS) requirements, i.e., real-time and reliable communication, because the sensed information must be transmitted to the sink or neighboring nodes reliably and in time. Delayed or lost data may cause WSN-based applications behave irregularly or fail.

Data transmissions in WSNs are more susceptible to suffer from packet loss than over traditional wired networks. That is because in wired network data loss occurs mainly due to congestion, whereas data loss in WSNs can be caused by various reasons such as node failures, environmental noise and simultaneous interferences. In addition, packet loss in the network can also waste energy with respect to the end-to-end reliability. Therefore, guaranteeing reliable communication, i.e., delivering data to destination successfully, has become a big challenging issue for researches and applications in WSNs.

More critical issues arise in RFID systems, because the interrogation activity is susceptible to suffer from the interferences of the simultaneous activities of other RFID readers or tags. The causes of unreliable communications in RFID systems can be classified into the following 3 types:

- Tag-to-Tag interference (TTI): a reader communicates at the same time with multiple tags located inside its interrogation zone and is unable to distinguish their signals;
- Reader-to-Tag interference (RTI): when two or more readers, independently of the working frequency, transmit at the same time, overlapping their read ranges and powering the same tag;
- Reader-to-Reader interference (RRI): when one reader interrogates a tag, it can receive strong signals from one or more readers that are interrogating other tags using the same radio frequency, disturbing the weak signal backscattered from the target tag.

Tag-to-tag collision is a well-known problem. The majority of the proposed solutions exploit Time Division Multiple Access (TDMA) [31], which splits the available channel among the tags. They are classified into the tag-driven and reader-driven categories, depending on the subject that controls the data transfer. In tag-driven protocols, the tags communicate only if they have information to send. A first solution was based on Aloha algorithm [32], in which successful communication is stopped by an acknowledge message. Subsequent implementations have divided time into timeslots, to reduce the occurrence of collisions [33, 34]. In reader-driven algorithms, the reader schedules the querying tags: the synchronization increases the scalability and reduces the length of the communication. The most relevant protocols of this family are classified in polling [35] and tree-based approaches [36, 37]. With polling, the reader has a list of the serial numbers of all the tags in its interrogation zone, and queries them in turn [35]. Tree-based protocols recursively split the set of colliding tags, to identify subsets of tags that can consecutively transmit [36, 37].

Reader-to-tag collision occurs when two or more readers overlap their reader-to-tag read ranges and try to read the same tag simultaneously. In this case, the

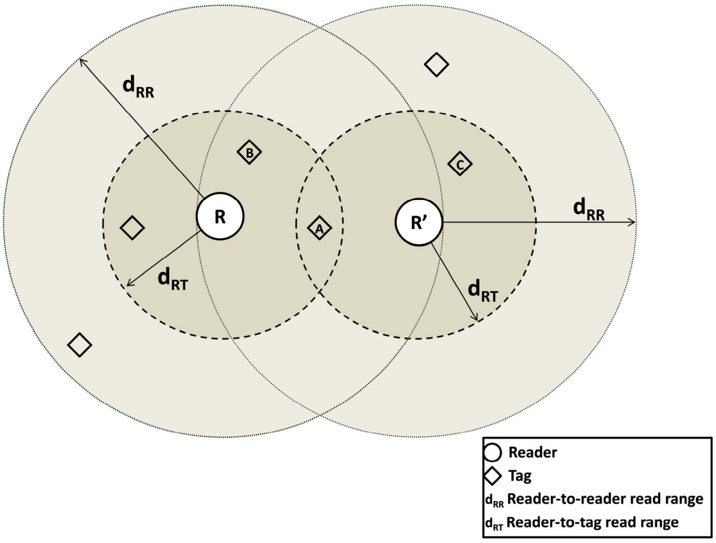

d_{RR}
B
R
A
R'
C
d_{RR}
d_{RT}
d_{RT}
○ Reader
◇ Tag
d_{RR} Reader-to-reader read range
d_{RT} Reader-to-tag read range

Figure 1.3. Reader interference

physical distance between these readers is lower than the double of the interrogation range. In Figure 1.3, if R and $R^{'}$ try to identify tag A, A receives electromagnetic waves from both readers simultaneously. Reader-to-tag collision can be partially solved by managing reader-to-reader collisions [38, 39]. If simultaneous interrogations of nearby readers are avoided, tags are not queried by more than one reader at the same time. However, two readers can generate a reader-to-tag collision but not a reader-to-reader collision if they operate at different frequencies. Therefore, approaches based on Frequency Division Multiple Access (FDMA) are less effective than TDMA-based techniques for limiting the reader-to-tag collision.

Reader-to-reader collision happens when the signal generated by one reader interferes with the reception system of other readers. It only occurs when the physical distance between two or more readers is lower than the interference range. Reader-to-reader collision hinders the tag identification process: a reader can receive strong signals from neighboring readers, interfering with the weak response signal from the tag. In Figure 1.3, if R reads data from tag B and, at the same time, $R^{'}$ sends data to tag C, $R^{'}$ interferes with R. While tag-to-tag and reader-to-tag collisions are limited by the interrogation range, the range of the reader-to-reader interference amounts to a larger area [40]. Reader-to-reader collisions are particularly critical in *Dense Reader Environments* (DREs), where multiple readers are located in close proximity to each other. These scenarios are common when a single reader is not enough to cover a specific identification area, or simply when the final application requires the existence of multiple checking areas. DREs can also be implemented to improve read rate and reliability, as they ensure high probability of tag identification [41].

Chapter 2

Reliable Transmission Mechanism in Wireless Sensor Networks

There are two categories of reliable transmission mechanisms in the end-to-end data transfer: the *non-acknowledgement (NoACK) based mechanism* and the *acknowledgement (ACK) based mechanism.* The two end-to-end transmission mechanisms differ in the number of transmissions and in the number of collisions, consequently they may have different performance. This chapter will analyze the two mechanisms under both the point-to-point model and the point-to-multipoint model. A selective acknowledgement mechanism considering the broadcast feature of WSNs is also proposed. Based on the results, metrics for the choice of the most appropriate transmission mechanism is presented and evaluated.

2.1 Duty-cycle WSNs

The limited energy of each sensor node is prime challenge of the wireless sensor networks. As a result, energy consumption is the primary concern and minimizing such is a key objective. On the other hand, there is a growing need for sustainable deployment of sensor systems to reduce operational cost and ensure service continuity. To bridge the gap between limited energy supplies and application lifetimes, energy optimization should be applied to wireless sensor network.

Typically, the energy used in communication can be optimized through

- Physical-layer transmission rate scaling [18]
- Link-layer optimization for better connectivity, reliability, and stability [19]
- Network-layer enhancement for better forwarders and routes [20, 21]

- Application-layer improvements for both content-agnostic and content-centric data aggregation and inference [22]

Although these solutions are highly diverse, they all assume a wireless network in which nodes are ready to receive packets and focus mainly on the transmission side. In recent years, as researches had discovered that nodes are idle for a long time if no sensor event happens which is usually referred as idle listening. For example [24], the widely adopted ChipCon CC2420 radio draws 19.7mA when receiving or idle listening, which is actually larger than the 17.4mA used when transmitting. More importantly, packet transmission time is usually very brief (e.g., 1.3 milliseconds to transmit a TinyOS packet using a CC2420 radio), while idle listening can be orders of magnitude longer. With a comparable current draw and a 3 4 orders of magnitude longer duration waiting for reception, idle listening is a major energy drain that accounts for most of the energy cost in communication. Therefore, low-duty-cycle network was introduced in which a sensor node schedules itself to be active for only a brief period of time and then stays dormant for a long time. Duty cycle is defined as the percentage of time a node is active in the whole operational time.

In low-duty-cycle network, as each sensor node is periodically active and dormant, it should have a schedule to follow. In order to deliver a packet, a sender may have to wait for a certain period of time (termed sleep latency [23]) until its receiver becomes active. From the communication energy point of view, a sensor in duty cycle wireless sensor network should have four states [25]: sleeping, receiving, transmitting and switching between the three former states.

Although efficient toward saving energy, duty-cycling causes many challenges such as difficulty in neighbor discovery due to asynchronous wakeup/sleep scheduling, time-varying transmissions latencies due to varying neighbor discovery latencies, and difficulty on multi-hop broadcasting due to non-simultaneous wakeup in neighborhood.

2.2 NoACK- and ACK-based Transmission Mechanisms

Many contention based MAC protocols for WSNs have been designed in the last years with the goal of avoiding collisions in order to reduce the energy consumption. Duty cycle mechanisms are considered in some MAC protocols like S-MAC [42], T-MAC [43], B-MAC [44] and X-MAC [45]. Duty cycle MAC protocols can be classified in two types: synchronous and asynchronous. In synchronous protocols, such as S-MAC and T-MAC, the schedule of a node is negotiated among the neighbors to specify when it is awake and asleep. In asynchronous protocols such as B-MAC and

X-MAC, preamble samplings are used by the sender to notify the receiver of a scheduled transmission. Both B-MAC and X-MAC work on top of the IEEE standard 802.15.4 [46] [47], which is used in WSNs. These MAC protocols manage to minimize the energy consumption by optimizing the lower layers. However, the routing path selection can still produce redundant transmissions even without any collision during the low layer communication. The management of redundant transmissions in the routing protocol becomes crucial in high density networks.

In traditional networks, the end-to-end communication is usually modeled by a *point-to-point* model. Although point-to-point model can be applied to duty-cycle and sparse WSNs, it does not take into account the broadcast characteristic of general WSNs in which one transmission may be listened by several neighbors. Considering broadcast characteristic, the one-to-many data transmission in WSNs can be modeled by the *point-to-multipoint* model. Besides, the transmission mechanisms to achieve reliable communication in WSNs can be categorized into *non-acknowledgement (NoACK) based mechanism* and *acknowledgement (ACK) based mechanism*. In the NoACK-based mechanism, the sender schedules the transmission multiple times to the receiver without knowing whether the transmission is successful or not. On the other hand, in the ACK-based mechanism, the sender expects an acknowledgement for each transmission. The two end-to-end transmission mechanisms differ in the number of transmissions and in the number of collisions, consequently they may have different performance. The choice of the most appropriate transmission mechanism is crucial in many applications and a precise evaluation is highly dependent on the communication characteristics.

2.3 Performance Analysis in the Point-to-Point Model

In the NoACK-based transmission mechanism, the sender transmits to the receiver for a predetermined number of times no matter whether the receiver has received the packet or not. In order to take into account the unreliability of a wireless transmission, each link is modeled with a probability q called *link quality*, which corresponds to the probability of a successful transmission along this link. The sender determines a priori the number of retransmissions so that the probability of receiving the message is larger than a threshold p. In the *Point-to-Point* model where one transmission can be received by only one receiver, the required number of transmissions can be calculated as

$$N_1 = min\{n \in N^+ : \sum_{i=1}^{n} q(1-q)^{i-1} \geq p\}. \tag{2.1}$$

Since the summation in the above equation is a geometric series, it can get

$$n \geq log_{1-q}(1-p). \tag{2.2}$$

And consequently,

$$N_1 = \lceil log_{1-q}(1-p) \rceil. \tag{2.3}$$

On the other hand, in the ACK-based transmission mechanism, the sender node expects an acknowledgement packet, which indicates a successful transmission. Whenever a node receives a packet, it replies to the sender with an acknowledgement packet. Only after receiving the acknowledgement, the sender stops transmitting. With this mechanism, a successful transmission means a successful data transmission and a subsequent successful acknowledgement transmission. Therefore, considering symmetric network where the link quality q is identical for the bidirectional communication, the probability of a successful transmission is q^2. Consequently the unsuccessful probability is $1 - q^2$. Based on Equation (2.1) and (2.2), the minimum number of transmissions N_s that guarantees a transmission with a successful probability greater than p is

$$N_s = \lceil log_{1-q^2}(1-p) \rceil \tag{2.4}$$

However, the number of attempted transmissions is usually smaller than the required one. The probability that the round-trip transmission in an ACK-based mechanism is unsuccessful until the i^{th} transmission is

$$p_i = q^2(1-q^2)^{i-1}. \tag{2.5}$$

In other words, the probability that the transmission succeeds with exactly i transmissions is p_i. Consequently the probability distribution of the required number of transmissions can be represented as a set of tuples $\{(i,p_i)\}$. The expectation value of the number of transmissions in the ACK-based mechanism is:

$$D = \sum_{i=1}^{N_s} i \cdot p_i. \tag{2.6}$$

Because of the symmetric link quality, half of the unsuccessful round-trip transmissions on the average is caused by the loss of the data packet, and the other half is due to the loss of the acknowledgment packet. Therefore, the number of acknowledgement transmissions can be estimated as half of the data transmissions. In order to compare the performance of the ACK- and NoACK-based transmission mechanisms, α is defined as the ratio between $\bar{e}_{ack}$, the cost of one acknowledgment transmission, and $\bar{e}_{data}$, the cost of one data transmission:

$$\alpha = \frac{\bar{e}_{ack}}{\bar{e}_{data}}. \tag{2.7}$$

Based on the above analysis, the expectation value of the number of acknowledgment transmissions is

$$A = \frac{\alpha}{2} \sum_{i=1}^{N_s} i \cdot p_i. \tag{2.8}$$

Finally, based on Equation (2.5), (2.6) and (2.8), the total number of transmissions in the ACK-based mechanism is:

$$N_2 = D + A = (1 + \frac{\alpha}{2}) \sum_{i=1}^{N_s} i \cdot q^2(1-q^2)^{i-1}. \tag{2.9}$$

where N_s is calculated using Equation (2.4) to avoid endless transmissions.

No matter the transmission mechanism, the interval between the first transmission and the first successful transmission is the same. The acknowledgement does not change the receive time of the receiver but just the number of transmissions. Therefore, the number of transmissions becomes the only valid metric to compare the performance.

In a duty-cycle and sparse WSN, broadcast is essentially realized by a number of point-to-point transmissions (or *unicasts*) since the probability that two neighbors are active at the same time is very low [2]. Consequently, the broadcast capability in WSNs fades away and a node needs to transmit packet to its neighbors one by one due to their different working schedules. In this situation, point-to-point model can be used in WSNs.

Figure 2.1 shows the numerical evaluation of the NoACK- and ACK-based transmission mechanisms under point-to-point model with respect to different link qualities. $p = 0.99$ is used as the threshold probability of a successful transmission and two α values are used (1 and 0.25). It can be observed that the ACK-based mechanism always outperforms the NoACK-based mechanism when the link quality is between 0.4 and p. When the link quality is between p and 1, the NoACK-based mechanism needs one transmission while the ACK-based mechanism needs one round-trip transmission. On the other hand, the NoACK-based mechanism in the point-to-point model gives better performance in a extremely high packet loss environment since low link quality is more likely to cause an acknowledgement loss. The ratio α influences the energy performance of the ACK-based mechanism, but this influence becomes smaller as the link quality increases. That is because when the link quality increases, the loss of acknowledgment reduces.

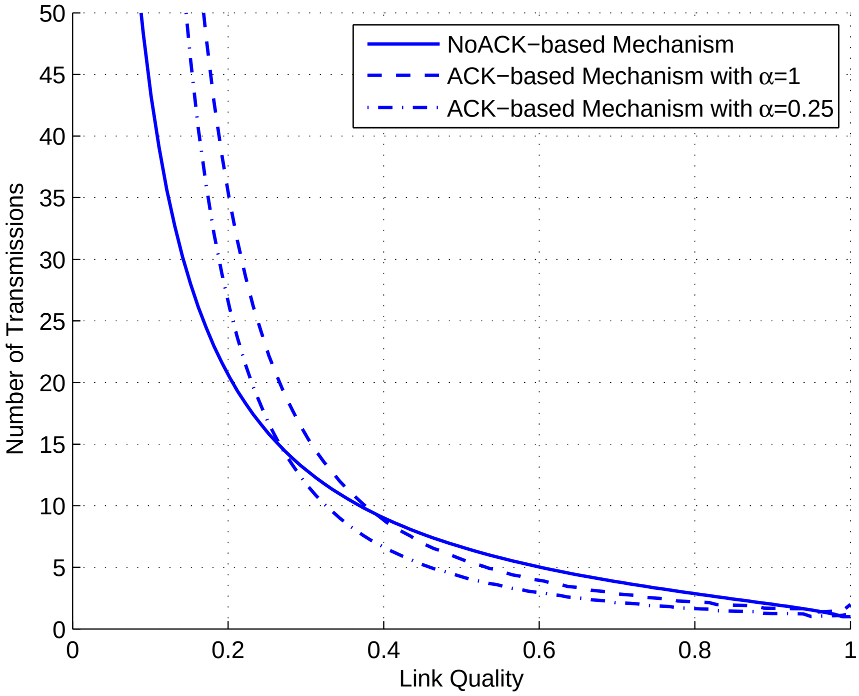


Figure 2.1. Comparison of NoACK- and ACK-based Transmissions in Point-to-Point Model

2.4 The Selective Acknowledgement Mechanism for the Point-to-Multipoint Model

According to the broadcast feature of the radio layer in WSNs, when a node sends out a packet, all the currently active neighbors receive the packet no matter what the expected destination node is. A neighbor is called *overhearing* when it is not the expected destination. In the NoACK-based transmission mechanism, since the sender does not need any reply from the receiver, the multi-transmission mechanism in the point-to-point model just evolves into "multi-broadcasting" in the point-to-multipoint model.

Instead, the ACK-based mechanism in the point-to-point model can produce redundant transmissions in the point-to-multipoint model. Firstly, since the overhearing nodes are not the actual destinations of the sender, it is not required that they send back the acknowledgements. Secondly, when there are multiple destinations, the nodes who have successfully sent back the acknowledgement do not need to respond to the subsequent broadcast packets anymore. For example, considering the scenario where a sender S wants to send packets to neighbors A and B, S will expect the acknowledgments from both of them. After several broadcasts, it may happen that S has already received the acknowledgement from A but B's reply is still missing. To ensure that B receives the packet, S will continue broadcasting the packet. Although A continues to receive the packet, it does not need to reply with an acknowledgement again.

To reduce this redundancy, a *selective acknowledgement mechanism* is proposed in which a field called *destination set* is added into each data packet. Before each transmission, the sender includes all the destinations' address in the destination set of the packet. When a node receives a packet, it first checks whether it is in the destination set of the received packet. Only if it is in the destination set, it will reply to the sender node with an acknowledgement packet. The overhearing nodes are the nodes who are not included in the destination set of the received packet. On the other hand, whenever a sender receives the acknowledgement packet from a destination node, it removes the corresponding node address from the destination set.

Another problem in the ACK-based mechanism caused by the broadcast feature of WSNs is the collision between the acknowledgments. When two nodes receive a packet from the same sender, if they both send back the acknowledgement packet immediately, a collision may occur. The situation when two nodes are trying to forward a packet to the same node without knowing each other is called *Hidden Terminal Problem* [2]. To alleviate this problem, the backoff method is used: before sending back the acknowledgement packet, each node waits a certain time in order to avoid collisions. The backoff time of each node is calculated based on the link quality and the destination set according to the following algorithm:

1. Sort all the nodes in the sender set S according to the descending order of the link quality;

2. Assume i is the index of node S_i, the backoff time of S_i is:

$$T_i = i \cdot \frac{T_{backoff}}{W}. \tag{2.10}$$

   where the backoff bound is $T_{backoff}$ and W is the size of the sender set.

In this way, the node with a better link quality will send the acknowledgement first and the minimum interval between two nodes is exactly $\frac{T_{backoff}}{W}$. It is assumed that the ACK delay is not larger than $\frac{T_{backoff}}{W}$ (which means one ACK should arrive before the starting time of the next ACK), otherwise, the ACK is considered as lost.

Figure 2.2 shows an example of the selective acknowledgement mechanism. When the node S plans to send a packet to A and B, it puts them into the destination set of the packet. As D has the same working schedule with A and B, it will also receive the packet simultaneously. However, D will not send back an acknowledgment because it is not in the destination set of the received packet. On the other hand, B will return the acknowledgement packet immediately but A has to wait a certain time to make sure that B has completed its transmission.

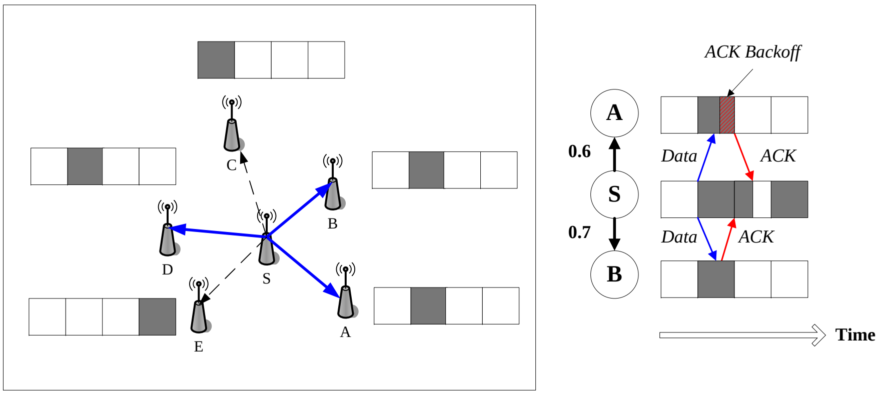


Figure 2.2. The Selective Acknowledgement Mechanism

2.5 Performance Analysis in the Point-to-Multipoint Model

Among the neighborhood $\triangle_S$ of a sensor node S, the neighbors have different link qualities to/from node S. Therefore, each couple of the sender node S and a neighbor can be modeled by a point-to-point model. According to the analysis in section 2.3, each neighbor j requires a different number of transmissions N_j. In the NoACK-based mechanism of point-to-multipoint model, since one broadcast data transmission is addressed to all the neighbors, the required number of transmissions is the maximum one among all the estimated N_j, i.e.,

$$N_1^{'} = max\{N_j : j \in \triangle_S\}. \tag{2.11}$$

where N_j is calculated according to Equation (2.1) corresponding to the link quality q_j from the sender A to the neighbor j.

In the ACK-based mechanism, the number of data packet transmissions is determined by the maximum one among all the estimated D_j according to Equation (2.6). On the other hand, the number of acknowledgement transmissions is the sum of all the estimated number of acknowledgement A_j according to Equation (2.8). The reason is that for every broadcast data transmission, the possible acknowledgment reply from the neighbors depends on the link quality q_j from the sender to j. Therefore, the total expected number of transmissions for the ACK-based broadcast is

$$N_2^{'} = max\{D_j : j \in \triangle_j\} + \frac{\alpha}{2} \sum_{j \in \triangle_j} A_j. \tag{2.12}$$

Figure 2.3 plots the numerical results in a point-to-multipoint model where the objective probability of a successful broadcast transmission is $p = 0.99$. The link qualities from the sender to all the neighbors are randomly generated between 0.5 and 1. The number of neighbors varies from 1 to 30 and for each case, 100 experiments are executed in order to alleviate the effect of randomness. It is assumed that no acknowledgement collision happens. The results show that when the number of neighbors is lower than 3, the ACK-based transmission mechanism outperforms the NoACK-based one no matter α is. When the neighborhood size is between 3 and 10, the ACK-based mechanism is better only for $\alpha = 0.25$. Finally, in a dense WSN with more than 14 neighbors, the NoACK-based mechanism gives a better performance than the ACK-based one. The number of transmissions in the ACK-based mechanism increases linearly with respect to the increase of the neighborhood size. Consequently, the average results turn out a linear relationship between the number of transmissions and the number of neighbors in Equation (2.12).

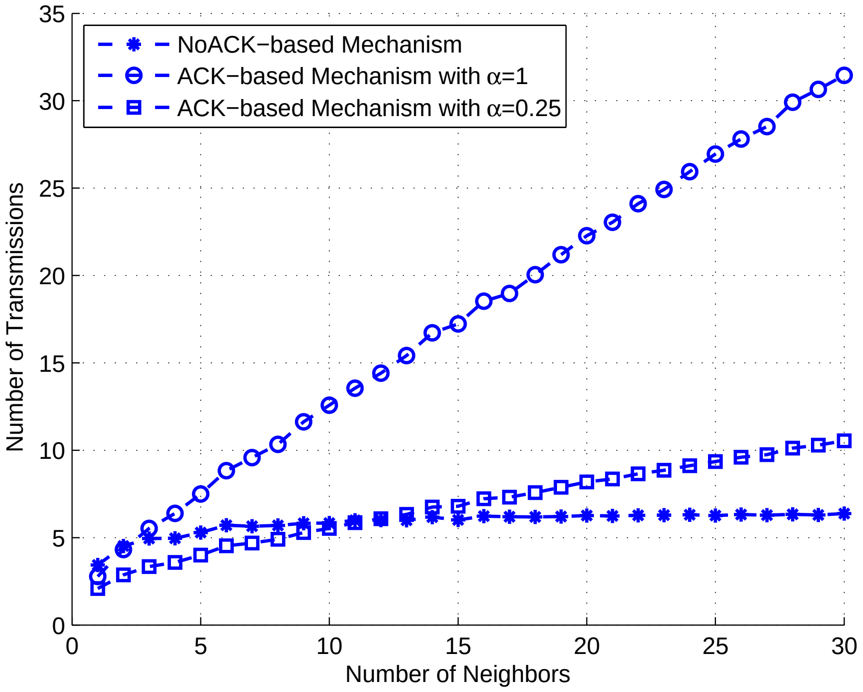


Figure 2.3. Comparison of Unreliable and Reliable Transmissions in Point-to-Multipoint Model

Chapter 3

ACK-based and NoACK-based Opportunistic Flooding in Wireless Sensor Networks

Considering the low-duty-cycle WSNs with unreliable links, the opportunistic flooding algorithm [2] is especially designed to make sure all the nodes in the network will receive the flooded data. However, adopting either NoACK- or ACK-based transmission mechanisms will strongly influence the performance of a protocol in WSNs. This chapter further analyzes the opportunistic flooding algorithm based on the NoACK- and ACK-based transmission mechanisms. Based on the evaluation results, the performance of the two transmission methods is presented and analyzed, providing a solid framework to decide which mechanism has to be used according to the network requirements.

3.1 Opportunistic Flooding Algorithm

The performance of the NoACK- and ACK-based transmission mechanisms is investigated when the two mechanisms are applied in conjunction with the opportunistic flooding algorithm. After describing the network model and assumptions, this section introduces the opportunistic flooding algorithm. The opportunistic flooding algorithm is composed by two parts: an initial estimation of static delay distribution and a decision making process in the flooding phase.

3.1.1 Network model and assumptions

The opportunistic flooding algorithm is designed for a duty-cycle network with unreliable links. From the communication energy point of view, a sensor node in the duty cycle network has four states [48]: sleeping, receiving, transmitting and switching between the three former states. Considering routing protocols in a higher layer, the states of the node in a duty cycle network can be further simplified into two states: *active* and *dormant*. In the active state the node can receive and transmit packets; when dormant, it turns off all its function modules. The switch between the two states follows the working schedule of the node. The working time is divided into frames of length T_f and each frame is further splitted into several time units of length t. Each node picks t_i as its active unit. Since a node can transmit a packet at any time, but can only receive a packet when it is active, the node should be active not only during its active unit but also when it has some packet to send.

The schedule of each node is normally periodic and, to make sure that a node knows when it can send a packet to its neighbors, it is assumed that each node's schedule is locally synchronized between all its neighbors using the MAC-layer time stamping technique [49]. A *hop count*, representing the hierarchical level of each node in the network, is introduced to indicate the minimum number of hops from the source, which is the root node in the routing tree. All the nodes can only transmit packets to nodes with larger hop count to avoid data loops in the flooding.

Figure 3.1 shows an example of the network model where the working period of each node is divided into 4 time units. The quality of the links A-B and B-C is 0.7 and 0.6, respectively. When A receives the flooding packet at the first active unit, it can schedule the transmissions to B according to B's active schedule. However, as the probability of a successful transmission from A to B is 0.7, node B may receive the packet in the second or third active unit. If B receives the packet at the second active unit, it can start the transmissions to C from the second active unit of C. Otherwise, it can only schedule the transmission after the third active time unit of C.

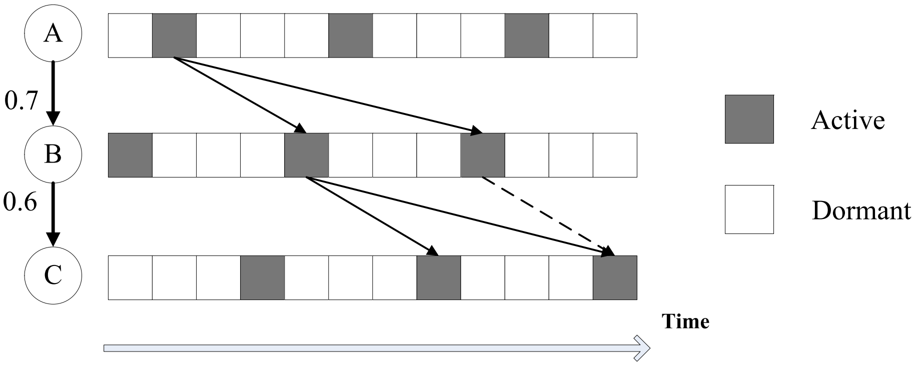


Figure 3.1. The network model considering duty cycle and unreliable links

When each node is assigned with a hop count, the topology of the network can be viewed as a directed acyclic graph (DAG). The weight of each edge is the corresponding link quality. Then an energy optimal tree (OPT) can be acquired along which the transmission of packets can be mostly reliable and thus minimize the expected total number of transmissions. The details of the OPT will be elaborated in the next section.

Generally opportunistic flooding is based on the OPT because of the maximum power saving it provides. However, flooding via the energy optimal tree may have a long flooding delay, since a node's parent may not receive the flooding packet as early as its other neighbors due to the unreliable nature of wireless communication. Therefore, opportunistic flooding provides another optional secondary path outside of the energy optimal tree. It utilize these outside links when the transmissions via the secondary path have a high chance of making the receiving node receive the packet "statistically earlier" than its parent. And this is where the keyword "opportunistic" comes from.

Clearly, the way to decide whether to send the opportunistic packet outside the optimal tree becomes the kernel part of the opportunistic flooding algorithm. When a node receives the flooding packet the first time, it should analyze whether the packet to be forwarded opportunistically (via the link outside the energy optimal tree) is statistically earlier than the packet that is otherwise delivered normally (via the energy OPT). Consequently, opportunistic flooding consists of three major steps, as illustrated in Figure 3.2:

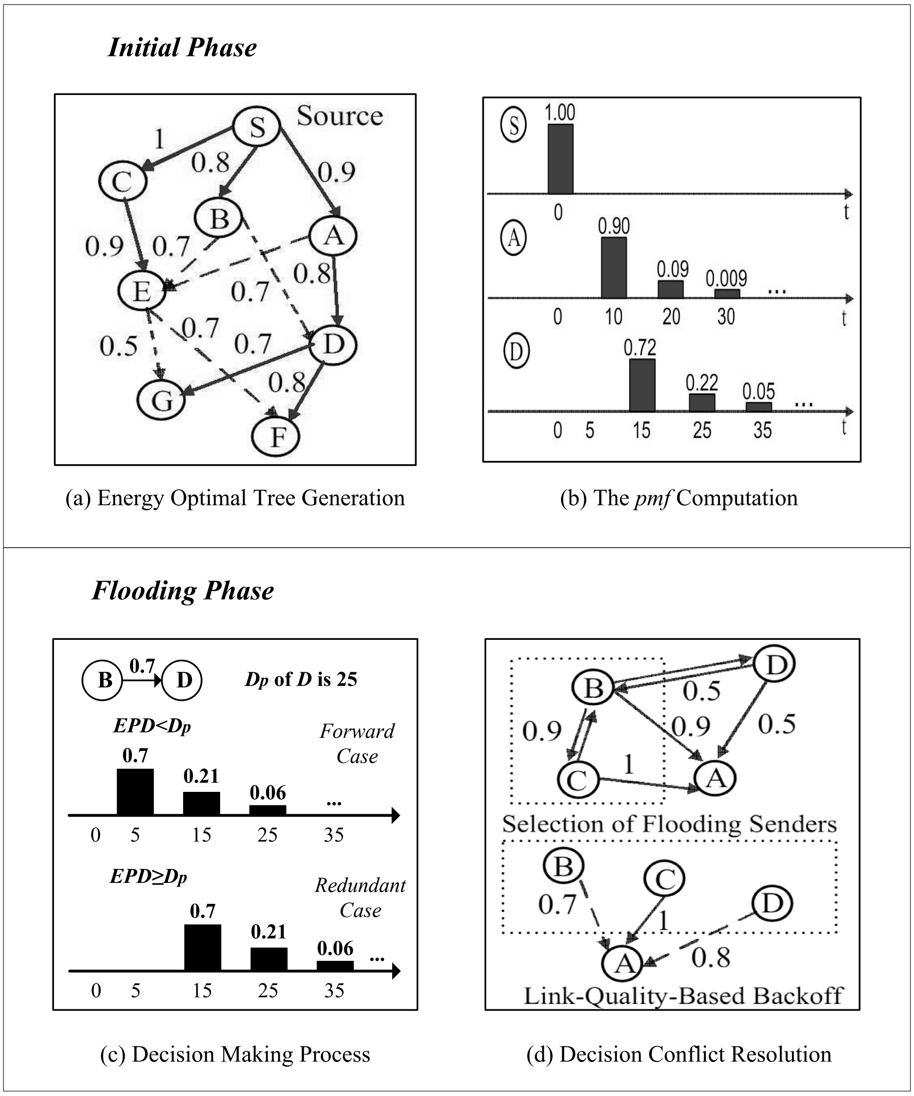
1. **The *pmf* Computation:** Due to unreliable links, the delay of a flooding packet arriving at each node through the energy-optimal tree is a random variable. But anyway the distribution of this delay can be calculated to estimate the receiving delay of each node in the energy optimal tree with a specific probability (P_{th}). In the design shown in Figure 3.2 (a) and (b), the probability mass function (*pmf*) of this delay is first derived for each node to guide the decision making process. From the *pmf*, each node computes its p-quantile delay D_p as the statistically significant threshold and shares this with all its pervious-hop nodes.

2. **Decision Making Process:** As shown in Figure 3.2(c), if the flood packet arrives earlier enough that it can significantly reduce the delay (the p-quantile delay D_p is used to control the statistical significance) when it's forwarded via the link outside of the energy OPT, it will be forwarded via the opportunistic link. Otherwise, it will ignore it. Specifically, a node makes its forwarding decision locally based on three inputs: (i) the receiving time of the flooding packet, (ii) the link quality between itself and the next-hop node, and (iii) the p-quantile.

3. **Decision Conflict Resolution:** Since each node makes its forwarding decision in a purely distributed manner, it would be the case that multiple nodes

decide to forward the same packet to a common neighbor, which is called decision conflict. Two conflict resolution techniques are designed to avoid collisions and save energy further, as shown in Figure 3.2(d).

In all, opportunistic flooding normally floods a packet via the links in the energy optimal tree to reduce redundancy and save energy, at the same time, it permit the packet to travel along an opportunistically fast route outside of the energy optimal tree. Detailed designs are shown in the following subsections.



(a) Energy Optimal Tree Generation

(b) The *pmf* Computation

(c) Decision Making Process

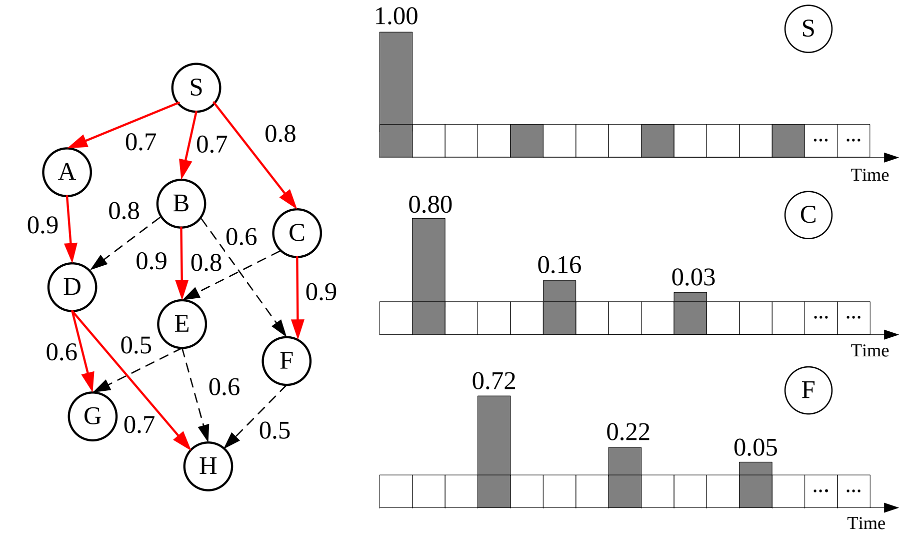
(d) Decision Conflict Resolution

Figure 3.2. Design overview of opportunistic flooding

3.1.2 Static delay distribution estimation

Each node has a specific hop count and a packet can be transmitted only to the nodes with a larger hop count. As a result, the flooding structure of the network is a directed acyclic graph. Therefore, an *Energy Optimal Tree* [2] can be generated by assigning to each node an incoming link with the best link quality among the available links. For example, as shown in Figure 3.3(a), node E has three incoming links from A, B and C with link quality 0.7, 0.7 and 0.9, respectively. The link from C to E needs the fewest number of transmissions among the three links. Therefore, E will pick C as its energy optimal parent node. The links with solid line compose the energy optimal tree of the network in Figure 3.3(a).

However, if the flooding only goes along the energy optimal tree, a node may receive the packet too late. A delay or a loss in the reception of the packet is propagated to all the successive nodes, leading to a reduced coverage ratio of the flooding. Therefore, in the opportunistic flooding algorithm, the flooding is normally routed along the energy optimal tree but some *opportunistically early* transmissions are forwarded using links outside the energy optimal tree, called *opportunistic links*. The opportunistic links give a higher chance of receiving the packets earlier than links along the energy optimal tree. To determine whether a transmission is *opportunistically early*, each node makes forwarding decisions based on the statistic packet delay distribution.



(a) Energy optimal tree generation (b) The *pmf* computation

Figure 3.3. The Estimation of Static Delay Distribution

The opportunistic flooding algorithm can be divided into two phases: *initial phase* and *flooding phase*:

Initial phase mainly calculates the delay distribution (*pmf*) of each node in the energy optimal tree, consequently acquired D_p using the Equation (3.2) and complete the selection of sender set. As the calculation of *pmf* depends on the link qualities and schedules of each node in the network, this phase should be refreshed every time the link quality or node schedule changed. In the network assumption, it has been explained that the rate of change is slow which is around every 15 minutes. Therefore, the initial phase can be operated in the same frequency and updated on a low cost.

Flooding phase is the phase where opportunistic flooding algorithm takes effect. As described before, in the flooding phase when a node first receives the flooding packet, it firstly sends the packet along the energy optimal tree if it has a child node in this tree structure. And then it makes the decision whether to forward a packet along the link outside of the energy optimal tree. When there is no event in the network, the flooding phase ended up with a specific delivery ratio as:

$$\text{deliveray ratio} = \frac{\text{number of the nodes that received the flooding packet}}{\text{the total number of nodes in the network}}$$

The probability mass function (*pmf*) of the delay distribution is first derived for each node as shown in Figure 3.3(b). Based on the *pmf*, each node computes its estimated delay D_p. Suppose that $t_l(i)$ is the ith active time unit of a level-l node (with hop count l), the *pmf* of its packet delay is denoted by a set of tuples $\{(t_l(i),p_l(i))\}$, where $p_l(i)$ is the probability of receiving the packet at time $t_l(i)$. Given an energy optimal tree, the *pmf* computation process starts from the level-*0* node (the source) whose *pmf* is $\{(0,1)\}$ and spreads through the network level by level as follows:

$$\begin{aligned} p_{l+1}(j) =& p_{l+1}(j-1)\cdot(1-q) \\ &+ \sum_{i:t_{l+1}(j-1)\leq t_l(i)<t_{l+1}(j)} p_l(i)\cdot q. \end{aligned} \tag{3.1}$$

where q is the corresponding link quality between a level-l node and a level-$(l+1)$ node.

The delay distribution of a level-l node is computed as $\{<t_l(1), p_l(1)>, <t_l(2), p_l(2)>, \cdots, <t_l(n), p_l(n)>\}$. Consequently D_p is the delay $t_l(\text{n})$ when

$$\sum_{i=1}^{n} p_l(i) \geq P_{th}, \tag{3.2}$$

where P_{th} is the threshold which defines the probability that a packet successfully reaches the destination after n transmissions. As soon as a node figures its D_p, it shares this value with all its neighbor nodes with a smaller hop count.

In the initial phase, the calculation of *pmf* depends on the link qualities and schedules of each node in the network. Therefore *pmf* and D_p should be refreshed every time the link quality or node schedule changes. As explained in [49], the local synchronization of the working schedules can be set once every 15 minutes, similarly the initial phase can be executed with the same frequency.

3.1.3 Decision making process

In the flooding phase, upon receiving a flooding packet, a node decides whether to send the packet along a link outside of the energy optimal tree or not. It first calculates the Expected Packet Delay (*EPD*) which indicates when the destination node of this link is likely to receive the packet; then it compares *EPD* with the previously calculated D_p of the destination node. If $EPD < D_p$, this transmission can reduce the flooding delay. Consequently, the flooding packet is forwarded via the link outside of the energy optimal tree. Otherwise, the transmission is considered redundant and will be ignored.

Let suppose that a level-l node, A, receives a packet at its ith active time unit with delay $t_l(i)$ and intends to make a forwarding decision toward one of its level-(l+1) neighbors, B, with active units $t_{l+1}(j)$s. The EPD from A to B can be computed using the following equation:

$$\begin{aligned} EPD = &\max\{t_{l+1}(j) : \\ &\sum_{j:t_{l+1}(j)>t_l(i)} q(1-q)^{n_{ij}} \geq P_{th}\}. \end{aligned} \tag{3.3}$$

where q is the link quality and P_{th} is the probability that the destination node receives the packet before EPD, as defined in the computation of D_p.

Figure 3.4 drafts an example of the decision making process. Considering the link $B - D$ which is outside of the energy optimal tree in Figure 3.3(a), D_p of node D is 25 when P_{th} is 0.9, as shown in Figure 3.3(b). If B receives the flooding packet before time 5, it can start the transmission to D at 5. According to Equation (3.3), EPD of D is 15, which is earlier than D_p, consequently B considers the transmission to D as useful to reduce the flooding delay. On the other hand, if B receives the flooding packet between 5 and 15, it can start the transmission to D at 15 and EPD results to be 25. In this case, EPD is equal to D_p of D and B will not send the transmission along $B - D$.

3.1.4 Decision Conflict Resolutions

The opportunistic flooding algorithm also presents a sender set selection method to alleviate the hidden terminal problem and a link-quality-based back off method to

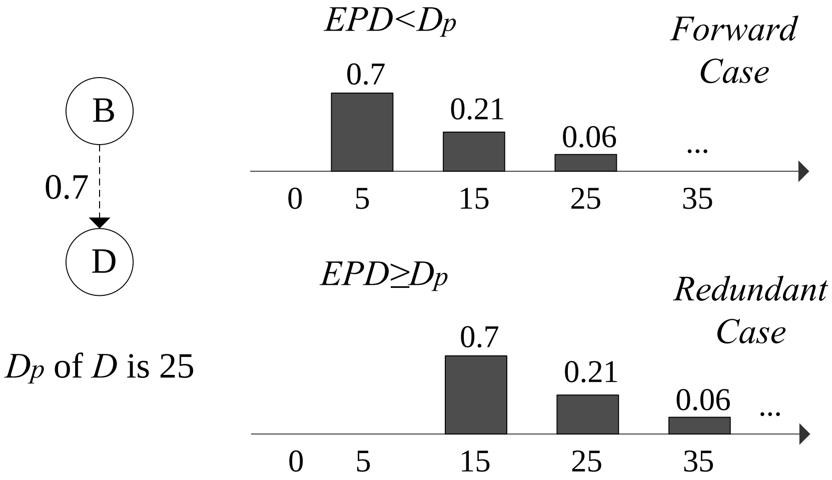


Figure 3.4. An Example of Decision Making

resolve the simultaneous forwarding conflicts caused by the hidden terminal problem. The key idea of the decision conflict resolution is to select a reduced sender set S for each node so that all the sending nodes can hear each other with a better link quality than a threshold L_{th}. The size of the sender set can be adjusted by modifying L_{th}. In the reduced sender set, all links between the selected senders should have a better link quality than L_{th}. The choice of L_{th} is a trade-off between flooding delay and energy cost. When a node in the sender set intends to start a transmission, it first waits for a period of time which is proportional to the link quality of the transmission. In this way, a source with a better link quality can transmit before another with a worse link quality.

3.1.4.1 The selection of flooding senders

The solution of opportunistic flooding to Hidden Terminal Problem is similar to the RTS/CTS control packets in CSMA/CA but limits the control packets into a reduced sender set for each node. The sender set is constructed based on another control parameter L_{th} so that all sending nodes can hear each other (with link quality better than L_{th}) to avoid the hidden terminal problem.

First of all, as a node only receives flooding packets from nodes that have a smaller hop count, the candidates for the sender set are the neighbor nodes with a smaller hop count. When the candidates are confirmed, the selection of the sender set for A goes as follows: first, it starts with the candidate that has the best link quality, which is also the only previous node in the energy optimal tree structure of A. This node is always included in the sender set. Then, check the other candidates in descending order of the link quality, for example, the second candidate to be checked should be the neighbor with the second best link quality and the smaller hop count. If the link quality between this candidate and the already selected senders are all better than L_{th}, this candidate is added to the sender set; otherwise, this link is disabled which means the flooding packet will never be transmitted from this candidate to A. When all the candidates are tested, the final sender set of A is gotten.

Based on the analysis in [2], L_{th} strikes a balance between delay and collision since the value of L_{th} controls the size of the sender set. On the one hand, a large sender set is needed to increase the chance of opportunistic early packets. The more nodes there are in a node's sender set, the shorter the delay in which the node could expect to receive the packet from the set. On the other hand, including more nodes into the sender set increases the chance of collision. Since links among senders are unreliable, the more nodes there are in the same set, the more nodes that will possibly send at the same time and the greater the chance that a transmission is not sensed by all the other nodes, leading to a collision.

3.1.4.2 Link-quality-based back Off

Once a sender set is formed, it needs to resolve the conflicts within the set. Ideally, a node with the best link quality has the highest priority to grab the channel and start a transmission with no collision. Selecting the best link always means the least number of transmissions is expected so that both the expected next-hop delay and energy cost are the smallest.

The solution is that when a node intends to start a transmission, it first backs off for a period of time. The duration of the back off depends on the link quality between the sender and the receiver. The better the link quality is, the shorter the back off duration. When multiple nodes within communication range make their decisions to send towards the same node, they back off first before transmission and the one with the best link quality starts first. Other nodes, after backing off for enough time, listen to the channel first and can catch the ongoing transmission. They will then abort their own transmission and mark transmission to this node as Redundant.

Specifically, an efficient back off calculation algorithm is suggested as follows:

1. Sort all the nodes in the sender set according to the descending order of the link quality, that means the previous node along the energy optimal tree will be the first and with index 0;

2. Assume i to be the index of node S_i in the sorted sender set, then the back off time of S_i should be:

$$t_i = i \times \frac{T_{backoff}}{W} \tag{3.4}$$

If using this algorithm, the back off time bound $T_backoff$ is split equally into W periods and each node in the sender set is assigned a period corresponding to its link quality to the destination node. The minimum time interval between two nodes will be exactly $\frac{T_{backoff}}{W}$. In reality, $\frac{T_{backoff}}{W}$ to be the minimum time needed for the node to listen to the channel and act correspondingly. The only problem is that the sort may be more complex and take more proceeding time. However the size of the sender set will be usually small which makes the proceeding time negligible. Besides the calculation of the back off time can be done in the initial phase which will be refreshed every 15 minutes. Therefore the only problem will be not a problem. By using the link-quality-based back off method, opportunistic flooding reduces not only collisions but also the chance that a packet is forwarded via a very weak link, since the winner must have a relatively good enough link quality to start early.

3.2 Evaluation Scenarios

In order to investigate the performance of the NoACK- and ACK-based opportunistic flooding algorithms, both of them were implemented using the simulator tool OMNeT++ (Object Modular Network Test Bed in C++) [50] which is an extensible, modular, component-based C++ simulation library and framework for building network simulators. Compared with other existing simulators, OMNeT++ is acquiring a good reputation in the simulations of wireless sensor networks thanks to its ability to address effectively the addition of new modules [51]. Specifically, the implementation is based on the framework of Castalia project [52].

3.2.1 NoACK-based opportunistic flooding

In the NoACK-based transmission mechanism, data is sent without requiring any acknowledgement from the receiver. In order to successfully transmit the data, usually the transmission is repeated multiple times. To simulate the NoACK-based transmission scheme, a counter based mechanism is employed to calculate the necessary number of transmissions for each pair of nodes (sender and receiver), and afterwards, each node schedules its transmission according to this number. Since several neighbors may be active at the same time unit and each of them may require a different number of repetition, the total number of transmissions is the maximum number of attempts among all the neighbors. In our implementation, this number is calculated in the initial phase of the opportunistic flooding algorithm according to Equation (2.11).

The maximum number of transmissions N could also be used to calculate EPD more efficiently. Since there is one transmission attempt per duty frame, the EPD of the receiver can be calculated by adding N frames to the first active time unit.

For example, by knowing the number N of attempted transmissions from A to B outside the energy optimal tree, A can calculate the EPD of B along the link A-B as follows:

$$EPD = \begin{cases} (t_B - t_A) + N \cdot T_f, & if\ t_B > t_A \\ (t_B - t_A) + (N+1) \cdot T_f, & if\ t_B \leq t_A \end{cases}. \tag{3.5}$$

where t_A and t_B are the active unit of node A and B, T_f is the frame time length. Compared with Equation (3.3), this formula slashes the complexity of computing EPD and consequently it reduces the processing time for each node in the flooding phase.

3.2.2 ACK-based opportunistic flooding

According to the features of the opportunistic flooding algorithm, when node A wants to send a packet to B, at each frame it schedules a transmission to B according to its working schedule and uses the frame time T_f as a timeout for the acknowledgement response from B. If at the end of T_f it has not received the acknowledgement packet, it schedules another transmission at the next frame. The selective acknowledgement mechanism and the backoff method are implemented in the opportunistic flooding to reduce the redundant acknowledgement transmissions and collisions.

In the ACK-based opportunistic flooding, the active time unit of each node should be larger than a round-trip transmission time, in order to ensure that the sender is active when the receiver replies with the acknowledgment. On the other hand, the different numbers of transmissions in the flooding mostly influence the energy cost. Besides, the ACK-based transmission may require a larger cache space for each node to store the data packet that has not yet received a acknowledgement.

3.2.3 Evaluation Metrics

The performance of the ACK- and NoACK-based opportunistic flooding algorithms have been simulated under several test scenarios with different parameters including network size, network density, duty cycle, P_{th} and L_{th}. For each scenario, the following metrics are evaluated:

- *energy cost*: the energy consumption during the flooding;
- *flooding delay*: the time elapsed from the broadcasting of a message from the source until it reaches a certain percentage of the nodes in the network;
- *delivery ratio*: the number of the nodes that received the flooding packets divided by the total number of nodes.

Since transmitting and receiving the packets consumes much more energy than acquiring the information through sensors and processing it, the energy cost is usually determined by the communication power [53]. According to [2], the energy cost of the opportunistic flooding algorithm can be divided into sender-side cost and receiver-side cost. While the receiver-side energy is mainly determined by their predetermined working schedule, the sender-side energy is the main source of the different energy costs when using the same duty-cycled schedules.

In the NoACK-based transmission mechanism, since the sender does not expect an acknowledgement from the receiver, the sender-side energy cost can be expressed as:

$$E_{NoACK} = N_{data} \cdot \bar{e}_{data}, \tag{3.6}$$

where N_{data} is the number of transmissions and $\bar{e}_{data}$ is the average energy consumed by transmitting a packet.

In the ACK-based mechanism, for each pair of sender and receiver, there is one more acknowledgement transmission. Thus, the energy cost in the ACK-based mechanism is:

$$\begin{aligned} E_{ACK} = N_{data} \cdot \bar{e}_{data} &+ N_{ack} \cdot \bar{e}_{ack} \\ &+ N_{ex} \cdot \bar{e}_{wack} \end{aligned} \tag{3.7}$$

where N_{ack} is the number of acknowledgement transmissions, $\bar{e}_{ack}$ is the average energy consumed by transmitting an acknowledgement packet, N_{ex} is the number of expected acknowledgements. Since the energy consumptions of the idle listening state and the receiving state are very close in a wireless network [54], $\bar{e}_{wack}$ indicates the average energy consumed when the sender is waiting or receiving the acknowledgement.

The power consumption when waiting or receiving the acknowledgement can be further modeled as P_r, and the power to transmit as P_t. In this way, for a single acknowledgment, the ratio between $\bar{e}_{ack}$ and $\bar{e}_{wack}$ is

$$\frac{\bar{e}_{wack}}{\bar{e}_{ack}} = \frac{P_r \cdot T_{ack}}{P_t \cdot T_{ack}} = \frac{P_r}{P_t} = \beta. \tag{3.8}$$

Moreover, when the ratio α between $\bar{e}_{data}$ and $\bar{e}_{ack}$ is introduced, Equation (3.7) can be converted into

$$E_{ACK} = \big(N_{data} + \alpha N_{ack} + \alpha\beta N_{ex}\big) \cdot \bar{e}_{data}. \tag{3.9}$$

Based on Equation (3.6) and Equation (3.9), N_{data} can be collected to measure the energy cost in the NoACK-based opportunistic flooding algorithm and use $N_{data} + \alpha N_{ack} + \alpha\beta N_{ex}$ as the corresponding measurement for the ACK-based opportunistic flooding.

Since the transmission energy consumption is proportional to the transmitted packet size when the transmission distance is fixed [55], the value of α is usually determined by the ratio between the acknowledgement packet size and the data packet size. Existing works have investigated the packet size optimization in different WSN applications [56] [57] and they have provided solutions to determine the appropriate packet size in various error conditions to improve the network efficiency. Since a large size of packet leads to high packet loss and low energy efficiency [58], a smaller data packet size (leading to a larger α) should be used in high BER (Bit Error Rate) condition (e.g., underwater and underground WSNs [56]) while a bigger packet size can be applied when working in lower BER situation. Besides, a smaller packet size is also used in real-time applications. On the other hand, in the multimedia WSN applications carrying a large traffic inherently, lost packets from multimedia blocks are tolerable due to the packet recovery module [59], and consequently large data packet (leading to a smaller α) can be used. On the other hand, β is specified by the data sheet of the sensor device. Therefore, the values of α and β are both application oriented.

3.3 Numerical Results

According to Section 3.2.3, α and β are two important parameters to investigate the energy cost of the ACK-based mechanism. Two values of α (1 and 0.25) are considered. β is set to 0.7 with respect to the power consumption of the MICA 2 platform: 29 mW for reception and 42 mW for transmission at 0 dBm [60]. In the simulations, 10 random network deployments are tested for each pair of parameters to alleviate the random factor. The parameters L_{th} and P_{th} are set to 0.7 and 0.95, respectively. The neighborhood initialization uses an indoor environment in which the path loss exponent n is set to 3.2 and the standard deviation σ is 3.8 [61]. All the nodes pick their active time units randomly according to the duty cycle.

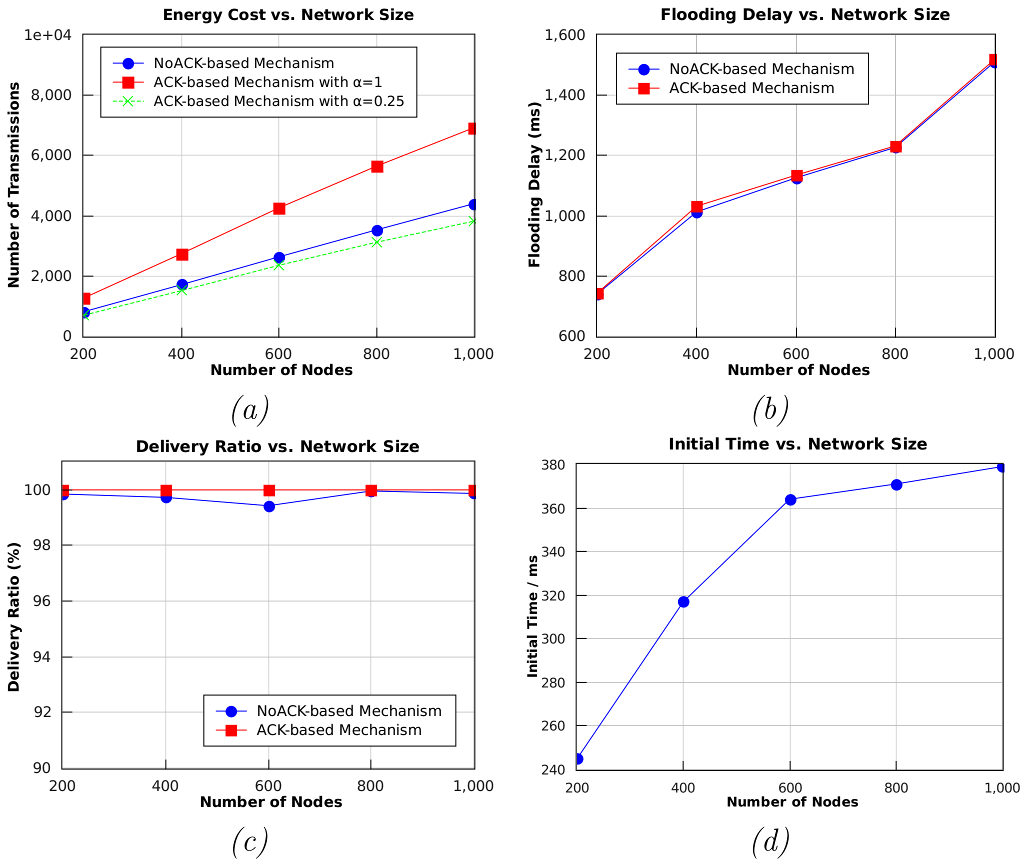
3.3.1 Different Network Sizes

In this evaluation scenario, the number of nodes in the network ranges from 200 to 1000. The side length of the deployment area changes from 150 m to 350 m to keep a similar density.

In Figure 3.5, the average flooding delay and energy cost increase as the network size increases, as expected. The comparison of the flooding delay shows a similar performance of the NoACK- and ACK-based opportunistic flooding algorithm. The reason is that the time required by a single transmission is the same for both the NoACK- and ACK-based transmission mechanisms since the two mechanisms do not influence the receiving time of the receiver. Considering the whole flooding performance, the delay may be slightly different since a node may need to delay the transmission to avoid losing the acknowledgement from other neighbors in the ACK-based transmission mechanism.

When α is 1, the ACK-based implementation needs more energy than the NoACK-based one. On the other hand, if α is 0.25, the required energy is lower than the NoACK-based one. As the network size increases, the differences of the energy cost increases. However, the flooding delay is almost the same except that the ACK-based mechanism may introduce a little delay due to the acknowledgement collision. The delivery ratio of the NoACK-based implementation fluctuates around 99.6% while the one of the ACK-based implementation stays 1.

The network size also influences the initial time in which each node calculates the *pmf* and shares with the neighbors. A larger network size introduces a larger initial time. This is because of the raise of hop counts caused by the change of the network size. When global hop count increases, the *pmf* computation process needs to traverse more nodes in the optimal paths and the initial time will increase.



(a)

(b)

(c)

(d)

Figure 3.5. Flooding Performance in Networks with Different *Network Sizes*

3.3.2 Different Network Densities

To evaluate the effect of the network density, 800 nodes are deployed in an area whose side length ranges from 200 m to 600 m. When the delivery ratio is lower than 99%, the delay is measured by the elapsed time to reach 90% of the node in the network.

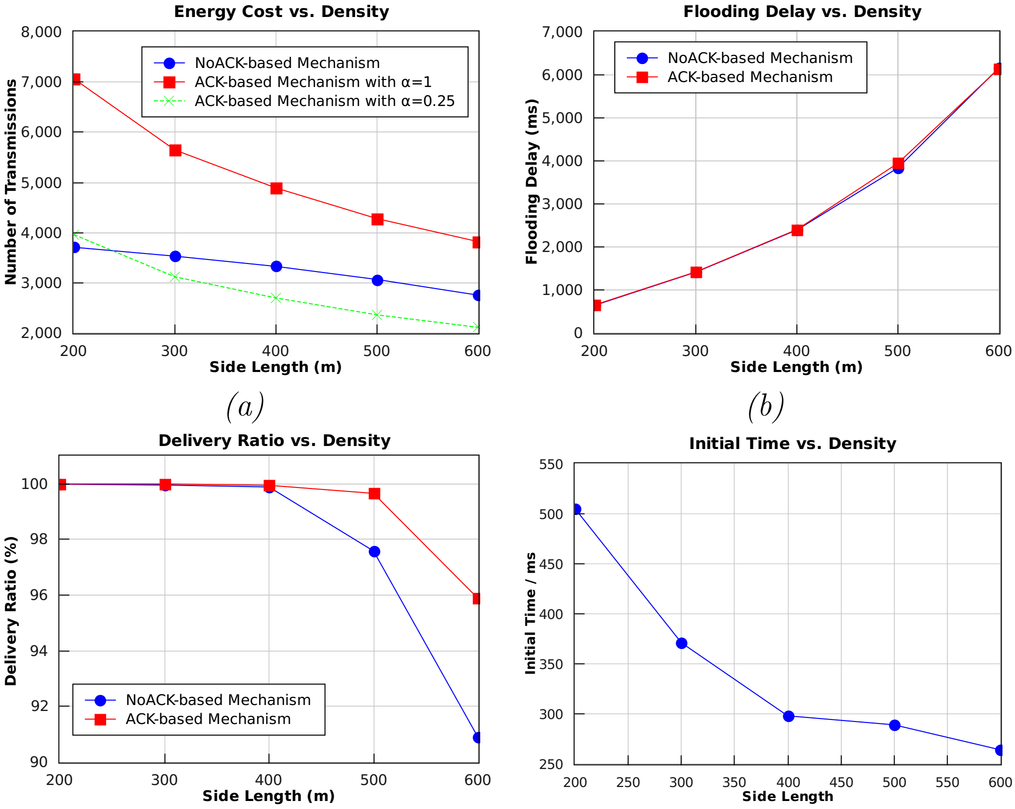
As shown in Figure 3.6, energy costs decrease as the network density decreases. When the side length is lower than 400 m, this is due to the reduction of the opportunistically links and consequently the total number of transmissions decreases. When the network area increases to 500 $m \times 500$ m and 600 $m \times 600$ m, the reason of the energy decrease is mainly due to the decrease of the delivery ratio. As the density decreases, the number of "isolated" nodes (the nodes which have no neighbors) increases and the inherent delivery ratio decreases. When $\alpha = 1$, the energy cost of the ACK-based transmission always goes above of the NoACK-based implementation, while, in the case of $\alpha = 0.25$, the cost falls below the NoACK-based one except for the 200 $m \times 200$ m field. Therefore, the NoACK-based implementation is better than ACK-based implementation in a high density scenario.

For both NoACK- and ACK-based opportunistic flooding algorithms, the flooding delay grows while the density decreases, because the average number of neighboring nodes decreases and one broadcast packet can be heard by few neighbors. Also the link quality becomes worse since the average distance between neighboring nodes is longer. Besides, the results again show the similar performances of the flooding delay in the two implementations. Furthermore, it can also be observed that the delivery ratio in the NoACK-based mechanism decreases faster than in the ACK-based one, because the average link quality decreases as the average distance between two node increases. This also confirms that in a low link quality environment, the ACK-based transmission gives a better performance than the NoACK-based transmissions. Considering the initial time, it is obvious that initial phase will be shorter as the density decreases because when the neighbor nodes become less, the needed transmissions in the initial phase also decrease.

3.3.3 Different P_{th}s

As explained in Section 3.1, P_{th} affects whether a packet is opportunistically early or not. The network is generated by randomly deploying 600 nodes on a 520 $m \times 520$ m field. The duty cycle is chosen to be 5%, the specific L_{th} is set to be 0.7 and P_{th} ranges from 0.7 to 0.95.

Figure 3.7 plots the measured metrics under different P_{th}. The energy costs grow slightly as P_{th} becomes larger because the number of opportunistic transmissions increases. For the flooding delay, the NoACK-based flooding algorithm can reduce the flooding delay compared to the ACK-based one when $P_{th} > 0.8$. This is because



(a) *(b)*

(c) *(d)*

Figure 3.6. Flooding Performance in Networks with Different *Network Densities*

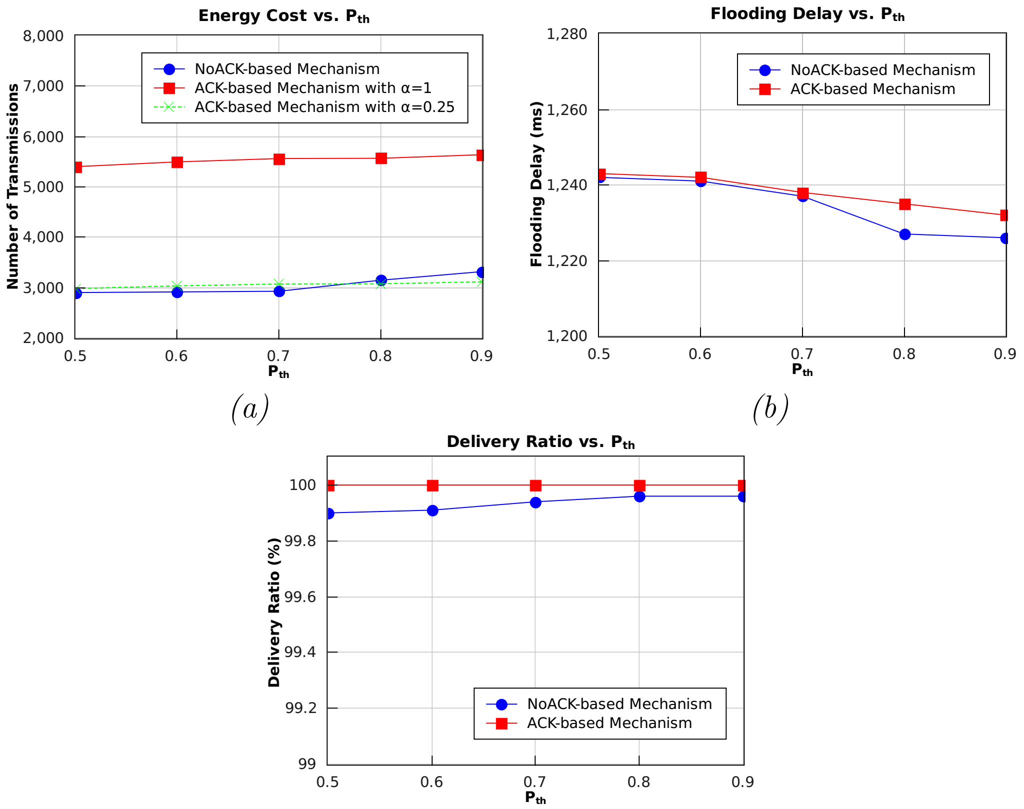
when P_{th} increases, the links outside the energy optimal tree increase and more collisions may be introduced by the acknowledgement transmissions.

It is also interesting to observe that the number of transmissions, the flooding delay and the delivery ratio stay almost invariant with respect to P_{th}. The reason is because the calculation of both the static delay distribution (pmf) and the expected packet delay (EPD) depends on P_{th}. When a node makes decision based on these two values, the comparison result does not change (or changes slightly) no matter how P_{th} changes, which resulting a unvarying flooding path. Therefore, P_{th} has little impact on the performance of opportunistic flooding algorithm.

As the topology is not changed in this scenarios, the initial time does not modify with respect to different P_{th}s.

3.3.4 Different L_{th}s

The simulation parameters are the same as in the P_{th} evaluation except that P_{th} is set to 0.95 and L_{th} varies from 0.7 to 1.



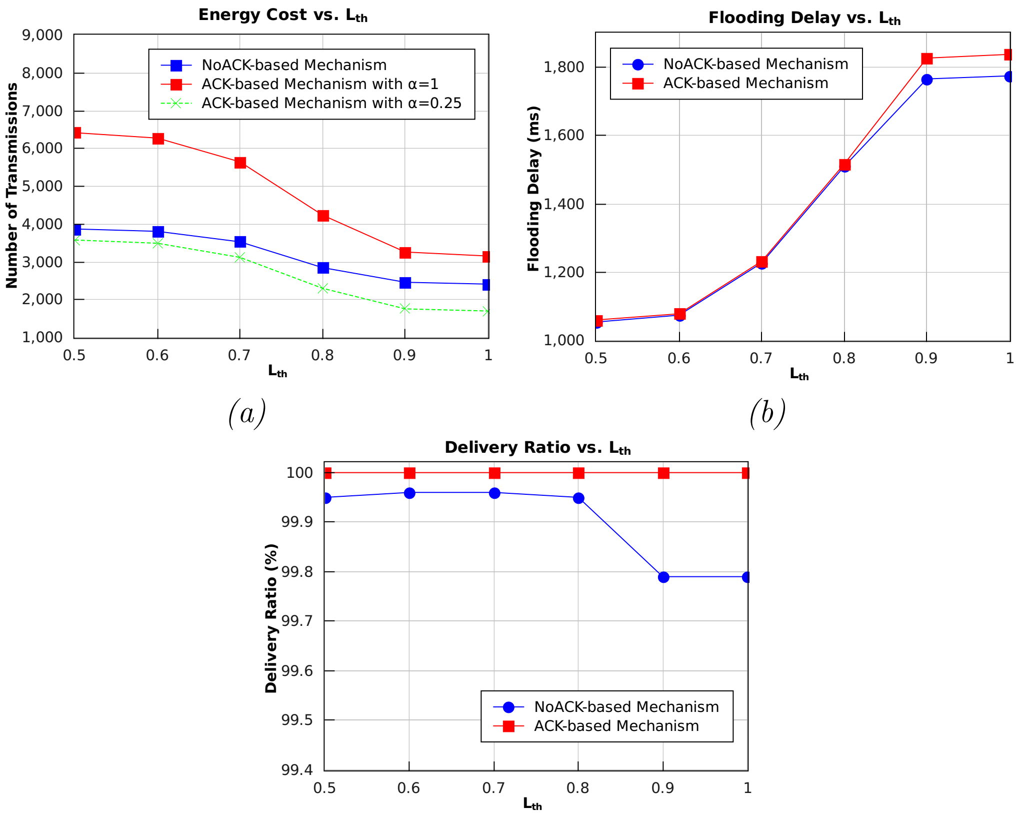
(a) *(b)*

(c)

Figure 3.7. Flooding Performance in Networks with Different P_{th}s

Figure 3.8 shows that as L_{th} increases, fewer nodes are included in the sender set, leading to fewer opportunistic forwarding and consequently reducing the energy cost. When L_{th} is lower than 0.8, the ACK-based transmission with $\alpha = 1$ consumes more energy than the NoACK-based transmission. When L_{th} grows more than 0.9, which means that there are few transmissions outside of the energy optimal tree, the ACK-based mechanism with $\alpha = 1$ saves more energy than the NoACK-based one. The opportunistic links outside the energy optimal tree make the acknowledgement based mechanism less efficient.

When the number of opportunistic transmissions decreases, the delivery ratio of the NoACK-based mechanism also decreases, since the opportunistic transmissions help to improve the inherent delivery ratio of the flooding. It is worth noting that when there is no opportunistic transmissions ($L_{th} = 1$), i.e., the flooding just goes along the energy optimal tree, a node can still receive a packet from a sender which is not its parent along the energy optimal tree due to the overhearing feature of WSNs. If it has not received any packet from its parent along the energy optimal tree before, this overheard transmission can make the node receive the packet earlier.



(a)

(b)

(c)

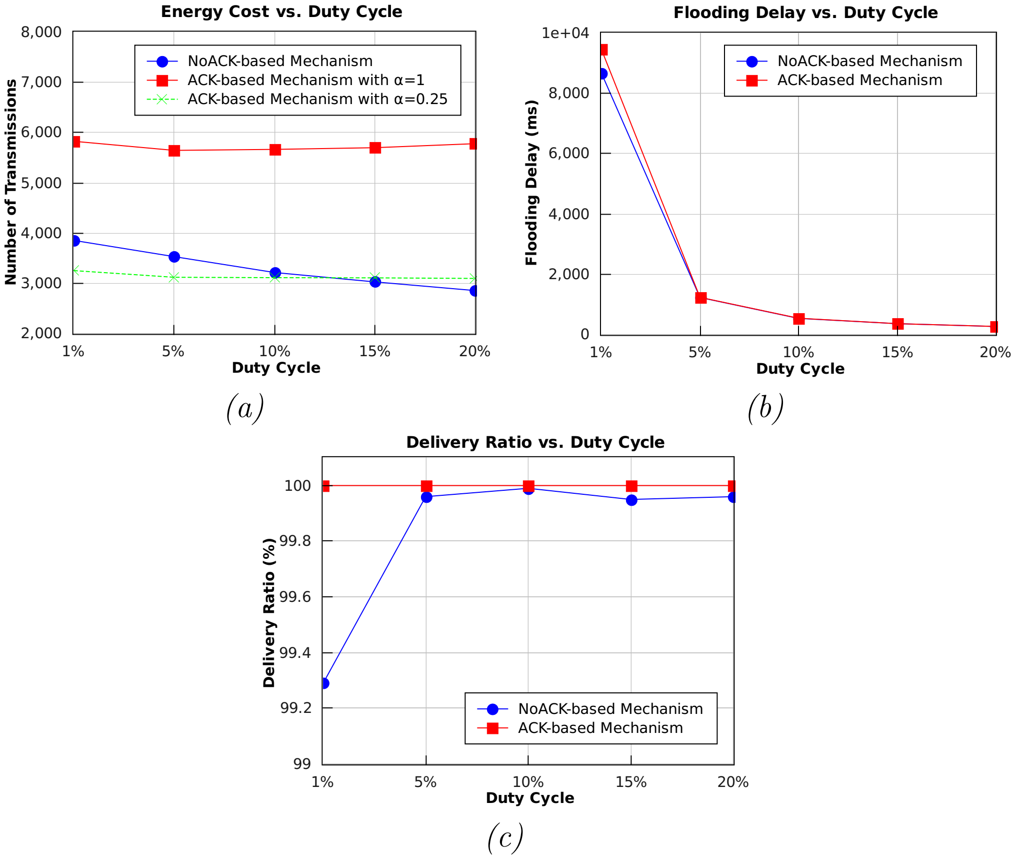
Figure 3.8. Flooding Performance in Networks with Different L_{th}s

3.3.5 Different Duty Cycles

The performances in networks with different duty cycles are evaluated by randomly deploying 600 nodes on a 520 $m \times 520$ m field.

It can be seen from Figure 3.9 that the energy cost of the ACK-based implementation does not change considerably. On the other hand, the energy cost of the NoACK-based mechanism decreases consistently when the duty cycle increases, because a packet can be received by more neighbors simultaneously. Although more neighboring nodes in the ACK-based implementation can receive the transmitting packet, more acknowledgement packets have to be sent back.

When the duty cycle increases, the active time of each node becomes longer and thus the flooding delay is shorter. For the NoACK-based mechanism, there is also an improvement on the delivery ratio when duty cycle increases, because a single transmission can be overheard by more nodes.



(a)

(b)

(c)

Figure 3.9. Flooding Performance in Networks with Different *Duty Cycles*

Chapter 4

Analysis and Comparison of Interference Models in RFID Systems

In this chapter, a survey of the interference models in RFID systems are investigated. Especially, the reader-to-reader interference is analyzed based on the survey. In order to provide support for the reader-to-reader collisions handling, a particular propagation model is proposed considering direct collisions and additive collisions. Furthermore, several evaluation scenarios are proposed to compare the performance of the single interference model and the additive interference model.

4.1 State-of-the-art Interference Models for Reader-to-Reader Collision

There are three types of interferences in RFID systems: tag-to-tag interference, reader-to-tag interference and reader-to-reader interference. Tag-to-tag interference can be avoided by tree-based algorithm [36, 37], ALOHA [32, 33, 34] and beam forming algorithm [62]. Reader-to-tag can be solved by separating reader interrogating ranges [63]. However, the reader-to-reader interference still requires more studies. So far, although a number of researches related to analyzing reader-to-reader interference have been conducted, there is not an agreed interference model that analyze the reader-to-reader interference in a mathematical way.

The current interference models for the reader-to-reader collision problem can be classified according to which kind of reader-to-reader collision they consider: the single interference model, which considers only direct interference between readers, and the additive interference model, which sums all the interference components generated by more than one source.

In a single interference model, only the one-to-one interference between two neighboring RFID readers is considered, without taking into account the interference received by other readers. This kind of model assumes that each reader can collide only with readers located within a fixed collision range. The possible interference between the couples of readers can be described by a graph. In some typologies of graph there is not a direct connection with the geographical deployment of the readers (e.g., planar graphs and trees [64]). However, more realistic graphs are based on metric spaces, such as the sphere of influence graph [65, 66] and the unit disk graph [67]. Given N points in a Euclidean plane, a unit disk graph is defined as a graph where each vertex corresponds to a point, and an edge connects two vertices if the distance between the corresponding points is below a threshold.

The group of additive interference models consider the power of all (or the majority of) the exchanged signals. It is based on the fact that the total interference power from multiple interfering readers to the target reader is additive, i.e., all the interference contributions are added non-coherently. Besides, it is assumed that the interfering readers are distributed over a 2-dimensional area, i.e., three-dimensional space deployment is not considered.

4.1.1 Single interference models

All the direct collisions that occur in the RFID network are predetermined by the single interference model and they can be represented by an *interference graph*. Each node of the interference graph coincides with a reader and an edge links two nodes if the corresponding readers collide when they query tags at the same time. Different kinds of interference graph can be generated, depending on the assumptions of each interference model. The main ones are described in the following.

4.1.1.1 Unit disk graph

A simple yet common criterion for predicting a collision between two RFID readers is their distance. If the distance is lower than a threshold D_{th}, the two readers collide with each other in case of a simultaneous transmission. Since the only condition for generating a collision is the relative distance between the two readers, in the interference graph an edge exists between two nodes r_1 and r_2 if r_1 is located within a circle centered in r_2 and with radius D_{th}. The so-formed graph is called *unit disk graph* [68].

Some variants of the basic model exist. If the deployment area is the unit square $[0,1]^2$ and the position of the readers is randomly chosen, the resulting graph is called *random geometric graph* [69]. This interference graph becomes a *random sector graphs* [70] if the antenna of the readers is directional.

Different evaluations of the threshold D_{th} are proposed. In [6] a homogeneous RFID network is analyzed, where all the readers have the same interrogation range d, they query tags with radio signals of power P_r and they are equipped with identical antennas of gain G_r. Similarly, all the tags are supposed identical, with antennas of gain G_t and power reflection coefficient R_t. Under these conditions, the value provided for the threshold is:

$$D_{th} = \sqrt[\alpha]{\frac{K_0 \Gamma P_r d^{2\alpha} G_r^2}{R_t P_r G_t^2 G_r^2 - N_0 K_0^2 \Gamma d^{2\alpha}}} \tag{4.1}$$

where α is the path loss exponent, N_0 is the background noise power and Γ is the SINR (Signal to Interference plus Noise Ratio) required by the reader to correctly detect the tag's reply. The coefficient K_0 can be either defined according to the adopted propagation model (for example, $K_0 = \left(\frac{4\pi}{\lambda}\right)^2$ in the free space model) or derived by measuring the power received in a sample transmission [71].

The analysis in [72] determines the presence of a reader-to-reader collision by correlating the distances between the two readers and the group of tags to query. Reader r_1 can identify tags near it without any interference from reader r_2 if the following condition is satisfied:

$$|r_1 - r_2| \geq (1 + \Delta)|r_1 - t| \tag{4.2}$$

where Δ is a positive constant, $|r_1 - r_2|$ is the distance between the two readers and $|r_1 - t|$ is the distance between r_1 and the farthest tag that is queried. Since the maximum distance at which a tag can be identified corresponds to the interrogation range d, the maximum distance expected in equation (4.2) such that two readers experience a reader-to-reader collision is:

$$D_{th} = (1 + \Delta)d \tag{4.3}$$

Some studies simplify equation (4.3) by assigning a constant value to D_{th} [38], without any explicit correlation to the interrogation range.

4.1.1.2 Quasi unit disk graph

In a real scenario, even with an omnidirectional antenna the signal emitted by a reader does not propagate equally in all the directions and thus its interference area differs from a disk. The causes can be the irregular shape of the field, some obstacles that obstruct the signal propagation, the atmospheric conditions, etc. This situation is modeled by the *quasi unit disk graphs* [73]. This kind of graph differs from the unit disk graph since it introduces a parameter ρ, with $0 < \rho < 1$. An edge exists between two nodes in the graph if their distance is lower than ρD_{th}. The two nodes may or may not be linked if their distance ranges between ρD_{th} and D_{th}. Finally, like in the unit disk graph, the two nodes do not interfere if they are placed at a distance higher than D_{th}.

A natural extension of the quasi unit disk graph is the *quasi random geometric graph* [74], where the nodes are independent and uniformly distributed on the unit square $[0,1]^2$. The presence of obstacles that reduce the interference between a pair of readers can be captured by other graphs, such as the *faulty random geometric graph* [75], which is obtained from a random geometric graph through random removal of edges and vertices.

4.1.1.3 Bernoulli random graph

The *Bernoulli random graph* is the simplest interference model. Some variants exist depending on the stochastic process that is followed to generate the graph. According to the definition in [76], for each pair of nodes an edge may be added with a probability p_{Brg} independent from every other edge. Another common definition is given in [77]. First, the total number of edges N_{Brg} among the set of vertices is fixed. Then, the Bernoulli random graph is randomly and uniformly chosen from the set of graphs that share the same set of vertices and have N_{Brg} edges.

The Bernoulli random graph models the randomness of the signal propagation in RFID networks due to external causes. Its main advantage is the simplicity of the model, which enables to exactly solve many average properties of the network. However it does not properly capture the behavior of real-world networks, because the probability that two nodes are linked is independent of their distance.

4.1.1.4 Protocol model

According to the protocol model [72], reader x can identify tag t without colliding with reader y if the following condition holds:

$$|x-y| \geq (1+\Delta)|x-t| \tag{4.4}$$

where Δ is a positive constant. The protocol model is a generalization of the unit disk graph model [78]. By assuming $D=(1+\Delta)d$, the condition for a successful tag identification in the unit disk graph model is stricter than in the protocol model:

$$|x-y| \geq D = (1+\Delta)d \geq (1+\Delta)|x-t| \tag{4.5}$$

since condition 4.3 applies also to the protocol model: as well as in the unit disk graph model, a reader can only identify tags located within its interrogation range d.

4.1.1.5 Capture threshold model

In this model, the power of the signal that the reader receives from a tag is compared with the power of the interference generated by another reader that is transmitting at the same time. The comparison is repeated for all the interfering readers in the surroundings. If the ratio between the signal received by a tag and the interfering signal is higher than a threshold, then the reader identifies the tag, otherwise a reader-to-reader collision occurs. More formally, the condition for the tag identification is the following:

$$\frac{P_{t,x}\, G_{t,x}}{P_{y,x}\, G_{y,x}} \geq \beta_{ct} \tag{4.6}$$

where $G_{t,x}$ is the propagation gain (including the antenna gains) from tag t to reader x and $G_{y,x}$ is the propagation gain from reader y to reader x. The capture threshold model is implemented by the NS-2 simulator[1], that uses a value of 10 dB for β_{ct}.

The capture threshold model is a generalization of the protocol model. The two models are equivalent if the following conditions holds:

- isotropic path loss is considered, thus the propagation gain between points a and b is $G_{a,b} = \left(\frac{|a-b|}{d_0}\right)^{-\eta}$, where d_0 is a constant and η is the path loss exponent;

- the readers are homogeneous: they transmit with the same power P_x and the ratio $\frac{P_{y,x}}{P_{t,x}}$ can be considered constant;

- the value of Δ is set to $\sqrt[\eta]{\beta_{ct}\frac{P_{y,x}}{P_{t,x}}} - 1$.

Under these hypotheses, equation 4.6 can be written as:

$$\begin{aligned}
&\frac{\left(\frac{|x-t|}{d_0}\right)^{-\eta}}{\left(\frac{|x-y|}{d_0}\right)^{-\eta}} \geq \beta_{ct}\frac{P_{y,x}}{P_{t,x}} \\
&\frac{|x-y|}{|x-t|} \geq \sqrt[\eta]{\beta_{ct}\frac{P_{y,x}}{P_{t,x}}} \\
&|x-y| \geq \left(\sqrt[\eta]{\beta_{ct}\frac{P_{y,x}}{P_{t,x}}} - 1 + 1\right)|x-t| = (1+\Delta)|x-t|
\end{aligned} \tag{4.7}$$

and the equivalence with equation 4.4 is proved.

[1] http://nsnam.isi.edu/nsnam/index.php/Main_Page

In order to correctly detect and decode the tag's reply, in the capture threshold model it is required that the power of the received signal is higher than a threshold Θ, called *carrier receive level*:

$$P_{t,x} \geq \Theta \tag{4.8}$$

In contrast with equation 4.6, condition 4.8 states that in the capture threshold model the interference range can not be assumed as directly proportional to the interrogation range.

4.1.2 Additive interference models

The criterion followed by additive interference models for determining the occurrence of a reader-to-reader collision is the evaluation of the SINR at the reader's antenna. If the measured SINR is higher than a threshold Γ, then the reader successfully detects the tag around it. More formally, the condition for the tag identification is:

$$\frac{P_{t,r}}{I + N_0} \geq \Gamma \tag{4.9}$$

where $P_{t,r}$ is the power of the reply that reader r receives from tag t and I is the interference generated by other readers in the RFID network. On the contrary, if equation (4.9) is not satisfied, the reader experiences a reader-to-reader collision.

The interference I received by a reader is given by the sum of the contributions generated by the other readers. This situation can be represented in a weighted graph, where the weight of an edge between two readers expresses the interference that the transmission of a reader provokes on the other one. A reader incurs a reader-to-reader collision if the sum of the weights of all its incoming edges in the graph is so high that equation (4.9) is not satisfied. There are two different categories of additive interference models, leading to two distinct interference graphs, depending on the quantity of readers in the network that are considered to calculate the interference perceived by the target reader.

4.1.2.1 Random proximity graph

The interference that a reader causes on another one is inversely proportional to their distance. Since the greatest amount of interference is generated by close readers, a good approximation of the total interference can be achieved by summing the contributions of the k closest readers. This is confirmed by the analysis in [8]. The interference graph that derives from this assumption is called *random proximity graph*. In this graph, the nodes are randomly deployed with an uniform distribution in the unit square $[0,1]^2$. For each node, the k closest nodes are identified according to the Euclidean distance. An ordered edge is added between a node and each of its neighbors.

The random proximity graph is often denoted as *K-nearest neighbor graph* in metric spaces, where a number of dimensions higher than 2 and a distance measure different from the Euclidean distance may be applied.

4.1.2.2 Physical model

The physical model [72] considers the distance L between the source and the destination of the signal and it applies the proportional decay $L^{-\alpha}$ of the signal with the distance in order to evaluate equation 4.10:

$$\frac{\frac{P_t}{|x-t|^\alpha}}{\mathcal{N} + \sum_{i=0}^{N} \frac{P_i}{|x-i|^\alpha}} \geq \Gamma \tag{4.10}$$

where N is the number of readers in the network (in addition to reader x).

The physical model is a simplification of the single-channel model. The two models are equivalent if all the interfering readers are homogeneous with antenna gain $G_y = \frac{G_x}{P_0}$ and if the gain of the tag's antenna is $G_t = \frac{G_x}{P_0\, E_{tag}}$.

4.1.2.3 IRRR model

Reader-to-reader interference reduces the value of SIR measured at reader x: since the power of the signal backscatterd by tags keeps constant, this reduces the interrogation range of reader x. The interrogation range reduction ratio (IRRR) is a parameter proposed in [79, 80] to evaluate the effect of reader-to-reader interference. The power of the signal that reader x receives from tag t is given as:

$$P_{t,x} = \alpha_{BW}\, E_{tag}\, P_x\, G_x\, G_t \cdot 10^{0.2 \cdot PL(|x-t|)} = \alpha_{BW}\, E_{tag}\, P_x\, G_x\, G_t \left(\frac{P_0}{|x-t|^\alpha}\right)^2 \tag{4.11}$$

where α_{BW} denotes the ratio of the spectrum power in the used channel to the available bandwidth. PL is the path loss between x and t: since it depends on their distance, the path loss P_0 at the reference distance $d_0 = 1$ m is adopted in the second formulation of equation 4.11. The total path loss between x and t is obtained by summing two contributions: the first one for the forwarding reader-to-tag query communication and the second one for the returning tag-to-reader response. Fading effects are ignored, because a line-of-sight propagation is assumed for the reader's query and the tag's response.

The interference that x receives from reader y is estimated as:

$$P_{y,x} = h_y\, P_y\, \beta_{mask\_y}\, G_x\, G_y \cdot 10^{0.1 \cdot PL(|x-y|)} = h_y\, P_y\, \beta_{mask\_y}\, G_x\, G_y\, \frac{P_0}{|x-y|^\alpha} \tag{4.12}$$

where h_y is a fading coefficient in the channel between x and y; β_{mask_y} is the limit level of the spectrum mask.

The total interference I_x sensed by x is obtained by summing each individual contribution given by equation 4.12 for all the other readers in the network. The estimation of equation 4.10 easily follows. An example of evaluating equation 4.10 is provided in [81] by considering free space propagation, with $P_0 = \left(\frac{\lambda}{4\pi}\right)^2$, and a time division multiple access (TDMA) scheme to manage the activity of the readers. In the TDMA channel access method, the readers share the same frequency channel by allocating their transmission into different time slots. A boolean flag is introduced for each reader to indicate if it can interfere with reader x:

$$\gamma_i = \begin{cases} 1 & \text{if reader } i \text{ operates at the same time slot of reader } x \\ 0 & \text{otherwise} \end{cases} \tag{4.13}$$

Under these assumptions, equation 4.10 becomes:

$$\frac{\frac{\kappa_1 \; P_{t,r}}{|x-t|^4}}{\sum_{i=1}^{N} \frac{\gamma_i \kappa_2 P_i \beta_{mask\_i}}{|x-i|^2} + \mathcal{N}} \geq \Gamma \tag{4.14}$$

where $\kappa_1 = \frac{\alpha_{BW} \; E_{tag} \; G_x \; G_t \lambda_x^4}{(4\pi)^4}$ and $\kappa_2 = \frac{h_i \; G_x \; G_i \lambda_i^2}{(4\pi)^2}$.

An alternative way to calculate I_x is provided in [80] by assuming a uniform random distribution of the readers. Firstly, the average interference generated by a single reader y is calculated by integrating equation 4.12 in the annulus where the reader y can be located. I_x is then estimated by multiplying the average interference for the average number of simultaneously active readers (given by the number of the readers in the network and their probability of querying tags).

The IRRR model extends the single-channel model by considering the availability of more than one channel for the communication among readers and tags. Furthermore, it considers fading effects in the interference among readers. The main difference between the two models lies in the estimation of $P_{t,x}$: in the single-channel model, the contribution of the antenna gains of the reader and the tag is counted twice, while in the IRRR model it is considered only once.

4.1.2.4 Rayleigh and shadow fading model

The interference model proposed in [82] assume that the signals emitted by the readers randomly attenuate during their propagation according to a Rayleigh distribution. In addition, obstacles among the readers may further reduce the signal intensity. As in the other additive interference models, Rayleight fading and shadowing are not considered for the communication between the reader and the tag, since it is in direct line of sight and within a short range. The power of the tag's reply detected by the reader is evaluated as follows:

$$P_{t,x} = K_1 \frac{P_x}{|x-t|^{4q}} \tag{4.15}$$

where K_1 is a constant that include the antenna gains of the reader and the tag, the wavelength and the modulation indexing; q models the path loss and its value depends on the environment where the signal propagates.

The interference that reader x noticed from another reader y is:

$$P_{y,x} = K_2 \frac{P_y}{|x-y|^{2q}} \cdot 10^{0.1\zeta} \cdot X_{xy}^2 \tag{4.16}$$

where $10^{0.1\zeta}$ takes into account the effect of shadowing and X_{xy} is a random variable with Rayleigh distribution that describes the deviation in the attenuation of the signal from reader y to reader x. K_2 is a constant that, similarly to K_1, considers the antenna gains of the two readers, the wavelength and the modulation indexing.

4.2 A New Propagation Model for Reader-to-Reader Interference

4.2.1 Basic model

In a passive UHF RFID system, as tags do not incorporate a battery and are powered by the carrier signal from readers, the backscattered signal arrives at the reader very weakly. In order to be recognized, the backscattered signal from the tag needs to satisfy two conditions. Firstly, the strength of the signal must be above a lower bound, named *carrier receive level* (or receiver sensitivity), which guarantees that it can be correctly detected and decoded. Let Θ denote the carrier receive level, this condition can be expressed as

$$P_{t,r} \geq \Theta, \tag{4.17}$$

where $P_{t,r}$ represents the signal power received by reader r from tag t.

The second condition for the signal detection requires that the ratio between the backscattered signal and the interference (possibly including also the background noise) exceeds a given threshold, which depends on the desired read rate and the bit error rate (BER). According to the estimation of the background noise power, the interference models can be categorized as *signal to interference ratio (SIR)* model and *signal to interference plus noise ratio (SINR)* model. In the SIR model [71], the background noise power is assumed as negligible with respect to the reader interference. In the SINR model [83, 63, 81], the noise power is included as a model parameter. Let Γ be the required threshold of the ratio, the following condition should be satisfied in the SIR model:

$$\frac{P_{t,r}}{I_r} \geq \Gamma \tag{4.18}$$

where I_r denotes the total interference that reader r receives from other readers.

When the noise power is taken into account, the condition in the SINR model becomes:

$$\frac{P_{t,r}}{I_r + N_0} \geq \Gamma \tag{4.19}$$

where N_0 is the power of the background noise. According to the conditions (4.17) and (4.19), to make sure that the reader can identify the tag when there is no interference from the other readers, the noise power has to satisfy

$$N_0 \leq \frac{P_{t,r}}{\Gamma}. \tag{4.20}$$

Let d be the maximum interrogation range of reader r without any interference. In [71], the received signal power at tag t from reader r is expressed as

$$P_{r,t} = P_r \frac{G_r G_t}{K_0 d^\alpha} \tag{4.21}$$

where P_r is the transmit power of the reader, G_r and G_t represent the antenna gain of the reader and the tag, respectively, and α is the path loss exponent. K_0 is a coefficient integrating the channel path loss and the fractional power ratio in the bandwidth. As the distance between the reader and the tag is short and the transmission path is a simple line-of-sight, fading effects can be ignored. K_0 can be derived by measuring the power P_t received by a tag at a reference distance d_0 (usually 1 m). Therefore K_0 can be set such that $P_r \frac{G_r G_t}{K_0} = P_t {d_0}^\alpha$. When $d_0 = 1$, $K_0 = \frac{P_r}{P_t} G_t G_r$.

Let R_t be the effective power reflection coefficient of the tag antenna, i.e., the ratio of the power received by the tag that is reflected to the reader. Then, the power received by the reader from the tag is given by

$$P_{t,r} = R_t P_{r,t} \frac{G_t G_r}{K_0 d^\alpha}. \tag{4.22}$$

In the SINR model, after substituting $P_{t,r}$ into condition (4.20) according to Equation (4.22) and (4.21), the maximal possible noise power is:

$$N_{max} = \frac{R_t P_r}{\Gamma} \left(\frac{G_r G_t}{K_0 d^\alpha} \right)^2. \tag{4.23}$$

Besides, in order to satisfy the condition in (4.17), the interrogation range d can be determined by the threshold Θ and the transmit power P_r of the reader. Θ and P_r are tuned according to the integrated circuit design and the environmental condition of the antenna. When the transmit power P_r and the threshold Θ are specified, d can be calculated by imposing Equation (4.22) equal to Θ. Therefore, when no background noise is considered, P_r must be larger than the threshold power required for the tag operation in order to satisfy the condition in (4.17).

Let D be the distance between two readers A and B. The interference power of reader B detected by reader A can be expressed as:

$$P_{r,r} = P_r \frac{G_r G_r}{K_0 D^\alpha}. \tag{4.24}$$

4.2.2 Single interference model

In a single interference model, each reader is characterized by its interrogation range, which depends on the output power used to query the tags. Within the interrogation range, the output power of the reader is enough to feed the circuitry of the tags and to receive a back scattered signal with adequate power. A reader can collect information from all the tags within its interrogation range, but it cannot query tags that are located outside. When a reader is receiving the backscattered signal from the passive tag, the signal may be damped by the signals of other readers that are simultaneously querying tags in the same channel, consequently the query operation fails. The threshold distance within which the signal of a reader is strong enough to disturb the activity of another reader is called *collision range*. As shown in Figure 4.1, the readers within the collision range of the target reader are prevented from collecting any tag information when the target reader is interrogating tags. All the readers that are located outside the collision range are not disturbed. The collision caused by a reader within the collision range is called *direct collision*.

Under the hypothesis of the single interference model, the reader collision can be described in a boolean way: two readers may collide if and only if they are located within a certain distance. The collision happens if they transmit simultaneously on the same channel. The relationship of potential collision among a set of readers can be described by a graph. Each reader is represented by a point. An edge exists between two nodes if and only if the Euclidean distance between the two nodes is below a fixed threshold. The graph obtained in this way is called *unit disk graph* [67]. If two nodes are connected by an edge in a unit disk graph, the corresponding readers may experience a collision.

According to the SIR model, the reader-to-reader collision occurs when the condition in (4.18) is not satisfied, i.e., the backscattered signal from the tag to the reader is too weak with respect to the interfering signals of other readers. To prevent the reader-to-reader collision problem, the key point is to determine the potential

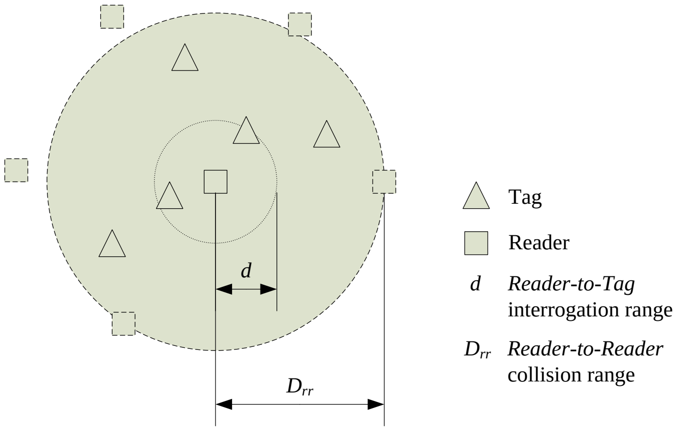

d
D_{rr}
Tag
Reader
d Reader-to-Tag interrogation range
D_{rr} Reader-to-Reader collision range

Figure 4.1. Single interference model

collision range within which the reply signal from the tag is not interfered by signals from other readers. Once the potential collision range is determined, FDMA or TDMA schemes prevent readers from concurrent tag interrogations. In the SIR single interference model with only one interfering reader B, the total interference I_r received by reader A is given by Equation (4.24). The reader-to-reader direct collision range, i.e., the minimum distance D_{rr} beyond which two concurrent readers do not generate a collision, is obtained by setting the SIR equal to the required threshold Γ, i.e.,

$$\frac{P_{t,r}}{P_{r,r}} = \Gamma. \tag{4.25}$$

In this formula, substituting $P_{t,r}$ and $P_{r,r}$ given by Equation (4.22) and (4.24), the direct collision range follows:

$$D_{rr} = d^2 \cdot \sqrt[\alpha]{\frac{K_0 \Gamma}{R_t {G_t}^2}}. \tag{4.26}$$

When the SINR model is considered, the bound of the condition in (4.19) is

$$\frac{P_{t,r}}{P_{r,r} + N_0} = \Gamma. \tag{4.27}$$

Consequently, the direct collision range can be calculated as

$$D_{rr} \geq \sqrt[\alpha]{\frac{K_0 \Gamma P_r d^{2\alpha} G_r^2}{R_t P_r G_t^2 G_r^2 - N_0 K_0^2 \Gamma d^{2\alpha}}}. \tag{4.28}$$

by substituting Equation (4.24) into I_r.

Consequently, the direct collision range in Equation (4.26) and (4.28) can be used to generate the unit disk graph: when the distance between two nodes is lower than the direct collision range, there is an edge in the corresponding graph; otherwise, the two nodes are not connected.

4.2.3 Additive interference model

Additive interference models are based on the basic assumption that the interference power from multiple interfering readers to the target reader is additive. They generalize the single interference models by considering multiple readers' collisions instead of just considering direct collisions. Assuming that all the RFID readers and tags have identical antenna gain G_r and G_t, respectively, in the presence of a group of n readers, the total interference that is generated towards one target reader A can be evaluated summing each individual contribution:

$$I_s = \sum_{i=1}^{n} P_r \frac{G_r G_r}{K_0 D_i^{\alpha}} \tag{4.29}$$

where D_i is the distance between reader A and reader i. According to the condition in (4.18) in a SIR model, the sum of all the interfering signals provokes a collision if I_s satisfies

$$I_s {\geq} \frac{P_{t,r}}{\Gamma}. \tag{4.30}$$

On the other hand, according to the SINR models, a collision happens if the following condition for I_s holds

$$I_s {\geq} \frac{P_{t,r}}{\Gamma} - N_0. \tag{4.31}$$

The ratios $\frac{P_{t,r}}{\Gamma}$ and $\frac{P_{t,r}}{\Gamma} - N_0$ are called the *interference threshold* in the SIR additive interference model and the SINR additive interference model, respectively.

4.2.4 Comparison

The single interference model only considers direct collisions and the occurrence of the collision depends on the distance between a pair of readers. Therefore, it is easy to detect reader-to-reader collisions in a single interference model. In a sparse deployment where each reader have only a small number of neighboring readers, the probability that more than 2 neighboring readers interrogate simultaneously is low and consequently the single interference is convenient and practical. However, in a dense deployment where, a reader receives interference from several neighboring readers, therefore make the single interference model unrealistic.

The additive interference model considers the composition of the interference from several simultaneous interrogation activities. It recognizes a higher number of collisions with respect to single interference model, but require more computational effort. Whereas interference in single interference models depend on a threshold distance, additive interference model always calculates the received interference power for every interrogating reader: this is not necessary in a sparse deployment or a scenario where the interrogation frequency is low.

In the next section, the single interference model and the additive interference model are compared in a quantitative way based on several evaluation scenarios.

4.3 Evaluation Scenarios to compare the additive interference model and the single interference model

In order to compare single and additive interference models, their performance is analyzed in two scenarios. The first one studies the interaction between a pair of interfering readers and a target reader. The second scenario inspects the relationship between the number of readers and the radius of the circular area within which the interference is detected. Furthermore, a particular hexagonal constellation deployment is considered.

4.3.1 Pair interaction

In this scenario, the interference produced by a pair of readers on a target reader is investigated. Depending on the considered interference model, the interference generated from the pair of readers has a different impact on the target reader. When the unit disk graph model is adopted, the two interfering readers generate collisions independently of each other. There are no collision only if both the interfering readers are out of the reader-to-reader direct collision range. On the contrary, in an additive interference model, a collision may occur even if both the readers are beyond the direct collision range. The pair of readers can interact and generates a stronger interference that disturb the target reader.

Let D_x (D_y) be the distance from reader R_x (R_y) to a target reader R_s. According to the additive interference model described in Section 4.2.3, the overall interference caused by R_x and R_y and perceived by R_s can be summed as:

$$I_{xy} = P_r \frac{G_r G_r}{K_0 D_x^\alpha} + P_r \frac{G_r G_r}{K_0 D_y^\alpha}. \tag{4.32}$$

If $\frac{P_{t,r}}{I_{xy}} \geq \Gamma$, the sum of the interferences from R_x and R_y disturbs the target reader, i.e., the combining effect of the activity of R_x and R_y generate a collision to R_s.

Since the RFID readers can be deployed one by one, it is useful to observe the effect of different positions of R_y when the position of reader R_x is fixed. The goal is to study when the simultaneous transmissions of the two readers do not interfere with the activity of the target reader. The constraint between the position of the two readers can be obtained by setting the ratio between $P_{t,r}$ and I_{xy} equal to Γ, beyond which the sum of the generated interferences causes a collision with the target reader. By substituting $P_{t,r}$ and I_{xy} according to Equation (4.22) and Equation (4.32), respectively, the relationship between the positions of R_x and R_y is represented by the following equation:

$$\frac{1}{D_x^\alpha} + \frac{1}{D_y^\alpha} = \frac{R_t G_t^2}{K_0 \Gamma d^{2\alpha}} \tag{4.33}$$

According to the above equation, D_y can be expressed as a function of D_x:

$$D_y = \sqrt[\alpha]{\frac{K_0 \Gamma d^{2\alpha} D_x^\alpha}{R_t G_t^2 D_x^\alpha - K_0 \Gamma d^{2\alpha}}}. \tag{4.34}$$

It is obvious that D_y should increase when D_x is smaller (i.e., reader R_x is closer to the target reader) in order to avoid a collision with the target reader, but here the mutual interaction between D_x and D_y is evaluated.

When the background noise is considered, according to the condition in (4.19), the minimum condition for a successful tag identification is:

$$\frac{P_{t,r}}{I_{xy} + N_0} = \Gamma \tag{4.35}$$

Substituting $P_{t,r}$ and I_{xy} according to Equation (4.22) and Equation (4.32), respectively, it is gotten the equation that regulates the mutual position of R_x and R_y such that they do not generate a collision with the target reader:

$$\frac{1}{D_x^\alpha} + \frac{1}{D_y^\alpha} = \frac{R_t G_t^2}{K_0 \Gamma d^{2\alpha}} - \frac{N_0 K_0}{P_r G_r^2}. \tag{4.36}$$

4.3.2 Ring deployment

Since in the additive interference models, the interference generated by each reader is summed in order to obtain the overall interference, a reader may experience a reader-to-reader collision even if none of the other n readers is located within the direct collision range D_{rr}. In particular, there is a special scenario where all the interfering readers R_i are positioned at the same distance from the target reader. In this case the readers are deployed along a ring, whose center is represented by the target reader. This scenario is studied in order to evaluate the maximum distance between the n simultaneously transmitting readers and the center of the ring, such as the target reader does not detect an interference. Besides, the influence of the environment parameters (for example, the pass loss exponent, etc.) is also analyzed.

In order to evaluate this scenario, the reader-to-n-readers collision range is defined as the maximum distance D_{rn} within which a reader-to-reader collision between a target reader and a group of n readers occurs. Figure 4.2 shows an example of the ring deployment scenario. Although the group of n readers can generate interferences between each other, the inter-interference among the readers on the circle is ignored. However, when the mutual interferences between the interfering readers are taken into account, the analysis of this scenario can be extended to a regular polygon deployment, such as the hexagonal constellation deployment analyzed in the next subsection.

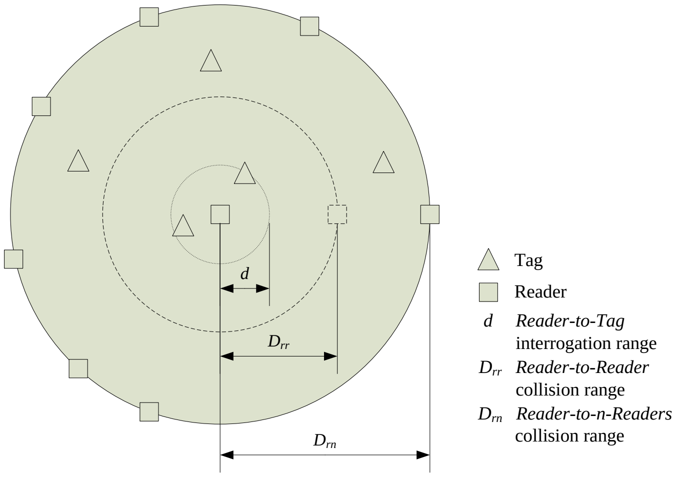

d
D_{rr}
D_{rn}
Tag
Reader
d Reader-to-Tag interrogation range
D_{rr} Reader-to-Reader collision range
D_{rn} Reader-to-n-Readers collision range

Figure 4.2. The additive interference model for the ring deployment scenario

The goal is to determine the minimum range D_{rn} from a target reader, at which n other readers can query tags without colliding with the target reader. According to Equation (4.29), the overall interference perceived by the target reader is:

$$I_r = n{\cdot}P_r\frac{G_rG_r}{K_0D_{rn}^{\alpha}}. \tag{4.37}$$

Substituting Equation (4.37) and Equation (4.22) into the condition in (4.18), D_{rn} has to satisfy:

$$D_{rn} \geq \sqrt[\alpha]{\frac{n{\cdot}K_0\Gamma d^{2\alpha}}{R_tG_t^2}}. \tag{4.38}$$

The minimum radius of the ring to avoid the interference of the group of n readers is determined only by the path loss exponent α and the threshold SIR Γ. In fact, D_{rn} is not related to the transmit power and the antenna gain of the reader when d is fixed.

If the noise power is taken into account, the radius of the ring deployment satisfies

$$D_{rn} \geq \sqrt[\alpha]{\frac{nK_0\Gamma P_r d^{2\alpha} G_r^2}{R_t P_r G_t^2 G_r^2 - N_0 K_0^2 \Gamma d^{2\alpha}}}. \tag{4.39}$$

according to condition (4.19).

4.3.3 Hexagonal constellation deployment

Given a target reader, all the other readers can be imagined as deployed on rings of different radiuses. The readers on the inner ring are defined as the *tier-1* interfering readers. In this section, all the mutual interference generated by the target readers and the tier-1 readers are considered. No other readers are involved. As the interferences between the concurrent readers are mutual, every group of three readers should form an equilateral triangle (for example, reader S, A and B in Figure 4.3). As a result, the maximum number of interfering readers on a ring is 6, independently of the radius D_{rn}. The readers are the vertices of a hexagonal constellation as in Figure 4.3: this is also the optimal disposition to completely cover an area [71]. The distance between each pair of readers in the SIR model is given as:

$$D_{r6} \geq \sqrt[\alpha]{\frac{6{\cdot}K_0\Gamma d^{2\alpha}}{R_t G_t^2}}. \tag{4.40}$$

In the SINR model, the distance will be

$$D_{r6} \geq \sqrt[\alpha]{\frac{6{\cdot}K_0\Gamma P_r d^{2\alpha} G_r^2}{R_t P_r G_t^2 G_r^2 - N_0 K_0^2 \Gamma d^{2\alpha}}}. \tag{4.41}$$

4.4 Evaluation Results

In this section, the previously described scenarios are evaluated according to the single interference model and the additive interference model and their contributions on the RFID reader-to-reader collision problem are compared. Since the models considering the noise power are more practical and precise, all the results take into account

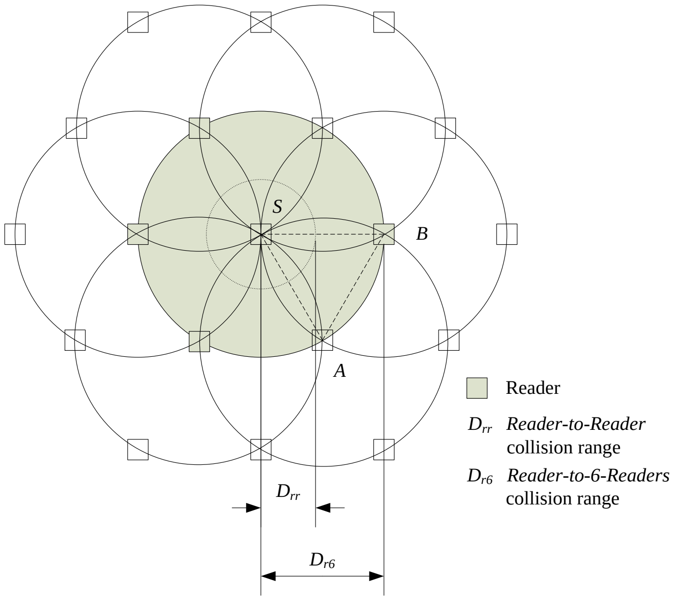

S
B
A
Reader
D_{rr} Reader-to-Reader collision range
D_{r6} Reader-to-6-Readers collision range
D_{rr}
D_{r6}

Figure 4.3. The hexagonal constellation deployment

Table 4.1. Evaluation Parameters

Parameters	Values
Path loss exponent (α)	2, 3, 4, 5
SIR Threshold (Γ)	1, 5, 10, 15
Reader antenna gain (G_r)	6 dBi
Tag antenna gain (G_t)	1 dBi
Tag's power reflection coefficient (R_t)	3/4
Reader's transmit power (P_r)	10 dBm
Constant coefficient (K_0)	G_r^2
Interrogation range (d)	$\sqrt[\alpha]{25}\ m$
Noise power (N_0)	0, -30, -35, -40, -45 dBm

the background noise. All the considered scenarios have been evaluated based on a custom implemented simulator using MATLAB, which is publicly available[2].

The effects of the number of interfering readers and of their distance is evaluated according to the parameters listed in Table 4.1. The antenna gains of the reader and tag are set as 6 dBi and 1 dBi, respectively. The power reflection coefficient on a tag is 3/4. The transmit power P_r of a reader is set to 10 dBm. K_0 is set to the lower bound, G_r^2, according to the received power P_0 measured at $d_0 = 1\ m$ [71]. The interrogation range d is set to 5 m when $\alpha = 2$. Given a fixed Θ in the

[2] http://ubi.polito.it/research/interferenceModels.htm

condition in (4.17), $d^{2\alpha}$ is fixed according to Equation (4.21) and (4.22). Therefore, d is set to $\sqrt[\alpha]{25}\ m$ with respect to different path losses. For each evaluation scenario, the impacts of the following three parameters are evaluated:

- The path loss exponent (α): in a free space mode, α is set to 2. Besides, the exact value of the path loss exponent in low power wireless links is between 4.3 and 5.1 in an outdoor environment, while it falls between 2.67 and 3.23 in an indoor environment [84]. Therefore, the value of α varies from 2 to 5. When the impacts of α is investigated, Γ and N_0 are set to 1 and 0, respectively.

- The SIR ratio threshold (Γ): in an ideal wireless communication channel with perfect capture capability [85], Γ is set to 1. Therefore, the impact of Γ is investigated by varying the values from 1 to 15 while $\alpha = 2$ and the background noise is assumed negligible.

- The background noise power (N_0): based on the assumed values in Table 4.1, the maximum noise power that ensures the successful interrogation activity is -29.2 dBm according to Equation (4.23). Therefore, the different values of the noise power are assumed as 0, -40 dBm, -35 dBm, -30 dBm, where 0 indicates a model without considering noise power and 30 dBm is close to the maximum value. In order to investigate the impact of the background noise, the SINR threshold Γ is set to 1 and α is set to 2.

4.4.1 Pair interaction

Figure 4.4 reports the results obtained by evaluating Equation (4.33) with respect to different SIR thresholds. The curvature of the curve reflects the interaction between the pair of interfering readers: the larger the curvature is, the more strongly they interact with each other. As a general rule, the results are symmetric since the interaction is mutual. For each line there are two asymptotes to D_{rr}, which indicates the minimum distance between readers to avoid collisions. When D_x (or D_y) is equal to D_{rr}, D_y (D_x) is infinite. As Γ decreases, the corresponding result approaches the asymptote more quickly and the curvature increases, which means that the two readers interact with each other more strongly. The minimum distance D_{rr} between two readers (i.e., the asymptote value) grows as the Γ increases, as confirmed in Equation (4.28). When $D_x = D_y$, the scenario evolves into a ring deployment with two interfering readers R_x and R_y; D_{r2} grows as Γ raises. Figure 4.5 shows the influence of α under an ideal channel where Γ is set to 1. It can be observed that the lower the value of α is, the smaller the bound value of D_x (or D_y) is.

Figure 4.4 and Figure 4.5 also show the horizontal and vertical lines corresponding to the unit disk graph model. From the comparison between D_{rr} in the unit disk graph model and D_x (or D_y) in the model described in Section 4.2.3, it can be observed in Figure 4.4 and Figure 4.5 that with a lower value of α the unit disk graph model often fails to identify collisions, as in presence of a high SIR. For example, when $\alpha = 4$ and $\Gamma = 1$, D_x and D_y in the model in Section 4.2.3 are almost the same of D_{rr} as in the unit disk graph.

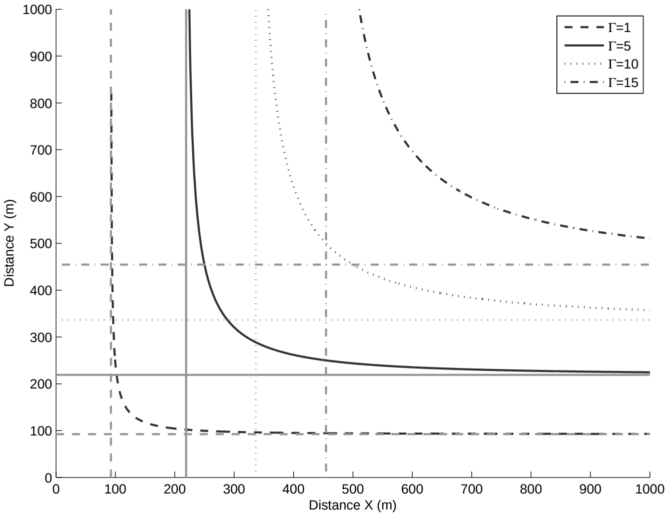


Figure 4.4. Reader pair interaction according to different SIR thresholds. The curve in light gray is for the unit disk graph model and in dark gray for the additive interference model.

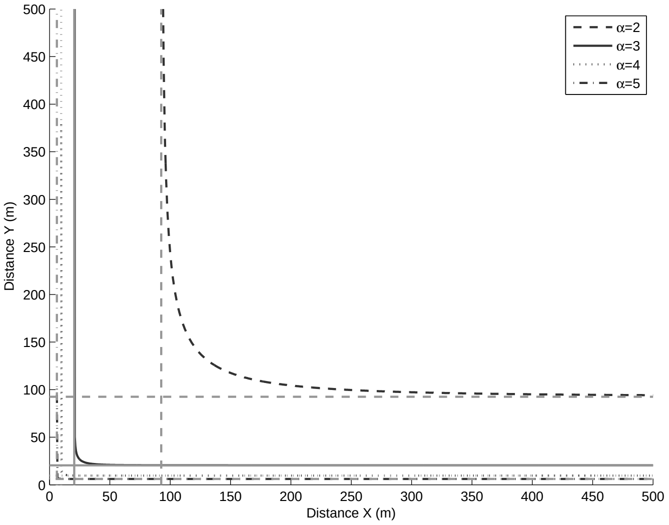


Figure 4.5. Reader pair interaction according to different path loss exponents. The curve in light gray is for the unit disk graph model and in dark gray for the additive interference model.

Figure 4.6 shows the impact of the background noise power on the pair interaction: it can be observed that the noise power plays an important role. When the noise is close to the maximal value (-30 dBm), the two interfering readers interact with each other more slightly since the curvature of the curve becomes smaller. On the other hand, a large noise power requires both of the two interfering readers further away from the target reader, in other words, D_{rr} in the single interference model grows when the noise power increases.

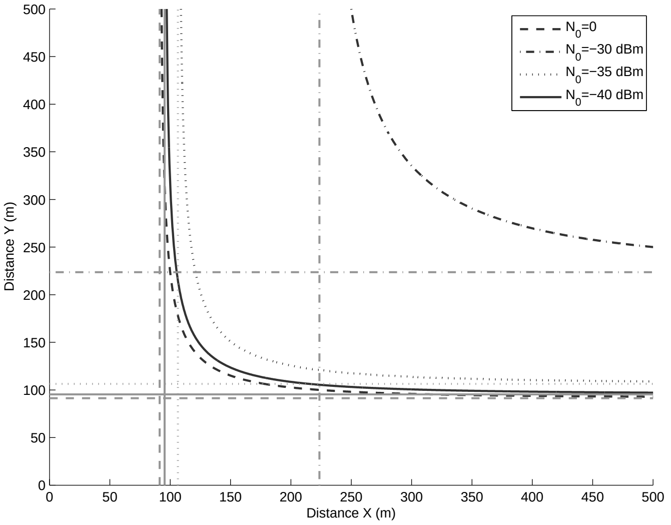


Figure 4.6. Reader pair interaction according to different noise power. The curve in light gray is for the unit disk graph model and in dark gray for the additive interference model.

4.4.2 Ring deployment

In Figure 4.7 and Figure 4.8, the reader-to-n-readers collision range is shown as a function of the number of interfering readers n according to different SIR thresholds and α. In the additive interference model, as the number of interfering readers grows, they need to be further from the target reader in order to avoid collision: the collision range D_{rn} is identical to D_{rr} only when n is equal to 1. Instead in the unit disk graph model, D_{rn} is always equal to D_{rr}. In Figure 4.7, D_{rn} increases as α decreases. Furthermore, the larger the pass loss exponent α is, the faster the distance increases. For example, when $\alpha = 2$, the distance increases from 92.51 m to 292.60 m, moving from 1 interfering reader to 10 interfering readers. The increase is smaller when α is 4 (from 9.62 m for 1 reader to 20.46 m for 10 readers). On the other hand, D_{rr} rises up as SIR threshold increases as shown in Figure 4.8. A larger SIR threshold implies that the target reader requires a lower interference to experience a collision, consequently the radius needs to be larger in order to reduce the interference generated.

The difference between the unit disk graph model and the additive interference model increases as the number of interfering readers grows. Moreover, the results in the ring deployment reflect again that lower α and higher SIR increase the differences in the two models. For example, when the number of readers is 5 in Figure 4.7, the gap between the two models grows from 4.76 m to 114.39 m when α falls from 4 to 2. On the other hand, in Figure 4.8, the difference is equal to 114.39 m when $SIR = 1$, while it reaches 415.8 m when $SIR = 10$.

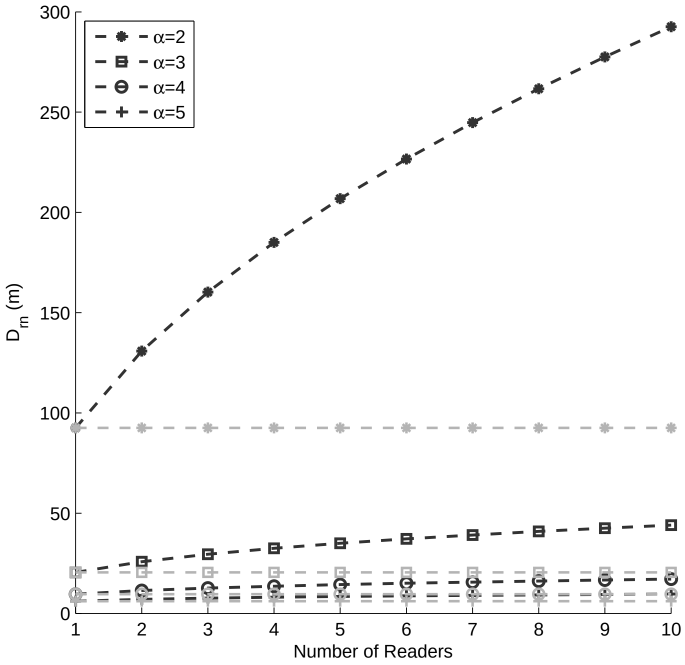


Figure 4.7. Ring deployment radius vs. number of interfering readers according to the path loss exponent. D_{rn} is shown in light gray for the unit disk graph model and in dark gray for the additive interference model.

Figure 4.9 illustrates the impact of noise power on the radius of the ring deployment. It can be seen that when the noise power grows, the radius of the ring deployment increases more quickly with respect to the number of readers. It is interesting to notice that D_{rr} grows as the noise power increases, which means the RFID readers are easier to suffer from reader-to-reader collisions in an environment with a larger noise power. By comparing the gap between the curves of the single interference model and additive interference model, it can be also observed that the two models give similar performance in an environment with low background noise

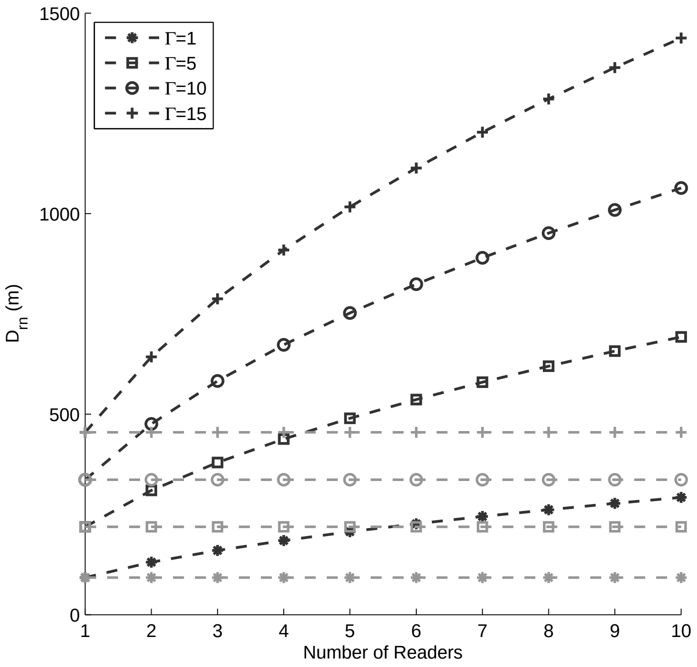


Figure 4.8. Ring deployment radius vs. number of interfering readers according to the SIR threshold. D_{rn} is shown in light gray for the unit disk graph model and in dark gray for the additive interference model.

power. On the contrast, the performance differs significantly in an environment with a large noise power. In other words, the single interference model give a good performance in a "quiet" environment but it is less accurate than the additive interference model in a "noisy" environment.

4.4.3 Hexagonal constellation

The results for different values of the side length of the hexagonal constellation with respect to various environments are shown in Figure 4.10. Similarly to D_{rr}, the side length of the hexagonal constellation goes down as α grows, and it goes up as Γ increases. It can be observed that the impact of Γ is slighter as α grows.

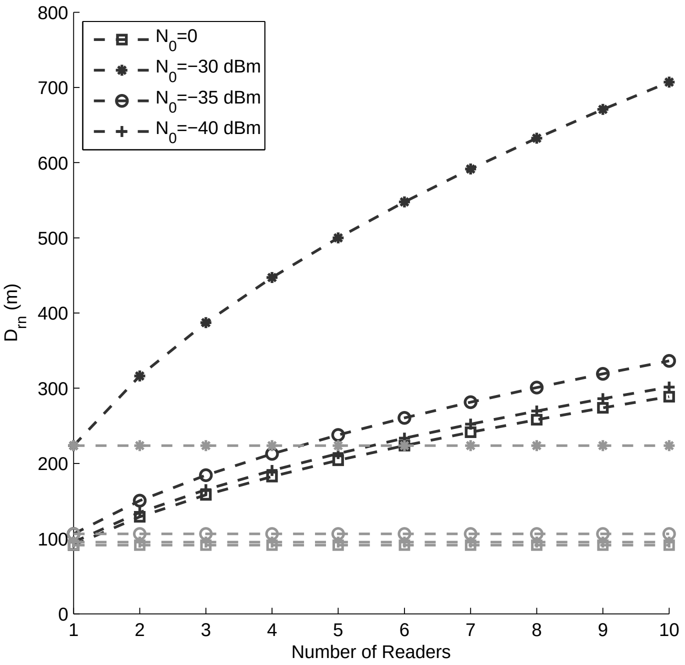


Figure 4.9. Ring deployment radius vs. number of interfering readers according to the noise power. D_{rn} is shown in light gray for the unit disk graph model and in dark gray for the additive interference model.

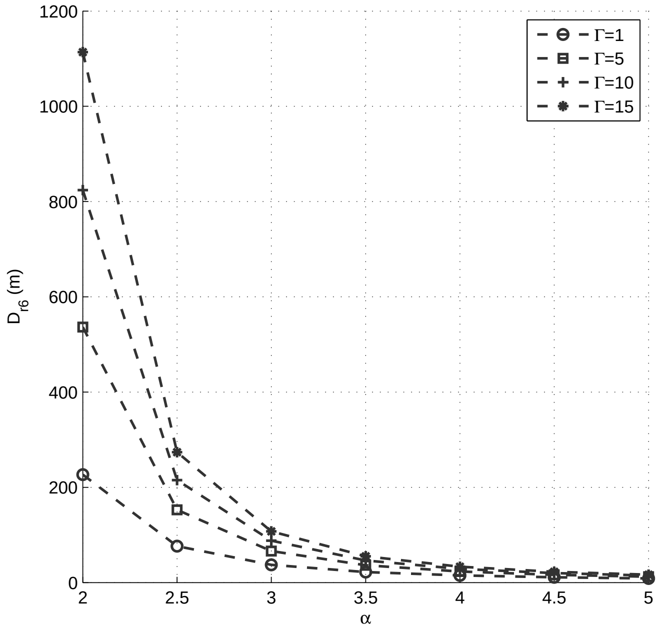


Figure 4.10. Side length of the hexagonal constellation vs. path loss exponent according to the SIR threshold

Chapter 5

Cardinality Analysis of the Additive Interference models

In this chapter, the additive interference model considering different number of simultaneously interrogating readers are analyzed. A branch and bound algorithm is proposed in order to choose the appropriate value of concurrent readers. Based on the results of the algorithm, the throughput tolerance and accuracy of collision detection are analyzed for the additive interference model considering different numbers of minimal *collision-set-n*.

5.1 The Evaluation Simulator

The difference between single interference models and additive interference models is the cardinality n of the considered collision set. This section numerically evaluates the impact of n on the detection accuracy of the reader interference. The evaluation is based on the single channel model described in the previous section. Besides, it is assumed that the background noise is negligible and all the RFID readers are identical with the same antenna gain and transmitting power.

For convenience, a collision set of cardinality n is referred to as $collision-set-n$. Besides, in order to avoid considering redundant collision sets, only *minimal collision sets* are considered. A minimal collision set is defined as the collision set in which the simultaneous interference of all the member can hamper the target reader's interrogation activity, but the overall interference of any subset will not disturb the target reader. In other words, a minimal collision set does not include any other collision sets. The proposed evaluation simulator is based on the collection of the minimal collision sets of each reader, through which the impacts of the size of the considered collision sets can be observed. Obviously, the value of n plays an important role in the evaluation of the reader collision models. The adopted interference model is an additive interference model which is based on the basic assumption that the total interference power from multiple interfering readers to the target reader is additive. It can be viewed as a generalized model of single interference model by considering multiple readers' collision instead of just considering direct collisions. Besides, it is assumed that the background noise is negligible and that the signal power at the receiver is only attenuated due to path loss. It is assumed that the RFID medium access uses a single-channel mode where the reader-to-tag query communication and tag-to-reader response communication share a bidirectional channel.

Algorithm 1 Calculate the collision sets in the RFID reader set R with cardinality lower than $Card_{max}$

```
for all RFID reader $i \in R$ do
   $P = \emptyset$;
   for all RFID reader $j \in R \backslash \{i\}$ do
      calculate the interference $P_{ji}$ according to Equation (4.24);
      $P = P \cup \{P_{ji}\}$;
   end for
   sort $P$ in descending order;
   call Subset($i$,$P$,0);
end for

Procedure Subset(id $i$, set $P$, float $S$)
for all Element $P_{ki} \in P$ do
   if $Stack.size < Card_{max}$ then
      push($P_{ki}$);
      if $S + P_{ki} > \frac{P_{t,i}}{\Gamma}$ then
         collisionSets[i].add(Stack);
      else
         $S = S + P_{ki}$;
         call Subset($i$, $P \backslash \{P_{ki}\}$, $S$);
      end if
      pop($P_{ki}$);
   end if
end for
End Procedure
```

In order to collect the minimal collision sets, each subset of the reader set R (without considering the target reader) is checked to find whether it is a minimal collision set of the target reader. As shown in algorithm 1, the collision sets are calculated for each reader in the deployment. The general idea is to adopt a branch and bound algorithm to collect all the minimal collision sets for each reader $i \in R$.

In order to consider all the subsets, all the element $j \in R \backslash \{i\}$ are first sorted by the descending order of the interference P_{ji} received by i. Then a recursive procedure is called to check all the subsets of $R \backslash \{i\}$ which are the minimal collision sets. In this procedure, a stack is used to store the current subset of $R \backslash \{i\}$ to decide whether the sum of the interference of the readers in this subset can generate a collision to the target reader. When the set in the stack turns out to be a collision set, all the subsets that contain the stack will be ignored since only minimal collision sets are considered. Besides, a control parameter $Card_{max}$ is introduced to indicate that only the subsets with cardinality lower than $Card_{max}$ are considered.

5.2 Numerical Results

The number of interfering readers (i.e., the cardinality n of the collision-set-n) is calculated according to the parameters listed in Table 5.1. A free space model is considered, assuming that no shadowing effect exists and the signal power at the receiver is attenuated with a path loss exponent equal to 2. The SIR threshold Γ is set to 10. All the RFID readers are considered homogeneous with an antenna gain of 6 dBi and a constant transmit power of 10 dBm. The antenna gains of the tags are set to 1 dBi. The power reflection coefficient of the tag is $\frac{3}{4}$. P_0 is set to the upper bound $\frac{1}{G_r^2}$ [71]. The distance between a reader and the queried tag $|x - t|$ is set to 5 m. Besides, the background power is considered negligible.

Table 5.1. Evaluation Parameters

Parameters	Values
Path loss exponent (α)	2
SIR Threshold (Γ)	10
Reader antenna gain (G_r)	6 dBi
Tag antenna gain (G_t)	1 dBi
Tag's power reflection coefficient (E_{tag})	$\frac{3}{4}$
Reader's transmit power (P_r)	10 dBm
Path loss at the reference distance d_0 (P_0)	$\frac{1}{G_x^2}$
Reader-to-tag distance ($\|x - t\|$)	5 m
Noise power ($\mathcal{N}$)	0

In the simulation, different groups from 20 to 50 readers are randomly deployed in a 1000 $m \times 1000$ m field and the simulation is repeated 1000 times to reduce the effect of randomness.

5.2.1 The number of readers affected by collision-set-n

If one reader has at least one collision-set-n, it is said to be affected by collision-set-n, i.e., it can experience a reader collision caused by n interfering readers. Figure 5.1 shows the number of readers affected by different collision-set-n with $n \leq 20$. Different scenarios are considered by increasing the number of readers deployed in the fixed field from 20 to 50. The number of readers affected by collision-set-n increases as the deployment density increases. It can be seen that the readers are more likely to suffer from the additive interference in a dense deployment.

Considering the scenario with 50 readers as example, it can be observed that almost all the readers have collision sets with cardinality from 1 to 5. The number of readers affected by collision-set-2 until collision-set-5 are almost the same as the number of readers affected by direct collisions (collision-set-1), which reflects that single interference models are not enough to cover all the collisions in a dense RFID deployment. From collision-set-6, the number of affected readers starts to reduce in a great scale. The RFID reader can be affected until the sum of 14 readers' interference are considered. There is not any minimal collision set with more than 14 readers that can generate a total interference that can hamper the target reader, which means that it is not necessary to consider additional interference of more than 14 readers.

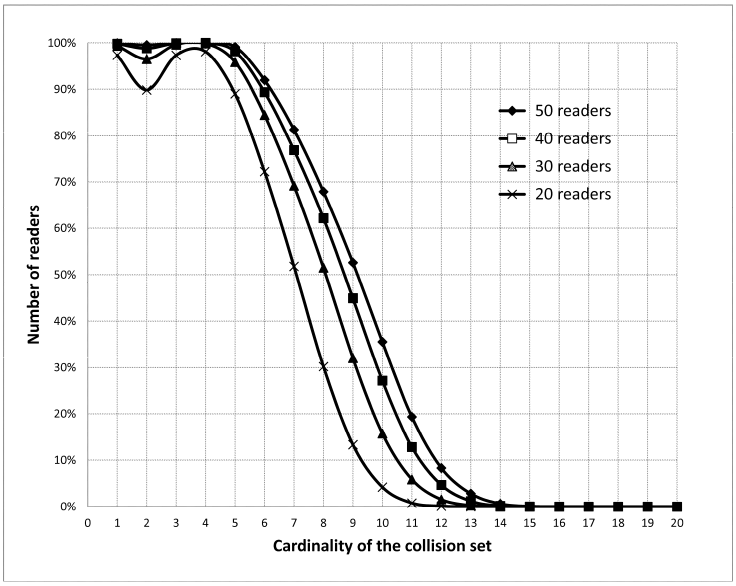


Figure 5.1. The number of readers affected by different collision-set-n

5.2.2 The average number of collision-set-n

The average number of collision-set-n is the total number of collision-set-n divided by the number of readers in the deployment. It can be seen in Figure 5.2 that the average number of collision-set-n follows a Gaussian distribution in each scenario. The exact shape of the distribution depends on the characteristics of the deployment. The x-coordinate value of the vertex of the parabola increases from 6 to 9 when the number of readers increases from 20 to 50. Besides, the amount of collision-set-n significantly grows when the total number of readers goes up.

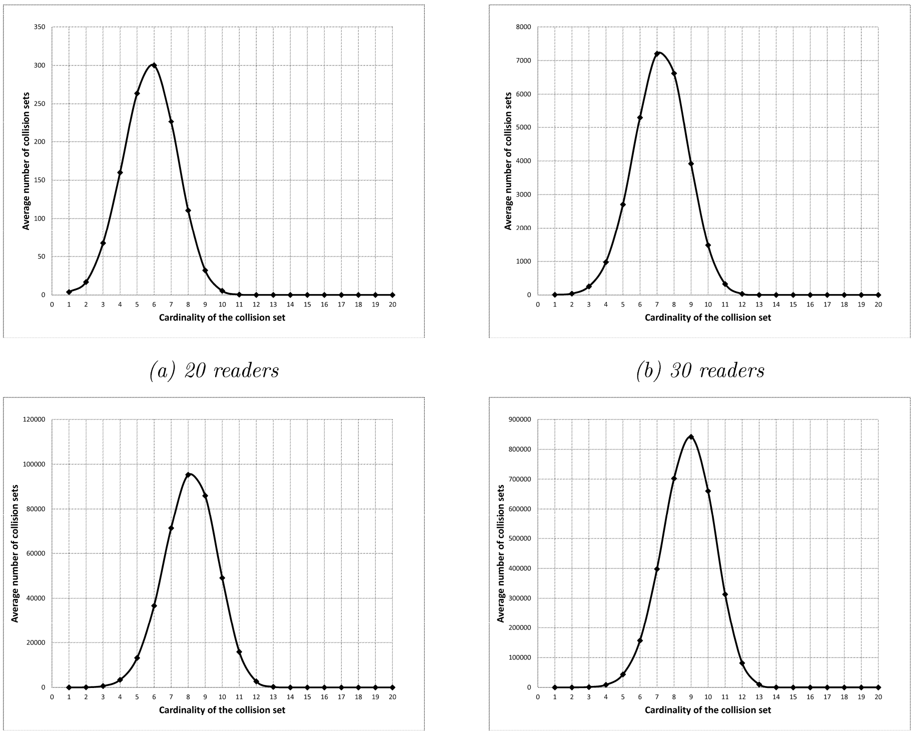
Under the scenario with 50 readers as shown in Figure 5.2 (d), the average number of collision-set-n first climbs up when n grows from 1 to 9. After reaching the peak with $n = 9$, it starts to fall down until $n = 14$. The average number of collision-set-15 stays at 0, which is in accordance with Figure 5.1. That is because all the readers sets with cardinality higher than 14 have a subset (i.e., a minimal collision set) that already generate an interference perceived by the target reader.

When $n < 9$, the average number of collision-set-n climbs up because of two reasons: firstly, the probability of generating collisions increases as the number of interfering readers grows; secondly, the number of potential subsets that may generate collisions grows with the cardinality n. For example, the total number of subsets with cardinality 1 is $\binom{50}{1} = 50$, while the number of subsets with cardinality 4 grows to $\binom{50}{4} = 230300$. Although the maximal number of subsets continues to grow when $9 < n < 20$, the subsets that can generate collisions fall down since many collision-set include minimal collision sets with cardinality lower than 9.

5.2.3 The distribution of collision-set-n

To some extent, the average number of collision-set-n disposes the influence of different collision-set-n on the reader interference model. However, how does the data is spread out is also important. If one reader has an extremely large number of collision-set-n while other readers has none, only the average number can not be used to evaluate the influence. In order to investigate on how the collision sets are spread out, some distributions of the collision-set-n number in the scenario with 50 readers (on a 1000 $m \times 1000$ m field) are plotted in Figure 5.3. It is generated by collecting how many readers have the specified number of collision-set-n. If a reader has few collision-set-n, it does not suffer or suffer slightly from collision-set-n. Otherwise, it suffers a lot from collision-set-n.

From Figure 5.3, it can be seen that the distribution of collision-set-n spreads more sparse as n increases. In Figure 5.3 (a), (b) and (c), the number of readers assume highly localized distribution around one peak value. For example, when considering direct collisions, 5.03 readers in average have 9 collision-set-1s and there



(a) 20 readers

(b) 30 readers

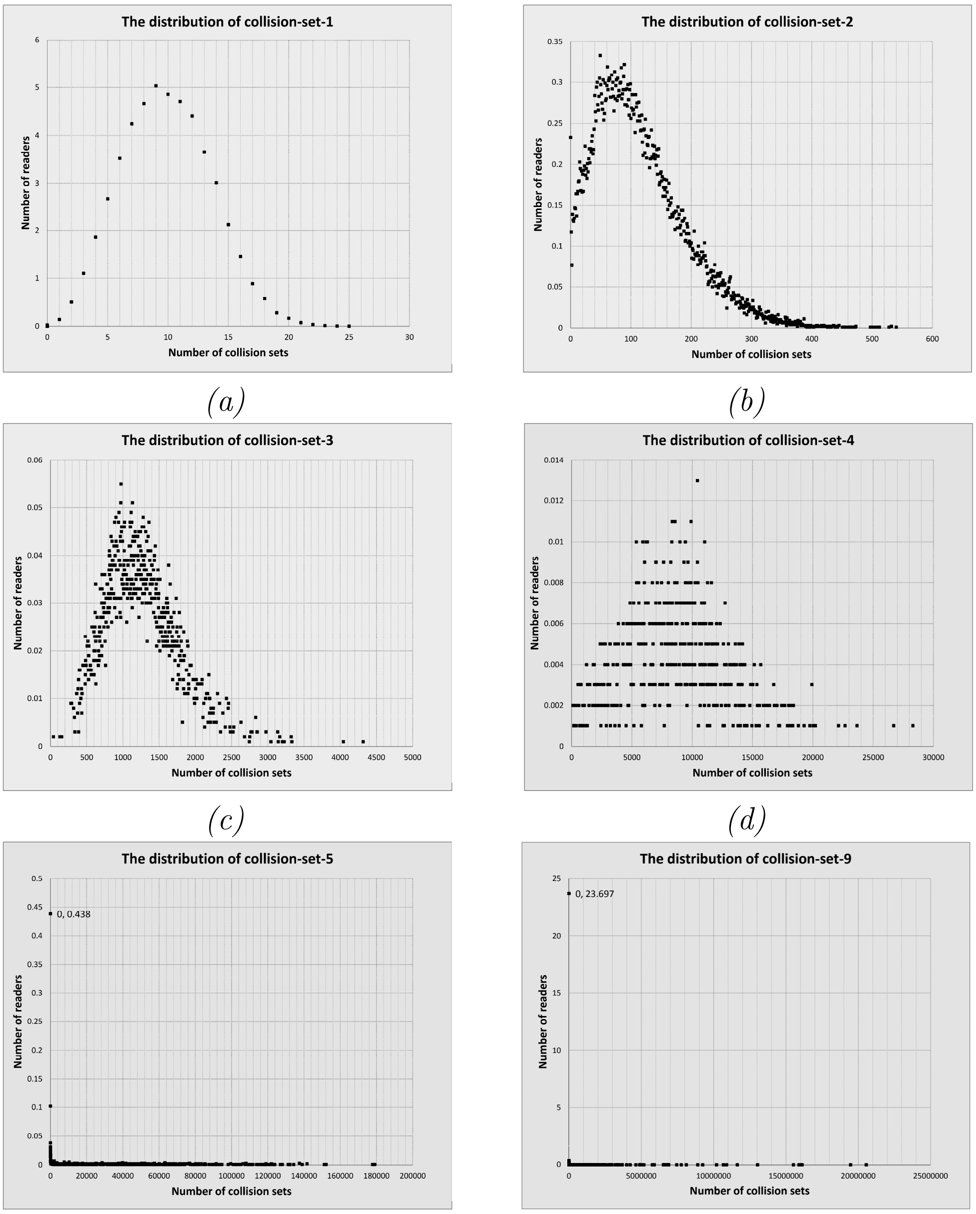
(c) 40 readers

(d) 50 readers

Figure 5.2. The average number of collision-set-n according to different scenarios

is no reader that does not suffer from collision-set-1. The more sparse the distribution, the slighter is the impact of collisions-set-n. Because when the distribution of collision-set-n is sparse, the peak value will be smaller which means that fewer readers has the same number of collision sets and they are interfered by the collisions more randomly. In Figure 5.3 (d), the distribution of collision-set-4 is more sparse than the previous 3 distributions, but it still holds the similar structure. Starting from $n = 5$, the collision sets spread more randomly and more readers do not suffer or suffer slightly from the sum interference. For example, in Figure 5.3 (e) and (f), the number of readers that do not have collision-set-5 or collision-set-9 is 0.44 and 23.697, respectively. Besides, the distribution concentrate in the area where the reader suffer from a few collision sets. Especially in the distribution of collision-set-9, only a few readers out of the total number suffered severely from the additive interference of collision-set-9, but most of other readers are safe from this collision.

Combining the numerical results in Figure 5.1, Figure 5.2, Figure 5.3, it can be concluded that in the specific deployment, the additive interference model that considers up to 4 readers is the minimum requirement in order to cover all the collision-sets-n that can affect more 99% of the total readers.



(a) *(b)*

(c) *(d)*

(e) *(f)*

Figure 5.3. Distributions of different collision-set-n

5.3 Throughput Analysis

The number of affected readers and the average number of collision-set-n intuitively expose the influence of different collision-set-n on the reader interference model. However, it is also important to take into account the probability that the reader will interrogate at a certain time. The probability that all the member readers within a collision-set-n try to query the tags simultaneously decreases when the cardinality of the collision set grows. Therefore, apart from the numerical results in the previous section, a further analysis is performed in this section. The analysis is based on the numerical results under the scenario that 50 RFID readers are deployed in a 1000 $m \times 1000$ m field.

Considering a TDMA (Time Division Multiplexing Access) reader-to-reader anti-collision scheme in which each reader tries to query tags in a time slot with probability p, the probability that a collision set with n readers generates enough noise to cause an interference is:

$$Pr(collision - set - n \; interferes) = p^n. \tag{5.1}$$

Fig. 5.4 shows how the probability that a set generates a collision exponentially decreases as n increases. The value of p reflects the interrogation frequency of the RFID system. It can be observed that a low value of p causes a sharper fall of the collision probability, which means that it is not necessary to consider a large cardinality n of the collision set. In other words, the additive interference model seems more necessary in a RFID system where the readers interrogate the tags more frequently.

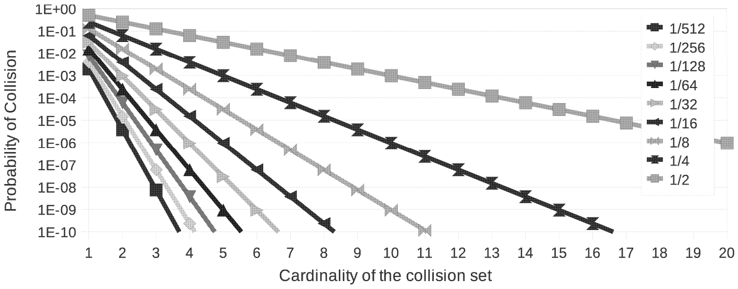


Figure 5.4. The probability that all the readers in collision-set-n interrogate simultaneously.

The average quantity of possible collisions that a reader receives at each time slot can be calculated as

$$Q_n = s_n \cdot p^n \tag{5.2}$$

where s_n represents the average number of sets with n additive components. In the case study of 50 readers deployed on a 1000 m per 1000 m square, the evaluation of (5.2) according to p and n is shown in Fig. 5.5. It can be observed that:

- if p is high, also the average number of possible collisions is high, so the probability of successfully querying tags is very low;

- if p is high, the distribution of the quantity of collisions according to cardinality of the collision set is similar to a Gaussian distribution;
- if p is low, the distribution curve constantly decreases and the most common collisions have only one component.

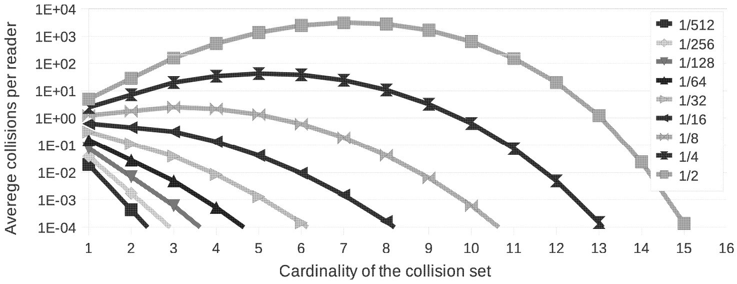


Figure 5.5. The average number of collision set for each reader

The above analysis indicates that the collision sets composed by many readers do not strongly affect the overall number of collisions. In order to further analyze the contribution of each group of collision sets, it is required to select a realistic value of p that guarantees a good throughput. Here, the throughput is defined as

$$T = p * p_{succ}, \tag{5.3}$$

where p_{succ} represents the probability of avoiding collisions. Since the probability that a collision within a collision-set-n is avoided is $1 - p^n$, if it is assumed that all the s_n collision-set-ns are independent from each other, the p_{succ} for s_n collision-set-ns is $(1-p^n)^{s_n}$. Considering all the collision-set-n in the specific RFID system, the overall probability p_{succ} of the whole RFID system could be calculated introducing an approximation:

$$p_{succ} = \prod_{n=1}^{N-1} (1-p^n)^{s_n}. \tag{5.4}$$

In order to decrease the approximation, the analysis takes into account the distribution of the number of collision-set-n. In a RFID system with N readers, the collision set with the maximum cardinality is collision-set-$(N-1)$. For each value of n between 1 to $N-1$, each reader has a certain number of collision-set-n which is from 0 to $\binom{N-1}{n}$. Let $d_n(i)$ represent the quantity of readers affected by i collision-sets-n and let X be the random number of collision-set-n, the discrete probability distribution of X is characterized by the following probability mass function

$$Pr(X = i) = \frac{d_n(i)}{N}, \tag{5.5}$$

where $X \in [0, \binom{N-1}{n}]$. Since the probability of avoiding collisions from the i collision-set-n is $(1-p^n)^i$, the probability to avoid collisions from all the collision-set-n can be calculated as

$$Pr(no\ collision\ from\ collision-set-n) = \sum_{i=0}^{\binom{N-1}{n}} Pr(X=i) \cdot (1-p^n)^i. \qquad (5.6)$$

Figure 5.6 evaluates Equation (5.6) for different values of p and n. It can be observed that when $p \leq \frac{1}{16}$, the probability of avoiding collisions constantly increases as n grows. When $p \geq \frac{1}{8}$, the largest impact of collision-set-n appears when $n = 3$ or $n = 4$. Besides, when n grows to more than 13, the value of n will have no impact on the probability of avoiding collisions no matter what value of p is, since no collision sets with cardinality higher than 13 exists.

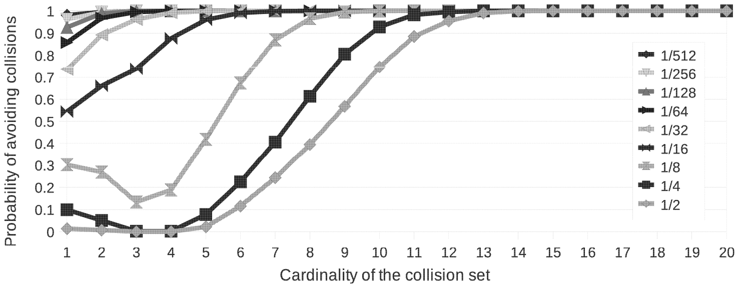


Figure 5.6. The probability of avoiding collisions considering different collision-set-ns

By combining Equation (5.5) and Equation (5.6), the overall probability of avoiding collisions in Equation (5.4) can be written as

$$p_{succ} = \prod_{n=1}^{N} \sum_{i=0}^{\binom{N-1}{n}} \frac{d_n(i) \cdot (1-p^n)^i}{N}, \qquad (5.7)$$

which considers the distribution of the collision sets.

Based on Equation (5.3) and Equation (5.7), the overall throughput of the RFID system is shown in Figure 5.7 with respect to different values of p. Since $p = \frac{1}{32}$ provides the best results, this value has been used for the subsequent analysis.

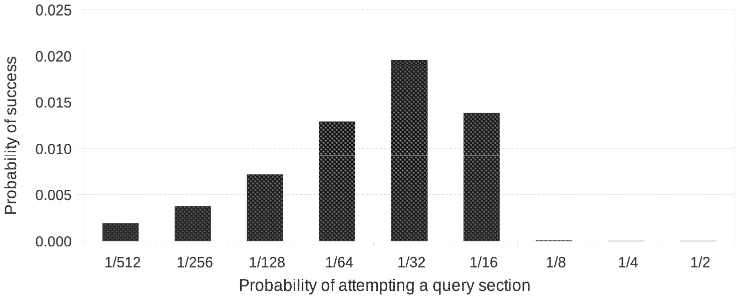


Figure 5.7. The throughput of the RFID system assuming different probabilities of the query per time slot per reader

5.4 Accuracy Analysis

Based on Equation (5.6), the probability that a collision is caused by collision-set-n and that no collisions are caused by a smaller collision-set-m, $m{\leq}n$, is:

$$p_n = \begin{cases} (1 - \sum_{i=0}^{N-1} \frac{d_{1i}(1-p)^i}{N}), & \text{for } n = 1 \quad (5.8a) \\ (1 - \sum_{i=0}^{\binom{N-1}{n}} \frac{d_{ni}(1-p^n)^i}{N}) \prod_{j=1}^{n-1} \sum_{i=0}^{\binom{N-1}{j}} \frac{d_{ji}(1-p^j)^i}{N}, & \text{for } n \geq 2 \quad (5.8b) \end{cases}$$

. Figure 5.8 shows the distribution of potential collision sets in the network and the

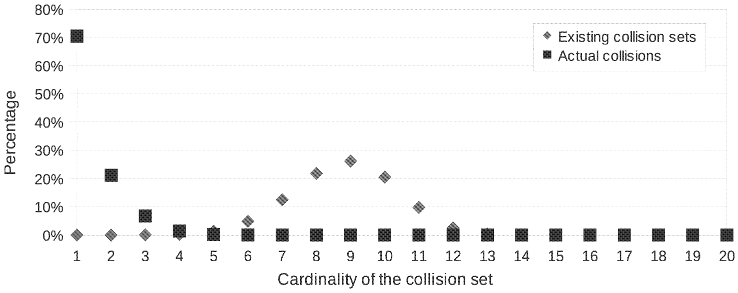


Figure 5.8. The distribution of the existing collision sets and the actual collisions

distribution of actual collision, where the distribution of collision sets is based on the numerical results in Figure 5.2 and the distribution of actual collision probabilities is calculated as follows:

$$D_n = \frac{p_n}{\sum_{n=1}^{N} p_n}. \tag{5.9}$$

It can be observed that although the distribution of the collision sets is similar to a Gaussian distribution, the actual collision probability with cardinality n decreases as the value of n increases. Figure 5.8 also shows that the majority of the collisions are due to sets composed by few readers, while the majority of the existing sets include many readers. Therefore, a large part of the collision sets can be not considered in the analysis of the performance of a protocol, without affecting significantly the accuracy of the results.

The percentage of error in the collision detection is shown in Figure 5.9. The percentage is evaluated according to the following ratio

$$E_n = 1 - \sum_{n=1}^{N} D_n. \tag{5.10}$$

Each point in Figure 5.9 shows the error in collision detection when considering collision sets with cardinality up to n. The result shows how the accuracy of collision detection increases as the cardinality of the collision sets grows. When $n \geq 11$, the error percentage is lower than 10^{-10} and consequently it is not shown because it is out of scale. Fig. 5.10 shows the percentage of collision sets that can be covered when up to n readers' interferences are summed. By comparing the two charts, it is possible to observe that the majority of the collisions can be detected even if the majority of the sets are excluded from the analysis of a RFID reader-to-reader protocol. For example, excluding all the the sets with a quantity of components larger or equal to 7, only 0.00205% of the collisions are not detected, and only 6.54546% of the collision sets are considered.

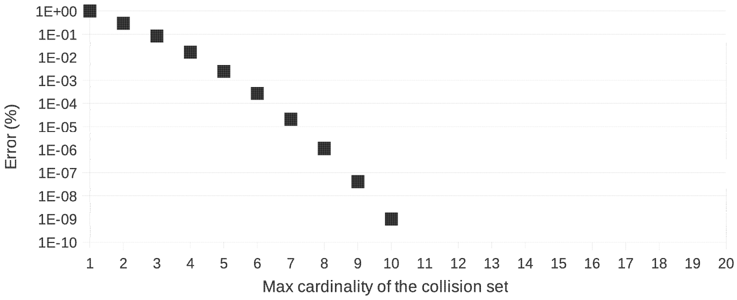


Figure 5.9. The accuracy of collision detection considering up to n concurrent readers

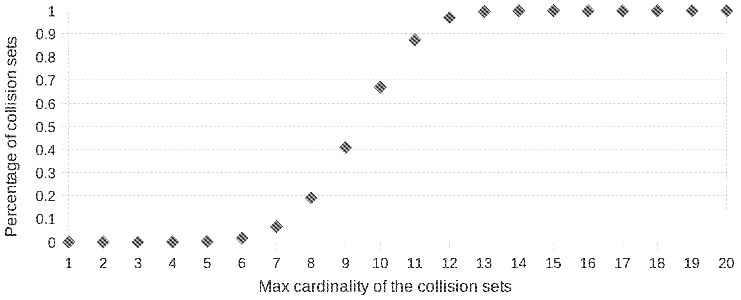


Figure 5.10. The percentage of covered collisions considering up to n concurrent readers

Chapter 6

Simulation of Reader-to-Reader Collisions in RFID Systems

This chapter investigates the available network simulators in the state-of-teh-art. Based on the investigation, the requirements for a RFID simulator is concluded. According to the requirements, a specific simulator for reader-to-reader anti-collision simulator based on OMNeT++ is introduced. In order to test the novel simulator, several scenarios are presented and evaluated. Furthermore, the test results also provide a simulation-based comparison between the single interference model and the additive interference model.

6.1 Simulation Tools in RFID research

6.1.1 General purposed simulators

Since the use of RFID technology for automatic identification is increasing, RFID networks composed of many readers are becoming common. In these systems, the interference among two or more UHF readers simultaneously querying passive tags on the same frequency leads to a reader-to-reader collision and represents a significant problem for the application reliability. Many reader-to-reader anti-collision protocols have been proposed to address this issue. Their evaluation is typically based on simulations, reducing costs and time of the testing phase. Simulations provide general results by analyzing different scenarios. Through the on-line modification of the network parameters, a simulator allows fast feedback about the effects of different configurations. Consequently simulations represent a natural choice for evaluating the performance.

Although the simulations of reader-to-reader anticollision protocols are widely exploited, publicly available ad-hoc simulators do not exist. Many researches present results based on simulations executed with general purpose network simulators, which rarely adapts to the peculiarity of RFID systems. Other researches exploit privately self-developed tools to run the simulations: this limits the reproducibility and the comparison of the results. Many reader-to-reader anti-collision protocols were evaluated by means of simulation tools for discrete event systems. An event is an individual transaction with a definite beginning and end, like the transmission or the reception of a data packet or the advancement of a timer. The main characteristics of each simulator are briefly described, providing some references about their use in studying reader interference.

- ***NS-2***

  NS-2[1] is an open source simulator developed in C++ and OTcl. C++ code is used to implement the network components. OTcl is an object-oriented programming language and it is used to configure the simulation scenario, including the initialization of the network topology, and to define a new network object by assembling existing ones. An OTcl script is also used to schedule the events during the simulation. NS-2 offers implementations of network protocols, different propagation models, several ad-hoc routing protocols, mechanisms for managing queues, models of traffic source. Some RFID reader anti-collision protocols were implemented from scratch and tested with NS-2.

  The open source simulator NS-3[2] has been developed as a distinct tool from NS-2 and not backward-compatible with it. The simulator is written in C++, with an optional Python interface: the user can generate the simulation scripts either in C++ or in Python. In a C++ script, each object of the network (such as a node, a channel and a network device driver) is modeled by a specific class. Some other classes act as topology helper to provide a convenient way to create, configure and manage the network objects. NS-3 is targeted for simulating the data link, network and transport layers in Internet systems and it implements several network protocols. Nevertheless NS-3 was successfully used for proposing new solutions for RFID reader interference [86].

- ***J-Sim***

  J-Sim (JavaSim)[3] is an object-oriented, component-based, compositional simulation environment for WSNs written in Java. The key strength of J-Sim is that modules can be easily added and deleted in a plug-and-play manner. It can be used both for network simulation and emulation by incorporating one or more real sensor devices. J-Sim provides support for simulating sensor

[1] http://nsnam.isi.edu/nsnam/index.php/Main Page

[2] http://www.nsnam.org

[3] http://j-sim.cs.uiuc.edu/

and sink nodes, sensor channels and wireless communication channels, physical media, power models and energy models. J-Sim [87] can be used to simulate the reader-to-reader anti-collision protocols by considering the RFID system as a particular case of wireless sensor networks.

- ***OPNET***

  OPNET[4] is a commercial platform for simulating communication networks. It supports three different kinds of simulation. Firstly, OPNET is a discrete event simulator to model transient network activities, such as data packet exchange. The second operating mode is Flow Analysis, which offers analytic techniques and algorithms to model the behavior of steady-state networks and to study characteristics like routing, reachability and fault tolerance. Finally, the two previous kinds of simulation can be combined in the Hybrid Simulation, which provides traffic modeling to deeply study application flows. Since OPNET describes the characteristics of wireless transmission, such as signal propagation, interference, antenna directionality and node mobility, some RFID anti-collision protocols were tested through OPNET [88, 89].

- ***TOSSIM***

  TOSSIM[5] is a discrete event simulator built specifically to simulate the Berkeley MICA mote hardware platform running applications built on TinyOS wireless sensor networks. Instead of running a TinyOS application on motes, users can compile it in the TOSSIM framework which runs on a PC. In this way, the application can be tested in a controlled environment and debuggers and other development tools are available for developing TinyOS code. TOSSIM supports four key requirements: scalability, completeness, fidelity and bridging. TOSSIM allows the evaluation of a high level application, but it is not sufficient for low level protocol such as MAC. The research in [90] used TOSSIM simulator to demonstrate the advantage of their proposed filtering scheme.

The lack of a specific simulator for RFID networks has led to the development of a huge number of independent solutions for the evaluation of the reader interference. The implementation choices extremely differ, both in the operative system and in the programming language, ranging from simulators written in Perl 5 and running on Linux machines [91], to Java implementations on the Windows platform [92]. However, C is the most frequently adopted programming language. The general disadvantage of these simulators relies on the fact that they are not publicly available, therefore the simulation results cannot be repeated.

[4] http://www.opnet.com

[5] http://tinyos.stanford.edu/tinyos-wiki/index.php/TOSSIM

6.1.2 Modeling framework based on OMNeT++

OMNeT++[6] is a C++-based open-source simulator. Its main feature is the modularity: the basic components are called simple modules and they can be grouped together to form compound modules. Whereas the behavior of the modules is implemented in C++, the topology of the network is described in the NED (Network Description) language. The user writes a NED file to declare simple modules and to specify how they are connected to form compound modules. OMNeT++ is suitable for modeling wired and wireless networks, validating hardware architectures, and evaluating the performance of software systems and communication protocols. As a particular use, this simulator was employed to evaluate the reader-to-reader anti-collision protocols in [93]. Besides, OMNet++ offers an Eclipse-based IDE, a graphical runtime environment, and a host of other tools. In addition, there are extensions for real-time simulation, network emulation, alternative programming language (Java, C#), database integration, System C integration, and several other functions. It is free for academic and non-profit use. Moreover, it proved various platforms support on Linux, Mac OS X, other Unix-like systems and Windows (XP, Win2K, Vista, 7). Actually, OMNeT++ itself is not a simulator of anything concrete, but rather provides infrastructure and tools for writing simulations. This infrastructure includes six components architecture for simulation models:

- Simulation kernel library
- Compiler for the NED topology description language
- OMNeT++ IDE based on the Eclipse platform
- GUI for simulation execution, link into simulation executable (Tkenv)
- Command-line user interface for simulation execution (Cmdenv)
- Utilities (make file creation tool, etc)
- Documentation, sample simulators, etc

The OMNeT++ model is a collection of hierarchically nested modules. The top-level module is also called the System Module or Network. This module contains one or more sub-modules each of which could contain other sub-modules. The modules can be nested to any depth and hence it is possible to capture complex system models in OMNeT++. Modules are distinguished as being either simple or compound. Generally an OMNeT++ based simulator includes four types of files: module declaration files (*.ned), module behaviors definition files (C++ source

[6] http://www.omnetpp.org

codes), message declaration files (*.msg) and simulation configuration files (*.ini). The structure of a simulation model is also described in the NED language, which lets the user declare simple modules, connect and assemble them into compound modules.

A simple module is associated with a C++ file that supplies the desired behaviors that encapsulate algorithms. Simple modules form the lowest level of the module hierarchy. Users implement simple modules in C++ using the OMNeT++ simulation class library. Compound modules are aggregates of simple modules and are not directly associated with a C++ file that supplies behaviors.

Modules communicate by exchanging messages. Each message may be a complex data structure. Messages may be exchanged directly between simple modules (based on their unique ID) or via a series of gates and connections. Messages represent frames or packets in a computer network. The local simulation time advances when a module receives messages from another module or from itself. Self-messages are used by a module to schedule events at a later time.

Simulation executions are easily configured via initialization files. They track the events generated and ensure that messages are delivered to the right modules at the right time. There are several modeling framework based on OMNeT++ including but not limited to:

- **INET Framework[7]:** A frame work contains models for IP, TCP, UDP, PPP, Ethernet, MPLS with LDP and RSVP-TE signaling, and other protocols. It also includes support for mobile and wireless simulations. Besides, there are several extensions for INET framework like xMIPv6 [8], which provides an extensible Mobile IPv6 simulation with conformance to IETF standard RFC 3775; ReaSE [9], which is a realistic simulation environment; and some ad-hoc routing protocol implementations.

- **MiXiM[10]:** An OMNeT++ modeling framework created for mobile and fixed wireless networks (wireless sensor networks, body area networks, ad-hoc networks, vehicular networks, etc.). MiXiM concentrates on the lower layers of the protocol stack, and offers detailed models of radio wave propagation, interference estimation, radio transceiver power consumption and wireless MAC protocols. It is the merger of several OMNeT++ frameworks including mobility framework [94] by Technische Universitaet Berlin and positif framework [95] by Technische Universiteit Delft.

[7] http://inet.omnetpp.org/

[8] http://www.kn.e-technik.tu-dortmund.de/de/forschung/ausstattung/xmipv6.html

[9] https://i72projekte.tm.uka.de/trac/ReaSE

[10] http://mixim.sourceforge.net/

- **OverSim**[11]**:** A flexible overlay network simulation framework, developed at the Institute of Telematics, Karlsruhe Institute of Technology (KIT). It was designed to fulfill a number of requirements that have been partially neglected by existing peer-to-peer simulation frameworks. Up to now, it contains several models for structured (e.g. Chord, Kademlia, Pastry) and unstructured (e.g. GIA) P2P systems and overlay protocols. The peer-to-peer framework of OverSim can be partially adopted for the RFID systems without a central server.

- **Castalia**[12]**:** Castalia is a Wireless Sensor Network (WSN) simulator for early-phase algorithm/protocol testing built at the Networks and Pervasive Computing program of National ICT Australia. It supports realistic channel and radio models, and provides support for defining versatile physical processes. It also supports enhanced modeling of the sensing devices and other often-neglected attributes of a WSN such as node clock drift.

Compared with the other simulators, OMNeT++ is acquiring more and more reputations. NS-2 is perhaps the most widely used network simulator and has been extended to include some basic facilities to simulate Sensor Networks. However, NS-2 object-oriented design introduces too much interdependence between modules, which makes the addition of new models difficult [96]. This problem is not significant for simulators targeted at traditional networks, because the set of popular protocols that have been implemented is relatively small. For example, Ethernet is widely used for wired LAN, IEEE 802.11 for wireless LAN, TCP for reliable transmission over unreliable media. Nevertheless, the situation for sensor networks is quite different since there are no dominant protocols or algorithms and there will be unlikely be any, because a sensor network is often tailored for specific applications.

Besides, the design of wireless sensor networks requires us to simultaneously consider the effects of several factors such as energy efficiency, fault tolerance, quality of service demands, synchronization, scheduling strategies, system topology, communication and coordination protocols. OMNeT++ which is chosen in this thesis has been shown to address these problems much better [97].

6.1.3 Simulator requirements

In order to properly simulate the activity of the readers in an RFID system, a tool should provide the following features:

- the definition of the initial network topology;

[11] http://www.oversim.org/

[12] http://castalia.research.nicta.com.au/index.php/en/

- a reader movement strategy;
- support for the reader-to-reader anti-collision protocol.

6.1.3.1 Network topology generation

The first step in simulating RFID systems is to define the *network topology*, i.e., how the readers are deployed and linked in the network. Finding the optimal topology is a crucial point for the success of RFID applications, since it affects the performance in several ways:

- coverage: the interrogation range of the readers should cover all the monitored area, even with mobile tags;;
- fault tolerance: in case of a breakdown of a reader, the application reliability is assured by neighboring readers;
- network lifetime: the presence of redundant readers in a region increases uselessly the total energy consumption;
- interference: close readers can prevent each other to discern the tag response, reducing the system throughput.

For small systems, the best location of the readers can be easily predicted, based on the designer experience or on predefined mathematical models. For example in the supply chain management, a typical use of RFID systems, the readers can be placed in the proximity of the fixed points to be monitored, such as dock doors, interior doorways, conveyor belts. However, this approach is not applicable for more complex systems. The mathematical models may fail, because the real world peculiarities deviate from the theoretical case study. Moreover, the performance of the readers may differ from the factory specification, due to environment conditions, such as the material of the tagged object, the orientation of the tag and reader antennas, the speed of the tagged object, the interference, etc. In these cases, the best deployment cannot be found a priori, and an optimal solution is frequently obtained by following a random trial-and-error strategy. The low set up cost is another advantage of the random deployment method. Thus, an RFID simulator should provide different facilities for the reader deployment. Firstly, it should allow to manually specify the position of the readers, in order to accurately simulate small systems. Secondly, it should be possible to generate random deployments for more complex networks. If the simulator does not directly manage the random reader placement, then the topology should be imported from an external tool.

6.1.3.2 Mobility models

The design of RFID applications may require mobile readers. For example, the employers in a department store can be equipped with mobile readers in order to inventory the tagged items. A mobility model is required to simulate the movement of the readers. The choice of the mobility model depends on the application scenario. The following introduce the most common mobility models.

The random waypoint model [98] is widely used in simulating mobile ad hoc networks [28]. Each node randomly selects a destination and a speed. The value of the speed is uniformly chosen in the interval $(0,V_{max}]$, where V_{max} is a parameter of the model. The nodes travel toward the destination at the selected speed: once a node reaches its destination, it pauses for a time period, which is another constant parameter of the model. Afterwards, the node chooses a new destination and speed, and the process is repeated until the simulation ends.

In the random walk model, a variant of the random waypoint model, the nodes change their speed and direction at each time interval. The speed is uniformly chosen in the interval $(0,V_{max}]$, whereas the direction is uniformly randomly selected in the range $(0,2\pi]$. No pauses are taken when the direction changes. There exist several particular cases of the random walk model. In the constant velocity mobility model and in the constant acceleration mobility model, the nodes select random directions, but keep the same speed or acceleration indefinitely until new values are set again explicitly during the simulation. In the Chiangs random walk mobility model [99], the movements of a node in each direction (x and y) fall in one of three possible states: 0 if the node does not move in the considered direction, 1 if it moves forward and 2 if it moves backward. The probability of passing from state i to state j is given by the (i,j) element of the following state transition matrix:

$$\begin{pmatrix} 0 & 0.5 & 0.5 \\ 0.3 & 0.7 & 0 \\ 0.3 & 0 & 0.7 \end{pmatrix}. \tag{6.1}$$

The random direction model is another variant of the random waypoint model. Speed and direction are randomly chosen as usual; the way they change originates several slightly different flavors of the random direction model. In [100], new values for speed and direction are selected when the node reaches a border. In [101], the changes can occur anywhere in a walk area. In [102], a relative variation is applied to the current direction to calculate its new value. Pauses between the speed and direction changes are optional.

The reference point group mobility model [103] considers the network as built up by several groups. Each group has a logical center; the members of the group are uniformly distributed around the neighborhood of the group center. The logical center determines the groups mobility behavior, by choosing the direction and the speed. At each instant, every member of the group defines its direction and speed by randomly deviating the values of the logical center.

The freeway mobility model [104] emulates the metropolitan traffic. It is applied to road topology graphs, which represent a map with several freeways. Each freeway has lanes in both direction; the motion of the nodes is restricted to a lane of the freeway. The speed of a node ranges in the interval $[V_{min},V_{max}]$. At any interval of time, a random acceleration is applied to the previous speed value to compute the new value. In order to avoid collisions between nodes in the same lane, a minimum safety distance is maintained between the nodes, by reducing the speed of the follower.

The Manhattan mobility model [104] is similar to the freeway model. The difference concerns the topology of the maps, which here are composed of horizontal and vertical streets. The nodes have a certain probability to change direction at the intersections of the grid: they keep moving in the same direction with probability 0.5; they move right with probability 0.25 and left with probability 0.25.

In the Gauss-Markov model [105], the direction and speed of the nodes are correlated over time according to a Gauss-Markov stochastic process and they depend on previous movements. The degree of dependence is proportional to the parameter α, with $0 \leq \alpha \leq 1$. If $\alpha = 0$, the current movement does not depend on previous ones: this configuration corresponds to the random walk model. If $\alpha = 1$, the node keeps constant speed. If $0 < \alpha < 1$, the speed at time t is:

$$v(t) = \alpha \cdot v(t-1) + (1-\alpha) \cdot \mu + \sqrt{1-\alpha^2} \cdot x(t-1), \tag{6.2}$$

where μ is the asymptotic mean of $v(t)$ for $t \to \infty$; $x(t)$ is an independent normal distribution, with mean $\mu_x = 0$. An analogous formula holds for the direction.

The movement in systems including heterogeneous classes of mobile nodes, such as people and vehicles in ad hoc networks, can be described by a hierarchical mobility model. This model combines the relative movement of the ”child“ entity to the absolute movement of the ”parent“ entity. The movement of the parent and the relative movement of the child are described by one of the previous mobility models.

The mass mobility [106] model simulates the effect of the mass on the movement of a node: it considers the momentum of the node when it turns, without abrupt starts, stops and turns. The node starts moving along a straight line for a number of seconds that is randomly selected from a normal distribution. At the end, the node makes a turn: the angle of the turn and the new speed are randomly selected from other two normal distributions. The mean and standard deviation of the three normal distributions are parameters of the model.

Table 6.1. Mobility models implemented in general simulators

	NS-2	NS-3	OPNET	OMNeT++
random waypoint	yes	yes	yes	yes
random walk	no	yes	yes	no
constant velocity	no	yes	no	yes
constant acceleration	no	yes	no	no
Chiangs random walk	no	no	no	yes
random direction	no	yes	yes	no
reference point group	yes	no	no	no
freeway	yes	no	no	no
Manhattan	yes	no	no	no
Gauss-Markov	no	yes	no	yes
hierarchical	no	yes	no	no
mass mobility	no	no	no	yes

6.1.3.3 Support for anti-collision protocols

The reader interference can be mitigated by adopting a multiple access scheme, in order to share the channel among several readers. The most adopted channel access methods in RFID systems are Carrier Sense Multiple Access (CSMA) and Time Division Multiple Access (TDMA). Besides, Frequency Division Multiple Access (FDMA) and Code Division Multiple Access (CDMA) are also adopted, however, they usually require more hardware or software resources.

In a CSMA protocol, the reader checks if the channel is free before transmitting. To be more effective against reader interference, this solution is enhanced with collision avoidance (CSMA/CA), deferring the transmission if the channel is busy. In TDMA protocols, the readers transmit in different time slots. This solution can be easily implemented in RFID systems, but it requires a synchronization among the readers.

6.2 Reader-to-Reader Anti-collision Protocols

6.2.1 CSMA protocols

6.2.1.1 Listen before talk

Listen Before Talk[13] is a CSMA protocol specified by the European Telecommunications Standard Institute (ETSI). This regulation in intended for passive RFID

[13] ETSI EN 302 208-1 V1.4.1, Nov. 2011, http://www.etsi.org

systems operating in UHF band from 865 MHz to 868 MHz. All frequencies are spaced 600 kHz apart. Before querying tags, a reader is in listen mode: it selects a channel and it monitors it for at least 5 ms. If the reader detects a signal of at least -35 dBm, it gathers that the channel is busy and it selects another channel. Otherwise, the reader can query the tags: it switches to talk mode for at most 4 s.

6.2.1.2 Pulse

Pulse [107] is a CSMA/CA protocol in which readers regularly exchange signals, called beacons, on a control channel to manage their transmission on the data channel. The beacon interval is a parameter of the protocol. At the beginning, each reader stands in the Waiting state and listens the control channel. If no beacons are detected for a period equal to 3 beacon intervals, the reader moves to the Contend state. Here, it monitors the control channel for a backoff time, which is randomly selected as a multiple of the beacon interval. If the reader does not receives any beacon, it queries the nearby tags. At the end, it goes back to the Waiting state.

6.2.2 TDMA protocols

6.2.2.1 Distributed Color Selection (DCS)

DCS [91, 108] is a TDMA protocol: communication is organized in rounds, formed by max_colors time slots, where max_colors is a parameter of the protocol. Each time slot is matched to a color: collisions occur among neighbors with the same color. Initially each reader selects a random color: it tries to communicate at the corresponding times lot of every round. If no neighbors have the same color, the reader queries tags, otherwise a collision occurs and the reader has to choose a new color. Moreover, in the following round, it advises its neighbors to change their colors through a signal called kick.

6.2.2.2 Probabilistic DCS (PDCS)

PDCS[109, 110] is an enhancement of DCS. In order to prevent consecutive collisions among the same readers, the choice of the new color after a collision is optional and depends on a defined probability.

6.2.2.3 Colorwave

Colorwave [91, 108] is another improvement of DCS. In DCS, max_colors is fixed: a high value causes too many unused time slots, while a low value introduces more overhead. In Colorwave, each reader varies its own max_colors by estimating the percentage of successful communications, given by the ratio between the number of collision-free interrogations and the number of attempts. max_colors is decremented if the success ratio is higher than an upper threshold, it is incremented if the ratio is below a lower threshold.

6.2.2.4 Distributed Color No cooperative Selection (DCNS)

Distributed color no cooperative selection (DCNS) [111] is a high throughput solution for static RFID networks based on Colorwave. The performance of Colorwave is strongly influenced by the value of the thresholds. The network throughput increases by using a specific set of values, called the Killer configuration [112]. With this configuration, the readers adopt a selfish behavior and they try to gain as much resources as possible. DCNS is designed to fully exploit the Killer configuration. Moreover, it reduces the overhead in the collision resolution subroutine of Colorwave and it manages a dynamic priority queue. In this way, high priority readers reach a good performance even in densely deployed areas.

6.2.2.5 Anticollision for Mobile RFID (AC_MRFID)

AC_MRFID [92] is a protocol based on DCS: similarly to Colorwave, it allows the readers to dynamically change their own max_colors. After colliding, a reader communicates with its neighbors in order to count the number of them inside its interrogation range. Then, it estimates the number of neighbors, according to the ratio between the interrogation area and the interference area. The new max colors is set to the estimated number of neighbors incremented by 1.

6.2.2.6 Neighbor Friendly Reader Anticollision (NFRA)

In NFRA [113], a polling server synchronizes the communication by sending an arrangement command (AC) and an ordering command (OC) to announce the beginning of a new round and of a new timeslot, respectively. After receiving an AC, each reader randomly selects a time slot. When the reader receives the corresponding OC, it sends a beacon to its neighbors. If two readers mutually exchange a beacon, they cannot communicate in the current round. Otherwise the reader sends an overriding frame and starts to query tags.

6.2.2.7 NFRA++

NFRA++ [114] exploits two mechanisms to improve the fairness of NFRA without penalizing the throughput. Firstly, it manages a dynamic priority among readers, according to the time elapsed from their request of transmission. Readers with many neighbors, which are likely to have the longest waiting time, reach a higher performance. Secondly, another beacon is exchanged to enhance the detection of reader collisions, with a consequent throughput improvement.

6.2.2.8 Geometric Distribution Reader Anti-collision (GDRA)

GDRA [115] increases the throughput of NFRA by enhancing the algorithm for managing the collisions. Readers select the time slot according to the *Sift* geometric distribution function, instead of the uniform distribution function used in NFRA. The *Sift* function minimizes the probability of collision among neighbors. Moreover, the implementation of GDRA is simplified with respect to NFRA.

6.2.2.9 Hierarchical Q-learning (HiQ)

Hierarchical Q-learning protocol intends to find dynamic solutions to the reader collision problem by mapping collision patterns among readers. It involves a hierarchical structure composed of three levels. The RFID readers, which represent the lowest level, require channel resources to the higher level (e.g., a computer in charge of multiple readers). The elements of the second level require resources to the highest level (e.g., a central server), and distribute them to the readers. This system requires a communication system for the resources management. The main shortcoming of this approach is that readers need to handle a huge amount of data; besides, the final outcome depends on the quality of the neural network training.

6.3 A Novel Simulator for Reader-to-Reader Collisions

6.3.1 Overview

In this section, the proposed simulator for the reader-to-reader collision problem is presented. The main goal of the simulator is to simulate the realistic scenarios and existing anti-collision protocols under the single interference model and additive interference model. It can provide a reference to compare, test and evaluate the anti-collision protocols according to both the single interference model and the additive model. All the modules in the simulator are highly tunable and is easy to build the specific protocols or application behaviors by instantiating the predefined abstract classes. The simulator is based on the OMNeT++ platform and it provides the following features:

- Modular: it is functional partitioned consisting of independent modules and each module has well defined interfaces and templates;

- Support for both single interference models and additive interference models: the propagation mechanism provides two models to detect interrogation collisions, which can be specified by configuration parameters; besides, it also provides interfaces to implement new propagation models;
- Support for the main anti-collision protocols in the state of art: both distributed protocols and centralized protocols have been developed such as DCS, Colorwave, NFRA, PDCS.
- The interrogation scheduler: the performance of anti-collision protocols can be tested under different interrogation scheduling scenarios defined by the user from the application layer;
- Reservation for Mobility Modules: up to now it is used mainly to test protocols in static RFID systems. But it provides a mobility module interface to update the dynamic location of RFID readers.

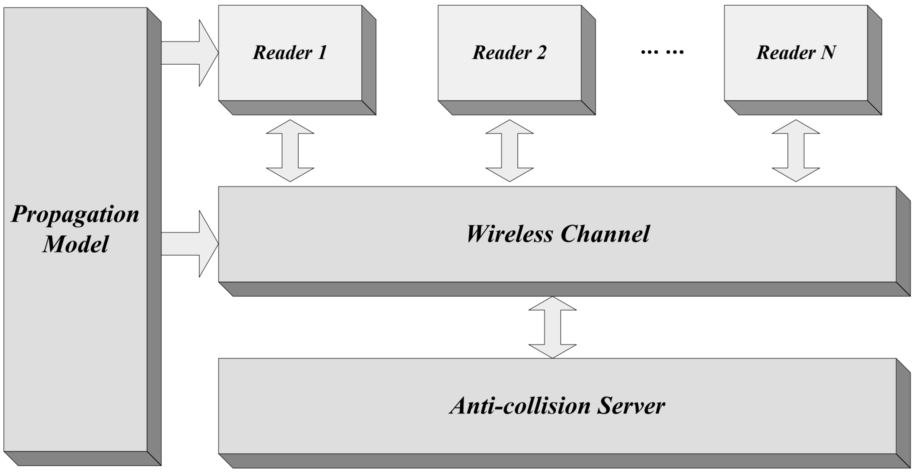


Figure 6.1. The communication overview in the RFID simulator

The design structure of the simulator is based on Castalia, but it is specially redesigned considering the characteristics of RFID system including the different propagation models and anti-collision mechanisms. Figure 6.1 shows the design overview of the RFID simulator. The RFID *readers* do not communicate or interrogate directly but through the *wireless channel module*. Whenever a reader wants to interrogate the tags, the wireless channel module computes the interference to the other readers according to the adopted propagation model. During the interrogation, each reader receives interference signals by other readers and the success of the interrogation is determined according to the *propagation model*. Apart from the interrogation, RFID readers in the simulators can also communicate with each other in a different frequency band in order to exchange the control signals in some anti-collision protocols. Besides, there is an optional module called *anti-collision server*, which is used only for the centralized protocols. The server can communicate with all the readers in the deployment field, send or receive control messages. Besides, since one of the main objectives of the simulator is to compare the performance of single interference model and additive interference model, a propagation module is also added. Each module can access the propagation module to acquire the information about the received interference and reader-to-reader collision existence.

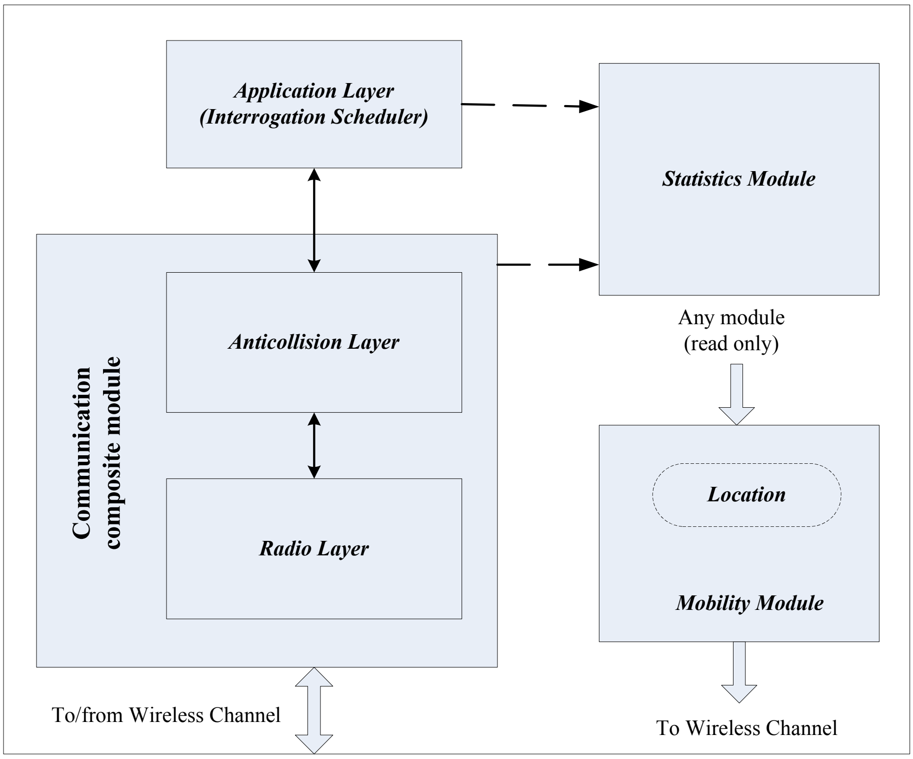


Figure 6.2. The node structure for each RFID reader

Figure 6.2 shows the structure for a reader in the RFID simulator, where the solid arrows means message passing and the dashed ones means function calling. It is a composite module in OMNeT++. The *application layer* (or called *interrogation scheduler*) simulates how the RFID system based application schedules the reader interrogations. It is usually application specific and can also be used to generate test cases for the anti-collision protocols. Whenever an application needs to interrogate the information on the tags, it sends request to the communication layer and the communication module determines the exact interrogation time with or without anti-collision algorithms. The *anti-collision layer* offers support for building the particular protocols and it propagates signals to the *radio layer*. The *mobility module* stores the current location of the RFID reader and updates it in real time with the wireless channel module. The *statistics module* collects the related information in the simulation, by which each module can write or update the useful data.

6.3.2 Modules

Each module of the simulator is defined in a OMNeT++ NED language [14] and related with a C++ code. Besides, some particular module is implemented as a set of function calling, such as the propagation module and the statistics module. The behavior of the module is defined by implementing the following functions:

```
virtual void initialize(int stage);
virtual void handleMessage(cMessage *msg);
virtual void finish();
```

where *initialize()* initializes all the variables and predefined information; *handleMessage(cMessage *msg)* implements the protocols to handle the process of receiving and sending packets, which defines how the node react on different message types it receives; *finish()* calls the statistic module at the end of the simulation and record all the useful information.

6.3.2.1 Propagation module

The propagation module provides the mathematical way to calculate the propagation loss and the propagation delay. Besides, it provides the mechanism to detect collisions. The main functions in the interface have been defined as the following:

```
virtual double calculatePower(double initial_output,
    ReaderPosition_type src, ReaderPosition_type dest);
virtual bool existCollision(double initial_output, double
    interference);
virtual outputPower_type getOutputPower(int id);
virtual double getPropagationDelay(double initial_output,
    ReaderPosition_type src, ReaderPosition_type dest);
virtual double getDrr(int id);
virtual double getDrrPower(int id);
```

where *calculatePower()* and *getPropagationDelay()* return the final signal power of the interference and the arriving delay from the source reader to the destination reader after the propagation loss, respectively; *existCollision()* determines whether there is a collision considering the output power and the total received interference; other functions relate to the simple models that detect a collision by considering

[14] http://omnetpp.org/doc/omnetpp/manual/usman.html

only the relative distance. The typical two interference models described in Chapter.4 including the unit disk graph model and the particular additive interference model have been implemented in the basic version, but all the other models can be user defined. The choice of the model can be simply configured by modifying the corresponding field as

```
SystemNetwork.PropagationModel_type = ”udgModel”
```

Furthermore, the configuration file can also specify all the related parameters such as the path loss exponent, the antenna gains, the SINR value, and so on.

6.3.2.2 Wireless channel module

The wireless channel module deploys the readers at the beginning of the simulation, the main functions of the module also include

- provides a medium for the readers to interfere and communicate with each other;
- provides a medium for the communication between the readers and the optional servers;
- updates the signal power based on the propagation model;
- dynamically updates the location status of each reader in a mobile RFID system.

The simulator provides the following types of network deployment: deterministic deployments, matrix deployments, random deployments and a hybrid combination of the above. In the deterministic deployment, the readers are manually positioned as specified in a configuration file. In the matrix disposition, readers are located at regular distance, in order to homogeneously cover all the deployment area. The position of the readers in random deployments can be freely chosen according to a uniform distribution or other distribution. Finally, a hybrid combination of deterministic and random deployments can be specified: for example, some readers are placed at specific positions, others are located according to a matrix scheme and the remainders are randomly distributed. Besides, it is always possible to repeat a simulation with the same placement.

As a medium for the communication, the wireless channel module determines which readers in the system can receive the interfering signals when a source reader is trying to interrogate. Considering the characteristics of both the single interference model and the additive interference model, the wireless channel module provides two modes to determine the receivers. The first one determines the receivers according to a power threshold, i.e., calculates all the possible receiving power for the potential receivers according to the propagation model; if the result power is higher than the carrier sense level, it marks the corresponding destinations and sends the data packets. This mode is used for broadcasting the reader-to-reader interference during the interrogation activity. The second one is based on the distance threshold, i.e., all the readers within the threshold distance to the source reader will receive the signals. This mode is used mainly for the delivery of the control packet in order to avoid computation costs.

6.3.2.3 Application module

The application layer is used to simulate the interrogation request according to the application requirements. Besides, it can also be used as a test case generator. For the use of application simulator, since it is application specific, it is mainly instantiated by the user. The user can plan the interrogation by determining all the interrogation time, or adopt cyclic interrogation schedulers. For the use of test cases generator, currently three mechanisms have been implemented. In the *probabilistic frame* interrogation, the lifetime of the RFID system is divided into frames with a fixed length. At the beginning of each frame, each reader tries to interrogate with respect to a predefined probability. In the *total number specified* interrogations, a fixed number of interrogations are planned. Each interrogation can start only when the previous interrogation has been performed successfully. In the *Poisson process* mode, the time interval between each pair of consecutive interrogations has an exponential distribution with parameter λ and each of these inter-arrival times is assumed to be independent of other inter-arrival times.

6.3.2.4 Anti-collision module

The anti-collision module in the simulator implements the behaviors of the self-configuration algorithms. Up to now, the proposed simulator provides support for DCS [108], PDCS [109], Colorwave [108] and NFRA [113]. Although each protocol adopts different anti-collision algorithms, the basic requirements for a protocol are:

- the ability to handle all the interrogation requests from the upper layer;
- the ability to response to the failure of the interrogation;
- the ability to schedule the interrogation activity efficiently.

Figure 6.3 illustrates the general process of received packets in the anti-collision protocols. Each packet is assigned with a field *pktKind* that specifies the kind of the messages. The packets are divided into two classes: self timer messages, which are used to implement timers and schedule the packet sending with a certain delay; data packets, which contain useful information that can determine the behavior of the anti-collision protocols. In order to react correctly, the protocols should build reactions for the packets from both the upper layer (i.e., the application layer) and the lower layer (i.e., the radio layer).

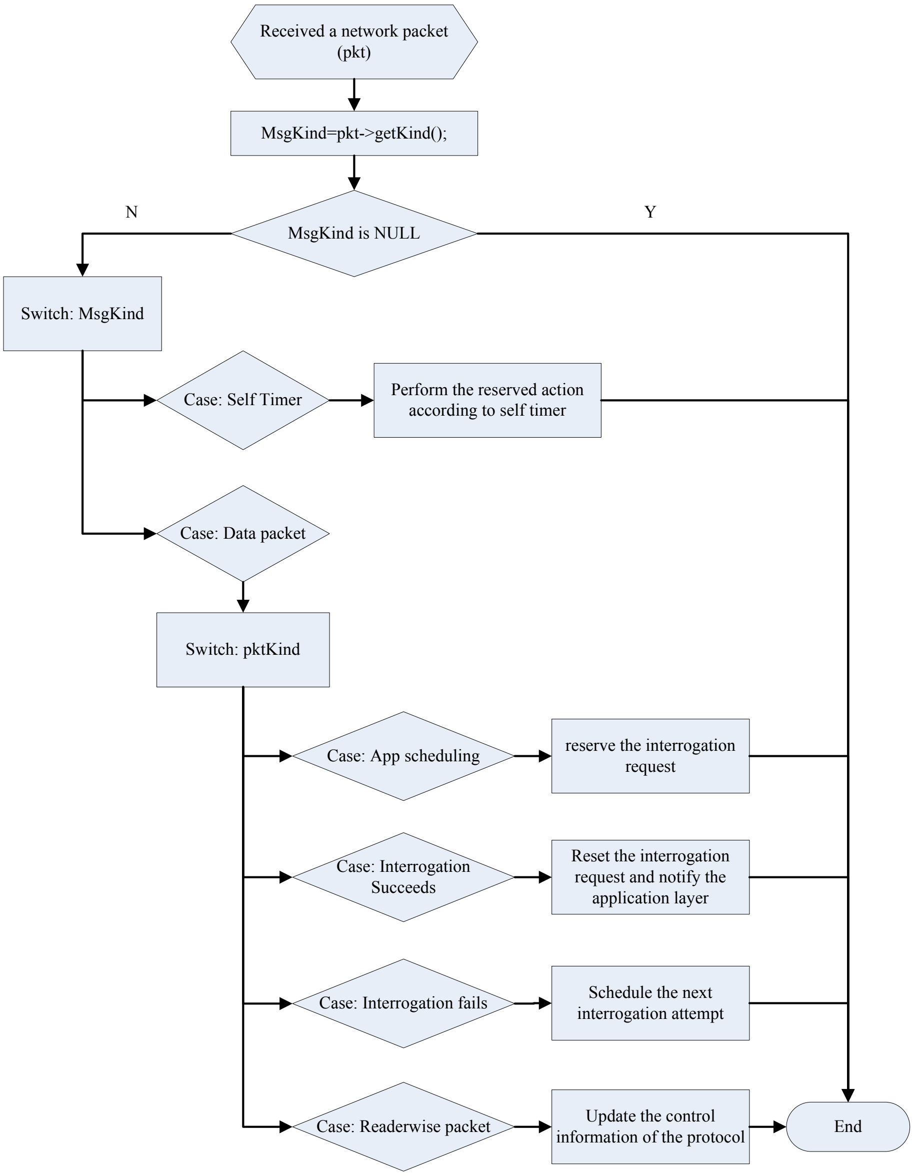

Received a network packet (pkt)
MsgKind=pkt->getKind();
N
MsgKind is NULL
Y
Switch: MsgKind
Case: Self Timer
Perform the reserved action according to self timer
Case: Data packet
Switch: pktKind
Case: App scheduling
reserve the interrogation request
Case: Interrogation Succeeds
Reset the interrogation request and notify the application layer
Case: Interrogation fails
Schedule the next interrogation attempt
Case: Readerwise packet
Update the control information of the protocol
End

Figure 6.3. The general message handling of the anti-collision layer

6.3.2.5 Radio module

The radio layer is a bridge between the anti-collision layer and the wireless channel. Its main function is to detect the reader-to-reader collisions based on the total received interference and the output power.

Firstly, it handles the interrogation requests from the anti-collision layer. When the radio layer receives a request of interrogation, it generates an interrogation packet with an assigned output power. Afterwards, it sends it to the wireless channel which will broadcast the interferences. At the same time with the beginning of interrogation, a timeout interval is set up. If the received interference does not generate a collision, it marks the interrogation as a successful one; otherwise, the interrogation fails and it notifies the upper layer.

Secondly, the radio layer evolves to a bypass layer when the upper layer wants to send readerwise packets. In this case, it just encapsulates the packet received from the anti-collision layer, assigns a higher output power or a communication radius and sends it out. When a readerwise packet is received, it decapsulates the packet and sends it to the anti-collision layer.

Finally, it handles the interrogation interference received from the other readers. This is where the reader-to-reader collision occurs: when a reader is interrogating, it marks a flag as true and then it begins to accumulate the received power of other readers' interrogation packets. Each time it receives a simultaneous interrogation, it accumulates the power and checks whether the total power exceeds the predefined threshold. If yes, the interrogation fails. If no further interference is received until the timeout period ends, a successful interrogation is returned.

6.3.2.6 Server module

The server module is used only for the centralized protocols that require a global server to schedule the interrogations. The central server collects tag's identifications, sends instructions to readers and exchange information from them. The generic module defines the basic server packet as follows:

```
packet GenericServerPacket {
    bool broadcast;
    int pktKind;
    int destlist[];
}
```

When the *broadcast* flag is true, the packet from the server is sent to all the readers in the RFID system. Otherwise, the packet is received by the readers which are contained in the vector *destlist[]*. Users can define particular packets by extending the basic class of the generic packet.

Up to now, only the NFRA server for the NFRA protocol [113] has been implemented. In NFRA protocol, the polling server is designated to divide the time into identification rounds. Every round begins with an arrangement command (AC), containing a random number from 1 to MN, broadcasted to all the readers. The readers that receive the AC generate their own random number. The server then issues an ordering command (OC), the readers then compare their random numbers with the value in the OC. If both values are same, the readers exchange beacons to determine whether a collision occurs or not. If a reader does not detect any collisions, it send overriding frame (OF) to its neighbors. In this case, the AC command and the OC command are generated in the NFRA server and are broadcasted to all the readers in the deployment. On the other hand, the OF packet is transmitted between the readers as readerwise communication data.

6.4 Evaluation Scenarios

In order to test the simulator, the comparison between single and additive interference models is performed by taking into account the unit disk graph model and the complete weighted graph model as reference of the two categories. Despite the use of an anti-collision protocol [116], the interrogation activity of an RFID reader depends on the application requirements. In order to take into consideration different behaviors, three scenarios have been considered for the performance simulation: probabilistic interrogation, slotted interrogation and the DCS protocol.

6.4.1 Probabilistic interrogation

In this hypothesis, a certain number of interrogation points is assumed. At each interrogation point, every reader tries to interrogate the tag with probability p. For each reader, the activity at one interrogation point is independent of other interrogation points. The sequence of an RFID reader's interrogation activity is a Bernoulli process, i.e., a discrete-time stochastic process, where at each interrogation point the reader interrogates with probability p. Compared with Poisson process, this scenario assumes discrete interrogation points where each reader are supposed to interrogate at the same time.

This scenario models an application that needs to randomly query the real-time information stored in the tags and the operation is memoryless, i.e., past interrogations provide no information about future interrogations. The probability p reflects the interrogation frequency of the RFID system. The number of successful interrogations is expected to change according to different interrogation probabilities and network densities.

6.4.2 Slotted interrogation

In the slotted interrogation scenario, the lifetime of the RFID system is divided into frames with a fixed length and each frame is further split into time slots. Initially, each reader picks one time slot in the frame as its interrogation slot. A reader interrogates the tags only in its interrogation slot. If the interrogation fails, the reader randomly selects a new time slot to be used in the next frame. If the number of time slots is large enough, after a period of self adjustment, the RFID system will finally reach a stable state in which all the readers are able to identify tags without any interference from other readers. However, the number of interrogation attempts in a fixed time period is expected to decrease as the number of time slots grows.

In anti-collision protocols, the *Time Division Multiple Access* (TDMA) mechanism [92] is one of the most adopted channel access methods [91]. Slotted mechanism is a distributed mechanism and does not require communication between readers. With slotted mechanisms, the nodes in the network operate at different time slots and this reduces the occurrence of reader-to-reader collisions. However, the number of time slots per frame (T_s) could critically influence the performance. Although the probability of collisions decreases when T_s grows, the response time to an interrogation request also increases and consequently less interrogations can be performed in a fixed period, i.e., the throughput reduces. Simulating the slotted interrogation scenario allows to find a tradeoff between the number of collisions and throughput.

6.4.3 The DCS protocol

The Distributed Color Selection (DCS) [91] protocol is one of the most popular and typical anti-collision protocols in the state-of-art. It is a distribute protocol based on the TDMA mechanism. DCS models the reader network using the unit disk graph model. The main idea is to use a certain number of colors ($maxColors$) to color all the readers in the system so that each reader has the smallest possible number of *direct neighbors* with the same color. Direct neighbors are defined as the neighbor nodes that are located within the direct collision range. Initially, each reader selects its own color ($currentColor_i$) and interrogates only in the corresponding time slot. Once a reader detects an interrogation failure, it randomly changes to a new color and broadcasts it to all the direct neighbors: the broadcast message is referred to as a *kick*. Besides, whenever a reader receives a kick message, it changes its own color to a new color that is different from the color stating by the received message. The main subroutines of DCS are described in the following:

- *Initialization phase*: all the readers in the RFID system select the initial color to be active;

```
    for all RFID reader $R_i \in R$ do
    timeslotID$_i$=-1;
    currentColor$_i$=intuniform(0,maxColors-1);
  end for
```

- *Interrogation request from the upper layer*: R_i receives the interrogation request from the application layer;

```
  if interrogation request received then
    interReserved=true;
  end if
```

- *Timeslot triggered*: each R_i updates the slot ID and determines whether to interrogate at the current time slot;

```
  timeslotID$_i$++;
  if ($timeslotID_i$ % $maxColors$) == $currentColor_i$ and interReserved then
    $R_i$ performs the interrogation;
  end if
```

- *Interrogation succeeds*: R_i receives the correct information from the tag;

```
  if backscattered information is received correctly then
    interReserved=false;
  end if
```

- *Interrogation fails*: R_i cannot get correct information from the current interrogation;

```
  if $R_i$ experiences a collision then
    $currentColor_i$=intuniform(0,maxColors-1);
    Sends kick packets stating the new $currentColor_i$;
  end if
```

- *Kick resolution*: R_i receives the *kick* message from other readers;

```
  if kick message received stating the color $newColor$ then
    while $currentColor_i$ == $newColor$ and $maxColors > 2$ do
      $currentColor_i$= intuniform(0,maxColors-1);
    end while
  end if
```

Differently from the scenario of slotted interrogation, DCS is a mature anti-collision protocol and it does not change the time slot pure randomly, instead, it selects the new color according to the information of the neighbors' states. Since the kernel design is based on the unit disk graph model which only considers the direct neighbors, the performance of the DCS in real simulations will probably be worse than the theoretical estimation caused by the additive collisions that have been ignored. Therefore, the DCS protocols will be implemented under both of the two models in order to observe the difference.

6.5 Experimental Results

Table 6.2. Evaluation parameters

Parameter	Symbol	Value
Path loss exponent	α	2
SINR Threshold	Γ	10
Reader antenna gain	G_r	6 dBi
Tag antenna gain	G_t	1 dBi
Tag's power reflection coefficient	R_t	3/4
Reader's transmit power	P_r	30 dBm
Model coefficient	K_0	$1/G_r^2$
Interrogation range	d	5 m
Noise power	N_0	0

In the simulation, RFID readers are deployed randomly and each reader interrogates and interferes each other just like the real RFID systems. Besides, the evaluation considers a homogeneous RFID network where each reader is identical with the same antenna gains. The values of the parameters adopted in the system are shown in Table 6.2 [8]. The threshold distance D_{th} of the unit disk graph model is given by equation (4.28): substituting the values in Table 6.2 into equation (4.28), it results $D_{th} = 288.675\ m$. This distance is used to determine whether two readers are neighbors in the unit disk graph model.

In the simulation of the RFID system, the readers are deployed on a 1,000 $m \times$ 1,000 m field. The number of readers varies from 10 to 60 in order to observe the influence of the deployment density and each simulation is repeated 100 times in order to reduce the effect of randomness. The following metrics are adopted to compare the interference models:

- Ratio of successful interrogations: the ratio between the number of successful interrogations and the total number of interrogation attempts;
- Throughput: the total number of successful interrogations during the simulation;
- Percentage of additive collisions in the additive interference model: the ratio between the number of collisions caused by more than one readers and the total number of reader-to-reader collisions.

6.5.1 Probabilistic interrogation

This section presents the performance of the two models in the probabilistic interrogation scenario where each reader interrogates with a probability p. In this scenario, 2,000 interrogation points are scheduled and the values of p vary from 0.1 to 1.

6.5.1.1 Ratio of successful interrogations

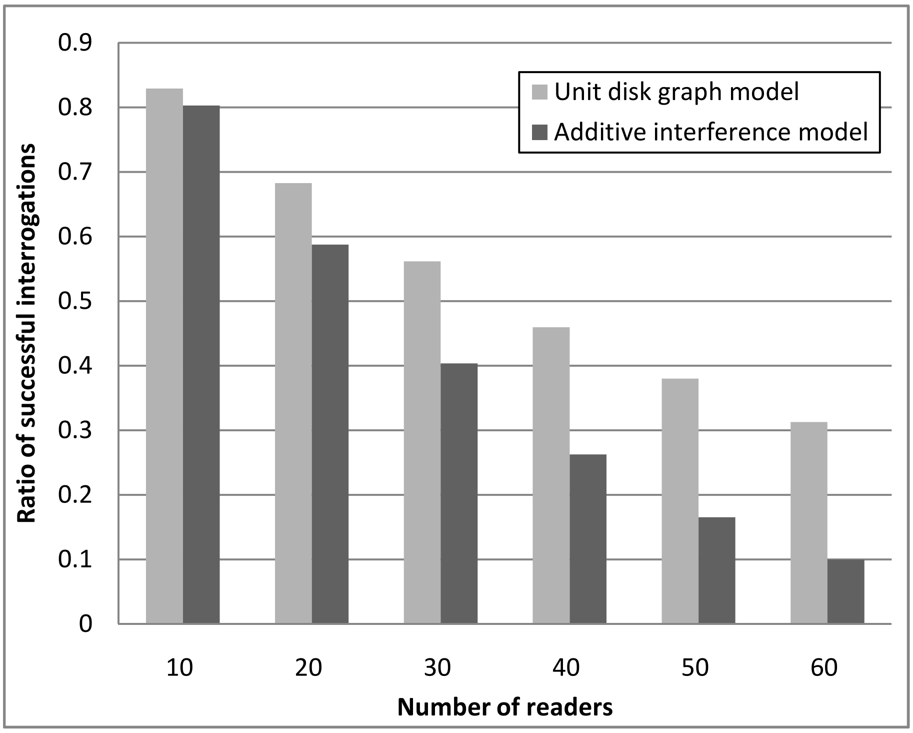


Figure 6.4. Ratio of successful interrogations, with interrogation probability of 0.1

Figure 6.4 and Figure 6.5 compare the ratio of successful interrogations in the two models, when the interrogation probability is set to 0.1 and 0.4. As the density of readers increases, the ratio of successful interrogations for both the additive interference model and the unit disk graph model decreases because the interrogations of a reader influences more neighbor nodes. The results in Figure 6.5 are lower than the corresponding results in Figure 6.4, since the probability that readers interrogate simultaneously increases as p grows.

The successful ratio in the unit disk graph model is generally higher than the one in the additive interference model under the same environment. It means that the additive interference model captures more reader-to-reader collisions than the unit disk graph model. The gap between the two models increases as the number

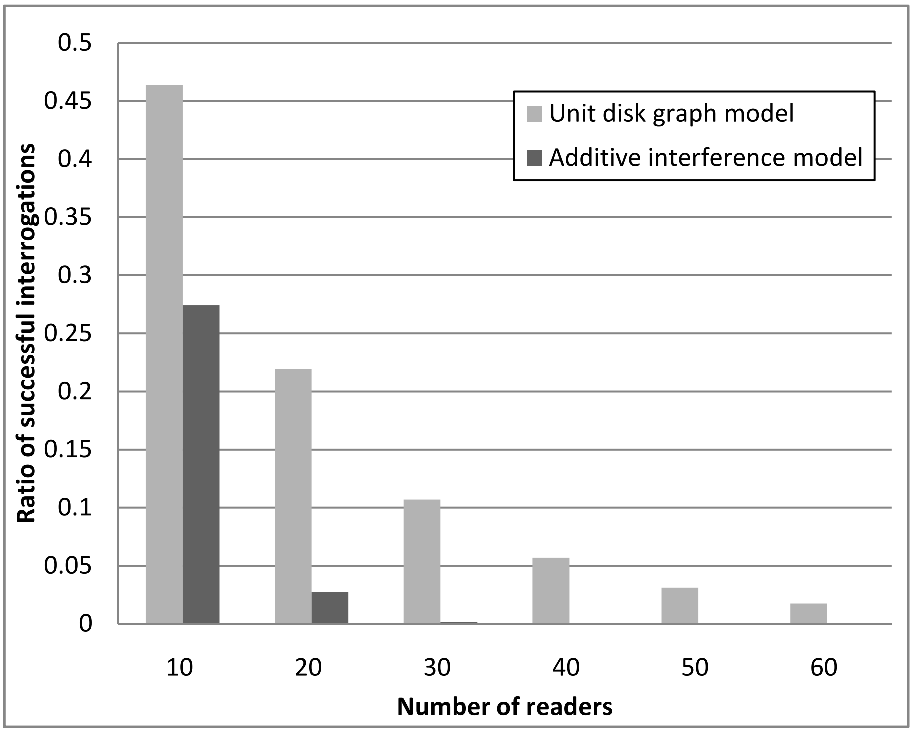


Figure 6.5. Ratio of successful interrogations, with interrogation probability of 0.4

of readers grows. For example, in Figure 6.4, the difference between the two ratios is around 0.02 with 10 readers. However, as the number of readers grows to 60, the difference increase to 0.2. This gap grows in a larger way as the interrogation probability increases from 0.1 to 0.4.

In Figure 6.5, the ratio in the additive interference model is close to 0 when there are more than 20 readers, which means that a successful interrogation is not possible. This is close to the behavior of a real RFID system. On the contrary, the ratio of successful interrogations under the unit disk graph model range from 0.12 to 0.02 which means that this model does not cover correctly the real behavior.

6.5.1.2 Throughput

Figure 6.6 shows the throughput of the probabilistic interrogation in the unit disk graph model. When the number of readers ranges from 10 to 30, the throughput first increases until it reaches a peak point and then it decreases. Besides, the peak point depends on the interrogation probability. For example, the highest throughput with 10 readers appears at $p = 0.5$; on the other hand, the throughput with 20 and 30 readers reaches the peak value at $p = 0.3$ and $p = 0.2$, respectively. When the number of readers is more than 30, the number of successful interrogations decreases

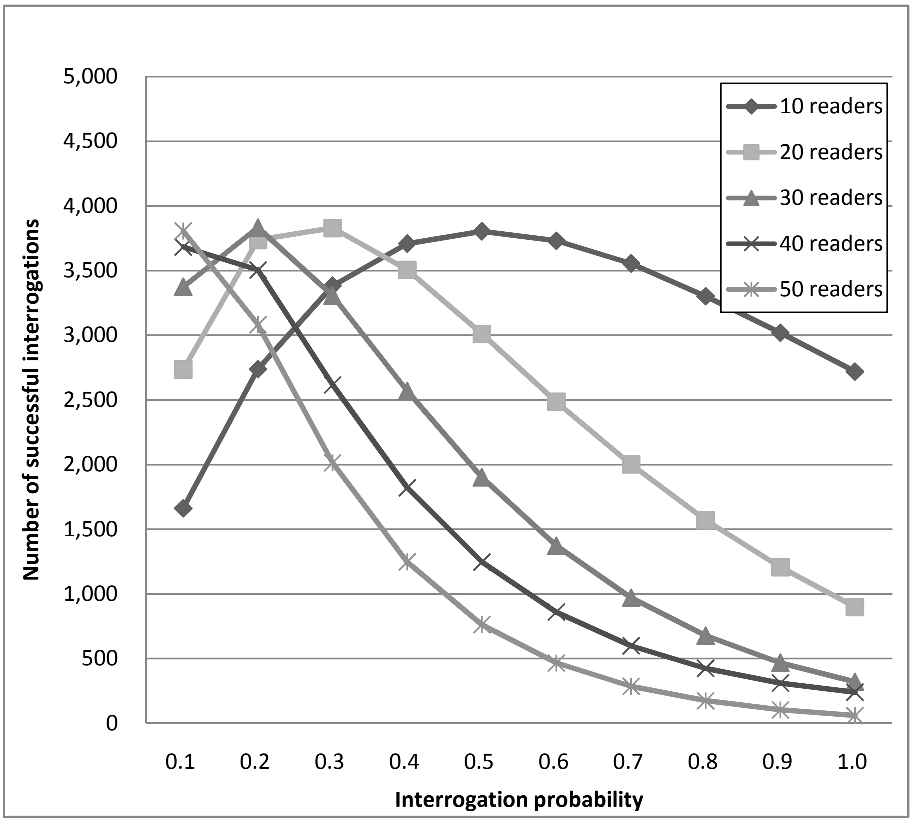


Figure 6.6. Number of successful interrogations for the unit disk graph model under the probabilistic interrogation scenario

with respect to the growth of p.

When $p = 0.1$, the throughput increases as the number of readers grows, because the total number of interrogation attempts increases. However, when the interrogation probability increases over 0.4, the throughput decreases as the number of readers raises. The reason is that the number of reader-to-reader collision grows and the increment of interrogation failure are greater than the growth of interrogation attempts.

The number of successful interrogations for additive interference model is shown in Figure 6.7. Differently from the unit disk graph model, only when the number of readers is 10, the ratio first increases to the peak point at $p = 0.3$ and then it decreases to 0. When $p = 0.1$, the best throughput is for 30 readers and the worst throughput appears when the number of readers is 10. When $p \geq 0.2$, the throughput decreases as the number of readers raises. It can be also observed that the number of successful interrogations becomes 0 during some simulations, which is in accordance with the successful probability shown in Figure 6.4 and Figure 6.5.

Observing the two graphs, it is possible to state that not only a comparative analysis of reader protocols based on the single interference model would provide inconsistent results, but even a selection of the parameters based on this model would decrease the throughput. Table 6.3 shows the best throughput for the two interference models and the corresponding interrogation probability. The loss in the best throughput from unit disk graph model to the additive interference model are also illustrated.

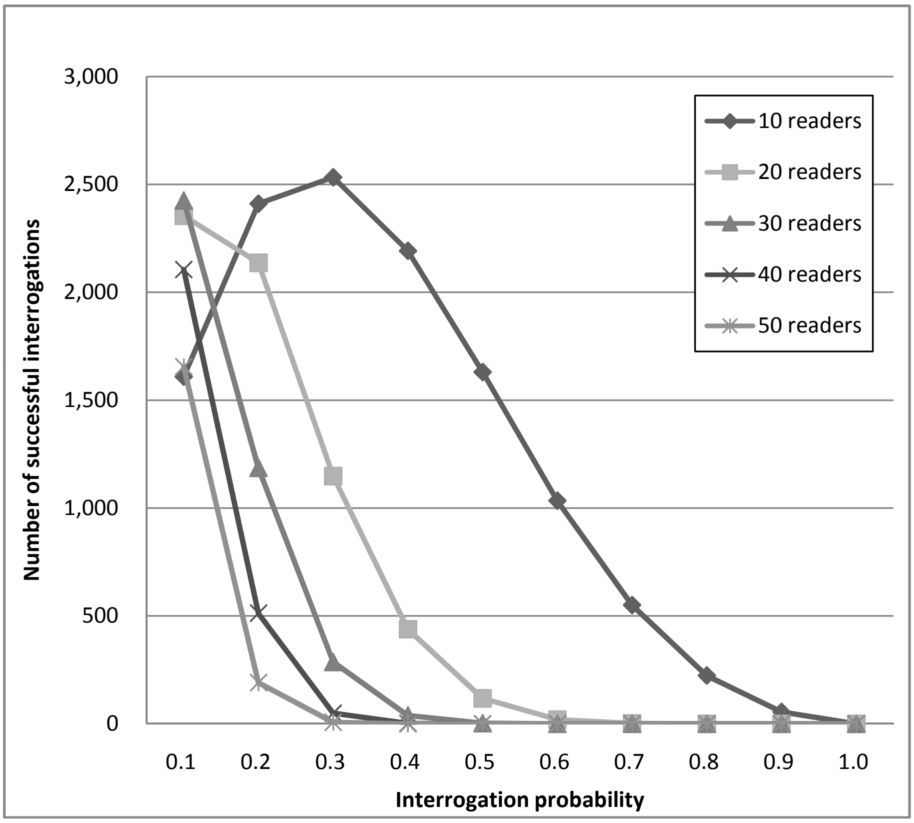


Figure 6.7. Number of successful interrogations for the additive interference model under the probabilistic interrogation scenario

Table 6.3. Analysis of the best throughput for the probabilistic interrogation

Readers	Unit disk graph model		Additive interference model		Loss
	Probability	Throughput	Probability	Throughput	
10	0.49	3803.56	0.27	2553.69	32.8%
20	0.26	3863.91	0.13	2471.03	36.0%
30	0.18	3850.09	0.09	2449.89	36.4%
40	0.14	3812.84	0.07	2418.40	36.6%
50	0.11	3811.80	0.05	2411.70	36.7%

6.5.1.3 Percentage of additive collisions

Figure 6.8 shows the percentage of additive collisions caused by additive interferences. The largest percentage of additive collisions is around 22% no matter how many readers there are. The peak points appear on different values of p. When $p > 0.4$, the percentage of additive collisions goes down along with the growth of deployment density because more readers are within their interference range when the number of readers raises. When the number of readers ranges from 10 to 30, the percentage first increases then decreases along with the growth of the interrogation probability. In the others cases with 40 and 50 readers, the percentage of additive collisions goes down monotonically.

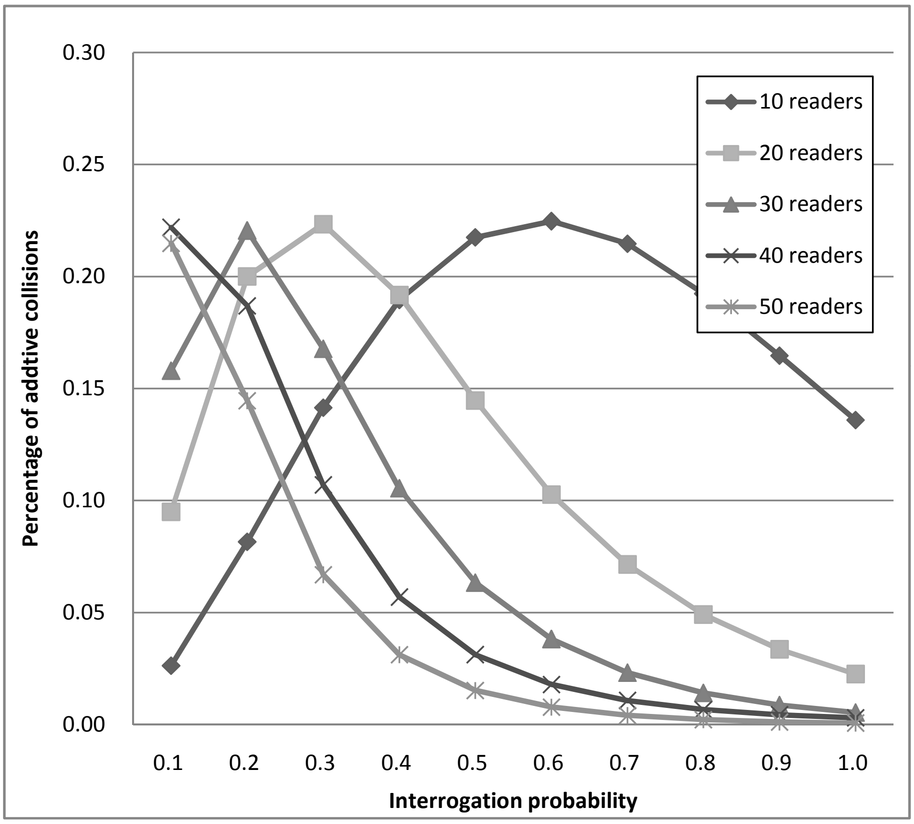


Figure 6.8. Percentage of additive collisions for the additive interference model under the probabilistic interrogation scenario

6.5.2 Slotted interrogation

This section investigates how the number of successful interrogations changes in the two interference models when the system operates under a slotted mechanism. In this scenario, the size of the time slot is set to be 0.5 s and the simulation lasts for 1,000 s. When the number of time slots per each frame increases, the number of idle slots grows and consequently the interrogation attempts during a fixed time falls down.

6.5.2.1 Ratio of successful interrogations

Figure 6.9 illustrates the ratio of successful interrogations for the two interference models when there are 5 time slots per each frame. The ratio for both the two interference models falls down as the number of readers increases. The difference between the two models first increases from 0.10 (when 10 readers exist) to 0.19 (when 30 readers exist), then it falls down to 0.09 (when 60 readers exist). When there are more than 50 readers, 5 time slots are not enough to avoid any collision during the additive interference models. When the number of time slots grows to 10 as shown in Figure 6.10, the ratio of successful interrogations improves a lot with respect to the results in Figure 6.9. For example, in the scenario with 10 readers, the ratio grows from 0.55 to 0.80 for the additive interference model and from 0.65 to 0.83 for the unit disk graph model. The ratio in additive interference model becomes larger than the ratio in unit disk graph model when the number of time slots changes

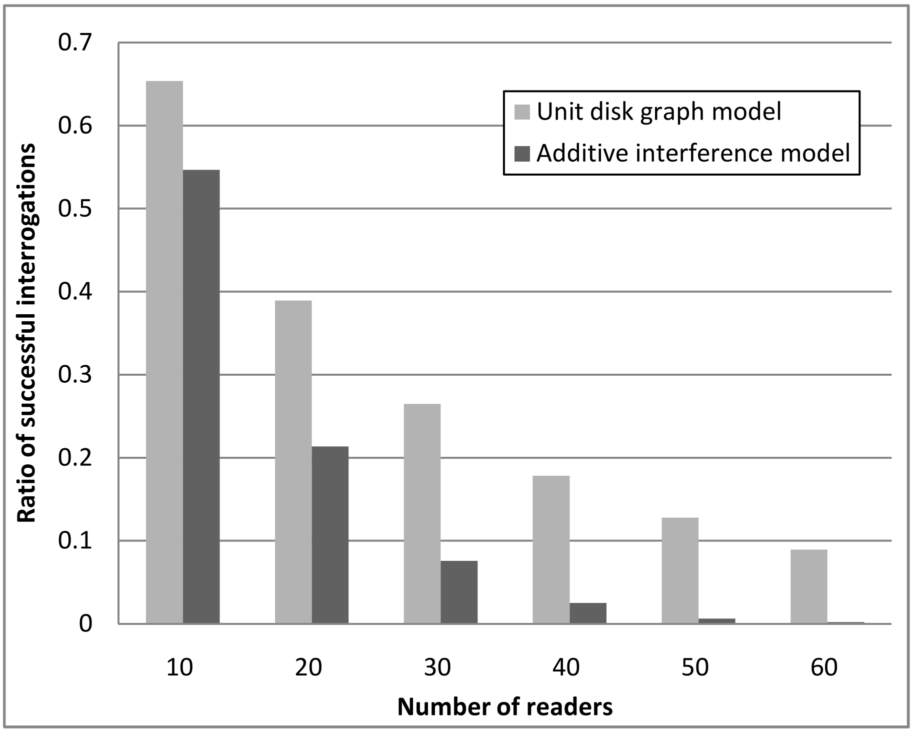


Figure 6.9. Ratio of successful interrogations, with 5 time slots per frame

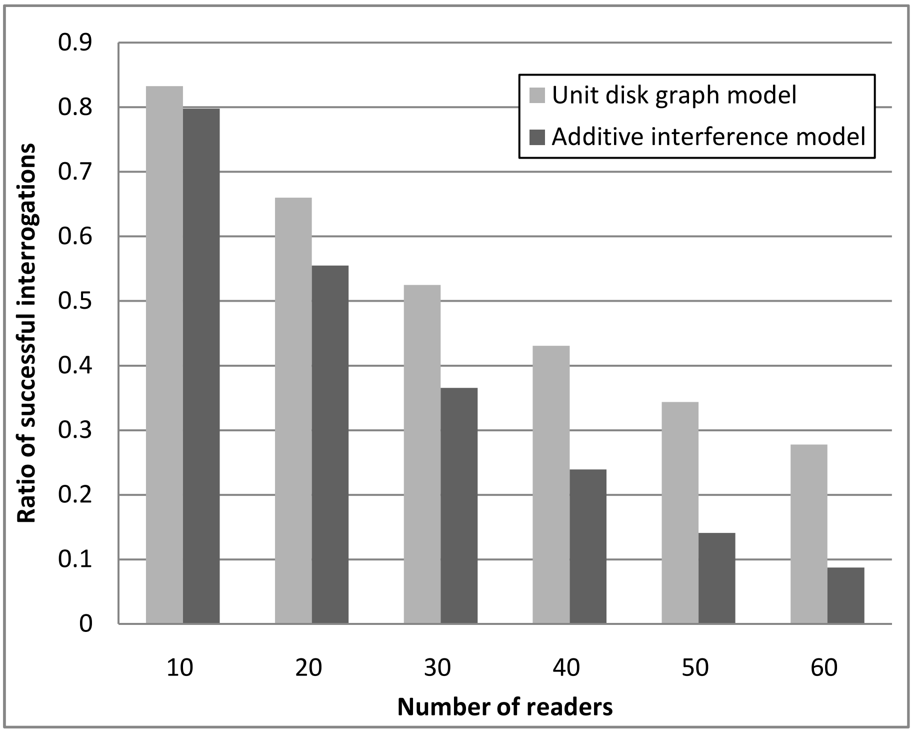


Figure 6.10. Ratio of successful interrogations, with 10 time slots per frame

from 5 to 10. It is also interesting to note that even when the number of time slots are equal to the number of total readers, the ratio of successful interrogations is not 1, because initially each reader picks its own time slot randomly and it takes time to reach the stable state that each reader interrogates at a different time slot.

6.5.2.2 Throughput

Figure 6.11 describes the throughput under the unit disk graph model. As illustrated, there is one specific slotted that can reach the best throughput for each scenario. The best throughput requires more time slots when the number of readers in the fixed field increases. For example, when there are 10 readers, the highest throughput appears when there are 3 time slots per frame; when there are 60 readers, 11 time slots per frame give the best performance. When the time slots are less than 3, the throughput becomes worse as the number of readers increases. However, when the time slots are more than 10, the throughput grows when there are more readers deployed in the system. Figure 6.12 shows the number of successful interrogations considering the additive interference model. The general behavior is similar to the one shown in Figure 6.11. Besides, the general throughput of unit disk graph model is better than the one of additive interference model since the latter

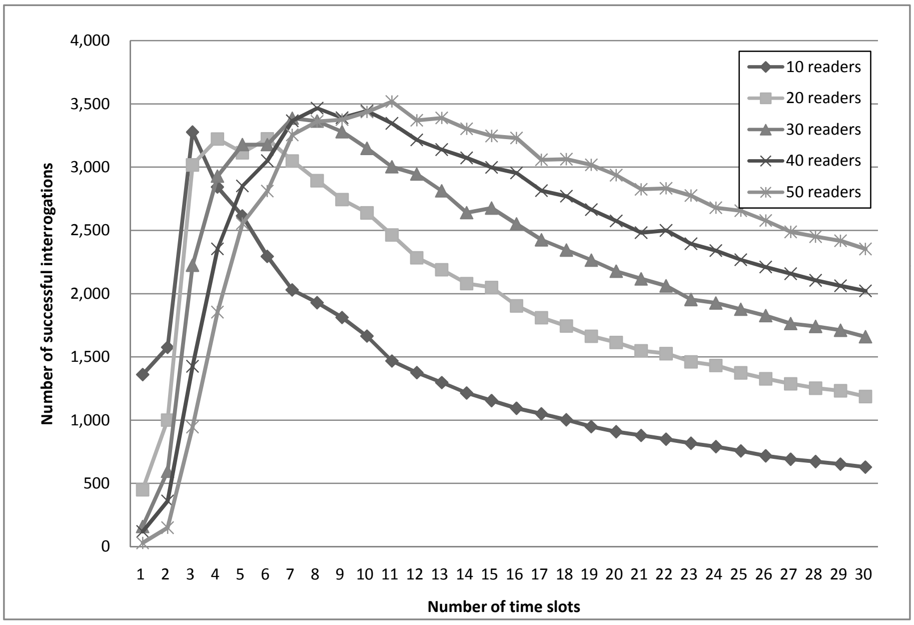


Figure 6.11. Number of successful interrogations for the unit disk graph model under the slotted interrogation scenario

Table 6.4. Analysis of the best throughput for the slotted interrogation

Readers	Unit disk graph model		Additive interference model		Loss
	Time slots	Throughput	Time slots	Throughput	
10	3	3276.93	5	2186.28	33.3%
20	6	3223.56	10	2218.79	31.2%
30	7	3385.89	13	2272.30	32.9%
40	8	3465.39	16	2332.50	32.7%
50	11	3517.74	19	2337.87	33.5%

one models more reader-to-reader collisions.

However, the required number of time slots to achieve the best performance in additive interference model is larger than the unit disk graph model. For example, when there are 10 readers in the RFID system, 5 times slots per frame gives best performance in Figure 6.12; while in Figure 6.6, the required number is just 3. This difference is more evident when the number of readers grows: in the system with 60 readers, the best number of time slots per frame is 11 and 19 for the unit disk graph model and the additive interference model, respectively.

Also in this scenario, the single interference model is not able to identify the best configuration as shown in Table 6.4. It can be observed that the loss in the best throughput from unit disk graph model to additive interference model ranges from

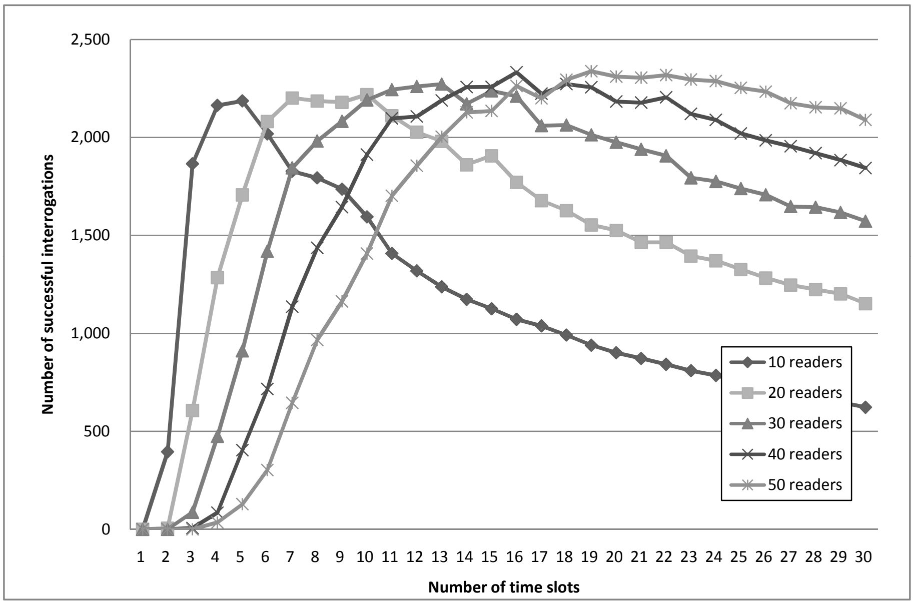


Figure 6.12. Number of successful interrogations for the additive interference model under the slotted interrogation scenario

31.2% to 33.5%.

6.5.2.3 Percentage of additive collisions

Figure 6.13 shows the percentage of additive collisions in the scenario of slotted interrogation. Except for the sparse system with 10 readers, the percentage of additive collisions does not change significantly as the number of time slots per frame changes, which means that the slotted interrogation alleviates the influence of additive interferences. Besides, the percentage of additive collisions goes down when the number of readers raises. It can be observed that the behaviors of 10 and 20 readers are different from the trends of more than 30 readers, that is because when the time slots grows to more than 20, the number of times slots is larger than the number of total RFID readers in the RFID system and the number of both the direct collisions and additive collisions decreases.

6.5.3 DCS anti-collision

This section investigates the performance of DCS protocol under the unit disk graph model and the additive interference model. The size of the time slot is set as 0.5 s and the total simulation time is 1000 s. All the readers are randomly plotted in a 1000 $m \times 1000$ m field. Besides, no collisions between the kick packets are assumed.

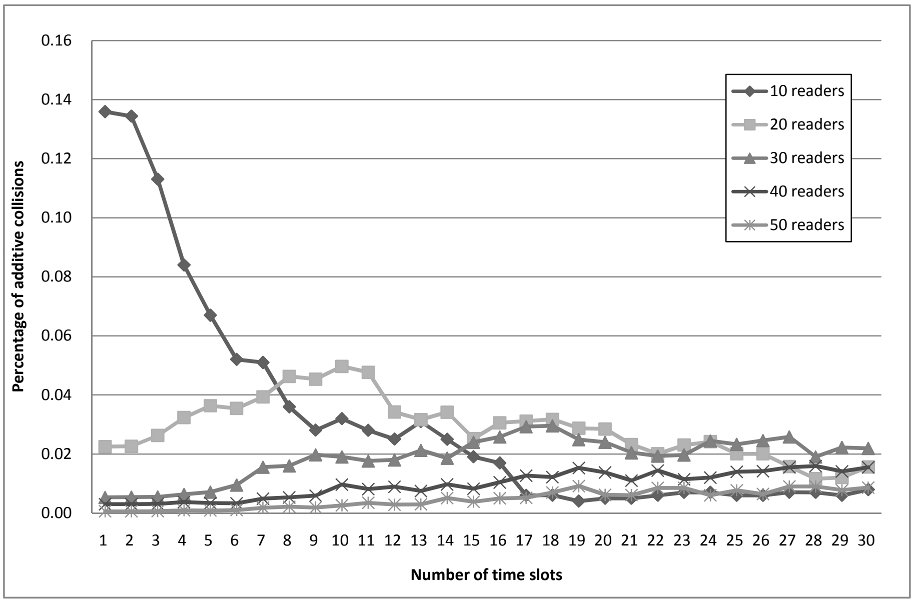


Figure 6.13. Percentage of additive collisions for the additive interference model under the slotted interrogation scenario

6.5.3.1 Ratio of successful interrogations

Figure 6.14 and Figure 6.15 present the ratio of successful interrogations achieved with DCS according to the two interference models. The values reported in both of the figures decrease as more readers are deployed, since more collisions appear when the density grows. It can be observed that the difference between the two models increases as the number of readers grows. When there are 10 readers, DCS shows a good performance no matter what the interference model is. However, when the number of readers grows to more than 20, there has been a sharp decline if the additive interference model is adopted for computing the received interference. In the additive interference model, if the number of readers is higher than 40, the ratio is close to 0, which means that 5 colors are not enough to avoid any collisions in such a dense deployment.

In the case of Figure 6.15, the performance are much greater than in Figure 6.15 since the value of *maxColors* increases to 10. 10 colors in DCS are suitable for the deployment with less than 30 readers in the unit disk graph model since the ratios are all above 0.99. On the other hand, the additive interference model requires more colors since the ratio decreases to 0.44 when there are 30 readers. Besides, the ratio gap between the two models firstly increases from 0.002 (with 10 readers) to 0.69 (with 40 readers), which is because the difference between the two models increases as the density grows. Afterwards, when the number of readers raises from 40 to 60, the ratio difference drops to 0.35 (with 60 readers). However, this drop does not

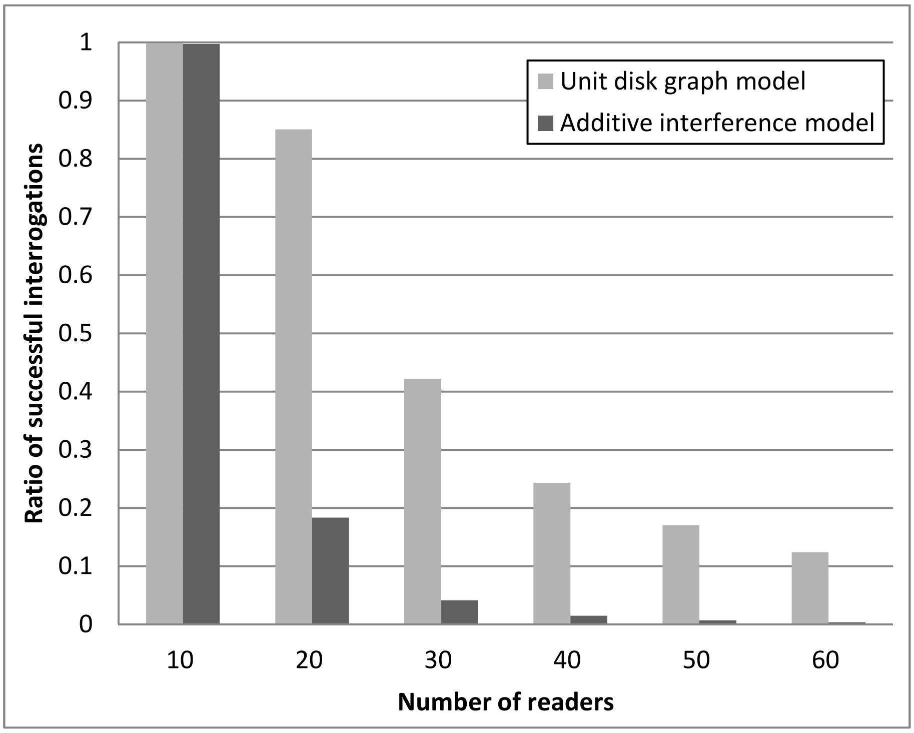


Figure 6.14. Ratio of successful interrogations in DCS, with $maxColors = 5$

indicate a performance approaching of the two models since it is simply because DCS under both of two models cannot achieve an acceptable successful ratio in the deployment with such a high density.

6.5.3.2 Throughput

Figure 6.16 presents the number of successful interrogations of DCS protocol in the unit disk graph model. There is always a peak throughput for each scenarios, which is the result of the compromise between the collision avoidance and the number of total interrogations. A larger value of $maxColors$ means a good ability to avoid collisions, but on the other hand, it also means less number of interrogation attempts in a fixed time period.

Figure 6.17 illustrates the throughput in the additive interference model. Compared with the performance in Figure 6.16, the performance of DCS protocol is generally better in the unit disk graph model since it ignores the additive collisions. Besides, it can be observed that in the additive interference model throughput changes in a smoother way than in the single interference model. In DCS, additive collisions from a collision set cause the colliding reader to change to a new color,

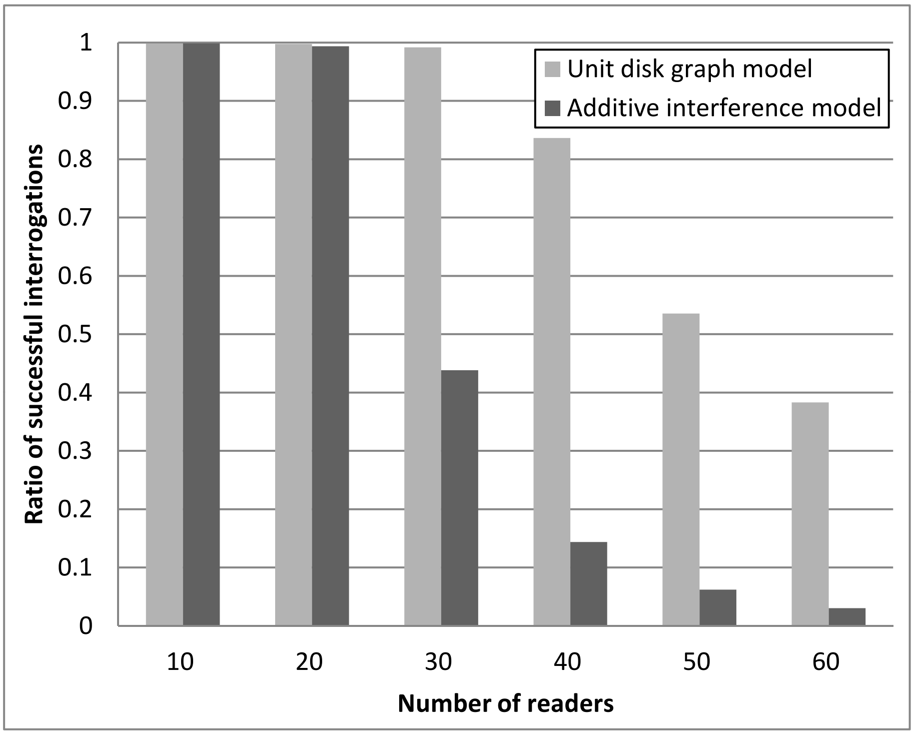


Figure 6.15. Ratio of successful interrogations in DCS, with $maxColors = 10$

however, it may collide again due to the interferences caused by a totally new collision set. Consequently, the influence of $maxColors$ is not as distinct as in the unit disk graph model.

As shown in Table 6.5, the best configuration to achieve the best throughput also varies according to the different interference model. For example, the best configuration of $maxColors$ for 40 readers is 10 in the single interference model; while the best throughput for 40 readers appears when $maxColors = 17$ in the additive interference models. The difference between the optimal configurations grows as the number of readers rises, for example, the difference raises from 3 with 20 readers to 12 with 60 readers. Besides, the throughput loss caused by the additive collisions ranges from 33.2% to 39.4%.

6.5.3.3 Percentage of additive collisions

By observing Figure 6.18, it can be concluded that the influence of additive collisions on the performance first increases and then decreases, with respect to the growing value of $maxColors$. For example with 40 readers, the ratio of additive collisions firstly grows to the peak point 0.41 (with $maxColors = 10$), because the direct collisions deceases as $maxColors$ grows, which is also reflected in Figure 6.16.

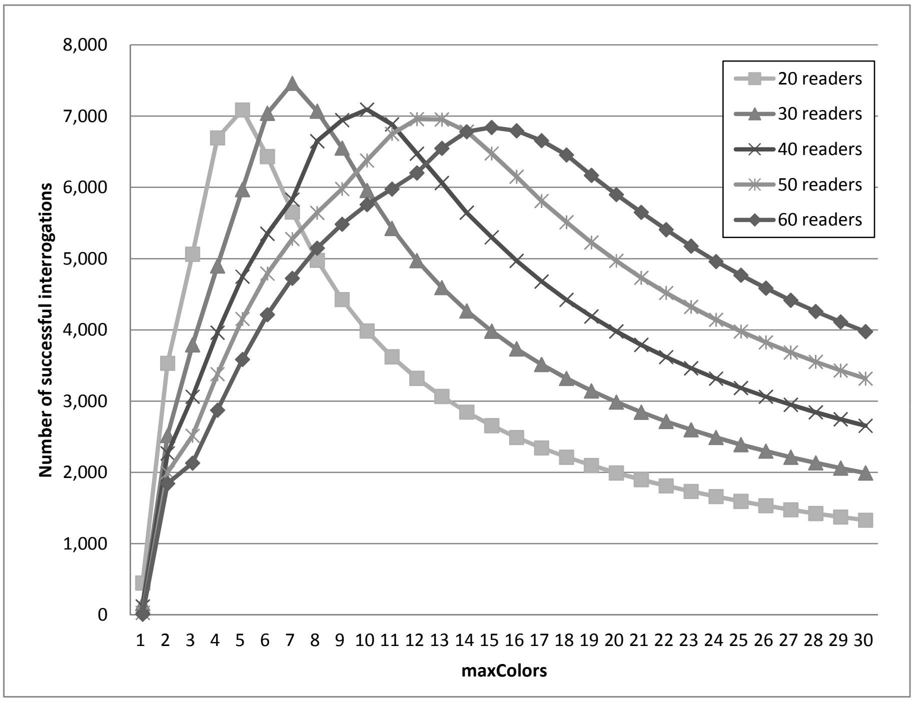


Figure 6.16. Number of successful interrogations for the unit disk graph model in DCS

Table 6.5. Analysis of the best throughput for the DCS protocol

Readers	Unit disk graph model		Additive interference model		Loss
	maxColors	Throughput	maxColors	Throughput	
20	5	7087.57	8	4734.11	33.2%
30	7	7461.20	12	4524.30	39.4%
40	10	7093.76	17	4364.72	38.5%
50	12	6959.38	22	4257.25	38.8%
60	15	6842.18	27	4157.28	39.2%

Afterwards, the ratio of additive collisions drops down until approaching 0 because DCS finally achieves a stable state in which each reader can perform the interrogation without interferences from other readers. Considering the density of the deployment, the configuration of *maxColors* where the additive collisions achieves its maximum effects rises from 5 to 15 as the number of readers increases from 20 to 60.

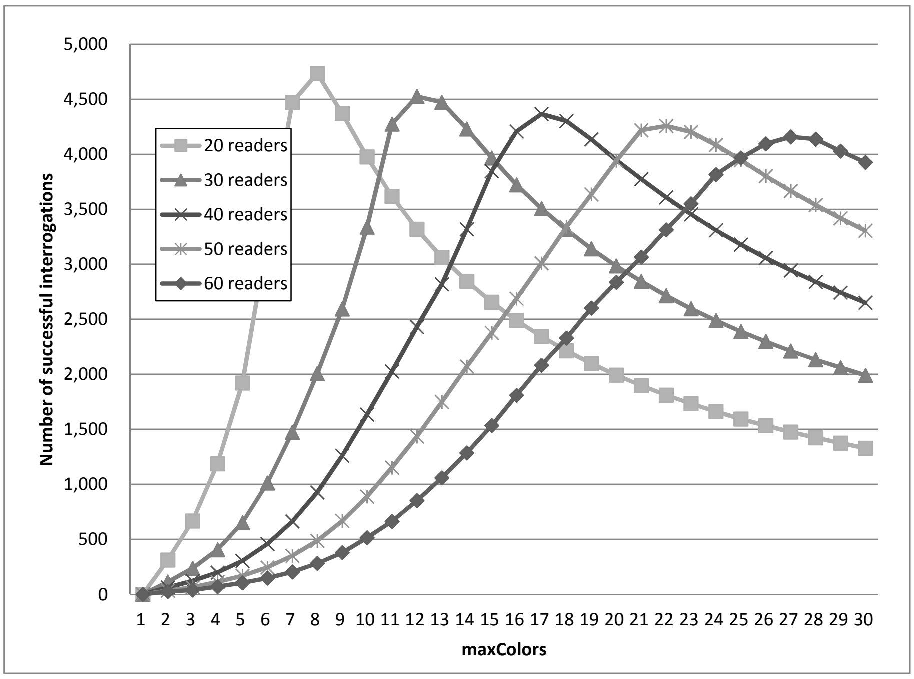


Figure 6.17. Number of successful interrogations for the additive interference model in DCS

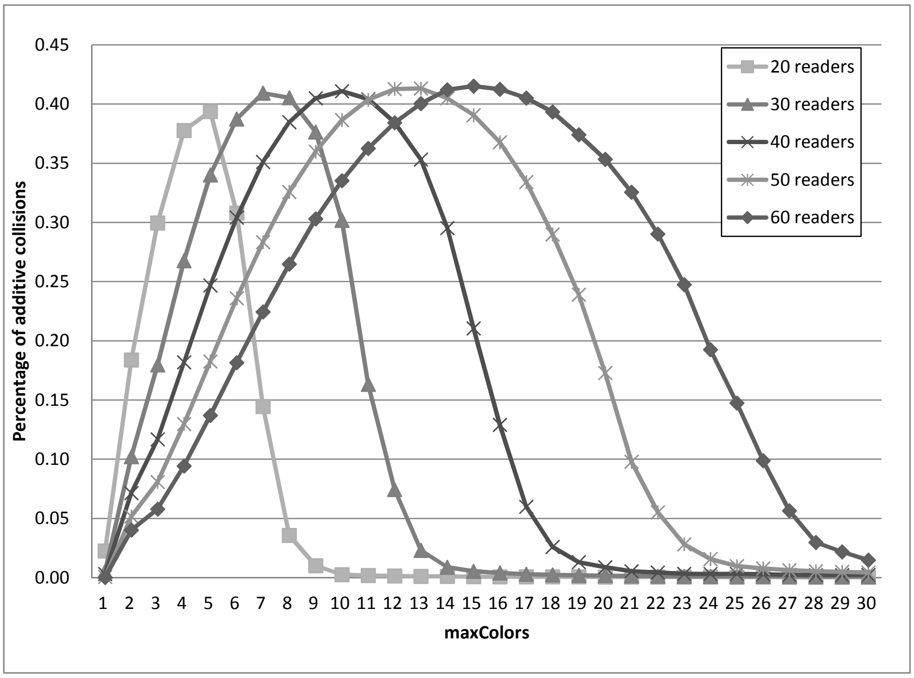


Figure 6.18. Percentage of additive collisions for the additive interference model in the DCS protocol

Conclusion

This thesis has analyzed and evaluated the reliable transmissions in wireless communication systems. Based on the proposed evaluation models and frameworks, it has proposed novel contributions for optimizing the performance of communication protocols in WSNs and RFID systems.

Firstly, the performance of the ACK- and NoACK-based transmission mechanisms have been compared, considering both the point-to-point model and the point-to-multipoint model. In the point-to-point model, the ACK-based mechanism always outperforms the NoACK-based mechanism when the link quality is larger than 0.4; on the other hand, the NoACK-based mechanism gives better performance in a extremely high packet loss environment. In the point-to-multipoint model with the proposed selective acknowledgement mechanism, the number of transmissions in the ACK-based mechanism increases linearly with respect to the increase of the neighborhood size. In a dense environment, the NoACK-based mechanism can probably give a better performance than the ACK-based one. Besides, the ratio between the cost of acknowledgement transmissions and the cost of data transmissions plays an important role in the performance of the two models.

Furthermore, the ACK- and NoACK-based implementations of the opportunistic flooding algorithm are investigated to compare their different performance. A deep evaluation and characterization of the opportunistic flooding protocol is presented considering the two transmission schemes. Simulation results under multiple scenarios show the different behavior of the two mechanisms while providing a frame of reference to choose one mechanism based on the application requirements. The analysis of the results shows that different scenarios require different implementation methods. The ratio between the data packet size and the acknowledgement packets size is crucial for the comparison of the performance. The NoACK-based mechanism can save more energy than the ACK-based one if the size of the acknowledgement packet is comparable to the size of the data packet. Otherwise, if the acknowledgement packet size is negligible with respect to the data packet, the ACK-based opportunistic flooding can provide a lower energy cost. On the other hand, the NoACK-based mechanism generates an intrinsic lower delivery ratio than the ACK-based one. Therefore, in a coverage critical flooding where a high delivery ratio is required, the ACK-based mechanism is recommended. However, in a dense network, the NoACK-based opportunistic flooding can also achieve an acceptable delivery ratio.

Secondly in RFID systems, the single and additive reader-to-reader interference models are analyzed and compared according to two different proposed scenarios: the pair interaction scenario and the ring deployment scenario. The single interference model is easier to be implemented, but the additive interference model is more precise. The interaction of a pair of interfering readers and the interaction of a group of readers deployed along a ring has been evaluated with different values of the path loss exponent (α), the interference threshold (Γ) and the noise power (N_0). As shown by the presented analysis, the single interference model is not enough precise to correctly describe the reader-to-reader collisions. However, in an environment with a high path loss or when the interference threshold is low, the difference between the performance of the two models is small. In these cases, the single interference model should be preferred due to its simplicity. Besides, it is interesting to notice that the RFID readers are easier to suffer from reader-to-reader collisions in an environment with a larger noise power.

Afterwards, the characteristics of the additive interference models are further studied. The single interference model is viewed as a special case of the additive interference model that considers only one reader's interference. In particular, the number of interfering readers n is analyzed. An evaluation simulator that collects all the minimal collision-set-n is proposed in order to evaluate the impact of n on the additive interference model. The numerical results are analyzed based on the affected readers, the average collision sets per reader and the distribution of the collision sets. The proposed evaluation framework can be used to find the appropriate n whenever a deployment requirement is specified. Besides, the impacts of the cardinality of the collision sets on the accuracy of the collision detection has been evaluated. It has shown that an analysis of anti-collisions protocols based on a model limited to direct interferences provide a low level of accuracy, since many collisions are not detected. However, few collisions are due to collision sets with high cardinality, so the models used for the evaluation of RFID reader-to-reader anti-collision protocols can be limited to small collision sets.

Finally, the characteristics and requirements of RFID reader-to-reader collision simulator have been investigated. Since none of the general purposed network simulators offers an implementation of the state-of-the-art reader-to-reader anti-collision protocols, a novel simulator based on OMNeT++ is proposed. It is modular, configurable and provides support to simulate the anti-collision protocols with respect to both single interference models and additive interference models. To test the simulator and observe the simulation results of the two interference models, three specific scenarios have been proposed in order to evaluate the simulation performance: probabilistic interrogation, slotted interrogation and the DCS anti-collision protocol. Considering the scenarios, the ratio of successful interrogations, the number of successful interrogations and the percentage of additive collisions are collected and analyzed. Based on the experimental results, it can be observed that the difference between the two interference models are various with respect to different environments. The analysis has shown that simulations of RFID reader protocols based on a single interference model brings to unreliable results.

Bibliography

[1] L. Zhang, R. Ferrero, E. R. Sanchez, and M. Rebaudengo, "Performance analysis of reliable flooding in duty-cycle wireless sensor networks," *Transactions on Emerging Telecommunications Technologies*, vol. 25, no. 2, pp. 183–198, 2014. [Online]. Available: http://dx.doi.org/10.1002/ett.2556

[2] S. Guo, Y. Gu, B. Jiang, and T. He, "Opportunistic flooding in low-duty-cycle wireless sensor networks with unreliable links," in *Proceedings of the 15th annual international conference on Mobile computing and networking*, ser. MobiCom, 2009, pp. 133–144.

[3] L. Zhang, E. R. Sanchez, and M. Rebaudengo, "Evaluation framework of opportunistic flooding in wireless sensor networks," in *Proceedings of the IFIP 9th International Conference on Embedded and Ubiquitous Computing*, ser. EUC, 2011, pp. 87–94.

[4] L. Zhang, E. Sanchez, and M. Rebaudengo, "Performance evaluation of reliable and unreliable opportunistic flooding in wireless sensor network," in *Networks (ICON), 2011 17th IEEE International Conference on*, 2011, pp. 7–12.

[5] L. Zhang, R. Ferrero, F. Gandino, and M. Rebaudengo, "A comparison between single and additive contribution in RFID reader-to-reader interference models," in *6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, July 2012, pp. 177–184.

[6] ——, "Evaluation of single and additive interference models for RFID collisions," *Mathematical and Computer Modelling*, 2013.

[7] L. Zhang, F. Gandino, R. Ferrero, and M. Rebaudengo, "Evaluation of the additive interference model for rfid reader collision problem," in *RFID Technology (EURASIP RFID), 2012 Fourth International EURASIP Workshop on*, Sept 2012, pp. 9–13.

[8] L. Zhang, F. Gandino, R. Ferrero, B. Montrucchio, and M. Rebaudengo, "Trade-off between maximum cardinality of collision sets and accuracy of RFID reader-to-reader collision detection," *EURASIP Journal on Embedded Systems*, vol. 10, 2013.

[9] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on

sensor networks," *Communications Magazine, IEEE*, vol. 40, no. 8, pp. 102–114, Aug 2002.

[10] T. Zahariadis, H. C. Leligou, P. Trakadas, and S. Voliotis, "Trust management in wireless sensor networks," *European Transactions on Telecommunications*, vol. 21, no. 4.

[11] F. Ishmanov, A. S. Malik, and S. W. Kim, "Energy consumption balancing (ECB) issues and mechanisms in wireless sensor networks (WSNs): a comprehensive overview," *European Transactions on Telecommunications*, vol. 22, no. 4.

[12] Y. Gu and T. He, "Data forwarding in extremely low duty-cycle sensor networks with unreliable communication links," in *Proceedings of the 5th international conference on Embedded networked sensor systems*, ser. SenSys, 2007, pp. 321–334.

[13] D. Arifler, "Optimality of homogeneous sensing range assignment in large-scale wireless sensor network deployments," *Communications Letters, IEEE*, vol. 16, no. 9, pp. 1489–1491, 2012.

[14] B. Kaminska and P. Gburzynski, "Sustainability of self-configuring wireless sensor networks," in *14th IEEE International Conference on Electronics, Circuits and Systems. ICECS*, dec. 2007, pp. 1348–1351.

[15] A. Martirosyan, A. Boukerche, and R. Pazzi, "A taxonomy of cluster-based routing protocols for wireless sensor networks," in *Proceedings of The International Symposium on Parallel Architectures, Algorithms, and Networks*, 2008, pp. 247–253.

[16] G. Sharma, S. Bala, and A. Verma, "Comparison of flooding and directed diffusion for wireless sensor network," in *India Conference (INDICON), IEEE*, dec. 2009, pp. 1–4.

[17] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, ser. MobiCom, 2000, pp. 56–67.

[18] X. Wang, J. Yin, Q. Zhang, and D. Agrawal, "A cross-layer approach for efficient flooding in wireless sensor networks," in *Wireless Communications and Networking Conference, IEEE*, vol. 3, march 2005, pp. 1812–1817 Vol. 3.

[19] J. K. Hart and K. Martinez, "Environmental sensor networks: A revolution in the earth system science?" *Earth-Science Reviews*, vol. 78, pp. 177–191, 2006.

[20] N. A. Pantazis, S. A. Nikolidakis, and D. D. Vergados, "Energy-efficient routing protocols in wireless sensor networks for health communication systems," in *Proceedings of the 2nd International Conference on Pervasive Technologies Related to Assistive Environments*, ser. PETRA, 2009, pp. 34:1–34:8.

[21] S. Li, A. Zhan, X. Wu, and G. Chen, "ERN: Emergence rescue navigation with wireless sensor networks," in *Proceedings of the 15th International Conference*

on Parallel and Distributed Systems, ser. ICPADS, 2009, pp. 361–368.

[22] M. Hussain, P. Khan, and K. kyung Sup, “Wsn research activities for military application,” in *Advanced Communication Technology, 2009. ICACT 2009. 11th International Conference on*, vol. 01, 2009, pp. 271–274.

[23] K. Martinez, J. Hart, and R. Ong, “Environmental sensor networks,” *Computer*, vol. 37, no. 8, pp. 50–56, 2004.

[24] J.-C. Wang, C.-H. Lin, E. Siahaan, B.-W. Chen, and H.-L. Chuang, “Mixed sound event verification on wireless sensor network for home automation,” *Industrial Informatics, IEEE Transactions on*, vol. 10, no. 1, pp. 803–812, 2014.

[25] R. Tesoriero, J. Gallud, M. Lozano, and V. Penichet, “A location-aware system using RFID and mobile devices for art museums,” in *4th International Conference on Autonomic and Autonomous Systems (ICAS)*, March 2008, pp. 76–81.

[26] P.-Y. Chen, W.-T. Chen, Y.-C. Tseng, and C.-F. Huang, “Providing group tour guide by RFIDs and wireless sensor networks,” *IEEE Transactions on Wireless Communications*, vol. 8, no. 6, pp. 3059–3067, June 2009.

[27] F. Gandino, E. Sanchez, B. Montrucchio, and M. Rebaudengo, “Opportunity and constraints for wide adoption of RFID in agri-food,” *International Journal of Advanced Pervasive and Ubiquitous Computing*, vol. 1, no. 2, pp. 49–67, July 2009.

[28] RNCOS, *Global RFID Market Forecast to 2014*. RNCOS Industry Research Solutions, Mar 2012.

[29] C. Wang, M. Daneshmand, K. Sohraby, and B. Li, “Performance analysis of RFID Generation-2 protocol,” *IEEE Transcations on Wireless Communications*, vol. 8, no. 5, pp. 2592–2601, May 2009.

[30] M. Bueno-Delgado, J. Vales-Alonso, C. Angerer, and M. Rupp, “A comparative study of RFID schedulers in dense reader environments,” in *IEEE International Conference on Industrial Technology (ICIT)*, March 2010, pp. 1373–1378.

[31] D.-H. Shih, P.-L. Sun, D. C. Yen, and S.-M. Huang, “Taxonomy and survey of RFID anti-collision protocols,” *Computer Communications*, vol. 29, no. 11, pp. 2150–2166, 2006.

[32] N. Abramson, “The ALOHA system: another alternative for computer communications,” in *Proceedings of Fall Joint Computer Conference*, 1970, pp. 281–285.

[33] M. Bueno-Delgado and J. Vales-Alonso, “On the optimal frame-length configuration on real passive RFID systems,” *Journal of Network and Computer Applications*, vol. 34, no. 3, pp. 864–876, 2011.

[34] I. Onat and A. Miri, “DiSEL: A distance based slot selection protocol for framed slotted ALOHA RFID systems,” in *IEEE Wireless Communications*

and Networking Conference, April 2009, pp. 1–6.

[35] J. Kim, “A combined polling and random access technique for enhanced anti-collision performance in RFID systems,” *IEICE Transactions on Communications*, vol. E92-B, no. 4, pp. 1357–1360, April 2009.

[36] Y.-C. Lai and C.-C. Lin, “Two blocking algorithms on adaptive binary splitting: Single and pair resolutions for RFID tag identification,” *IEEE/ACM Transactions on Networking*, vol. 17, no. 3, pp. 962–975, June 2009.

[37] Y.-H. Chen, S.-J. Horng, R.-S. Run, J.-L. Lai, R.-J. Chen, W.-C. Chen, Y. Pan, and T. Takao, “A novel anti-collision algorithm in RFID systems for identifying passive tags,” vol. 6, no. 1, pp. 105–121, Feb. 2010.

[38] D. Engels and S. Sarma, “The reader collision problem,” in *IEEE International Conference on Systems, Man and Cybernetics*, vol. 3, Oct. 2002.

[39] G. Joshi and S. Kim, “Survey, nomenclature and comparison of reader anti-collision protocols in RFID,” in *IETE Tech Rev*, vol. 25, no. 5, 2008, pp. 285–292.

[40] K. Leong, M. Ng, and P. H. Cole, “The reader collision problem in RFID systems,” in *Proc. of IEEE International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications*, 2005, pp. 658–661.

[41] C. Wang, B. Li, M. Daneshmand, K. Sohraby, and R. Jana, “On object identification reliability using RFID,” *Mobile Networks and Applications*, vol. 16, pp. 71–80, Feb. 2011.

[42] W. Ye, J. Heidemann, and D. Estrin, “An energy-efficient MAC protocol for wireless sensor networks,” in *INFOCOM. Proceedings of the 21th Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 3, 2002.

[43] T. Van Dam and K. Langendoen, “An adaptive energy-efficient MAC protocol for wireless sensor networks,” in *Proceedings of the 1st international conference on Embedded networked sensor systems*, ser. SenSys, 2003, pp. 171–180.

[44] J. Polastre, J. Hill, and D. Culler, “Versatile low power media access for wireless sensor networks,” in *Proceedings of the 2nd international conference on Embedded networked sensor systems*, ser. SenSys, 2004, pp. 95–107.

[45] M. Buettner, G. V. Yee, E. Anderson, and R. Han, “X-MAC: a short preamble MAC protocol for duty-cycled wireless sensor networks,” in *Proceedings of the 4th international conference on Embedded networked sensor systems*, ser. SenSys, 2006, pp. 307–320.

[46] K.-J. Park, K. Jeong, H. Lim, and D. Park, “Carrier sense adaptation with enhanced fairness in IEEE 802.15.4 WPAN,” *European Transactions on Telecommunications*, vol. 22, no. 5.

[47] S. Ergen, C. Fischione, D. Marandin, and A. Sangiovanni-Vincentelli, “Duty-cycle optimization in unslotted 802.15.4 wireless sensor networks,” in *Global Telecommunications Conference, IEEE GLOBECOM*, Dec. 2008, pp. 1–6.

[48] A. G. Ruzzelli, G. M. P. O'Hare, R. Tynan, P. Cotan, and P. J. M. Havingat, "Protocol assessment issues in low duty cycle sensor networks: The switching energy," in *Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, 2006, pp. 136–143.

[49] M. Maróti, B. Kusy, G. Simon, and A. Lédeczi, "The flooding time synchronization protocol," in *Proceedings of the 2nd international conference on Embedded networked sensor systems*, ser. SenSys, 2004, pp. 39–49.

[50] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," in *Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops*, ser. Simutools. Brussels, Belgium: ICST, 2008, pp. 60:1–60:10.

[51] X. Xian, W. Shi, and H. Huang, "Comparison of OMNET++ and other simulator for WSN simulation," in *3rd IEEE Conference on Industrial Electronics and Applications. ICIEA*, june 2008, pp. 1439–1443.

[52] Y. Tselishchev, A. Boulis, and L. Libman, "Experiences and lessons from implementing a wireless sensor network MAC protocol in the Castalia simulator," in *Wireless Communications and Networking Conference (WCNC), IEEE*, april 2010, pp. 1–6.

[53] R. Agarwal, R. V. Martinez-Catala, S. Harte, C. Segard, and B. O'Flynn, "Modeling power in multi-functionality sensor network applications," in *Proceedings of the 2nd International Conference on Sensor Technologies and Applications*, 2008, pp. 507–512.

[54] R. Khalaf and I. Rubin, "Improving the Bit-per-Joule performance of IEEE 802.11 based wireless networks through high power transmissions," in *Proceedings of 17th International Conference on Computer Communications and Networks. ICCCN*, aug. 2008, pp. 1–6.

[55] X. Cheng, J. Xu, J. Pei, and J. Liu, "Hierarchical distributed data classification in wireless sensor networks," *Computer Communications*, vol. 33, pp. 1404–1413, July 2010.

[56] M. Vuran and I. Akyildiz, "Cross-layer packet size optimization for wireless terrestrial, underwater, and underground sensor networks," in *INFOCOM. The 27th Conference on Computer Communications. IEEE*, april 2008, pp. 226–230.

[57] N. Yaakob, I. Khalil, and J. Hu, "Performance analysis of optimal packet size for congestion control in wireless sensor networks," in *Proceedings of the 9th IEEE International Symposium on Network Computing and Applications*, ser. NCA, 2010, pp. 210–213.

[58] T. Zhao, T. de Guo, and W. guo Yang, "Optimal transmission radii and packet size for wireless sensor networks based on bi-level programming model," in *International Conference on Intelligent Computing and Integrated Systems (ICISS)*, oct. 2010, pp. 840–844.

[59] J. a. Almeida, A. Grilo, and P. R. Pereira, “Multimedia data transport for wireless sensor networks,” in *Proceedings of the 5th Euro-NGI conference on Next Generation Internet networks.* Piscataway, NJ, USA: IEEE Press, 2009, pp. 70–77.

[60] G. Girban and M. Popa, “A glance on WSN lifetime and relevant factors for energy consumption,” in *International Joint Conference on Computational Cybernetics and Technical Informatics (ICCC-CONTI)*, may 2010, pp. 523–528.

[61] M. Zuniga and B. Krishnamachari, “Analyzing the transitional region in low power wireless links,” in *1st Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks*, oct. 2004, pp. 517–526.

[62] A. Mindikoglu and A.-J. van der Veen, “Separation of overlapping RFID signals by antenna arrays,” in *Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference on*, 2008, pp. 2737–2740.

[63] D.-Y. Kim, B.-J. Jang, H.-G. Yoon, J.-S. Park, and J.-G. Yook, “Effects of reader interference on the RFID interrogation range,” in *37th European Microwave Conference*, Oct. 2007, pp. 728–731.

[64] S. Ramanathan and E. L. Lloyd, “Scheduling algorithms for multi-hop radio networks,” *SIGCOMM Comput. Commun. Rev.*, vol. 22, pp. 211–222, Oct. 1992.

[65] “Sphere of influence graphs in general metric spaces,” *Mathematical and Computer Modelling*, vol. 29, no. 7, pp. 45–53, 1999.

[66] “Sphere of influence graphs: Edge density and clique size,” *Mathematical and Computer Modelling*, vol. 20, no. 7, pp. 19–24, 1994.

[67] B. N. Clark, C. J. Colbourn, and D. S. Johnson, “Unit disk graphs,” *Discrete Mathematics*, vol. 86, no. 1-3, pp. 165–177, Dec. 1990.

[68] C. McDiarmid, “Random channel assignment in the plane,” *Random Structures & Algorithms*, vol. 22, no. 2, pp. 187–212, 2003.

[69] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, “Stochastic geometry and random graphs for the analysis and design of wireless networks,” *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 7, pp. 1029–1046, 2009.

[70] J. Díaz, J. Petit, and M. Serna, “A random graph model for optical networks of sensors,” vol. 2, no. 3, pp. 186–196, July-Sept. 2003.

[71] W. Yoon and N. H. Vaidya, “RFID reader collision problem: performance analysis and medium access,” *Wireless Communications and Mobile Computing*, vol. 12, no. 5, pp. 420–430, 2012.

[72] P. Gupta and P. Kumar, “The capacity of wireless networks,” vol. 46, no. 2, pp. 388–404, Mar. 2000.

[73] F. Kuhn, R. Wattenhofer, and A. Zollinger, “Ad-hoc networks beyond unit disk graphs,” in *Proceedings of the joint workshop on Foundations of mobile*

computing, ser. DIALM-POMC '03. ACM, 2003, pp. 69–78.

[74] S. A. Aly, V. Kapoor, J. Meng, and A. Klappenecker, "Bounds on the network coding capacity for wireless random networks," in *Information Theory and Applications Workshop.* IEEE, 2007, pp. 231–236.

[75] J. Díaz, J. Petit, and M. Serna, "Faulty random geometric networks," *Parallel Processing Letters*, vol. 10, no. 04, pp. 343–357, 2000.

[76] E. N. Gilbert, "Random graphs," *The Annals of Mathematical Statistics*, vol. 30, no. 4, pp. 1141–1144, 1959.

[77] P. Erdős and A. Rényi, "On random graphs I." *Publicationes Mathematicae*, vol. 6, pp. 290–297, 1959.

[78] A. Iyer, C. Rosenberg, and A. Karnik, "What is the right model for wireless channel interference?" *IEEE Transactions on Wireless Communications*, vol. 8, no. 5, pp. 2662–2671, May 2009.

[79] D.-Y. Kim, J.-G. Yook, H.-G. Yoon, and B.-J. Jang, "Interference analysis of UHF RFID systems," *Progress In Electromagnetics Research B*, vol. 4, pp. 115–126, 2008.

[80] D.-Y. Kim, H.-G. Yoon, B.-J. Jang, and J.-G. Yook, "Effects of reader-to-reader interference on the UHF RFID interrogation range," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 7, pp. 2337–2346, July 2009.

[81] H. Seo and C. Lee, "A new GA-based resource allocation scheme for a reader-to-reader interference problem in RFID systems," in *IEEE International Conference on Communications (ICC)*, May 2010, pp. 1–5.

[82] K. Cha, S. Jagannathan, and D. Pommerenke, "Adaptive power control protocol with hardware implementation for wireless sensor and RFID reader networks," *IEEE Systems Journal*, vol. 1, no. 2, pp. 145–159, Dec. 2007.

[83] J. Choi and C. Lee, "An MILP-based cross-layer optimization for a multi-reader arbitration in the UHF RFID system," *Sensors*, vol. 11, no. 3, pp. 2347–2368, 2011.

[84] M. Zuniga and B. Krishnamachari, "Analyzing the transitional region in low power wireless links," in *First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON)*, Oct. 2004, pp. 517–526.

[85] K. Whitehouse, A. Woo, F. Jiang, J. Polastre, and D. Culler, "Exploiting the capture effect for collision detection and recovery," in *The Second IEEE Workshop on Embedded Networked Sensors (EmNetS-II)*, May 2005, pp. 45–52.

[86] C. Meguerditchian, H. Safa, and W. El-Hajj, "New reader anti-collision algorithm for dense RFID environments," in *Electronics, Circuits and Systems (ICECS), 2011 18th IEEE International Conference on*, 2011, pp. 85–88.

[87] A. Sobeih, M. Viswanathan, D. Marinov, and J. Hou, "J-sim: An integrated

environment for simulation and model checking of network protocols," in *Parallel and Distributed Processing Symposium, 2007. IPDPS 2007. IEEE International*, March 2007, pp. 1–6.

[88] D. Wang, J. Wang, and Y. Zhao, "A novel solution to the reader collision problem in RFID system," in *Wireless Communications, Networking and Mobile Computing, 2006. WiCOM 2006.International Conference on*, 2006, pp. 1–4.

[89] H. Dai, S. Lai, and H. Zhu, "A multi-channel mac protocol for RFID reader networks," in *Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on*, 2007, pp. 2093–2096.

[90] W. Chun, E. Noel, and K. Tang, "The tag duplication problem in an integrated WSN for RFID-based item-level inventory monitoring," in *Networked Sensing Systems, 2008. INSS 2008. 5th International Conference on*, 2008, pp. 59–62.

[91] J. Waldrop, D. Engels, and S. Sarma, "Colorwave: a MAC for RFID reader networks," in *IEEE Wireless Communications and Networking*, vol. 3, March 2003, pp. 1701–1704.

[92] K. C. Shin, S. B. Park, and G. S. Jo, "Enhanced TDMA based anti-collision algorithm with a dynamic frame size adjustment strategy for mobile RFID readers," *Sensors*, vol. 9, no. 2, pp. 845–858, 2009.

[93] M. V. Bueno-Delgado, J. Vales-Alonso, C. Angerer, and M. Rupp, "A comparative study of RFID schedulers in dense reader environments," in *Industrial Technology (ICIT), 2010 IEEE International Conference on*, 2010, pp. 1373–1378.

[94] W. Drytkiewicz, S. Sroka, V. Handziski, A. Köpke, and H. Karl, "A mobility framework for omnet+," 2003.

[95] K. Langendoen and N. Reijers, "Distributed localization in wireless sensor networks: a quantitative comparison," *Computer Networks*, vol. 43, no. 4, pp. 499 – 518, 2003, wireless Sensor Networks. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128603003566

[96] E. Egea-Lopez, F. Ponce-Marin, and J. Vales-Alonso, "Obiwan: wireless sensor networks with OMNeT++," in *Electrotechnical Conference, 2006. MELECON 2006. IEEE Mediterranean*, 2006, pp. 777–780.

[97] X. Xian, W. Shi, and H. Huang, "Comparison of omnet++ and other simulator for wsn simulation," in *Industrial Electronics and Applications, 2008. ICIEA 2008. 3rd IEEE Conference on*, June 2008, pp. 1439–1443.

[98] H. Simaremare, A. Syarif, A. Abouaissa, R. Sari, and P. Lorenz, "Performance comparison of modified aodv in reference point group mobility and random waypoint mobility models," in *Communications (ICC), 2013 IEEE International Conference on*, 2013, pp. 3542–3546.

[99] K.-H. Chiang and N. Shenoy, "A random walk mobility model for location management in wireless networks," in *Personal, Indoor and Mobile Radio*

Communications, 2001 12th IEEE International Symposium on, vol. 2, 2001, pp. E–43–E–48 vol.2.

[100] D. Hong and S. Rappaport Stephen, "Traffic model and performance analysis for cellular mobile radio telephone systems with prioritized and nonprioritized handoff procedures," *Vehicular Technology, IEEE Transactions on*, vol. 35, no. 3, pp. 77–92, 1986.

[101] R. Guerin, "Channel occupancy time distribution in a cellular radio system," *Vehicular Technology, IEEE Transactions on*, vol. 36, no. 3, pp. 89–99, 1987.

[102] M. Zonoozi, P. Dassanayake, and M. Faulkner, "Mobility modelling and channel holding time distribution in cellular mobile communication systems," in *Global Telecommunications Conference, 1995. GLOBECOM '95., IEEE*, vol. 1, 1995, pp. 12–16 vol.1.

[103] X. Hong, M. Gerla, G. Pei, and C.-C. Chiang, "A group mobility model for ad hoc wireless networks," in *Proceedings of the 2Nd ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, ser. MSWiM '99. New York, NY, USA: ACM, 1999, pp. 53–60. [Online]. Available: http://doi.acm.org/10.1145/313237.313248

[104] F. Bai, N. Sadagopan, and A. Helmy, "The {IMPORTANT} framework for analyzing the impact of mobility on performance of routing protocols for adhoc networks," *Ad Hoc Networks*, vol. 1, no. 4, pp. 383 – 403, 2003. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870503000404

[105] B. Liang and Z. Haas, "Predictive distance-based mobility management for pcs networks," in *INFOCOM '99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 3, 1999, pp. 1377–1384 vol.3.

[106] C. Perkins and K.-Y. Wang, "Optimized smooth handoffs in mobile ip," in *Computers and Communications, 1999. Proceedings. IEEE International Symposium on*, 1999, pp. 340–346.

[107] S. Birari and S. Iyer, "PULSE: A MAC protocol for RFID networks," in *Embedded and Ubiquitous Computing*, ser. LNCS, 2005, vol. 1, pp. 1036–1046.

[108] J. Waldrop, D. Engels, and S. Sarma, "Colorwave: an anticollision algorithm for the reader collision problem," in *IEEE International Conference on Communications (ICC)*, vol. 2. IEEE, 2003, pp. 1206–1210.

[109] F. Gandino, R. Ferrero, B. Montrucchio, and M. Rebaudengo, "Introducing probability in RFID reader-to-reader anti-collision," in *8th IEEE International Symposium on Network Computing and Applications*, July 2009, pp. 250–257.

[110] ——, "Probabilistic DCS: an RFID reader-to-reader anti-collision protocol," *Journal of Network and Computer Applications*, vol. 34, no. 3, pp. 821–832, 2011.

[111] ——, "DCNS: An adaptable high throughput RFID reader-to-reader anticollision protocol," *IEEE Transactions on Parallel and Distributed Systems*, in print.

[112] ——, "Increasing throughput in RFID multi-reader environments avoiding reader-to-reader collisions," in *IEEE International Conference on Consumer Electronics (ICCE)*, Jan. 2011, pp. 37–38.

[113] J. Eom, S. Yim, and T. Lee, "An efficient reader anticollision algorithm in dense RFID networks with mobile RFID readers," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 7, pp. 2326–2336, 2009.

[114] R. Ferrero, F. Gandino, B. Montrucchio, and M. Rebaudengo, "A fair and high throughput reader-to-reader anticollision protocol in dense RFID networks," *IEEE Transactions on Industrial Informatics*, vol. 8, no. 3, pp. 697 –706, aug. 2012.

[115] M. Bueno-Delgado, R. Ferrero, F. Gandino, P. Pavon-Marino, and M. Rebaudengo, "A geometric distribution reader anti-collision protocol for RFID dense reader environments," *Automation Science and Engineering, IEEE Transactions on*, vol. 10, no. 2, pp. 296–306, 2013.

[116] M. Bueno-Delgado, J. Vales-Alonso, C. Angerer, and M. Rupp, "A comparative study of RFID schedulers in dense reader environments," in *IEEE International Conference on Industrial Technology, ICIT*, March 2010, pp. 1373–1378.