Coexistence Study on Different Medium Access Mechanisms Using a Software Defined Radio Testbed

Alexander Pastor

Bachelor Thesis

October 24, 2017

Examiners

Prof. Dr. Petri Mähönen
Prof. Dr.-Ing. Marina Petrova

Supervisors

Prof. Dr. Petri Mähönen
Peng Wang, M.Sc.
Andra Voicu, M.Sc.

Institute for Networked Systems
RWTH Aachen University

The present work was submitted to the Institute for Networked Systems

Coexistence Study on Different Medium Access Mechanisms Using a Software Defined Radio Testbed

Bachelor Thesis

presented by
Alexander Pastor

Prof. Dr. Petri Mähönen
Prof. Dr.-Ing. Marina Petrova

Aachen, October 24, 2017

(Alexander Pastor)

Acknowledgements

We thank...

Contents

ABSTRACT

Abstract here.

1

INTRODUCTION

Introduction here.

2

BACKGROUND

In this chapter the theoretical foundations and tools for the succeeding work are treated. Firstly, the MAC layer is introduced in the context of the OSI reference model. Successively, a glance on a number of different MAC protocols and mechanisms is taken, while analyzing weaknesses with respect to the challenges coming up in wireless transmission. The chapter concludes with naming the advantages of software-defined radio.

2.1 MAC PROTOCOLS

2.1.1 MAC Layer in the OSI Model

The OSI model is a layered architecture that divides a telecommunication system into several manageable layers. The original model features seven layers, where the focus in this thesis is on the MAC layer. Nevertheless, each layer's responsibilities is briefly listed. Then, a closer look on different realizations of the MAC layer is taken. Note that the data link layer has been split into two sublayers: the medium access and the logical link control sublayers.

Layer	Responsibilities
Physical Layer	dealing with mechanical, electrical and timing interfaces of data transmission
MAC Sublayer	controlling medium access and frame synchronization
LLC Sublayer	multiplexing to enable different network protocols coexist, flow control and error control.
Network Layer	routing and congestion control
Transport Layer	transmission reliability, same-order-delivery, congestion avoidance
Session Layer	token management, dialog control, synchronization
Presentation Layer	abstracting syntax and semantics of transmission
Application Layer	user application protocols, such as http, ftp, smtp and many more

TABLE 2.1: Layers in the OSI model

2.1.2 ALOHA

ALOHA is arguably the most simple MAC protocol. The basic idea is whenever a user wants to send data he does so. The higher the channel load, i.e. sending requests per time unit, the more likely collisions will occur, which render all transmitted information useless.

The question that comes to mind is, how likely is it that a collision will not occur. In other words, how efficient is an ALOHA channel? Making a statement requires a few preliminary assumptions:

1. We are taking a look at pure ALOHA as described above.
2. We simplify the calculation by assuming a fixed frame length.
3. The number of packets generated during a frame time is a poisson-distributed random variable X.
4. The channel load G comprises of two portions: "new" and retransmitted frames.

The probability mass function of the Poisson distribution and thus the probability of k frames being generated during a given frame time amounts to:

$$Pr(X = k) = \frac{G^k \cdot e^{-G}}{k!} \tag{2.1}$$

The probability of zero frames being generated during the transmission of the frame is $Pr(X = 0) = e^{-G}$ (assumption 3). If no collision occurs during the transmission of frame F no other frame was sent off during that transmission. Conversely, F itself did not collide with a frame sent off prior to F. We conclude that the vulnerability period during which collision may corrupt data is two frame times (assumption 2).

The probability that no frame other than the frame to be transmitted is generated during the two frame time vulnerability period is $P_0 = e^{-2G}$. The throughput S is given by $S = GP_0 = Ge^{-2G}$.

The maximum throughput is achieved when $\frac{\partial S}{\partial G} \stackrel{!}{=} 0$:

$$\begin{aligned} \tfrac{\partial S}{\partial G} &= \frac{\partial}{\partial G} G e^{-2G} && (2.2)\\ &= e^{-2G}(1 - 2G) && (2.3)\\ &\stackrel{!}{=} 0 && (2.4)\\ \Leftrightarrow \quad G &= 0.5 && (2.5) \end{aligned}$$

This means that for $G = 0.5$ the throughput S reaches its maximum $S_{\text{ALOHA,max}} = \frac{1}{2e} \approx 0.18$. This result is very reasonable, since the transmission of a frame is vulnerable for the duration of two frame times, so the maximum is achieved when sending exactly every second slot, where a slot is equivalent to the frame time.

As an aside, the throughput can be doubled with slotted ALOHA. In contrast to pure ALOHA, slotted ALOHA allows transmission only at the beginning of slots, which effectively halves the vulnerability period to only one slot, since frames transmitted prior to a frame F cannot interfere with F anymore. Thus, $S_{\text{ALOHA,max}} = \frac{1}{e} \approx 0.36$, reached at $G = 1$. However, this comes at the cost of an additional frame delay of t_{slot} in the worst case and $\frac{t_{\text{slot}}}{2}$ in the average case.

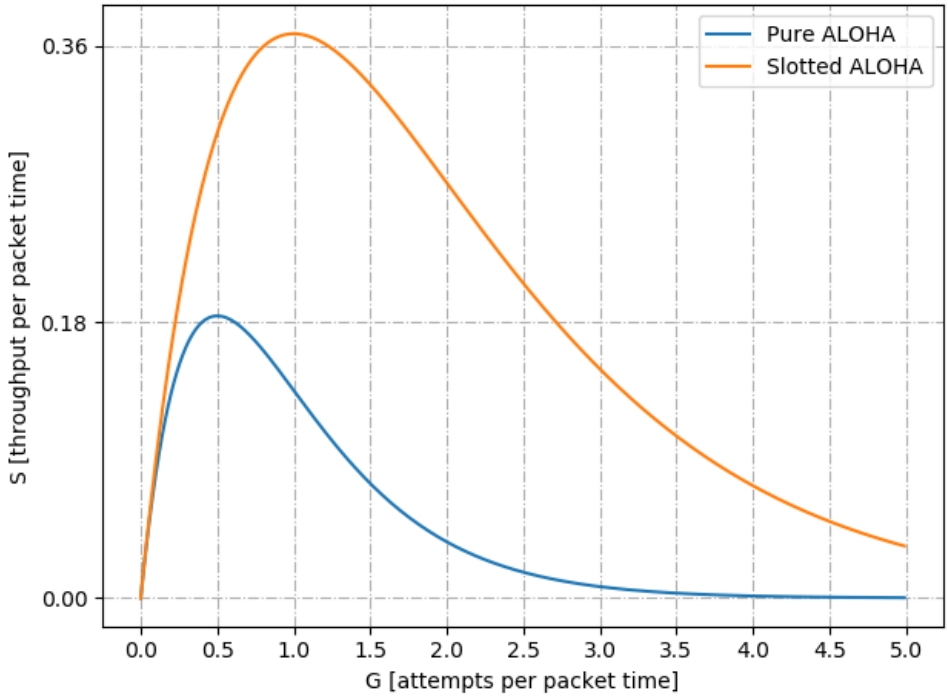


FIGURE 2.1: Pure ALOHA and slotted ALOHA's performance.

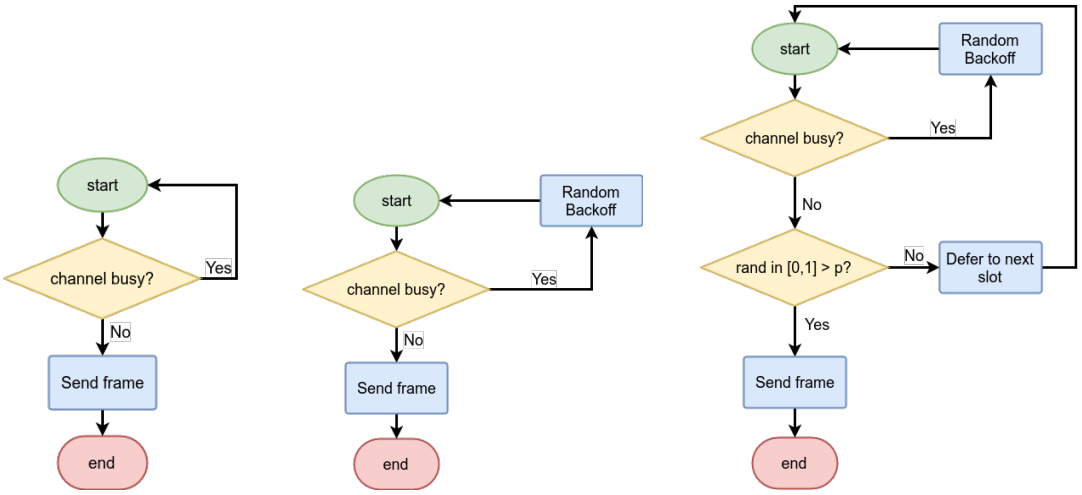
As shown above in figure 2.1 and the preceding paragraphs ALOHA's performance is discouraging and improvements over ALOHA were found.

2.1.3 CSMA

Main problem of ALOHA is the negligence of concurrent traffic in the channel. A solution to this problem is offered by the "listen before talk" (LBT) mechanism, which means in order to avoid collisions we sense the channel and refrain from sending should it be busy. This is the simple, yet effective basic idea of carrier sensing multiple access (CSMA) which comes in three flavors, as depicted in figure 2.2 which will be discussed next.

2.1.3.1 1-persistent CSMA

When the channel is busy 1-persistent CSMA waits until the channel becomes idle. As soon as the channel is found idle a frame is transmitted with a probability of 1, hence



(a) 1-persitent CSMA (b) non-persistent CSMA (c) p-persistent CSMA

FIGURE 2.2: The three flavors of CSMA

1-persistent CSMA. If the frame collides with another, the node waits for a random backoff time and then the whole process is started all over again.

Despite being a substantial improvement over ALOHA, this protocol has at least two problems:

- Provided propagation delay is zero or negligible, collisions can still occur. Imagine a three-node-scenario with nodes A, B and C. A is transmitting, while B and C are waiting for their turn. Once A finished transmission B and C will lunge onto the channel like a pack of wolves leading to collision.
- If propagation delay is not negligible the protocol suffers from another problem. In this scenario A has just begun sending. B will assume the channel is idle and send off his frame, since, due to the propagation delay, B has not yet heard of A. This is why propagation delay may significantly hamper this protocol's performance.

2.1.3.2 *Non-persistent CSMA*

In order to alleviate 1-persistent CSMA's problem with several nodes trying to seize the channel as soon as it becomes idle a less greedy attempt is made with non-persistent CSMA. Instead of continuously sensing the channel until it becomes idle nodes wait a random backoff time until they listen again. As a result, this protocol leads to better channel utilization with the downside of higher delays.

2.1.3.3 *P-persistent CSMA*

P-persitent CSMA is a protocol for slotted channels. Whenever a node A wishes to send off a packet the channel is sensed. If the channel is found idle it transmits its

packet with a probability of p. With a probability $1 - p$ it defers the transmissions to the next slot. This process is repeated until one either the packet is sent off or the channel is found busy again. In the latter case A acts as though a collision had taken place and waits a random time until starting again.

This flavor of CSMA can be regarded as a compromise between 1-persistent CSMA and non-persistent CSMA, where the choice of p determines the greediness. The smaller p, the less greedy and thus the closer p-persistent CSMA approximates non-persistent behavior. An appropriate choice of p can get the best out of both worlds: minimal delays as in 1-persistent CSMA, as well as high channel efficiency as in non-persistent CSMA.

2.1.4 CSMA with Collision Detection

A way to further improve CSMA-family protocols is to immediately cancel transmissions once a collision is detected. There is no point in continuing these transmissions, as the transmitted data is lost in any case. Stating the obvious, aborting transmission saves both bandwidth and time.

CSMA/CD is used on wired LANs and serves as basis of the wide-spread Ethernet. However, this mechanism is not extensively made use of in wireless networks. Concerning the reason, it is cardinal to understand that collision detection is an analog process. A collision is detected by comparing the received and transmitted signal's energy or pulse width, which premises transmission and reception taking place simultaneously.

This condition mostly is not met for wireless nodes, which are half-duplex. The reason for this lies in the conservation of energy.

$$P = \int_A I(\vec{x})\, dA \tag{2.6}$$

Where P is the power, I the intensity as function of the position $\vec{x}$ and dA the differential element of a closed surface around the source. Assuming that the integration takes place over the surface of a sphere with the radius r the term simplifies to:

$$P = \quad |I(r)| \cdot 4\pi r^2 \tag{2.7}$$

$$\Leftrightarrow \quad |I(r)| = \quad \frac{P}{4\pi r^2} \tag{2.8}$$

Another, and more common quantity in telecommunications is signal-to-noise ratio (SNR), which is defined as follows, where P is the signal power and N the noise power:

$$SNR[dB] = 10\, log\left(\frac{P}{N}\right) \tag{2.9}$$

Equations 2.8 and 2.9 imply if we increase the distance r by $\sqrt{2}$ the signal's intensity halves or lose 3dB in SNR, respectively. To make up for the loss in signal strength

we would have to employ expensive signal processing hardware making wireless equipment less affordable. Alternatively, we could increase the transmit power, but this increases interference with other nodes, as well as electricity consumption.

2.1.5 Challenges for Wireless MAC Protocols

Wireless MAC protocols have to tackle a few problems that do not occur in wired data exchange. Among them are the hidden node and the exposed node problem, which will be discussed by reference to 2.3. Further challenges, such as energy limitations will also be delineated.

2.1.5.1 The Hidden Node and the Exposed Node Problem

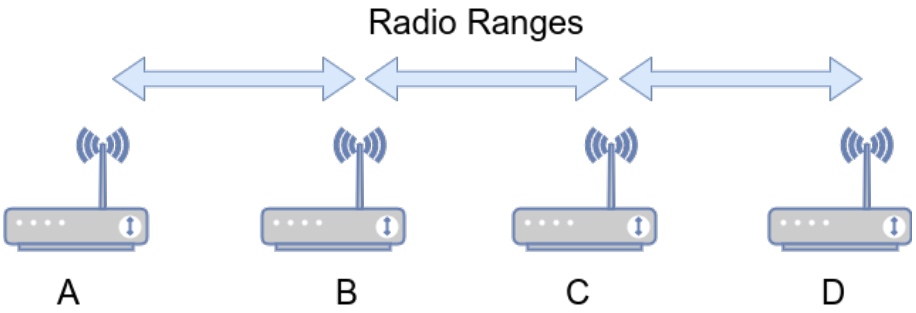


FIGURE 2.3: Setup to explain the hidden and exposed node problem. Each node can only reach its neighbors.

Suppose that the node's radio range is limited to the neighboring nodes and A would like to transmit to B. If C just started transmitting A won't hear C and falsely assume that the channel is idle and start transmitting. This is the hidden node problem.

For the same configuration, in another scenario B would like to send to A and C is already transmitting to D. B refrains from sending despite collisions would only take place between B and C, where it does not matter. This is the exposed node problem.

2.1.5.2 Further Challenges

Further challenges to MAC protocol design include the power conservation when faced with constrained power resources, as in wireless sensor networks (WSN) where devices rely on batteries for their supply with power. Attempts to mitigate waste of energy have been made in several specialized, duty-cycle based MACs such as Sensor MAC, Timeout MAC and Berkley MAC.

On the same page, due to constrained energy resources, WSN are especially susceptible to denial of sleep attacks, a special form of denial of service (DoS) attack, drastically increasing energy consumption and thus reducing the system's lifetime.

It is due to this fact that security is paramount in biomedical or military fields of application.

2.1.6 CSMA with Collision Avoidance

802.11 is a set of physical layer (PHY) and MAC specifications for wireless local area networks (WLANs). When the dominant mode of operation, the so-called distributed coordination function (DCF) is employed CSMA/CA is used in the MAC layer.

Beside physical carrier sensing previously simply referred to as carrier sensing another mechanism, namely virtual carrier sensing in combination with RTS/CTS exchange is employed to mitigate the trouble caused by hidden nodes.

In order to explain these mechanisms we refer to the setup of figure 2.3 with a slight modification in so far as that each node's radio range shall span across two neighboring nodes in both directions. That is to say, A can hear B and C, but not D and so on. Figure 2.4 visualizes the chain of events whose explanation follows.

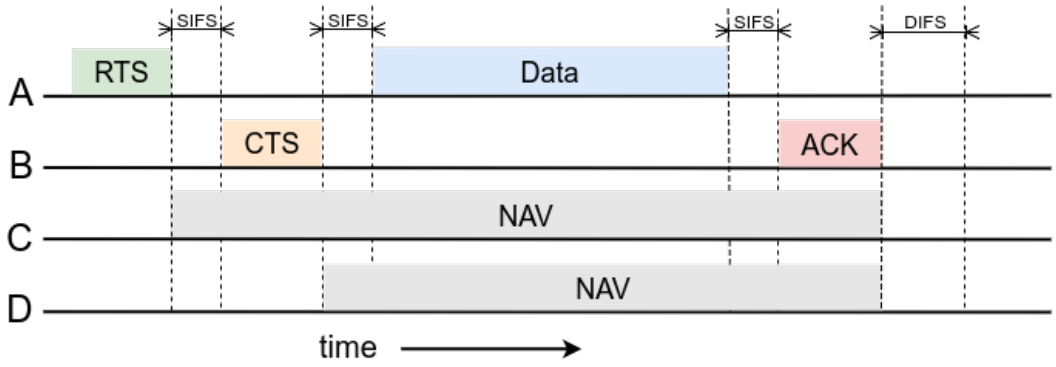


FIGURE 2.4: Virtual Carrier Sensing in CSMA/CA

A wants to send to B, hence issues a request to send (RTS). Every node receiving the RTS is shut down, except for B that in response to the RTS creates a clear to send (CTS) frame. Not only A receives this CTS frame, but also D, a hidden node from A's point of view. Upon reception of CTS D is silenced as well. Therefore, RTS/CTS is addressing the hidden node problem. RTS/CTS are frames of 30 bytes length containing the length of the frame in this case A wants to transmit. Based on this length C and D setup the so-called network allocation vector (NAV), which are node-internal timers reminding C and D that the channel is still in use. Due to the fact, that no physical process is running to detect the channel status this mechanism get its name virtual carrier sensing. Shutting down nodes has the beneficial side-effect of reducing overhearing and therefore reduces energy consumption.

As further depicted in figure 2.4 there are named intervals of specified length between each of the frames. Varying lengths of these interval types serve the purpose of prioritizing certain frames over others.

The short interframe spacing (SIFS) is the interval until the next control frame or next fragment (of a fragmented data frame) may be sent. SIFS is designed to allow one party out of the two parties in dialog send off their frame without interference by another node.

The longer interval DCF interframe spacing (DIFS) is the interval after which any station may try to seize the channel for their transmission.

For the sake of completeness, we briefly mention two consciously left out intervals, namely point coordination function interframe spacing (PIFS) and extended interframe spacing (EIFS). If 802.11 is operated in an alternative mode of operation, where a base station acts as a coordinator of traffic the standard prescribes an interval of length PIFS to allow the base station to send certain control (beacon and poll) frames. EIFS is used to report the reception of a bad or unknown frame and due to this action's low priority is the longest interval among the mentioned four.

As a remark on the exposed node problem: MAC protocols such as MACA that feature the RTS/CTS exchange, but no ACK from the receiver also solve the exposed station problem. The inclusion of the ACK however "resurrects" the exposed station problem, since the receiver's ACK can now interfere with node's that are out of the sender's range. However, renouncing on ACKs was dropped in the revised version MACAW, because the absence of lost frames was not noticed until much later in the transport layer, causing huge drops in throughput.

2.1.7 Duty-Cycle-Based MAC Protocols

... Sensor MAC, Timeout MAC, Berkley MAC ...

2.2 SOFTWARE DEFINED RADIO

2.2.1 Purpose of Software Defined Radio

Traditional radio equipment is "hardware-defined", i.e. that the signal processing runs on a specialized electrical circuit.

2.2.2 GNU Radio

3

Measurement Methodology

This chapter is dedicated to answering the questions of what was measured and how results were obtained. Firstly, the GNU Radio flowcharts are explained. Secondly, with reference to the flowcharts measurement metrics are formally defined. Subsequently follows an overview of the semi-automatic measurement script system designed to automate, therefore accelerate the process of file system management, data processing and plotting the results. Lastly, the measurement setup is discussed in the view of the necessity of data verification.

3.1 GNU Radio Flowcharts

3.2 Measurement Metrics

3.3 Measurement Script System

3.4 Measurement Setup

4

Measurement Results

In this chapter various

5

Conclusions and Future Work

Conclusions and Future Work here.

A

ABBREVIATIONS

CSMA/CA carrier sense multiple access with collision avoidance

CSMA/CD carrier sense multiple access with collision detection

CTS clear to send

DCF distributed coordination function

DIFS DCF interframe spacing

EIFS extended interframe spacing

GNU GNU is not unix

LAN local area network

LBT listen before talk

MAC medium access control

NAV network allocation vector

PCF point coordination function

PHY physical (layer)

PIFS PCF interframe spacing

RTS request to send

SIFS short interframe spacing

SDR software defined radio

SNR signal-to-noise ratio

WLAN wireless LAN

WSN wireless sensor networks

Bibliography

Eidesstattliche Versicherung

Name, Vorname

Matrikelnummer (freiwillige Angabe)

Ich versichere hiermit an Eides Statt, dass ich die vorliegende Arbeit/Bachelorarbeit/ Masterarbeit* mit dem Titel

selbständig und ohne unzulässige fremde Hilfe erbracht habe. Ich habe keine anderen als die angegebenen Quellen und Hilfsmittel benutzt. Für den Fall, dass die Arbeit zusätzlich auf einem Datenträger eingereicht wird, erkläre ich, dass die schriftliche und die elektronische Form vollständig übereinstimmen. Die Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Ort, Datum

Unterschrift

*Nichtzutreffendes bitte streichen

Belehrung:

§ 156 StGB: Falsche Versicherung an Eides Statt

Wer vor einer zur Abnahme einer Versicherung an Eides Statt zuständigen Behörde eine solche Versicherung falsch abgibt oder unter Berufung auf eine solche Versicherung falsch aussagt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

§ 161 StGB: Fahrlässiger Falscheid; fahrlässige falsche Versicherung an Eides Statt

(1) Wenn eine der in den §§ 154 bis 156 bezeichneten Handlungen aus Fahrlässigkeit begangen worden ist, so tritt Freiheitsstrafe bis zu einem Jahr oder Geldstrafe ein.

(2) Straflosigkeit tritt ein, wenn der Täter die falsche Angabe rechtzeitig berichtigt. Die Vorschriften des § 158 Abs. 2 und 3 gelten entsprechend.

Die vorstehende Belehrung habe ich zur Kenntnis genommen:

Ort, Datum

Unterschrift