Security of Wireless Networks
Master Solution of the Lab 2022

Teaching Assistants: Dr. Giovanni Camurati,
Claudio Anliker, Carl Friess
Authors of the Labs: Martin Kotuliak, Simon Erni

v5.1
December 14, 2022

Course responsible: Prof. Dr. Srdjan Capkun

Contents

Laboratory 1 Solution

Laboratory 1: Introduction to Software Defined Radios

1

1.1 Analytic Signals

Question 1.1

What is an analytic signal?

Solution: The analytic signal is a convenient representation of generic signals in terms of amplitude and phase in the complex domain.

More formally, a generic signal $x(t) = a(t)\cos(\phi(t))$ with amplitude $a(t)$ and phase $\phi(t)$ can be conveniently represented as the real component $Re(x_a(t))$ of the analytic signal $x_a(t) = a(t)e^{j\phi(t)}$ (polar notation).

More intuitively, the signal is seen as a vector in the complex plane, the norm of the vector is the amplitude, the angle is the phase, and the "speed" of rotation is the frequency.

Comment: This topic was covered in depth during the lectures. Please check lecture material.

Question 1.2

What are the properties of a signal that can be changed by modulation?

Solution: Amplitude, frequency and/or phase of a signal can be modulated (analog or digital) in order to transmit information. Recall that the instantaneous frequency $f(t)$ is $\frac{1}{2\pi}\frac{d\phi(t)}{dt}$.

Comment: This topic was covered in depth during the lectures. Please check lecture material.

Question 1.3

How many dimensions does an analytic signal have? Name them.

Solution: An analytic signal is defined in the complex domain. In a way, we can say that it has two dimensions, i.e., amplitude/phase or real/imaginary depending on the notation.

Comment: This topic was covered in depth during the lectures. Please check lecture material.

1.2 Introduction to the USRP device

No questions in this section.

1.3 Introduction to GNU Radio

Question 1.4

Describe the four types of plots and what each of them represents.

Solution:

- Frequency Display: it displays the spectrum of the input signal.
- Waterfall Display: aka Spectrogram, it displays the frequency (y axis) over time (x axis) where the color represents the intensity.
- Time Domain Display: it displays the input signal as is, in the time domain. In case of complex signals, we can see I and Q.
- Constellation Display: it displays the input signal in the complex domain. In other words, it plots I(t) and Q(t) as a point (I(t) + jQ(t)) in the complex plane. It is useful when the signal is modulated in PSK, QPSK, QAM, etc. (See quadrature modulator and example constellations in the lecture slides.)

Comment (if you are curious, not necessary for the exam): There exist fast digital algorithms to compute the discrete Fourier transform. The waterfall is an example of "time-frequency analysis", it is implemented by running a Fourier transform on a sliding window over time. There is a fundamental trade-off between resolution in time (short window) and resolution in frequency (large window).

1.4 Spectrum Analyzer

Question 1.5

Search online for an FM radio station for which you expect a good reception. What are the center frequency and the bandwidth of the FM radio signal? How did you configure the reception gain to make the band clearly visible?

Solution: Any reasonable local station / gain configuration is a valid solution. Gain values depend on the station and on the location within the lab. For example, we observed a signal at 94.6MHz, we checked online and it corresponds to SRF 1 Zurich Schaffhausen. The modulation used by these stations is WBFM (wide band frequency modulation). The bandwidth for Mono audio is 19 kHz. We used a gain of 40dB.

Question 1.6

Describe the three "Gain Types" you can use to specify the gain in the USRP source block.

Comment: We noticed that this question was confusing because the Gnuradio block for the USRP is not very clear and well documented. Therefore, we provide a more general answer that should get everyone up to speed with dB and dBm.

Solution:

- Linear scale
  - Input power in Watts Pin [W]
  - Output power in Watts Pout [W]
  - Gain (no units, it's a ratio) G = Pout [W] / Pin [W]
  - Therefore, Pout [W] = G Pin [W]
  - Optional: if the output power is less than the input power, it is more convenient to define the Loss as Pin [W] / Pout [W].
- Log scale
  - Input power in dBm: 10log10(Pin [W] / 1mW)
  - Output power in dBm: 10log10(Pout [W] / 1mW)
  - Gain in dB: G [dB] = 10log10(Pout [W] / Pin[W])
  - You can see the advantage of using the log scale:
    - Pout [W] = G Pin [W] is a multiplication (complicated)
    - Pout [dBm] = Pin [dBm] + G [dB] is an addition (easy)
    - Optional: if you have a Loss in dB, you can subtract it.
- Now, to the question:
  - Absolute gain is G [dB] and it is in the range supported by your radio, e.g., 0dB to 70dB.
  - Normalized gain is G [dB] / (Gmax [dB] - Gmin [dB]) so that it is conveniently represented as a number between 0 "min" and 1 "max"
  - Absolute power in dBm is P [dBm] = 10log10(P [W] / 1mW). We found that this setting is not well documented. We assume that it allows to set the output power directly in dBm (which is possible if the USRP is calibrated such that we know the output power corresponding to a given gain). The important thing to remember for you is the difference between the gain in dB and the absolute power in dBm.

1.5 FM Receiver

Practical Question 1.1

Which radio station are you listening too? Compared to the question before, did you have to change the configuration or the hardware setup to improve your reception?

Solution: Again, any reasonable setting. For example, we tuned our FM receiver at the same frequency as before, i.e., 94.6MHz. We increased the gain and played with the position of the antenna until we could clearly hear the audio.

1.6 QPSK Receiver

Question 1.7

How does the constellation plane of a QPSK modulation scheme look like? How many bits can be represented by one QPSK symbol?

Solution: In ideal conditions, the QPSK constellation is made of 4 symbols, each symbol has the same amplitude, and 1 out of 4 equally-spaced values for the phase. Since there are 4 symbols, each symbol can represent log2(4) = 2 bits We can then chose how to map 00, 01, 10, 11 to the fours symbols. Extra: draw the constellation or list the symbols as complex numbers.

Comment: This topic was covered in depth during the lectures. Please check lecture material.

Question 1.8

What main problem(s) arise(s) from the two radios not having the same shared clock?

Solution: The receiver and the transmitter have two clocks running at two (slightly) different speeds causing an offset in the carrier frequency, in the phase, in the sampling frequency, in the timings of the symbols, etc. These cause, for example, rotations of the constellation that prevent decoding. Proper techniques are required to compensate for these problems.

Comment: This is a very interesting topic. We expect you to have grasped only the intuition of the problems/solutions.

Question 1.9

What is differential coding? Which adverse effect can be mitigated by having a differential coding?

Solution: In BPSK (QPSK) a phase rotation of n times 180° (n times 90°) leads to another symbol which is valid but different. Therefore, in absence of any synchronization sequence, when the receiver tries to synchronize with the transmitter, it will find 2 (4) valid positions. This causes some ambiguity on the value of the received symbol. To solve this, we can use differential encoding, which encodes the bit in the difference between current and previous symbol, instead of in the current symbol only. More formally, instead of y[i] = x[i], we transmit y[i] = x[i] xor y[i-1]. Now, if at the receiver you do y[i] xor y[i-1] you get x[i] xor y[i-1] xor y[i-1] = x[i] even if y[i] and y[i-1] are rotated. In other words, the symbol is not encoded in the phase but in the difference between phase of current and previous symbol.

Practical Question 1.2

Compare the output of the `QT GUI Constellation Sink` (a) without any correction and (b) with differential coding and clock synchronization enabled. What are the differences?

Solution: Before correction, we cannot distinguish QPSK symbols. The constellation keeps rotating and we only see a big noisy circle. After correction, the incoming symbols have been properly sampled (e.g., thanks to clock synchronization) and form a nice constellation with 4 distinct symbols.

Practical Question 1.3

What changes in the plots when you move or obstruct the antenna?

Solution: We can see various impairments (e.g., rotation, amplitude) in the constellation plot. The error rate increases/decreases.

Question 1.10

Briefly explain what the channel correction block does as a whole. You don't have to go into details of the individual blocks.

Comment: This is a very interesting topic. We expect you to have grasped only the intuition of the problems/solutions, i.e., the presence of various impairments and reception and the necessity to compensate them. Below is a more in-depth answer.

Solution: The channel correction block is made of three main components, which compensate for various problems in the received signal until a clean constellation is found and can be decoded:

- Polyphase Clock Synch Block: clock recovery to align sampling, matched filter to remove inter-symbol interference, downsampling (leave only one sample per symbol after having found the best sampling point).
- Linear equalizer: equalization in the frequency domain to compensate for multi-path.
- Costas Loop: compensation for phase and frequency offset using a control loop that tracks frequency/phase (it will work as long the initial difference is not too big).

These are followed by:

- Constellation decoder: decodes from complex symbols to bits.
- Differential decoder: applies differential decoding, differential encoding is used to avoid errors caused by ambiguity in the phase that can occur if there is no initial synchronization frame, see previous answer for more details.
- Map: exact mapping to bits that matches the one used for transmission.

Good reference: `https://wiki.gnuradio.org/index.php/Guided_Tutorial_PSK_Demodulation`.

Practical Question 1.4

Is the data being received correctly? How would you improve the BER during the transmission?

Solution: It depends. In general, errors occur. To bring the error rate close to 0 we can, for example, put the radios in line of sight and increase the gain.

Practical Question 1.5

What is the sampling rate of the receiver? What is the symbol rate and what is the effective data rate (bits/s)?

Solution:

- Sampling rate: 390.62 kHz
- Symbol rate: 97.655 symbols/second = 97.655 Bd (Baud = Symbol/s).
- Bit rate: 195.31 kbps (2 bits per symbols in QPSK).

Laboratory 2 Solution

Laboratory 2: GPS Spoofing

2

2.1 Receiving Real GPS signals

Question 2.1

How big is the isolation (in dB) between the two ports coming into the splitter? Assuming we are transmitting with -50dBm, what is the strength of the leaked signal in dBm? You can check online for your splitter model: https://www.minicircuits.com/WebStore/Splitters.html

Solution: The splitter is used to combine the GPS signal from the active GPS antenna and the one from the USRP. A DC block is used in front of the USRP to cut the DC voltage provided by the GPS receiver to the active antenna (or we would damage the USRP). We care about the USRP signal (the adversarial one) not to leak on the cable that goes to the GPS antenna, so we want to know that the splitter has a good isolation between the port used for the antenna and the port used by the USRP. For example, the ZFRSC-42-S+ has a typical isolation of 6.5dB in the range of frequencies of interest. So if the input on the USRP port is -50dBm, the strenght of the leaked singal on the other port is -50dBm -6.5dB = -56.5dBm.

Comment: The rationale behind this question was to have you reason about the setup and work with decibels, and to read a datasheet.

Question 2.2

What type of antenna are we using (active / passive) and why are we not using the other type? What C/N_0 should we expect to get for the best satellite?

Solution: The signal is coming from space and it is very weak. An active antenna includes a low noise amplifer. Amplifying the signal before it travels to the receiver via a long cable improves the noise figure. The typical value of C/N_0 for a well designed receiver is 44dBHz to 50dBHz.

Comments (for your own curiosity, will not be part of the exam): In the solution we were lenient but beware that:

- An amplifier does not "reduce noise". Actually, it even adds a bit of noise (fortunately not much in a Low-Noise Amplifier (LNA)). So where is the advantage? Well, in a reception chain every block adds some noise (Noise Factor). If you amplify the signal early in the chain, then the Signal-to-Noise ratio (SNR) at the end of the chain is better. (Check this formula if you are interested in more details https://en.wikipedia.org/wiki/Friis_formulas_for_noise.) In our case we have a long cable, so it is worth amplifying before the cable. More in general, there is also another reason for

amplifying a signal. It is important to amplify a signal such that its dynamic range (range of values it takes) matches the dynamic range of the Analog-to-Digital Converter (ADC) in order to minimize quantization noise. Just think of the extreme case. If the signal is so small that it fits in one step of the converter, the digital output will always have the same value. Conversely, if dynamic range of the input signal is larger than the one of the ADC, we have clipping/saturation.

- In our specific setup, we inject the jamming signal after the antenna, so naturally a better antenna protects better from jamming by increasing the power of the legitimate signal that is added to the jamming signal. In a real scenario the jamming signal will also arrive to the antenna (in other words in a real scenario both legitimate and jamming signal will be amplified by the LNA in the active antenna).
- C/N0 is a carrier-to-noise density, i.e., expressed over a bandwidth of 1Hz. This is why it is dB/Hz not in dB. It is useful, for example, to compare receivers with different bandwidths.

Question 2.3

Briefly explain your setup. What would be the attacker's setup in the real-world scenario?

Solution: The signal from the antenna (GPS) and the signal from the USRP (jammer/spoofer) are combined with a splitter and sent to a GPS receiver. The attacker signal is going through a cable and the splitter has a high isolation between input ports, to avoid leaking the attack signal outside. In a real-world scenario, both GPS and USRP signal would arrive at the antenna.

Comment: A splitter is a passive element that works also in the other direction, combining two signals into one.

Practical Question 2.1

What are the coordinates of the receiver position?

Solution: The lab's location near CAB, e.g. 47°22'41.9"N 8°32'54.4"E.

Comment: If you were unlucky and did not get a fix, we still give points.

Practical Question 2.2

Does the sky plot in u-center match the sky plot on the website?

Solution: Yes they match, as expected.

Comment: If you were unlucky and did not get a fix, we still give points.

Question 2.4

Briefly summarize which bands and types of signals GPS uses.

Solution:

- GPS uses three bands, i.e., L1 (1575.42 MHz), L2 (1227.60 MHz), and L5 (11.76.45 MHz).
- GPS signals generally use DSSS with BPSK modulation.

Comment: More info at `https://gssc.esa.int/navipedia/index.php/GPS_Signal_Plan`. We also accepted other answers as long as they described something about the singals. We gave 0.5 points for answers only mentioning the bands.

2.2 GPS Jamming Attack

Practical Question 2.3

Report the following values:

1. TX gain needed to jam the GPS signal for at least ~30s
2. Difference in Automatic Gain Control (AGC) value on the u-blox with jamming and without jamming
3. Noise value with jamming and without jamming
4. What is the jamming indicator on the u-blox signalling – does it report a jamming/spoofing during the attack? Does it turn red or stay green?

Solution:

1. Several tens of dB. It also depends on the power of the legitimate signal, the attenuators in your setup, etc.
2. The AGC gain is much lower with jamming (e.g., 10%) than without jamming (e.g., 40%). (As a side note, this happens because the signal's dynamic range (range of values) is higher with the strong jamming signal, so we need less gain in order to march the dynamic range of the receiver's analog to digital converter.)
3. The noise value is clearly higher (e.g., 160) with jamming than without (e.g., 100). (As a side note, this value and its units are not well documented in the receiver's software.)
4. It is some proprietary jamming detection algorithm with an indicator scale and an alert status. Generally we can see them trigger during jamming.

Comment: We accept reasonable values that show your experiments were successful and you understood them. Same if you did not get a fix.

2.3 Replay Attack

Practical Question 2.4

Do you need more power than for the jamming only attack? What jamming/signal ratio have you used for replay?

Solution: There is no exact solution, again because each setup was different (e.g., presence of the legitimate signal or no, value of the attenuators, jamming and replay on two different setups). Each of you configured the setup until it worked. Please check the comment below.

Comment (Important even if you had full points and especially if you used more power): You can reinterpret this question in light of the last two labs on jamming and on the capture effect. GPS is a DSSS signal. It is hard to jam because the legitimate signal gets despreaded (processing gain) while the noise you send does not. However, when you replay, you are using a valid spreading code, so your attack signal gets despreaded, too. You only need a bit more power than the legitimate signal in order to form a higher peak at the correlator. However, since the GPS receiver locks on the legitimate signal and continuously tracks it, you might need to take extra action to let the attacker takeover (e.g., use more power, jam the the legitimate signal before the attack to make the receiver loose the lock, do a cold restart of the receiver). An advanced attack would first send the legitimate signal, then increase the power, then slowly drift away (smooth takevoer). Also note that you might have conducted jamming and reply on two different setups with different attenuation.

2.4 GPS Signal Generator

Question 2.5

Why do we need a GPS ephemerides file?

Solution: Our goal is to generate rogue GPS signals corresponding to a fake location. To correctly generate the signals as if they were coming from the real constellation, we need to know some (public) information about the satellites contained in the ephemerides file.

Comment: From the gps-sdr-sim README `https://github.com/osqzss/gps-sdr-sim`: "The user specifies the GPS satellite constellation through a GPS broadcast ephemeris file. The daily GPS broadcast ephemeris file (brdc) is a merge of the individual site navigation files into one. The archive for the daily file can be downloaded from: `https://cddis.nasa.gov/archive/gnss/data/daily/`. Access to this site requires registration, which is free. These files are then used to generate the simulated pseudorange and Doppler for the GPS satellites in view. This simulated range data is then used to generate the digitized I/Q samples for the GPS signal."

Question 2.6

Which signals must a GPS spoofer generate and what channel properties does it need to emulate?

Solution: The spoofer must generate the satellite signals that the receiver would receive if it were at the spoofed location. Therefore, the main channel property to emulate is the delay between each satellite and the victim. In addition, the spoofer can take into account Doppler shifts due to speed and the impact of the Ionosphere.

Comment: The main point here was to mention the delay/arrival time and one or more other channel effects (Doppler, Ionosphere, weather, multi-path, ...).

Practical Question 2.5

Check the source code of the GPS spoofer on GitHub. Where does it update the location and by how much?

Solution:

- https://github.com/simonerniethz/gps-sdr-sim/blob/c7aba55955c796398e3409088a1e80d8230a046b/gpssim.cpp#L2336
- llh[0] += 0.00001 / R2D ; ==> by 0.00001 degrees, converted to radians by dividing by the radians2degrees ratio.

Comment: We also accept other solutions based on the original version of the code.

Practical Question 2.6

Briefly describe your spoofing experiment. What effect do you see on the receiver's satellites? What is the sky plot? Press a button to change the position. Does it successfully change the position? How fast does the position change? During the experiment, did it trigger the jamming indicator and for how long?

Solution: After turning the spoofer on, the position changes. Similarly, the sky plot and the date/time are also different. Pressing the button updates the position live (by the amount specified in the previous question). Normally the jamming indicator does not trigger. Some fine-tuning of the power levels and/or a cold restart might be necessary.

Comment: Succeeding is not always straightforward and it also depends a bit on the setup. Some of you also had issues with the VMs. All of you have seen it working at least on the machine of another group and/or on the phones in the anechoic box. We give points independently of the success of the experiment. Overall, the point of these exercises was to see what it takes to conduct these attacks, and face the many practical challenges that occur when trying experiments in the real world (tuning of the gain, overflow/underflows when talking to the SDR, cold restart, etc.).

2.5 Discussion

Question 2.7

Briefly describe pros/cons (in a sentence or two) for relay, replay and signal generator (spoofing) attacks.

- Relay: easy, works on any signal (even encrypted), but it causes a clock offset that can be detected, if the position is very different it might cause an initial loss of lock and sudden jump in position. Only current time.

- Replay: similar to relay, without the disadvantage of streaming, but requires recording, might require a cold start. Only time in the past, which could likely be detected even with a relatively inaccurate time reference.
- Generator: the most flexible, signals can be transmitted also in advance avoiding the clock offset detection, but it does not work if we do not know something in advance (e.g., if the signal is encrypted), it can be synchronized for smooth takeover.

Comment: Two of the more important points to consider when comparing the attacks were cryptographic countermeasures (encryption/authentication) and time offsets. As a side note, while a relay attack shows (almost) the right date/time (as opposed to a date in the past for replay), since all signals are delayed, it can be detected as a sudden offset in the clock error if the receiver has a good time reference (see slides).

Question 2.8

Which of the discussed attacks would you think would work against authenticated Galileo messages and why/why not?

Galileo OSNMA authenticates the navigation messages using a delayed key disclosure scheme. Therefore, we assume satellite and transceiver have a notion of time slot in which a message is valid (before the next disclosure). The attacker cannot replay a message afterwards (when the key has been released). However, if a receiver has no notion of time from an accurate clock or out-of-band communication, the attacker could cold-restart the receiver and replay an entire sequence. The time-of-arrival of the signals is not directly authenticated. The attacker could slightly delay a signal and the navigation bits would still be valid. A relay attack is then possible. The unpredictability of the authentication bits makes it however impossible to generate/transmit signals in advance. (This has cryptographic guarantees, the MAC cannot be forged without knowing the key.) Hence, the generator attack is impossible.

Comment: Check the slides for a more in-depth discussion. Please note that timestamps are used in the TESLA scheme of OSNMA (e.g., to avoid pre-computing hash chains). Our description in the slides is (admittedly) simplified to focus on the core ideas. There exist attacks (Early-Detect Late-Commit and Forward Error Estimation) that allow to slightly advance even the unpredictable bits, but they were not covered in the class (only mentioned).

Question 2.9

What would you recommend to DoS the GNSS module inside a modern smart phone?

Solution: One approach would be to jam all constellations (e.g., GPS, Galileo, Glonass, BeiDou) on all bands.

Laboratory 3 Solution

Laboratory 3: Jamming Resistant Communication

3

Question 3.1

What are the benefits of DSSS? What are the disadvantages? What does the Processing Gain of DSSS mean, what is the formula for it?

Solution:

- Advantages: DSSS increases jamming resistance, provides shared access to the medium (if different spreading codes are used, which essentially results in *Code Division Multiple Access (CDMA)*), and is harder to intercept due to the lower Power Spectral Density (PSD).
- Disadvantages: DSSS requires more complex receiver implementations, and possibly long acquisition times (i.e. correcting for Carrier Frequency Offset, see GPS cold start).
- Processing gain formula: in dB: $10 \cdot log_{10}(c/b)$, where c is the chip rate and b is the bit rate. The processing gain is the difference in energy per frequency between the despread and the spread signal. Note that the accumulated signal energy stays the same. For example, if the spreading code is 2 bits long, then the signal's bandwidth is doubled when the signal is being spread, and again halved when it is being despread. Therefore, despreading doubles the energy per frequency (J/Hz) in this example (i.e. 3 dB gain).

Question 3.2

Assume that the jammer and the transmitter are at the same location. Express the J/S ratio of simple unspread QPSK, and spread QPSK (after post-processing) for narrow-band and wide-band jammers. Compare the J/S ratio of unspread QPSK with spread QPSK for both types of jammers.

Hint: Plug in the formula for the processing gain into the equation (6.1). When comparing the J/S of QPSK and DSSS for the wide-band jammer, do not forget to take into account the signal bandwidth.

Solution: The processing gain is 10log10(chip rate / bit rate) = 10log10(spread bandwidth B / narrow bandwidth b). PT and PJ are the powers of transmitter and jammer in dBm, respectively. We assume the wideband jammer has bandwidth B and the narrowband jammer has bandwidth b. We assume that distance and antenna gains are the same for legitimate transmitter and jammer, so they factor out in the formula. Then:

- Narrowband jammer, narrowband transmitter: J-S = PJ - PT (nothing special).
- Narrowband jammer, DSSS transmitter: J-S = PJ - PT - 10log10(B/b) (the legitimate signal is despread thus having a processing gain, the jammer is spread).

- Wideband jammer, narrowband transmitter: J-S = PJ - PT - 10log10(B/b) (only a part of the jamming signal hits the narrowband transmitter).
- Wideband jammer, DSSS transmitter: J-S= PJ - PT -10log10(B/b) (the legitimate transmitter is despread leading to a processing gain, the jammer is not despread).

Comment: We provide individual feedback for this answer, but please check this global solution as general reference.

3.1 Lab Setup

Practical Question 3.1

How did we reduce the bandwidth? Compute the bandwidth of the QPSK signal. Does the measured bandwidth confirm your computation? Explain why not if the two values do not agree.

Hint: you can use `QT GUI Sink` of the jamming USRP to observe the bandwidth of the transmission.

Solution: Given how the flowgraph is constructed, we can reduce the bandwidth by either reducing the sample rate or increasing the samples per symbol. Indeed, the symbol rate is 65536 [samples/s] / 8 [samples/symbols].

Comment: The expected bandwidth is a bit smaller than what we see on the spectrum, because in the real transmission we are also using additional frequencies (*excess bandwidth*) to shape the pulses and reduce *inter-symbol interference (ISI)*.

3.2 Jamming

Make sure the location and orientation of the antennas of the USRP devices is fixed for the rest of the exercises.

Practical Question 3.2

What are the data rates of these two modes of operations? Compare the lengths of the messages.

Solution:

The key point in this exercise is to realize the difference between symbols and chips. If, because of spreading, each symbol is made of n chips, then the symbols rate is equal to the chip rate divided by n. (As a side note, we could repeat the same code multiple times in the same symbols instead of increasing n.) If you fix the chip rate, then increasing the code length decreases the symbol rate. If vice versa you fix the symbol rate, increasing the code length increases the chip rate. And so on and so forth. It is easier to think about this for BPSK, where 1 symbol => 1 bit and symbol rate => bit rate. In our DSSS QPSK flowgraph the computations were less intuitive and made cumbersome by a bunch of transformation,

but the principle stays the same. We were lenient in the grading. Be sure to understand the main point explained here.

Practical Question 3.3

Which values for the jammer's Low Pass Filters are reasonable for narrow-band and wide-band jammer.

Solution: A simple solution is to have:

- Narrow band jammer: same occupied bandwidth as narrow band QPSK signal.
- Wideband jammer: same occupied bandwidth as the wide band DSSS signal.

These values would match the assumptions in the formulas in Question 3.2 and allow easy comparisons among the four cases. If the bandwdiths are not the same for DSSS and QPSK, it becomes harder to compare the cases without taking that into account.

Comment: In practice you do not have an ideal filter so you have to set a cut-off frequency and a transition width.

Narrow-band Jamming

No questions in this section

Wide-band Jamming

Practical Question 3.4

Report the values for the gain for all four combinations of DSSS/QPSK and narrowband/wideband jammer, for all BER values 0.025, 0.15, 0.4 that you have found in the previous exercises.

Comment: It is hard to collect accurate values with a non-fixed setup and limited time. Comparison between cases might be hard if you used different jammer bandwidths for QPSK and DSSS. The important point is that you observed (or made a guess) on the difference between the four scenarios.

Solution: Jamming a narrow-band signal with a narrow-band jammer is straightforward. Jamming a narrow-band signal with a wide-band jammer takes more power than with a narrow-band jammer, simply beacuse a lot of power is "wasted" outside the band of the victim. Jamming a DSSS signal without knowing the spreading code takes more power, because the legitimate signal has a processing gain. Indeed, the legitimate signal is despreaded. Instead, wideband noise is not despreaded and narrow-band noise is spreaded.

Practical Question 3.5

Find a way to decrease BER for DSSS for the same gain values of

the jammer and transmitter and the same chip rate. You can modify variables mentioned in the Section 4.3. Briefly explain what you did.

Solution: You have to decrease the BER. You cannot decrease the gain of the jammer, you cannot increase the chip rate. But you can still decrease the data rate to increase the processing gain. You can do by decreasing the message_per_second variable. You could also spread each data symbol with a longer spreading code. Finally, you could increase the transmit power or change the transmit frequency (but these were not really intended solutions). Decreasing the jammer bandwidth would also work (but it does not make sense from the point of view of the defender).

Practical Question 3.6

Compare your results with the theoretical results you formed at the beginning of the lab. Is simple QPSK more susceptible to jamming than DSSS?

Solution: Yes, QPSK is more susceptible to jamming while DSSS is more robust.

Comment: Even if you setup in the lab was not appropriate for accurate measurements and comparisons, it should have let you experience in practice how DSSS is definitely more robust to narrow-band interference than a narrow-band transmission.

Question 3.3

Look up a critical infrastructure which relies on wireless communication. How difficult would it be to jam it? Can an attacker with B210 USRP make an impact on the infrastructure? Look-up Tx power and bandwidth of the radio devices in your chosen infrastructures. Argue with the results you observed in this lab.

Solution: We accept any reasonably well explained example. It is important that you mention the range of frequencies that the USRP can cover, the bandwidth (also in relation to they type of jamming you need), the power of the legitimate transmitter and the modulation type, the output power of the USRP, you distance from the victim, and other similar considerations.

Question 3.4

Can you think of a way to send multiple parallel DSSS streams on the same carrier frequency with the same chip rate?

Solution: Yes. This is one of the advantages of DSSS. Each stream should use a different orthogonal code, hence it is called Code Division Multiple Access. Also see answer on the advantages of DSSS.

Comment: Please revise this in light of the lectures on DSSS and GNSS. We have seen that one spreading code C must have a good auto-correlation (correlation of the signal with itself has one single clear peak). This

way, the receiver can look for by cross-correlating a copy of C with the incoming signal. When we want to transmit at the same time on the same frequency, we must use two orthogonal codes C1 and C2. It means that their cross-correlation is low. This way, the receiver can cross-correlate the incoming signal with a copy of C1, and C2 will just look like noise. Vice versa, the receiver can cross-correlate the incoming signal with a copy of C2 and C1 will just look like noise. In other words, the two signals are orthogonal and can be separated and received independently even if they are sent at the same frequency at the same time.

Laboratory 4 Solution

Laboratory 4: Signal Overshadowing

4

4.1 Overshadowing

Question 4.1

Which cryptographic primitive can be used to detect overshadowing? Which physical properties of the received signal are affected by overshadowing? Is it possible to detect overshadowing based on physical properties of the signal?

HINT: you might want to come back to this question at the end of the lab, after having gained a practical understanding of this phenomenon.

Solution:

- *Which cryptographic primitive can be used to detect overshadowing?* Overshadowing aims at changing the message content. Therefore, cryptographic integrity protection, i.e., a Message Authentication Code (MAC) can be used for detection.
- *Which physical properties of the received signal are affected by overshadowing?* With overshadowing, at least a part of the genuine signal is, in essence, replaced by a stronger attacker signal. Thus, overshadowing increases the amplitude in that message part significantly. Furthermore, depending on how well-synchronized the attack is, changes in phase or even in frequency could be measurable.
- *Is it possible to detect overshadowing based on physical properties of the signal?* Monitoring the received signal's amplitude could be used to detect sudden changes. However, since such changes can have benign causes (e.g. passing by an obstruction, such as a building), it could be difficult to reliably distinguish these cases from attacks in practice.

Practical Question 4.1

Put the two USRPs close to each other. Observe how much gain the attacker needs to overshadow the original message. How does the capture effect work? You can consult the code for the `peak_selection` block in `https://github.com/kotuliak/gr-peak_selection/blob/master/lib/peak_selection_impl.cc`.

Solution: The capture effect works whenever the stronger of two signals determines the symbol decoded by the receiver. Note that the capture effect works differently for DSSS and non-spread QPSK (later question).

In the case of DSSS, a stronger attacker signal (that uses different data but the same spreading code) is despread by the receiver, but the higher power leads to a higher correlation peak. For the receiver, it intuitively

makes sense to consider the strongest of the correlation peaks, which is also what the code of the peak selection block does.

Question 4.2

Generally speaking, does the overshadowing attacker require more or less power than the noise jammer we considered in the last lab?

Argue whether we can use the overshadowing attacker as a generic jammer (against all DSSS signals with the same code length) too.

Solution: The overshadowing attacker requires *less* power because they know the spreading code. Thus, the attacker signal is being despread by the receiver along with the legitimate signal, and the attacker benefits from the processing gain.

The overshadowing attacker could only be used as a generic jammer if it knew the spreading codes of all n victim clients / UEs. However, since the spreaded messages would be completely different, the attacker would have to send all of them, essentially investing n times the power.

Without knowing the code, the attacker loses its power advantage. Under these conditions, it could only be used as a generic jammer if it sent with the same power like the noise jammer from last lab.

4.2 Hands-on experience with QPSK

Practical Question 4.2

Does the capture effect apply to QPSK as well? What would be the resulting IQ diagram for QPSK if two signals were transmitted at the same time under perfect conditions (perfect phase- and frequency-synchronization of both signals, no noise, etc.)?

Solution: Yes, the capture effect applies to QPSK as well, although it works differently than in the DSSS case. Here, the symbols of the genuine signal and the attacker signal can both be modeled as points in the I/Q plane. At reception, they are simply added together to form a new symbol (i.e. vector addition in the constellation plane), meaning the stronger symbol dominates the decoding. Sending two signals with similar power changes the standard QPSK constellation to one with 3x3 clusters: symbols with opposing I/Q signs create new clusters between them, leading to a high bit error rate.

4.3 Overshadowing attacks on LTE

Question 4.3

Which of the attacks (in AdaptOver) have been demonstrated to you? Shortly describe each attack and its impact. You can reference to diagrams in the respective papers.

Solution: We conducted the "Attack Reject" and "Service Reject" attacks, meaning we only attacked the downlink, i.e., the communication from the eNodeB to the UE. Although the attacks overshadow different messages, they are conceptually very similar: in both cases, the UE is made to believe that it is being rejected by the operator, leading to a temporary denial-of-service.

Practical Question 4.3

Can you distinguish adversarial messages from the benign messages?

Solution: *On the protocol layer*, there is no way to distinguish a malicious from a benign message due to the lack of cryptographic integrity checks. Of course the "Attach Reject" message in the log file suggests an attack in our scenario, but this message could also have been sent by the base station.

Practical Question 4.4

Think about the waterfall diagram you saw when observing the demo over the air. Based on that, were you able to distinguish the AdaptOver attacks from the normal operation? Do you think this could be used as a defense? Would it have some limitations?

Solution: The increased power in the frequency band of our LTE channel clearly suggests that an attacker manipulated the transmission within this short period of time. This should be clearly visible in the Waterfall diagram through a change of colors (i.e. a blue signal turning yellow or even red).

In theory, this can be used to detect overshadowing, but in practice it could be difficult for the receiver to clearly identify an attack. Even if the receiver managed to detect the attack, there is not much it can do.

For example, consider the following countermeasure: The receiver detects and demodulates a signal, then subtracts it from the reception, and repeats the procedure. By doing this, it could detect and demodulate the weaker, genuine signal too, and then simply reject the stronger one. However, if the attacker knew about this countermeasure, they could just transmit their signal at a *slightly lower power*. This would cause the receiver to reject the genuine signal, and to accept the injected one instead.

Question 4.4

Would classical Fake Base Station detection mechanisms [1–6] work against AdaptOver? Pick one of the paper mentioned - what does it look for, and would AdaptOver be detected in your opinion? **IMPORTANT:** remember that in our scenario the AmariSoft mini is the *real* base station, not the attacker.

Solution: No, traditional fake base station detection mechanisms won't work. On a high level, the reason is that the attacker behaves not at all like a fake base station, but rather overshadows only specific messages sent to the target device in a directional manner for surgical manipulations.

Question 4.5

Are the adversarial messages used in the overshadowing attacks against LTE authenticated? Why?

Solution: They are not authenticated, because the base station and the device do not share a secret key yet at this stage of the protocol. Furthermore, there is not Public Key Infrastructure (PKI) for base stations that would allow cryptographic signatures. The reason is mainly the complexity of the global cellular infrastructure.

Note that authenticating or signing these messages would not prevent DoS attacks reliably, because any overshadowing-induced bit flip would cause integrity checks to fail. However, the protocol-level DoS attack shown in this lab (e.g., the device not trying to connect anymore assuming it has been rejected by the operator) would not be possible anymore.

Bibliography

[1] CellularPrivacy. *CellularPrivacy/Android-IMSI-Catcher-Detector*. Last accessed: 07.12.2020. Dec. 2020. URL: https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector (visited on 12/07/2020) (cited on page 24).

[2] Cooper Quintin. *Detecting Fake 4G Base Stations in Real Time*. Published: DEF CON, Last accessed: 07.12.2020. 2020. (Visited on 12/07/2020) (cited on page 24).

[3] Adrian Dabrowski et al. 'IMSI-catch me if you can: IMSI-catcher-catchers'. en. In: *Proceedings of the 30th Annual Computer Security Applications Conference on - ACSAC '14*. New Orleans, Louisiana: ACM Press, 2014, pp. 246–255. DOI: 10.1145/2664243.2664272. (Visited on 12/07/2020) (cited on page 24).

[4] Zhenhua Li et al. 'FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild'. In: Jan. 2017. DOI: 10.14722/ndss.2017.23098 (cited on page 24).

[5] Thanh van Do et al. 'Detecting IMSI-Catcher Using Soft Computing'. en. In: *Soft Computing in Data Science*. Ed. by Michael W. Berry, Azlinah Mohamed, and Bee Wah Yap. Vol. 545. Series Title: Communications in Computer and Information Science. Singapore: Springer Singapore, 2015, pp. 129–140. DOI: 10.1007/978-981-287-936-3_13. (Visited on 12/07/2020) (cited on page 24).

[6] Prajwol Kumar Nakarmi and Karl Norrman. *Detecting false base stations in mobile networks*. en. Last accessed: 07.12.2020. June 2018. URL: https://www.ericsson.com/en/blog/2018/6/detecting-false-base-stations-in-mobile-networks (visited on 12/07/2020) (cited on page 24).