Last Name: **lastname**

First Name: firstname

Student ID: studentid

Security of Wireless Networks AS2021

(252-1411-00L)

Srdjan Capkun, Kari Kostiainen

Examination Rules:

1. **DO NOT TURN OVER THIS PAGE UNTIL INSTRUCTED TO DO SO BY AN EXAMINER!**
2. Closed-book, written exam, 90 minutes total.
3. Check that the name on your exam is correct.
4. Put your Student ID card visible on the desk during the exam.
5. No books, no calculators, no computers or communication devices are allowed. Turn off your mobile phone.
6. If you need more space for your answers, blank pages are available upon request. Please write your name and legi number on the extra pages you received.
7. Write with a non-erasable black or blue pen (no pencil, no green or red color). Don't use correction fluid (e.g. Tipp-Ex). Answers will only be evaluated if they are readable.
8. If you feel disturbed, immediately call an assistant.
9. Wear your mask over mouth and nose and remove it only to eat or drink.
10. You are permitted to leave the exam early, but not within the last 10 minutes of the exam. If you wish to leave, please raise your hand and wait for an assistant.

Question	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Total**
Points	10	8	14	10	13	14	8	7	6	90
Score										

1. Physical Layer

(a) (3 points) Consider a signal $x(t) = a(t)\cos(\phi(t))$ and its analytical representation $x_a(t) = a(t)e^{i\phi(t)}$. Complete the diagram in Figure 1 by showing:

i. The amplitude.

ii. The phase.

iii. The in-phase and quadrature components.

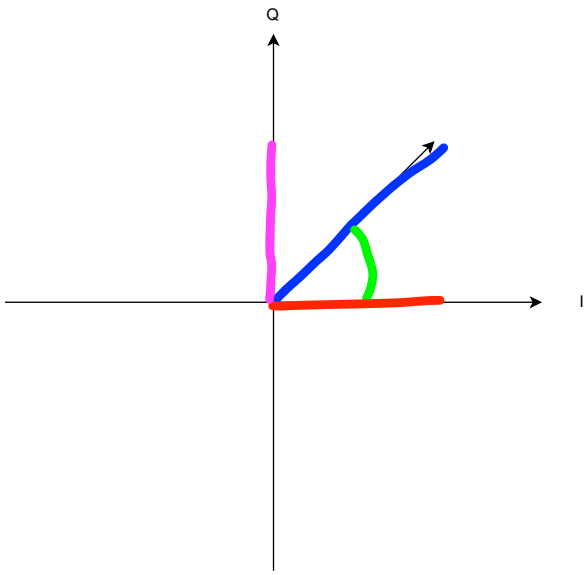


Figure 1: Analytical Signal

(b) A baseband signal $x_{baseband}(t) = a(t)\cos(\phi(t))$ is upconverted to carrier frequency f_c, becoming $x_{RF}(t) = a(t)\cos(2\pi f_c t + \phi(t))$, with f_c=125MHz. Figure 2 shows the spectrum of the baseband signal in the frequency domain.

i. (2 points) Complete the figure by drawing the spectrum of the upconverted signal. Highlight carrier frequency and occupied bandwidth.

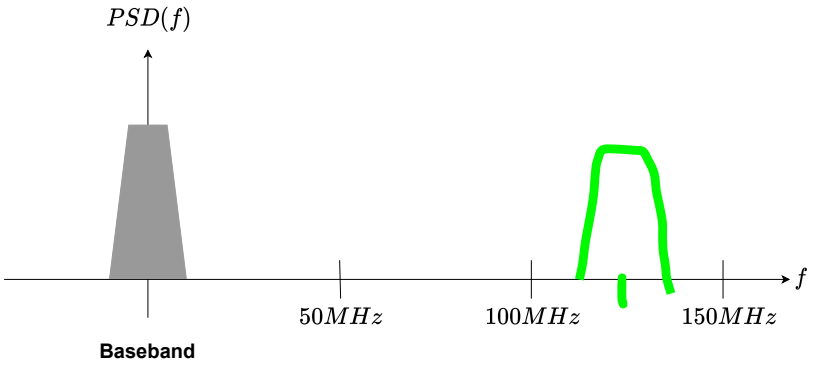


Figure 2: Upconversion

ii. (1 point) Why is upconversion necessary for radio communications?

Mainly for two reasons:
1) To enable simultaneous transmission of different signals by using a different carrier frequency for each in the upconversion
2) To transform a complex signal into a real one, since only real signals can be actually transmitted.

iii. (1 point) What component is used to upconvert a signal?

The baseband signal is converted to a passband signal by multiplication with a radio frequency carrier. The component is called quadrature modulator

(c) (3 points) Figure 3 shows three different types of digital modulation. For each of the three modulation schemes, complete the figure as follows:

i. Write the name of the modulation scheme.

ii. Identify the beginning and the end of each symbol.

iii. Associate a bit to each symbol.

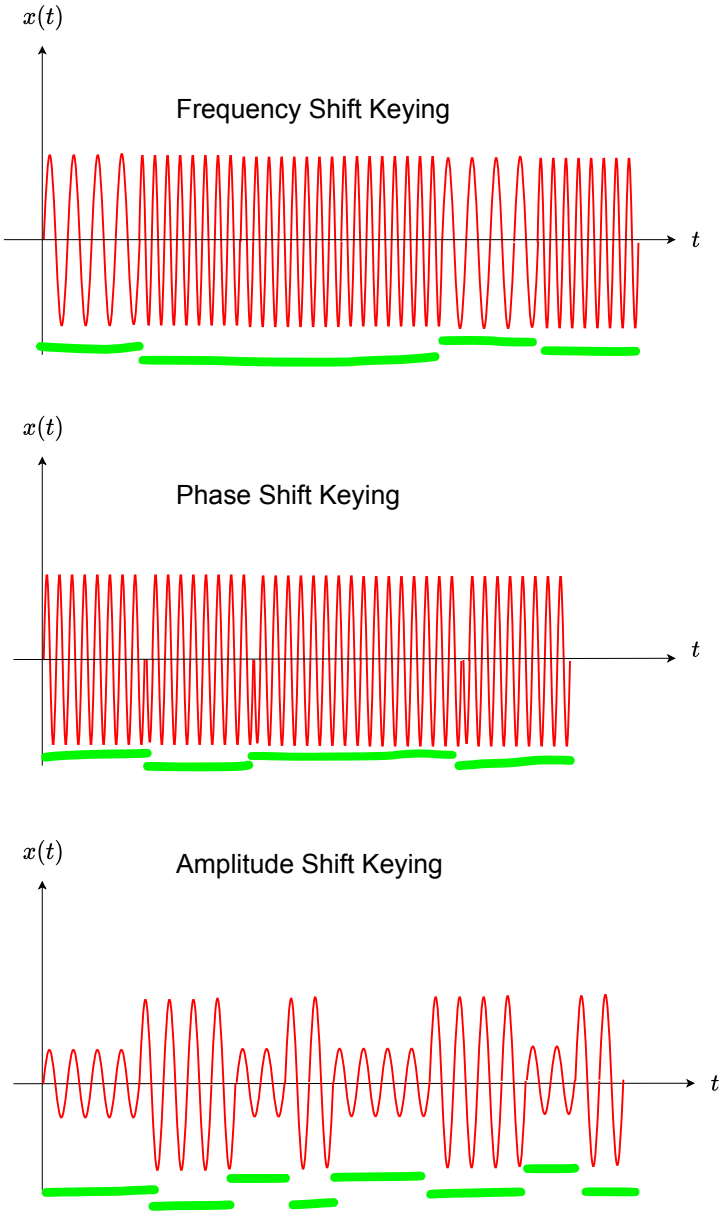


Figure 3: Digital Modulation

2. Physical Layer Security

(a) (2 points) The wireless channel is location-dependent and reciprocal. Can those properties in general be used to authenticate a user in a mobile environment? Explain how, or why not.

Not really, because with relay and replay attacks the attacker could fake its position.

(b) Integrity codes

i. (2 points) Briefly describe how integrity codes are modulated (i.e., how each bit is represented and demodulated at the receiver) and why.

Each bit is encoded using Manchester encoding and then transmitted using OnOff keing.
At the receiver, given a threshold to distinguish between one and zero, the signal gets demodulated and considered valid if the hamming weight (the number of non-zero bits) is equal to half of the number of transmitted bits.

ii. (2 points) What is the hardness assumption for integrity codes to be secure against a physical layer attacker?

The attacker cannot block the legitimate signal from reaching the receiver antenna.
Also, it needs to be hard to annihilate 1 bits, (turning bits with value 1 into bits with value 0 by “guessing” the random signal -different from zero- to encode bit 1)

iii. (2 points) Why is it important that the user knows to be close to the legitimate transmitter?

Otherwise the attacker would be able to inject whatever he wants??

—to have a defined noise floor

3. Jamming

(a) (1 point) What is the essential mathematical operation to decode a DSSS signal that is below the noise floor?

Correlation

Let's assume an honest transmitter and receiver are using DSSS to communicate with each other. In DSSS, every bit of the message is spread with a spreading code of length L over the bandwidth B. The adversary, who does not know the spreading code, wants to jam their communication. All three parties are using the same model of software defined radio with the same model of an omnidirectional antenna. The distances between all three are equal. The adversary is transmitting gaussian noise on the same frequency with bandwidth B. The bit error rate of the DSSS transmission between the transmitter and the receiver under the current conditions is the BER.

(b) (2 points) The adversary increases the bandwidth of the gaussian noise and keeps the same overall signal power. What is the impact on the BER of the legitimate DSSS transmission? Briefly explain why.

BER decreases, since transmitting over a larger bandwidth with the same power results in a lower overall amplitude

The transmitter and the receiver increase the chip rate by using a longer spreading code, while keeping the message bitrate constant. The new bandwidth is B'.

(c) (2 points) Is $B' = B$, $B' > B$, or $B' < B$?
What about the processing gain, does it stay the same, increase, or decrease?

B'>B, a signal with a higher variance in time occupies a larger bandwidth. The processing gain (chip rate/information bit rate) increases, more chip bits for the same information bits.

(d) (2 points) The adversary changes the bandwidth of the gaussian noise from B to the new bandwith B' while also increasing his Tx power. How much does the adversary needs to change the gain to keep the BER same as before? Express it in decibels in terms of B and B'.

BER = B/tx
BER2 = B'/tx'
BER = BER2 -> tx' = tx*B'/B

ratio = tx*B'/B

new gain = 10log_10 (ratio)

(e) (2 points) What are the consequences if the adversary learns the spreading code? Devise a strategy how the adversary can jam the signal more effectively. What J/S does it need to be successful?

By knowing the spreading code, he can avoid wasting power on frequencies that, after despreading, would be discarded and focus on the narrowband.
He could create a narrowband jamming, spread it with the spreading code and send it with all the power he has, so that all of it would be received by the legitimate receiver.
Usually, a J/S >= 0 yields a successful jamming.

(f) (2 points) Expain how the transmitter and the receiver can communicate in presence of a jammer without a pre-shared secret.

There are two techniques commonly used, Frequency hopping spread spectrum and Direct sequence spread spectrum. Both have the “uncoordinated” version, which saves the need of pre-sharing secrets, at a cost of a lower information rate with respect to the same bit/rate.

(g) (3 points) Give an idea how the transmitter and the receiver can generate a dynamic spreading code which changes frequently, given they agreed on a pre-shared secret. Identify pros and cons of your aproach.

They could use a random generator function and the pre-shared secret as a seed.
This would let them have the same “random” output and it’d be easy to implement and use.
However, if the secret is not long enough it could be bruteforced by the attacker, making the whole thing useless. Same thing if it gets leaked. Also, it wouldnt be forward secret.

4. GNSS Security

(a) (4 points) Briefly describe how civilian GPS works and what its main vulenerabilities are.

It's goal is to estimate one's position on earth. It consists in an artificial constellation of satellites in the sky and uses triangulation to determine the position of the receiver.
The satellites use radio signals to trasmit the time and their position. Using the time of flight (the time needed for the signal to reach the receiver, at the speed of light), the receiver can then compute its distance from the satellite.
With data from at least 4 satellites, the receiver can estimate both time (time error wrt precise satellite clocks) and position. The more satellites you have, the more precise the result is.
Civilian gps uses L1 band at around 1,6 GHz with C/A (coarse acquisition) codes, which allow for a very slow data rate. These codes are publicly known, which means that everybody would be able to craft arbitrary signals, which would be considered totally valid by any receiver.
The signal gets to the receiver with very little power, 16 dB below thermal noise, but since it uses DSSS, the receiver is able to obtain the narrowband signal, which is well above the noise floor.
Possible attacks are jamming, changing the message or time of arrival leading to incorrect position, the signal can also be canceled by sending a perfectly sincronized copy of the signal, but with a 180 degree phase offset.

(b) Explain how Galileo OSNMA works, in particular:

i. (2 points) Sketch a simplified explanation of what satellites and receivers do to guarantee that messages are authenticated

Notes: time delayed auth doesnt prevent replay or relay but prevents generation of arbitrary signals.
there is no confidentiality and it assumes that transmitter and receiver are sincronized.
The satellite chooses a value Kn randomly, hashes it n times to obtain a chain and then starts sending messages Mi, Ki-1, MAC(Mi, ki). Ki can only be used once, and it will be disclosed (once no longer valid) in the following message so that the receiver can know that it was sent by the legitimate person

ii. (2 points) Explain why this solution was chosen over other symmetric or asymmetric cryptographic protocols

Symmetric crypto needs the same key on every receiver, and you can't trust it to stay secret (if it gets disclosed it's totally useless)
Asymm crypto doesn't work because signatures are too long and don't fit in the limited bandwidht, also computationally expensive.

iii. (2 points) Briefly mention whether certain classes of attacks are not defeated by OSNMA and why.

It's possible to anticipate a signal (through early detect late commit), also delaying a signal is possible, but detectable with a clock offset test.
This is because OSNMA authenticates the message, but not it's integrity nor the origin so replay/relay attacks are still doable.

5. Secure Ranging

(a) (3 points) What is a distance commitment in the context of UWB ranging? Why is it used?

Distance commitment is the Time of Arrival measured over a public preamble and then verified using payload pulses generated using UWB pulse reordering. The timing of the preamble is binding. An attacker needs to advance payload if he advances the preamble. It's the way of knowing the distance between transmitter and receiver.
As the attacker needs to advance the payload as well, he needs to guess and send before the legitimate pulse arrives, which gives him immediate feedback, and the attacker can then adjust the subsequent pulses in order to reach the needed net energy level.

(b) (10 points) Consider a physical layer for secure ranging that uses burst position modulation. This technique represents each bit by transmitting a burst of pulses in either of two consecutive intervals, each of duration T_{Burst}. An example for such a symbol is provided in Figure 4. The receiver integrates the signal power in both intervals and detects Bit 0 if the first interval contains more energy than the second, or Bit 1 otherwise.

The goal of this task is to evaluate this system against an external distance-reducing attacker (early-detect/late-commit). You can assume the attacker to have a negligible reaction time.

i. Sketch a possible physical-layer attack strategy for distance reduction.

ii. Provide an estimate on how much (timewise) an attacker can at most advance the signal time of arrival, as a function of T_{Burst}.

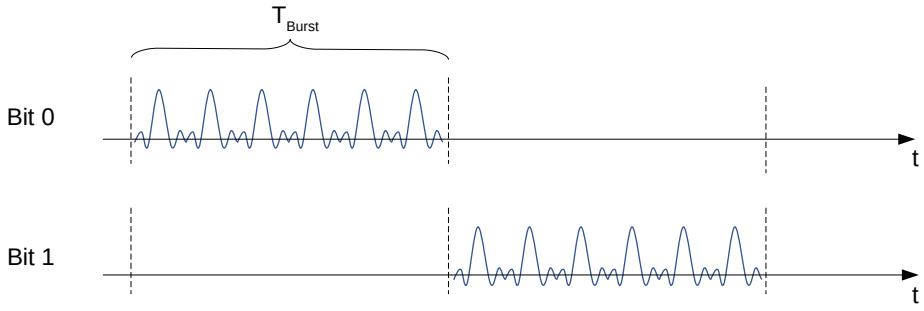
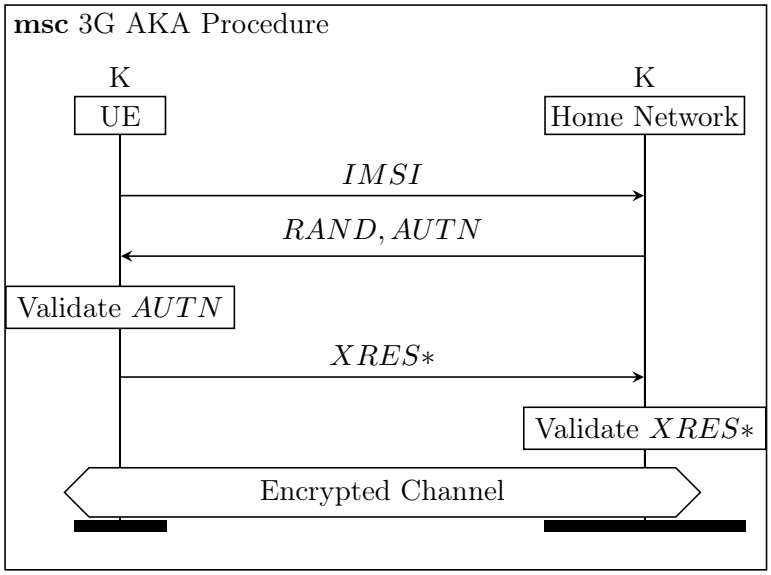


Figure 4: Burst position modulation

6. Cellular Security



(a) (4 points) From 3G onwards, the AUTN parameter in the AKA procedure contains, amongst other things, a concealed sequence number. In the UE, it is checked that this sequence number is always increasing with every authentication attempt. Describe what attack this sequence number check prevents.

It prevents replay attacks, because a message can only be considered valid until the following one is sent out. For example, a fake BS might want to convince a UE to connect to itself by sending a legitimate message originally sent by a legitimate BS. This is no longer possible because the UE is keeping its own SQN to compare to the one received.

(b) Imagine your LTE phone was stolen. Luckily, you happen to know its IMSI. Moreover, your friend agrees to let you use his network of passive LTE uplink sniffers distributed around Zurich. You know that the phone is turned on, in reach of an uplink sniffer, and (re-)attaches periodically.

i. (2 points) You captured every Attach and Service Request of every phone in the city for the last 2 days. However, none of those contained your IMSI. Explain briefly why.

It's not contained because those requests use the TMSI, a temporary identificator, in place of the IMSI.

ii. (4 points) Your friend reveals that his network consists of software-defined radios and is thus capable of receiving and transmitting arbitrary IQ samples. Briefly describe an attack that will allow you to capture the IMSI of your phone and thereby find out to which base station your phone is connected to.

During both the attach and service requests, an attacker can use an LTEProbe (an uplink/downlink passive sniffer) to intercept messages and AdaptOver (an overshadowing attack). The attacker needs to send a perfectly alined "Identity request" message to any security or attach requests from the UE, causing it to send its IMSI.

iii. (4 points) Assume your phone uses 5G only, and instead of the IMSI, you know the SUCI of your phone. Describe how you can find out to which base station your phone is connected to, using the same network of SDRs as described in (ii).

Similarly to the IMSI Catcher, there it is possible to create a SUCI Catcher. The SDRs could MiTM and use the UE as an oracle to verify which SUCI corresponds to which SUPI by trying out different SUCIs and forwarding the Serving Network response. If the UE sends a RES* then the SUPI guessed is the correct one, otherwise it isn't.

7. WiFi Security

(a) (3 points) Imagine you share one 802.11ac WiFi access point with a lot of other clients. You want to upload an important file as fast as possible, preferrably taking all the available bandwidth, no matter if the other clients get very little or none at all. How can you do this?

I could modify the driver of my wifi card such that the backoff time is always zero, which means that I would use the channel as soon as it becomes free

(b) (5 points) There is a WPA3 802.11ac WiFi access point, whose firmware has never been upgraded. You are the adversary, with no control over the access point and no knowledge of any keys. With what attack can you inject arbitrary IP packets on the connection? What is your required setup and what actions does the victim need to do for your attack to be successful?

A FragAttack consists in flipping an (unauthenticated) bit in the frame header, which will result in the receiver thinking that the packet received is composed of multiple packets. This has been used to inject arbitrary frames inside of it.
The attacker needs to MiTM the victim and the IP, by forcing the victim to connect to the attacker, or anyways have a way to modify the traffic.

The victim needs to connect to a server under the attacker's control, and this can be done with social engineering/sending email with malicious attachments, etc…

8. Bluetooth Low Energy (BLE)

(a) (3 points) Imagine your BLE fitness tracker was stolen. As in question 6b, your friend got you access to a city-wide network of SDRs. It is collecting the MAC address of all BLE advertisements for you. Your fitness tracker is using random resolvable address randomization, and you know the LTK between your phone and the fitness tracker. How can you find amongst all advertisements the one advertisement that comes from your fitness tracker?

During the first pairing, my fitness tracker agreed on a Identity Resolving Key with my device, which allows it to find it and connect it. I can compare it to the ones collected with the BLE advertisements

(b) (4 points) Explain the high level idea behind the Method Confusion Attack in BLE with all the involved parties. As a user, how can you defend against the Method Confusion Attack?

The method confusion attack consists in a MiTM attack, where the attacker uses one association method with one device and another one with the other. Since the “pins” or keys used in the association are stored in the same variables, different methods are techincally compatible with each other.
As a user, I can make sure that both devices are using the same association method.

9. True or False

Instructions
Answer each question with *True* or *False*. No answer will result in 0 points, a correct answer +1 point, an incorrect answer -1 point. At the minimum, you'll get 0 points from all true-false questions together.

(a) (1 point) The higher the variability of a signal in the time domain, the smaller its bandwidth in the frequency domain.

(b) (1 point) Unspread communication is less resistant against a wide-band jammer compared to a spread signal.

(c) (1 point) With Galileo Open Service Navigation Message Authentication (OSNMA) in place, an attacker is never able to transmit signals in advance because some bits transmitted by the satellites are unpredictable.

(d) (1 point) In a WEP network, an attacker does not need to transmit anything to determine the plaintext of all messages.

(e) (1 point) In 5G, due to the SUCI catcher attack, an attacker can still figure out what the SUPI was.

(f) (1 point) Using the LTrack attack, you can determine an unambiguous position of a UE with 2 uplink sniffers.

False (because we need 1 uplink and 1 downlink sniffer — LTEProbe

Extra space for your answers