Last Name:

First Name:

Student ID:

Security of Wireless Networks AS2020

(252-1411-00L)

Srdjan Capkun, Kari Kostiainen

Examination Rules:

1. Written exam, 90 minutes total.
2. No books, no calculators, no computers or communication devices.
3. Write all your answers on this document, space is reserved for your answers after each question. Blank pages are available upon request.
4. Put your Student ID card visible on the desk during the exam.
5. If you feel disturbed, immediately call an assistant.
6. Answers will only be evaluated if they are readable.
7. Write with a black or blue pen (no pencil, no green or red color).

Question	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**Total**
Points	6	8	19	7	4	7	6	11	10	7	85
Score											

This page intentionally left blank

1. Wireless Basics

(a) (2 points) Does a wireless channel, in general, affect all frequencies of a signal equally? Explain.

It depends on what kind of noise/interference is present on the channel. If it's general thermal noise, then yes, all frequencies will be generally affected in a similar way. However, if there are other communications happening, then the frequencies used by those transmissions will have a greater noise level.
Also, higher frequency signals suffer from greater attenuation due to the distance travelled compared to lower frequency signals.

(b) (2 points) Which two properties of the wireless channel are leveraged by systems that rely on those for physical-layer based key establishment?

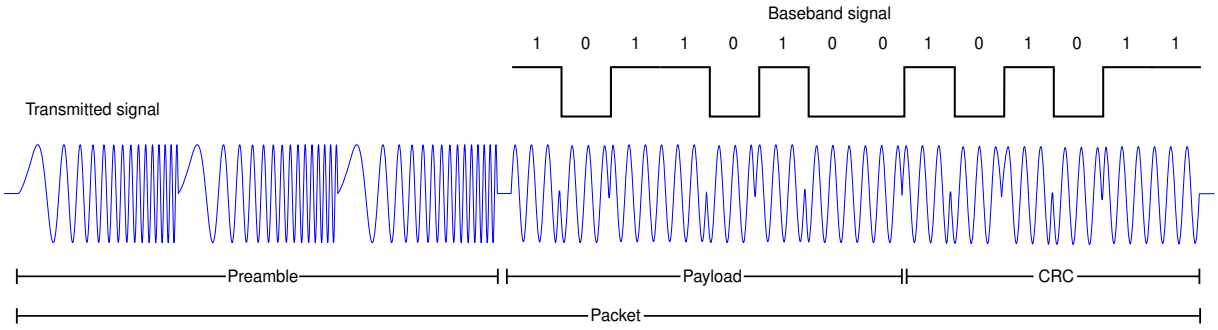
One can use channel impulse response and received signal strength.

(c) (2 points) As part of this course, you evaluated a cantenna that extends the range of a WiFi connection, operating in the 2.4GHz band. If you were to use the same device for the LTE band at 700MHz, would you expect it to work equally well? Explain.

Not so much, since antennas then to work well only on a subset of the whole frequency spectrum.

2. Jamming

Consider a wireless communication protocol that operates on a 5 MHz wide channel at a carrier frequency of 1.5 GHz. Every packet contains a static preamble for synchronization, variable payload and cyclic-redundancy-check (CRC) for error correction. The preamble consists of three linear frequency sweeps that span the entire channel of 5 MHz. The data-bearing part of the packet is encoded with BPSK (binary phase shift keying). Every packet contains random data. The frequencies shown in the figure below are not drawn to scale.



In order to jam such a wireless protocol, an attacker could deploy a constant blanket jammer to cover the entire 5 MHz channel and drown all packets.

(a) (4 points) Identify two other jamming approaches. Write down how your jammers work and describe their emitted signals.

One could keep sending preambles at a higher power so that the receiver doesn't know when to connect. (meh)
Another one could be syncronizing to the legitimate signal using the preamble and then overshadowing the CRC with something wrong.
The last one I can think of is destructive interference. Syncing using the preamble and then emitting the legitimate signal, shifted by 180°, so that nothing should reach the receiver.

(b) (4 points) Compare your approaches to blanked jamming in terms of J/S value, effectiveness and jammer complexity. A comparison in words is sufficient (no mathematical analysis required).

Overshadowing need far less power than blanket jamming but is more difficult/complex because we need to very closely synchronised in time.

Destructive interference demand even less because we have J/S =1 for it to work, but its even more complex because we need to be time synchronised but also we need to have a J/S that is really close to 1.

??

3. Cellular Security

(a) (3 points) What capabilities does an adversary need to perform location tracking on a 4G network?

He needs to get a hold of the IMSI of the UE. This can be done overshadowing a legitimate message after a service or attach request with a Identity Request message, to which the UE will happily reply with its IMSI.
Or he can use two passive base stations to record the propagation delay.

(b) (3 points) Describe the security requirements (Authentication, Encryption and Integrity) for the control and user plane in 4G. What does the standard prescribe/recommend? Do the operators follow those recommendations?

Authentication is required in both the control and user plane, encryption is optional for both but often used, integrity is mandatory for control plane but not user data

(c) (2 points) Imagine a group of hackers manages to (fully) compromise the Serving Gateway of a 4G service operator. List two different possible attacks on user privacy that the hackers are able to launch.

Leaking the IMSI and thus tracking the end user easily, just by sendind a Identity request.
2 ??

(d) (3 points) Describe the effect of increasing or decreasing the sub-carrier spacing in an OFDM modulated signal. Assuming the overall bandwidth of the channel stays the same, how does the sub-carrier spacing affect **Symbol length**, **Throughput** and **complexity of the receiver**?

increasing sub carrier spacing decreases symbol length because it increases symbol time
A longer symbol length makes it more resilient against multipath interference, but it probably needs a more complex receiver.
Throughput should stay the same

(e) (2 points) In the 4G resource grid, the primary and secondary synchronization signals (PSS, SSS) occupy only one symbol (in time) but they cover a very wide frequency range. Why are PSS and SSS allocated in such a way? What does this mean for a jammer if the goal was to block just these signals in order to mount a denial-of-service attack on the cell?

By making it occupy only one symbol in time, it'd be hard to selectively jam it, and also, since it's transmitted over a very wide frequency range, the power needed to properly jam it is higher.
The jammer would need to start jamming as soon as it starts receiving the SS, and also have a lot of power available.

(f) (2 points) Briefly explain what the TMSI (Temporary Mobile Subscriber Identity) and RNTI (Radio Network Temporary Identifier) are and describe one way how an eavesdropping attacker could link TMSIs and RNTIs of different UEs.

They're temporary identifier, meaning that they change rather frequently and their goal is to reduce the times the actual identifier is disclosed. "RNTI is used to indentify one specific radio channel from other radio channel and one user from another user". Operator assigns temporary identity (TMSI) and it's changed according to the operator policy.

Maybe eavesdropping the RRC connection request and setup

(g) (1 point) Why does the modulation on the uplink of 4G not use standard OFDM/OFDMA similar to the downlink. Give at least one reason.

For the LTE uplink, a different concept is used for the access technique. Although still using a form of OFDMA technology, the implementation is called Single Carrier Frequency Division Multiple Access (SC-FDMA).

One of the key parameters that affects all mobiles is that of battery life. Even though battery performance is improving all the time, it is still necessary to ensure that the mobiles use as little battery power as possible.

With the RF power amplifier that transmits the radio frequency signal via the antenna to the base station being the highest power item within the mobile, it is necessary that it operates in as efficient mode as possible. This can be significantly affected by the form of radio frequency modulation and signal format.

Signals that have a high peak to average ratio and require linear amplification do not lend themselves to the use of efficient RF power amplifiers. As a result it is necessary to employ a mode of transmission that has as near a constant power level when operating. Unfortunately OFDM has a high peak to average ratio.

While this is not a problem for the base station where power is not a particular problem, it is unacceptable for the mobile. As a result, LTE uses a modulation scheme known as SC-FDMA - Single Carrier Frequency Division Multiplex which is a hybrid format. This combines the low peak to average ratio offered by single-carrier systems with the multipath interference resilience and flexible subcarrier frequency allocation that OFDM provides.

(h) (3 points) Explain how the ReVoLTE attack works. Don't forget to include how an adversary would launch such an attack in the wild. Is a sniffer required? If so, what traffic needs to be eavesdropped? Describe the attack in about 6 sentences.

It uses a vulnerability where the same input parameters to the encryption algorithm are used in case of multiple calls over VoLTE done by the UE when connected to the same base station. So, two VoLTE calls are encrypted using the same keystream.
The attacker records first call. Then he calls the victim and records both plaintext and ciphertext. Now he has the keystream, which he can use to decrypt the first call.
He does need a sniffer because he needs to record calls.

He needs to eavesdrop the first call.

4. GPS

(a) (3 points) Assume a next-generation civilian GPS that uses TESLA, without any further changes to the system. Is the system secure? Explain.

No, it would only be secure against spoofing with illegitimately crafted signals, but it wouldn't be protected against relay/replay attacks.

(b) (2 points) List the assumptions behind the security of Kuhn's scheme against a distance-modifying attacker.

The receiver needs to be loosely synchronized with the satellite (otherwise the attacker would get a chance of using the key while it's still considered valid by the attacker)
Requires pre shared public satellite keys

(c) (2 points) Assume a terrestrial positioning system that replicates Kuhn's scheme. Are the security guarantees the same as for a satellite positioning system that employs it? Explain.

5. Signal Integrity and I-codes

In the lecture, we discussed a version of I-codes (integrity codes) that encode the raw bits with Manchester-encoding and then transmit the encoded bits using OOK (on-off-keying).

(a) (4 points) Can I-codes be implemented with PSK (phase-shift-keying) modulation? If so, write down the construction. If not, state the reasons why such a scheme would be insecure.

It'd be possible, but not advisable since it would not be secure. OOK of a Manchester encoded stream allows the receiver to check whether the transmission has been tampered with by looking at the number of 0s and 1s, and, since an attacker could only turn 0s into 1s but not viceversa, n 0s = n 1s.
PSK on the other hand wouldn't stop an adversary from turning 1 into 0 and 0 into 1

6. Broadcast anti-jamming

(a) (1 point) Under which assumption is frequency hopping based on a (pre-distributed) group key not sufficient against a jammer in a broadcast scenario?

the attacker cannot guess the next-hop or detect-and-jam
also, he must not know the pre shared key

(b) (2 points) Can the use of public-key infrastructure (for establishing a shared hopping sequence or spreading code) by itself prevent a jamming attack by an outsider? Explain.

No, it would lead to a circular dependency cycle, where, to establish the keys, you need a secure channel.

(c) (2 points) In Uncoordinated DSSS, the receiver is uncertain about the spreading code used by the transmitter. How is communication achieved?

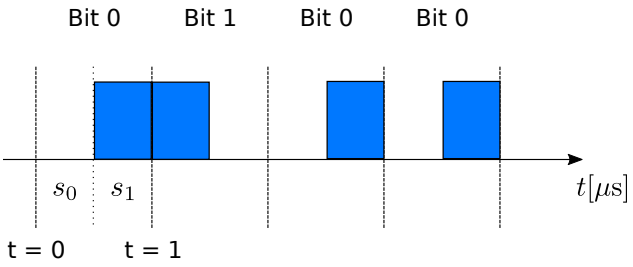
There is a public finite set of possible spreading codes. Just trial and error until he finds the correct one

(d) (2 points) What is the advantage of using a large codeset in UDSSS? What is the disadvantage?

The advantage is that it will be harder for the attacker to jam. The disadvantage is that the receiver will waste more time trying to find the correct spreading code, so the actual throughput will be lower

7. Pulse-position modulation

Pulse-position modulation is a modulation technique that encodes bits by allocating signal energy to one of two possible time slots s_0 or s_1 of equal duration. Here is an example of this modulation for four bits:



In the following, we assume an ideal communication channel (without noise).

(a) (2 points) A simple technique for demodulation at the receiver is to compare the energy in both slots and declare a bit 1 if $E(s_0) > E(s_1)$ and bit 0 if $E(s_1) \geq E(s_0)$. This technique is vulnerable to a reactive attack on message integrity. Assume the attacker cannot annihilate the signal (i.e., the phase being randomized). Explain the attack. What is the attacker's requirement on reaction time?

He needs to transmit enough energy in the s0 slot in order to be able to inject a 1

(b) (2 points) How can the demodulation at the receiver be improved to prevent physical-layer attacks on the integrity of one particular message?

It could check for the variance in the high slots and discard the message if that's too high, or check if the hamming weight of the message is |m|/2 since teoretically the number of highs and lows are equal.

(c) (2 points) Consider an air-traffic control scenario, where an airplane periodically sends messages to ground control stations, using pulse position modulation (with randomized phase). In the scenario, would this modification (part b) be enough to counteract spoofing attacks? Explain.

No, one could craft seemingly legitimate signals by always using the same amount of energy in each symbol

8. Distance Bounding

(a) (2 points) What is the wormhole attack? How can an adversary use it to reduce the accuracy of the ranging systems such as contact tracing system?

In a wormhole attack, the attacker receives signals in one point of the network, tunnels them to a different location and replays them back into the network (see here).

Using such an attack, an adversary could trick a contact tracing system into thinking an infected person is near (for example in the case of COVID).

(b) (3 points) Suppose you are assigned a task to design a secure ranging system, and you have full control of the physical and logical layer. Propose a physical layer design, with the checks you will apply at the receiver to prevent distance manipulation attacks.

I would check if the direction from which the signal is coming is the one i expect
use distance commitment to set an upper bound
use nonces in order to avoid replays

(c) (2 points) Why does reducing the spacing between pulses (as in HRP STS) affect the UWB ranging system's security?

By reducing the spacing between pulses, the system gets more susceptible to inter-pulse-interference, which in turn results in more noise. This additional noise makes it more difficult to find the Early Path, which is required to get the correct time of arrival, therefore making the system less reliable (and less secure).

(d) (3 points) For the UWB long symbols, why is randomizing pulse polarity not sufficient to achieve secure ranging? Why is randomizing both pulse polarity and position helpful in realizing a secure ranging system?

we need to hide from the attacker the actual position where the symbol starts

(e) (1 point) How can you reduce effective symbol duration (where energy is aggregated) for the OFDM symbols?

(f) (1 point) Why does the use of wider subcarrier reduces latency of the OFDM based ranging system?

9. WiFi Security

(a) (3 points) Explain two approaches that an attacker can use to prevent communication between the WiFi client and access point.

keep triggering carrier sense
modify card driver so that the attacker has 0 backoff time

(b) (4 points) What is the ChopChop technique? How does is compromize security of the WPA/TKIP operation?

It's a techinque which allows the attacker to obtain the original plaintext of the message one byte at a time, using the AP as an oracle

(c) (2 points) What vulnerabilities of the WPA2 protocol does an attacker exploit in the key reinstallation attack?

If the AP gets no response to the third message in the handshake, the AP retransmits it and each time the client reinstalls the same PTK.
So the attacker does a MiTM and blocks MSG4, triggering the retransmission of MSG3, and thus a key reusage of a key that should be used only once, allowing partial or complete decryption of all packets.

10. True or False

(a) (1 point) In broadcast anti-jamming based on frequency hopping (with a shared secret), the transmitter randomly selects among frequencies known to all receivers.

(b) (1 point) In a DSSS system, a lower chip rate is associated with higher processing gain.

(c) (1 point) Using UDSSS for establishing a secret DSSS sequence allows for quicker decoding and, hence, longer messages.

(d) (1 point) The enodeBs (base stations) in an LTE network are not mutually authenticated with the UEs.

(e) (1 point) The home subscriber server (HSS) in LTE receives the authentication vector from the UE.

(f) (1 point) The uplink of LTE features a congestion control mechanism that works similar to the one in WiFi. True

(g) (1 point) Military GPS is essentially a TESLA-enabled civilian GPS.