Open questions

General

Wireless Communication

GNSS

Explain the informations sent by the GNSS satellite to the received and how they are used to compute the PVT

Difference between Jamming and spoofing in GNSS, how they influence the PVT , what is more harmful and why?

Describe meaconing compare work other type of GNSS ATTACKS.

Describe two interferences mitigation techniques in GNSS

Explain in general detection and mitigation techniques for interference signals in both domain. Explain in detail mitigation technique in frequency domain and in time domain

Describe the mitigation techniques (at least 3) of GNSS spoofing and the relative leves in which they act.

List and describe some possible spoofing countermeasures for satellite navigation systems. (3 points). Identify at least three spoofing countermeasures. Briefly describe how each countermeasure works. Explain the effectiveness of each countermeasure in mitigating spoofing attacks. Specify the levels of a satellite navigation system at which these countermeasures can be implemented. (3 points) Identify the different levels within a satellite navigation system. For each of the countermeasures mentioned above, indicate the level(s) at which they can be applied.

What are the effects of a spoofing attack on a GNSS receiver? (2 pts) How can a receiver fail or fail to respond to a spoofing attack? (2 pts) Possible disruptions of the attack? (2 pts)

WLAN - wifi

Power saving mode in 802.11 + attack

Consider a setup in which 2 STA (STA-1 and STA-2) are connected to the same WLAN managed by an AP. A third device (ETH-1) is connected with Ethernet technology. For each setup, describe and justify the expected goodput in the following cases:

- **Scenario 1 (3 points): Both STA-1 and STA-2 use 802.11g on the ISM band, ETH-1 uses Fast Ethernet technology with a physical link capacity of 100Mb/s**

1. STA-1 sends data to ETH-1 using UDP
2. STA-1 sends data to ETH-1 using TCP
3. STA-1 sends data to STA-2 using UDP
4. STA-1 sends data to STA-2 using TCP

- **Scenario 2 (2 points): What changes if STA-1 now connects to the same WLAN but using the 5GHz band? Again, consider the cases**

  1. STA-1 sends data to ETH-1 using UDP
  2. STA-1 sends data to ETH-1 using TCP
  3. STA-1 sends data to STA-2 using UDP
  4. STA-1 sends data to STA-2 using TCP

- **Scenario 3 (1 point), what changes if now both STA-1 (on 5GHz band) and STA-2 (on 2.4GHz band) upgrade their technology to using 802.11ax (WiFi 6)?**

  1. STA-1 sends data to ETH-1 using UDP
  2. STA-1 sends data to ETH-1 using TCP
  3. STA-1 sends data to STA-2 using UDP
  4. STA-1 sends data to STA-2 using TCP

Consider UDP header of 8B, TCP header of 20B, IP header of 20B, Ethernet header c' of 38B.

Describe the frames exchanged by an STA and an AP to inform the STA about the SSID of the AP; what kind of attack exploits this mechanism? Descrive step For OPEN AUTH sydtem when the Ap communicate EESID and when not

Describe the sequence of messages that an STA and an AP exchange during association and authentication processes in an open system(?) in the following cases: case 1 - AP broadcasts beacon messages (2 points) case 2 - ESSID is hidden, AP does not broadcast WLAN EISS in beacons (2 points) (enumerate the steps) which types of attacks do these mechanisms allow? (2 points)

WPAN - Bluetooth

Secure simple pairing + MITM attack

Differences between BT BR/EDR and BLE (frequencies, FEC/ARQ, . . .)

Which are the privacy offered by Bluetooth? Describe how the IRK is used to provide resolvable private addresses.

What are the 4 association modes in Bluetooth and what capabilities a device must have to support them(in general); Why they are used? For every association mode, tell which capabilities a device must have

to support them (for Numerical comparison the devices must have these capabilities and so on and so forth)

Bluetooth modes OOB, Just works, passkey entry, numeric comparison and hardware required to use them

Describe the 4 states of a Bluetooth device (standby, advertiser, scanner, initiator and master/slave) (3 porints) and prove an example with all the steps, A sends frame to B, B sends broadcast to A, A extract YYYY, ZZZZ from XXX to get GGGG etc (3 points)

Explain the main design goals for the BT technology and the technical constraints that guided the design (2 pts). Describe BT network topologies and the role of nodes in each scenario (2 pts). Describe the physical layer com mechanisms implemented in BT BR/EDR and the differences since BLE was introduced: which frequency range does it use, which multiple access scheme does it use, which FEC/ARQ mechanism it provides etc. (2 pts)

WWAN - mobile