Example Questions

Security of Wireless Networks

Question 1 (Key Establishment)

Question 1.1: What are the basic requirements of the uncoordinated frequency hopping (UHF)? (3 Marks)

Answer 1.1:
a) $P_a > P_t$ (Received power of the legitimate transmission (P_a) is enough to decode the message)
b) Transmitter (A) send on the same channel as the receiver (B) is listening
c) Each node holds a public/private key pair and capable of performing public key operations.

Question 1 (Key Establishment)

Question 1.2: What the main components of the UFH message transfer process? (2 Marks)

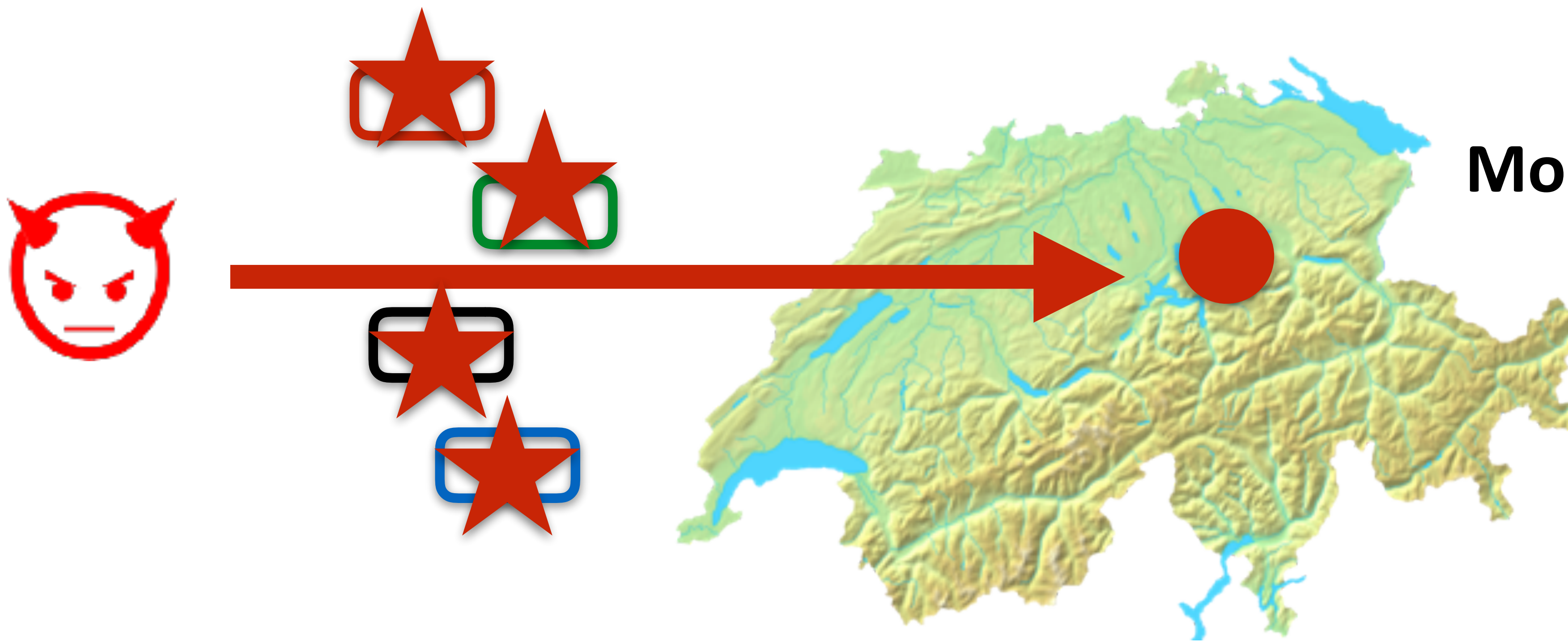
Answer 1.2:
a) Fragmentation
b)Transmission
c) Reassembly

Question 2 (GPS)

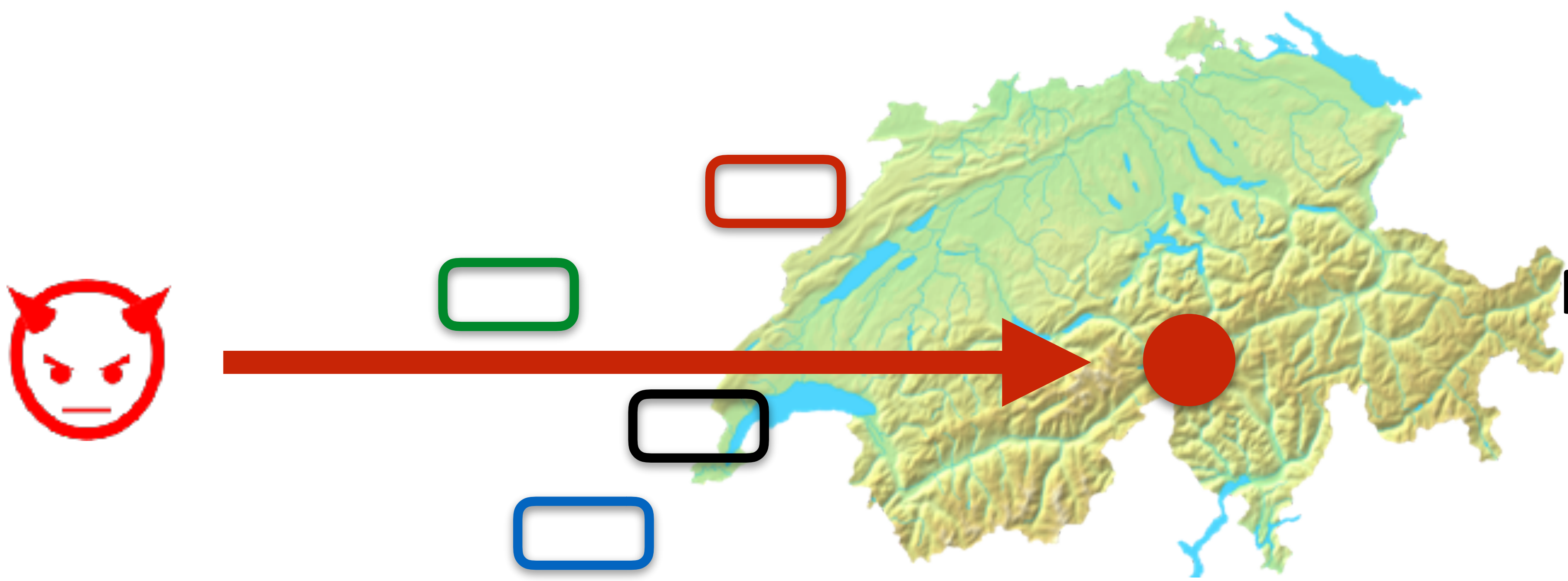
Question 2.1: Explain signal-synthesis and selective-delay attack.

Answer 2.1:

GPS spoofing attacks



Modify the contents of the navigation message



Modify the arrival time

Question 2 (GPS)

Question 2.2: Explain the hidden markers approach to prevent signal-synthesis and selective-delay attack. What are the assumptions on the time synchronization of the receiver's clock?

Answer 2.2:

Proposal for a Secure GPS (Kuhn)

Devices hold satellite public keys

At time t, a satellite uses a secret code to spread the navigation signal

- The receiver uses a broadband receiver to receive the whole signal band (receiver does not know the despreading code yet)
- At time t+dt, the satellite discloses its secret code, signed with its private key
- The receiver gets the code, verifies the signatures and de-spreads the signals.

Prevents the generation of fake signals and their individual shifts.

Question 2 (GPS)

Question 2.3: There are two GPS receivers, at coordinates (0,0) and (0,10). A spoofer, located at (5,0), transmits signals that make receiver 1 believe it's at (10,0). Assume receiver 2 receives the same signals: Where is it being spoofed?

Answer 2.3: (10,0)

Question 3 (Distance Bounding)

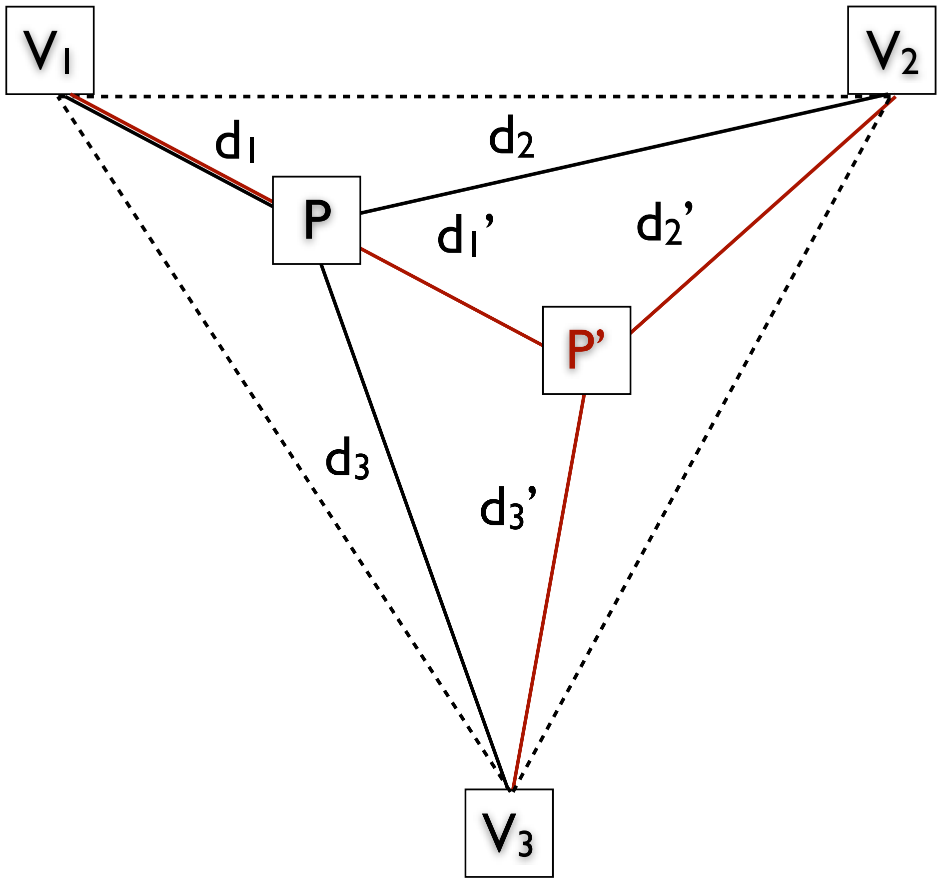
Question 3.1: What are the properties of Verifiable Multilateration?

Answer 3.1:

Verifiable Multilateration

Properties:

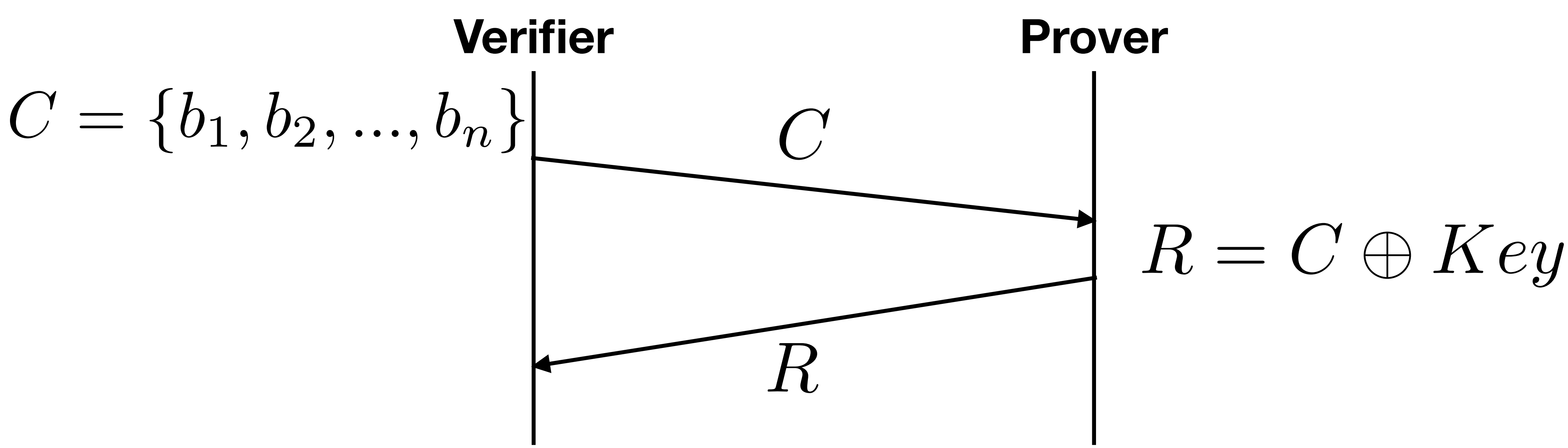
1. *P cannot successfully claim to be at P'≠P, where **P' is within the triangle***
2. *M cannot convince Vs and P that P is at P'≠P where **P' is within the triangle***
3. *P or M can spoof a location from P to P' where P' is **outside the triangle***



P→P' => d2'<d2

Question 3 (Distance Bounding)

Question 3.2: What are the security vulnerabilities in the following distance bounding protocol (6 Marks)



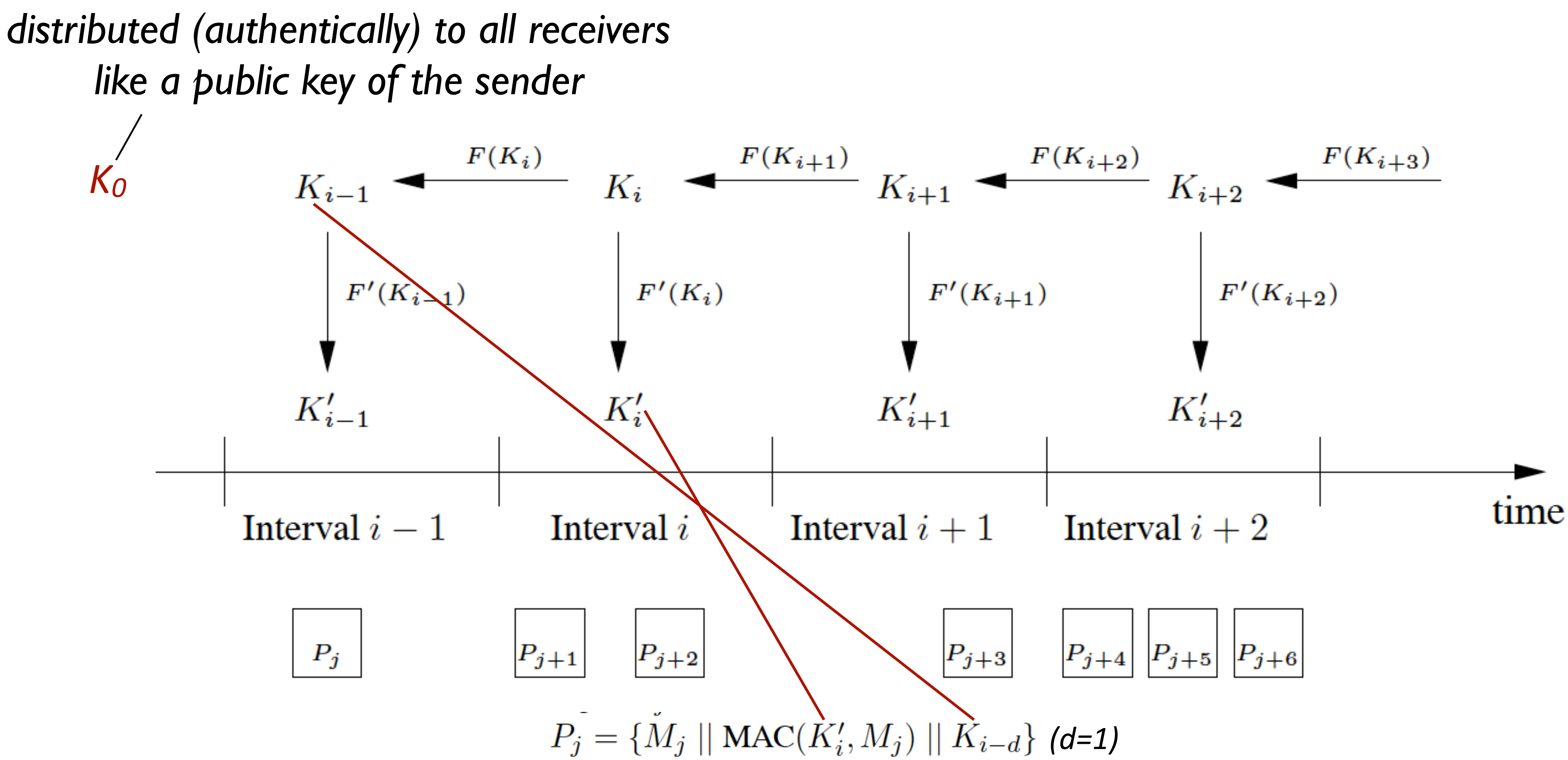
Answer 3.2:

Question 4 (Tesla)

Question 4.1: Explain packet construction $P_j = \{M_j \| MAC(K_i', M_j) \| K_{i-d}\}$ in the Tesla. How does receiver verify the authenticity of packet P_j?

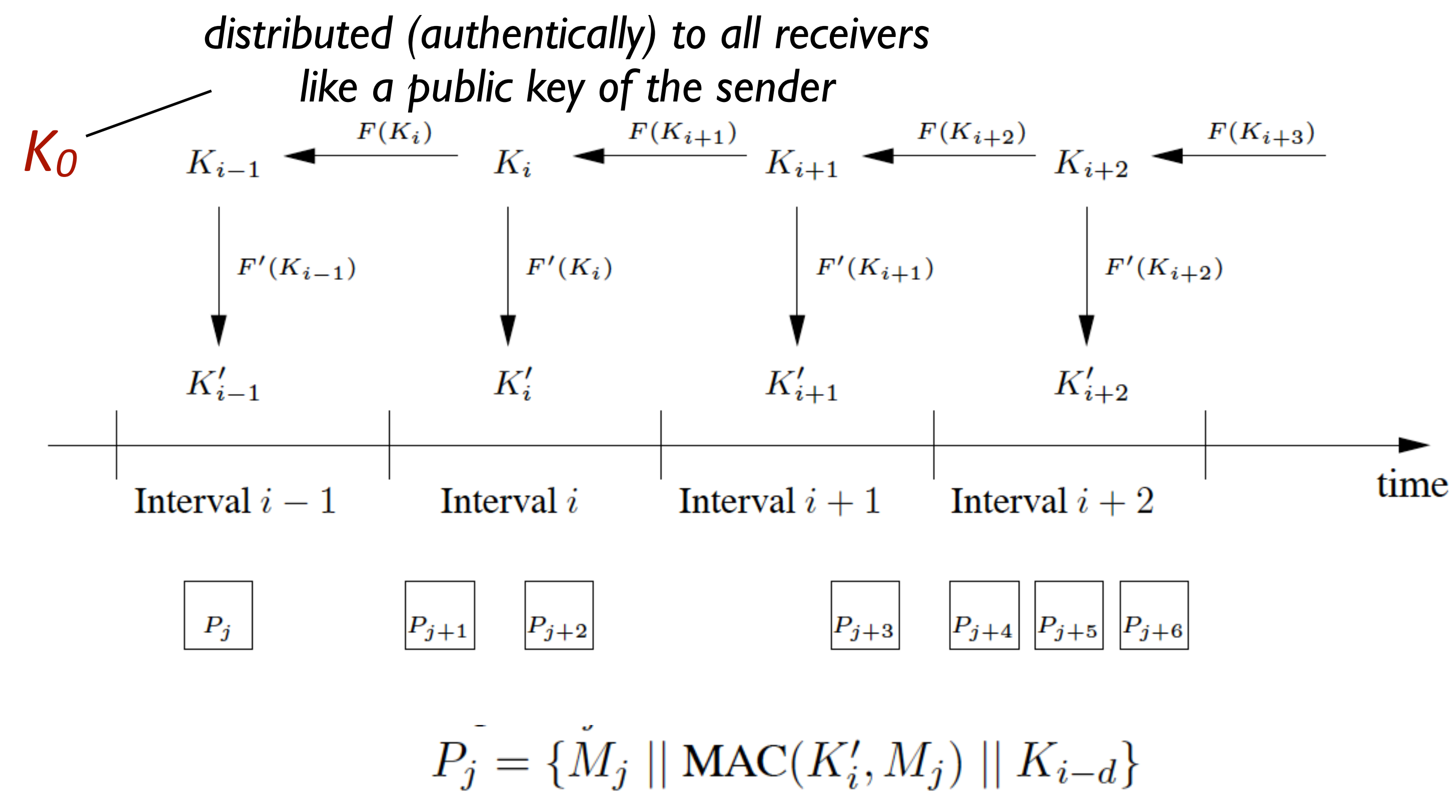
Answer 4.1:

Broadcast Authentication based on Delayed Key Disclosure (TESLA)



- To transmit a message M_j, the sender MAC's M_j with the key of the current time interval (K_i')
- The key is used *ONLY WITHIN ITS INTERVAL*
- Each key is *explicitly disclosed in cleartext after the interval*

Broadcast Authentication based on Delayed Key Disclosure (TESLA)



Message Verification:

- Receive M_j
- Receive K_i
- Compute $K_i' = F'(K_i)$
- Verify MAC
- Verify that $F^n(K_i) = K_0$
- *Verify that the message was received within the key validity interval (before the key was disclosed)*

- The keys are authenticated using one-way hash chains
- The messages are authenticated using the keys
- If the key is used after the interval, the message is ignored

Question 5 (Friendly Jamming)

Question 5.1: Suppose devices J and D are using friendly jamming to communicate in the presence of an attacker. How can an attacker separate the signal and noise in the following scenarios:

a) DJ $> \lambda/2$
b) DJ $>> \lambda/2$
c) DJ $< \lambda/2$

Answer 5.1:

Friendly Jamming

- Jamming signal is much stronger and covers the spectrum of the data signal.
- If DJ > λ/2, attacker equipped with two antennas can separate signals from J and D (different channels).
- If DJ >> λ/2 attacker can use directional antennas to separate the signals.
- => the only "safe" case seems to be when DJ < λ/2

Lessons learned

- Using Jamming for confidentiality is not without risk
  - MIMO-like attacker can retrieve data despite DJ < λ/2.
  - The attack works from many locations (with some post-processing).
  - The attack can be effective even when jammer and source are mobile.

- Note: Friendly Jamming works well for access control.

Question 6

Question 6.1: What is spatial diversity?

Question 6.2: What does the term jamming margin refer to?

Question 7

Question 7.1: Why is a handshake alone sufficient to break the password in the WPA protocol?

Question 7.2: Why are broadband signalling schemes (e.g., DSSS) more difficult to jam? Would DSSS be effective against Wideband jammers?