PA197 Secure network design

Basic wireless networking

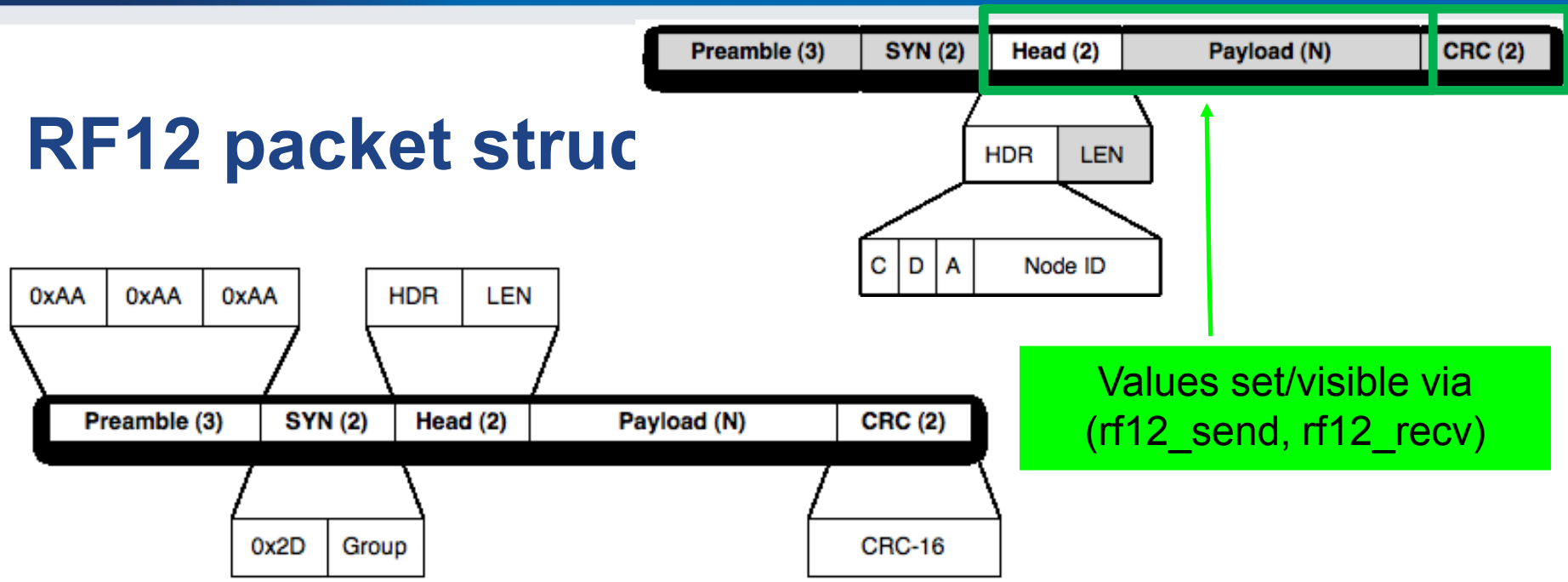
Lukáš Němec

Centre for Research on Cryptography and Security

Laboratory

- Jammer attack
- Simple static routing via one intermediate node
  - Sender→Transmitter (receive, send)→Receiver (blink)
  - Single parent for routing towards “BS” (e.g., CTP)
- Node-to-node routing
  - Simple flooding routing with multiple neighbours
  - Packet with target ID, retransmitted to all neighbours

RF12 packet struc



- C = CTL, D = DST, A = ACK, 5-bit node ID
  - A bit (ACK) – indicates if sender wants to get ACK back
  - D bit (DST) – indicates if node ID bits specify destination or source node
  - C bit (CTL) – 1 if packet is ACK (and A must be 0)
- http://jeelabs.org/2011/06/09/rf12-packet-format-and-design/index.html

Jammer

- Write your own jammer

Non-discriminative jammer

- Occupies/distorts whole channel
  - Sending packets all the time without waiting for clear channel
  - No need to send correctly formatted packets or use same type of radio
- How to detect non-discriminative jammer?
  - Abnormally high number of lost packets
  - Abnormally high send waiting time (clear channel)
  - Abnormally low RSSI
  - Detection by whole channel monitoring (e.g., SDR)

Selective jammer

- Not jamming continuously, bursts to corrupt particular message

1. Disturb next message that is expected to be send
   - Attacker in promiscuous mode, receives $message_i$
   - Prevents transmission of $message_{i+1}$ (occupies channel…)
2. Disturb rest of a currently transmitted message based on initial part
   - Requires high speed processing of radio channel and low latency decision
     - Not possible with our RF12 module (whole packet only)
   - Disturb only part of a message (e.g., CRC checksum)
     - Message is dropped upon reception

- How to detect selective jammer?
  - Detection of abnormally high number of corrupted or lost packets
  - Sensing of channel with different radio and detection of burst transmissions

Simple static routing via one intermediate

- Pair together with two other colleagues
  - Same as previous one-hop exercise
  - Output message with counter to serial port (monitor packet loss)
- Use one intermediate node (fixed routing topology)
  - Sender→Transmitter (receive, send)→Receiver (blink)
- Test on distance (hall space, other floors…)
  - How far you can extend coverage?
- Straightforward extension to fixed routing to BS
  - Every one has single parent for routing towards BS
  - e.g., The Collection Tree Protocol (CTP)
- Think about advantages and disadvantages
  - Flexibility, robustness, malicious passive/active attacker

Any node to any node routing - flooding

- What are options for any-to-any routing?
  - Think about limitations in context of ad-hoc/WSNs
- Node-to-node routing
  - Simple flooding routing with multiple neighbours
    - Establish list of neighbouring nodes
  - Packet contains target node ID (data section)
  - Locally retransmitted to all neighbours
- How to eventually stop flooding?
  - Time To Live? (TTL decrement after every hop, 0 => drop)
  - Packet Unique ID (seen twice => do not resend, state)

Homework – Attack against routing

1. Influence routing discovery phase of laboratory testbed to create sink-hole attack
   - messages routed towards your malicious node
   - Route discovery phase runs for 5 minutes (LEDs are blinking fast)
2. Capture packets during message exchange phase
   - 5 minutes, no blinking
   - Capture all packets routed to you, format: #num1#num2
     - E.g., #3289#893756
   - Replace second number after # with your UCO
     - E.g., #3289#394036
3. Send modified captured packet to BS
   - BS will reply, store all responses into file to be submitted as solution

Homework – Attack against routing

- Produce short (1xA4) text description of solution
  - How routing discovery phase is done
  - How were packets analyzed
  - Describe in detail the attack on routing.
  - How resend was done to maximize number of captured packets
- Try to maximize number of captured/resend packets
- Submit before: 26.4. 23:59