12. WSN Security II.

Specific attacks on WSN, protection

Wireless sensor networks

Martin Úbl
ublm@kiv.zcu.cz

2023/24

<DCSE> DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Security

Initial remarks

- when considering WSN security, there are lots of possible views
- important remark: protecting everything with maximum security costs a fortune!
- goal: balance costs and reasonable protection and security
- important remark: if the attacker truly wants to compromise our network, he will eventually find a way
- goal: make it cost him more than us (ideally)

Security

Initial remarks

- an attack is possible on all layers
- it depends on what is the goal of the attacker
  - take down our network?
  - inject a node?
  - fail the mission by poisoning data?
  - deplete our batteries?
  - raise false alarms?

Security

Initial remarks

- many types of attacks
  - denial of service (DoS) – reduce availability or shut down the network
  - depletion attack – attempt to deplete battery quickly
  - injection attack – injecting fake data
  - redirection attack – redirect traffic (L2, L3, ...)
  - spoofing attack – attempt to spoof node info and impersonate one
  - congestion attack – imitation of traffic, nodes sense carrier wave and do not transmit
  - man in the middle attack (MitM) – transparently spoofing both sides of communication
  - side-channel attack – extract information from other than a primary source (e.g., timing attack, ...)
  - etc.

Security

Physical layer

- **attacks on physical layer**
- *jamming*
  - transmitting garbage data on our channel
  - a type of DoS attack
  - protection: spread spectrum techniques
    - DSSS – a slightly more resistant against jamming
    - FHSS – frequency hopping requires the attacker to jam more frequencies
    - rapid-hopping FHSS – jam all the frequencies

Security

Physical layer

- *tampering*
  - stealing the node to deconstruct it, reverse engineer it, or scan its memory
  - can be dangerous – reading the memory directly may reveal encryption keys
  - protection:
    - physical node security – encasement, anchoring
    - encasement with self-destruction tampering protection
    - – when someone tries to steal the node, sensor detects it and performs self-destruction
    - detonates a small charge
    - or erases the memory

Security

Physical layer

- *on-site node scan*
  - do not steal the node, but attempt to read the memory/analyze it on-site
  - for example – read the crypto keys from external memory
  - protection:
    - physical node security – encasement, anchoring
    - encrypted external flash memory
    - short-lived keys

Security

Data link layer

- **attacks on data link layer**
- *fake preamble injection* (asynchronous TDMA)
  - depletion attack
  - attacker injects fake preambles to wake up nodes
  - protection:
    - do not use asynchronous TDMA
    - pseudo-random information in preables
    - frequency hopping or FDMA in general – additional form of security to make it harder

Security

Data link layer

- *targetted slot attack* (synchronous TDMA)
  - specific attack on a specific protocol
  - in general, synchronous TDMA are hard to exploit without any prior knowledge about their implementation
  - but if somebody manages to extract that info from the binary code of stolen node, there is a chance
  - protection:
    - allow MAC protocol reconfiguration
    - dynamic MAC protocols
    - dynamic slot allocations

Security

Data link layer

- *spoofing attack*
  - attacker injects a node, that tries to spoof another node
  - it uses its address (HW address), frequency band and other characteristics
  - protection:
    - authentication on L2, Message Authentication Code
    - duplicate detection (if the attacker did not shut down the other node)
    - upper layer authentication methods

Security

Data link layer

- *Sybil attack* – a variant of spoofing attack
  - to introduce an element of confusion, the attacker tries to spoof different nodes at different times
  - this will probably seem like an error to the programmer
  - the attacker may proceed with another attacks, since he distracted the administrators
  - protection:
    - same as the spoofing attacks
    - it is just important to know about this type of attack

Security

Data link layer

- *Hello attack*
  - advertising L2 hello packets to create false neighborhoods
  - form of a redirection attack
  - protection:
    - authentication on L2 (MAC-based auth)
    - handshake procedure instead of a simple hello frame (with a form of authentication)

Security

Network layer

- **attacks on network layer**
- *sinkhole attack*
  - an attacker injects a node, that merely routes the data
  - other nodes stores the advertised path and start to use it
  - the attacker now legitimately routes part of the data
  - protection:
    - L3 encryption (to avoid using injected nodes for relaying data)
    - diverting part of data through a redundant path
    - lower layer node injection protection

Security

Network layer

- *wormhole attack*
  - a variant of sinkhole attack, that advertises a very efficient network route to the data sink
  - nodes start to use the route
  - attacker now legitimately routes all the data from this part of network
  - protection:
    - message authentication codes on routing info
    - L3 encryption
    - redundant paths
    - lower layer node injection protection

Security

Network layer

- *flooding attack*
  - forces nodes to route injected data (conforming to protocol)
  - form of a DoS attack
  - protection:
    - L3 encryption
    - flooding node detection
    - lower layer node injection protection

Security

Network layer

- *spoofing attack* or *Sybil attack*
- practically the same implications, as on L2
- additionally, we may protect implicitly by using lower layer security mechanisms

Security

Network layer

- *black hole attack*
  - always in combination with spoofing, wormhole or sinkhole attacks
  - the injected node drops all the packets
  - form of a DoS attack
- *grey hole attack*
  - as above, but drops just a part of packets
  - this also introduces a confusion element and distracts the administrators

Security

Transport layer

- **attacks on transport layer**
- *acknowledge attack*
  - injecting false acknowledge packets
  - may induce congestion, if we aim for higher data rates
  - may acknowledge data, that were lost on its way
  - potentially combined with black/grey hole attacks – the attacker drops the L3 packet, but acknowledges it on L4
  - protection:
    - lower layer node injection protection
    - ACKs may contain checksums of acknowledged data
    - authentication on L4 for ACKs
    - redundant ACKs for groups of data, e.g., 4 segments, 4 partial ACKs and 1 "whole data ACK"

Security

Transport layer

- *congestion attack*
  - attacker injects packets to induce congestion
  - not necessarily at the rate to induce a real congestion
  - e.g., if using the sliding window approach (rarely in WSN), attempt to inject false congestion detection segments
  - protection:
    - lower layer node injection protection
    - authentication on L4 for control overhead segments
    - distributed congestion detection (not end-to-end)

Security

Transport layer

- *connection flood attack*
  - if using a stateful approach, the attacker may create a fake connection attempts
  - this floods the node connection table with fake info
  - results in node DoS
  - protection:
    - ideally do not use stateful L4 approach in WSNs
    - authentication during state establishment
    - state information timeout

Security

Transport layer

- *NACK attack*
  - injecting fake NACK messages to force retransmission
  - may be seen as a depletion attack
  - protection:
    - authentication for acknowledgments
    - do not use NACK-based protocol
    - do not use reliable protocol at all, if it is not really required

Security

Transport layer

- *desynchronization attack*
  - inject a fake data to alter state information
  - e.g., inject segments which imitates next part of data, so the target node is forced to acknowledge it
  - this triggers a resynchronization of both nodes, because sequence numbers no longer match
  - protection:
    - authentication
    - checksums for acknowledged data
    - fixed segment sizes

Security

Application layer

- **attacks on application layer**
- *time synchronization attack*
  - attacker attempts to inject fake time source
  - this potentially desynchronizes all nodes
  - all nodes lose synchronization $\rightarrow$ no communication (if using e.g., synchronous TDMA)
  - protection:
    - authentication of time sources (carefully – crypto actions induce additional delays)
    - require multiple time sources
    - lower layer node injection protection (may not work as the time source may be implicitly an external node)

Security

Application layer

- *localization attack*
  - injecting fake location info
  - e.g., the attacker imitates the anchor node
  - since anchor nodes may be implicitly external nodes, this might be possible
  - protection:
    - authentication of external nodes (also carefully – some localization methods require precise timing)
    - require more location sources, detect outliers

Security

Application layer

- *protocol-specific attacks*
- some attacks may be targetted to a specific application protocol used
- MQTT – publish flooding
  - MQTT supports authentication and authorization – use it
- CoAP – query flooding
  - pretty much the same
- lots of attacks can be avoided by using encryption or authentication

Security

Final remarks

- it’s not about implementing all protection mechanisms
  - that would take a long time
  - consume too much memory
  - consume too much computational time
  - eventually, we will "shoot ourselves in foot", because our security measurements will consume too much energy
- depending on application, choose the most important ones
- implement the most important mechanisms

Security

Final remarks

- use proven techniques
- "security by obscurity" is a very dangerous paradigm in low-power applications
  - obscurity usually indicates additional work
  - energy consuming

Security

Final remarks

- the first thing somebody usually tries – L1 attacks
  - steal a node
  - jam the frequency
  - read the memory
  - destroy network sink
  - etc.
- do not confuse mistake with intent

Security

Final remarks

- use encryption and authentication
  - at least on some layers
- if your network supports firmware updates, OAD or dynamic retasking, always use digital signatures
  - exploiting this procedure may lead to taking over the whole network

Security

Final remarks

- use advanced encryption and security on all nodes outside WSN
  - edge and cloud nodes should use the highest possible protection
- there is much higher probability, that somebody attempts to compromise your server in the Internet, than your WSN
- if your server can control the WSN, taking over the server means taking over the WSN