PA197 Secure Network Design

Wireless Sensor Networks – attacker models, secure routing, IDS

Petr Švenda svenda@fi.muni.cz
Faculty of Informatics, Masaryk University

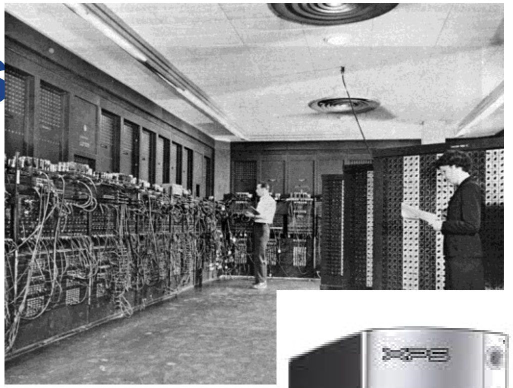
CROCS
Centre for Research on Cryptography and Security

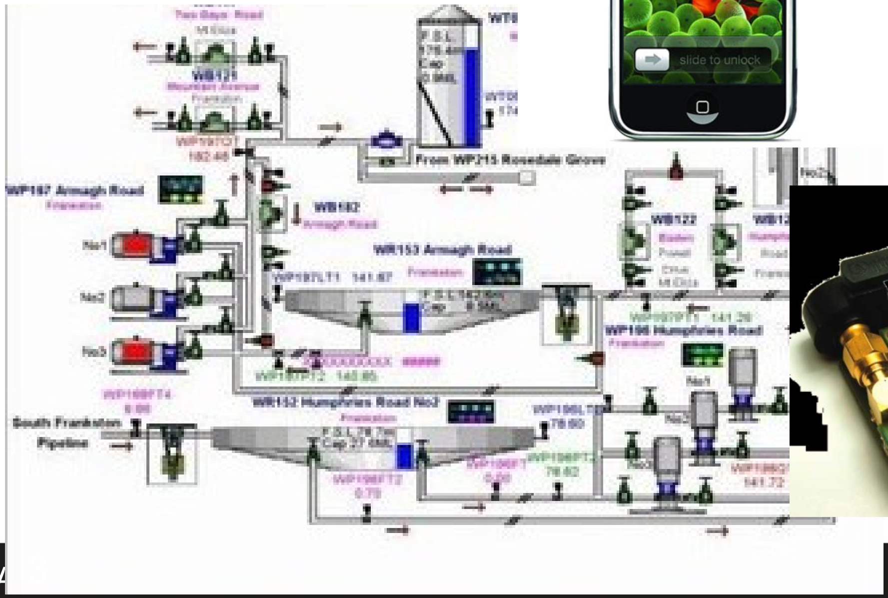
Overview

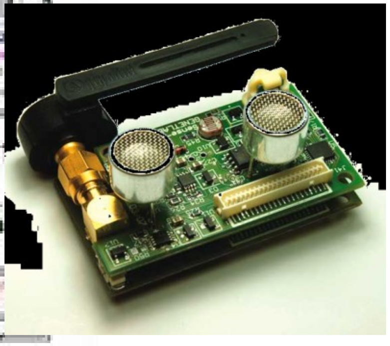
- Intro to wireless sensor networks
- Security considerations
  – Why are WSNs special?
- Attacker models
- Routing → attacks → secure routing
- Intrusion detection, reaction

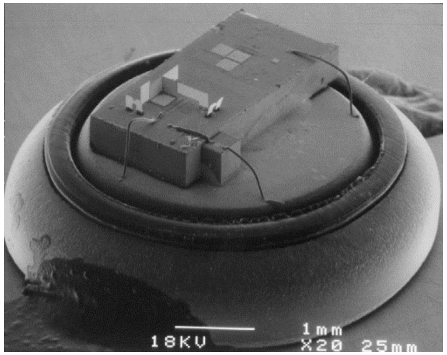
Route to nodes

From Computer Desktop Encyclopedia
© 2006 The Computer Language Company Inc.

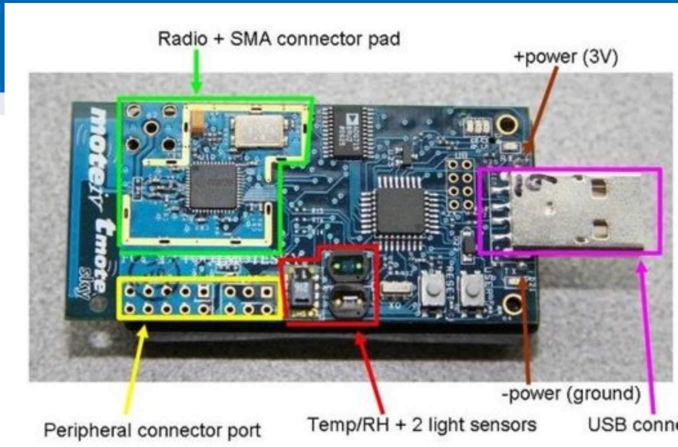


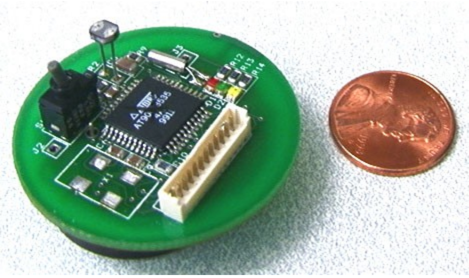




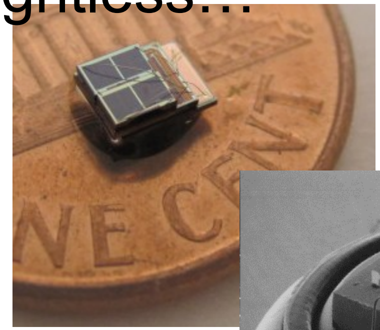


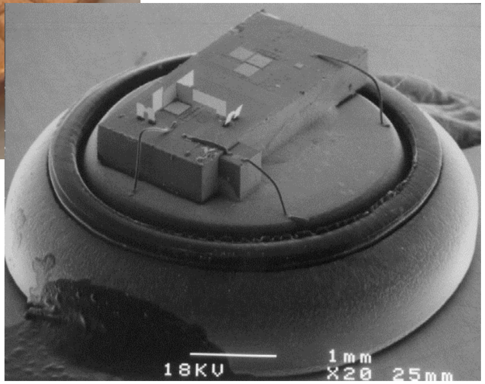
Wireless Sensor Node





- Basic technology
  - 8 bit CPU, ~1 kB RAM, ~10^2 kB flash
  - short range radio, battery powered
  - condition sensor (temperature, pressure, …)
  - xBow MicaZ, TelosB, BT LE, Weightless…
- Putting pieces together…
  - battery-powered small MCU
  - + efficient radio module
  - + environmental sensor
  - => Wireless Sensor Network (WSN)

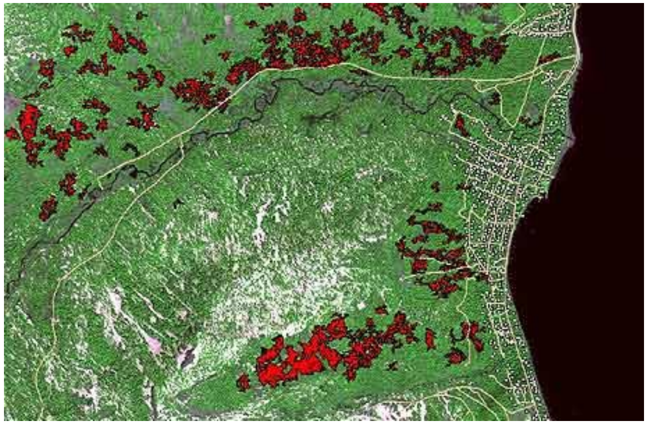




Do we have useful application for WSN?

Traffic control

Medical information



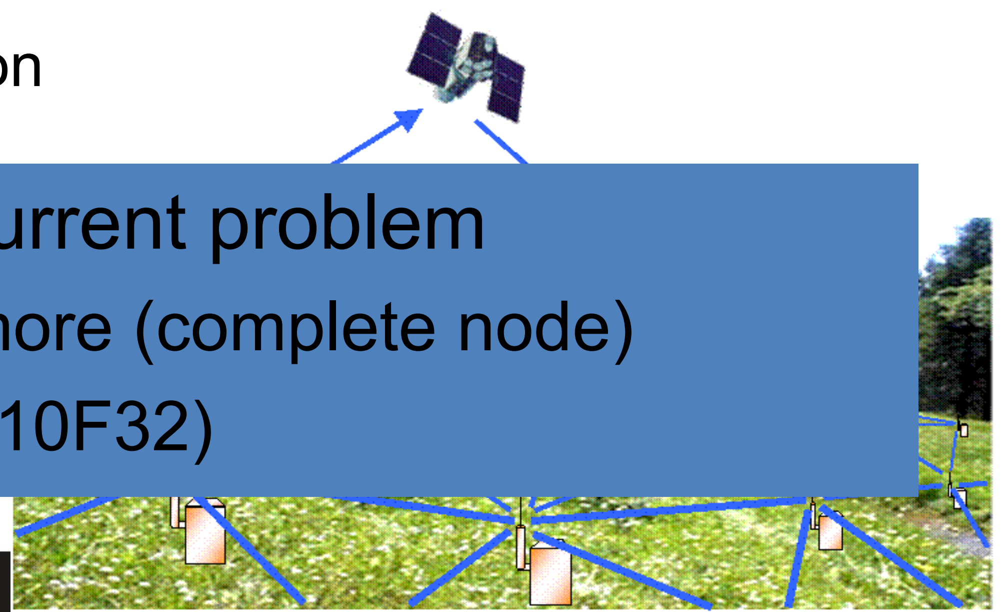
Remote fire detection

Combat field control

Ideal in 2000:
WSN is highly distributed network with high number of low-cost sensor nodes powered by battery connected via multi-hop communication with base station

Large scale Wireless Sensor Networks

- Network of nodes and few powerful base stations
  - $10^2 - 10^6$ sensor nodes
  - particular nodes deployed randomly, e.g., from plane
- Network characteristics
  - covering large areas - distributed
  - ad-hoc position/neighbours – not known in advance
  - multi-hop communication



- The price (still) is a current problem
  - currently ~100$ or more (complete node)
  - (but 3.35 $ for CC1110F32)

Science, Technology and Innovation

Projects

Subscribe Enews Alerts

Search...

HOME | MAGAZINES | R&D PROJECTS | FEATURES | OPINION | NEWS | EVENTS | FI WEEK

Categories

- Agriculture/Food
- Biology/Medicine
- Energy
- Environment/Climate
- ICT
- Industry/Technology
- Society/Economy
- Transport/Construction

Wireless Sensor Networks: The greatest invention since the Internet?

Although a relatively young technology, the potential of wireless sensor networks is encouraging intense research focus. Future systems are likely to require both small nodes and a high density of deployment, making efficiency and adaptability crucial to further development, says Professor Anders Rydberg.

The potential of wireless sensor networks (WSNs) – thousands of tiny monitoring devices which interconnect with physically remote environments – is of great excitement amongst the research

Reality in 2016 ☹:

WSN is ~~highly distributed~~ centralized network with ~~high~~ small number of ~~low-cost~~ high-cost sensor nodes powered by ~~battery~~ power grid ~~connected via multi-hop communication with~~ communicating directly to base station

But situation is getting better ☺

Current low(er)-cost technology

Diymall Ibeacon Module

- IEEE 802.15.4 standard for low-rate PANs
  - Basis for ZigBee tec.
- Bluetooth LE/Smart enabled devices
  - ~$10 for BT module
- Weightless-N/P/W (IoT), http://www.weightless.org/
  - 5 km range, 10 years lifetime, $2 price (planned ☺)
  - Thanks to large range, fewer hops to reach sink node
- Libelium Waspmote (multi-RF node)
- Simple processing can be run directly on network controller chip (if accessible)
  - Espressif ESP8266 ($1.6) WiFi module

Operating systems for WSNs

1. Should work on very limited device (10^2-10^3B RAM)
2. Should provide concurrency (perceived, real)
3. Should be flexible enough to support different usage scenarios
4. Should conserve as much energy as possible

- Examples: TinyOS, Contiky, RIOT…

TinyOS architecture (Berkley)

- Used to be the most popular operating system for sensor nodes
  - first version released in 2002 (TinyOS 1.2), current 2.1.2 (released in 2012)
  - Open-source work https://github.com/tinyos/tinyos-main (active)
  - network protocols, sensor drivers and data acquisition tools
- Basic design principles
  - Event-driven (routines serving particular event)
  - Telescoping abstractions
    - abstractions with spectrum of levels, portability and optimization
  - Partial virtualization
    - top layers of telescopic abstractions are shared or virtualized
  - Static binding and allocation
    - no dynamic allocation, all required resources allocated statically
- Applications written in Network Embedded System C (nesC)
  - optimized for low memory, real-time applications

Contiki

The Open Source OS for the Internet of Things

Contiki architecture

- Initial release 2003, current version 3.0 (2015)
  - http://contiki-os.org/
- Basic design principles
  - Dynamic loading and unloading of code at runtime
  - Event-driven kernel
  - Proto-threads (small routines executed after event)
- OS requires about 10 kilobytes of RAM (minimum)
  - More complex than TinyOS (400B RAM only)
  - TCP/IP stack… Optional addition of GUI etc.

We (will) have exciting technology.

Why/What security measures should be used?

Where do we need security in WSNs?

- Sensitive data are often sensed/processed
  - military application
  - medical information, location data (privacy)
- Commercially viable information
  - information for sale – cost for owner of the network
  - know-how - agriculture monitoring
- Protection against vandalism
  - distant non-existing fires blocks fireman

Early stage of WSN allows to build security in rather than as late patch

Why not "Just use TLS"?

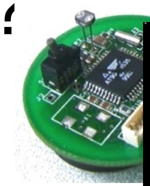
- What are differences from standard networks and why classical solutions mail fail?
  – Why we cannot use standard "TLS" for protection of data?
  – Party authentication, confidentiality, integrity, freshness…
- Sometimes we can! (don't be dogmatic)
- But: certificates, asymmetric crypto, revocation control, high data/computational overhead, session management, authentication of data, local aggregation…

Some differences from standard networks

- Running on battery (limited resource)
  - days for personal network
  - years for large scale monitoring network
  - especially communication is energy-expensive
- Relatively limited computation power
  - powerful CPU possible, but energy demanding
- Links can be temporal, network often disconnected
  - by design, by necessity

Some differences from standard networks

- Nodes can be captured by an attacker
  - all secrets can be extracted from unprotected nodes
  - and returned back as malicious node
- How to detect malicious node?
- How to react on detected malicious node?

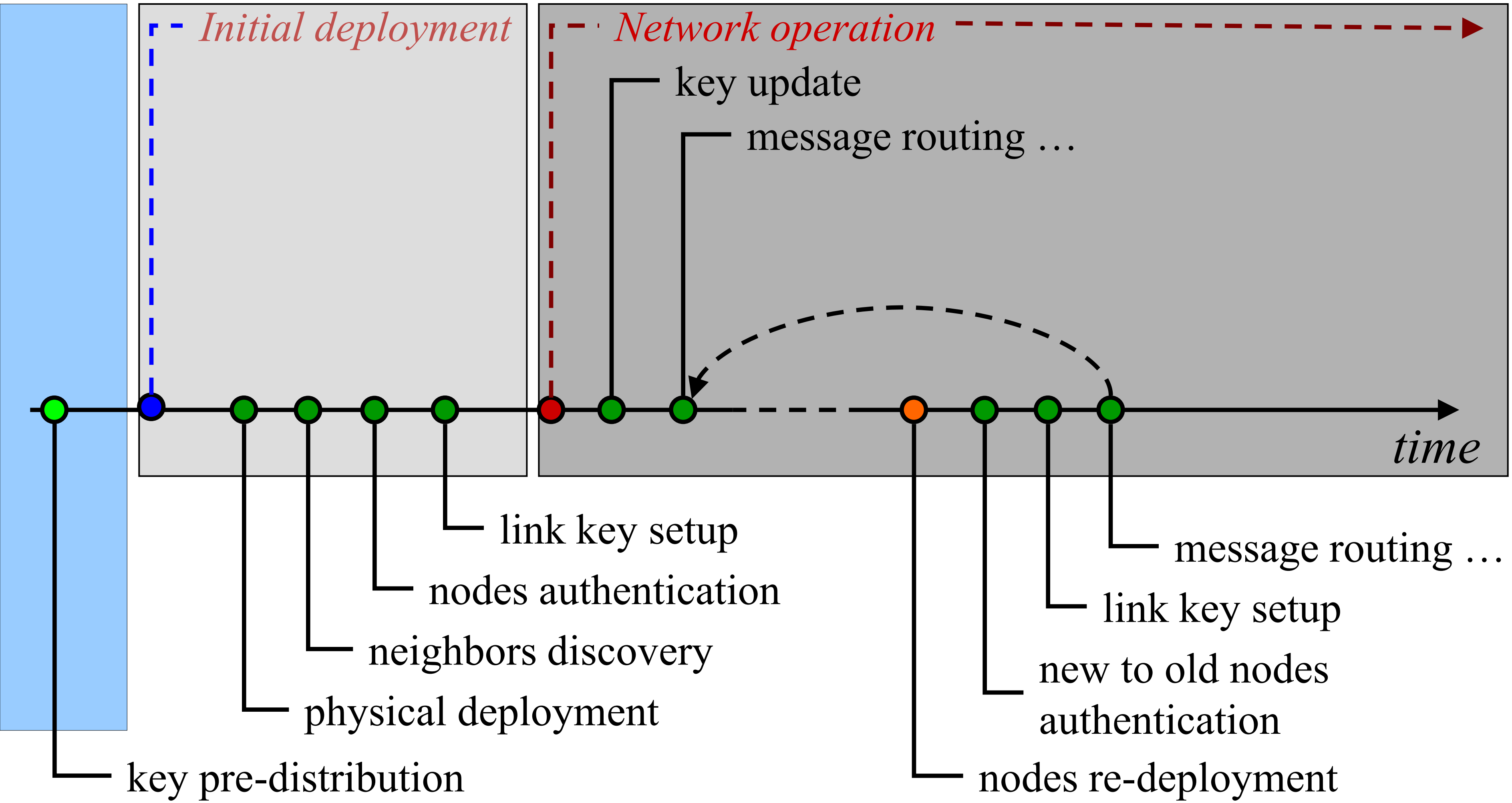


When detection/reaction is hard, focus on prevention

Main topics in WSNs (network security)

- Establishing network
  - Deployment, redeployment
  - Neighbor discovery, clustering
- Using and maintaining network
  - Sensing, data collection, data aggregation
  - Routing and reliable communication
  - Energy efficiency of all tasks (running on battery)
- Supporting security functions
  - Key management (pre-distribution, establishment, use)
  - Secure communication, authentication
  - Partially compromised network

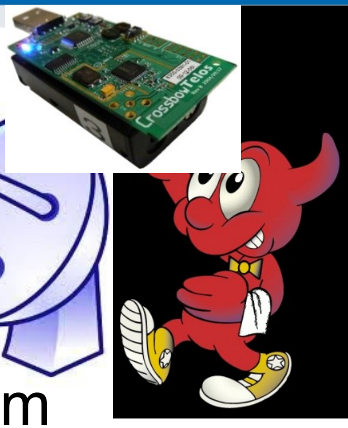
Network lifetime



Wireless Networks – Attacker Models

ATTACKER MODELS

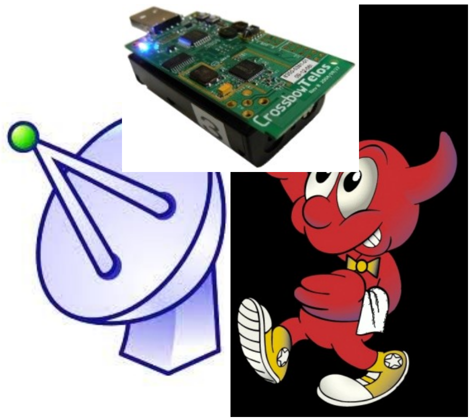
Attacker models - capabilities



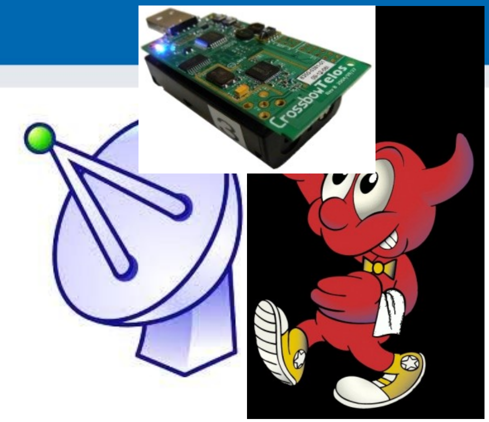
- Passive attacker
  - Does not inject/modify messages and does not jam
- Active attacker
  - May inject/modify messages or perform jamming
- External attacker
  - Not a legitimate member of a network
  - Not compromised any node or used key (yet)
- Internal attacker
  - Legitimate member of a network
  - compromised a single/few static/mobile sensor node(s) and/or possesses a single/few key(s)

Attacker models – capabilities (cont.)

- Local attacker
  - Can overhear only a local area: single or few hop(s)
  - Depending on antenna, transmission signal strength…
- Global attacker
  - Can overhear most/all node-to-node and node-to-base station communication simultaneously for all the time

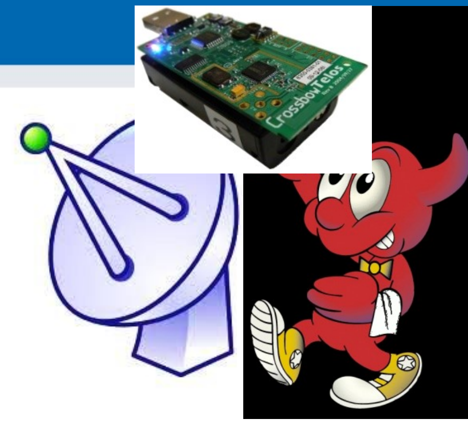


Attacker models - levels



- Level 1 attacker
  - A low cost attacker with minimum equipment requirements
  - Typical capabilities: Passive, External, Local
- Level 2 attacker
  - A medium cost attacker with distributed eavesdropping and transmitting device(s), but no compromised node
  - Typically a group of people with radio devices
  - Typical capabilities: Active, External, Global

Attacker models – levels (cont.)

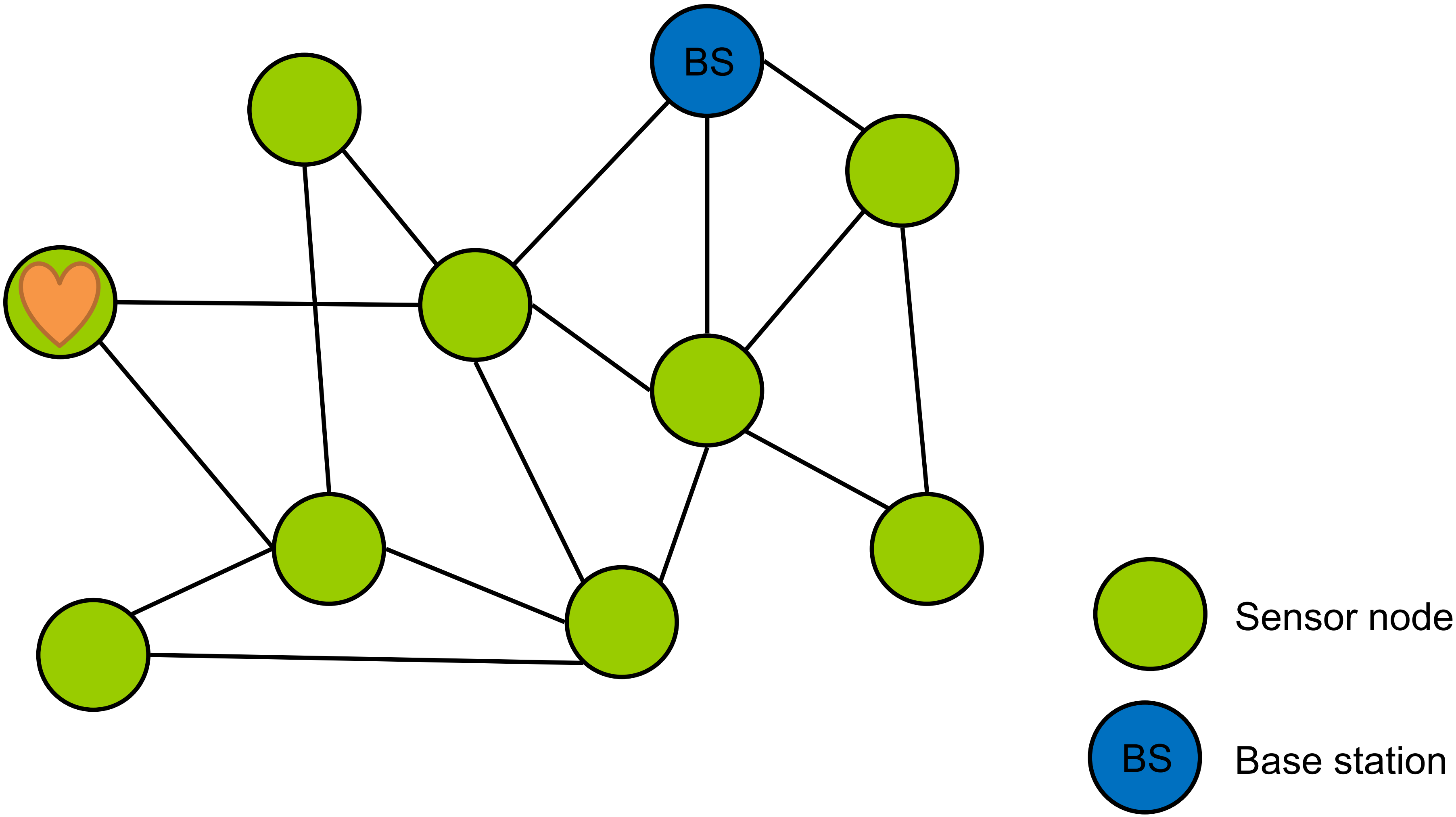


- Level 3 attacker
  - A medium cost attacker with common or special equipment and knowledge
  - The most common one as far as intentional serious attacks on a network are concerned
  - Typical capabilities: Active, Internal, Local
- Level 4 attacker
  - A high cost attacker with special equipment and knowledge (well-funded organization with high motivation)
  - Typical capabilities: Active, Internal, Global

Wireless Networks – Routing

ROUTING

Target network topology

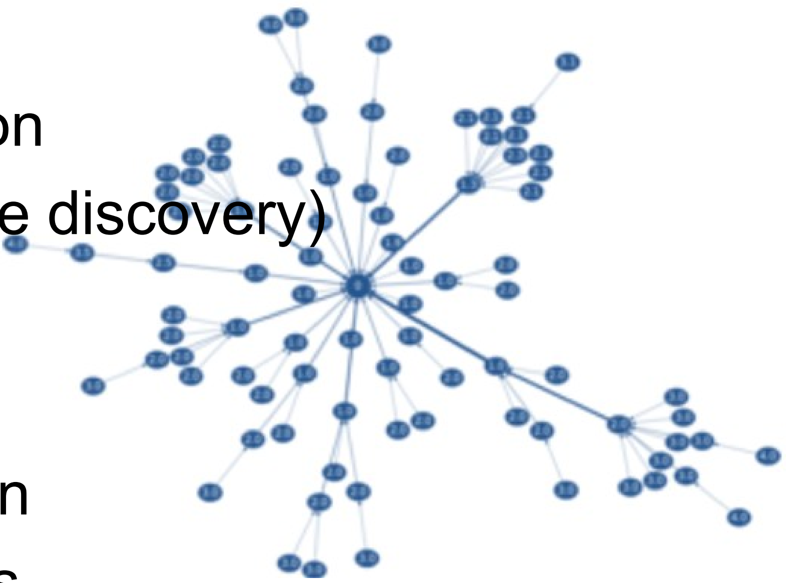


Routing influenced by data reporting model

- Time-driven
  - Periodic, continuous
  - E.g., “send current temperature every 10 seconds”
- Event-driven
  - when event happens
  - E.g., “report if temperature is more than 80°C”
- Query-driven
  - When someone (base station) asks
  - E.g., “send me current temperature measured on node 42”
- Hybrid (combination)

Example: static fixed routing tree

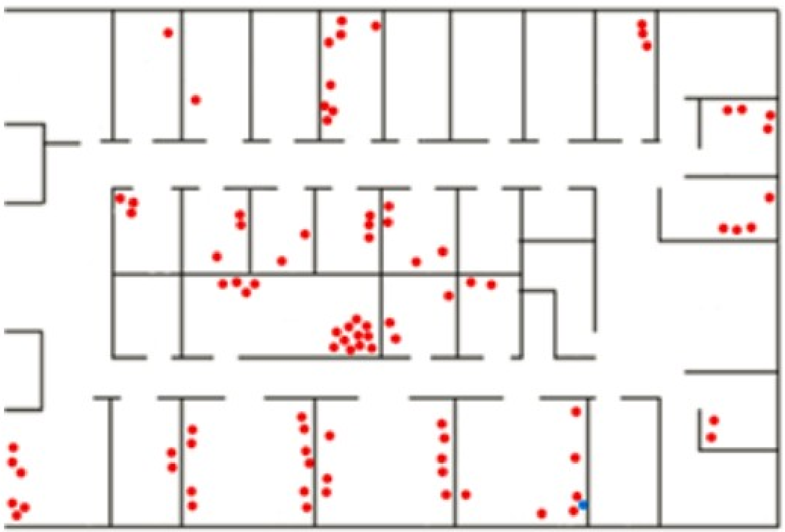
- Every node is preloaded with ID of parent node closer to BS
  - Received message is forwarded to parent node
- Advantages
  - Simple, low-memory consumption
  - Reduced attack surface (no route discovery)
- Disadvantages
  - Disconnect on node's failure
  - Non-uniform battery consumption
  - Not adapting to network changes



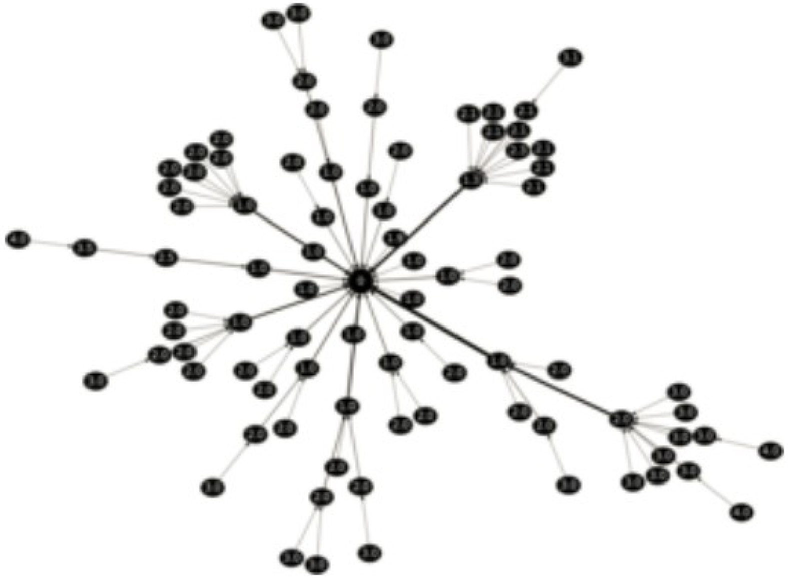
Example: Collection Tree Protocol (CTP)

- Collection Tree Protocol (CTP), default in TinyOS
  - Many-to-one collection data collection protocol (nodes to BS)
  - Address-free routing (only route towards BS)
- Routing metric is number of steps to BS (sink node)
  - Number of expected transmissions (ETX) to reach sink node
  - Each node keeps only smallest ETX to nearest sink node
  - Routes with lower metric are preferred
  - Message is send only from higher ETX to lower ETX
- Routing loops prevention
  - In case of message with lower ETX then own => update path
- Possibility to periodically refresh routing metric
  - Continuous adaptation to network changes

CTP – resulting routing tree



Powernet Deployment map

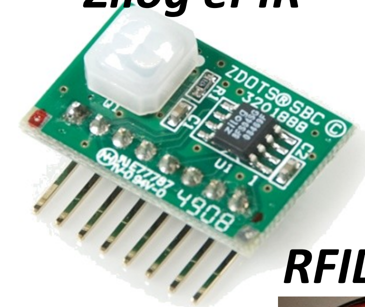


CTP Routing Topology on Powernet

Source: http://sing.stanford.edu/gnawali/ctp/

Hardware used, testbed

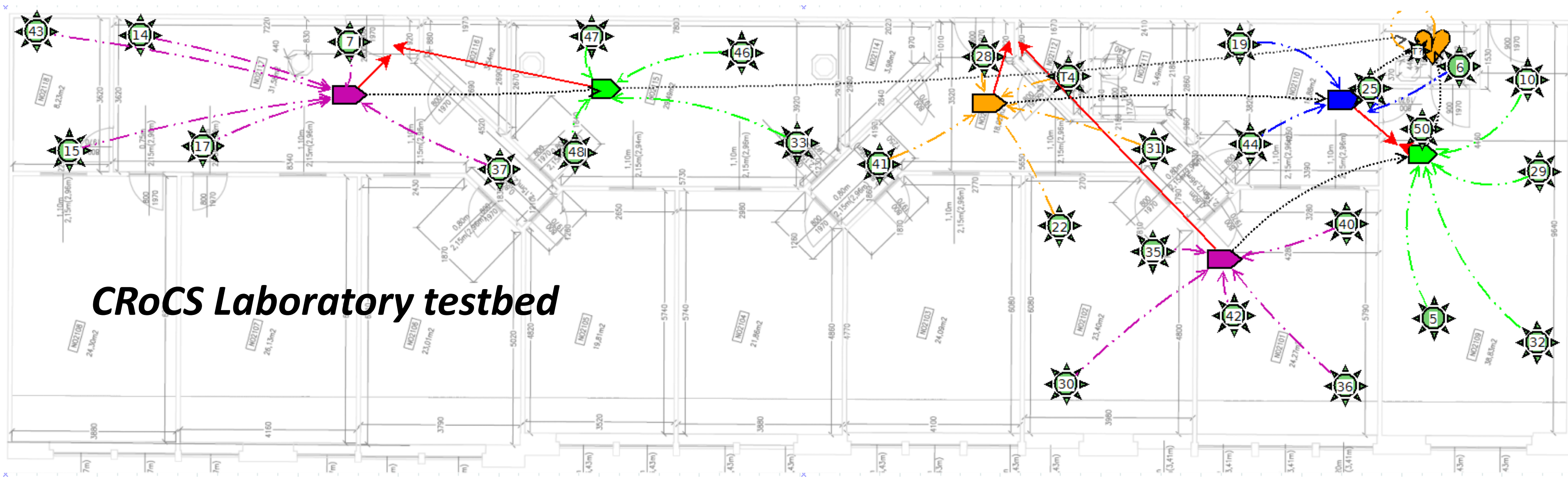
Zilog ePIR



RFID reader 125kHz

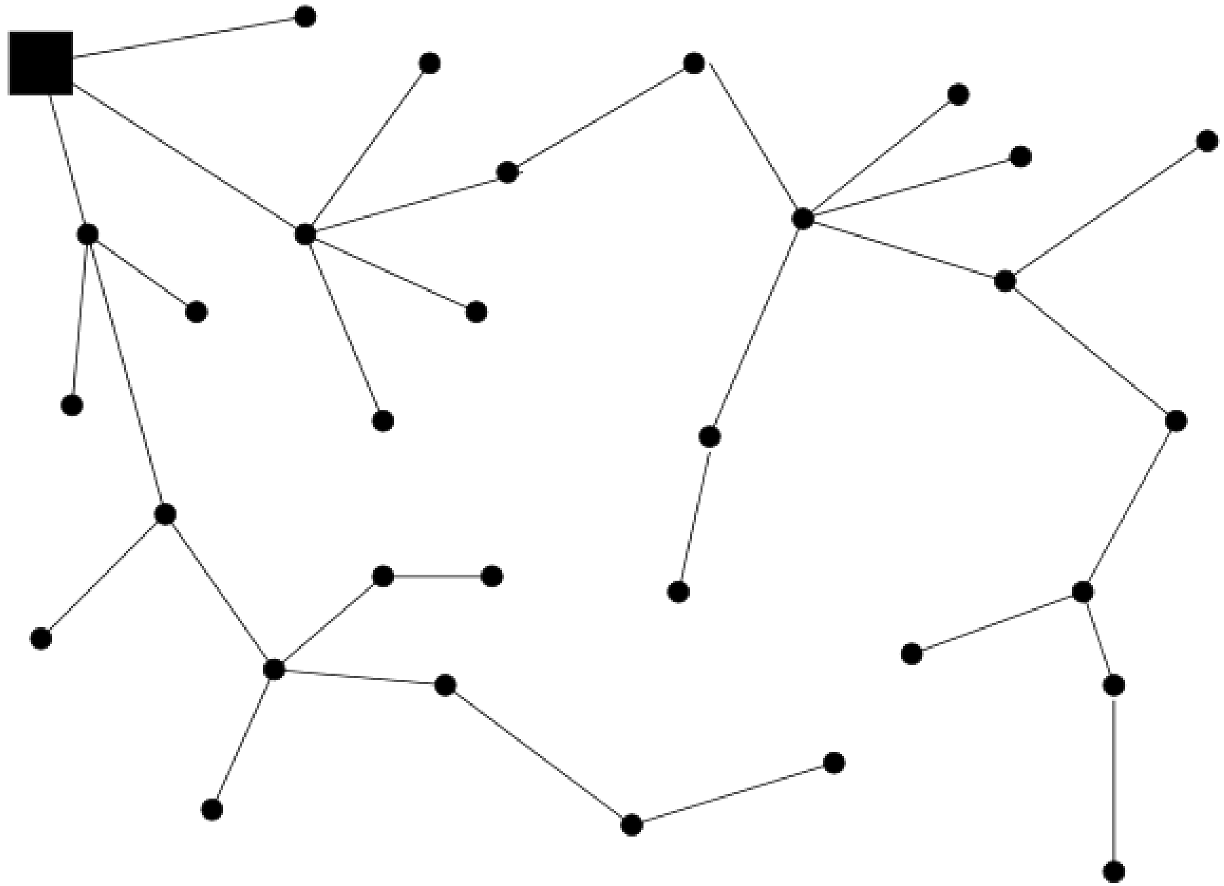
Crossbow TelosB

Crossbow MICAz



CRoCS Laboratory testbed

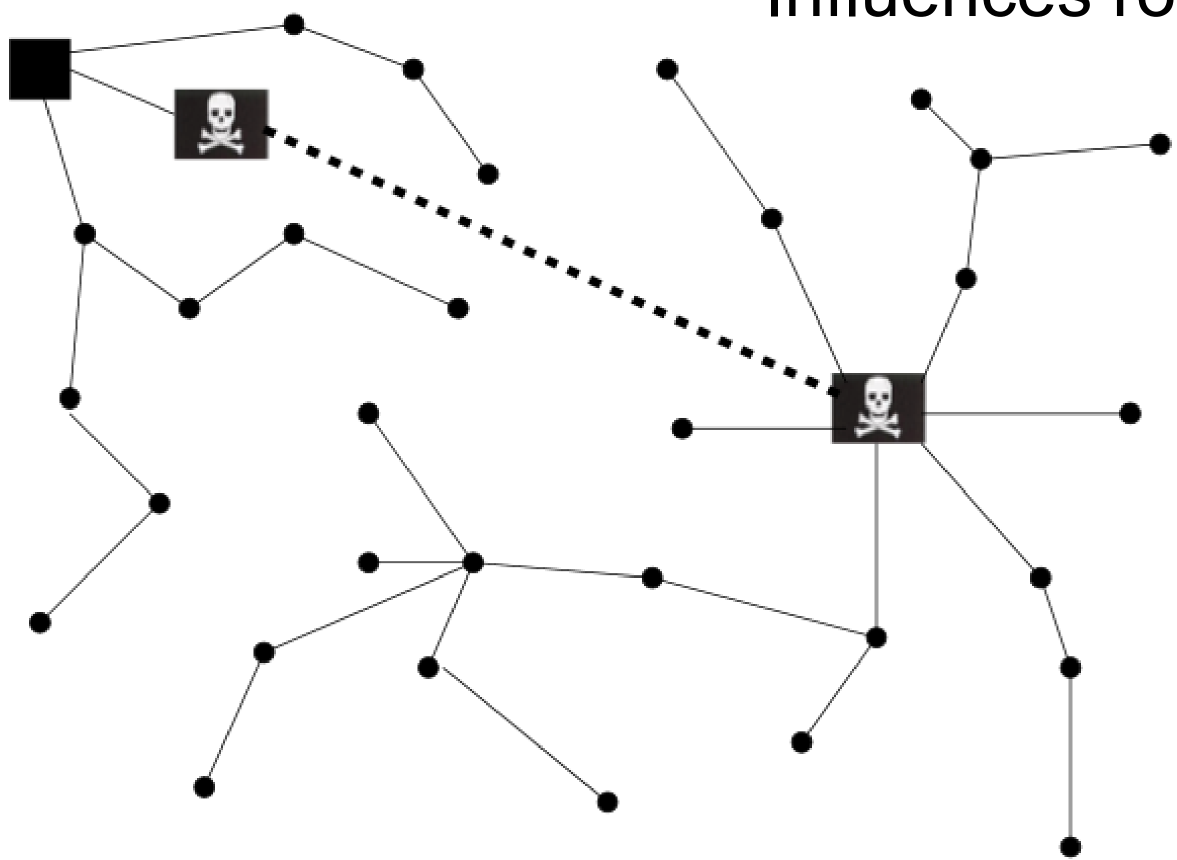
Basic topology with single sink node



Source: *http://webs.cs.berkeley.edu/papers/sensor-route-security.pdf*

Wormhole attack

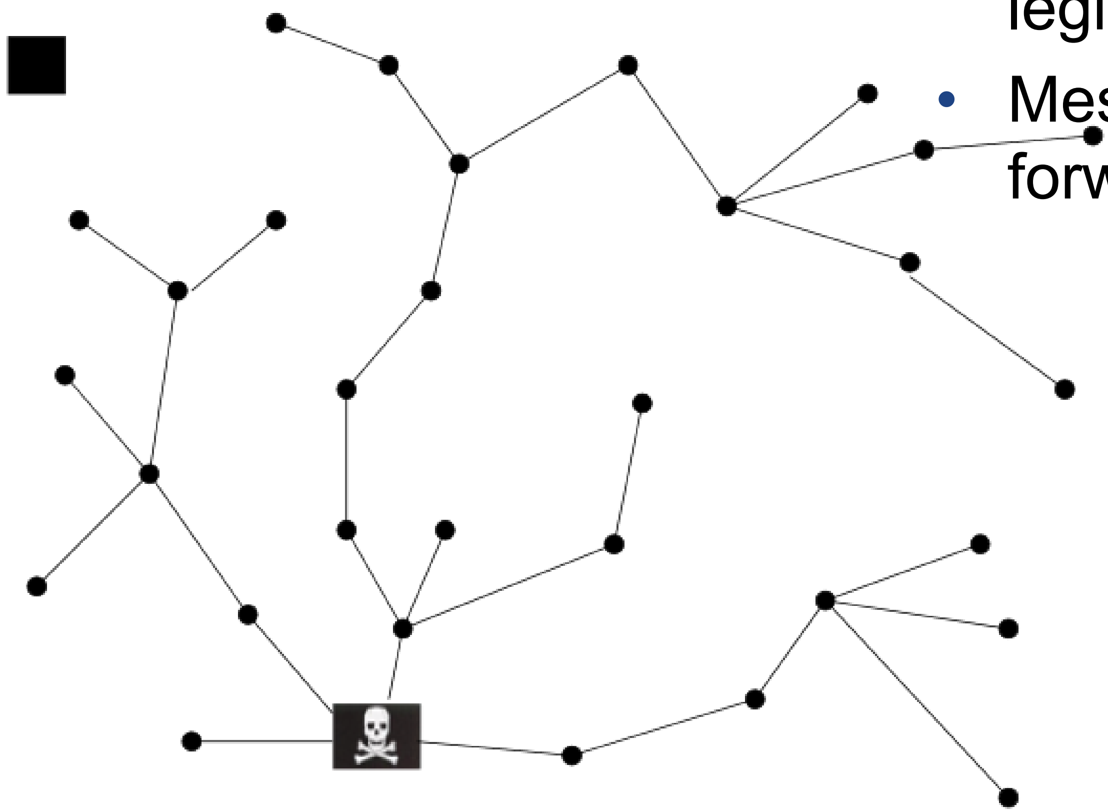
- Artificially short path(s)
- Perception of locality
- Influences routing metrics



Source: http://webs.cs.berkeley.edu/papers/sensor-route-security.pdf

Sinkhole attack

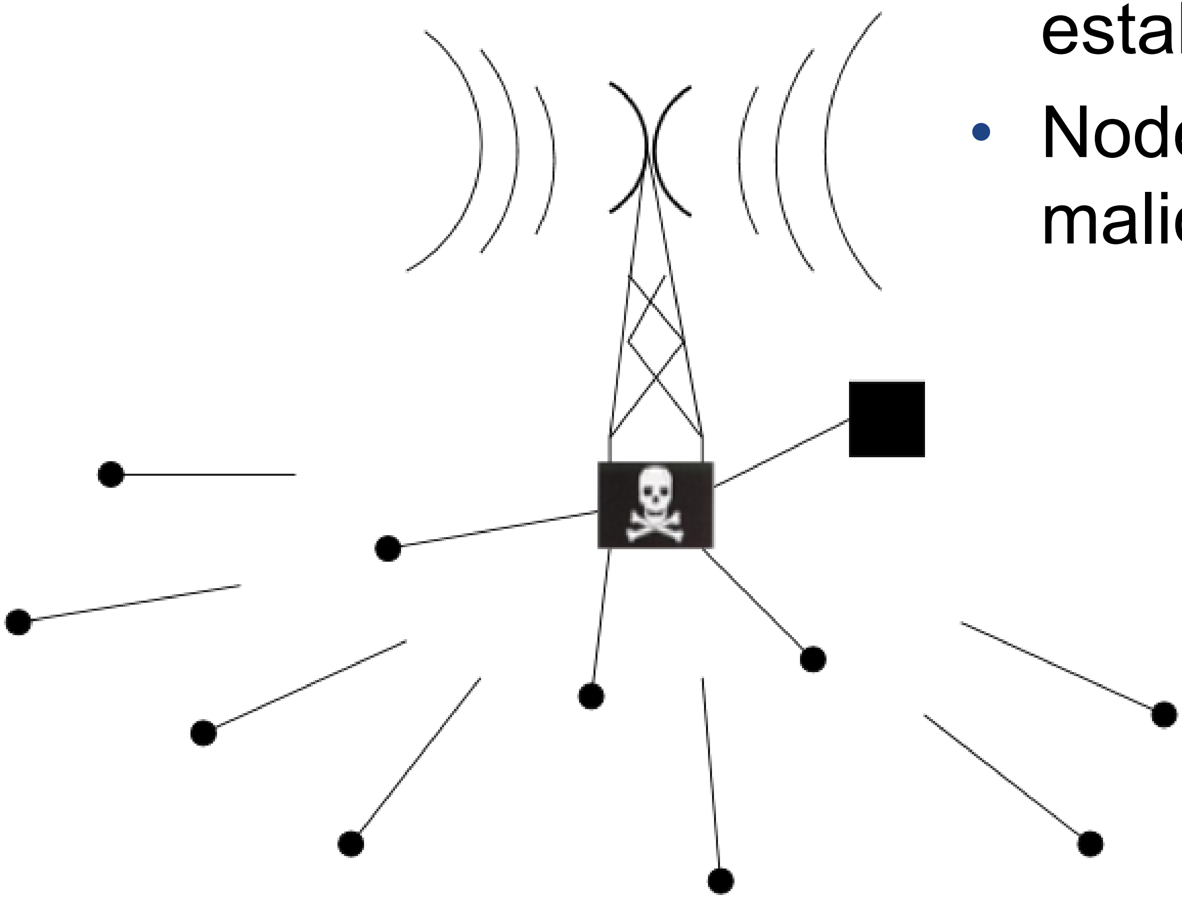
- Forge routing information, becomes malicious sink
- Messages not delivered to legitimate sink
- Messages selectively forwarded to legitimate sink



Source: http://webs.cs.berkeley.edu/papers/sensor-route-security.pdf

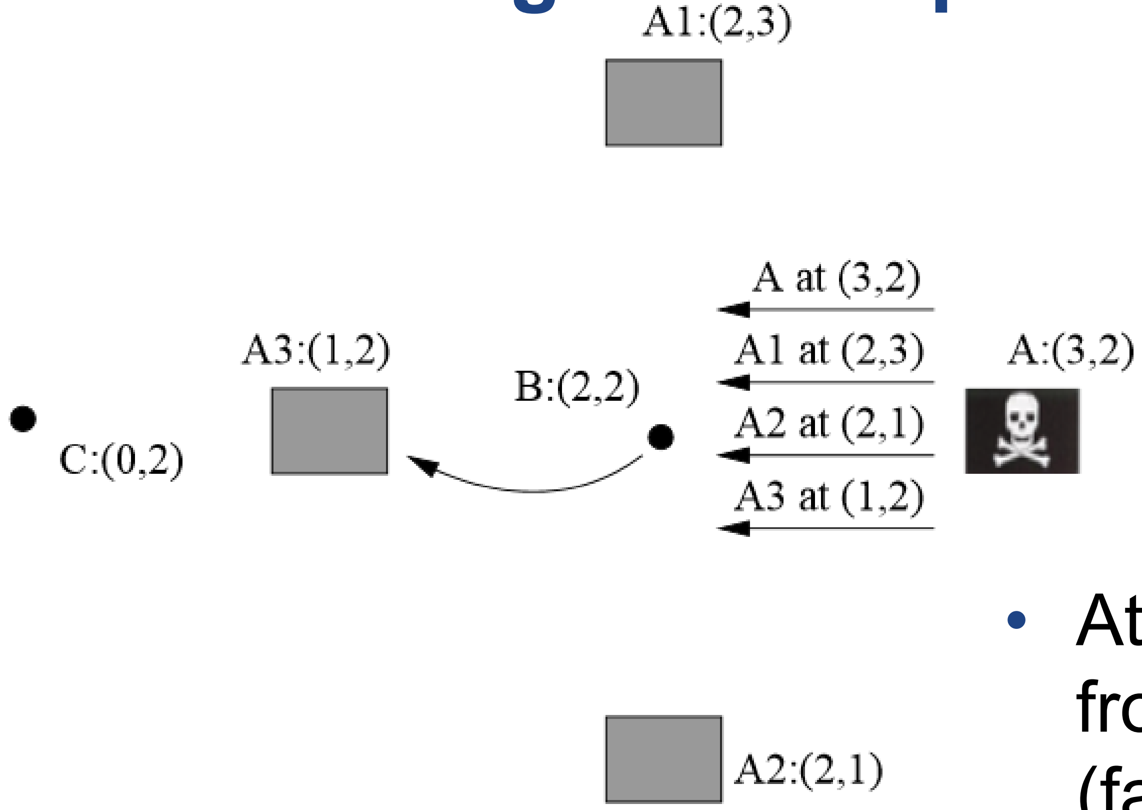
HELLO flood attack

- Strong transmission of neigh. discovery or route establishment packet
- Nodes will try to contact malicious sender



Source: *http://webs.cs.berkeley.edu/papers/sensor-route-security.pdf*

Acknowledgements spoofing

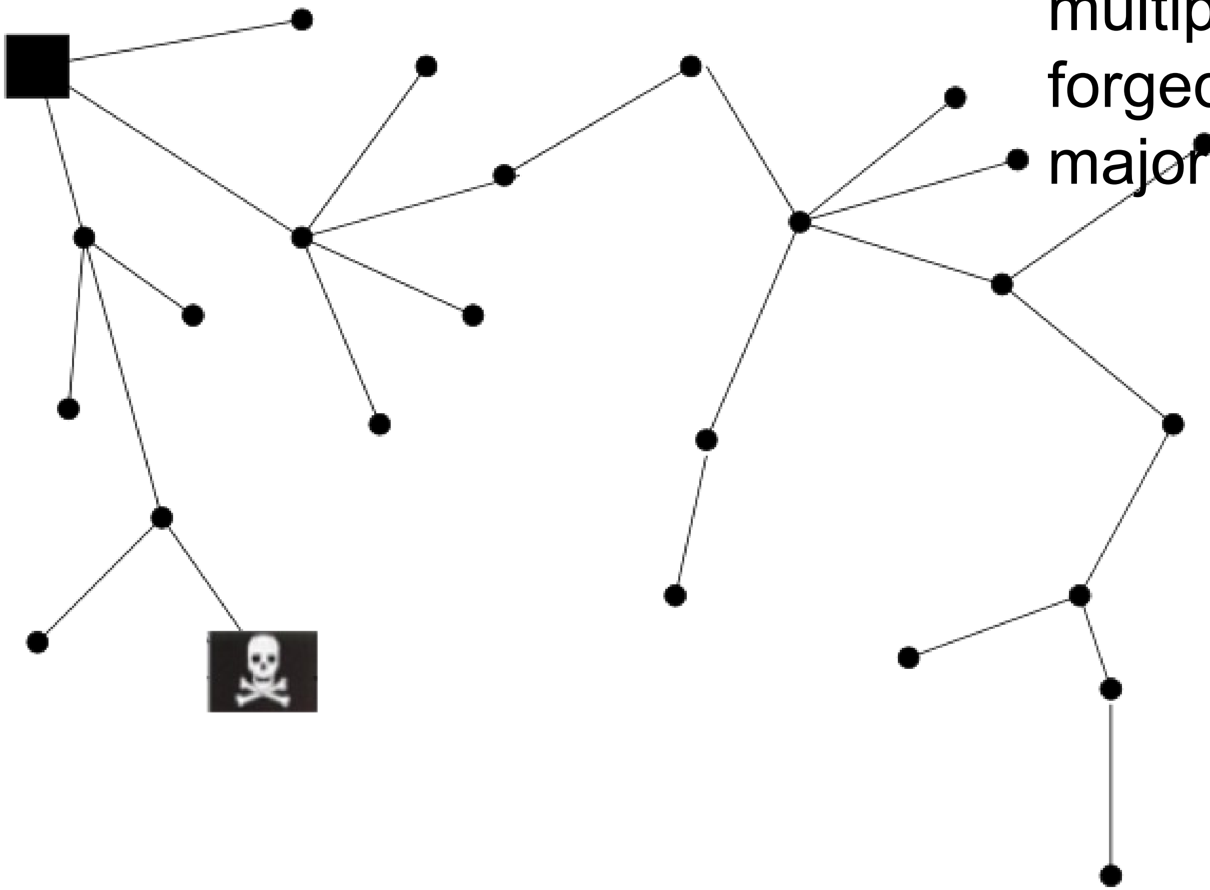


- Attacker fakes response from legitimate nodes (faster)
- Perception of closeness of non-reachable nodes

Source: http://webs.cs.berkeley.edu/papers/sensor-route-security.pdf

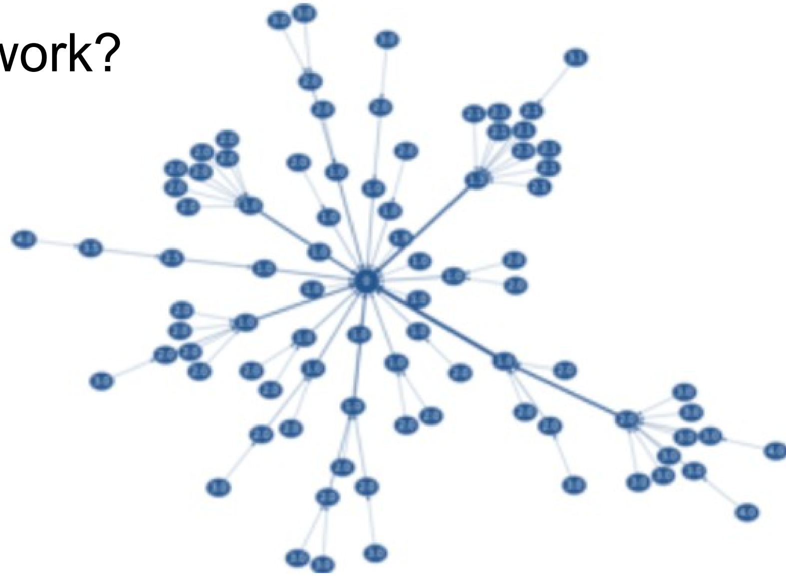
Sybil attack

- Attacker pretends to have additional nodes connected behind him
- Creates perception of multiple nodes sensing same forged event, influences majority voting…



Source: *http://webs.cs.berkeley.edu/papers/sensor-route-security.pdf*

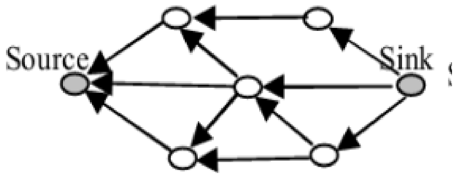
Collection Tree Protocol - security?



- How would you attack CTP-enabled network?
- Bogus routing information
  - Manipulate propagated ETX values
- Selective forwarding
  - No control of delivery
- Sinkhole
  - Advertise itself as base station (sink hole)
- Wormhole attack
  - Shortcut path between two nodes via different medium (=> preferred path)
- HELLO flood attack
  - Flood network with CTP beacons, corrupt paths and drain energy
- …

Example: Directed diffusion

- Base station floods network for named data (interest)
  - “Which node has temperate higher than 80°C?”
- Gradients with distance from base station
  - If data found, returned back via reverse path
- Properties:
  - Data-centric routing
  - Robust due to flooding
- No cryptographic protection
  - Basic version, many extensions
- Attacks:
  - Suppress flow, cloning flow (eavesdropping)
  - Selective forwarding…



(a) Propagate interest

Wireless Networks – Secure Routing

SECURE ROUTING

Why we need special routing for WSN?

- MANY existing routing schemes for ad-hoc networks
- Should have low packet overhead and node state
  - Energy efficiency
  - But: CPU/radio efficiency improves
- Should not be based on public key cryptography
  - Increases cost of hardware / transmission
  - But: ECC or pairing-based crypto?
- Should omit unnecessary complexity “any two nodes”
  - Data-centric routing
  - Energy-aware routing
  - But: depends on usage scenario

Security and efficiency tradeoff

- There is tradeoff between security and efficiency
- Q: Should I require packet/message confirmations?
  - Or just hope to be delivered to save energy?
- Q: Should I require cryptographically signed ACKs?
  - Or just detect discrepancies on base station?
- Q: Should I use multiple paths to deliver?
  - Or just one to save energy? Aggregate data?

- Always confront to your expected attacker model and usage scenario

Multipath routing algorithms

- Targets improved reliability, security and load balance
  - Reliability – probabilistically bypassing unrealiable path
  - Security – limits localized sinkhole (by bypassing it)
  - Load balance – spread of communication load (energy)
- Nature of algorithms
  - Infrastructure-based (more stable paths, infrastructure help)
  - Non-infrastructure-based (paths discovered adhoc)
  - Coding based (message split into parts via different routes)

C

Protocol Name	LFT	LB	PDR	NoP	RST	TF	PLen	Delay
EEMR [30]	VG	GD	GD	Low	Mid	Low	Low	Low
M2RC [32]	VG	GD	GD	Low	Low	Low	Low	Low
QEMPR [21]	GD	GD	GD	Low	Mid	Low	Mid	Low
EEAMR [16]	VG	FR	GD	Low	Mid	Low	Low	Low
REEM [49]	FR	GD	GD	Low	High	Mid	Mid	Low
MRMS [7]	VG	GD	VG	Low	High	Low	Low	Low
EBMR [61]	FR	FR	FR	Low	Mid	Mid	Low	Low
N-to-1 [29]	GD	FR	GD	Low	Mid	Low	Mid	Mid
SCMR [3]	GD	FR	GD	Low	Mid	Mid	Low	Low
MEEDMR [36]	PR	PR	FR	Low	Low	Low	Low	Low
SOAMR [37]	FR	FR	PR	VLow	Low	Low	Low	Low
MPDD [14]	FR	GD	VG	High	Mid	High	Mid	Mid
EERCM [46]	FR	GD	GD	Low	Low	High	Mid	Mid
HMRP [50]	FR	FR	FR	Low	Low	Mid	Low	Low
MR-ACS [56]	GD	PR	GD	Low	Low	Low	Mid	Mid
CACO [59]	GD	GD	FR	Low	Low	Low	Mid	Mid
EECA [52]	FR	FR	GD	Low	Mid	Low	Mid	Mid
MMPRSF [10]	VG	FR	GD	High	High	Low	Mid	Mid
ReInForM [8]	PR	FR	PR	Low	Mid	High	Mid	Mid
MREC [54]	FR	GD	GD	High	Mid	High	Low	Low
CAMP [19]	VG	GD	GD	High	Mid	Mid	Low	Low
REER [58]	VG	GD	GD	High	Mid	Low	Low	Low
DCHT [28]	PR	FR	FR	Mid	Low	Mid	Mid	Mid
HREEMR [16]	GD	GD	GD	High	Low	Low	Low	Low

Multipath Routing Techniques in Wireless Sensor Networks: A Survey; Kewei Sha, Jegnesh Gehlot, Robert Greve

Wireless Networks – Intrusion Detection System

INTRUSION DETECTION

Distributed intrusion detection

- Attacks considered: Jammer, Dropper, Selective dropper, Sybil, Sinkhole…

1. Promiscuity eavesdropping on IDS node
2. Gather runtime characteristics about neighbours
3. Compute monitored node "reputation"
4. If significant deviation is detected => reaction
   - Report to BS or neighbours, change routing path, block offender (time-limited suicide)…

IDS monitored network characteristics

- Signal Strength (of received packet from node)
- Carrier Sensing time (time to be clear to send)
- Packet Delivery Ratio (packets successfully forwarded by monitored node)
- Packet Send Ratio (how many packets send by monitored node were forwarded further?)
- …

Generic problems with IDS

- How long to store characteristics?
  - limited memory
- How to reliable measure all wanted characteristics?
  - usually impossible, missed/unheard transmissions
- How to detect deviances in noisy environment?
  - Natural packet loss rate, attacker just below threshold
- How monitoring node should survive on batteries?
- How NOT to be tricked by attacker to blame legitimate node?

Summary

- WSNs specifics: Limited communication, local knowledge, partial compromise
- Many factors influence resulting network settings
  - Usage scenario
  - Available hardware parameters => network topology
  - Sensitivity and nature of data processed => attacker model
- Area is currently flooded with different protocols
  - Have good understanding of basic principles
  - Be critical in judging various proposal
  - Have clear definition of usage scenario & attacker model

Mandatory reading

- Ch. Karlof, D. Wagner, Secure routing in wireless sensor networks: attacks and countermeasures (2003)
- http://webs.cs.berkeley.edu/papers/sensor-route-security.pdf