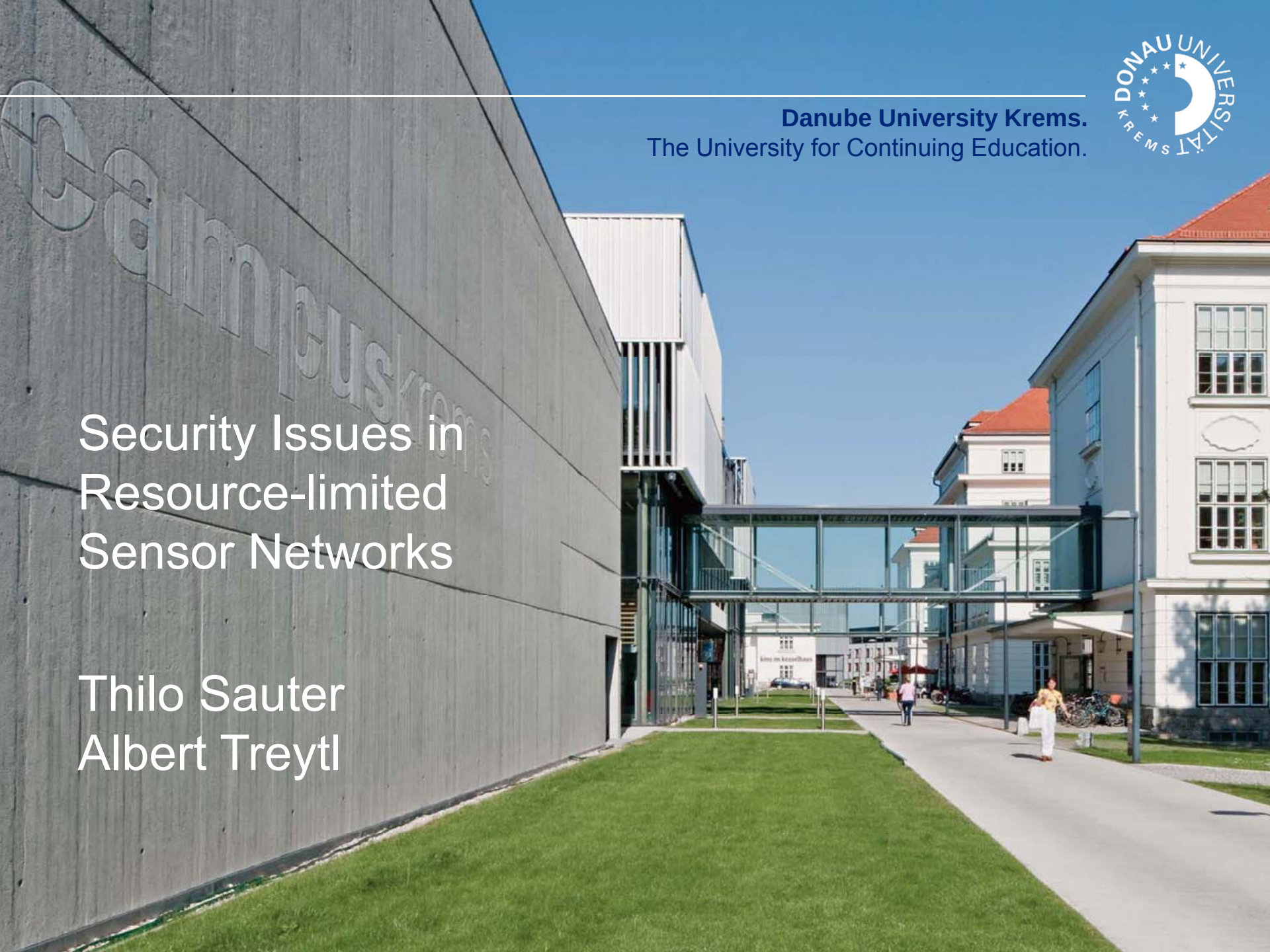
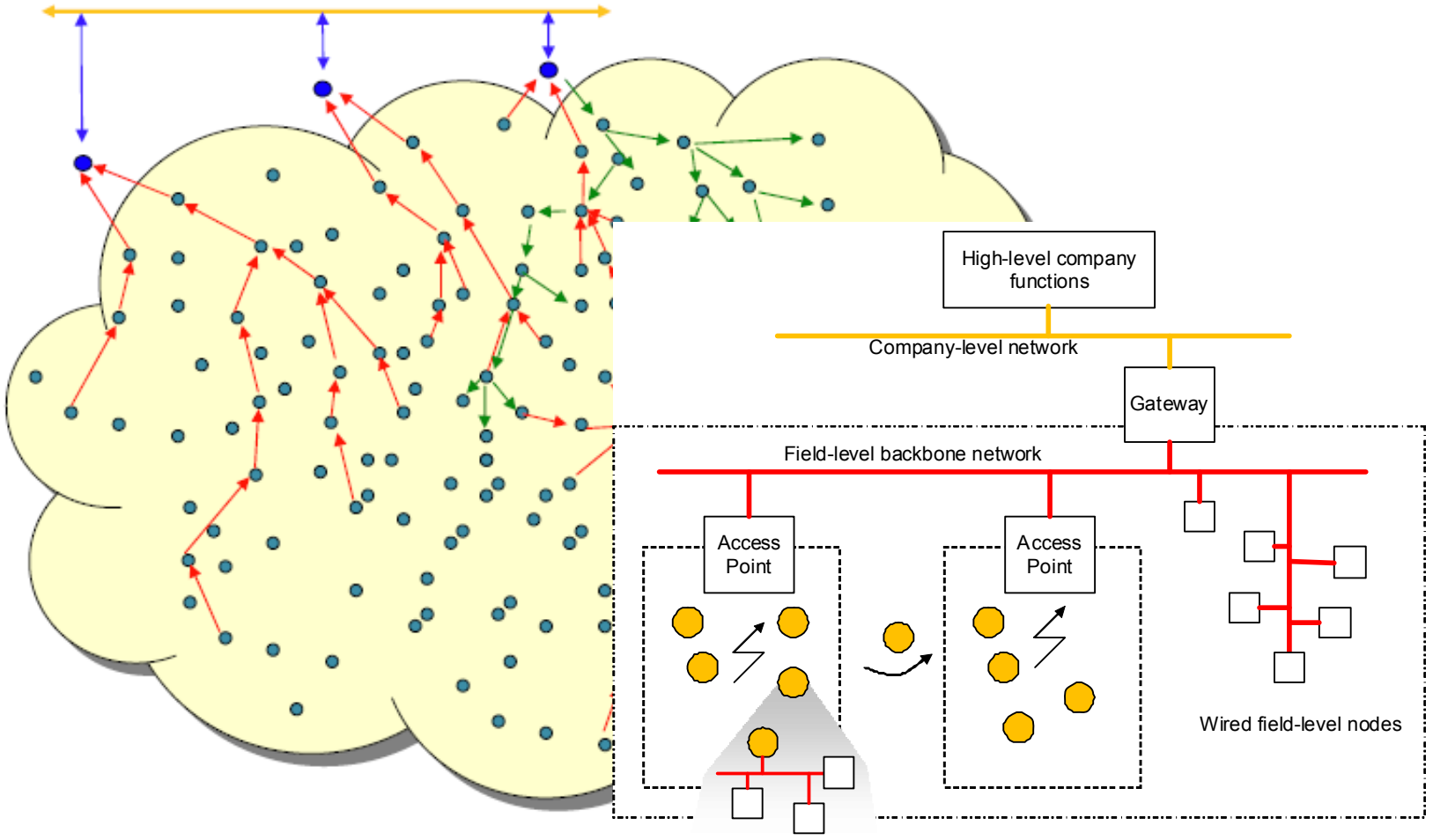

Danube University Krems.
The University for Continuing Education.
Security Issues in Resource-limited Sensor Networks
Thilo Sauter
Albert Treytl

Wireless Sensor Network Vision



Content – Take Home Messages

- Security needs proven methods
  - But sensor networks are different from IT networks
- Security needs time
  - But computing resources are limited
- Security needs extra communication
  - But bandwidth is often limited
- Outlook
  - Security beyond classical protection

Basic Security Considerations

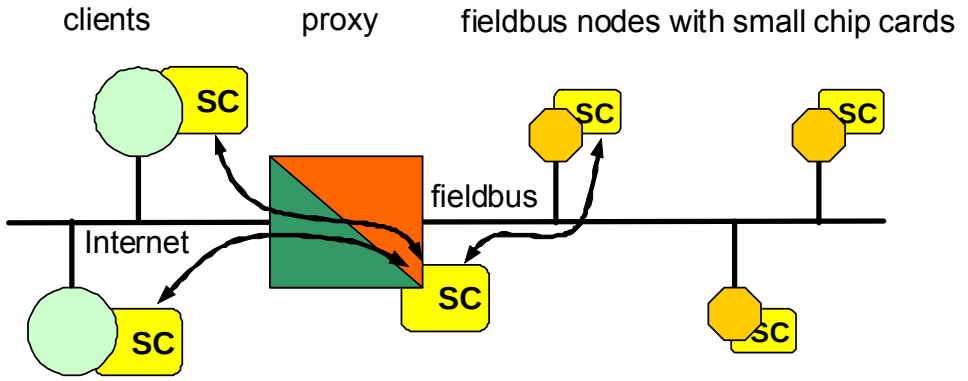
- Kerkhoff principle
  - The security of a system should only rely on the secrecy of the used credentials (keys)
  - An algorithm can only be assumed to be save when it is publicly reviewed
  - No security by obscurity!
  - Security tokens can/should be used to store keys and execute crypto algorithms
- Claude Shannon: “The enemy knows the system.”
  - Attackers are using powerful computers, not raspberry pies
- Use standard cryptography!
  - No shorter keys
  - No other, weaker algrorithms

Security vs. Interoperability

- Sensor networks require interoperability
  - Automatic configuration (ad-hoc networking)
  - Plug and Play/Participate/Produce
  - Extensibility of installations
  - Open system
- Security goals are contradicting
  - “What is not explicitly allowed is forbidden”
  - Access restriction to permitted entities
  - No intrusion via attachment of additional external devices
  - Closed system

The Real (W)SN World

- Nodes are not always under the control of the operator
  - Worst case: building automation, energy distribution
  - Easy access for potential hackers
  - Tamper-proof hardware in distributed systems is difficult
- Use of dedicated security tokens
  - Limited node resources
  - Bottleneck serial interface
- End to end security connections
  - Integration of gateways to translate between different resources/domains



Content – Take Home Messages

- Security needs proven methods
  - But sensor networks are different from IT networks
- Security needs time
  - But computing resources are limited
- Security needs extra communication
  - But bandwidth is often limited
- Outlook
  - Security beyond classical protection

Security Considerations

- Computing time needed for security algorithms is crucial
  - Especially in real-time networks
  - Transmission time is another issue (message size)
- Symmetric cryptography (shared keys)
  - Small overhead, short length for message authentication codes
  - Lightweight implementation even in small processors
- Asymmetric cryptography
  - Popular in the IT world (public key infrastructures)
  - Large messages and computing times -> no real-time capabilities
- Symmetric keys are not as bad as their reputation

Performance Analysis

- For 8051 core
  - 8 bit, 8 MHz
  - Still used in field devices
- 3-DES has smallest oberhead, yet is outdated
- Asymmetric algorithms are very slow
  - In particular RSA
  - ECC has less overhead
- AES seems best suited overall

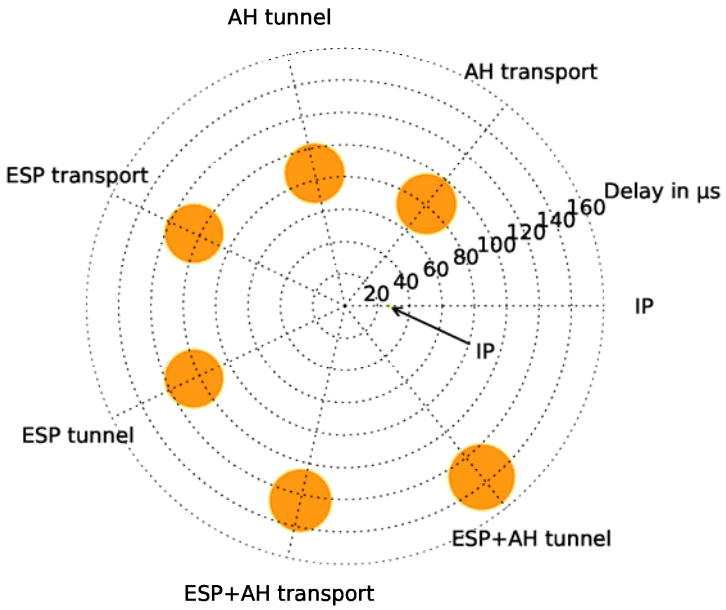
Algorithm	Block size for encryption and MAC	Execution time
3-DES	8 bytes	18ms
AES (128-bit key)	16 bytes	12.195ms
AES (128-bit key) CBC	16 bytes	13.536ms
AES (128-bit key) CFB	16 bytes	15.663ms
RSA	128 bytes	6.12s/155s**
ECC	40 bytes	40.5s/600s**

** for signature and verification, respectively

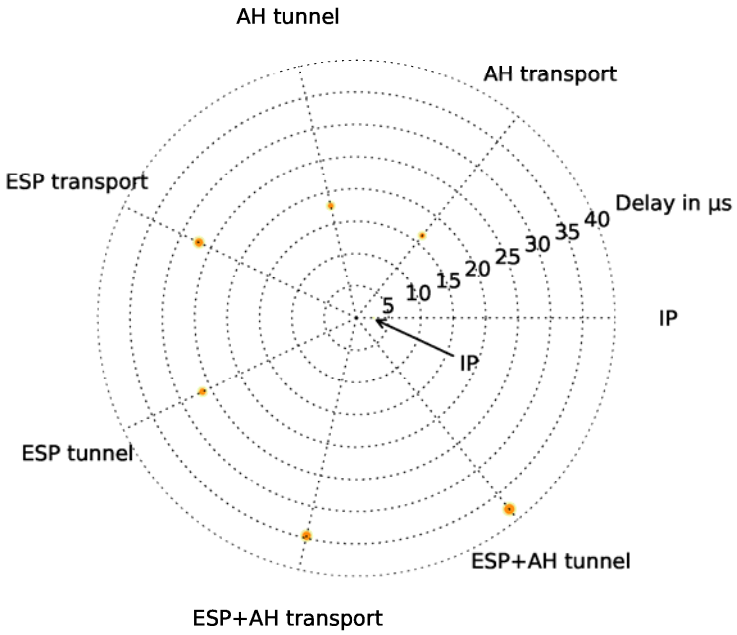
MAC – Message Authentication Code, AES – Advanced Encryption Standard,
DES – Data Encryption Standard, RSA – Rivest, Shamir und Adleman crypto algorithm,
ECC – Elliptic Curve Cryptography

Computation Delay of IPsec Layer

Delay of Incoming IP Packets



Delay of Outgoing IP Packets



- Embedded Linux device
  - 32 bit, 200 MHz

AH … Authentication Header
ESP … Encapsulating Security Payload

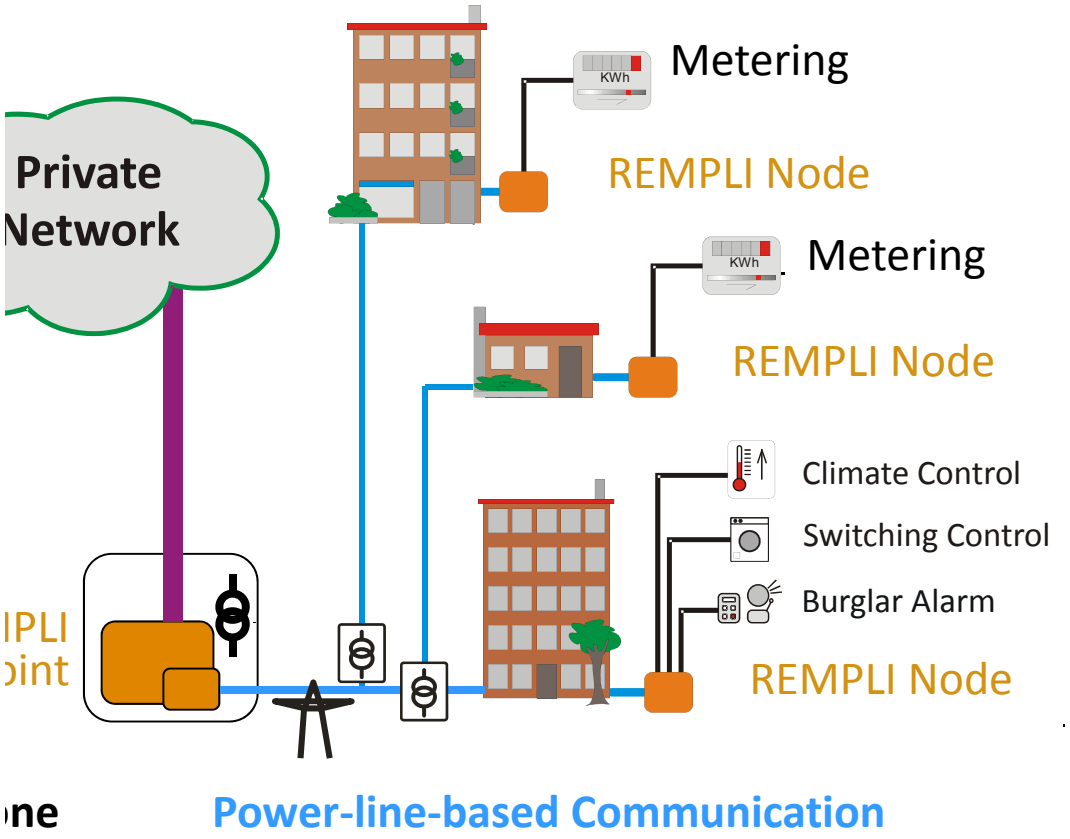
Content – Take Home Messages

- Security needs proven methods
  - But sensor networks are different from IT networks
- Security needs time
  - But computing resources are limited
- Security needs extra communication
  - But bandwidth is often limited
- Outlook
  - Security beyond classical protection

Utility Company

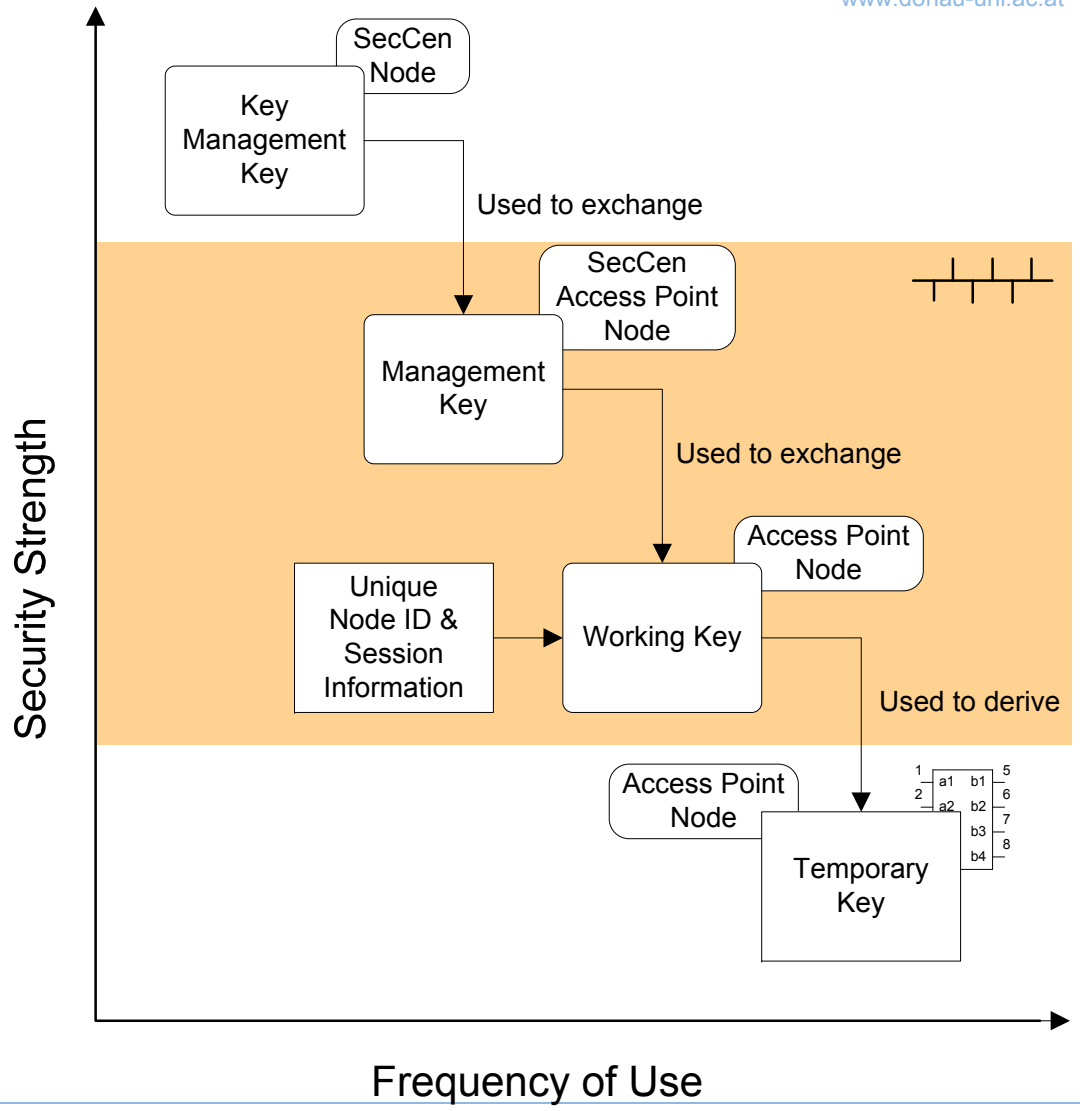
- Limited bandwidth
  - 30-100 kbit/s
  - 20% packet loss
- Small packet size
  - 20 to 50 byte payload
  - Up to 100 kB application data
  - Mostly only MAC, no complex encryption
- End-to-end communication
  - Strict limits for packet delay
  - Security measures critical
- Low-cost node (processor)
  - Limited resources

Customers



Key Management

- Security does not only mean MAC and cipher overhead in the messages
- Regular key update is needed too
  - Secure distribution process!
  - Mind the network load!
- Solution: hierarchical key derivation
  - Lower-level keys are derived from higher-level keys and distributed
  - Update more frequently for lower levels
- Limited lifetime for low-level keys
  - Stored in (insecure) processor memory
  - Lowest-level keys are derived autonomously, not distributed

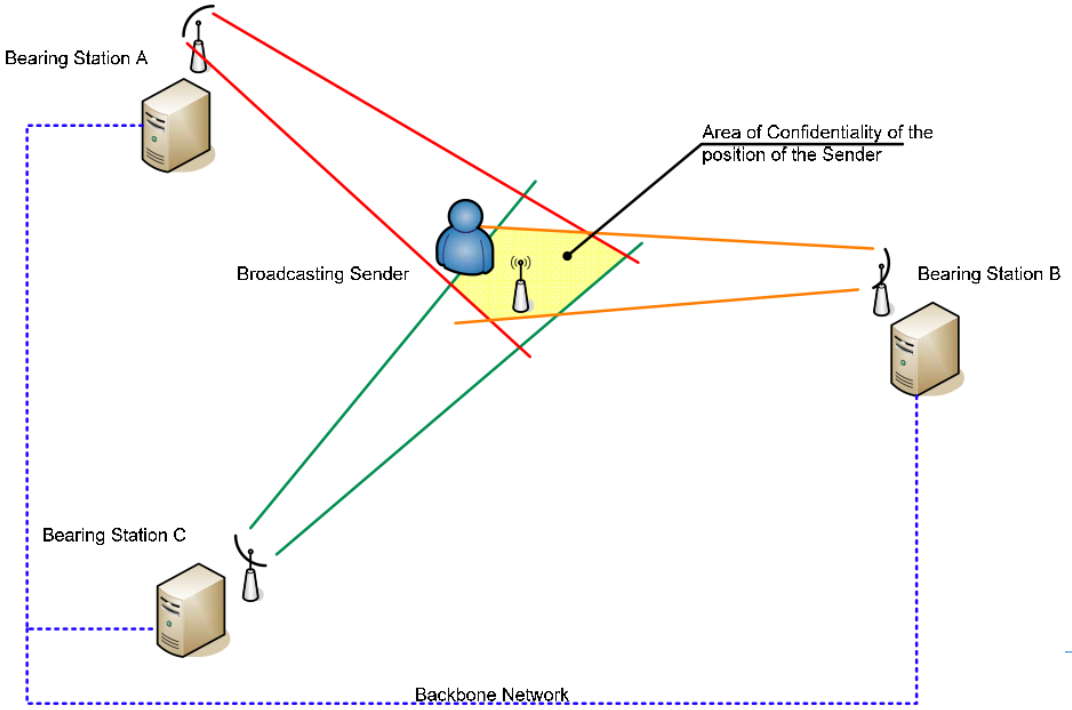


Content – Take Home Messages

- Security needs proven methods
  - But sensor networks are different from IT networks
- Security needs time
  - But computing resources are limited
- Security needs extra communication
  - But bandwidth is often limited
- Outlook
  - Security beyond classical protection

Location-based Security

- Nodes are moving, can we trust them?
  - Position detection is a feature of the (trusted) network infrastructure
  - Access to communication resources depends on the location
- Inverse GPS scenario
  - No need to modify client
  - Each point must be covered by multiple (≥3) access points
- Security benefits
  - Strengthen defense-in-depth concept by integration of physical access barriers
  - Combine the security advantages of wired systems with the flexibility of wireless systems



Conclusions and Outlook

- Sensor networks are different from classical IT networks in many ways
  - Spatial extension
  - Ad-hoc behaviour
  - Limited computing and communication resources
  - Often real-time applications
- Still we need to employ proven IT security mechanisms
  - But combined in a clever way
  - Tailored to the needs and capabilities of the system
- Further issues
  - Inspection/correlation of data
  - Statistical or model-based anomaly detection
  - Intrusion detection

Danube University Krems.
The University for Continuing Education.

Albert Treytl, Thilo Sauter
Center for Integrated Sensor Systems
Danube University Krems

www.donau-uni.ac.at/ziss
Thilo.sauter@donau-uni.ac.at