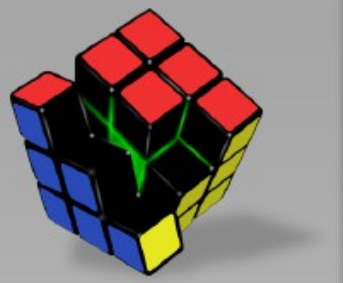


technische universität
dortmund

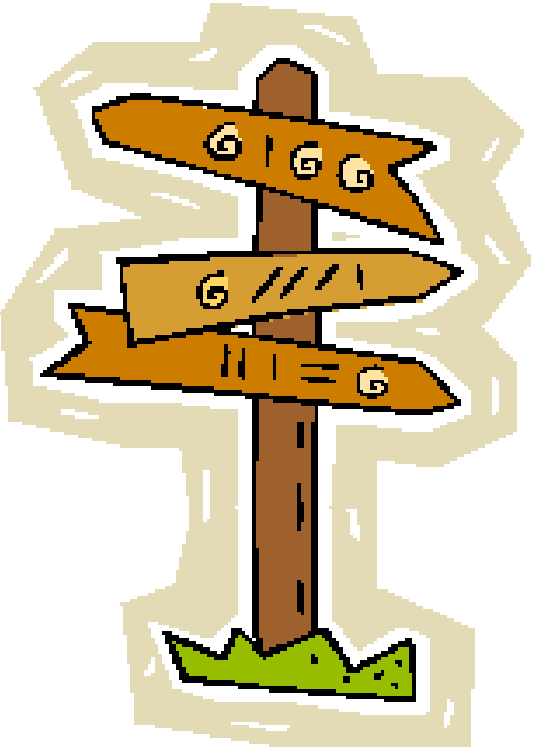
Sicherheit in Sensornetzwerken

Seminarphase zur PG Solar Doorplate
WS 2015/16

Todor Nikolov | Haltern am See | 17.10.2015

Gliederung

- Sensornetzwerke: Motivation und Einblick
- Sicherheitsanforderungen
- Angriffsarten
- Sicherheitsprotokolle
- MSP430-Krypto-Einheit
- Zusammenfassung

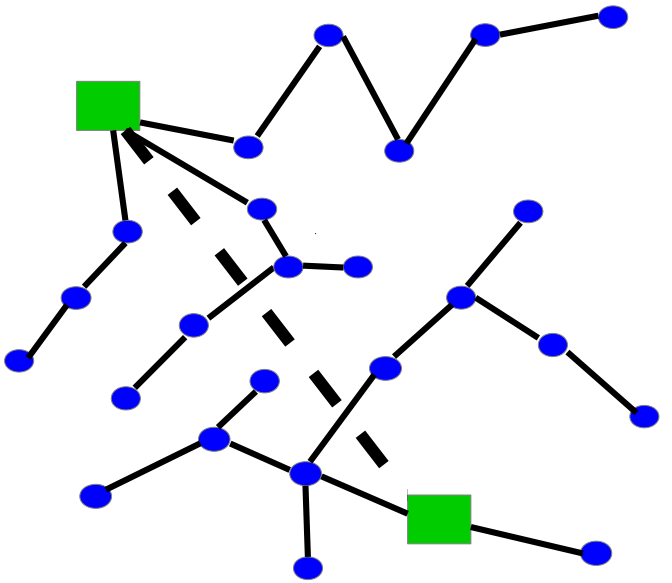


Warum Sicherheit ?

- Schutz der Privatsphäre
  - Geheimhaltung von personenbezogenen Daten
  - keine illegale Überwachung
- Bewahrung von Firmengeheimnissen
  - Verhinderung von unfairer Konkurrenz durch Datenklau
- vertrauenswürdige Informationen
  - Nachweis von Herkunft und Korrektheit
- ...

Sensornetzwerke: Struktur

- Basisstation(en)
  - hinreichend viel Speicherplatz und Energie
  - leistungsvolle Funkkommunikation mit großer Reichweite
- Sensoren
  - extreme Ressourcenknappheit
  - teure Funkkommunikation
- Kommunikationsmuster
  - viele zu einem
  - eins zu vielen
  - lokaler Nachrichtenaustausch



Basisstation

Sensorknoten

geringe Bandbreite

große Bandbreite

Gefahren

- unsichere Kommunikationskanäle
  - Abhören, Duplikation, Modifikation
- kooperierende böswillige Sensorknoten
- Basisstation(en) als Vertrauensgrundlage
  - legitimes Verhalten, sichere Datenaufbewahrung
- keine Manipulationssicherheit von Sensorknoten
  - Zerstörung, Umprogrammierung
  - Diebstahl von kryptographischen Schlüsseln

Sicherheitsanforderungen

- Die Klassiker:
  - Vertraulichkeit
  - Authentizität (Damit auch Integrität)
  - Datenfrische
  - Verfügbarkeit

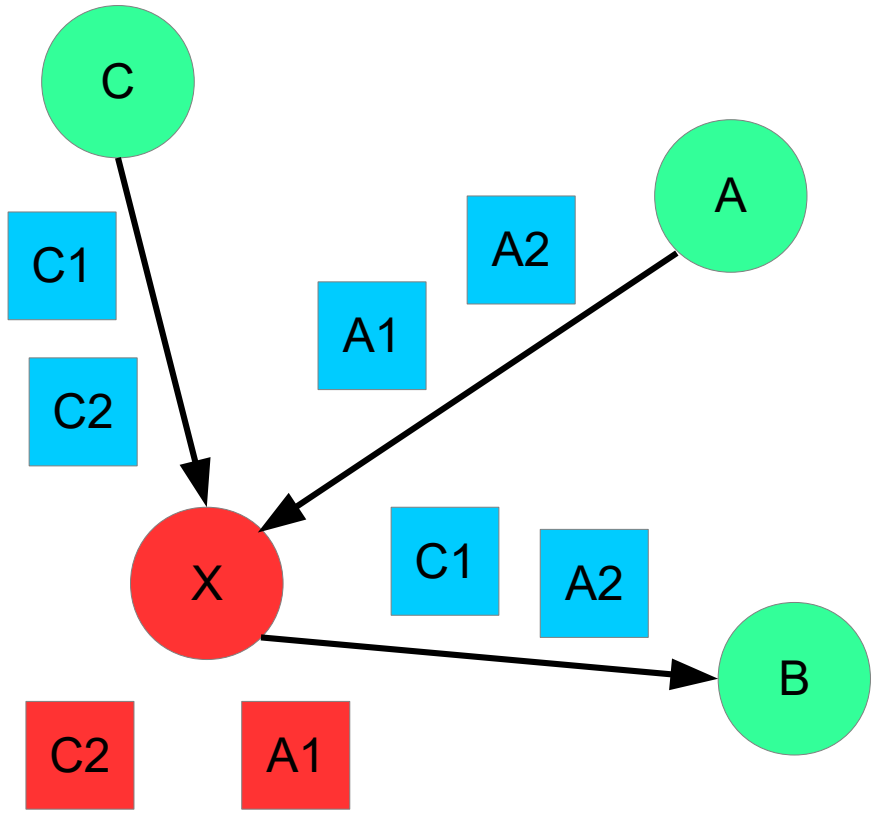
- Speziell für Sensornetzwerke
  - Zeitsynchronisation
  - Standortermittlung
  - Crypto-Key Management

Angriffe: DoS - Attacke

- Denial of Service = Dienstausfall
- Zu verursachenden Schäden
  - Lahmlegung der Kommunikation
  - Batterieaustrocknen
  - ...
- Umsetzungswege
  - Senden von Rauschen (Übertragungsschicht)
  - Auslösung von Paketkollisionen (Sicherungsschicht)
  - Verhinderung des Routings (Netzwerkschicht)
    - Selektive Weiterleitung
    - Sybilangriff
    - ...

Routingsattacken (1)

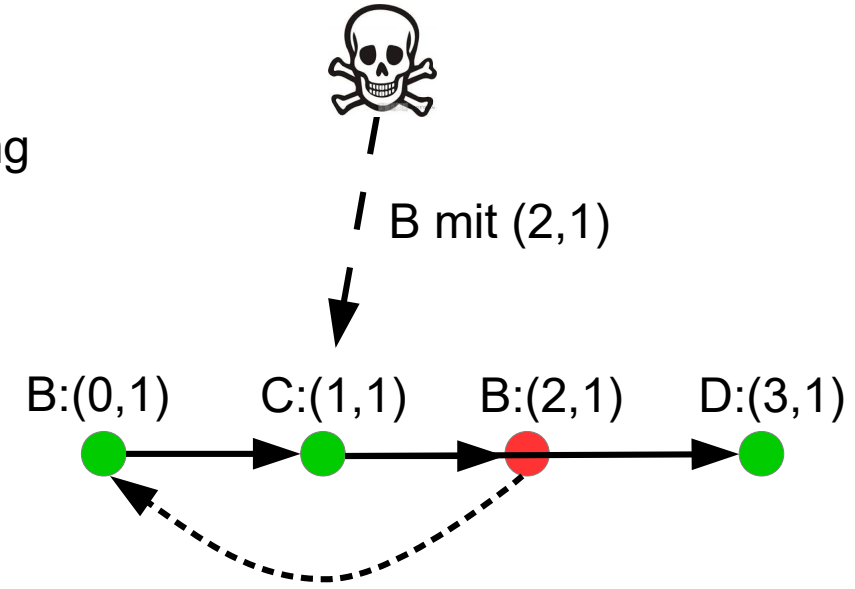
- Selektive Weiterleitung
  - (teilweises) Verwerfen von Datenpaketen



- Manipulation von
  - Datenkenngrößen (Mittelwert)
  - Basisstationanfragen
- Abwehr:
  - Mehr-Pfad-Routing
    - Senden des gleichen Pakets über ***n*** disjunkte Pfade
  - Zufälliges Routing
    - Nicht-deterministische Auswahl des nächsten Hops

Routingsattacken (2)

- Sybilangriff
  - Verwendung von mehreren Identitäten
  - Ziele:
    - Verhinderung von Mehr-Pfad-Routing
    - Erzeugung von Dead-Links
    - Verlängerung von Routen
    - Routing-Schleifen
  - Einfluss auf
    - Netzwerktopologie
    - Fehlertoleranz – Mechanismen



- Identitätsverifikation als Gegenmaßnahme notwendig

Schutzmechanismen

- Beispiele
  - Kryptographie
  - Sequenzzahlen
  - Nonce (= einmaliges Zufallsdatum)

- zwei fundamentale Probleme
  - keine asymmetrische (!) Verschlüsselung möglich
    - Grund: Knappheit von Speicherplatz
    - Umweg über symmetrische Verfahren
  - sichere Verteilung und Verwaltung von Kryptoschlüsseln

    ==> SPINS

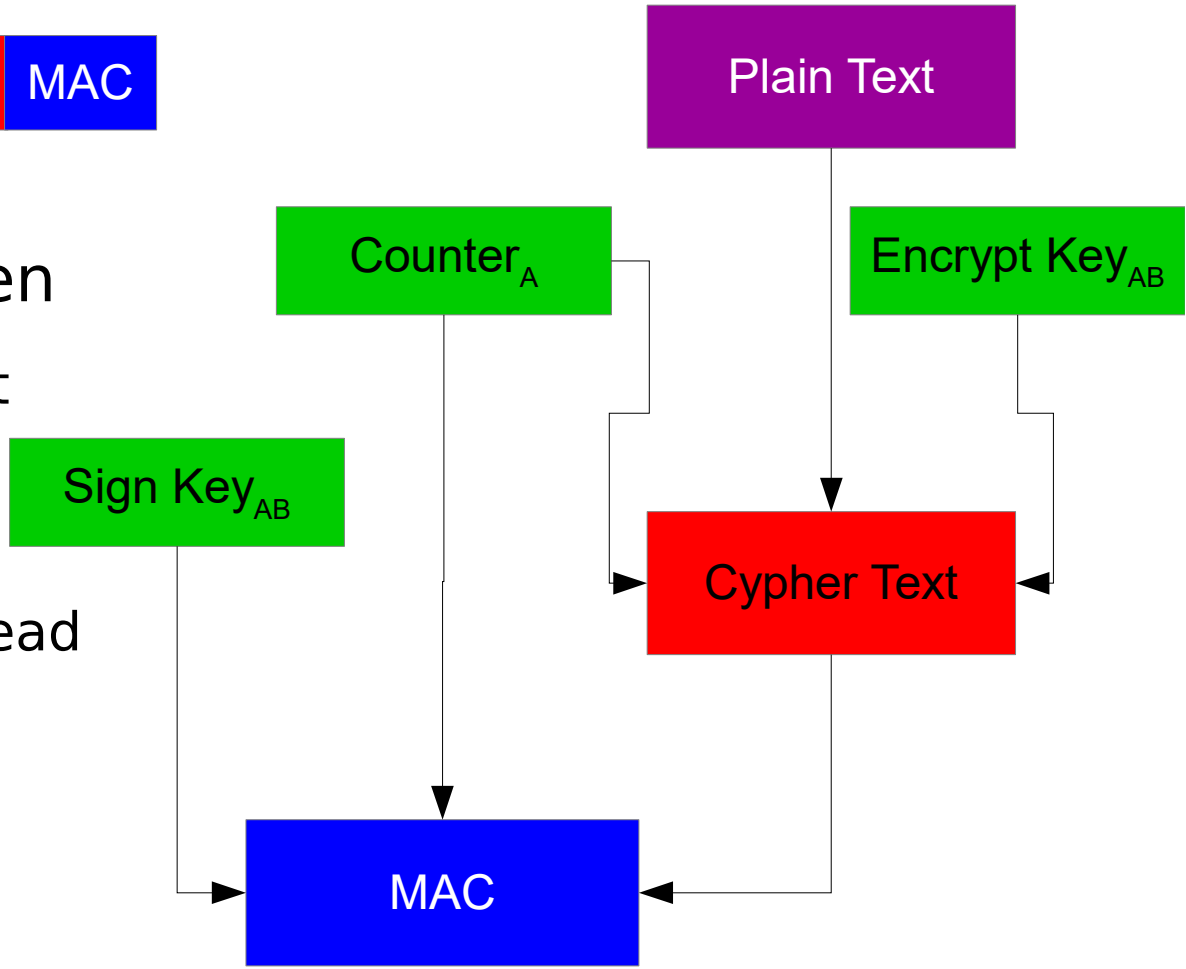
SPINS: Ein Sicherheitsansatz

- SPINS = Security Protocols for Sensor Networks
- Zwei Komponenten
  - SNEP (Secure Network Encryption)
    - Vertraulichkeit
    - Authentizität
    - Datenfrische
  - µTesla (abgespeckte Version von TESLA)
    - authentifiziertes Broadcast
      - Konzeptionel für Basisstationen
      - Anwendbar auch für Sensorknoten
- Grundannahmen
  - Sensorknoten angreifbar, Basisstationen sicher

SNEP (1)

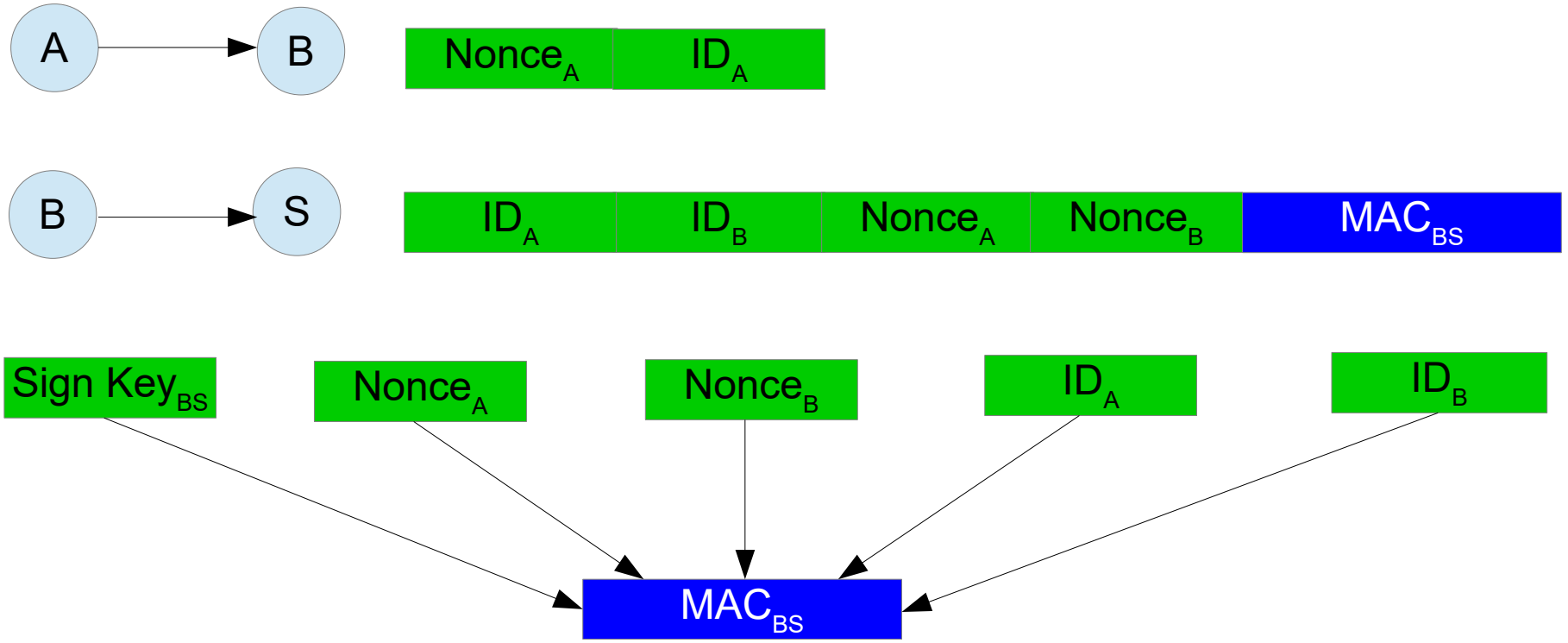
- Nachrichtenaustausch

- Erreichte Eigenschaften
  - semantische Sicherheit
  - Datenauthentizität
  - geringerer Kommunikationsoverhead
  - Datenfrische

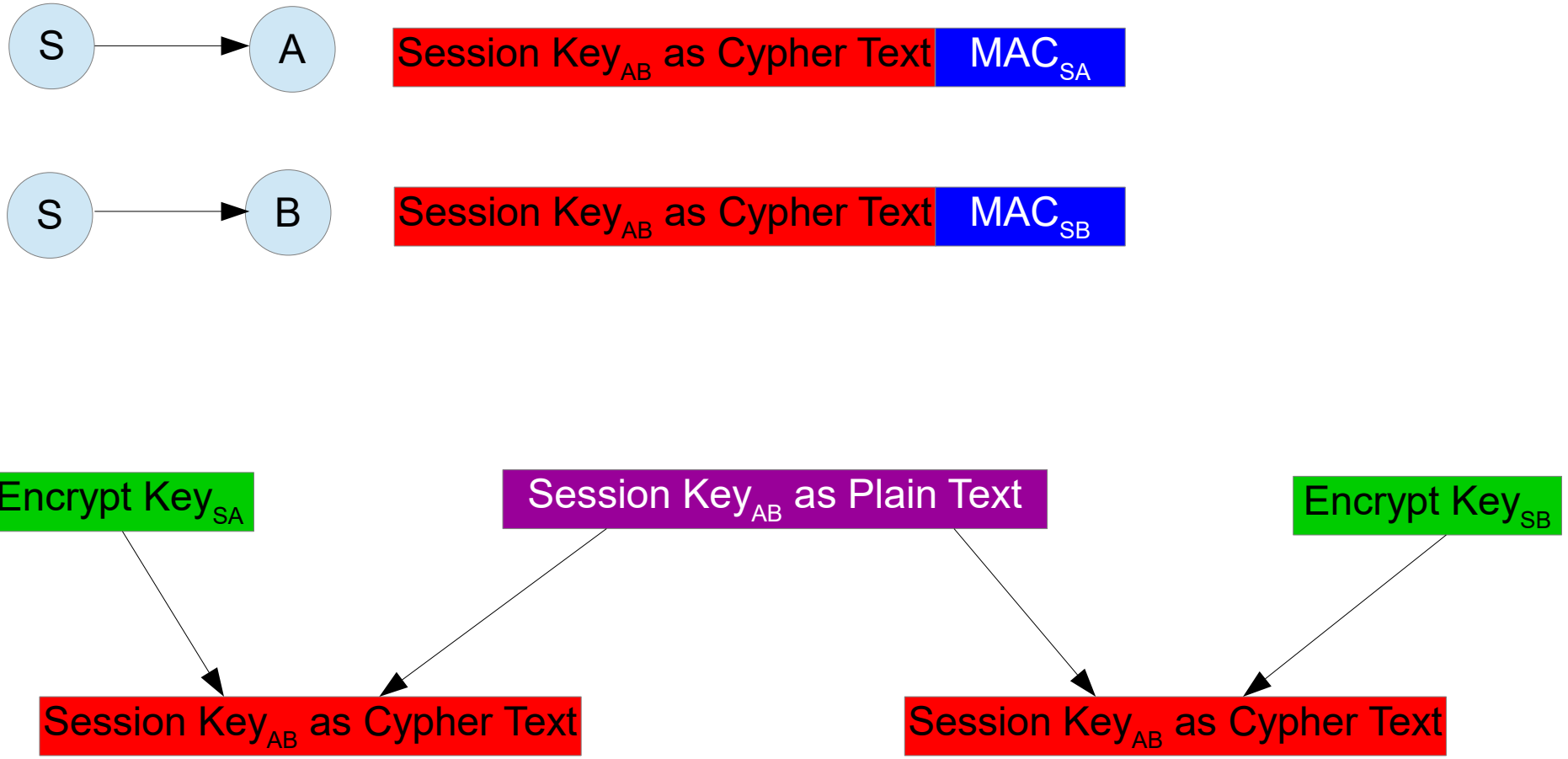


SNEP (2)

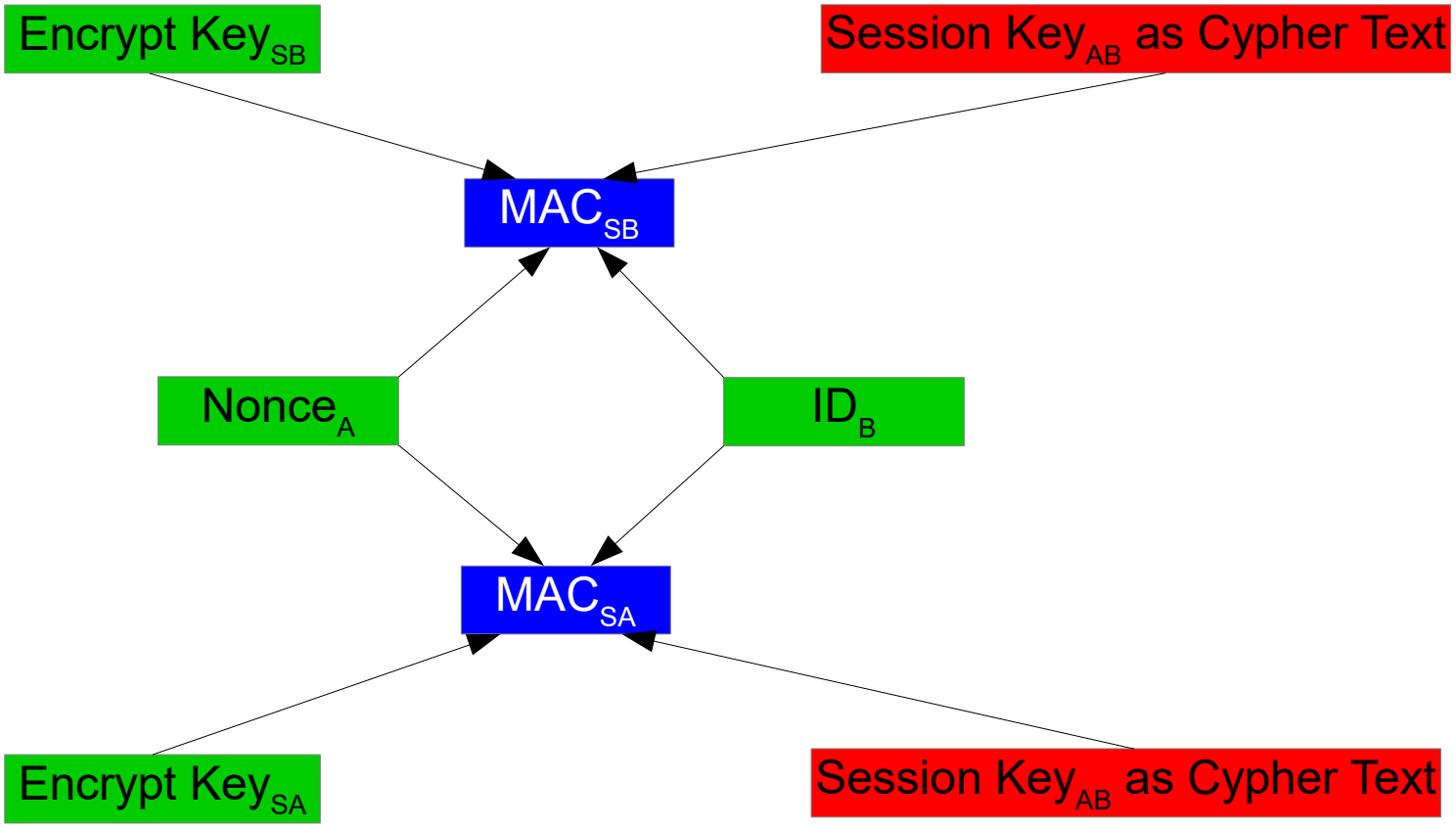
- Einsatz von Key – Bootstrapping
  - Ein mit der Basisstation geteilter Schlüssel pro Knoten
  - Keine gemeinsamen Kryptoschlüssel zwischen den Knoten
- Vereinbarung von Sitzungsschlüsseln notwendig



SNEP (3)


S
A
Session Key$_{AB}$ as Cypher Text
MAC$_{SA}$
S
B
Session Key$_{AB}$ as Cypher Text
MAC$_{SB}$
Encrypt Key$_{SA}$
Session Key$_{AB}$ as Plain Text
Encrypt Key$_{SB}$
Session Key$_{AB}$ as Cypher Text
Session Key$_{AB}$ as Cypher Text

SNEP (4)


Encrypt Key$_{SB}$
Session Key$_{AB}$ as Cypher Text
MAC$_{SB}$
Nonce$_{A}$
ID$_{B}$
MAC$_{SA}$
Encrypt Key$_{SA}$
Session Key$_{AB}$ as Cypher Text

µTESLA (1)

- Zweck: Authentifiziertes Broadcast
  - durch symmetrische Kryptographie realisiert!

- Kette von Kryptoschlüsseln K_0, K_1, …, K_n

  K_n - zufällig generiert

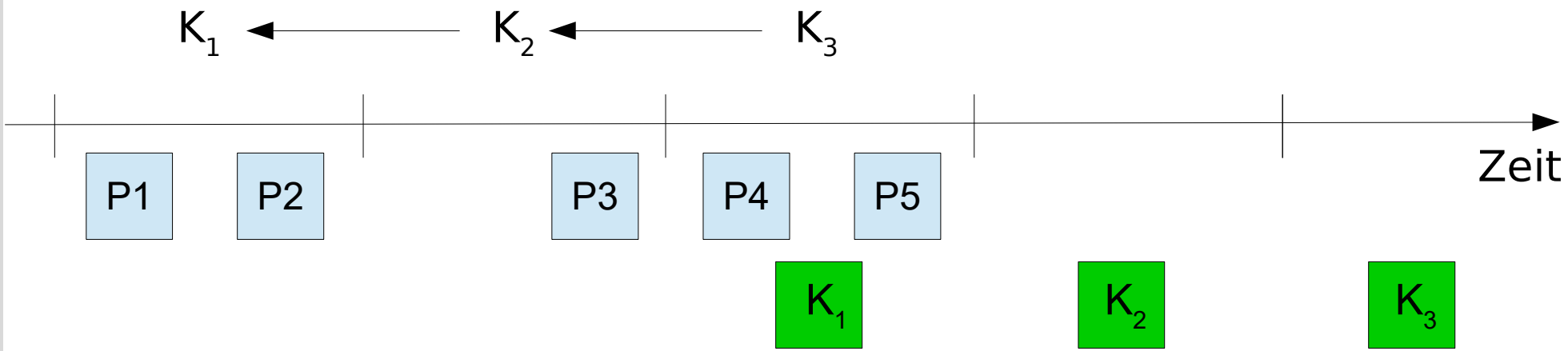
  $K_i = G(K_{i+1})$ $0 <= i < n$

  $K_0 \xleftarrow{G} K_1 \xleftarrow{G} K_2 \xleftarrow{G} K_3$

  G kryptographische one-way Hashfunktion

- Zwei Phasen eines Sendevorgangs:
  - Abschicken von signierten Paketen
  - Offenlegung der Signaturschlüssel (mit Verspätung)

µTESLA (2)



- Auch zwei Schritte für Paketauthentifizierung

  (1) Zeitpunkt des Ankommens

  Vor Bekanntgabe des Signaturschlüssels: Aufbewahrung

  Nach / während Bekanntgabe des Signaturschlüssels: Verwerfung

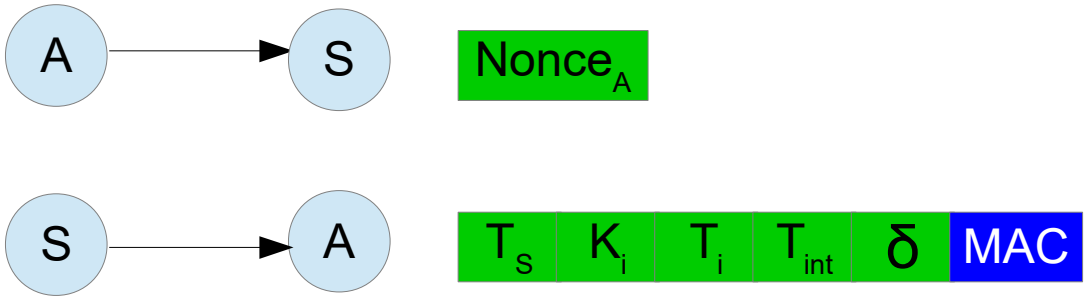
  (2) Schlüsselverifikation

  Gilt $K_v = G^{i-v}(K_i)$? Falls ja Authentizität nachgewiesen!

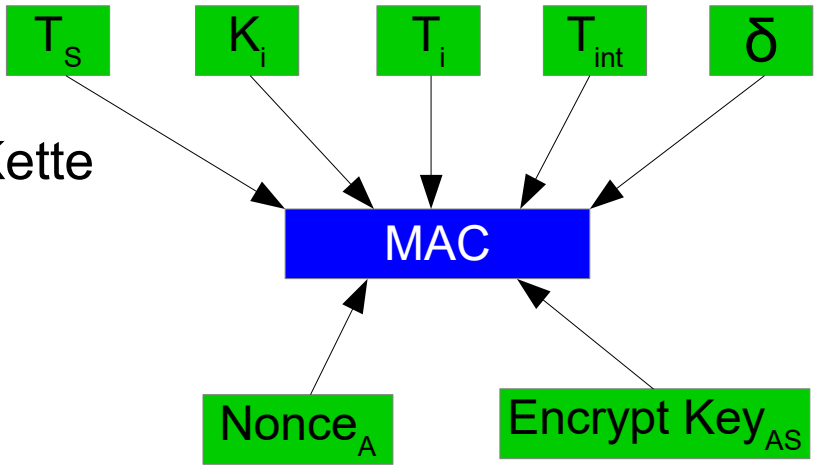
  K_i zu verifizierende Schlüssel K_v letzter verifizierter Schlüssel

µTESLA (3)

- Hinzufügen eines neuen Empfängers (Knoten A)



- T_s aktuelle Zeit
- K_i letzter offengelegter Schlüssel aus der Kette
- T_i Startzeitpunkt des letzten Zeitintervals i
- T_{int} Länge eines Zeitintervals
- δ Verspätung für Schlüsselbekanntgabe



SPINS: Fazit

- Sicherstellung von
  - Vertraulichkeit
  - Authentizität
  - Datenfrische
- Authentifiziertes Broadcast

  ==> Grundlage für sicheres Routing
- Zeitsynchronisation
- Schlüsselverwaltung
- Verwendung von Zählerwerten als potenzielle Schwachstelle
  - Kommunikationsoverhead und Energiekosten für den Austausch
  - Speicherplatz für die Aufbewahrung

MSP430: AES256 Accelerator

- kryptographisches Peripherie-Modul
  - symmetrische Ver-/Entschlüsselung
  - Implementierung von Advanced Encryption Standard (AES)
- Eingabe auf 128-Bits-Worte begrenzt
- variable Schlüssellänge: 128, 192 oder 256 Bits
- vier Chiffrierungsmodi
  - Electronic Code Block (ECB)
  - Cipher Block Chaining (CBC)
  - Output Feedback (OFB)
  - Cipher Feedback (CFB)
- Mögliche Implementierungsgrundlage für SNEP

Zusammenfassung

- Sensornetzwerke
  - sehr geringe Speicherplatz und Rechenleistung
  - unsichere Umgebung
  - störanfällige Kommunikation
  - kaum Energie und Bandbreite
  - hoch dynamische Topologie

  ==> “klassische” Sicherheitsverfahren nicht (ohne Weiteres) anwendbar

- Geeignete Protokolle notwendig
  - SNEP, µTESLA, ...

FRAGEN?