Implementation of an IEEE 802.15.4 Compliant Self-organizing Energy-efficient Wireless Sensor Network for Use in Anti-Theft System

Volker Delport, Christian Georgi, Vinzenz Lorenz,
Jan Kuhnert, Silvio Rößler

Professur Kommunikationstechnik/Funktechnik
Fakultät Angewandte Computer- und Biowissenschaften

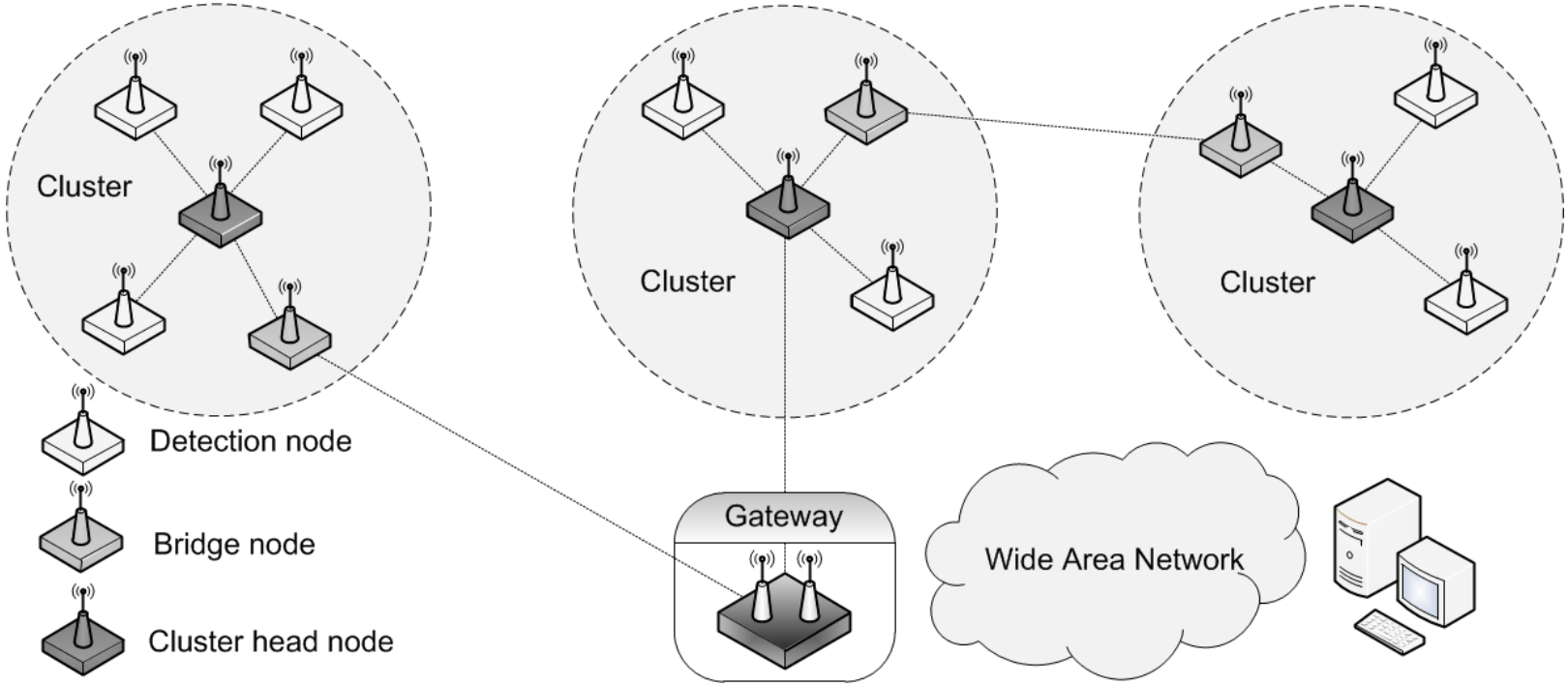
Hochschule Mittweida

Das Projekt wurde vom Bundesministerium für Wirtschaft und Energie (BMWi) gefördert.

Anforderungen

Eigenschaft	Parameter	Anforderung
schnelle Plug-&-Play-Installation	Installationszeit:	wenige Stunden
räumliche Skalierbarkeit	Ausdehnung innerhalb von Gebäuden:	mehrere Etagen
	Ausdehnung außerhalb von Gebäuden:	min. 500 x 500 m
hohe Verfügbarkeit, u. a. durch redundante Sensorknoten	maximale Anzahl der Sensorknoten:	200
ausreichender Datendurchsatz (Selbstorganisation, Alarmierung, IT-Sicherheit)	durchschnittlicher Datendurchsatz:	500 bit/s
schnelle Weiterleitung des Alarmsignals eines Meldesensors	Latenzzeit des Alarmsignals:	max. 120 s
IT-Sicherheit	optionale Verschlüsselung und Authentifizierung der Frame-Daten	
langer energieautarker Betrieb	wartungsfreie Betriebszeit:	min. 3 Monate

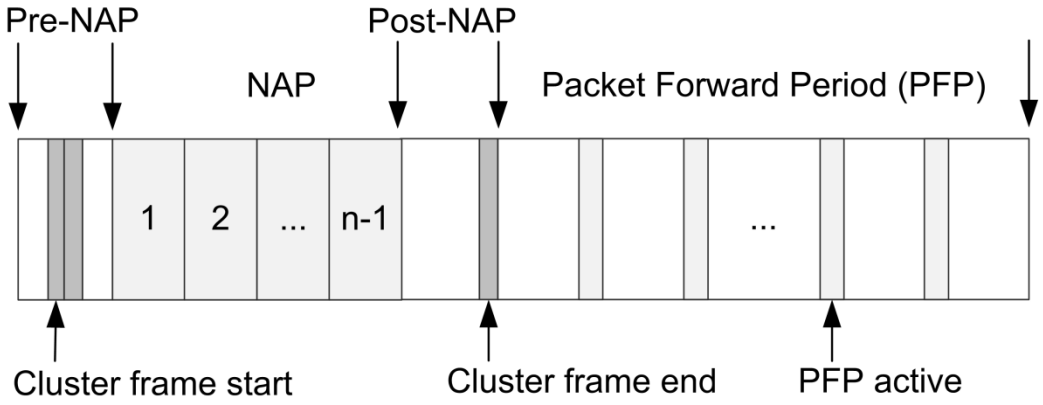
Sensornetztopologie



- Jedes Cluster ist ein eigenes IEEE 802.15.4 kompatibles WPAN.
- Cluster Head: ist der PAN-Koordinator des Clusters.
- Meldeknoten: sendet Sensorwerte und ggf. ein Alarm-Frame an den Cluster Head.
- Bridge-Knoten: leitet Sensordaten und Alarm-Frames an benachbarte Cluster weiter.
- Jeder Knoten kann die Rolle als Cluster Head, Melde- oder Bridge-Knoten erfüllen.

Clusterkommunikation

- Alle Knoten und Cluster arbeiten auf derselben Frequenz.
- Pre-NAP:
  - Cluster Head erwacht, geht in den Empfangsmodus und erfasst eigene Sensorwerte.
  - Cluster-Frame-Start-Kommando vermeidet Clusterkollisionen.
- NAP (ohne CSMA-CA):
  - Melde-/Bridge-Knoten senden Sensorwerte in zugeordneten Zeitschlitzen.
  - Cluster Head gibt in seiner Bestätigung die Schlafzeit des Knotens vor.
- Post-NAP:
  - Cluster Head prüft die gesammelten Sensorwerte und beendet NAP.

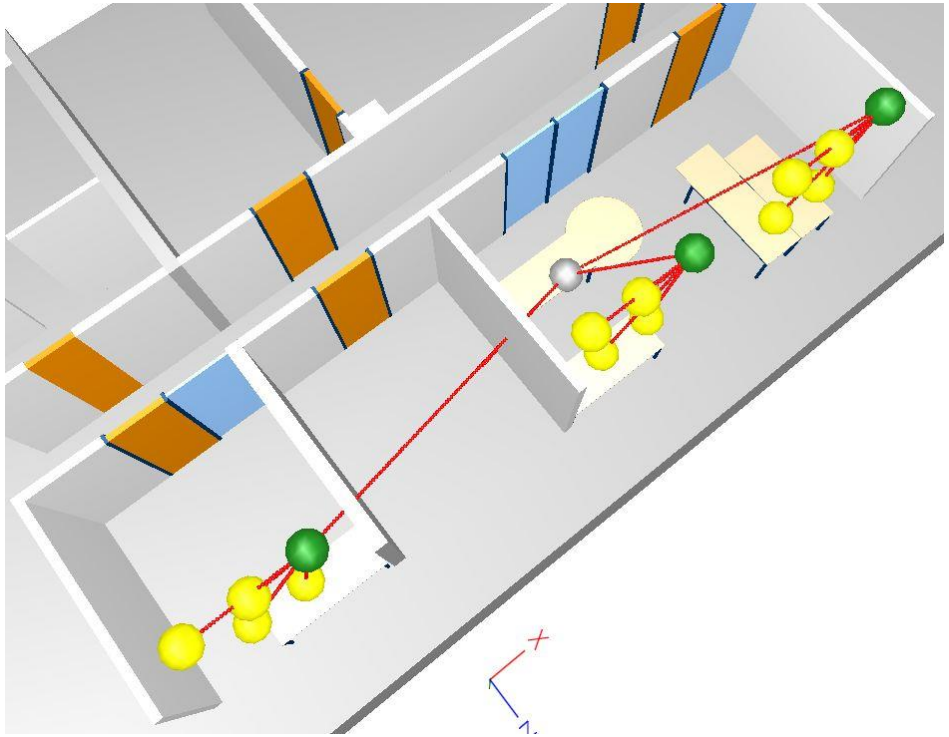


NAP: Node Access Period

- PFP (mit CSMA-CA):
  - Alle Knoten gehen in einen Duty Cycle und prüfen ihre Sensorwerte.
  - Meldeknoten senden ggf. Alarm-Frames. Cluster Head und Bridge-Knoten sind gleichzeitig empfangsbereit.
  - Alarm- und Status-Frames werden von Cluster Head und Bridge-Knoten an benachbarte Cluster per Multi-Hop weitergeleitet.

Selbstorganisation: Plug & Play

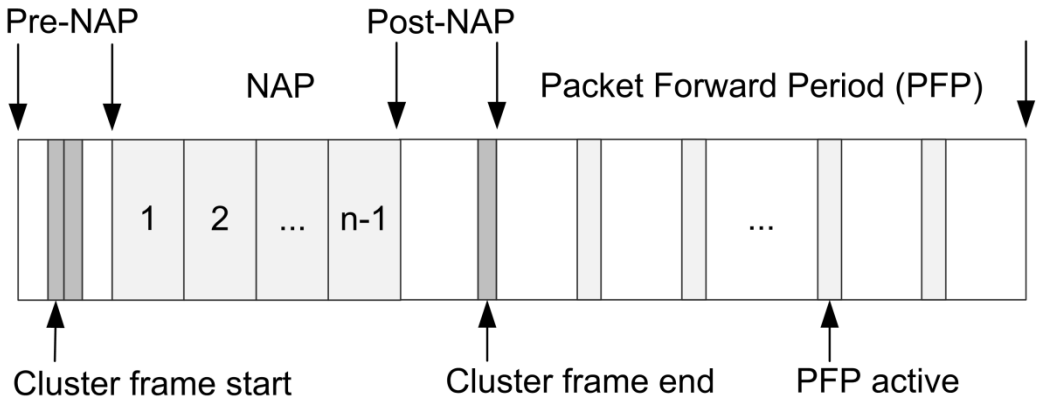
- Die Funksensorknoten bilden nach dem Einschalten der Versorgungsspannung selbstständig Cluster.
- Der erste eingeschaltete Knoten kürt sich automatisch zum Cluster Head.
- Während des Anmeldeprozesses (Packet Forward Period) entscheidet der Cluster Head über die Rolle des neuen Knotens im Cluster.
- Die Clustergröße ist begrenzt, um die Cluster Heads energetisch zu entlasten.
- Gescheiterte Anmeldeversuche werden erst nach wenigen Sekunden wiederholt.
- Nach mehreren gescheiterten Anmelde-versuchen wird der betreffende Knoten ein neuer Cluster Head.

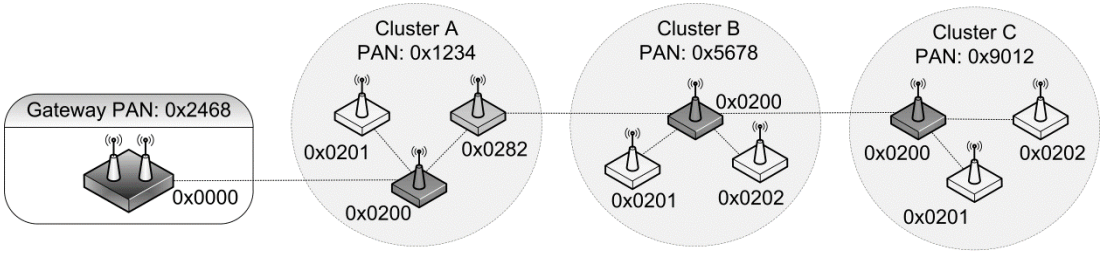


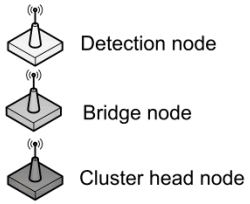
- Wiederholte Anmeldeversuche in ein fremdes Netzwerk werden durch eine „schwarze Knotenliste“ verhindert.

Selbstorganisation: Adressierung und Routing

- Knotenadresse: besteht aus einer 2-Byte-PAN-ID und einer 2-Byte-Kurzadresse.
- Kurzadresse: kennzeichnet den Frequenzkanal, den Sensortyp und den Knotentyp.
- Knotentabellen: Adressen der Clustermitglieder, der direkt erreichbaren Bridge-Knoten oder Cluster Heads, der Nachbarcluster sowie die PAN-IDs erreichbarer Cluster.
- Routing-Tabellen:
  - werden nach der Inbetriebnahme erzeugt und laufend aktualisiert.
  - Die Zeilen enthalten jeweils die Kurzadresse und die PAN-ID des Next-Hop-Knotens sowie die Ziel-PAN-ID.







Cluster head node in cluster A:

Short adress	PAN ID	Target PAN ID
0x0000	0x2468	0x2468
0x0282	0x1234	0x5678
0x0282	0x1234	0x9012

Bridge node in cluster A:

Short adress	PAN ID	Target PAN ID
0x0200	0x1234	0x2468
0x0200	0x5678	0x5678
0x0200	0x5678	0x9012

Cluster head node in cluster B:

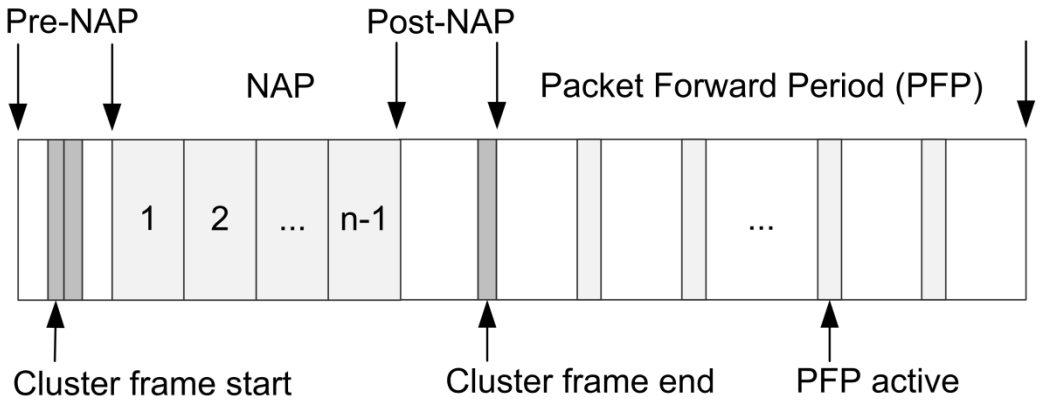
Short adress	PAN ID	Target PAN ID
0x0200	0x9012	0x9012
0x0282	0x1234	0x2468
0x0282	0x1234	0x1234

Cluster head node in cluster C:

Short adress	PAN ID	Target PAN ID
0x0200	0x5678	0x2468
0x0200	0x5678	0x5678
0x0200	0x5678	0x1234

Selbstorganisation: dynamischer Rollenwechsel

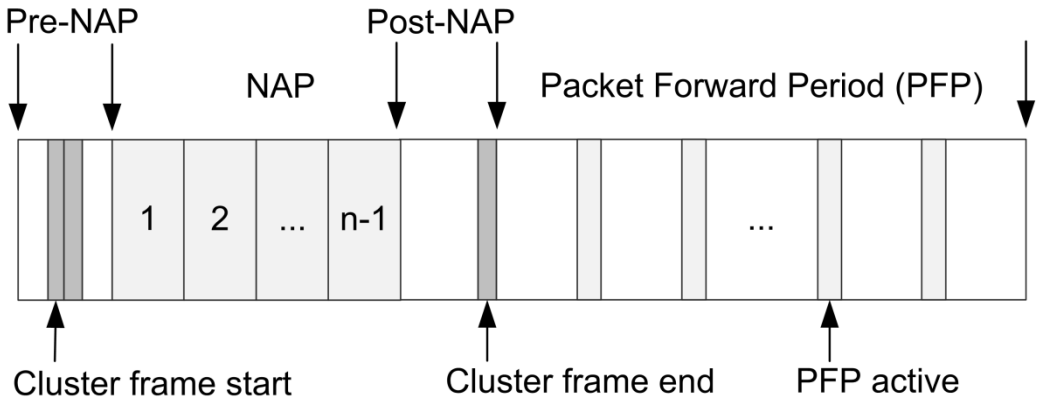
- Die gewählten Duty Cycles beeinflussen die Energieeffizienz des Sensornetzes.
- Cluster Heads und Bridge-Knoten sind länger aktiv und verbrauchen deshalb mehr Energie.
- Durch einen dynamischen Rollentausch während des laufenden Netzwerk-betriebs wird der Energieverbrauch des Sensornetzes auf alle Knoten verteilt.
- Sinkt die Batteriespannung eines Cluster Head mit einem definierten Schwellwert unter die mittlere Batteriespannung aller Clustermitglieder, gibt der Cluster Head seine Rolle an den Meldeknoten mit der größten Batteriespannung ab.
- Mit dem Bridge-Knoten wird ähnlich verfahren.



- Test mit einem Cluster aus sechs Knoten in einem klimatisierten Serverraum:
  - Duty Cycle des Cluster Head: 0,7 %
  - Duty Cycle der Meldeknoten: 0,2 %
  - Durch den dynamischen Cluster-Head-Wechsel kann die Zeitdauer bis zum ersten energiebedingten Knotenausfall mindestens verdoppelt werden.

Selbstorganisation: Übertragungssicherheit

- Verbindung zwischen Knoten und Cluster Head unterbrochen:
  - Knoten broadcastet Daten in einem „Sicherheitszeitschlitz“ am NAP-Ende.
  - Resynchronisation in der PFP
    - Anzahl der Resynchronisations-versuche ist zufällig.
  - automatischer Neustart des Knotens nach mehreren gescheiterten Resynchronisationsversuchen
- Ausfall eines Cluster Heads:
  - automatischer Neustart aller Cluster-mitglieder
- Superframes der Cluster driften:
  - Cluster Heads kündigen NAP-Ende an und verlängern ggf. die Knoten-Schlafzeiten.

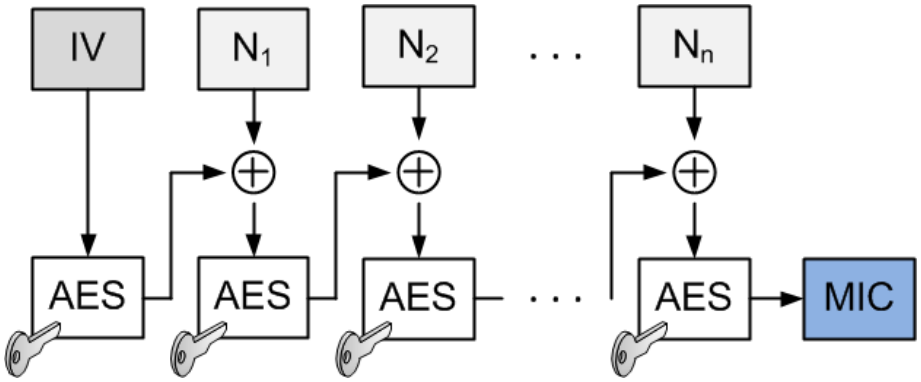


- Cluster kollidieren (NAP vs. PFP):
  - Cluster Heads kündigen NAP-Anfang an.
  - Bridge-Knoten und Cluster Heads anderer Cluster pausieren das Senden in der PFP.
- Route zu Gateway im Alarmfall unterbrochen:
  - Bridge-Knoten und Cluster Heads broadcasten Alarm Event Frame in der PFP über mehrere Superframe-Perioden.

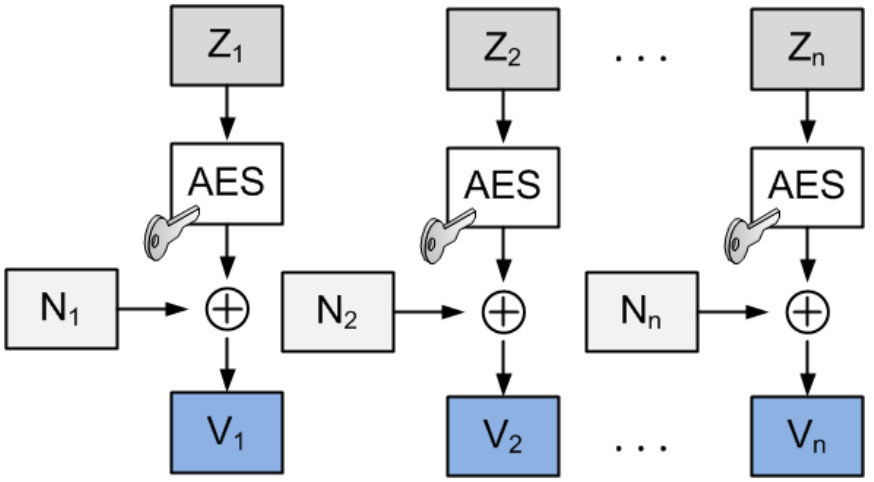
IT-Sicherheit

- symmetrische Blockverschlüsselung mit CCM* (Counter with Cipher Block Chaining Message Authentication)
- Schlüssellänge: 128 Bit
- Die Schlüssel sind in einem gegenüber Auslesen geschützten Speicherbereich des Knotens abgelegt.
- Ein Schlüsselaustausch erfolgt über die Schlüsselindizes und wird durch das Gateway ausgelöst.
- CC2530 (Sensorknoten): trotz AES-Coprozessor zusätzliche Software-implementierung notwendig.
- CC2520 (Gateway-Transceiver-Modul): vollständig durch die Hardware unterstützt.
- CCM* verlängert die Aktivzeiten der Knoten um 10 ms.

CBC-MAC:



CTR:

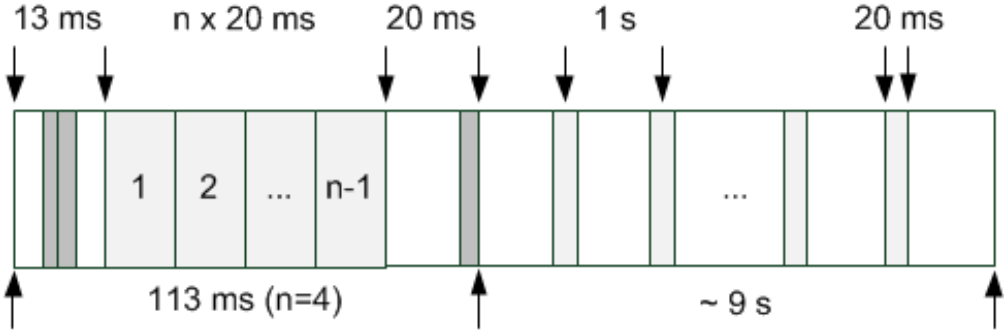


Labortest im Gebäude

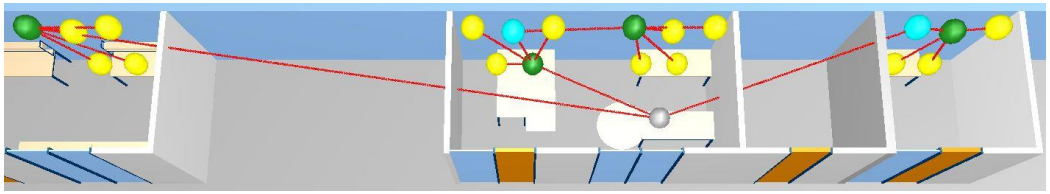
- Ausdehnung: ca. 100 m²
- Frequenz: 2.455 MHz
- 2 Ni-MH-Akkus pro Knoten (1.900 mAh)
- Superframe-Periode: 10 s
- CCM*-Verschlüsselung
- Start: 20 Sensorknoten in vier Clustern
- Inbetriebnahme in ca. 30 Minuten
- Laufzeit 120 Tage
- 25.900.894 erfasste Sensordatenpakete
- 28 Cluster Head- und 18 Bridge-Knoten-Wechsel
- 14 energiebedingte Knotenabmeldungen
- Die eingesetzten TI-Batterie-Boards mit Pull-Down-Widerstand erhöhen den Ruhestromverbrauch um ca. Faktor 100.
- Alle (ca. 120) ausgelöste Alarme kamen beim Gateway an.

CC2530 (30 mA / 1µA)

DK-LM3S9B96 + CC2520



Tag 9



Eigenschaften

Eigenschaft	Parameter	Anforderung
schnelle Plug-&-Play-Installation	Installationszeit:	ca. 1 Minute / Knoten
räumliche Skalierbarkeit durch Cluster und Multi-Hop-Kommunikation	Ausdehnung innerhalb von Gebäuden:	mehrere Etagen
	Ausdehnung außerhalb von Gebäuden:	> 500 x 500 m
hohe Verfügbarkeit durch redundante Sensorknoten	Anzahl der Sensorknoten:	> 200
ausreichender Datendurchsatz (Selbstorganisation, Alarmierung, IT-Sicherheit)	durchschnittlicher Datendurchsatz:	ca. 30 kbit/s
schnelle Weiterleitung des Alarmsignals eines Meldesensors	Latenzzeit des Alarmsignals:	max. 1 s / Hop
IT-Sicherheit	optionale Verschlüsselung und Authentifizierung durch das CCM*-Verfahren	
langer energieautarker Betrieb	wartungsfreie Betriebszeit:	min. 4 Monate [1]

1: mit CCM*-Authentifizierung und -Verschlüsselung

Vielen Dank für Ihre Aufmerksamkeit

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

Kontakt:

Prof. Dr.-Ing. Volker Delport

Professur Kommunikationstechnik/Funktechnik

Fakultät Angewandte Computer- und Biowissenschaften

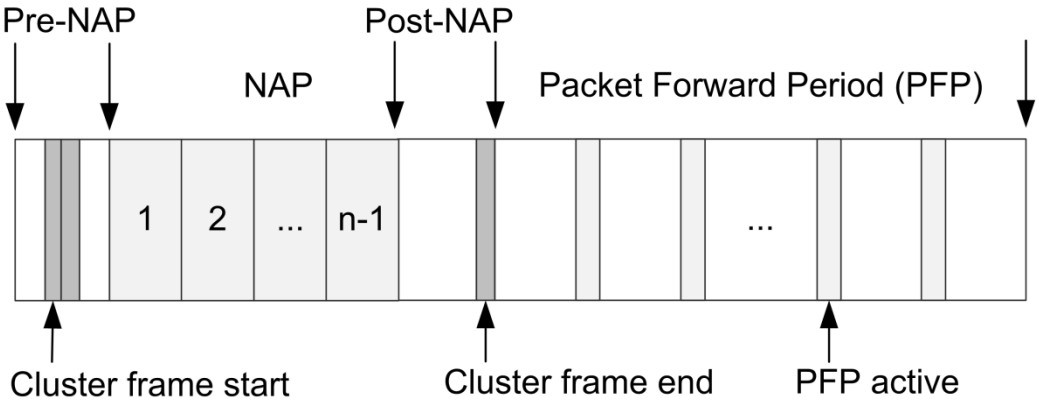
Hochschule Mittweida

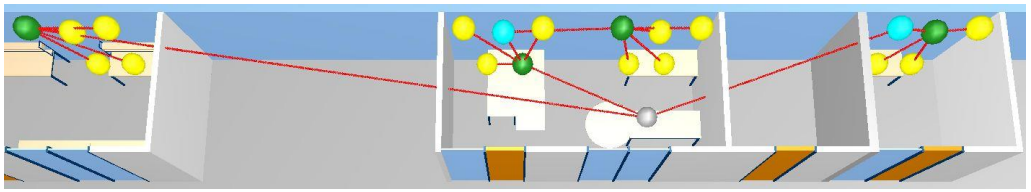
Tel.: +49 3727 58-1078

mailto: delport@hs-mittweida.de

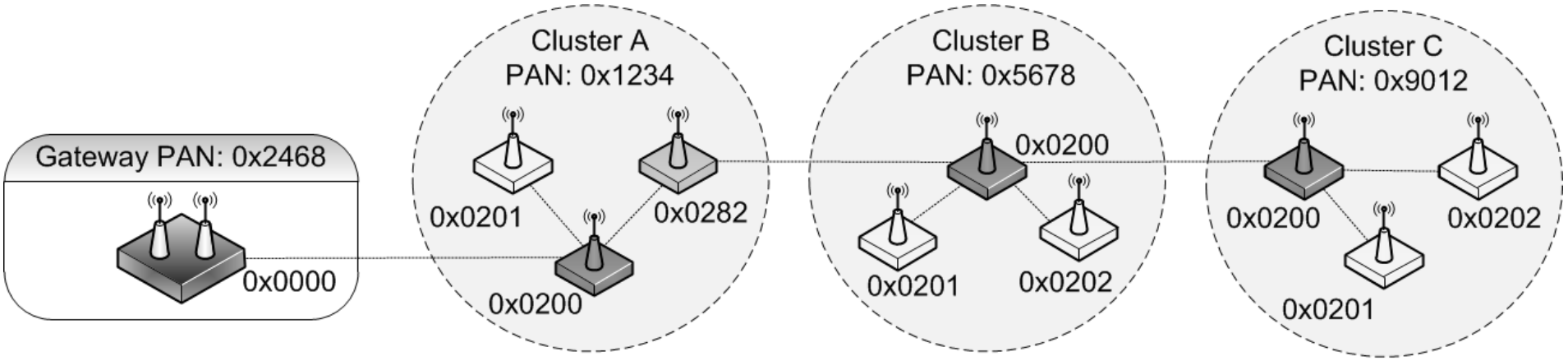
WWW1: www.hs-mittweida.de/delport/

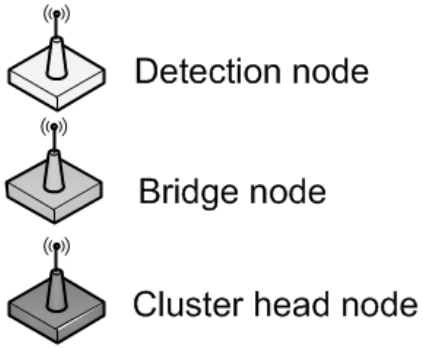
WWW2: http://blockchain.hs-mittweida.de





Routing-Tabellen (Beispiel)





Cluster head node in cluster A:

Short adress	PAN ID	Target PAN ID
0x0000	0x2468	0x2468
0x0282	0x1234	0x5678
0x0282	0x1234	0x9012

Bridge node in cluster A:

Short adress	PAN ID	Target PAN ID
0x0200	0x1234	0x2468
0x0200	0x5678	0x5678
0x0200	0x5678	0x9012

Cluster head node in cluster B:

Short adress	PAN ID	Target PAN ID
0x0200	0x9012	0x9012
0x0282	0x1234	0x2468
0x0282	0x1234	0x1234

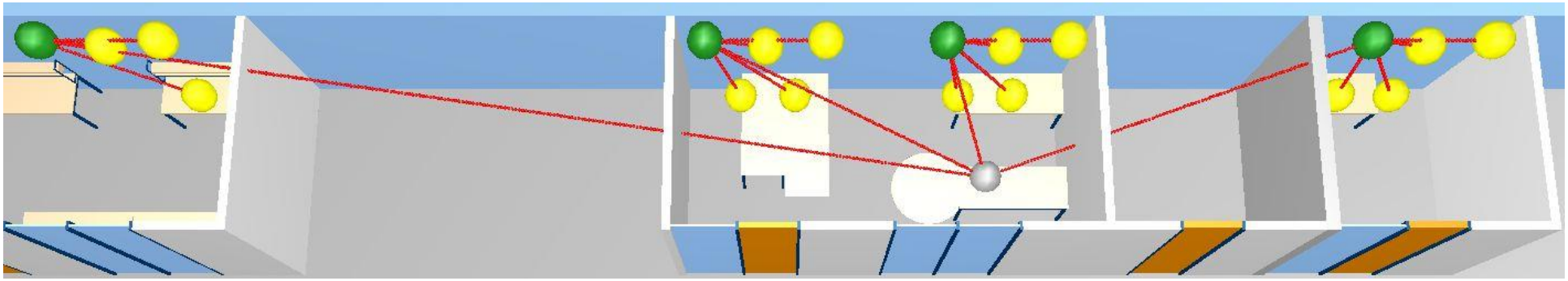
Cluster head node in cluster C:

Short adress	PAN ID	Target PAN ID
0x0200	0x5678	0x2468
0x0200	0x5678	0x5678
0x0200	0x5678	0x1234

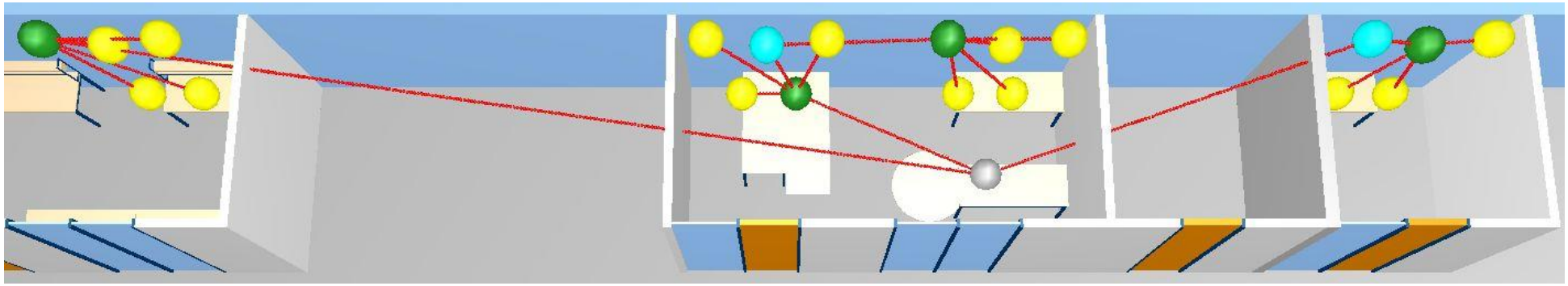
Selbstorganisation

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

Tag 1 (nach der Inbetriebnahme):



Tag 9:



Gateway Cluster Head Bridge-Knoten Meldeknoten

Wartungsfreie Betriebszeiten Cluster Head (Schätzung*)

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

Parameter	Konfiguration	Eigenschaft	nicht verschlüsselt	verschlüsselt
Meldeknoten n	4	$t_{PFP-Aktiv}$	10 ms	20 ms
Ladung pro Sensorknoten	1900 mAh	$t_{CF-Start}$	3 ms	3 ms
		$t_{Pre-NAP}$	10 ms	10 ms
		t_{NAP}, $t_{Post-NAP}$	10 ms	20 ms
Aktivstrom	30 mA (CC2530)	Aktivzeit t_{aktiv}	153 ms	293 ms
Ruhestrom	1 µA (CC2530)	relative Aktivzeit $\frac{t_{aktiv}}{t_{zyklus}}$	1,53 %	2,93 %
Zykluszeit	10 s	relative Ruhezeit $\frac{t_{ruhe}}{t_{zyklus}}$	98,47 %	97,07 %
Δt_{PFP}	1 s			
Anzahl der PFP-Wakeup-Intervalle n_{PFP}	9	wartungsfreie Betriebszeit $t_{Betrieb}$	4272 h 5 m 28 d	2233 h 3 m 3 d

*ohne dynamischen Rollenwechsel

Wartungsfreie Betriebszeiten Knotentypen (Schätzung*)

Knotenfunktionen	wartungsfreie Betriebszeit	
IT-Sicherheit (CCM*)	nein	ja
Cluster Head	5 Monate + 28 Tage	3 Monate + 3 Tage
Bridge-Knoten	7 Monate + 17 Tage	3 Monate + 28 Tage
Meldeknoten	20 Monate + 17 Tage	11 Monate + 29 Tage

*ohne dynamischen Rollenwechsel