Technische Universität Braunschweig

Institut für Betriebssysteme und Rechnerverbund

Sicherheit in DTN-basierten ÖPNV-Netzen

Johannes Morgenroth, Lars Wolf

Essener Workshop zur Netzsicherheit 2011

Gliederung

Motivation

Bildmaterial: Open Transport Tycoon

Motivation

Idee

- Busse bewegen sich im gesamten Stadtgebiet
- Flächendeckende Aufnahme von Messwerten
- Zeitnahe Übertragung der Daten?
- Mobilfunk verursacht hohe laufende Kosten

OptraCom

- Aufbau eines unterbrechungstoleranten Kommunikationssystems
- Nutzung von WLAN (kostengünstig, lizenzfrei)
- ÖPNV-Fahrzeuge als mobile Sensoren und Datentransporter

Motivation

Bildmaterial: Open Transport Tycoon

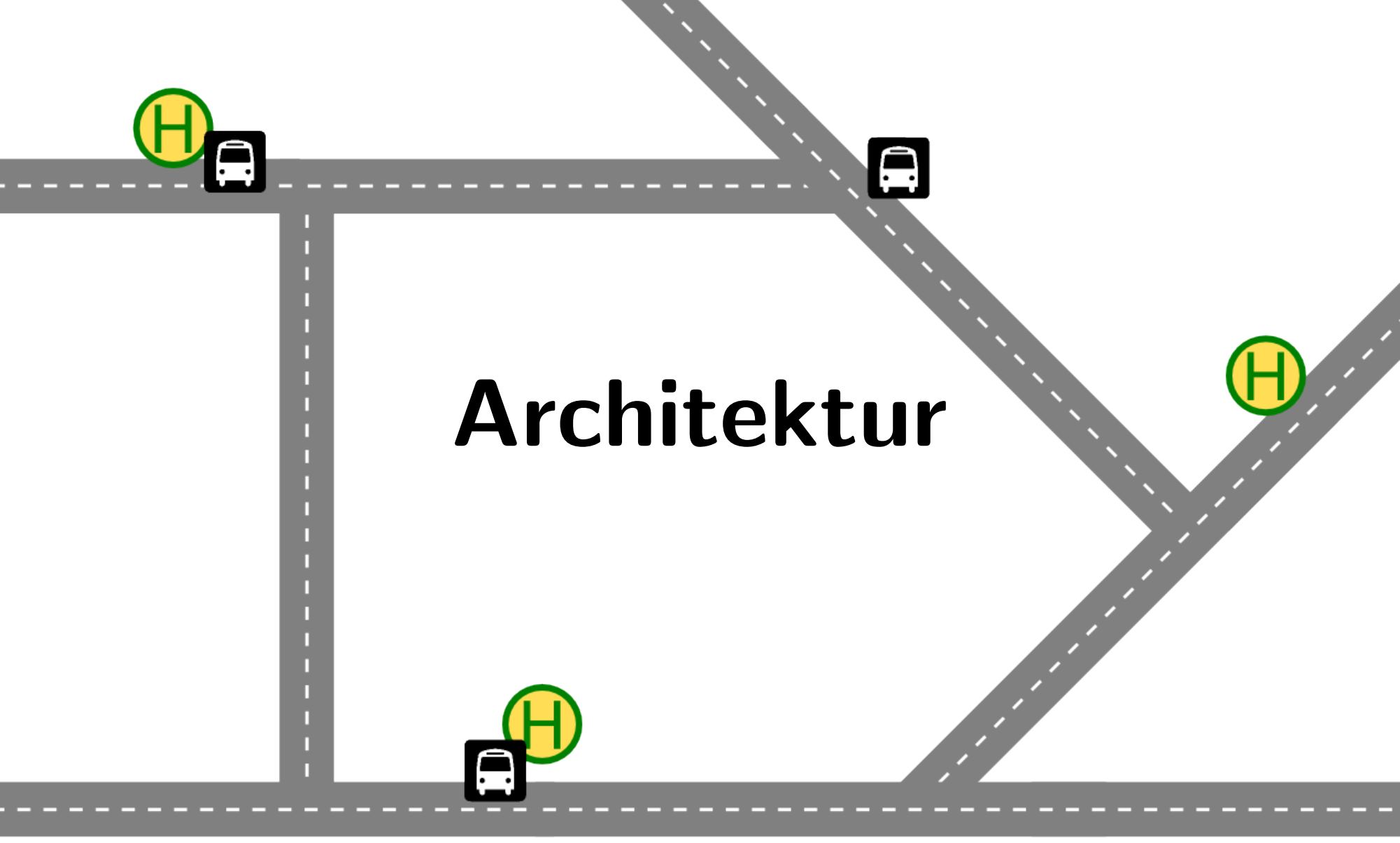
Anwendungen

Aufnahme von Messwerten

- Umwelt: Temperatur, Luftgüte, ...
- Statistiken: Anzahl der Passagiere, Fahrgeschwindigkeit, Fehlfunktionen

Fahrgastinformationssystem

- Versorgung mit aktuellen Fahrplänen
- Transport von Multimediainhalten
- Rückführung von Nutzungsstatistiken
- Systemaktualisierungen

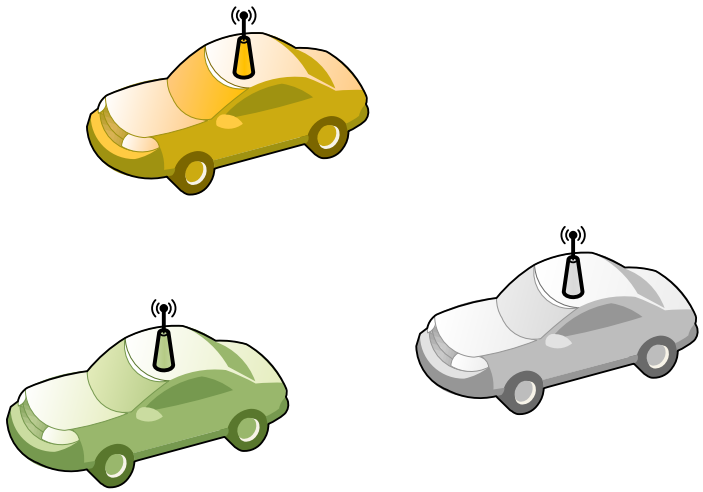

Architektur

Komponenten

- Mobile Knoten auf Fahrzeugen
- Stationäre Knoten
  - Steigerung der Kapazität
  - Verringerung von Latenzen
- Netzanbindung bei stationären Knoten (optional)

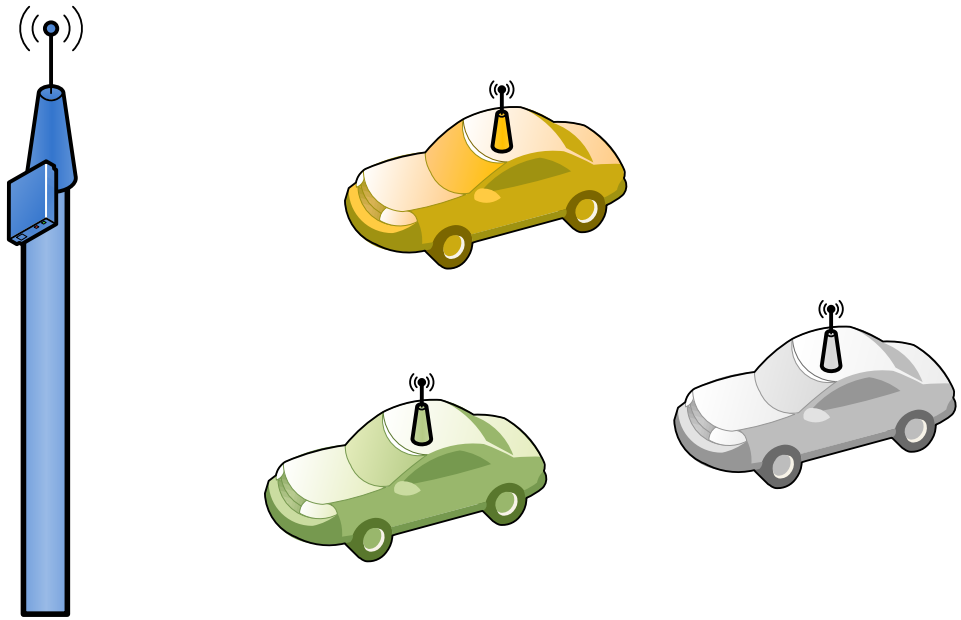
Komponenten

- Mobile Knoten auf Fahrzeugen
- Stationäre Knoten
  - Steigerung der Kapazität
  - Verringerung von Latenzen
- Netzanbindung bei stationären Knoten (optional)



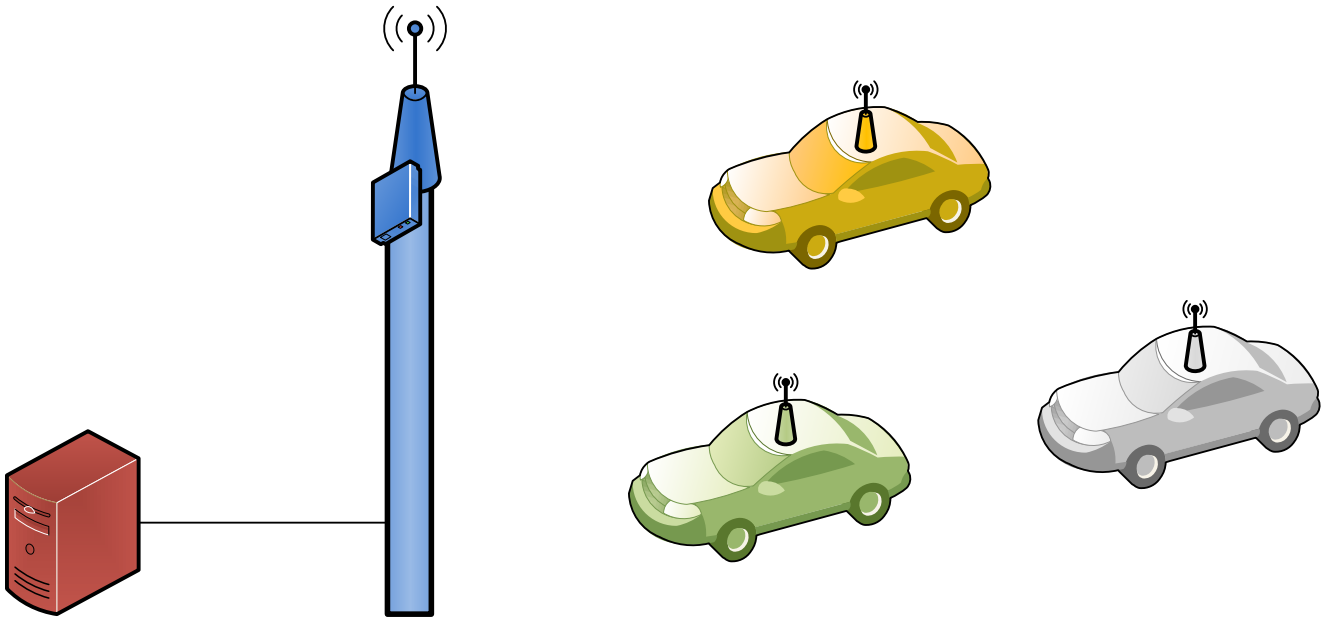
Komponenten

- Mobile Knoten auf Fahrzeugen
- Stationäre Knoten
  - Steigerung der Kapazität
  - Verringerung von Latenzen
- Netzanbindung bei stationären Knoten (optional)



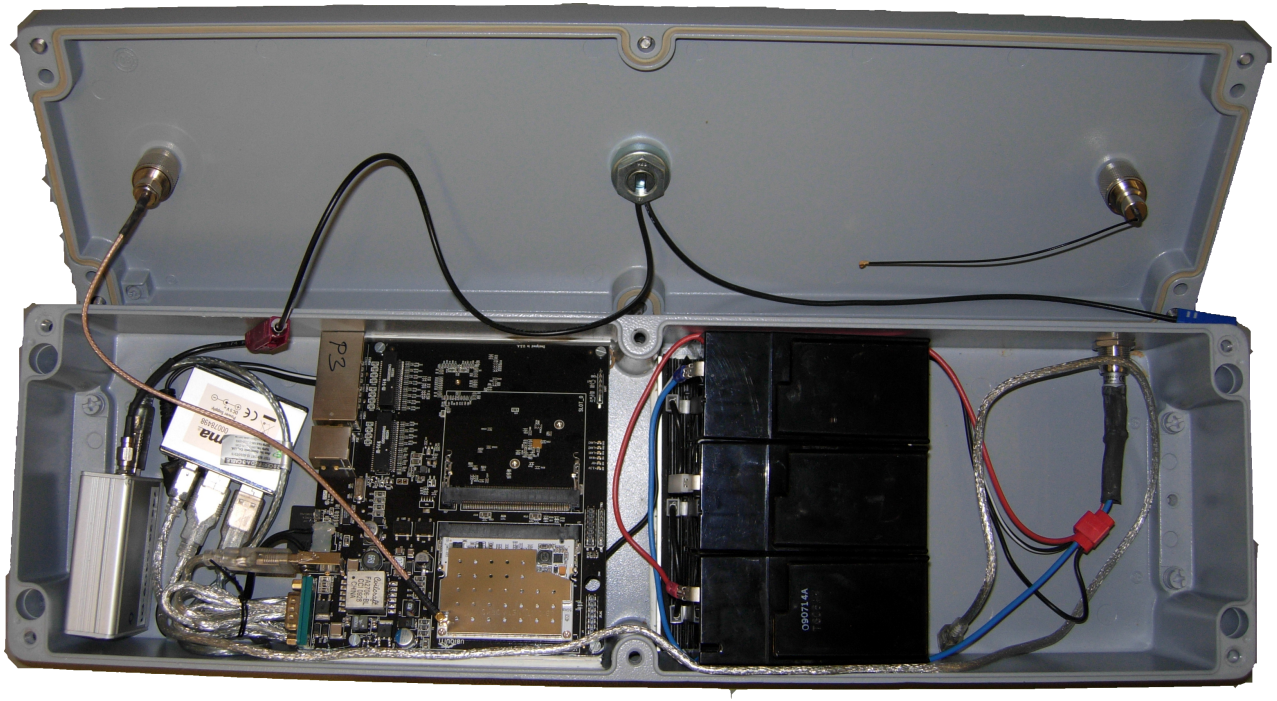
Komponenten

- Mobile Knoten auf Fahrzeugen
- Stationäre Knoten
  - Steigerung der Kapazität
  - Verringerung von Latenzen
- Netzanbindung bei stationären Knoten (optional)



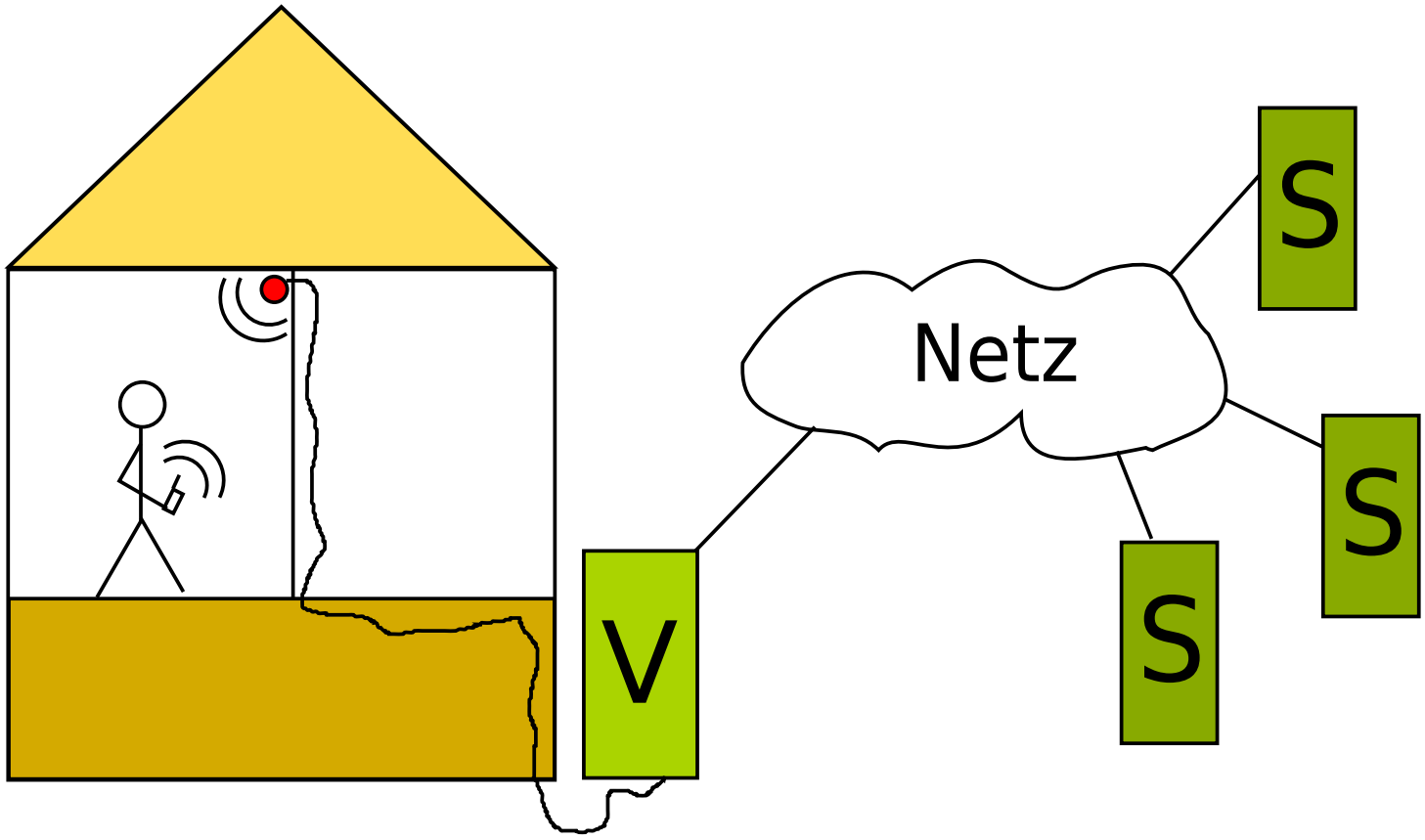
Hardware

- Ubiquiti Routerstation Pro
  - Atheros AR7161 (MIPS) 680MHz, 128MB RAM, USB 2.0
- Massenspeicher (USB), WLAN (IEEE 802.11a/b/g)
- GPS, Bleiakku



Hardware

Moderne Kommunikationsnetze



durchgängige Ende-zu-Ende Verbindung

Mobile Ad-Hoc Netze

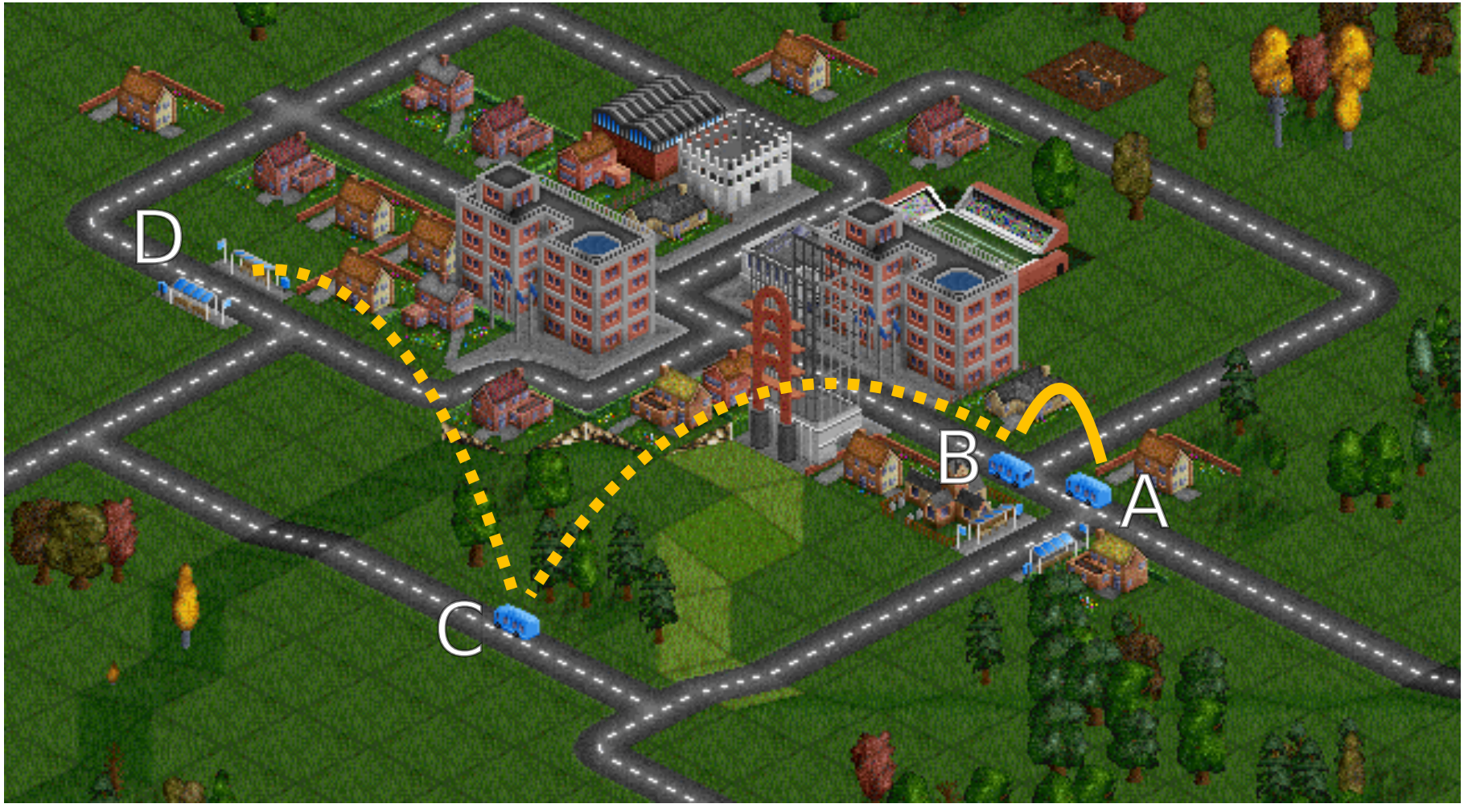
Herausforderung

- Knoten permanent in Bewegung → wechselnde Nachbarn
- Kommunikation zwischen Knoten über Ad-Hoc WLAN
- Durchgehende Ende-zu-Ende Verbindung nicht verfügbar

Delay Tolerant Networking (DTN)

- Store-Carry-Forward
- Übertragung der Daten in Bündeln
- Architekturbeschreibung (RFC 4838)
- Bundle Protocol Spezifikation (RFC 5050)

Store-Carry-Forward Prinzip



Bildmaterial: Open Transport Tycoon

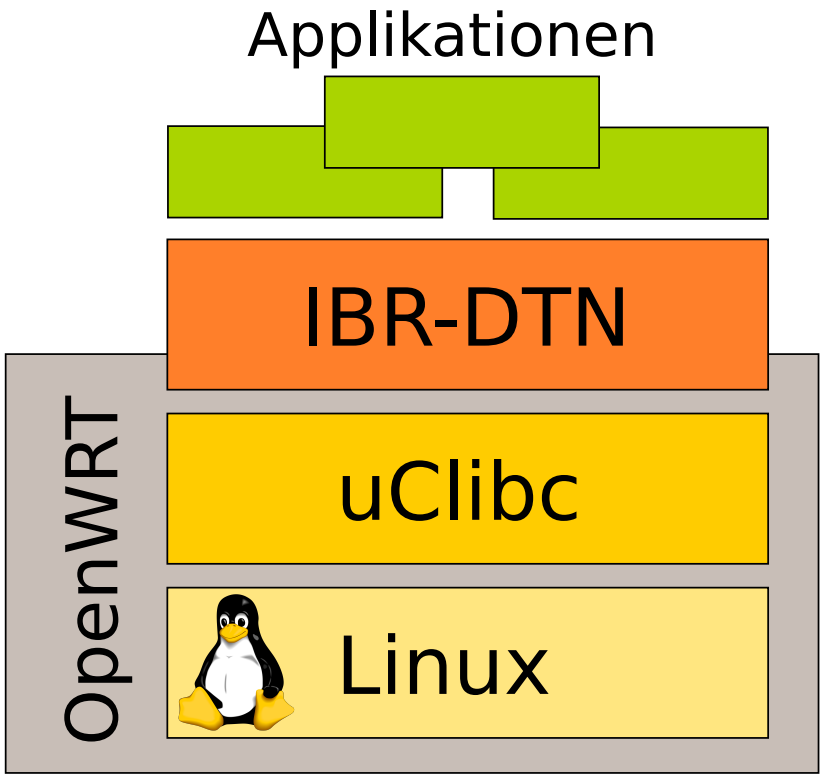
Software

OpenWRT

- Baukasten für Router-Firmware
- Plattform für Embedded Hardware
- Linux Kernel + uClibc

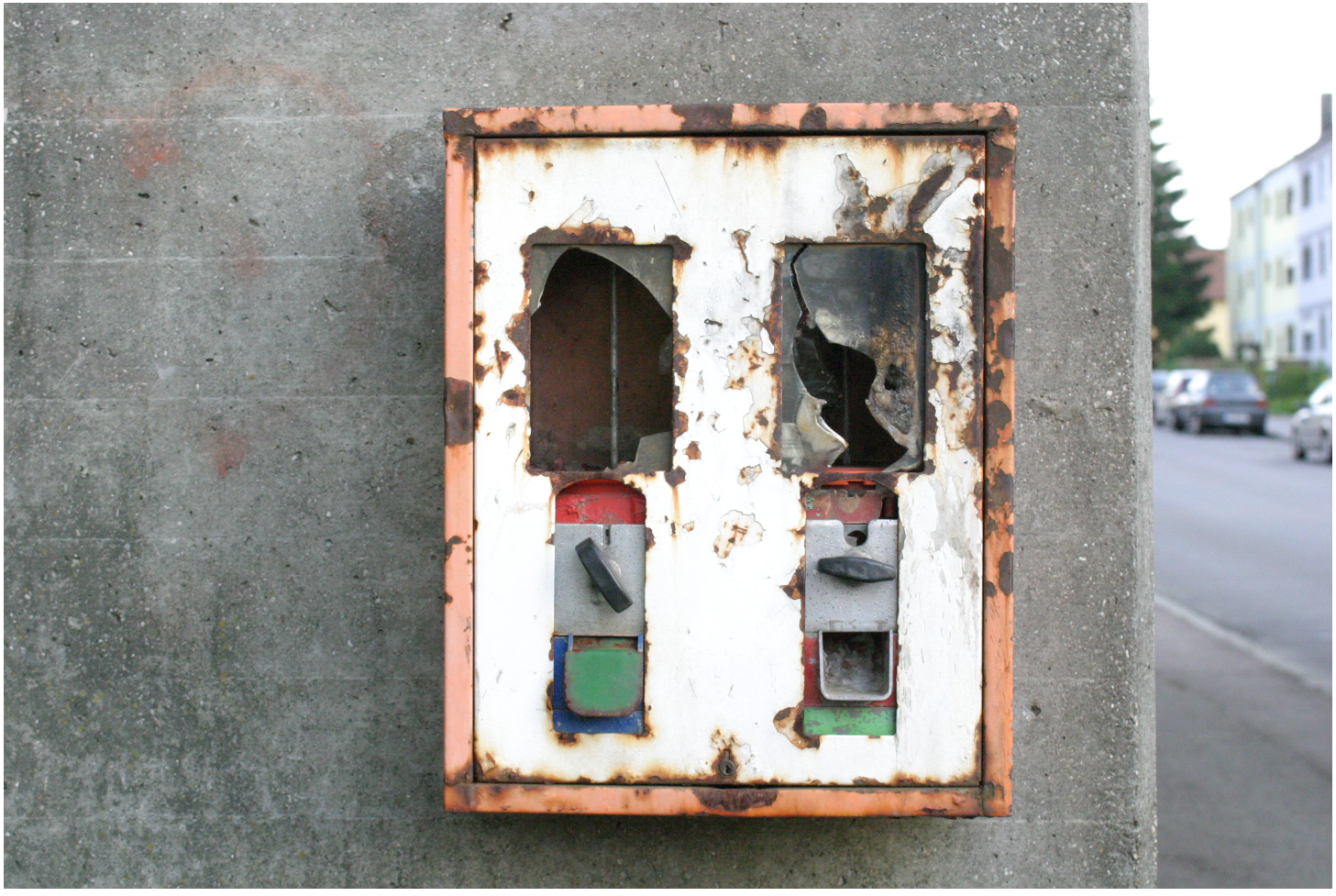
IBR-DTN

- Bundle Protocol Stack
- Wegewahl, Speicherung, Weiterleitung, API, ...
- Stark modularisiert
- Optimiert für eingebettete Systeme



Sicherheit

Gefahren - Vandalismus



Quelle: http://www.versicherung-recht.de

Gefahren - Jamming

Quelle: http://connect.in.com

Gefahren - (D)DoS-Attacken

Quelle: The Specs Effect, youtube.com

Gefahren

- Vandalismus
- Jamming
- (D)DoS-Attacken
- Bugs in der eingesetzten Software

Gefahren

- Vandalismus (nicht zu verhindern)
- Jamming (nicht zu verhindern)
- (D)DoS-Attacken
- Bugs in der eingesetzten Software

Gefahren

- Vandalismus (nicht zu verhindern)
- Jamming (nicht zu verhindern)
- (D)DoS-Attacken
- Bugs in der eingesetzten Software

Gegenmaßnahmen

- Penetrationstests und Werkzeuge zur Risikoklassifizierung
- Prozesse zur Einrichtung und Sicherung von neuen Knoten

Systemanalyse

- Betrachtung des Systems als „White Box“
- Welche Software existiert auf dem System?
- Einsatz von Port- und Schwachstellenscanner
  - nmap, OpenVAS, Metasploit

Potenzielle Schwachstellen

- **Linux Kernel** (2x)
  - Fehler in IPC kann zum Kernel Oops führen
  - Fehler in Keyring Verwaltung kann zur Kernel Panic führen
- **OpenSSL** (1x)
  - Mangelnde NULL Pointer Prüfung bei Verwendung von `bn_wexpand`
  - Pufferüberlauf möglich: Absturz oder Übernahme denkbar
  - Relevanz für unser System ist unklar

Systemanalyse: IBR-DTN

Code Review

- Statische Quellcodeanalyse (Flawfinder)
- Keine Risiken festzustellen

DoS Angriff

- Neighbor Discovery
- Beacons benötigen keine Authentifizierung
- Ankündigung von vielen Knoten
  $\rightarrow$ hohe CPU Last, Kommunikation nicht mehr möglich

Schutz vor Angreifern

Angriffsszenarien

- Einschleusen von Bündeln
- Mitlesen von Bündeln
- Abfangen von Nachrichten

Schutz vor Angreifern

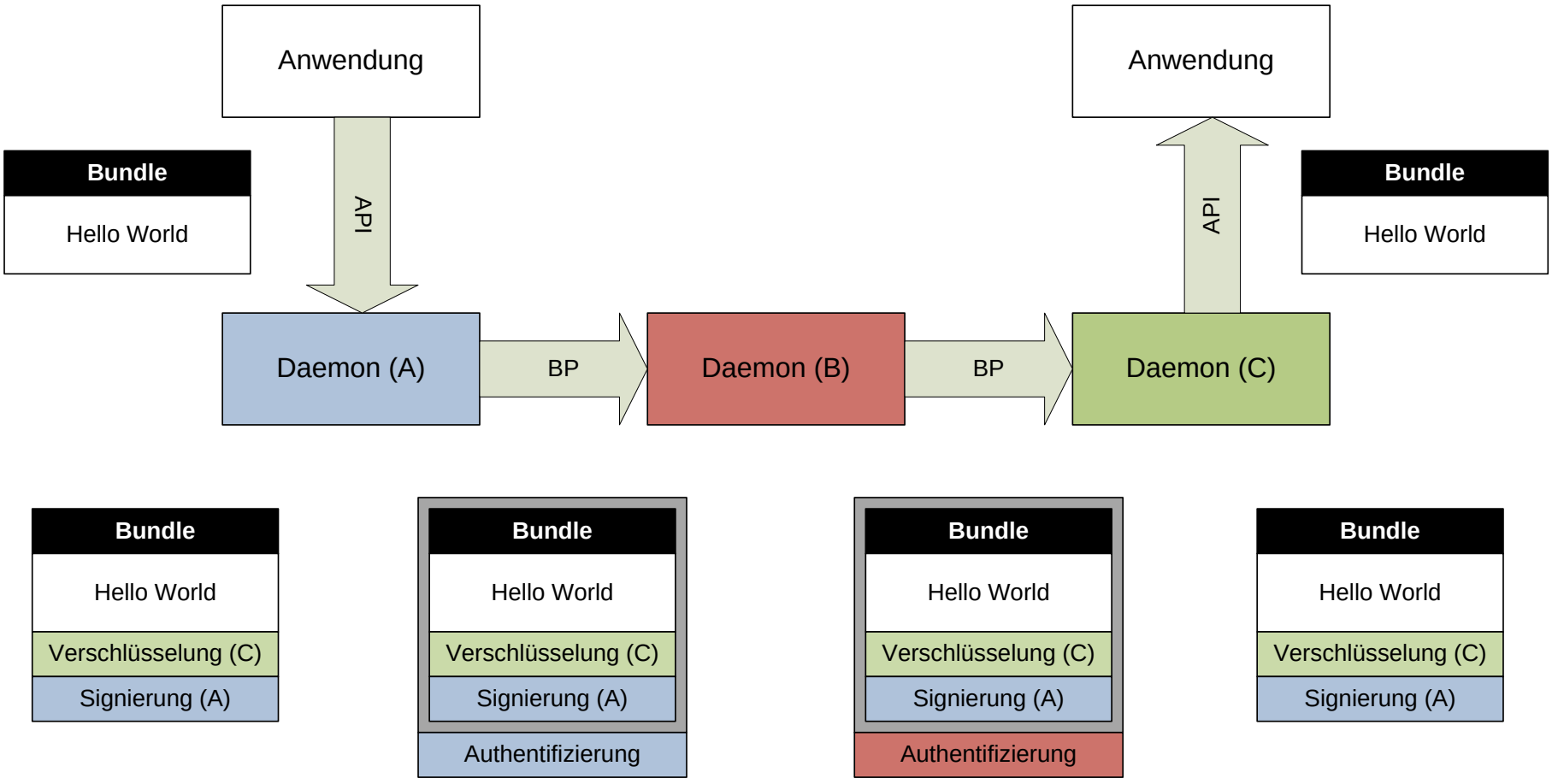
Angriffsszenarien

- Einschleusen von Bündeln
- Mitlesen von Bündeln
- Abfangen von Nachrichten

Bundle Security Protocol

- Optionale Erweiterung des Bundle Protocol
- Authentifizierung, Integrität und Vertraulichkeit
- Ende-zu-Ende und Hop-by-Hop

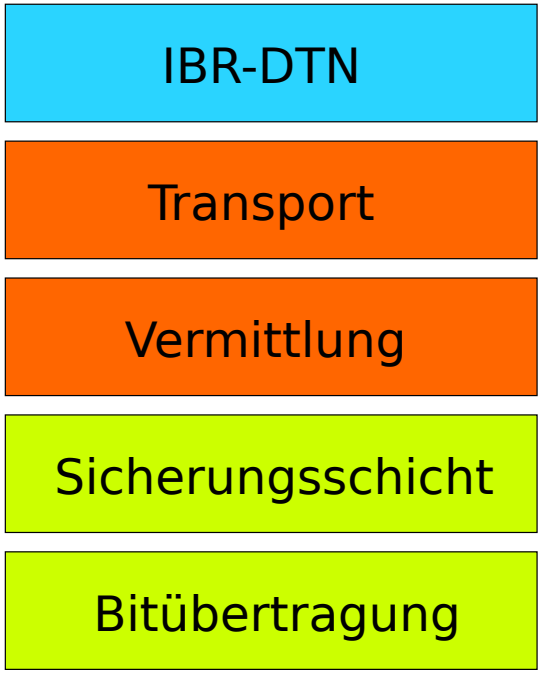
Bundle Security Protocol



Schutz vor Angreifern

Angriffsszenarien

- Abfangen von Nachrichten
- (D)DoS Attacke
- Softwarelücken ausnutzen



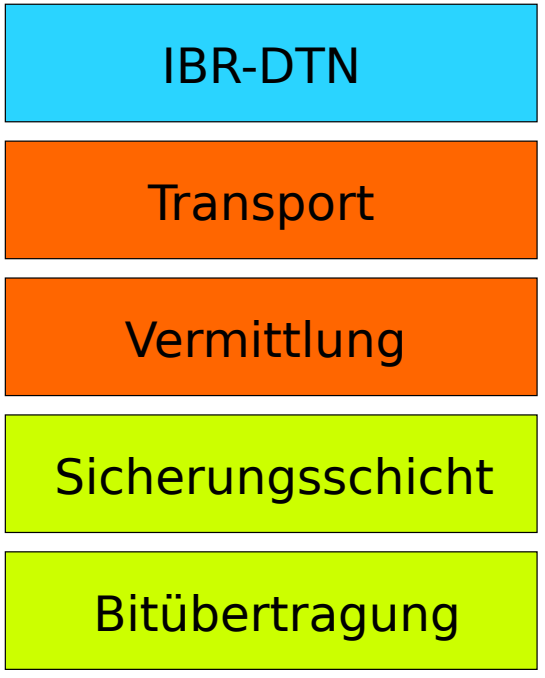
Schutz vor Angreifern

Angriffsszenarien

- Abfangen von Nachrichten
- (D)DoS Attacke
- Softwarelücken ausnutzen

Netz kryptographisch schließen

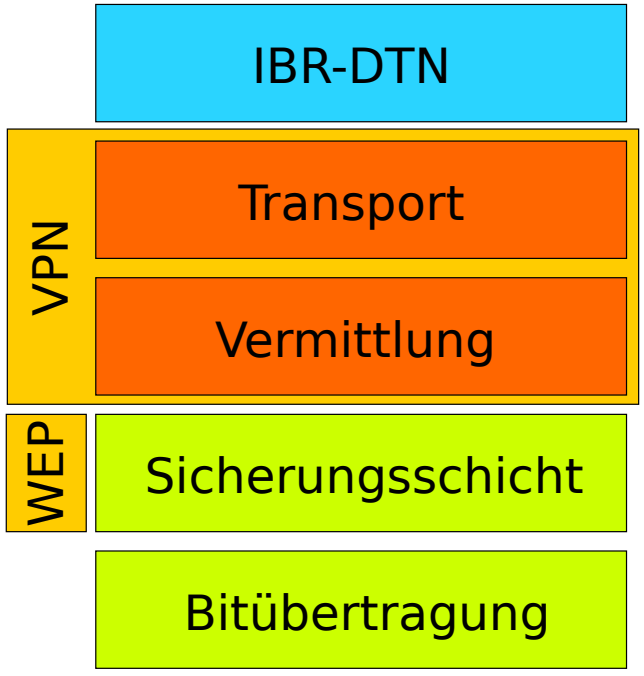
- WEP unsicher/geknackt
- WPA (kein Ad-Hoc Mode)
- WPA2 (kein Ad-Hoc Treiber verfügbar)



Schutz vor Angreifern

Netz kryptographisch schließen

- Ad-Hoc VPN (tinc) kapselt die Kommunikation zwischen Knoten
- Firewall blockt alles bis auf Kommunikation mit VPN Daemon
- Zugriff ausschließlich mit gültigen Zertifikaten möglich
- WEP-128 zum Schutz vor „versehentlichem“ Zugriff



Zusammenfassung

- Motivation
  - Nutzung von ÖPNV-Fahrzeugen zum Transport von Daten
  - Kostengünstige Infrastruktur
  - Hohe Abdeckung bei Aufnahme von Messwerten
- Architektur eines unterbrechungstoleranten Kommunikationssystems
- Netzkomponenten basierend auf Linux und IBR-DTN
- Netzkommunikation über WLAN → Sehr exponiert!
- Mehrschichtiges Sicherheitskonzept
- Penetrationstests
  - Keine signifikanten Lücken festgestellt
  - Stellt lediglich die Anwesenheit von Sicherheitsmängeln fest

Ausblick

- Neighbor Discovery
  - Stabilität gegenüber DoS Angriffen
  - Angriffe erkennen und blocken
  - Authentisierung der Beacons
- Sink-Hole Angriff (ohne VPN)
  - Studentische Arbeit
  - Erkennen ob ein Bündel den anderen Knoten erreicht hat
  - Verwendung von TLS zur Authentifizierung
- Tests
  - Dauerhaftes virtuelles Testbed
  - Angriffe „ausprobieren“
  - Aktualisierungsstrategien erproben

Fragen?

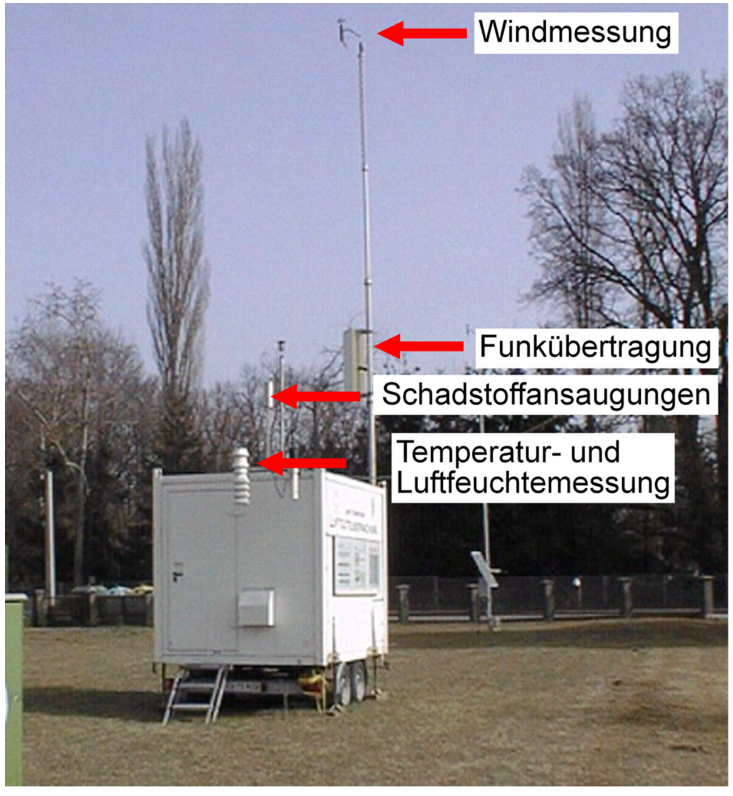
Johannes Morgenroth
morgenroth@ibr.cs.tu-bs.de

http://www.optracom.de/

Motivation

Stationäre Erfassung von Messwerten

- Typischerweise ein Container
- Beobachtung über längeren Zeitraum möglich
- Installation aufwendig
- Lokal beschränkt
- Periodisches einsammeln der Daten notwendig



Quelle: http://www.ubz-stmk.at/

Motivation

Mobile Erfassung von Messwerten

- Umgerüstetes Fahrzeug mit Messtechnik
- Flächendeckend bei entsprechendem Aufwand
- Schnell verfügbar
- Momentaufnahme, keine Entwicklung

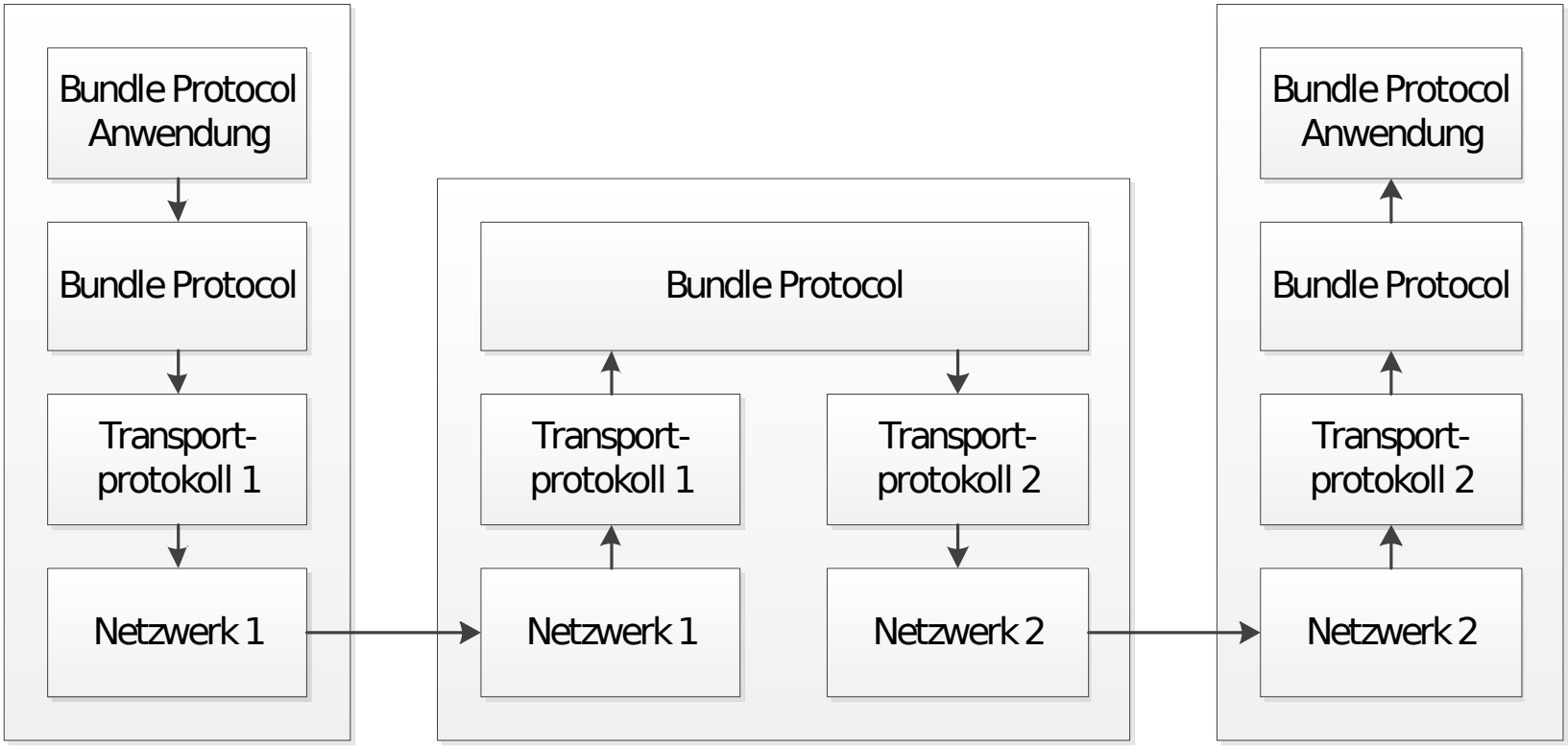
Quelle: http://www.dlr.de/

Anwendungen

Überwachung von streckenseitigen Anlagen

- Gleisanlagen oder Signalgeber
- Erweiterung durch Funkmodule
- Einsammeln von aufgezeichneten Daten

DTN Stack



Quelle: Diplomarbeit, Oliver Langner

Aktualisierungen

Eigenschaften

- Mehrstufiges Verfahren
- Verteilung von Aktualisierungspaketen über DTN
- Aktualisierung erfolgt über einen längeren Zeitraum
- Mischbetrieb im virtualisiertem Testbed erproben
  - Neue Softwareversionen müssen zusammen mit der vorherigen Software eine Basisfunktionalität beibehalten
- Jeder aktualisierte Knoten sendet einen Aktualisierungsstatus

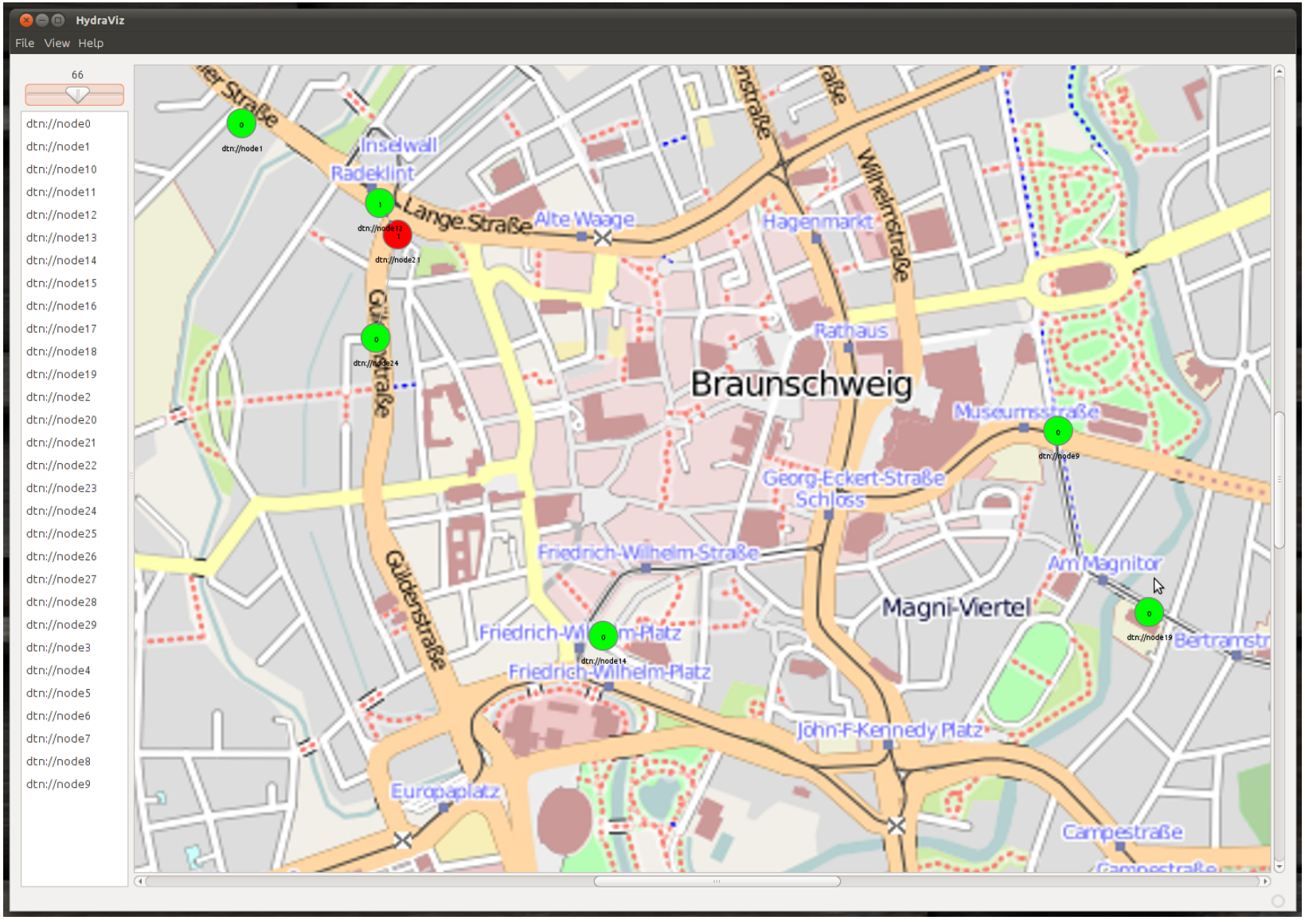
Hydra - Virtualisiertes Testbed

Eigenschaften

- Schneller Aufbau von Szenarien
- Bewegungssimulation in Echtzeit
- Virtualisierte Hardware (XEN, VirtualBox, ...)
- Einbindung echter Hardware möglich
- Identische Software

Anwendungsfälle

- Erprobung von Aktualisierungen
- Testen neuer Wegewahlverfahren
- Sicherheitskritische Angriffe


HydraViz
File View Help
66
dtn://node0
dtn://node1
dtn://node10
dtn://node11
dtn://node12
dtn://node13
dtn://node14
dtn://node15
dtn://node16
dtn://node17
dtn://node18
dtn://node19
dtn://node2
dtn://node20
dtn://node21
dtn://node22
dtn://node23
dtn://node24
dtn://node25
dtn://node26
dtn://node27
dtn://node28
dtn://node29
dtn://node3
dtn://node4
dtn://node5
dtn://node6
dtn://node7
dtn://node8
dtn://node9
Inselwall
Radeklint
Lange Straße
Alte Waage
Hagenmarkt
Wilhelmstraße
Rathaus
Braunschweig
Museumsstraße
Georg-Eckert-Straße
Schloss
Friedrich-Wilhelm-Straße
Am Magnitor
Magni-Viertel
Friedrich-Wilhelm-Platz
John-F-Kennedy Platz
Europaplatz
Campestraße