Autonomer Betrieb und Simulation robuster WLAN-Mesh-Netze für Hochsicherheitsanwendungen

Erläuterung der Problemstellung, die mit der Idee gelöst werden soll:

Die Benutzung drahtloser Netze ist in Szenarien ohne vorhandene Infrastruktur für eine kurzfristige Bereitstellung von Netzwerkressourcen unabdingbar, da deren Installationszeiten wesentlich geringer sind. Jedoch sind die Aufrechterhaltung von Sicherheitseigenschaften und ein zuverlässiger Betrieb derzeit zumeist kompliziert und damit fragil. Heutige Lösungen werden oftmals manuell konfiguriert und besitzen daher lange Konfigurations- und Entstörzeiten. In diesem Bereich existieren bereits proprietäre Speziallösungen, diese können jedoch mit dem aktuell verfügbaren Stand der Technik nicht Schritt halten. Dies betrifft deren Leistungsfähigkeit, Sicherheitseigenschaften und Robustheit des Routings gegenüber Ausfällen. Weiterhin ist der Netzwerkzustand verteilt arbeitender drahtloser Mesh-Systeme mit derzeitiger Technik nur schwer und nicht skalierbar erfassbar.

Die Netze müssen ein breites Spektrum an Nutzungsanforderungen unterstützen, etwa Übertragung von Lagedaten, Ereignissen, Messdaten oder Videos und Sprache. Letztere Szenarien der Multimediaübertragung erfordern geringe Latenzen und Jitter. Im Allgemeinen jedoch ist für jegliche Art der Kommunikation ein ausfalltolerantes und robustes Routing unabdingbar. Bisherige Systeme skalieren durch häufigen Broadcast-Verkehr nicht für mehrere hundert oder tausende Teilnehmer. Gruppenkommunikation muss je nach Anwendungsfall, z.B. für Push-to-Talk, unterstützt werden.

Mesh-Netze lassen sich zwar vergleichsweise einfach mit zentralen Instanzen, etwa Authentisierungsservern betreiben, diese stellen jedoch einen leicht zu störenden Single-Point-of-Failure dar. Sicherheitsanforderungen der Übertragung von Verschlusssachen erfordern eine umfassende Sicherheitsarchitektur, welche in diesem Fall verteilt realisiert werden muss. Die Kompromittierung einzelner Mesh-Knoten darf dabei nicht die Sicherheit des Gesamtnetzes oder die Vertraulichkeit bisheriger, möglicherweise abgefangener und aufgezeichneter, Kommunikation gefährden. Darüber hinaus ist eine Anbindung von Endgeräten und die Bereitstellung von Netzwerkdiensten für die Akzeptanz des Systems essenziell. Hierfür ist eine Ende-zu-Ende Absicherung des Verkehrs zwischen den jeweiligen Mesh-Knoten der Endgeräte notwendig, welche in bisherigen WLAN-Mesh-Standards nicht vorgesehen ist.

Ein fundamentales Problem ist die schwer abzuschätzende Realisierbarkeit großer Netze auf Basis von kleinen Testinstallationen. Systeme müssen daher Mechanismen extensiver Skalierbarkeitstests noch vor einem produktiven Deployment vorsehen. Dieser Entwicklungsprozess soll zudem möglichst kosteneffizient sein und dabei das Ergebnis einer zuverlässigen Implementierung garantieren.

Beschreibung der Idee und wie sie das Problem lösen soll:

IP-basierte (Layer 3) Mesh-Netzwerke sollen mit konventioneller Standardhardware aufgebaut werden. Zusätzliche Eigenschaften wie skalierbares Routing, autonome Konfiguration von Hop-by-Hop- und Ende-zu-Ende-Verschlüsselung, Mobilitätsunterstützung und

Monitoring-/Betriebskonzepte werden software-defined bereitgestellt. Bei den Einzelverfahren wird, im Unterschied zum Stand der Technik, primär auf geringe Übertragungslatenzen und Robustheitsaspekte geachtet. Durch eine direkte Integration von Netzwerk-Simulatoren ist ein Pre-Deployment-Testing und eine umfassende Leistungsbewertung möglich.

Die vorgeschlagene Lösung wird daher Maßnahmen in Bezug auf die folgenden Aspekte vorsehen:
- Ende-zu-Ende-Absicherung zwischen Mesh-Knoten auf Layer 2/Layer 3
- Attestierte und gesicherte Anbindung handelsüblicher Endgeräte (auf Layer 2) mit optionaler zusätzlicher Ende-zu-Ende-Absicherung auf Layer 3
- Skalierbares, robustes Routing mit Unterstützung für mehrere hundert Mesh-Knoten und optionalen Backup-Pfaden
- Sachgerechte Betriebsunterstützung durch automatisiertes, sicheres Enrollment, skalierbares Monitoring, übersichtliche Diagnose- und Managementwerkzeuge
- Simulation mit weitgehend Code-identischen Protokollimplementierungen zur Prädiktion des Leistungs- und Skalierbarkeitsverhaltens in spezifischen Szenarien

Als Ausgangspunkt für die Realisierung des Konzepts kann ein Framework verwendet werden, welches im Rahmen von zwei Forschungsprojekten gefördert durch die RWTÜV-Stiftung am Fachgebiet Telematik/Rechnernetze entstand. Dieses ermöglicht einen Entwicklungsprozess, welcher Simulation und realen Einsatz derselben Software mit identischer Codebasis gleichermaßen ermöglicht. Weitere Vorarbeiten werden an späterer Stelle in diesem Abschnitt erläutert. Für die vorgeschlagene Lösung sind aus technischen Gesichtspunkten zunächst die angesprochene Sicherheitsarchitektur und Routing-Lösung weiter zu entwickeln, welche den autonomen Betrieb ermöglichen. Ein signifikanter Anteil der Arbeit wird insbesondere für die Realisierung von Hochsicherheitsanforderungen notwendig.

Konzeptionell realisiert die Sicherheitsarchitektur eine Ende-zu-Ende-Sicherung auf Layer 3 durch automatisch konfigurierte IPsec-Tunnel. Zusätzlich werden alle drahtlosen Links auf Layer 2 durch die WLAN-Hardware Hop-by-Hop verschlüsselt. Herkömmliche Clients werden über ein Access Point Interface angebunden. Weitere Interfaces im Mesh-Modus realisieren das Mesh-Backhaul. Die Zuordnung von Clients zum aktuellen Mesh-Knoten wird durch Erweiterungen des Routing-Protokolls umgesetzt. Weiterhin sind die Clients optional in der Lage, ihre Assoziation mit dem aktuellen Access-Point kryptographisch zu attestieren. Das Vorliegen einer aktuellen Attestation kann optional verpflichtend für das Anlegen einer Route zum entsprechenden Client über den derzeitigen Access Point auf der Remote-Seite gestaltet werden. Die Möglichkeit herkömmliche Clients anzubinden umfasst hierbei insbesondere auch IoT-Devices, etwa kleine Geräte und Sensoren.

Robustheit erreicht das eingesetzte Routing-Verfahren wahlweise durch Abstimmung auf schnelle Konvergenzzeiten bzw. die Nutzung von Ersatzpfaden. Ausgehend von DSDV/Babel werden Cross-Layer Optimierungen, sowie geschickte Delta-Updates zur Verringerung des Nachrichtenaufwandes und zum Erreichen schneller Umschaltzeiten im Fehlerfall eingesetzt. Durch die Bildung kleiner L2-Kollisionsdomänen (geroutete /32 oder /128 Netze) wird eine starke Reduktion des Broadcast-Verkehrs, etwa verursacht durch ARP, erreicht. In seltenen Fällen (vom Verkehrsaufkommen her gesehen) ist jedoch trotzdem ein Broadcast an alle Teilnehmer notwendig, etwa im Push-To-Talk-Funkszenario. Dieses wird durch authentisierten Application Layer Multicast abgedeckt. Durch die automatische, verteilte Auswahl

verschiedener Funkkanäle wird zudem ein hoher Durchsatz zwischen Endgeräten erreicht. IP-Adressen von Clients werden per X.509-Zertifikat attestiert und anschließend für die lokale Konfiguration von DHCP-Einträgen und Routen verwendet. Die initiale Kommunikation zwischen Endgeräten ist kurzzeitig Hop-by-Hop-gesichert, nach einem kurzen Delay werden reaktiver Aufbau von IPsec-Tunneln auf Basis von Informationen aus dem Routing über die Client-Access-Point-Zuordnung aufgebaut.

Funkkanäle werden unter Berücksichtigung von Kanal-Interferenz automatisch und verteilt gewählt. Das Routing-Verfahren ist mittels hybrider Metriken in der Lage eine Folge von drahtlosen, sowie drahtgebundenen Links zu benutzen. Hiermit können beliebige Mischformen aus drahtloser und verdrahteter Infrastruktur realisiert werden.

Durch die Trennung der Implementierung des Protokollautomaten von der eigentlichen Paketweiterleitung wird die Anwendung der gleichen Code-Basis mit Linux-Systemen und im Simulator ermöglicht. Es werden Pre-Deployment-Tests mit groß angelegten Simulationsstudien und Funktionstests mit einem kleinen Testbed durchgeführt. Weiterhin besteht hierdurch die Möglichkeit komplexe Regressionstests auf Basis realer Fehlerbilder zu modellieren.

Für den Betrieb wird an einer oder mehreren Positionen ein dediziertes Monitoring-System betrieben, zu dem die WLAN-Geräte einen Reverse-Multicast-Baum aufbauen und ihre Monitoring-Daten übertragen. Anschließend kann über das Monitoring-System auf aggregierte Sichten und Entstörhinweise zugegriffen werden. Über diese Monitoring-Systeme können die Knoten außerdem initial provisioniert und anschließend umkonfiguriert werden. Alles in allem ist mit einem verhältnismäßig geringen personellen Aufwand für den Betrieb zu rechnen.

Zur Hardware-technischen Umsetzung im Realsystem können kompakte Embedded-PCs, welche WLAN und Ethernet-Schnittstellen bieten, eingesetzt werden. Weitere Funkhardware, etwa Richtfunk, kann mittels passender Peripherie oder über Ethernet und geeigneten Gateways angebunden werden. Client-Hardware ist durch die angedachte Architektur nahezu beliebig wählbar, solange gängige WLAN-Standards unterstützt werden. Umfangreiche Simulationsstudien sind entweder mit Desktop-Hardware, vorzugsweise jedoch mit leistungsstarker Server-Hardware umsetzbar.

Im derzeitigen Entwicklungsstadium gibt es Prototypen des Routing-Verfahrens und der Mobilitätsunterstützung aus Vorarbeiten der RWTÜV-Stiftung-geförderten Projekte am Fachgebiet Telematik/Rechnernetze. Diese Prototypen können auf Wunsch während der Konferenz vorgeführt werden. Hinsichtlich der Sicherheitsarchitektur, des Monitorings, sowie des Enrollments und der Konfiguration sind jedoch noch Arbeiten zu leisten. Weiterhin sind umfangreiche Maßnahmen zur Erlangung von Produktreife, sowie Härtung der Implementierung für Hochsicherheitsanforderungen notwendig. Zwar wird während des Entwicklungsprozesses bereits inhärent auf Sicherheit geachtet, jedoch sind weitere Maßnahmen insbesondere im Hinblick auf eine mögliche Zulassung unentbehrlich. Sollen gleichzeitig viele WLAN-Karten und ein schneller Prozessor mit Hardwarebeschleunigung eingesetzt werden, so ist diese Kombination in kompakter Form derzeit nicht erhältlich. Dies kann bspw. durch einen Cluster-Modus aus mehreren Mesh-Knoten, durch angepasste Embedded-Hardware oder Standard-Server-Hardware mit Unterstützung mehrerer WLAN-Interfaces bewerkstelligt werden. Die jeweilige Lösung kann hierbei spezifisch auf die Einsatzbedingungen flexibel abgestimmt werden.

Für die Produktisierung ist die Zusammenarbeit mit Unternehmenspartnern im Bereich Netzwerksicherheit notwendig. Ausgehend von den Erfahrungen des Fachgebietes bei der Überführung des Autokonfigurationssystems SOLID in die Produktreife, bietet sich beispielsweise die secunet Security Networks AG (Ansprechpartner: Dr. Kai Martius) als möglicher Verbundpartner an. Die secunet verfügt über umfangreiche Expertise im Hinblick auf zugelassene Sicherheitslösungen für alle Sicherheitseinstufungen.

Aufgrund der Weiterleitung von Paketen auf Layer-3 (IPv4/IPv6) ist das System mit bestehenden Netzwerke interoperabel. Weiterhin kann ein inkrementelles Deployment mit ggf. angepassten Gateways realisiert werden. Das Monitoring-System kann derart konzipiert werden, dass vorhandene Komponenten unterstützt werden (z.B. Syslog-Server und SNMP-Traps).

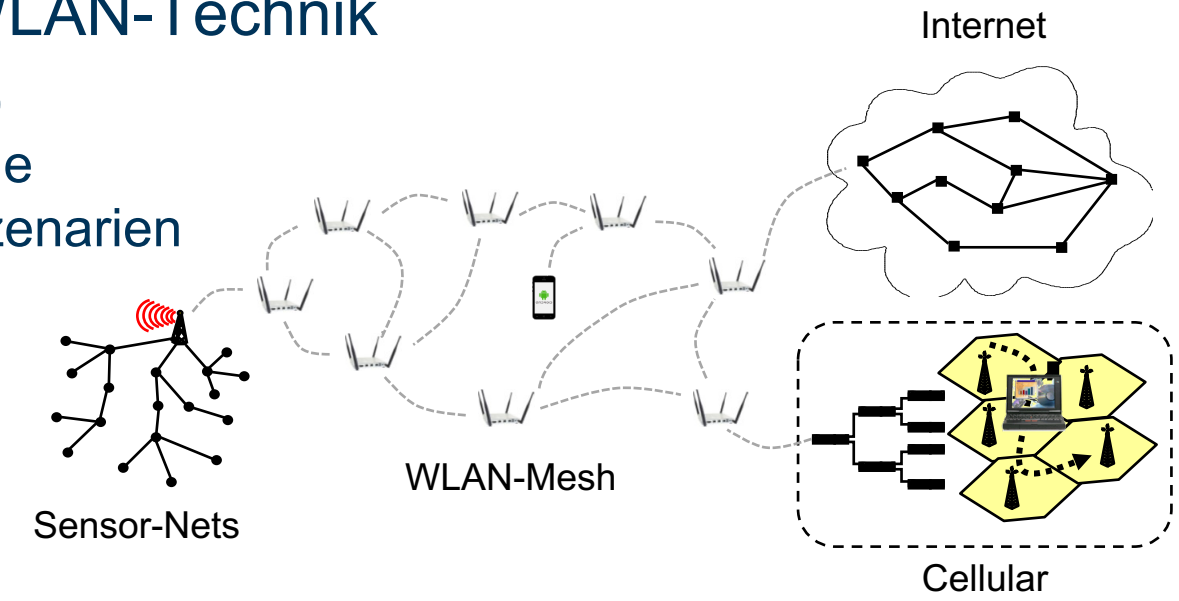
Prof. Dr.-Ing. Günter Schäfer

M. Sc. Martin Backhaus · M. Sc. Markus Theil · Dr.-Ing. Michael Roßberg

AUTONOMER BETRIEB UND SIMULATION ROBUSTER WLAN-MESH-NETZE FÜR HOCHSICHERHEITSANWENDUNGEN

Motivation

- Neuartige Anwendungsszenarien für WLAN-Technik
  - Ad-hoc-/Mesh-Netzwerke (Funknetzwerke)
    - Automatisierungstechnik in der Industrie
    - Polizeiliche Großlagen/Katastrophenszenarien
    - City Mesh Networks
    - …
  - Internet of Things



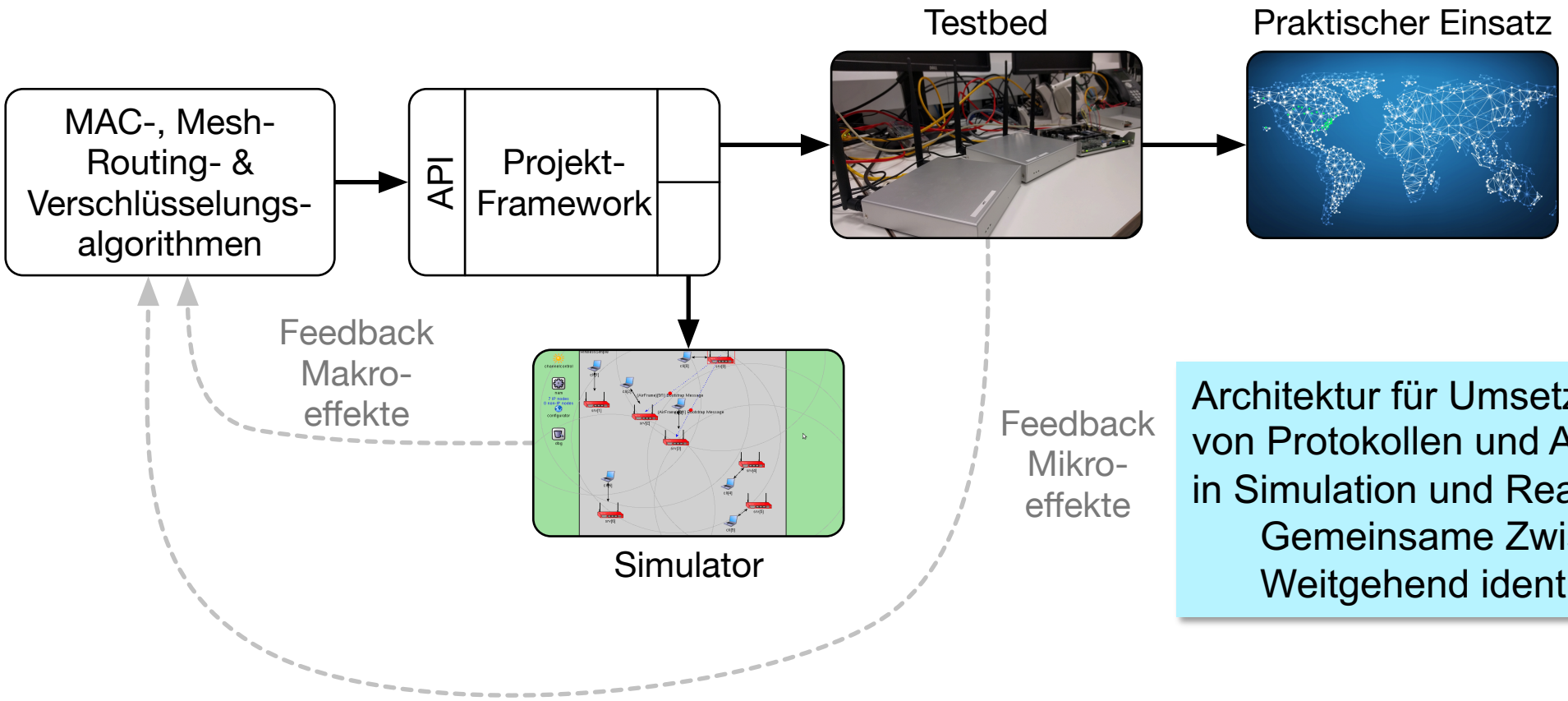
- Herausforderungen:
  - Zunehmende Komplexität
  - Skalierbarkeit unklar
  - Ausfalltolerantes Routing bzw. schnelle Reparatur bei Ausfällen
  - Unzureichende Ende-zu-Ende-Sicherheit, Verkehrsflussanalysen mögl.
  - Monitoring & Management
  - Dienstqualität schlecht einschätzbar/optimierbar

Diskrepanz bei Verfahren aus Forschung und Praxis

- Forschung meist auf Grundlage idealisierter Simulationsstudien ODER kleiner Realsysteme [1]
- Simulative Untersuchungen unabdingbar:
  - Reproduzierbarkeit
  - Verhalten sehr großer Netze
  - Paralleles Testen durch mehrere Entwickler
- Praktische Untersuchungen auch unabdingbar:
  - Verhalten bei paralleler Ausführung
  - Realzeitverhalten
  - Verhalten unter Last (Interferenz!)
  - Echte Hardware und Umgebungseinflüsse

[1] G. Papadopoulos; K. Kritsis; A. Gallais; P. Chatzimisios; T. Noe: Performance Evaluation Methods in Ad Hoc and Wireless Sensor Networks: A Literature Study. IEEE Communications Magazine 54.1 (2016): 122-128.

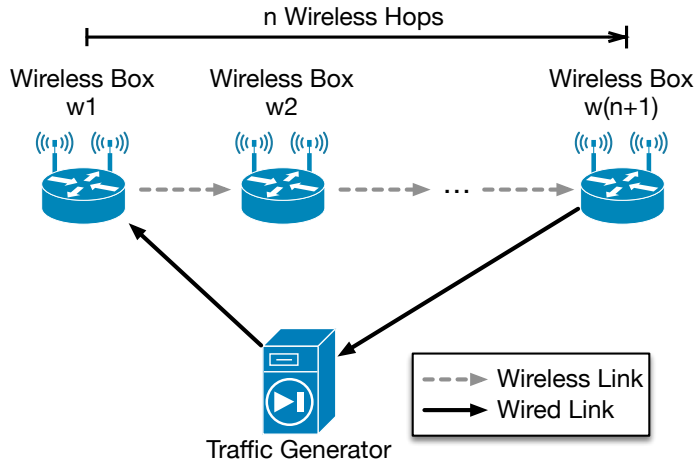
Beitrag: Framework zur Entwicklung und Bewertung skalierbarer, robuster, sicherer, betreibbarer WLAN-Meshs

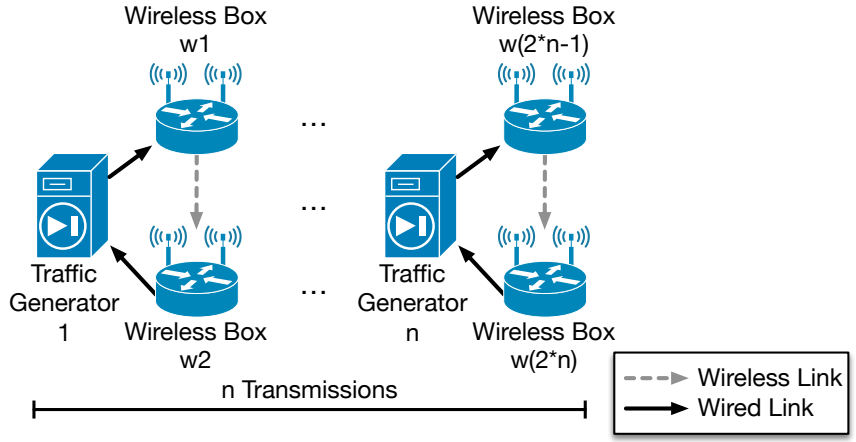


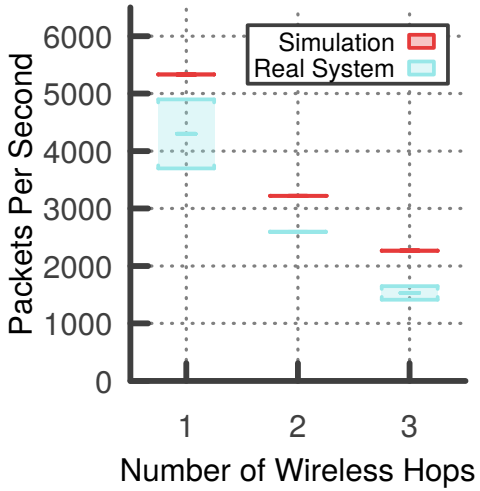
Architektur für Umsetzung
von Protokollen und Algorithmen
in Simulation und Realsystem
- Gemeinsame Zwischenschicht
- Weitgehend identischer Code

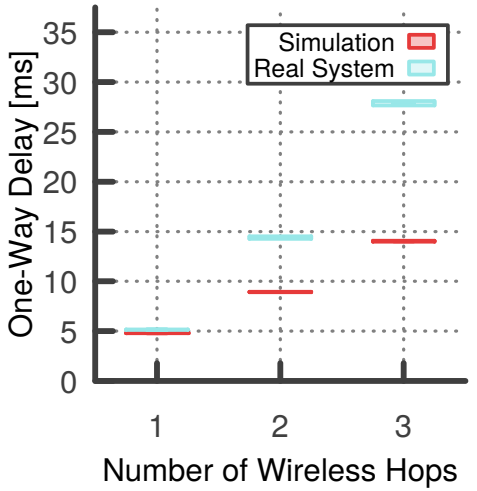
[2] M. Backhaus, M. Theil, M. Rossberg, G. Schaefer, D. Sukiennik: A Comprehensive Framework to Evaluate Wireless Networks in Simulation and Real Systems, IEEE/ACM DS-RT, 2018.

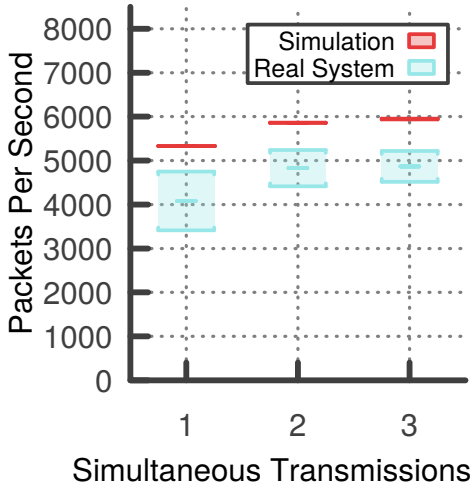
Simulation vs. Realsystem

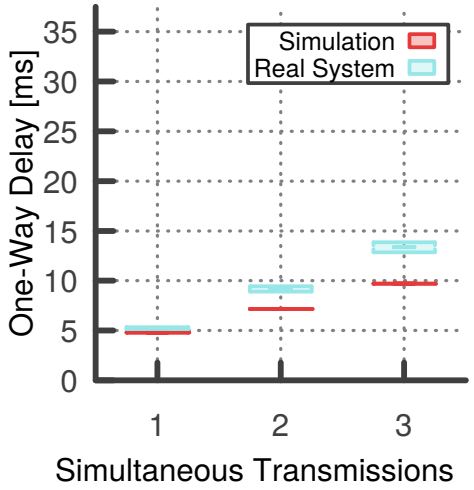






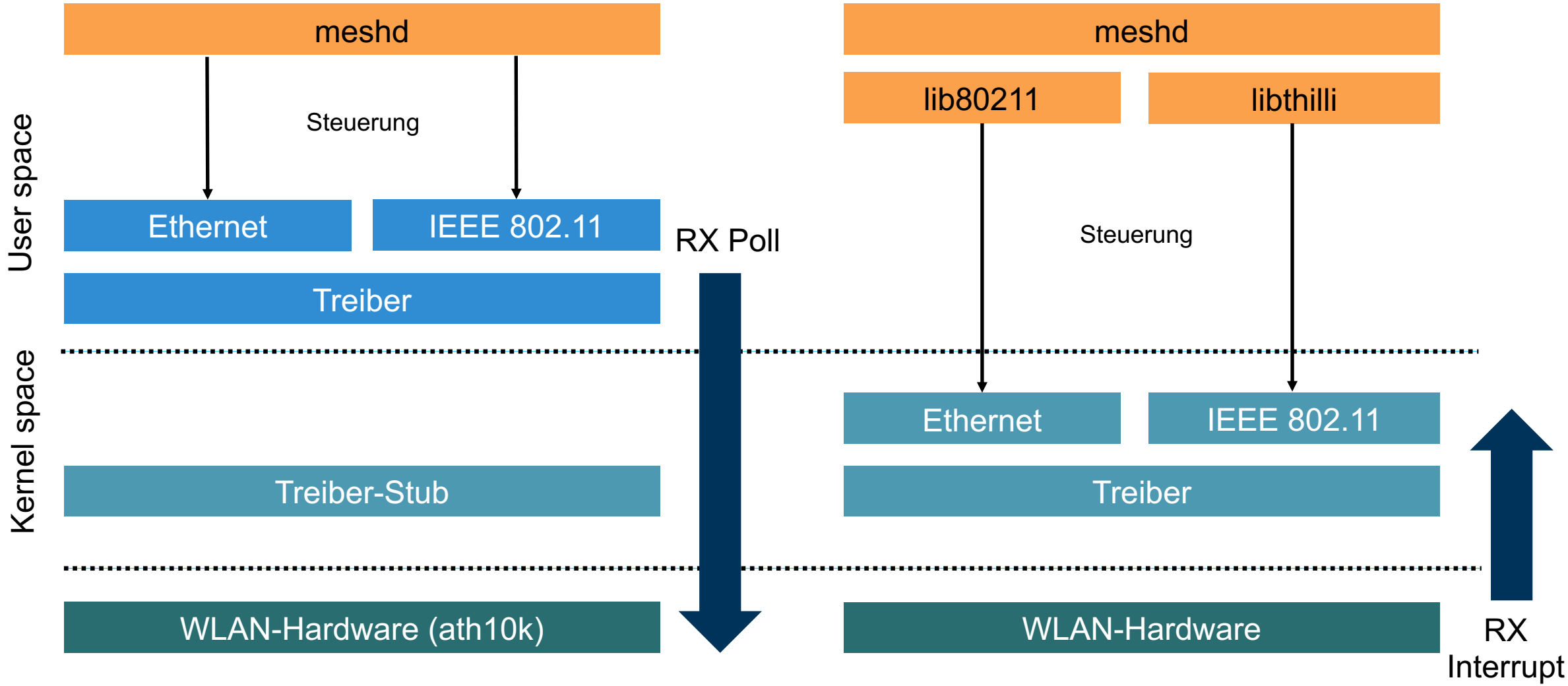




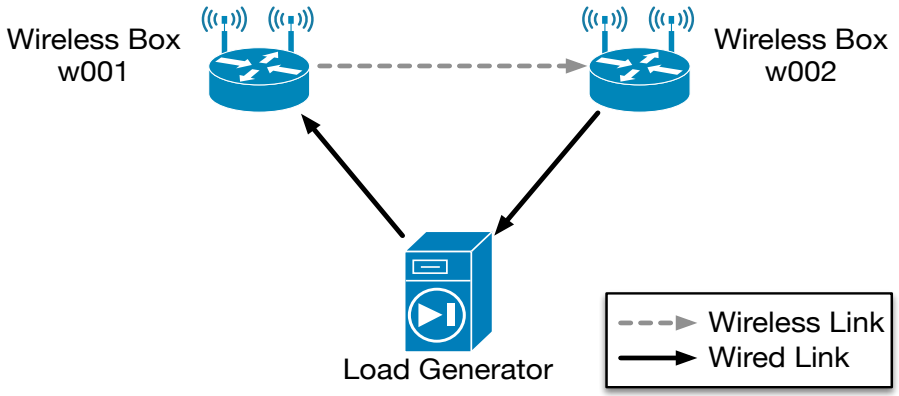


[2] M. Backhaus, M. Theil, M. Rossberg, G. Schaefer, D. Sukiennik: A Comprehensive Framework to Evaluate Wireless Networks in Simulation and Real Systems, IEEE/ACM DS-RT, 2018.

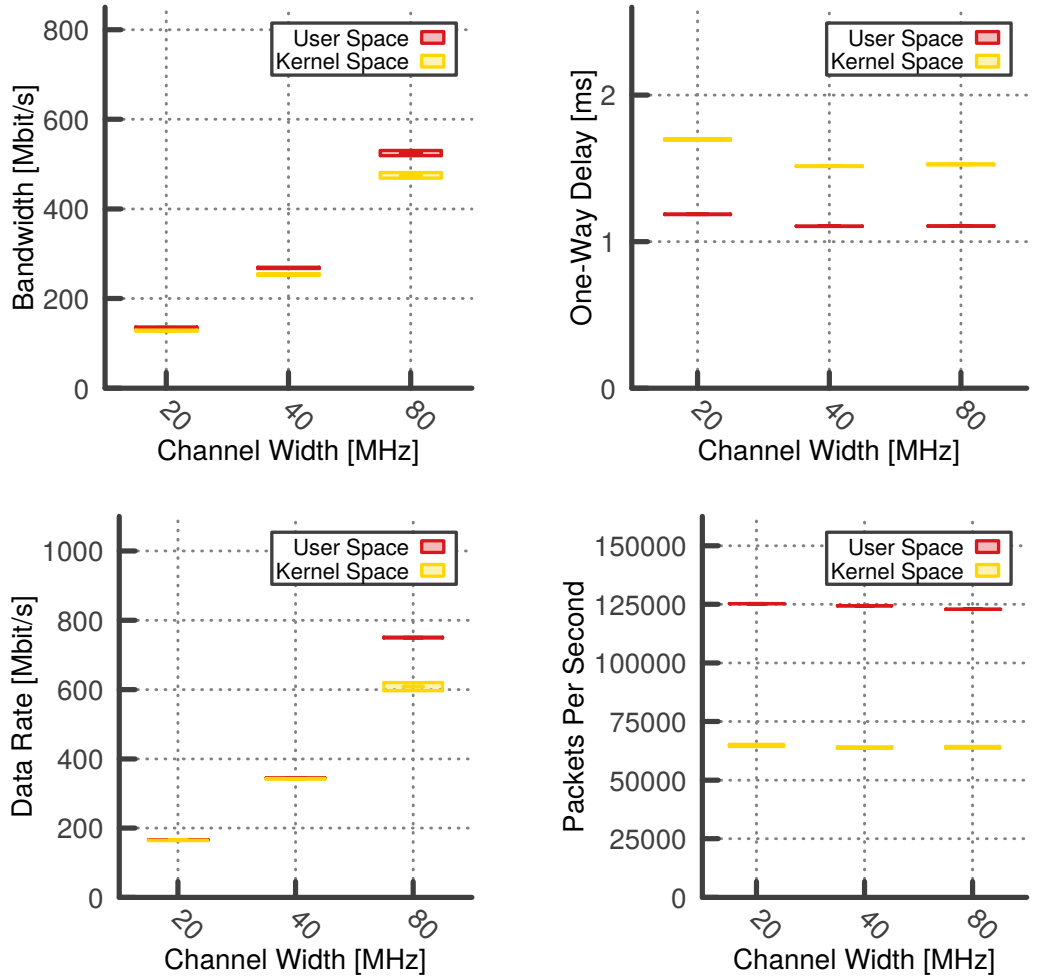
DPDK vs. Kernel-Modus



User-Space vs. Kernel-Space



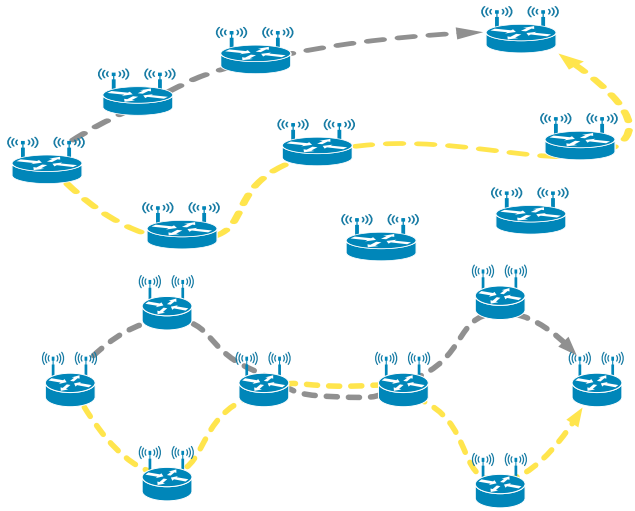
- Vorteile User-Space:
  - Einfachere Code-Entwicklung
  - Bessere Performance
- Vorteile Kernel-Space:
  - Unterstützung vielfältiger Hardware
  - Unterstützung aller WLAN-Funktionen (AP-Modus, Neuerungen etc.)



[3] M. Backhaus, M. Theil, M. Rossberg, G. Schaefer: Towards a Flexible User-Space Architecture for High-Performance IEEE 802.11 Processing, IEEE WiMob, 2018.

Robustes & Skalierbares Routing

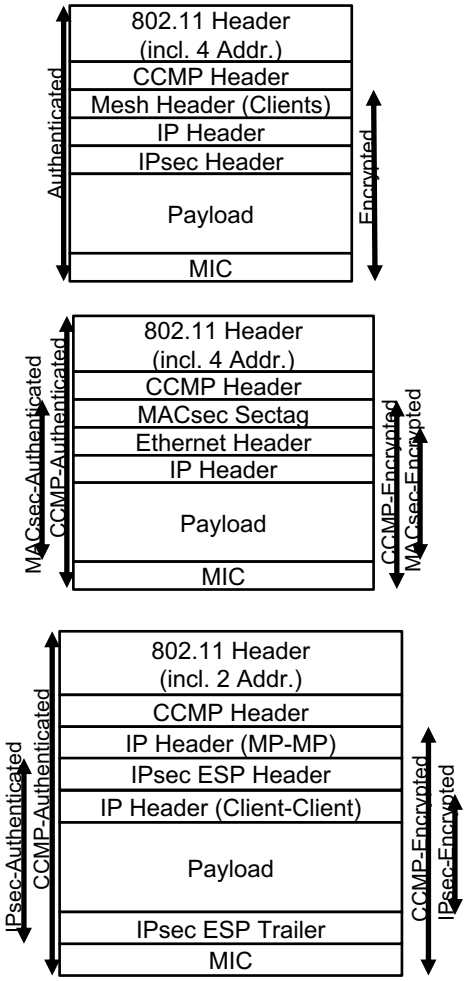
- Bisher: WLAN-Mesh-Standard 802.11s
  - Einfaches Routing: beschränkt auf Erreichbarkeit, kein Fokus auf Robustheit
  - Regelmäßiges Fluten von Beacons
  - Andere Verfahren: BATMAN, Path Request/Response Dialog (AODV, HWMP)
- Erster Ansatz – Ziel: Robustheit per Backup-Pfade
  - Globale Verteilung der Netztopologie
  - Source-Routing über Hauptpfad bzw. Backup-Pfad
  - Backup-Pfade Interferenzzonen-disjunkt [4]
- Aktueller Ansatz – Ziel: Skalierbarkeit + Robustheit
  - Optimierung von Distanzvektorverfahren (BABEL + Delta-Advertisements)
  - Schnelle (lokale) Reparatur bei teilweisen Ausfällen



[4] M. Backhaus, M. Theil, Markus; M. Rossberg,G. Schaefer: Robust and Scalable Routing in Wireless Mesh Networks Using Interference-Disjoint Backup Paths, IFIP WMNC, 2019

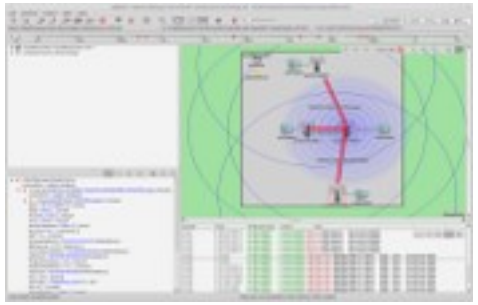
Unterstützung von Hochsicherheitsanwendungen

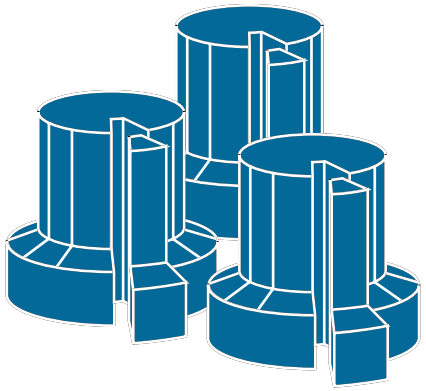
- Bisher: WLAN-Mesh-Standard 802.11s
  - Hop-by-Hop-Verschlüsselung ⇒ Keine Ende-zu-Ende-Absicherung
  - Schlüsselaushandlung mit gemeinsamem Geheimnis
  - Kein Schutz vor Verkehrsflussanalysen (E2E-MAC-Adressierung)
- Erster Ansatz:
  - Weiterentwickelte E2E-MACsec-Verschlüsselung [5]
  - Dezentrale & zertifikatsbasierte Schlüsselaushandlung (inkl. zertifizierte MAC-Adressen)
  - Noch offen: Authentizität von IP-Adressen
- Aktueller Ansatz:
  - Zertifikatsbasiertes Schlüsselaushandlungsverfahren für Hop-by-Hop-L2-Verschlüsselung
  - E2E-Verschlüsselung auf Basis von IPsec (inkl. Key Mgmt.)
  - Attestierung von IP-Adr. & MP-Zuordnung von Clients



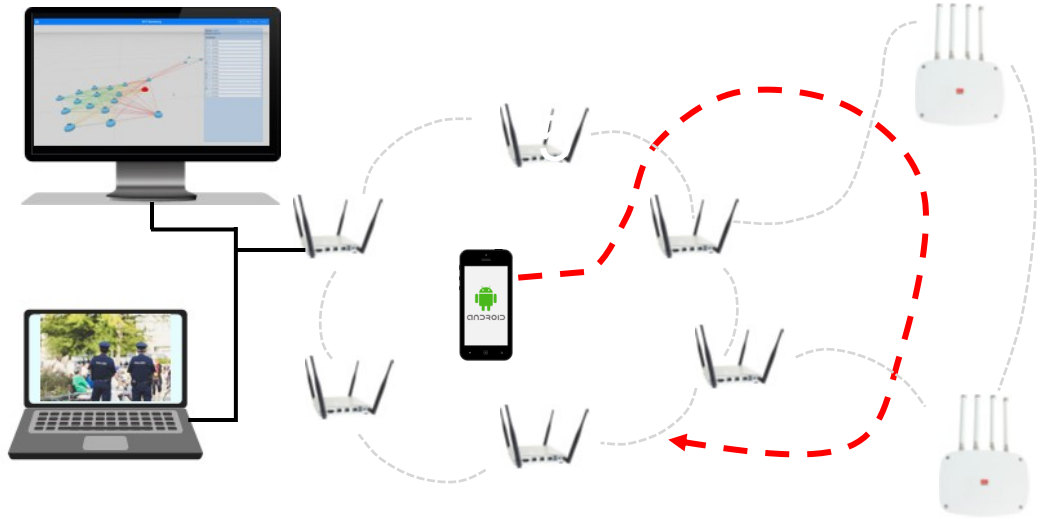
[5] M. Theil, M. Backhaus, Martin; M. Rossberg, G. Schaefer: Towards a Security Architecture for Hybrid WMNs, ARES 2019 (5G Workshop)

Demonstration: Überblick





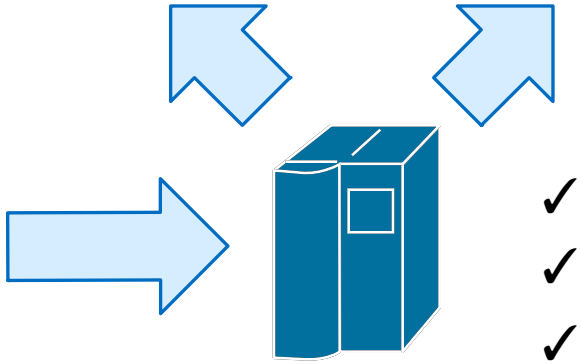
Simulations-Cluster
✓ Anpassungen für Simulation



Realsystem
✓ Kernel-Instrumentierung

Feature-Entwicklung:
✓ Robustes Routing
✓ Ende-zu-Ende-Sicherheit
✓ Monitoring

Entwickler
✓ Einheitliche API



Build Server

✓ Build für Simulationen
✓ Build für Realsystem
✓ Automatisches Ausrollen der Experimente

Vielen Dank für Ihre Aufmerksamkeit

Wir danken der RWTÜV-Stiftung für die finanzielle Unterstützung im Rahmen zweier Projektförderungen