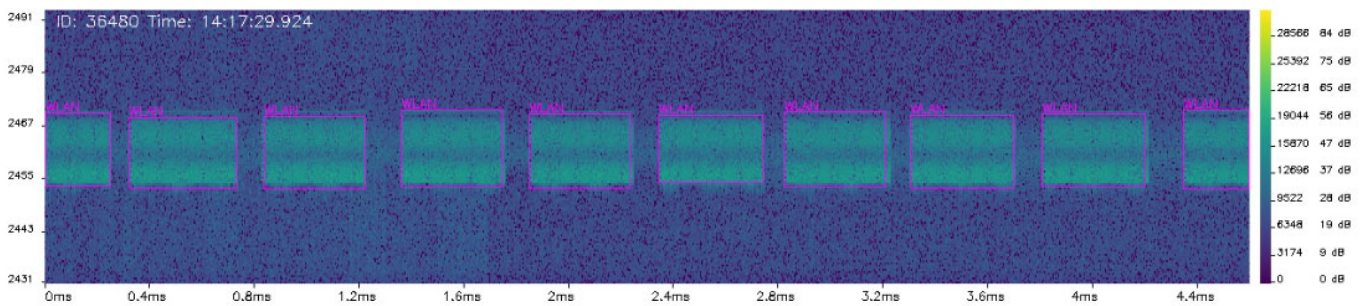
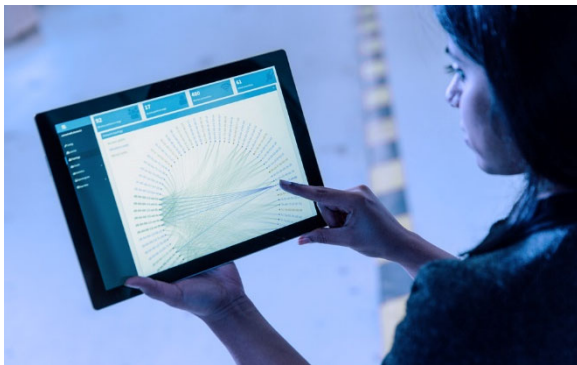


FRAUNHOFER-INSTITUT FÜR INTEGRIERTE SCHALTUNGEN IIS
INSTITUTSTEIL ENTWICKLUNG ADAPTIVER SYSTEME EAS

BERICHT SUNRISE



Entwurf und Entwicklung von Tools für drahtlose
Netzwerksicherheit von IoT Geräten

SUNRISE

Kooperative IoT Security

Jakob Wicht

Dr. Andreas Frotzsch

Fraunhofer-Institut für Integrierte Schaltungen IIS, Institutsteil Entwicklung Adaptiver Systeme EAS
in Dresden.

Projektnummer: 16ES0974

Version: 1.0
Stand: 17. April 2023

Inhalt

1	Einleitung.....	7
1.1	Aufgabenstellung.....	7
1.2	Stand der Technik	7
2	Ablauf des Vorhabens	8
2.1	Konzeption	8
2.2	Erzeugung der Trainings- und Testdaten	9
2.3	Demonstrator.....	11
2.4	Synchronisation mit der Protokollanalyse.....	14
2.5	Sonstige Tätigkeiten.....	15
3	Erzielte Ergebnisse	16
3.1	Wissenschaftliche Dissemination	16
3.2	Voraussichtliche Nutzen und Verwertbarkeit der Ergebnisse.....	17
4	Zahlenmäßiger Nachweis	18
	Abbildungen	19
	Impressum.....	20

1 Einleitung

1.1 Aufgabenstellung

Das SunRISE-Projekt ist Teil der Forschungsstrategie von Fraunhofer, einen Beitrag zur Überwachung und zum Management von drahtlosen Kommunikationstechnologien zu leisten. Fraunhofer erweitert innerhalb von SunRISE seine Expertise auf dem Gebiet der Analyse und Überwachung von drahtlosen Netzwerken. Im SunRISE-Projekt fokussiert sich das Fraunhofer IIS/EAS vor allem auf die Echtzeit-Überwachung und Detektion von drahtlosen Bedrohungen und IT-Angriffen auf Basis verteilter End- und Edge-Knoten. Hierzu wird eine neuartige Plattform zur Überwachung und Analyse von Funksystemen entwickelt, welche die herkömmliche Funkanalyse um Funktionen des RF-Fingerprinting, der Interferenzerkennung und Kollisionsdetektion erweitert.

1.2 Stand der Technik

Drahtlose Netzwerke sind in der heutigen Produktion und Automatisierung unverzichtbar. In einer industriellen Umgebung werden sie insbesondere für die Vernetzung von beweglichen oder unzugänglichen Teilen einer Fabrik eingesetzt. Aufgrund der schwierigen Signalausbreitungsbedingungen sowie koexistierender drahtloser Netzwerke sind Übertragungsfehler, die zu Störungen in der Anwendung führen können, oft nur sehr schwer zu erkennen. Insbesondere im industriellen Kontext können Systemausfälle, die durch Fehler innerhalb der komplexen drahtlosen Infrastruktur verursacht werden, zu schweren finanziellen Verlusten führen. Eine zeiteffiziente Fehlersuche und vorbeugende Gegenmaßnahmen können nur gewährleistet werden, wenn die drahtlosen Kommunikationsnetze mit Hilfe von Fehlersuchgeräten ständig überwacht werden.

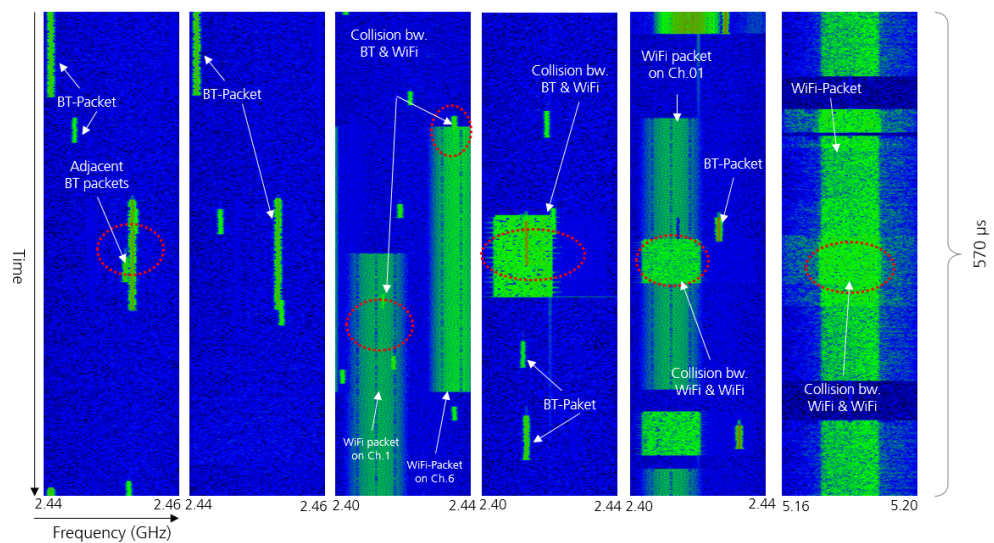
Üblicherweise werden hierfür Funkpakete eines Standards erfasst und dekodiert, sogenanntes sniffing, um so über Protokollanalysen indirekt auf Probleme rückzuschließen. Nicht dekodierbare Pakete und Pakete anderer Funkstandards bleiben bei diesem Verfahren jedoch unberücksichtigt. Einige Anbieter entwickeln Messgeräte, welche die Protokollanalyse mehrerer Funkstandards unterstützen. Erweiterungen um zusätzliche Funkstandards oder Updates bestehender Standards sind jedoch sehr aufwändig und teuer. Weiterhin bieten einige Hersteller Methoden an, welche die Kanalnutzung über sehr einfache spektrale Energiemessung schätzen. Der Informationsgehalt zur Ursachenanalyse ist dabei begrenzt, da keine Rückschlüsse über die tatsächliche Kanalauslastung oder Interferenzen getroffen werden können. Auch der Einsatz von üblichen Messgeräten zur Erfassung des Spektrums ist dadurch limitiert, dass zur Auswertung die Anwesenheit eines Experten erforderlich ist. Dieses Vorgehen ist lediglich eine Stichprobenmessung, da eine lückenlose Speicherung des vollständigen Spektrums über einen längeren Zeitraum die Speicherkapazität sehr schnell erschöpft.

2 Ablauf des Vorhabens

2.1 Konzeption

Diese Arbeit soll einen Beitrag zur Verbesserung von Fehleranalysewerkzeugen für drahtlose Netzwerke leisten. Der grundlegende Ansatz beruht auf einer Erweiterung von Standard-Protokollanalysewerkzeugen durch sensitive Messungen eines Spektrum Analysators. Die herkömmliche Spektralanalyse bietet tiefe Einblicke in die physikalische Schicht und liefert dadurch wichtige Informationen zur Beseitigung von Interferenzen (Koexistenzproblemen) zwischen einzelnen Kommunikationsteilnehmern. Der Vorteil gegenüber der Protokollanalyse besteht hierbei in der Erkennung von Interferenzen sowie Statistiken wie der Kanalauslastung bei gleichzeitiger Unabhängigkeit von vorhandenen Funkstandards. Abbildung 1 zeigt beispielhaft eine Spektrogrammabschnitte häufig Auftretender FUNKSITUATIONEN im lizenzfreien ISM Band.

Abbildung 1 Beispielspektrogramme von Messungen typischer Funkstandards im ISM Band sowie häufig vorkommender Interferenzszenarien



Die Innovation der Projektergebnisse liegt in der vollautomatisierten Analyse des Spektrums, welche die kontinuierliche, lückenlose Langzeiterfassungen ermöglicht, ohne dass die Anwesenheit eines Experten im Falle auftretender Störungen der Zielanwendung erforderlich ist. Hierfür werden sowohl die einzelnen Funkpakete als auch Paketkollisionen im zu analysierenden Funkkanal detektiert und klassifiziert. Anschließend werden Statistiken über die erkannten Funkereignisse berechnet, dargestellt und ausgewertet. So kann das Netzwerkmanagement frühzeitig über aufkommende Störungen informiert werden und eine der folgenden Handlungsempfehlungen zur Lösung vorgeschlagen werden:

- Wechsel auf oder Sperren eines spezifischen Kanals bei kontinuierlichen Störern
- Anpassung der Sendeleistung zur Erhöhung der Robustheit gegenüber weit entfernter Störsender
- Alarmierung des Netzwerkmanagements, im Falle von Überauslastung der Kanalkapazität oder Erkennung von Funkstandards, welche ggf. auf einer lokalen Blacklist geführt sein könnten.

In Kombination mit Informationen aus der Protokollanalyse können einerseits umfangreiche Ursachenanalysen durchgeführt werden, als auch einmalige Merkmale abgeleitet werden, um beispielsweise eine hochsichere Geräteidentifikation zu ermöglichen.

Wie in Abbildung 1 gezeigt, wird bei der Darstellung des erfassten Funkfrequenzspektrums über die Zeit die Energie über Helligkeit oder Farbe kodiert, um es für uns Menschen leicht lesbar darzustellen. In dieser verbreiteten Darstellungsform liegt es nahe, Bildverarbeitungsalgorithmen zur Analyse zu nutzen. Die Entwicklung rein heuristischer Algorithmen hat den Vorteil des schnellen Prototypenentwicklung ohne die Anforderung an eine große Menge gelabelter Trainingsdaten. Dieser Ansatz birgt aber die Nachteile, dass viele Effekte realer Funkausbreitung komplexe Muster in der Erscheinungsform zur Folge haben und die Vielzahl verschiedener Standards und möglicher Konstellationen im Falle von Paketkollisionen das Abfangen von Sonderfällen äußerst komplex werden lassen.

Im Rahmen von SunRISE werden, unter Verwendung eines, auf maschinellem Lernen basierenden, Objekterkennungsalgorithmus einzelne Pakete verschiedener Funktechnologien in Echtzeit erkannt und entsprechend ihres Kommunikationsstandards klassifiziert. Dabei können einzelne Pakete auch im Falle niedriger Signal-Rausch-Verhältnisse und Interferenzen zuverlässig unterschieden werden. Hierfür wurde yolov4¹ verwendet, eine moderne Architektur eines Neuronales Netz, welche sowohl auf Geschwindigkeit als auch Detektionsgenauigkeit optimiert ist. Das Modell wurde von grundauf für den spezifischen Anwendungsfall neu trainiert und erfordert daher eine große Menge an annotierten Daten.

Im Laufe des Projektfortschritts wurde im Gebiet der Spektralanalyse ein ähnlicher Ansatz bekannt², welcher mittels Methoden des maschinellen Lernens Funkpakete klassifiziert. Methodisch unterscheidet sich der Ansatz jedoch dahingehend, dass ein Klassifikation anhand des Zeitsignals vorgenommen wird und der Fokus auf Interferenzerkennung fehlt, insbesondere auch die Detektion von Kollisionen.

Nach einer initialen Machbarkeitsstudie wurde eine simulationsbasierte Methode zur Erzeugung eines umfangreichen Trainingsdatensatzes umgesetzt, das Training, optimierung und evaluation des Detektionsmodells durchgeführt, sowie eine echtzeitfähige Implementation des eigentlichen Messgerätes realisiert. Am Beispiel von WiFi und Bluetooth kann gezeigt werden, dass sowohl Funkpakete und Kollisionen zwischen Paketen mit einer sehr hohen Genauigkeit erkannt werden können.

2.2 Erzeugung der Trainings- und Testdaten

Obwohl ML-basierte Ansätze eine signifikante Verbesserung der Genauigkeit im Vergleich zu heuristischen Ansätzen zeigen, ist die Generierung eines umfangreichen markierten Bilddatensatzes eine Herausforderung. Vor allem bei Machine-Learning-basierten Objekterkennungssystemen ist die Verfügbarkeit von markierten (labeled) Daten von größter Bedeutung. Die Erfassung von Spektrogrammen einer echten drahtlosen Kommunikation in einer abgeschirmten Umgebung wäre eine intuitive Idee. Ein HF-Kanalemulator könnte die erforderliche Vielfalt an unterschiedlichen Umgebungen bieten. Das manuelle Markieren der Positionen von Funkpaketen innerhalb der Bilder ist jedoch zu zeitaufwändig. Die Bestimmung der Zeitstempel und der Dauer der gesendeten Funkpakete ist nicht realisierbar, da der reale Verkehr auf dieser Ebene schwer zu messen und zu reproduzieren ist. Um annotierte Spektrogramme zu erzeugen, wurde in diesem Projekt eine umfangreiche Pipeline zur Datenerweiterung entwickelt.

¹ Bochkovskiy, A., Wang, C. Y., & Liao, H. Y. M. (2020). Yolov4: Optimal speed and accuracy of object detection. *arXiv preprint arXiv:2004.10934*.

² T. J. O'Shea, T. Roy and T. C. Clancy, "Over-the-Air Deep Learning Based Radio Signal Classification," in *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 1, pp. 168-179, Feb. 2018, doi: 10.1109/JSTSP.2018.2797022.

Abbildung 2 Datenflussgraph der emulativen Generierung von Trainingsdaten

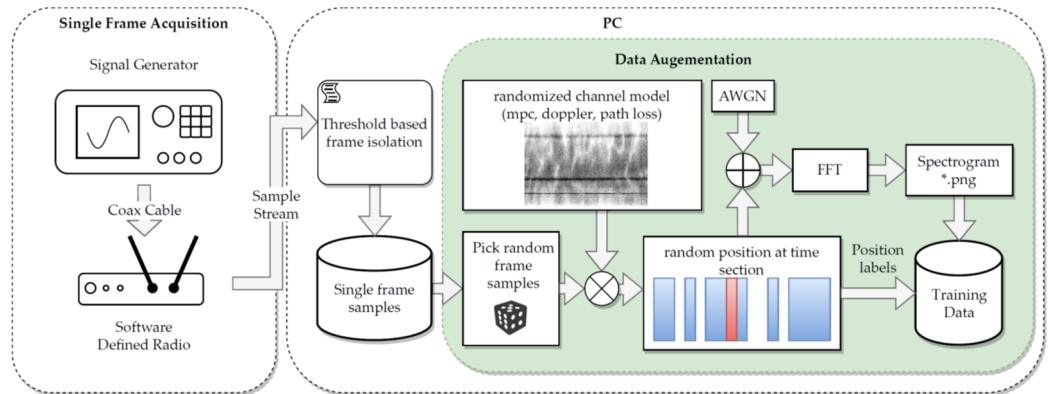
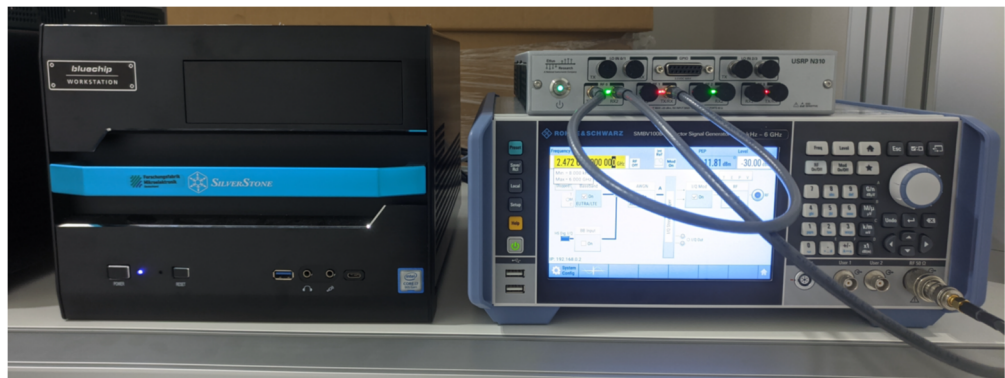


Abbildung 2 ist eine schematische Darstellung der Verarbeitungsschritte zur Erzeugung des Datensatzes, welcher 20.000 Spektrogramme umfasst. Jedes Spektrogramm repräsentiert einen Zeitabschnitt von 4,5 ms und enthält Signale mehrerer WiFi und/oder Bluetooth pakete verschiedenster Konfigurationen wie:

- Standard - verschiedene Ausprägungen von 802.11x (WiFi), Bluetooth classic, Bluetooth Low Energy (BLE)
- Bandbreite
- Mittenfrequenz
- Nutzlast
- Modulationsverfahren
- Randomisiertes Mehrwege-Kanalmodell mit Pfadverlust und Doppler-Effekt
- Signal-Rausch-Verhältnis

Abbildung 3 Hardware Aufbau zur Aufzeichnung der verschiedenen Einzelpakete der Funkstandards. Links: Host-PC mit GPU und 10Gbps Ethernet-Karte; Rechts unten: Vector Signal Generator SMBV100B; rechts oben: Software Defined Radio USRP N320



Die Grundlage für die Verarbeitungspipeline bilden analoge Funk-Signale, welche durch einen Vector Signal Generator automatisiert erzeugt und durch ein Software Defined Radio (SDR) wieder aufgezeichnet werden. Die einzelnen Funkpakete werden anschließend Vereinzelt und auf dem Host-PC abgespeichert. Unter Verwendung der voraufgezeichneten Funkpakete werden diese zufällig, gemäß einer standard spezifischen Richtlinie, angeordnet und anhand eines Kanalmodells modifiziert. Die genaue Position in Zeit und Frequenz jedes Funkpakets wird als Teil des Labels im Bilddatensatz gespeichert. Auf diese Weise ist die genaue Position und Dimension jedes Pakets bekannt, während die Ähnlichkeit der spektralen Darstellungen mit den realen Messungen erhalten bleibt. Außerdem können auf diese Weise Kollisionen zwischen mehreren Funkpaketen erzeugt werden, die in einer realen Umgebung schwer zu erkennen sind. Die Anzahl der Pakete pro Spektrogramm innerhalb des emulierten

Trainingsdatensatzes wurden so gewählt, um möglichst viele der möglichen Paketkonstellationen abzudecken, ohne dass die zuverlässige Unterscheidbarkeit der Einzelpakete leidet.

Abbildung 4 zeigt ein Beispiel Spektrogramms, welches durch die emulative pipeline erzeugt wurde. Das mit 1 Markierte Funkpaket ist ein CCK moduliertes WiFi Paket, Paket 2 ist 2 MHz BLE, Paket 3 OFDM moduliertes WiFi, Paket 4 Bluetooth classic und Paket 5 ist ein WiFi Paket teilweise außerhalb der Erfassungsbandbreite. Der Überlappungsbereich zwischen kollidierenden Paketen wird als Kollision gekennzeichnet und ist in der Unterabbildung b) rot markiert. Es werden Spektrogramme mit 4 verschiedene Erfassungsbandbreiten emuliert, um das Modell unabhängig von der letztlich eingestellten Messbandbreite des Spektrumanalysators zu gestalten.

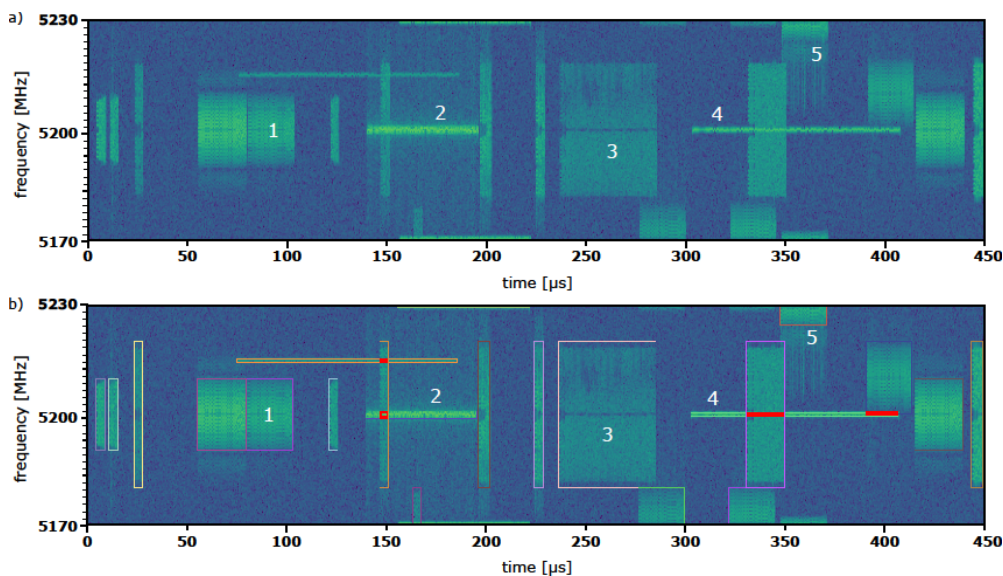


Abbildung 4 Beispiel eines generierten Spektrogramms. Unterabbildung (b) zeigt das gleiche Spektrogramm wie Unterabbildung (a), jedoch mit farbigen Umrandungen zur Veranschaulichung der beschrifteten RF-Frames.

Dieser so erzeugte Datensatz und die detaillierte Beschreibung der Erzeugung wurde der Öffentlichkeit zugänglich gemacht, sodass der Datensatz sowohl für Forschung und Entwicklung als auch die Lehre in Bereichen des Deep-Learnings und der Bilderkennung Anwendung finden und als neuartiges Anwendungsbeispiel dienen kann¹.

2.3 Demonstrator

Anhand des erzeugten Bilddatensatzes wurde ein neuronales Netz zur Objekterkennung trainiert und gemeinsam mit dem generierten Datensatz iterativ optimiert, mit dem Ziel das Verfahren zur Anwendung zu bringen. Das trainierte Modell wurde anhand künstlich erzeugter Testdaten sowie echten Messungen validiert. Die automatisierte Paketdetektion erreicht eine „mean Average Precision“ von über 95 % bei einem festgelegten Intersection over Union (IoU, auch Schnittmenge über Vereinigung genannt) Threshold von 50 % (mAP@50). Die Detektion von Paketkollisionen, weisen eine mAP@50 von rund 60 % auf, wobei die erzeugten Testdaten erhöhte Schwierigkeiten aufweisen was einen Anteil der Paketüberlappungen betrifft. So sind beispielsweise Pakete mit schwacher

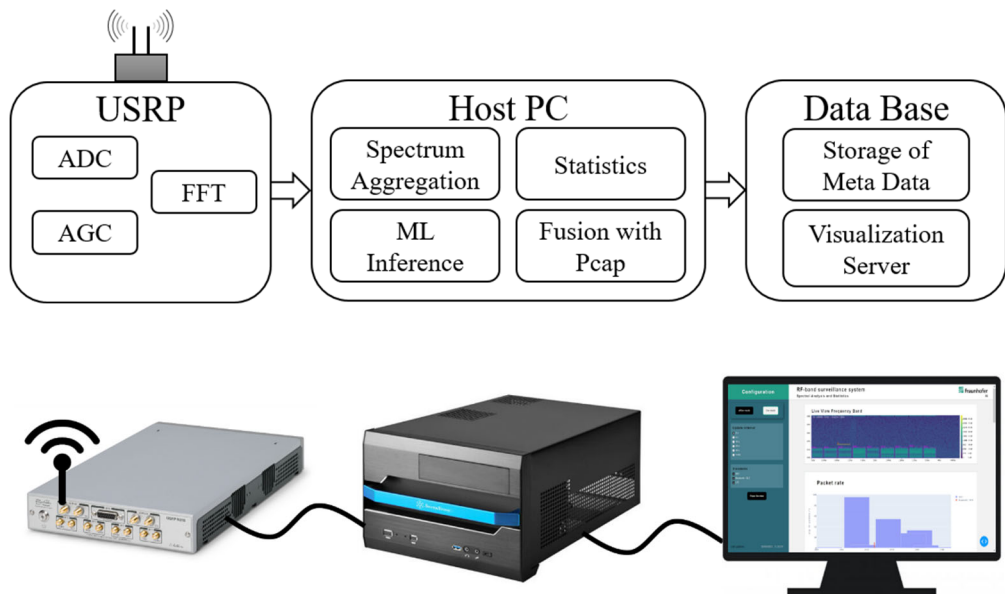
¹ Wicht, J.; Wetzker, U.; Jain, V. Spectrogram Data Set for Deep-Learning-Based RF Frame Detection. *Data* 2022, 7, 168. <https://doi.org/10.3390/data7120168>

Empfangsleistung innerhalb starker Pakete so gut wie unsichtbar, aber ebenfalls annotiert.

Für eine echtzeitfähige, lückenlose und kontinuierliche Erfassung eines beliebigen Messzeitraums darf keine Komponente der Pipeline für die Verarbeitung eines Spektrogramms länger benötigen als den Zeitraum, den das Spektrogramm umfasst. Auch der größte Flaschenhals, die Objekterkennung, muss daher in der Lage sein über 250 Bilder pro Sekunde (bei Signalabschnitten von 4,5 ms mit 0,5 ms Überlappung) auszuwerten. Daher ist es nötig das Seitenverhältnis sowie Auflösung der Spektrogramme derart anzupassen, dass möglichst wenig Bildinformationen durch die Kompression verloren gehen und gleichzeitig die geforderte Bildrate während der Inferenz erfüllt bleibt.

Zum Nachweis der Echtzeitfähigkeit der erforschten Verfahren wurde ein Demonstrator entwickelt, in dem das Verfahren integriert wurde und dessen Ergebnisse in einem Dashboard ansprechend visualisiert werden. Damit können direkt die nutzbringenden Eigenschaften des System gezeigt und anwendungsnah präsentiert werden. Im weiteren Bericht wird dieser Demonstrator als RF-Band Surveillance System bezeichnet. Abbildung 5 zeigt eine Schematische Darstellung der Komponenten des RF-Band Surveillance Systems, welches den entwickelten Spektrumanalysator im Produktivbetrieb repräsentiert.

Abbildung 5 Datenflussdiagramm des entwickelten Gesamtsystems



Die erste Einheit in der Verarbeitungskette ist die Funk Schnittstelle in Form eines SDRs (USRP N310). Dessen Aufgabe ist das Empfangen und Verstärken der analogen Funkwellen und die Konvertierung der Signale in die Digitale Domäne. Auf diese Weise ist die Weiterverarbeitung der Signale durch digitale Rechentechnik möglich und können bei Bedarf abgespeichert werden. Zusätzlich wurden wichtige Signalverarbeitungsschritte in die konfigurierbare Hardware des SDR implementiert. Würden die Abtastraten von bis zu 125 MSps ($\approx 1\text{GB}$ pro Sekunde für ein komplexwertiges 64 bit Datenformat) in Software realisieren werden, wäre eine Gewährleistung der Echtzeitfähigkeit unmöglich. Daher wurde die Transformation des Zeitsignals in den Spektralbereich innerhalb des digitalen Datenpfads im FPGA des SDR integriert. Folgende Funktionsblöcke wurden implementiert:

- Fensterfunktion zur Periodisierung von Signalabschnitten
- Fast-Fourier-Transformation (FFT) zur Überführung von Signalabschnitten in den Frequenzbereich
- Logarithmieren und Betragsbildung der komplexwertigen Spektralbilder
- Übertragung des Spektralbilder an den Host-PC
- Ein separater Datenpfad, welcher jeweils den maximalen Wert innerhalb des Signalabschnitts im Zeitsignal extrahiert und an den Host-PC übergibt, welcher den Eingangsverstärker des Radios optimal aussteuert - Automatic Gain Control (AGC)

Die an den Host-PC übertragenen Spektren werden von einem, im Rahmen des Projektes entwickelten, C++ Programm weiter verarbeitet. Die Architektur des Programms ist multi-threaded und besteht aus mehreren Erzeuger-Verbraucher-Ketten, deren Abarbeitung parallel ausgeführt werden. Die erste Funktion besteht in der Konfiguration und Steuerung des SDR sowie dem Empfang der Spektren. Im Folgenden werden die Einzelspektren aggregiert zu Spektrogrammen in einem Datenformat der Bildverarbeitungsbibliothek OpenCV. Die erzeugten Bilder werden nun an die Paketdetektion übergeben. Zur Inferenz des trainierten neuronalen Netzes zur Paketerkennung innerhalb der Bilder wird ebenfalls eine Funktion der OpenCV Bibliothek genutzt, welche eine sehr performante CUDA Implementierung darstellt und unter Nutzung einer Nvidia Turing GPU echtzeitfähig ist. Anschließend werden aus den berechneten Bounding Boxes essentielle Merkmale zur Beschreibung des detektierten Funkpakets extrahiert. Hierzu gehören Mittenfrequenz, Bandbreite, Start- und Endzeitpunkt, Funkstandard, mittlere Empfangsleistung sowie ob das Paket an einer Kollision beteiligt ist. Diese Metainformationen sind ein vielfaches kompakter als das aufgezeichnete Funksignal. Dies ermöglicht erst die echtzeitfähige Speicherung für eine lückenlose Langzeitüberwachung. Daher werden lediglich die extrahierten Merkmale in einer Elasticsearch Datenbank abgespeichert. Elasticsearch bietet die Möglichkeit einer sehr effizienten Filterung und einfacher statistischer Berechnungen direkt bei der Abfrage der Datenbank.

Abschließend wurde ein Dashboard auf Basis der plotly dash Python Bibliothek entwickelt. Hierzu werden für einen Analysezeitraum die betreffenden Einträge aus der Elasticsearch-Datenbank abgefragt und anschließend folgende Statistiken berechnet:

- Paketrate pro Standard und Mittenfrequenz über die Zeit und der Frequenz
- Kanalauslastung (Duty Cycle) pro Standard und Mittenfrequenz über die Zeit und der Frequenz
- Kollisionsrate pro Standard und Mittenfrequenz über die Zeit und der Frequenz
- Empfangsleistung nach Funkstandard und Häufigkeit über die Frequenz

Die Ergebnisse werden übersichtlich in verschiedenen Graphen visualisiert und liefern auf diese Weise eine abstrahierte Sicht auf den Funkverkehr. Dabei stehen dem Nutzer des Dashboards zwei Grundlegende Modi zur Verfügung, eine live Ansicht für eine Echtzeit Analyse während einer Messung sowie einer Offline Analyse zur detaillierten Analyse eines beliebigen Zeitraums vergangener Messungen.

Abbildung 7 Live Analyse mit Vorschau ausschnittsweiser Spektrogramme samt Markierungen der detektierten Pakete

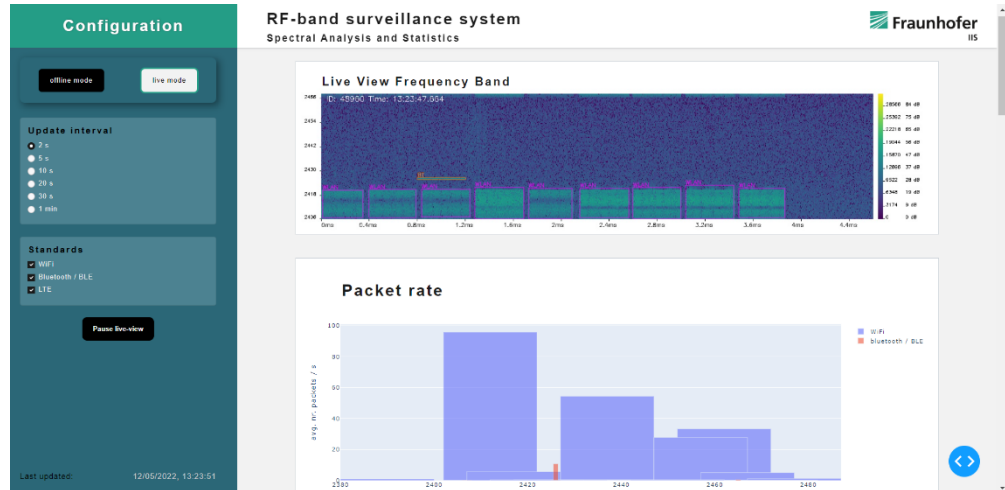
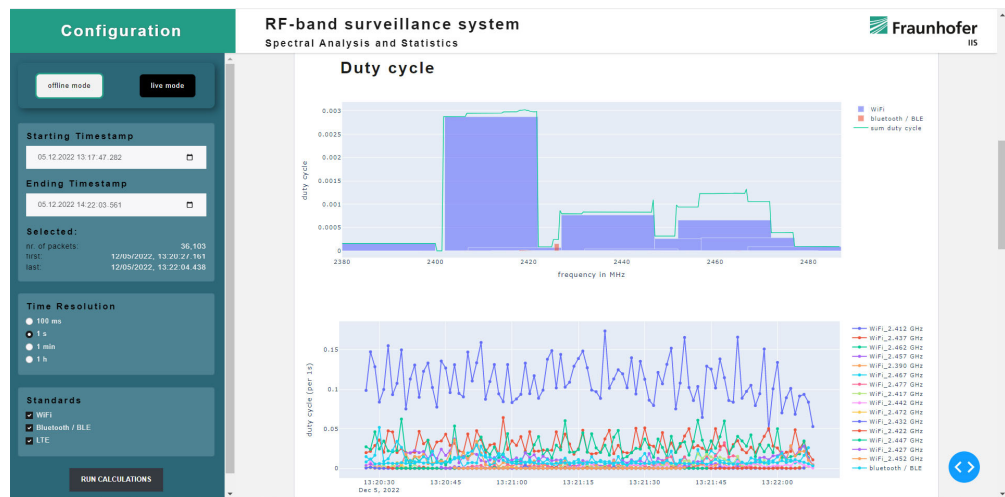


Abbildung 6 Offline Analyse mit definierbaren Analysezeitraum



Das entwickelte Messsystem wurde bereits auf verschiedenen Veranstaltungen vorgestellt. Dabei wurde mithilfe einer mobilen Industrie-WLAN Anwendung und einem WiFi-Jammer typischen Funksituationen nachgestellt und der Vorteil und die Leistungsfähigkeit des entwickelten Systems präsentiert.

2.4 Synchronisation mit der Protokollanalyse

Das RF-Band Surveillance System ist in der Lage aus den als Funkpaket detektierten Bereichen weitere Merkmale zu extrahieren, wie zum Beispiel die out-of-band Energie, welche der Geräteidentifikation dienen können. Für eine erfolgreiches Fingerprinting sind jedoch auch Merkmale aus höheren Ebenen notwendig, wie beispielsweise die MAC-Adresse. Diese sind jedoch nur aus den demodulierten Signalen extrahierbar, welche durch sniffing basierte Protokollanalyse aufwandsarm Verfügbar gemacht werden können. Die Zuordnung der Pakete der Protokollanalyse zu denen der Spektralanalyse ist jedoch nicht trivial. Ungenaue Zeitstempel und zeitlicher Jitter der demodulierten Pakete sowie verschiedene fehlende Pakete in beiden Domänen erfordern einen Ansatz, der die Synchronisierung auf der Grundlage verschiedener Merkmale durchführt, die in beiden Domänen vorhanden sind. Hierfür wurde im

Rahmen des Projekts ein neues, auf Dynamic Time Warping basierendes, Verfahren entwickelt. Es wird „Sliding Adaptive Dynamic Time Warping“ genannt und nutzt eine Mehrstufige Synchronisation basierend auf der Analyse der Dauer und Empfangsstärke der Funkpakete. Diese Merkmale sind hierfür besonders geeignet, da sie in beiden Domänen (Spektraldomäne und Protokollomäne) zuverlässig erfasst werden können.

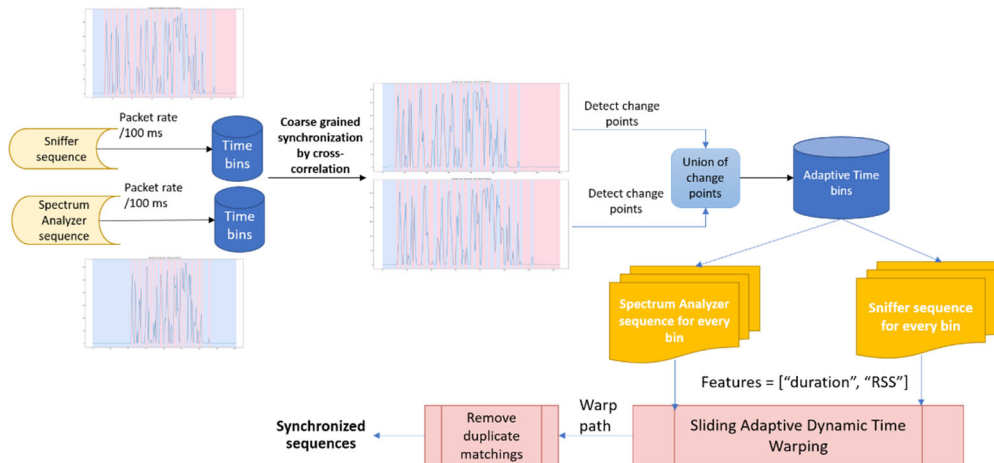


Abbildung 8 Ablaufdiagramm des „Sliding Adaptive Dynamic Time Warping“ Ansatzes

Auf diese Weise können verschiedene Informationen der unterschiedlichen Messdomänen kombiniert und vervollständigt werden. Dies hilft zum einen der Ursachenanalyse während der Funküberwachung und bildet zum anderen die technische Grundlage einer praktikablen Implementierung von RF-Fingerprinting. RF-Fingerprinting liefert eine zusätzliche Verbesserung der Sicherheit im Vergleich zu bestehenden Ansätzen zur Geräteidentifikation, welche üblicherweise lediglich auf Merkmalen der Protokollebene beruhen.

Ein weiterer Ansatz, wie das RF-Band Surveillance System zur Verbesserung der Sicherheit eingesetzt werden kann, ist die Erkennung von grundlegenden Jamming-Angriffen durch die entwickelte Interferenzdetektion. Die automatisierte Klassifikation von komplexeren reaktiven und funktions-spezifischen Jamming-Angriffen stellt das Ziel zukünftiger Entwicklungen dar, welche auf der in SunRISE entstandenen Technologie aufbauen.

2.5 Sonstige Tätigkeiten

Während der Projektlaufzeit wurden 5 studentische Praktika betreut, welche sich mit folgenden Themen beschäftigen:

- Optimierung der Trainingsdatengenerierung sowie finden passender Funkkanalmodelle, um das Erscheinungsbild der Spektrogramme realistischer zu gestalten.
- Test und Optimierung des neuronalen Netzes
- Erweiterung des Trainings- und Testdatensatzes sowie Anlernen des Modells um weitere Funkstandards wie Bluetooth, BLE und LTE
- Untersuchung von „Active Learning“ zur effizienten Modellerweiterung im Falle neuartiger Funkumgebungen oder unbekannter Funkstandards unter Verwendung einer geringen Anzahl manuell annotierter Beispiele. Herausforderung ist die Detektion und Auswahl informationsreicher Beispiele während einer Messung, welche einem menschlichen Nutzer zur Annotation präsentiert werden und die anschließende Feinabstimmung des vortrainierten Modells.

- Dynamic Time Warping basierte Synchronisierung der Spektral- und Protokollanalyse
- Performanz- und Layout-Optimierung des Demonstrator-Dashboards

Weiterhin wurden während der Kollaboration mit dem Europäischen Konsortium drei Hauptanwendungsfälle zum Thema Sicherheit und Datenschutz in verteilten IoT System in den Bereichen Medizintechnik, Smart Metering in Energie Gemeinden sowie Cloud Infrastruktur ausgearbeitet. Insbesondere im Bereich Cloud Infrastruktur gab es eine enge Zusammenarbeit von Fraunhofer mit den Partnern Cloud&Heat, NXP, Universität Ulm und AncudIT mit dem Ziel „Prädiktion der Energieeffizienz von Mikro-Datenzentren“. Diese Rechenzentren sind an die Warmwasserversorgung einzelner Haushalte angeschlossen, deren Wärmebedarf unter Wahrung des Datenschutzes präzisiert werden sollen, um so Energieintensive Rechenaufträge zeitlich anzupassen. In diesem Zusammenhang wurden von Fraunhofer gemeinsam mit dem Inhaber des Anwendungsfalls Datenquellen identifiziert und im Rahmen des Arbeitspakets 3 eine Datenvorverarbeitungskette sowie die Berechnungsvorschrift zur Modellierung des Energiebedarf eines Datacenters anhand von Temperaturmesswerten der Wasserkühlung entwickelt.

Im Rahmen der Leitung des Arbeitspakets 3 im Konsortialprojekt koordinierte das Fraunhofer IIS/EAS eine Reihe von Videokonferenzen zur Erarbeitung von Anforderungen und Verfügbarkeit von Datensätzen in den verschiedenen Hauptanwendungsfällen. Die Teilschritte und Ergebnisse wurden in zwei Deliverables dokumentiert. „D3.1 Partitionierungs Strategie für Datenanalyse Schritte in verteilten IoT Architekturen“ dokumentiert vornehmlich die Datensammlung der Hauptanwendungsfälle sowie dessen Kategorisierung und Definition von Anforderungen an die Datensätze mit Augenmerk auf Datenschutz. Im Rahmen von D3.2 wurden, neben dem Katalog effizienter Merkmalsextraktions- und Datenfusionsmethoden, Diagramme der kritischen Datenflüsse generiert, um so mögliche Leckagen von sensiblen Nutzerdaten aufzudecken und zu vermeiden.

3 Erzielte Ergebnisse

3.1 Wissenschaftliche Dissemination

Die essenziellen im Projekt erzielten Ergebnisse wurden im Rahmen von Open-Access Publikationen der Forschungsgemeinschaft bekannt gemacht. Ebenso wurde der erzeugte Trainingsdatensatz zur Verwendung auf dem Gebiet der fortgeschrittenen ML und DL-Modelle für Bilderkennung und Computer Vision zugänglich gemacht. Folgende Publikationen wurden während der Projektlaufzeit erstellt und sind als Anhang dem Bericht beigefügt:

- European Wireless Konferenzbeitrag 2021: “Deep Learning Based Real-Time Spectrum Analysis for Wireless Networks”¹ – Die Veröffentlichungsrechte liegen bei VDE Verlag, daher ist das Paper kein Teil dieses Berichts
- MDPI Data Journal 2022: “Spectrogram Data Set for Deep-Learning-Based RF Frame Detection”

¹ J. Wicht, U. Wetzker and A. Frotzcher, "Deep Learning Based Real-Time Spectrum Analysis for Wireless Networks," European Wireless 2021; 26th European Wireless Conference, 2021, pp. 1-6.

- European Conference on Wireless Sensor Networks Poster 2022: “Synchronizing Spectral and Protocol Analysis for Complementary Troubleshooting of Wireless Standards”

In naher Zukunft ist eine weitere Publikation des neuartigen Algorithmus zur Synchronisation der Protokoll- und Spektraldomäne als Grundlage von RF-Fingerprinting sowie verbesserter Analysemöglichkeiten bei der Fehlerursachenanalyse von Drahtlosen Netzwerken in IEEE Letters geplant und bereits bearbeitung.

Neben einer Vielzahl studentischer Arbeiten, beschäftigte sich auch eine Post-Doktorantin des ERCIM Austauschprogramms mit dem Sunrise Themenkomplex.

3.2 Voraussichtlicher Nutzen und Verwertbarkeit der Ergebnisse

Neben der wissenschaftlichen Verwertung ist vor allem das im Projekt SunRISE entwickelte RF-band Surveillance System und dessen Demonstrator einer der Hauptergebnisse. Neben der Präsentation der entwickelten Verfahren während Messen und Fachveranstaltungen, bildet das System die Grundlage zur Erweiterung der Angebote des Fraunhofer IIS/EAS an Industriekunden. Die neu geschaffene Möglichkeit der automatisierten Funküberwachung stellt in diesem Detailgrad auf physikalischer Ebene einen deutlichen Mehrwert im Vergleich zu bestehenden Lösungen auf dem Markt dar. Die entwickelte Lösung kann sowohl für temporäre Messdienstleistungen als auch zur permanenten Überwachung und Analyse industrieller Funksysteme eingesetzt werden. Das Fraunhofer IIS/EAS plant dieses Gerät über Lizenzverträge an Troubleshooting-Dienstleister, an Hersteller von Troubleshooting-Tools, als auch an Betreiber von industriellen Funknetzwerken zu verwerthen.

Für einen zukünftigen Verwertungszweig wird eine Integration der entwickelten Verfahren in Standardisierungsvorhaben angestrebt, sowie die weitere Integration der entwickelten Algorithmen des RF-Band Surveillance Systems als IP-Block für neuartige, echtzeitfähige Funktechnologien zur Verfügung zu stellen, um einen zuverlässigen Betrieb der Funksysteme auch in den lizenzfreien Frequenzbändern zu ermöglichen und somit eine weltweite Einsetzbarkeit der Funksysteme zu gewährleisten. Auch eine Integration in ein Mobilfunknetzwerk wie 5G und darüber hinaus ist denkbar. Eine Implementation in einen der Basisknoten eines verteilten Systems bietet hier eine Möglichkeit, durch die erweiterten Monitoringfunktionen bei gleichzeitig maximaler Erfassungsabdeckung, die Kommunikation resilienter zu gestalten und so die Quality-of-Service für den Endanwender zu erhöhen.

Schlussendlich bildet das RF-Surveillance System in Verbindung mit der synchronisierten Protokollanalyse eine elaborierte Grundlange für die konkrete Implementierung einer praktikablen Lösung für ein gerätebasiertes Authentifizierungssystem mit erhöhter Sicherheit unter Nutzung von Merkmalen des RF-Fingerprintings. Dessen Test und anschließende Verwertung weitere Schritte in der Zukunft darstellen.

4 Zahlenmäßiger Nachweis

Die wichtigsten Positionen des zahlenmäßigen Verwendungsnachweises sind die Personalkosten für Wissenschaftler und Hilfwissenschaftler bzw. Ingenieure. In wesentlich geringerem Maße sind Kosten für Reisen (Projekttreffen, Konferenzen) sowie Materialkosten entstanden.

Der detaillierte zahlenmäßige Nachweis erfolgt separat durch die zentrale Verwaltung der Fraunhofer-Gesellschaft.

Abbildungen

Abbildung 1 Beispielspektrogramme von Messungen typischer Funkstandards im ISM Band sowie häufig vorkommender Interferenzszenarien	8
Abbildung 2 Datenflussgraph der emulativen Trainingsdatengenerierung	10
Abbildung 3 Hardware Aufbau zur Aufzeichnung der verschiedenen Einzelpakete der Funkstandards. Links: Host-PC mit GPU und 10Gbps Ethernet-Karte; Rechts unten: Vector Signal Generator SMBV100B; Rechts oben: Software Defined Radio USRP N320.....	10
Abbildung 4 Beispiel eines generierten Spektrogramms. Unterabbildung (b) zeigt das gleiche Spektrogramm wie Unterabbildung (a), jedoch mit farbigen Umrandungen zur Veranschaulichung der beschrifteten RF-Frames.....	11
Abbildung 5 Datenflussdiagramm des entwickelten Gesamtsystems	12
Abbildung 6 Live Analyse mit Vorschau ausschnittsweiser Spektrogramme samt Markierungen der detektierten Pakete	14
Abbildung 7 Offline Analyse mit definierbaren Analysezeitraum	14
Abbildung 8 Ablaufdiagramm des „Sliding Adaptive Dynamic Time Warping“ Ansatzes	15

Impressum

Herausgeber

Fraunhofer-Institut für Integrierte Schaltungen IIS,
Institutsteil Entwicklung Adaptiver Systeme EAS
Münchner Str. 16, 01187 Dresden

Ansprechpartner:
Jakob Wicht
Telefon +49 (0) 351 45691-374
jakob.wicht@eas.iis.fraunhofer.de

Alle Rechte vorbehalten.
Nachdruck nur mit Genehmigung der Redaktion.

© Fraunhofer IIS/EAS, Dresden, Dezember 2022