ITG news
INFORMATIONSTECHNISCHE GESELLSCHAFT IM VDE
01/2020

Liebe ITG-Mitglieder,

für das neue Jahr wünsche ich Ihnen und Ihren Familien viel Glück, Erfolg und Gesundheit.

In diesen ITG-news finden Sie unter anderem Beiträge zu den Themen 5G-Sicherheit, technologische Souveränität und elektromagnetische Exposition – alles Themen, die zurzeit nicht nur Fachleute, sondern auch Öffentlichkeit und Politik beschäftigen und teilweise stark emotionalisieren. Es ist nicht immer einfach, Experten zu finden, die sich zu derart heiklen Themen äußern wollen … es ist aber dringend nötig. Insbesondere die Erreichung klima- und energiepolitischer Ziele wird gut balancierte technische Maßnahmen erfordern und hierbei werden auch ITK-Lösungen eine große Rolle spielen. Mut – auch zu unbequemen Aussagen und Empfehlungen – wird nötig sein, um diese Diskussion sachlich zu führen.

Insbesondere die Erreichung klima- und energiepolitischer Ziele wird gut balancierte technische Maßnahmen erfordern.

Ingenieure entwickeln Technik für Menschen. Das taktile Internet erlaubt hierbei eine engere und echtzeitfähige Interaktion von Mensch und Maschinen und ermöglicht so eine neue Stufe der Mensch-Maschine-Zusammenarbeit. Über einen Workshop des Exzellenzclusters CeTI – Centre for Tactile Internet with Human-in-the-Loop der TU Dresden berichtet Prof. Fitzek.

Im Rahmen des VDE-Hauptstadtforums werden die ITG-Mitglieder geehrt, die sich in besonderer Weise engagiert haben oder Herausragendes in Forschung und Lehre, in Technikentwicklung und deren Umsetzung geleistet haben. So konnten wir auch dieses Jahr in einer kurzweiligen Veranstaltung wieder verdienten Mitgliedern für ihre Leistungen um die Facharbeit oder Konferenzorganisation danken und hervorragende Veröffentlichungen oder Promotionen auszeichnen. Höhepunkt war die Ernennung von vier besonderen Persönlichkeiten zu ITG-Fellows, die

die Informationstechnik in Deutschland mit geprägt haben und uns allen als Vorbild dienen.

Viel Spaß beim Lesen der ITG-news,
Ihr

PROF. DR.-ING. HANS D. SCHOTTEN
ITG-Vorsitzender

ITG-MITGLIEDERVERSAMMLUNG 2020

Einladung zur ITG-Mitgliederversammlung

Die ordentliche Mitgliederversammlung der ITG findet am 26. Februar in Berlin am ersten Tag des VDE Tec Summit 2020 statt. Sie beginnt um ca. 13.15 Uhr (bis ca. 14.30 Uhr) im Workshopraum 1. Alle ITG-Mitglieder sind herzlich hierzu eingeladen. Auf der Tagesordnung stehen folgende Punkte:

- Begrüßung
- Tätigkeitsbericht der ITG für den Zeitraum 2019/2020
- Aussprache über die Tätigkeit der ITG
- Änderung der ITG-Geschäftsordnung
- Bekanntgabe der Preisträger der ITG 2019
- Verschiedenes

Aus organisatorischen Gründen bittet die ITG-Geschäftsführung darum, Fragen bzw. Diskussionspunkte zum Tagesordnungspunkt „Verschiedenes“ bis spätestens **1. Februar 2020** (per Brief oder E-Mail: itg@vde.com) an die ITG-Geschäftsstelle zu senden.
Mehr zum VDE Tec Summit unter:
// tecsummit.vde.com

Inhalt

Meldungen 02
Thema
ITG-Positionspapier 03
5G am Start – Wie geht es weiter? 04
Bericht
Preisverleihung 11
ITG-Preise 12
Termine 12

Bild: TU Dresden

CETI SUMMER SCHOOL 2019

Taktiles Internet mit Mensch-Maschine-Interaktion im Fokus

Das Exzellenzcluster CeTI – Centre for Tactile Internet with Human-in-the-Loop der TU Dresden veranstaltete vom 23. 9. bis zum 27. 9.2019 die CeTI Summer School 2019.

Das Exzellenzcluster CeTI will die Zusammenarbeit zwischen Mensch und Maschine auf eine neue Stufe heben. Menschen sollen künftig in der Lage sein, in Echtzeit mit vernetzten automatisierten Systemen in der realen oder virtuellen Welt zu interagieren. Für dieses Ziel arbeiten im Exzellenzcluster Wissenschaftler der TU Dresden aus den Fachgebieten Elektro- und Kommunikationstechnik, Informatik, Psychologie, Neurowissenschaften und Medizin mit Forschern der TU München, des Deutschen Zentrums für Luft- und Raumfahrt und der Fraunhofer-Gesellschaft sowie internationalen Wissenschaftseinrichtungen zusammen. Interdisziplinär erforschen sie Schlüsselbereiche der menschlichen Kontrolle in der Mensch-Maschine-Kooperation, im Soft- und Hardware-Design, bei Sensor- und Aktuatortechnologien sowie bei Kommunikationsnetzen. Die Forschungen sind Grundlage für neuartige Anwendungen in der Medizin, der Industrie (Industrie 4.0, Co-working) und dem Internet der Fähigkeiten (Bildung, Rehabilitation).

Die CeTI Summer School bot eine Woche lang über 60 internationalen Teilnehmerinnen und Teilnehmern die Möglichkeit, sich mit dem Thema taktiles Internet mit Mensch-Maschine-Interaktion auseinanderzusetzen. Wissenschaftler der Technischen Universität Dresden, der Universität Ulm, der Technischen Universität München, der Universität Tübingen und der Universität Innsbruck gaben Einblicke in ihre Forschungsfelder und stellten neueste Ergebnisse vor. Thematisch standen unter anderem 5G, Netzwerksicherheit und Network Coding, neue Sensor- und Aktuatortechnologien sowie die Mensch-Maschine-Kooperation aus psychologischer und medizinischer Sicht im Fokus. Neben zahlreichen Vorträgen wurde zusätzlich ein Industry Day veranstaltet, bei dem sich Start-ups präsentieren konnten und ein fachlicher Austausch ermöglicht wurde. Die nächste CeTI Summer School wird im nächsten Sommer 2020 stattfinden.

Weitere Informationen finden Sie unter www.ceti.one

PROF. DR.-ING. DR. H.C. FRANK FITZEK
Inhaber des Deutsche Telekom Lehrstuhls für Kommunikationsnetze an der TU Dresden, der zudem das 5G Lab Germany koordiniert. Er ist Sprecher des DFG-Exzellenzclusters CeTI.

ITG-POSITIONSPAPIER

Technologische Souveränität

Das bereits angekündigte Positionspapier der ITG zur „technologischen Souveränität" ist fertiggestellt und wird auf dem VDE Tec Summit 2020 vorgestellt werden. Über ein paar Erkenntnisse möchte die ITG bereits an dieser Stelle berichten.

Die technologische Souveränität hat für den exportorientierten Industriestandort Deutschland eine herausragende Bedeutung. Die Bundeskanzlerin führte diesbezüglich am 11. September 2019 im Deutschen Bundestag als Beispiele für Technologien, in denen wir nur im europäischen Kontext wieder den Anschluss an die Weltspitze erreichen können, u.a. Mikroelektronik, Datenmanagement und -plattformen an.

Im Rahmen der Diskussionen zur „Souveränität" existieren verschiedene Begrifflichkeiten, wie „digitale Souveränität", „Mediensouveränität" und eben auch „technologische Souveränität", die alle etwas unterschiedlich verstanden werden, letztlich aber das gleiche grundsätzliche Ziel adressieren. Wesentliches Merkmal der „Souveränität" ist die Befähigung des Staates zu eigenständigem und unabhängigem Handeln, und dass in der Ausübung des eigenständigen Handelns auch die letzte Entscheidungsgewalt liegt. Die Befähigung zu souveränem Handeln ist gleichermaßen auch für andere Marktakteure, beispielsweise Unternehmen, relevant.

„Technologische Souveränität" ist die Fähigkeit eines Staates oder einer Gesellschaft, politische und gesellschaftliche Prioritäten umsetzen zu können, ohne dabei durch unzureichende oder fehlende Kontrolle über Technologien behindert zu werden. Sie ist von Autarkie einerseits und von Fremdbestimmung andererseits abzugrenzen.

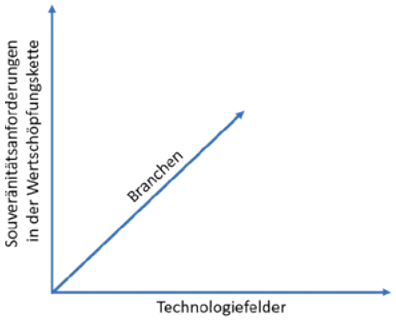
Das Positionspapier befasst sich zunächst damit, wie Technologien strukturiert und bewertbar gemacht werden können. Nicht allen Technologien kommt eine ähnliche Bedeutung für die Gewährleistung einer „technologischen Souveränität" zu. Kriterien sind neben dem volkswirtschaftlichen Nutzen und der Zukunftsfähigkeit unter anderem auch sicherheitspolitische Erwägungen und die gesellschaftliche Akzeptanz. Das Papier strukturiert Technologien in Technologiefelder. Technologiefelder werden verstanden als ein sehr weit gefasstes Umfeld, dessen Aufgabe die Bereitstellung wesentlicher essenzieller Funktionen ist. Es ist durch eine hohe zeitliche Konstanz charakterisiert. Beispiele sind die IKT, Energietechnik, digitale Plattformen und künstliche Intelligenz. Zur Realisierung von Systemen und Funktionen gibt es Technologiesegmente und Schlüsseltechnologien. Beispielsweise gliedert sich das Technologiefeld „IKT" in die Technologiesegmente „Kommunikation", „IT" und „Sicherheit". „5G" wird als Schlüsseltechnologie für die Kommunikation betrachtet. Wir brauchen mehr denn je technische Systeme zur Kommunikation. Die zur Realisierung der Kommunikation eingesetzten (Schlüssel-)Technologien verändern sich über die Zeit sehr deutlich, abhängig von grundlegenden technischen Entwicklungen.

Technologiefelder sind abzugrenzen von Branchen und Anwendungsfeldern, da Technologien in sehr unterschiedlichen Branchen zum Einsatz kommen können. Die Informations- und Kommunikationstechnik (IKT) ist hierfür ein sehr gutes Beispiel. Die IKT ist zugleich ein gutes Beispiel, dass die Betrachtungsperspektive relevant ist, da die IKT nicht nur ein Technologiefeld, sondern auch eine eigene Branche darstellt. Bei der Betrachtungsweise „Technologiefeld" stehen essenzielle technische Funktionen und die zur Realisierung erforderlichen Techniken im Vordergrund.

Die Anforderungen, die für eine souveräne Handlungsfähigkeit formuliert werden, variieren beträchtlich, je nachdem, aus welcher Perspektive man die Souveränität betrachtet: als Hersteller, als Betreiber, aus der Politik oder als Bürger der Gesellschaft. Ausgehend von dieser Beobachtung schlägt das Positionspapier eine Systematik vor, die Anforderungen an die technologische Souveränität entlang einer generalisierten Wertschöpfungskette zu erheben.

Dies erlaubt sehr strukturiert, die zur Erfüllung der Aufgaben innerhalb einer Wertschöpfungsstufe notwendigen Anforderungen zu erfassen. Im Ergebnis zeigt sich, dass der Ausbildung und der Forschung eine ganz zentrale Bedeutung zukommt, damit wir überhaupt in der Lage sind, in späteren Stufen der Wertschöpfung, also in der Produktentwicklung, Produktion und im Betrieb, und damit gerade auch in den Stufen, in denen wirtschaftlicher Wert geschaffen wird, eine technologische Souveränität ins Auge fassen zu können. Ohne Souveränität im Wissen ist keine technologische Souveränität möglich. Das bedeutet vor allem eine frühzeitige Bildung in Schulen, Universitäten und gerade auch in den Ausbildungsberufen. Die Bildung muss auch alle Bürger erreichen. Hierbei geht es nicht nur um gesellschaftliche Akzeptanz der auf der Technologie beruhenden Anwendungen, sondern auch darum, Interesse an einer Ausbildung in diesen

Generalisierte Wertschöpfungskette, entlang der die Anforderungen an die technologische Souveränität definiert wird



„Branche“, „Technologiefeld“ und „Souveränitätsanforderungen in der Wertschöpfungskette“ als Dimensionen eines Koordinatensystems

Technologien zu wecken. Diese Bildung ist die Voraussetzung dafür, die Technologie auch tatsächlich eigenverantwortlich einsetzen zu können. Die Anforderungen an eine technologische Souveränität im Bereich der Forschung beinhalten vor allem die finanzielle Ausstattung der nationalen Forschungsteams in einem Umfang, die eine substanzielle eigenständige Forschung auch möglich macht. Dazu gehört aber auch der Zugang zu uneingeschränkt nutzbarer Software, zu Algorithmen und Daten bzw. Rohstoffen und Komponenten, um relevante Forschung betreiben zu können.

Das Positionspapier setzt die Aspekte „Branche“, „Technologiefeld“ und „Souveränität in der Wertschöpfungskette“ als Dimensionen eines Koordinatensystems zueinander in Beziehung. Dies erlaubt Aussagen abzuleiten, welche Technologien für welche Branchen im Hinblick auf souveränes Handeln tatsächlich relevant sind.

Eine umfassende Analyse aller Technologiefelder und korrespondierender Souveränitätsanforderungen für alle Branchen durchzuführen, sprengt den Rahmen und die Möglichkeiten des Positionspapiers. Das Positionspapier stellt eine Systematik vor, wie eine übergreifende Analyse und Standortbestimmung realisiert werden kann. Anhand von zwei Beispielen, der Schlüsseltechnologie „5G“ und dem Technologiefeld „KI“, wird die Systematik konkret vorgestellt.

Das Positionspapier leitet aus der Analyse eine Reihe konkreter Handlungsempfehlungen ab. Zugleich will das Papier aber auch einen Prozess mit dem Ziel anstoßen, branchenübergreifend zu identifizieren, wo auf nationaler Ebene besondere Anstrengungen zur Erlangung einer technologischen Souveränität erforderlich sind, wobei die konkreten Anforderungen an die „technologische Souveränität“ als Teil des Prozesses ermittelt werden.

DR.-ING. KLAUS ILLGNER-FEHNS
Editor des Positionspapiers, ITG-Vorstandsmitglied

5G AM START – WIE GEHT ES WEITER?

Die Sicherheitsarchitektur von 5G-Mobilfunknetzen

Welche Sicherheitsarchitekturen sind nötig, um 5G-Netze und die darin transportierten Informationen wirksam gegen Cyberangriffe zu schützen? Ein Überblick.

Einführung

5G-Netze werden nicht nur Smartphone-Benutzer mit höheren Datenraten versorgen, sondern sollen neue Anwendungen in zahlreichen Bereichen unterstützen. Viele davon sind kritisch in dem Sinne, dass Menschenleben in Gefahr sind, wenn diese Anwendungen nicht mehr korrekt arbeiten oder ganz ausfallen. Markante Beispiele sind die Steuerung der Energieversorgung oder das autonome Fahren. Damit ist klar, dass der Schutz von 5G-Netzen gegen Cyberangriffe eine hohe Priorität hat. Neben der Verfügbarkeit der Netze muss auch ihre Integrität sowie der Schutz der Informationen, die in solchen Netzen transportiert werden, stets sichergestellt werden.

Mobilfunknetze sind stark standardisiert, sodass Netzelemente und Endgeräte der verschiedensten Hersteller problemlos zusammenspielen können. Diese Standardisierung wird maßgeblich von 3GPP, dem „Third Generation Partnership Project“, vorangetrieben. Die Spezifikationen von 3GPP umfassen auch den Bereich der Netzsicherheit – das dafür maßgebliche Dokument ist die 3GPP Technical Specification 33.501 [1]. Dieser Beitrag gibt eine Übersicht über die 3GPP-Sicherheitsarchitektur gemäß dieser Spezifikation und zeigt auf, welche Erweiterungen und Verbesserungen im Vergleich zur 4. Mobilfunkgeneration (LTE) standardisiert wurden.

Die 3GPP-Sicherheitsarchitektur ist jedoch nur eine der Säulen, auf denen die Sicherheit von 5G-Netzen basieren muss. Bild 1 visualisiert ein Drei-Säulen-Modell, bei dem zwei weitere Säulen wesentliche Bestandteile der 5G-Sicherheitsarchitektur bilden, die an dieser Stelle aber nur kurz angesprochen werden können.

Natürlich muss jedes einzelne Netzelement für sich sicher sein und darf keine Schwachstellen enthalten, die von Angreifern dafür ausgenutzt werden können, das Netzelement lahmzulegen oder für bösartige Zwecke umzufunktionieren. Mit der zunehmenden Virtualisierung von Netzen sind Netzelemente überwiegend sogenannte virtualisierte Netzfunktionen (Virtual Network Functions, VNFs), die auf Telco-Cloud-Plattformen implementiert werden. Deshalb wird die entsprechende Säule nicht als „Netzelement-Sicherheit“, son-

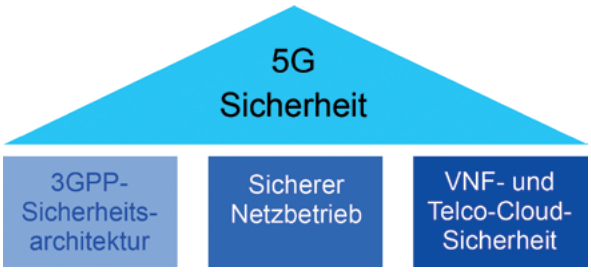


Bild 1: Drei Säulen der 5G-Sicherheitsarchitektur

dern treffender als „VNF- und Telco-Cloud-Sicherheit“ bezeichnet. Neben sicherer Hardware steht dabei insbesondere die Sicherheit der Software im Fokus, was aufgrund ihrer hohen Komplexität eine echte Herausforderung darstellt. Der Bereich der Netzelement-Sicherheit war bislang in der Regel proprietär, d.h. verschiedene Hersteller haben jeweils individuelle Methoden dafür angewendet. In der 4. Mobilfunkgeneration hat 3GPP aber damit begonnen, durch sogenannte Security Assurance Specifications auch diesen Bereich zu adressieren. Außerdem umfasst auch die Standardisierung der Netzvirtualisierung (Network Function Virtualization, NFV) durch die ETSI ISG (Industry Specification Group) Empfehlungen für Sicherheitsmechanismen für Virtualisierungsplattformen und virtualisierte Netzfunktionen.

Die dritte Säule ist der sichere Netzbetrieb. Dies umfasst Netzsicherungsmaßnahmen, wie den Schutz des Netzperimeters durch Firewalls, das Einteilen von Netzen in verschiedene Sicherheitszonen, die Trennung und Isolierung unterschiedlicher Verkehrstypen, die Verwendung sicherer Methoden und Protokolle bei Betrieb und Wartung (Operation and Maintenance, O&M) sowie den Einsatz von dedizierten Sicherheits-Werkzeugen (Security Tools) für die Netzsicherheit. 5G-Netze werden aufgrund der Virtualisierung und der Verwendung von Software Defined Networking (SDN) zunehmend dynamisch sein. Ihre Komplexität wird hoch sein, insbesondere auch durch das Konzept des „Network Slicing“, bei dem mehrere logische Netze auf einer gemeinsamen Infrastruktur implementiert sein können. Um dem Rechnung zu tragen, müssen Security Tools zunehmend automatisiert werden und mit Methoden des maschinellen Lernens und der künstlichen Intelligenz in der Lage sein, sich an wechselnde Netzkonfigurationen und Verkehrsszenarien anzupassen und mögliche Sicherheitsprobleme stets schnell zu erkennen und ggf. autonom zu bekämpfen. Im Bereich des sicheren Netzbetriebs können zahlreiche standardisierte Schnittstellen, Protokolle und Prozeduren zum Einsatz kommen. An einigen Stellen handelt es sich eher um „Best Practices“ (allgemein anerkannte Methoden) als um verbindliche Standards. In seiner Gesamtheit ist der sichere Netzbetrieb nicht standardisiert.

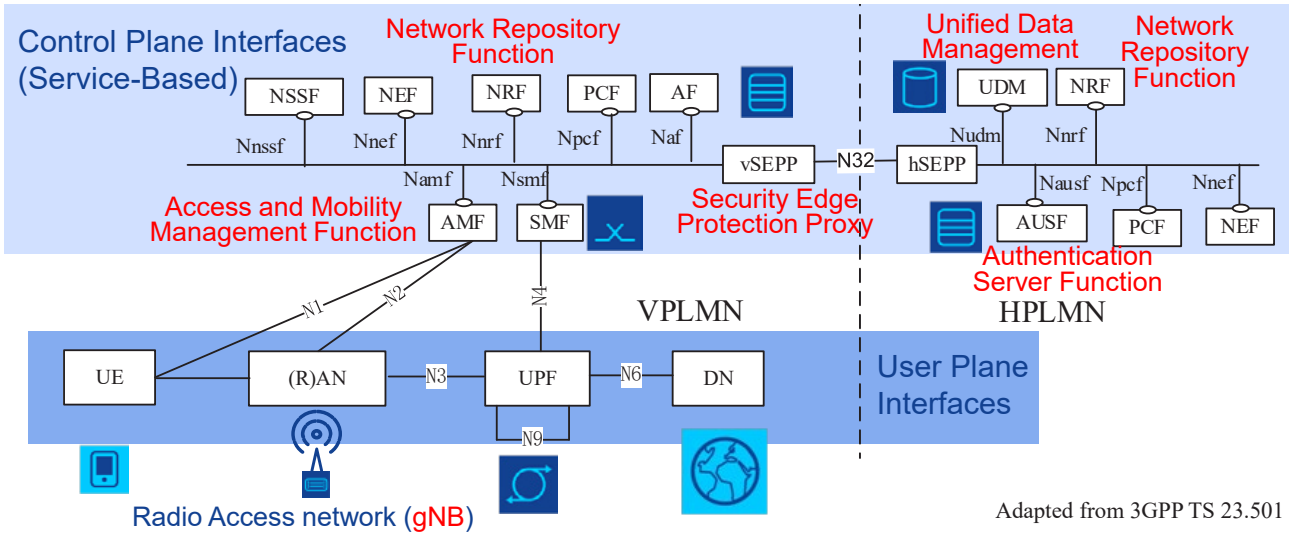
Diese beiden Säulen sind nicht explizit mobilfunkspezifisch, sondern für jede Art von Kommunikationsnetzen relevant. Mobilfunkspezifisch ist hingegen die 3GPP-Sicherheitsarchitektur, die im Folgenden erläutert wird.

Die 5G-Sicherheitsarchitektur gemäß 3GPP

Bild 2 zeigt die 3GPP-5G-Architektur, basierend auf einer Abbildung aus [2]. Sie beinhaltet den Fall des Roamings, d.h. sie unterscheidet zwischen dem „Heimnetz“ (Home Public Land Mobile Network, HPLMN) und dem „Besuchten Netz“ (Visited PLMN, VPLMN). Die Schnittstellen in der Kontrollebene (Control Plane Interfaces) folgen dem Ansatz der sogenannten servicebasierten Architektur (Service-Based Architecture). Dabei bietet jede Netzfunktion (Network Function, NF) eine Reihe von Services, die von anderen NFs aufgerufen werden können. Im Bild sind die Funktionen, die wesentlich für die Sicherheitsarchitektur sind, hervorgehoben und mit ihren (englischen) Langtiteln bezeichnet.

Die Funktion Unified Data Management (UDM) ermöglicht den Zugang zu den Teilnehmerdaten, die insbesondere einen kryptographischen Schlüssel umfassen. Dieser ist auch im Endgerät verfügbar, sicher gespeichert auf der SIM-Karte. Es handelt sich also um einen gemeinsamen Langzeit-Schlüssel (shared key), der die Basis für die gegenseitige Authentisierung zwischen Endgerät und Netz bildet. Natürlich hat jeder Teilnehmer einen individuellen, eindeutigen Schlüssel.

Bei jedem Authentisierungs-Vorgang holt die Authentication Server Function (AUSF) Authentisierungsinformation vom UDM und leitet daraus einen nur für eine Session gülti-



Alle Grafiken: Nokia

Bild 2: Überblick über die 3GPP-5G-Architektur

gen Schlüssel ab, der genutzt werden kann, um Signalisierungsverkehr zwischen einem Endgerät und dem HPLMN so zu sichern, dass auch das VPLMN diesen Verkehr nicht lesen oder unbemerkt modifizieren kann. Außerdem leitet die AUSF aber auch einen weiteren Schlüssel ab, der an das VPLMN weitergegeben wird. Diese im Netz erzeugten Schlüssel werden auch im Endgerät erzeugt, auf Basis des mit dem Netz geteilten Langzeitschlüssels und einer vom Netz gewählten Zufallszahl. Auf diese Weise muss nur diese Zufallszahl, niemals aber ein Schlüssel über die Funkschnittstelle übergeben werden.

Die Access and Mobility Management Function (AMF) wickelt den Teil der Authentisierungsprozedur ab, der im VPLMN stattfindet. Basierend auf dem vom HPLMN erhaltenen Schlüssel wird eine sichere Verbindung zwischen dem Endgerät und der AMF aufgebaut, über die der Signalisierungsverkehr transportiert werden kann.

Der Signalisierungsverkehr (d.h. der Verkehr in der Kontrollebene) zwischen zwei PLMNs wird mittels einer in 5G neu eingeführten Netzfunktion abgewickelt, dem sogenannten Security Edge Protection Proxy (SEPP). Wie der Name andeutet, schützt der SEPP ein PLMN an der Stelle, wo es mit anderen PLMNs verbunden ist, typischerweise über ein sogenanntes IPX, ein internetprotokollbasiertes „Exchange Network". Der gesamte Signalisierungsverkehr zwischen zwei PLMNs läuft immer über die SEPPs in beiden Netzen. Wenn also in der oben beschriebenen Authentisierungsprozedur die AMF im VPLMN einen Service der AUSF im HPLMN aufruft, sendet sie den Aufruf zum SEPP im eigenen Netz (vSEPP in Bild 2). Dieser leitet ihn weiter zum SEPP im HPLMN (hSEPP), und der hSEPP sendet ihn zur AUSF.

Zwischen den SEPPs werden Sicherheitsmechanismen benutzt, die es erlauben, selektiv einen Teil der Signalisierungsinformation zu verschlüsseln, andere Teile dagegen im Klartext zu belassen. Dies ermöglicht es Knoten im IPX, das Routing des Verkehrs basierend auf dieser unverschlüsselten Information vorzunehmen. Dies wiederum ermöglicht Geschäftsmodelle, bei denen Roaming-Agreements nicht notwendig paarweise zwischen je zwei PLMNs geschlossen werden müssen, sondern bei denen ein „Broker" im IPX Roaming-Dienste zu einer ganzen Gruppe von PLMNs anbieten kann. Natürlich ist die gesamte Signalisierungsinformation stets gegen Modifikation geschützt (Integrity Protection). Es kann aber notwendig sein, dass Zwischenknoten im IPX Signalisierungsinformation nicht nur lesen, sondern sogar zusätzliche Information hinzufügen müssen. Dazu gibt es ein sicheres Verfahren, bei dem der SEPP auf der Empfangsseite prüfen kann, dass die hinzugefügte Information nur von dafür autorisierten Zwischenknoten stammt. Durch diese in 5G neu eingeführten Mechanismen wird die Sicherheit im IPX also sehr viel flexibler und unterstützt gängige Geschäftsmodelle bzw. die daraus resultierenden operativen Anforderungen im IPX.

In der servicebasierten Architektur gibt es eine neue, zentrale Funktion, die Network Repository Function (NRF). Sie bietet für andere Netzfunktionen, oder genauer gesagt, Instanzen von Netzfunktionen, die Möglichkeit, sich einerseits zu registrieren, andererseits aber auch Informationen über andere registrierte Netzfunktionen zu erhalten. Außerdem kann die NRF als Autorisierungs-Server eingesetzt werden, d.h. sie entscheidet, welche Aufrufe zwischen zwei Netzfunktionen erlaubt sind. 3GPP hat dafür die Nutzung des OAuth-Verfahrens gemäß [3] spezifiziert. Nach diesem Verfahren muss eine „Consumer"-NF, d.h. eine NF, die einen Service einer anderen NF (genannt „Producer"-NF) nutzen möchte, sich dafür von der NRF autorisieren lassen. Die NRF prüft dabei, ob ein gewünschter Service-Aufruf gemäß der dafür konfigurierten Regeln zulässig ist, und liefert ggf. ein Autorisierungs-Token an die Consumer-NF. Diese übergibt das Token beim Service-Aufruf an die Producer-NF. Diese prüft, ob es sich um ein gültiges Autorisierungs-Token handelt, und beantwortet nur in diesem Fall den Service-Aufruf.

Dieser Autorisierungs-Mechanismus muss gemäß Standard von den NFs unterstützt werden – er muss aber nicht notwendigerweise immer angewendet werden. Beispielsweise könnte sich ein Netzbetreiber dafür entscheiden, ihn nur für Service-Aufrufe aus anderen PLMNs zu nutzen, nicht aber für interne Service-Aufrufe im eigenen PLMN. Durch den Autorisierungs-Mechanismus wird die NRF zur zentralen Instanz für die Speicherung und Durchsetzung aller Regeln, mit denen ein Betreiber die Kommunikation zwischen Netzfunktionen kontrollieren kann, und damit ein zentrales Element der Sicherheitsarchitektur.

Auch die 5G-Basisstation, der sogenannte gNB, hat eine wichtige Funktion in der Sicherheitsarchitektur. Der gNB behandelt die Sicherheitsmechanismen für die Funkschnittstelle. Dies umfasst den kryptografischen Schutz des Signalisierungsverkehrs und des Endnutzerverkehrs zwischen dem Endgerät und dem gNB. Dieser Schutz basiert auf einem Schlüssel, der individuell für den gNB und für die aktuelle Session im Netz und im Endgerät erzeugt wird und beispielsweise bei jedem Handover zu einem anderen gNB geändert wird. In der Kontrollebene gibt es damit stets zwei verschiedene sichere Verbindungen, die zwischen dem Endgerät und dem gNB und die oben erwähnte zwischen dem Endgerät und der AMF. Aller Verkehr zwischen dem gNB und dem Core-Netz, bestehend aus allen Funktionen der Kontrollebene gemäß Bild 2 sowie der User Plane Function (UPF), wird außerdem durch einen IPsec-Tunnel geschützt [4].

Die meisten hier beschriebenen Sicherheitsmechanismen betreffen den Schutz des Signalisierungsverkehrs sowie den Schutz des Endnutzerverkehrs zwischen Endgerät und Core-Netz. Endnutzerverkehr kann natürlich auch innerhalb des Core-Netzes sowie zwischen unterschiedlichen PLMNs geschützt werden. Hierfür bieten sich die bekannten VPN-Techniken (Virtual Private Network) an, beispielsweise mittels IPsec-Tunnel. Diesen Bereich hat 3GPP in der aktuellen Version des Standards (Release 15) jedoch nicht explizit adressiert. Jedoch sollten sensitive Anwendungen generell einen Ende-zu-Ende-Schutz verwenden, der die Kommunikation auch über unterschiedliche Netze hinweg sichert (also z.B. Wi-Fi-Netze, das Mobilfunknetz und das allgemeine In-

4G (LTE) Security	5G Security
Für die Authentisierung zwischen Endgerät und Netz gibt es zwei verschiedene Verfahren, eines für den Zugang über Mobilfunk und eines für andere Zugangsnetze, z. B. Wi-Fi.	Zwei verschiedene Authentisierungsverfahren sind spezifiziert, die beide unabhängig vom Zugangsnetz eingesetzt werden können. Eines der beiden ist zudem erweiterbar, sodass zusätzliche Authentisierungsmethoden zukünftig leicht ergänzt werden können.
Ein VPLMN kann in betrügerischer Absicht Authentisierungsinfo für ein Endgerät des HPLMN erhalten, auch wenn das Endgerät sich gar nicht im VPLMN registrieren will. Diese sensible Information kann von einem betrügerischen VPLMN missbraucht werden.	Verbesserte Kontrolle durch das HPLMN bei Roaming: Wenn ein VPLMN ein Endgerät autorisiert, erhält das HPLMN einen vom Endgerät erzeugten kryptografischen Beweis dafür, dass das Endgerät sich tatsächlich registrieren will.
Die Identität eines Teilnehmers wird in manchen (seltenen) Situationen im Klartext über die Funkschnittstelle übertragen. Ein Angreifer kann mit einer gefälschten Basisstation eine solche Situation vorspiegeln und somit die Identitäten aller Teilnehmer in einem lokalen Bereich feststellen. Der Angriff ist bekannt unter dem Begriff „IMSI-Catching“.	Die Teilnehmeridentität muss niemals im Klartext über die Funkschnittstelle übertragen werden. Es ist ein Verfahren definiert, bei dem die Identität mit einem öffentlichen Schlüssel des HPLMN verschlüsselt wird und somit nur vom HPLMN entschlüsselbar ist.
Der Endnutzerverkehr ist über die Funkschnittstelle verschlüsselt, aber nicht zusätzlich gegen Modifikation geschützt. Das erlaubt trotz Verschlüsselung bestimmte Angriffe, bei denen unter geeigneten Voraussetzungen gezielte Veränderungen des Verkehrs möglich sein können.	Integritätsschutz für den Endnutzerverkehr über die Funkschnittstelle ist spezifiziert. Das Verfahren muss von Endgeräten und Netzen unterstützt werden, allerdings nicht für beliebig hohe Bandbreiten. Der Einsatz des Verfahrens ist optional.
Wenn ein Endgerät über das Mobilfunknetz auf ein anderes Netz, genannt Data Network, zugreifen will, gibt es die Möglichkeit, nach einem starren Schema minimale Authentisierungsinformation zwischen dem Endgerät und dem Data Network zu transportieren.	Das neue Konzept der „secondary authentication“ bietet einen flexiblen Rahmen, um beliebige Authentisierungsinformation zwischen Endgeräten und Data Networks zu transportieren, und erlaubt es so, starke Authentisierungsmethoden für den Zugang zu Data Networks zu implementieren.
Signalisierung im Core-Netz erfolgt mit dem Diameter-Protokoll. Dieses kann mit IPsec gesichert werden, wird aber häufig ohne Sicherung eingesetzt.	Die servicebasierten Schnittstellen nutzen als Protokoll HTTP/2 mit Transport Layer Security (TLS). Außerdem ist OAuth als Autorisierungskonzept für Service-Aufrufe zwischen Netzfunktionen spezifiziert.
Für den Kontrollverkehr zwischen verschiedenen PLMNs ist die Nutzung von direkten IPsec-Verbindungen zwischen PLMNs spezifiziert. Das steht in Konflikt mit üblichen Roaming-Geschäftsmodellen, sodass in vielen Fällen auf diesen Schutz verzichtet wird.	Die neue Funktion SEPP (Security Edge Protection Proxy) schützt PLMNs an der Grenze zum IPX-Netz und bietet flexiblen Schutz für den Signalisierungsverkehr zwischen PLMNs. Sensible Information kann Ende-zu-Ende geschützt werden, während andere Information für bestimmte Knoten im IPX-Netz sichtbar bleiben kann, um beispielsweise flexibles Routing von Nachrichten zu ermöglichen.

Tabelle: Vergleich der Sicherheitsfunktionen von 4G (LTE) und 5G

ternet). Typisch ist hier die Verwendung von TLS [5], z. B. zwischen einer Online-Banking-App und dem entsprechenden Online-Banking-Server.

Die hier nur grob skizzierten Sicherheitsmechanismen wurden von 3GPP im Detail spezifiziert. Das dafür maßgebliche Dokument ist [1].

Verbesserungen in 5G im Vergleich zu LTE

5G stützt sich prinzipiell auf die bewährten Sicherheitskonzepte von 4G, bietet aber einige signifikante Erweiterungen und Verbesserungen. In der Tabelle sind diese Erweiterungen zusammengefasst und dem Stand bei LTE gegenübergestellt.

Zusammenfassung

3GPP hat für die 5. Mobilfunkgeneration signifikante Verbesserungen und Erweiterungen der Sicherheitsarchitektur spezifiziert. Basis sind die erprobten Konzepte aus der 4. Generation; Erweiterungen finden sich vor allem im Bereich der Authentisierungsmethoden, dem Schutz der Teilnehmeridentität, dem Schutz der Kommunikation zwischen verschiedenen Mobilfunknetzen über ein IPX-Netz sowie der Einführung eines Autorisierungskonzepts für Service-Aufrufe zwischen verschiedenen Netzfunktionen eines oder verschiedener Mobilfunknetze. Die 3GPP-Sicherheitsarchitektur stellt eine wesentliche Säule für die Sicherheit von 5G-Netzen dar. Ein gesamtheitlicher Ansatz muss daneben aber auch andere Bereiche abdecken, insbesondere die Sicherheit von virtualisierten Netzfunktionen und den zugrunde liegenden Cloud-Plattformen sowie den sicheren Netzbetrieb mit dem Einsatz automatisierter Methoden zur Erkennung und Bekämpfung von Angriffen.

Referenzen

[1] 3GPP TS 33.501 Security Architecture and Procedures for 5G System

[2] 3GPP TS 23.501 System Architecture for the 5G System. www.3gpp.org

[3] IETF RFC 6749 The OAuth 2.0 Authorization Framework

[4] IETF RFC 4301 Security Architecture for the Internet Protocol

[5] IETF RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3

PETER SCHNEIDER
Sprecher der ITG-FG 5.2.2 Network Security, Senior Specialist Network Security Nokia Bell Labs

JOSEF URBAN
Technology Lead in Corporate CTO Nokia Bell Labs

5G AM START – WIE GEHT ES WEITER?

Konzepte für zuverlässige Immissionsmessungen an 5G-Basisstationen mit massivem MIMO

Welche immissionsrelevanten Unterschiede gilt es zwischen Basisstationsantennen für bisherige Standards und 5G-Antennen mit massivem MIMO zu beachten und welche Herausforderungen sind damit verbunden?

Abstract

Basisstationen für den Mobilfunkstandard 5G unterliegen nationalen Zertifizierungsverfahren und müssen Grenzwerte zum Schutz des Menschen in hochfrequenten elektromagnetischen Feldern einhalten. Aufgrund der gegenüber bisherigen Mobilfunkstandards modifizierten Signalstruktur in Zeit- und Frequenzbereich und der Ausnutzung des räumlichen Bereichs durch Strahlformungs-Antennen sind messtechnische und rechnerischeImmissionsbewertungsverfahren für konventionelle 2G/3G/4G-Mobilfunksysteme mit statischen Versorgungsbereichen für 5G-Basisstationen mit massivem MIMO nicht mehr anwendbar. Vorliegender Beitrag beschreibt die wichtigsten immissionsrelevanten Unterschiede zwischen Basisstationsantennen für bisherige Standards und 5G-Antennen mit massivem MIMO und leitet Herausforderungen sowie erste Konzepte für korrekte Immissionsmessungen ab.

Einführung und Motivation

Das im Aufbau befindliche 5G-Mobilfunknetz erfordert geeignete Immissionsbewertungsverfahren zur Erstellung von Standortbescheinigungen, zur Überprüfung der Einhaltung von Immissionsgrenzwerten und zur Ermittlung der Immission in öffentlich zugänglichen Bereichen. Gemäß den deutschen Bestimmungen ist dabei die Immission bei maximal möglicher Anlagenauslastung maßgeblich [1]. Messverfahren für konventionelle 2G/3G/4G-Mobilfunksysteme können für 5G-Basisstationen nicht mehr angewendet werden, da das bisher abgestrahlte, zeitlich konstante Antennendiagramm in dynamische Einzelstrahlungsrichtungen (beams) für Signalisierungsdaten (broadcast beams) und Verkehrsdaten (traffic beams) aufgeteilt wird. Darüber hinaus sind zellenspezifische Referenzsignale, die als Grundlage für eine Immissionsextrapolation auf die maximale Verkehrsauslastung in 4G-Systemen dienten, in 5G nicht mehr verfügbar. Insofern ergeben sich folgende Fragen im Hinblick auf die Entwicklung eines geeigneten Messverfahrens:

1. Welche Strahl-Konfiguration erzeugt die höchste Immission an einem bestimmten Messpunkt?
2. Wie geht man mit dem Thema dynamischer Strahlschwenkung und der räumlichen Trennung von Signalisierungs- und Verkehrsdaten (broadcast und traffic beams) um?
3. Welche verkehrslastunabhängigen Signale stehen für die Hochrechnung auf die maximale Auslastung der Station zur Verfügung?

Diese Fragen werden in den folgenden Abschnitten behandelt.

„Worst Case"-Konfiguration

Bei 2G/3G/4G-Basisstationen sind Signalisierung und Daten in einem Strahl (beam) konzentriert, dessen Abstrahlverhalten sich zeitlich nicht ändert. Bei 5G-Basisstationen mit massivem MIMO hingegen wird das Antennendiagramm in Signalisierungs- und Verkehrsdaten unterteilt (broadcast beams und traffic beams). Der broadcast beam sendet Steuersignale und wird entweder zyklisch durch mehrere Ausrichtungen geschaltet oder ist statisch. Die traffic beams werden dynamisch auf die Endgeräte ausgerichtet, wobei je nach Anzahl der Nutzer mehrere räumlich getrennte beams gebildet werden können.

Der Gewinn und die pro traffic beam übertragene Leistung nehmen mit der Anzahl der gleichzeitig gesendeten beams ab. Daher wird die maximale Immission an einem definierten Messpunkt dann erzeugt, wenn nur ein einziger traffic beam mit maximalem Gewinn und maximaler Sendeleistung ausgebildet wird. Im Regelbetrieb kann die Basisstation jedoch nicht angewiesen werden, für den Zeitpunkt der Messung einen einzigen definierten traffic beam zum Messpunkt zu formen. Daher müssen andere Methoden entwickelt werden, die diesen Zustand nachbilden. Diese werden im nächsten Abschnitt beschrieben.

Broadcast und traffic beams

Zur Lösung der Problematik, dass ein traffic beam während der Messung nicht definiert zum Messpunkt ausgerichtet werden kann, wurde folgendes Messkonzept entwickelt:

- In einem ersten Schritt wird die Immission durch verkehrslastunabhängige Signale im broadcast beam gemessen. Diese Steuersignale können auch ohne Anwesenheit von

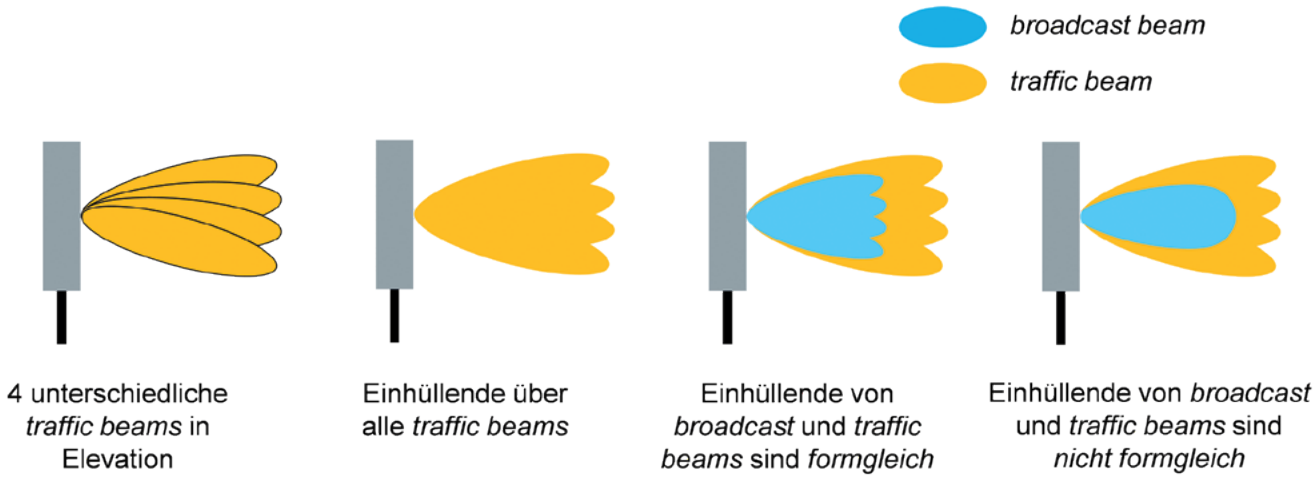


Bild 1: Formgleichheit bzw. Nicht-Formgleichheit der Einhüllenden von broadcast beams und traffic beams

Endgeräten an jeder Stelle der Zelle empfangen werden, da sie zur Anmeldung neuer Endgeräte in der Zelle benötigt werden.

- Die maximal mögliche Gesamtimmission wird aus der gemessenen Immission durch die broadcast-beam-Signale extrapoliert, wobei sowohl die Differenz zwischen der gesamten Signalbandbreite und der Bandbreite der gemessenen verkehrslastunabhängigen Signale als auch die Gewinndifferenz zwischen broadcast beam und traffic beam berücksichtigt werden; Letztere kann bis zu 10 dB betragen. Damit wird die Ausrichtung eines traffic beams mit maximaler Sendeleistung und Gewinn auf den Messpunkt emuliert.

Dieses Hochrechnungsverfahren setzt gemäß Bild 1 jedoch voraus, dass die Einhüllenden von broadcast beam und traffic beam formgleich sind. Ob diese Bedingung immer erfüllt ist, wird im Folgenden untersucht.

Um dieses Extrapolationsverfahren zu testen, wurden Messungen an einem 4G-System mit massiver MIMO-Funktionalität durchgeführt. Eine 4G-Anlage wurde deswegen ausgewählt, um die Komplexität der Strahlformung von der einer noch nicht verfügbaren codeselektiven Messmethode der Steuersignale (5G-Signalstruktur) zu trennen. Für 4G existiert ein etabliertes codeselektives Messverfahren, das die Immission anhand von zellenspezifischen Referenzsignalen (CRS) bestimmt [2]. Die Ergebnisse der extrapolierten CRS-basierten Immissionsmessung wurden durch parallele spektrale Breitbandmessungen bei maximaler Verkehrslast der Basisstation verifiziert. Die Verkehrslast wurde durch ein softwaremodifiziertes Smartphone erzwungen, das über eine App einen FTP-Download initiierte und einen traffic beam auf den Messpunkt ausrichtete. Als Messgerät wurde das selektive Strahlungsmessgerät SRM-3006 von Narda in den Modi LTE-TDD (codeselektive Messung) und Level Recorder (spektrale Breitbandmessung) eingesetzt.

Die Ergebnisse, die im ausführlichen Beitrag im Detail vorgestellt und diskutiert werden, zeigen Differenzen zwischen der spektralen Verifikationsmessung und der codeselektiven Messung mit Extrapolation zwischen −1,0 dB und +33,2 dB. An sechs von 15 Messpunkten lag die Differenz in einem Bereich von ≤ 3 dB und an weiteren zwei Messpunkten in einem Bereich von ≤ 6 dB. Eine umfangreiche Analyse ergab, dass die beste Übereinstimmung beider Messmethoden an den Messpunkten innerhalb der Abdeckungsbereiche von sowohl broadcast beam als auch traffic beam, definiert durch die Halbwertsbreiten der jeweiligen Einhüllenden, erreicht wird. Messpunkte außerhalb des broadcast beams, aber innerhalb des traffic beams zeigten hingegen große Abweichungen in Form einer Unterschätzung. Die naheliegende Annahme, dass die Einhüllenden beider beams nicht formgleich waren, wurde durch eine rechnerische Analyse der Versorgungsgebiete bestätigt.

Verkehrsunabhängige Signale in 5G

Da 5G keine zellenspezifischen Referenzsignale mehr verwendet, könnte der zellen- und beam-spezifische SS/PBCH-Block (synchronization signal and physical broadcast channel block, SSB [3]) alternativ als verkehrslastunabhängiges Signal für Immissionsmessungen verwendet werden. Der SSB umfasst 240 Unterträger, die bei 30 kHz Trägerabstand einer Bandbreite von 7,2 MHz entsprechen und als Teil des SSB-Bursts übertragen werden, wobei jeder SSB einer anderen Strahlrichtung entspricht, wie in Bild 2 illustriert.

Erste Messungen an realen MIMO-5G-Systemen zeigen, dass der SSB durch Spektralmessungen leicht identifiziert werden kann, wenn die Verkehrsauslastung der Basisstation gering ist. Bei einer künstlich erzeugten Verkehrslast werden die SSB-Emissionen jedoch durch den Verkehr überdeckt, was zum Teil auf die Gewinndifferenz zwischen traffic beam und broadcast beam zurückzuführen ist. Eine Lösung können hier codeselektive Messungen darstellen, die aber derzeit für einschlägige Immissionsmessgeräte noch nicht verfügbar sind.

Schlussfolgerungen und Ausblick

Bisherige Berechnungs- und Messansätze zur Bestimmung der hochfrequenten Immission gegenüber 2G/3G/4G-Basisstationen sind für 5G nicht mehr ohne Weiteres anwendbar.

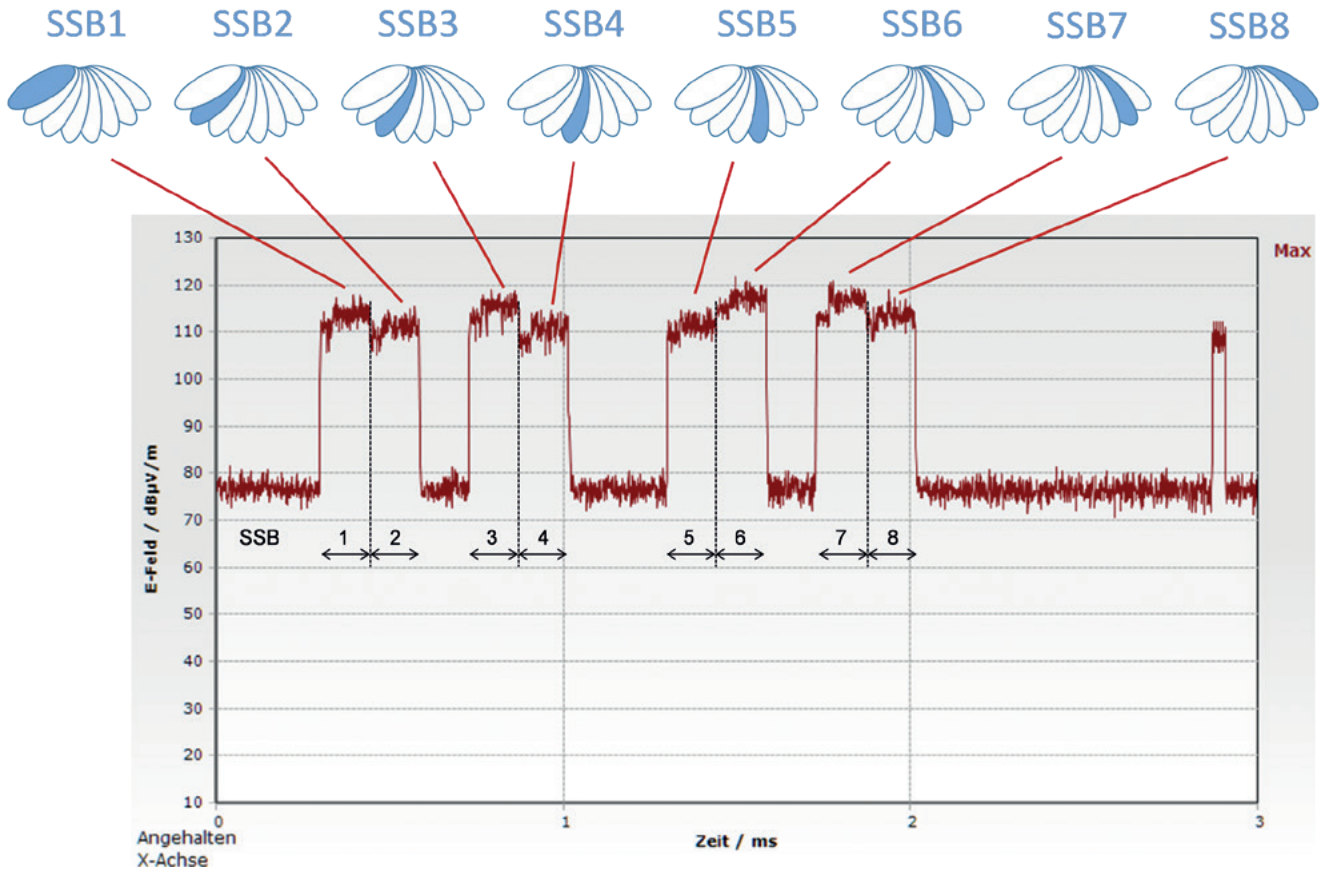


Bild 2: Zeitbereichsmessung eines aus acht SSB bestehenden SSB-Bursts

Da die Erweiterung vieler Standorte mit 5G hinsichtlich der Immissionsvorschriften an ihre Grenzen stößt, sind solche akzeptierten Verfahren jedoch dringend erforderlich. Geeignete Messverfahren können beispielsweise auf der Erfassung der Immission des im broadcast beam übertragenen SSB und der anschließenden Extrapolation auf den traffic beam basieren. Die Grundlage der Extrapolation, d. h. die Gewinndifferenz zwischen den beiden beams, hängt von der Position des Messpunkts in Bezug auf diese ab. Das Messverfahren liefert daher nur für Messpunkte im Abdeckungsbereich beider beams zuverlässige Ergebnisse.

Trotz des vielversprechenden Konzepts bleiben zahlreiche Fragen zu beantworten, bevor ein reproduzierbares und akzeptiertes Messverfahren definiert werden kann. Bei der Entwicklung neuer Funktechnologien ist es dringend erforderlich, eine Möglichkeit zur Bewertung der Immission zu implementieren, z. B. durch geeignete Testmodi.

Abschluss

Der aktuelle Beitrag widmet sich den bislang noch nicht adäquat gelösten Herausforderungen bei der Entwicklung eines Immissionsmessverfahrens für 5G-Basisstationen mit massivem MIMO. Der vorgestellte Lösungsweg basiert auf einer Erfassung der SSB-Immissionen im broadcast beam und anschließender Extrapolation auf maximale Anlagenauslastung.

Referenzen

[1] 26. Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (26. BImSchV). Verordnung über elektromagnetische Felder in der Fassung der Bekanntmachung vom 14. August 2013 (BGBl. I S. 3266)

[2] Bornkessel, C.; Hein, M.; Wuschek, M.: Measurement of human exposure to LTE base stations present status and future challenges in measurement methodology. 2015 European Microwave Conference (EuMC), Paris, 2015, S. 881–884. doi: 10.1109/EuMC.2015.7345905

[3] 3GPP TS 38.211, 5G; NR; Physical channels and modulation. 3GPP TS 38.211, version 15.2.0, Release 15, 2018

DR.-ING. CHRISTIAN BORNKESSEL
TU Ilmenau

CO-AUTOREN
M. SC. THOMAS KOPACZ
DIPL.-ING. SASCHA SCHIESSL
PROF. DR.-ING. DIRK HEBERLING
RWTH Aachen

PROF. DR. RER. NAT. HABIL. MATTHIAS A. HEIN
TU Ilmenau

Das Paper zu diesem Beitrag wird auf dem EMV Kongress 2020 in Köln veröffentlicht.
Das Programm und die Registrierung sind unter www.e-emv.com verfügbar.

Bild: Hannibal/VDE

Beim VDE-Hauptstadtforum wurden von der Informationstechnischen Gesellschaft im VDE (ITG) insgesamt 20 Auszeichnungen vergeben

ITG-PREISVERLEIHUNG 2019

Auszeichnungen für herausragende Leistungen

Die ethischen Implikationen der Künstlichen Intelligenz und die Würdigung menschlicher Ingenieurs-Intelligenz standen im Mittelpunkt des VDE-Hauptstadtforums 2019, das mit der Preisverleihung der Informationstechnischen Gesellschaft im VDE (ITG) verbunden war.

Ein Höhepunkt beim VDE-Hauptstadtforum war die Verleihung der Preise und Auszeichnungen 2019 der ITG für außergewöhnliche Leistungen des akademischen Nachwuchses und herausragende Wissenschaftler in der Elektro- und Informationstechnik.

ITG-Auszeichnungen in fünf Kategorien vergeben

Prof. Dr. Hans Schotten, Vorsitzender der ITG, konnte insgesamt 20 Auszeichnungen vergeben – sowohl an altgediente Informationstechniker als auch an junge Nachwuchskräfte am Beginn ihrer Elektrokarriere.

ITG-Fellow 2019

Zum ITG-Fellow werden Wissenschaftler für hervorragende Leistungen auf dem Gebiet der Informationstechnik ernannt, die grundlegende Erkenntnisse in wissenschaftlicher oder technischer Hinsicht wesentlich gefördert haben. Die höchste Ehrung der ITG in diesem Bereich erhielten in diesem Jahr Prof. Dr.-Ing. habil. Dr.-Ing. E.h. Paul Walter Baier (TU Kaiserslautern), Prof. Dr.-Ing. Dr.-Ing. E.h. Joachim Hagenauer (TU München), Prof. Dr. rer. nat. Dr. h.c. Hermann Rohling (TU Hamburg-Harburg) sowie Prof. Dr.-Ing. Dr. h.c. Dr.-Ing. E.h.mult. Werner Wiesbeck (KIT).

VDE-Ehrenurkunde und ITG-Wissenschaftspreis

Mit der VDE-Ehrenurkunde wurden Prof. Dr.-Ing. Stefan Breide (FH Südwestfalen), Dr.-Ing. Wolfgang H. Döring (RWTH Aachen), Dr.-Ing. Jörg-Peter Elbers (ADVA), Prof. Dr. Dr. Wolfgang A. Halang (FernUniversität Hagen) sowie Prof. Dr.-Ing. Ralf Tönjes (HS Osnabrück) ausgezeichnet.

Der Wissenschaftspreis der ITG 2019, die höchste Auszeichnung der Fachgesellschaft für das Lebenswerk, die nur alle drei Jahre verliehen wird, ging an Prof. Gerhard M. Sessler von der TU Darmstadt für seine herausragenden Leistungen auf dem Gebiet der Elektroakustik.

ITG-Preis 2019

Den Literaturpreis der ITG, der mit 3 000 Euro dotiert ist, erhielten in diesem Jahr Prof. Dr.-Ing. Amelie Hagelauer (TU Dresden) und Dr.-Ing. Andreas Tag (Qorvo Inc, Apopka/Florida), Dr.-Ing. Ina Kodrasi und Prof. Dr. Simon Doclo (Idiap Research Institute, Martigny/Schweiz) sowie ein Forscherteam des Deutschen Zentrums für Luft- und Raumfahrt e.V. (DLR), bestehend aus Dr.-Ing. Felipe Queiroz de Almeida, Dipl.-Ing. Tobias Rommel, Dr. Gerhard Krieger und Prof. Dr.-Ing. Alberto Moreira.

Dissertationspreis 2019

Mit dem Dissertationspreis für herausragende Dissertationen aus dem Bereich der Informationstechnik wurden drei Nachwuchswissenschaftler ausgezeichnet: Dr.-Ing. Harry Weber (Hella GmbH & Co. KGaA), Dipl.-Ing. Tobias Rommel (DLR) und Dr.-Ing. Jens Steinwandt (Rohde & Schwarz GmbH & Co. KG).

+++ ITG-Preise 2020 +++

Aufruf für den Dissertationspreis der ITG 2020
Seit 1994 verleiht die Informationstechnische Gesellschaft im VDE (ITG) jährlich bis zu drei Dissertationspreise. Mit diesem Preis werden besonders herausragende Dissertationen junger Wissenschaftlerinnen/Wissenschaftler und Ingenieurinnen/Ingenieure auf dem Gebiet der Informationstechnik gewürdigt. Die Bewerberinnen und Bewerber müssen der ITG spätestens zum Zeitpunkt der Einreichung angehören. Jeder Preis ist mit einer Geldprämie von 2 000 Euro sowie einer Urkunde verbunden.
Der Vorstand der ITG bittet deshalb alle infrage kommenden ITG-Mitglieder, die 2019 ihre Dissertation angefertigt haben und nicht älter als 32 Jahre sind, ihre Arbeit bis spätestens **3. Februar 2020** an die ITG-Geschäftsstelle, Stresemannallee 15, 60596 Frankfurt, zu senden.

Aufruf für den Preis der ITG 2020
Seit dem Jahr 1956 wird der Preis der ITG für besonders hervorragende Publikationen auf dem Gebiet der Informationstechnik an Wissenschaftler und Ingenieure verliehen, sofern sie ITG-Mitglieder sind. Jeder Preis ist mit einer Geldprämie von 3 000 Euro sowie einer Urkunde verbunden.

Hauptkriterien für die Beurteilung der Arbeiten sind
- Originalität,
- theoretische und/oder praktische Behandlung des Themas,
- Darstellung und Form sowie
- Bedeutung der Arbeit.

Auch Übersichtsaufsätze als überzeugend gelungene zusammenfassende Darstellung eines größeren Fachgebiets sind preiswürdig, ohne dass solche Arbeiten unbedingt neue wissenschaftliche Erkenntnisse vermitteln müssen. Der Vorstand der Informationstechnischen Gesellschaft im VDE (ITG) bittet um die Einreichung der Unterlagen zur Bewerbung bis **15. Februar 2020.**

Weitere Informationen und Einzelheiten zu den verschiedenen Preisen der ITG finden Sie unter
// www.vde.com/itgpreise

Grafik: Fotolia_Jlgarts

Veranstaltungen

18.–20.02.2020, Hamburg
24th International ITG Workshop on Smart Antennas (WSA 2020)
ITG
// www.wsa2020.net

26.–27.02.2020, Berlin
VDE Tec Summit 2020
VDE
// tecsummit.vde.com

03.03.2020, Magdeburg
ITG-Workshop Sprachassistenten: Anwendungen, Implikationen, Entwicklungen
ITG
// www.vde.com/de/itg/veranstaltungen

04.–06.03.2020, Magdeburg
ESSV 2020 – Elektronische Sprachsignalverarbeitung
Otto von Guericke University Magdeburg
// www.essv.de/essv2020

09.–11.03.2020, Cottbus
GeMiC 2020 – German Microwave Conference
BTU Cottbus, ITG, IMA e.V.
// www.b-tu.de/gemic2020

16.–19.03.2020, Hannover
DAGA – Jahrestagung für Akustik
DEGA, NAGA, LUH, ITG, DPG, DIN/VDI-Normenausschuss NALS
// 2020.daga-tagung.de

23.–24.03.2020, Berlin
14. ITG-Fachkonferenz Breitbandversorgung in Deutschland
ITG-FA KT 2, FG 5.2.5
// www.vde.com/de/itg/veranstaltungen

31.03.–01.04.2020, Tübingen
2. KuVS-Fachgespräch Network Softwarization
GI/ITG-FG KuVS
// kn.inf.uni-tuebingen.de/kuvs-fg-netsoft/2020

02.–03.04.2020, Tübingen
ITG-Workshop on IT Security
ITG-FG 5.2.2
// kn.inf.uni-tuebingen.de/itg-itsec/2020

04.–09.05.2020, Barcelona, Spanien
45th International Conference on Acoustics, Speech, and Signal Processing ICASSP 2020
IEEE
// 2020.ieeeicassp.org

06.–08.05.2020, Verona, Italien
26th European Wireless (EW)
// ew2020.european-wireless.org

13.–14.05.2020, Leipzig
21. ITG-Fachtagung Photonische Netze
ITG-FA KT 3, ITG-FG 5.3.3
// www.vde.com/de/itg/veranstaltungen

13.–14.05.2020, Osnabrück
25. ITG-Fachtagung Mobilfunkkommunikation
ITG-FA KT 2
// www.vde.com/de/itg/veranstaltungen

08.–10.06.2020, Potsdam
29. FKTG-Fachtagung 2020
FKTG
// www.fktg.org /node/14881

Impressum

ITG-news

Herausgeber: Informationstechnische Gesellschaft im VDE, Frankfurt am Main

Redaktion: Dr. Volker Schanz, Silvia Buhlmann

Telefon: 069/6308-360/-362
E-Mail: itg@vde.com
Internet: www.vde.com/itg

Konzept und Realisation: HEALTH-CARE-COM GmbH, ein Unternehmen der VDE VERLAG GmbH, Projektleitung: Anne Wolf

Druck: Heenemann GmbH & Co. KG, Berlin