Aus der Forschung

Abteilung für Informationstheorie und Kommunikationssysteme (Jorswieck)

1. Forschungsfelder der Abteilung

Im ersten Jahr des Bestehens der Abteilung konnten die Forschungsfelder Zellulare Kommunikationssysteme und Zugangsnetze sowie Sicherheit auf der Übertragungsschicht gestärkt und weiter ausgebaut werden. Im Bereich der Sicherheit auf der Übertragungsschicht haben wir große Fortschritte in der Berechnung der sicheren Kapazität für bestimmte Abhörer-Kanäle mit Störern erzielt [JAN/JOR2]. Die resultierenden Kapazitätsausdrücke eignen sich zwar noch nicht für den Systementwurf, zeigen aber die Grenzen der erreichbaren sicheren Datenraten deutlich auf. Die Kanalsymmetrierung spielt dabei eine wichtige Rolle. Im Moment beschäftigen wir uns mit einer Erweiterung der Kanalsymmetrierung, nämlich der sogenannten Überschreibbarkeit von Kanälen. Die große Hoffnung besteht darin, dass es Eigenschaften von Kanälen gibt, die eine sichere und zuverlässige Kommunikation trotz böswilligem Störer und Abhörer erlauben. In einer weiteren Arbeit konnten wir ein Verfahren für die heimliche (stealthy) und sichere Schlüsselerzeugung entwickeln [LIN/JAN/JOR1].

Für die zellulare Kommunikation und die Optimierung der Ressourcen-Vergabe für Zugangsnetze haben wir einige sehr interessante Algorithmen und Verfahren entwickelt [JOR10], [JOR3], [JOR5]. Das erste Deployment von 5G-Netzwerkinfrastruktur hat gezeigt, dass höhere Datenraten und geringere Latenzzeiten erreicht werden. Allerdings ist auch der Energieverbrauch der Basisstationen ca. um den Faktor 5 gestiegen. Das steht im krassen Gegensatz zu dem Ziel, die Energieeffizienz in [bits/Joule] um den Faktor 100 bis 1000 zu steigern. Deshalb konzentrieren wir uns weiter auf die Steigerung der globalen Energieeffizienz von zellularen Netzwerken. Die Hardware-Architektur [JOR7] sowie die Ressourcen-Vergabe [JOR6] bieten viel Raum zur Energieeffizienzverbesserung.

Die zwei Buchkapitel „Optimization techniques for energy efficiency“ [JOR2] und „Resource Allocation for Shared Spectrum Networks“ [JOR1] sind aus Kooperationen mit einem ehemaligen Doktoranden, der jetzt an der Universität Bremen eine Gruppe leitet, und einem Kollegen, der jetzt bei Nokia Bell Labs in Paris arbeitet, hervorgegangen.

Besonders bemerkenswert ist die überdurchschnittliche Anzahl von Veröffentlichungen in IEEE Journals und Transactions im Berichtszeitraum, die aus der Forschung entstanden sind. Das ist ein sehr guter Start für die Abteilung.

2. Projekte

Wir haben die DFG-geförderten Gemeinschaftsprojekte fortgesetzt oder erfolgreich abgeschlossen. Sehr erfreulich ist der Start eines BMBF-geförderten Projektes im Bereich der Ressourcen-Vergabe durch Maschinelles Lernen. Ein Antrag auf ein Forschungsgroßgerät wurde fristgerecht im September bei der DFG mit dem Arbeitstitel: 'Multiple-Input Multiple-Output (MIMO) Prototyping System für Zellulares Mobilfunklabor' eingereicht. Im Berichtszeitraum sind bzw. waren wir in nachfolgenden Forschungsvorhaben engagiert.

2.1 Internationale Projekte

Das DFG-geförderte Gemeinschaftsprojekt mit dem Titel „Effiziente Ressourcenvergabe in drahtlosen Software-Defined Networks“ mit Professor Nader Mokari von der Tarbiat Modares Universität in Teheran, Iran, setzte seine Forschungen an neuen Optimierungsverfahren für die effiziente Ressourcenvergabe in drahtlosen Interferenznetzwerken fort. Besonders das für 5G hoch gehandelte Vielfachzugriffsverfahren Non-orthogonal Multiple-Access (NOMA) befindet sich auf dem Prüfstand – insbesondere in Multi-Zell-Umgebungen. Für die European Association for Signal Processing (EURASIP) ist Prof. Jorswieck Herausgeber (Editor-in-Chief) des Springer Journals on Wireless Communications and Networking. Außerdem ist Prof. Jorswieck als Associate Editor für die IEEE Transactions on Information Forensics and Security aktiv. Es sind während des Berichtszeitraums die Journal-Veröffentlichungen [JOR11], [JOR4], [JOR5], [REZ/JOR1] hervorgegangen.

2.2 Nationale Projekte

Das DFG-geförderte Gemeinschaftsprojekt „Sicherheit auf der Übertragungsschicht für Kanäle mit Zuständen und aktiven Angreifern“ mit Professor Holger Boche von der TU München wurde erfolgreich abgeschlossen. Die wesentlichen Ergebnisse sind zurzeit sowohl als Einreichung bei IEEE Transactions on Information Theory in Begutachtung als auch im DFG-Abschlussbericht zusammengefasst. Es laufen weiterhin die beiden DFG-Projekte „Robuste Rekonstruktion für drahtlose Body Area Sensor Netzwerke“ gemeinsam mit Dr. Dargie von der TU Dresden und „Informationssicherheit auf der Übertragungsschicht in Multimode-Faser-Kommunikationssystemen“ mit Prof. Czarske von der TU Dresden.

Das BMBF-Verbundprojekt “Anwendungsspezifische Ressourcenallokation und effizientes Management in drahtlosen Netzwerken mit hohem Anteil an IEEE 802.11-Zugangssystemen mit maschinellen Lernansätzen“ wird seit August 2020 innerhalb der Bekanntmachung “Künstliche Intelligenz in Kommunikationsnetzen“ im Rahmen der High-Tech-Strategie 2025 des BMBF gefördert. Gemeinsam mit der Hochschule Nordhausen, dem Fraunhofer Institut für Nachrichtentechnik HHI, dem Max-Planck-Institut für Informatik, der Evernet e. G., der Montanuniversität Leoben, NewMedia-Net GmbH und BISDN GmbH wird in diesem Projekt an intelligenten verteilten Algorithmen zur Steuerung der WLAN-Zugangsnetze geforscht.

3. Mitarbeiterinnen und Mitarbeiter der Abteilung

Die Forschungsgebiete der informationstheoretisch sicheren Übertragung über Abhörerkanäle bearbeiten die Herren Dr. Pin-Hsun Lin, Carsten Janda und Andrew Lonnstrom. Der neue Post-Doktorand Dr. Bile Peng, ein ehemaliger Doktorand aus der Abteilung Mobilfunksysteme, der sich in diesem Institutsbericht vorstellt, bringt seine Kenntnisse aus dem maschinellen Lernen für Kommunikationssysteme in die Abteilung ein. Herr Karl-Ludwig Besser arbeitet an einem Framework für die Analyse von statistischen Abhängigkeiten in drahtlosen Kommunikationsnetzwerken. Im gemeinsamen DFG-Projekt mit dem iranischen Partner hat Herr Sepehr Rezvani seine Arbeit fortgesetzt. Herr Martin Le konnte sich in die Multi-Armed Bandit-Algorithmen einarbeiten. Das Ziel ist die Entwicklung von neuen Algorithmen zur Ressourcen-Vergabe in Netzwerken, welche sich zwischen Erkundung (Exploration) und Nutzung (Exploitation) der Funkressourcen optimal entscheiden. Die Gastwissenschaftlerin Frau Jiaying Liu wird weiterhin von der Chinesischen Akademie der Wissenschaften gefördert und arbeitet an der Modellierung und Optimierung von drahtlosen optischen Empfängern mit räumlicher Diversität.

Unser Support-Team besteht zurzeit aus Frau Andersen (bis 31. Oktober), Frau Brandt, Frau Haase, Frau Sengpiel und den Herren Eisenberger, Gottwald, Gudat und Hellrung.

3.1 Arbeiten des IT-Serviceteams

Das IT-Serviceteam bestehend aus Herrn Schlegel und Herrn Gudat hat in diesem Jahr, neben den ständig anfallenden Aufgaben im IT-Bereich, wie immer auch diverse kleinere Projekte bearbeitet. Zu den regelmäßigen Aufgaben des Teams gehören administrative Arbeiten, der Betrieb der institutseigenen Server, die erforderliche Aktualisierung der Hardware und Software bei allen Instituts-Rechnern, allgemeine Reparaturen sowie anfallende Wartungsarbeiten. Besonders hervorzuheben ist dieses Mal die Erneuerung des institutseige-

nen Exchange-Servers und die Ertüchtigung aller Arbeitsplatz-PCs, der SAP-Rechner, der Simulationsumgebungen, der Firewall und der VPN-Zugänge, sodass auch in Corona-Zeiten ein Arbeiten für nahezu alle Mitarbeiterinnen und Mitarbeiter des Instituts von zuhause aus wie gewohnt möglich ist. Weiterhin wurde ein Hochleistungs-Simulationsrechner neu beschafft, zusammengebaut und aufgesetzt. Da das Institut einen Raum abgeben musste, war auch eine umfangreiche Entsorgung diverser alter Hardware notwendig.

Im Folgenden bieten wir einen knappen Überblick über die Forschungsaktivitäten in den oben genannten Bereichen. Dieses Jahr konzentrieren wir uns auf die Sicherheit auf der Übertragungsschicht (PhySec) und die zellulare Kommunikation zusammen mit Zugangsnetzen (CelCom).

4. Sicherheit auf der Übertragungsschicht (PhySec)

4.1 Sicherheit auf der Übertragungsschicht für Kanäle mit Zuständen und aktiven Angreifern (Play Scate)

Datensicherheit in einem sich potentiell feindlich verhaltenden Umfeld ist ein wesentliches Zielkriterium in modernen Kommunikationssystemen. Wyner[1] untersuchte sichere Kommunikation über verrauschte Kanäle und führte den **W**ire**t**ap **C**hannel (WTC) ein. Später wurde seine Arbeit auf das Senden von vertraulichen Nachrichten über einen Broadcast-Kanal ausgeweitet[2]. Mit dem Broadcast-Kanal wird in der Informationstheorie ein Kanalmodell mit einem Sender und mehreren Empfängern beschrieben, über das unabhängige Nachrichten an die Empfänger übertragen werden. Das steht im Gegensatz zum Begriff der Broadcast-Übertragung für Multimedia-Daten. Die drahtlose Kommunikation ist anfällig für Abhörer. Daher ist die Motivation der beiden vorhergehenden Arbeiten, einem passiven Lauscher die Möglichkeit zu nehmen, sensible und vertrauliche Nachrichten abzuhören. Dies erfolgt, indem die physikalischen Eigenschaften des Übertragungsmediums geschickt berücksichtigt werden und eine Codierungsstrategie entwickelt wird, die gleichzeitig informationstheoretische Sicherheit und zuverlässige Kommunikation gewährleisten kann. Gemeinsam war diesen Arbeiten, dass der Gegner als passiv, also als reiner Abhörer angenommen wurde. Durch die Einführung von Kanalzuständen können aktive Gegner, die den Kanalzustand willkürlich ändern können, durch den **A**rbitrarily **V**arying **C**hannel (AVC) modelliert werden.

Wenn Sicherheitsanforderungen mit aktiven Angriffen auf Kommunikationssysteme modelliert werden sollen, ist der **A**rbitrarily **V**arying **W**iretap **C**hannel (AV-

[1] Aaron Wyner. The wire-tap channel. Bell Syst. Tech. J., 54(8):1355–1387, October 1975

[2] Imre Csiszár and János Körner. Broadcast Channels with Confidential Messages. IEEE Transactions on Information Theory, 24(3):339-348, May 1978

WC) das richtige Kanalmodell. Die Autoren in[3] leiten eine allgemeine Multi-Letter-Formel für die allgemeine Random-Code-Sicherheitskapazität und eine Single-Letter-Formel für den stark degradierten Fall mit mittlerem Fehlerkriterium ohne zusätzliche Nebeninformationen beim Störsender her.

Wir betrachten den AVWC mit nicht-kausalen Nebeninformationen beim Störsender. Nicht-kausale Nebeninformationen bedeutet, dass Codewörter bei einem aktiven Angreifer bekannt sind, bevor sie übertragen werden. Wir stellen die Random-Code Sicherheitskapazität mit maximalem Fehlerkriterium für den Fall bereit, dass es einen besten Kanal für den Abhörer gibt, und unter der Bedingung, dass der Abhörkanal in Bezug auf den Hauptkanal stark degradiert ist. Durch Berücksichtigung des maximalen Fehlerkriteriums ermöglichen wir dem aktiven Angreifer, auch die Nachrichten (und nicht nur den Kanaleingang) zu kennen. Für den betrachteten Fall können wir eine Single-Letter Formel für die Sicherheitskapazität bereitstellen.

Theorem 1. *Gegeben sei ein AVWC $(\mathcal{W}, \mathcal{V})$. Falls $(\mathcal{W}, \mathcal{V})$ stark degradiert ist und es einen besten Kanal zum Abhörer gibt und falls der Störsender nicht-kausale Seiteninformationen über den Kanaleingang $x^n \in \mathcal{X}^n$ (und die korrespondierenden Nachrichten) hat, dann ist die Random-Code Sicherheitskapazität gegeben durch*

$$\widehat{C}_S^{ran}(\mathcal{W}, \mathcal{V}) = \max_{P_X} \left(\min_{\theta \in \mathcal{P}(\mathcal{S}|\mathcal{X})} I(X; Y_\theta) - \max_{\theta \in \mathcal{P}(\mathcal{S}|\mathcal{X})} I(X; Z_\theta) \right) \tag{1}$$

$$= \max_{P_X} \left(\min_{\theta \in \mathcal{P}(\mathcal{S}|\mathcal{X})} I(X; Y_\theta) - I(X; Z_{\theta^*}) \right) \tag{2}$$

$$= \max_{P_X} \left(\min_{W \in \widehat{\widehat{\mathcal{W}}}} I(P; W) - \max_{V \in \widehat{\widehat{\mathcal{V}}}} I(P; V) \right). \tag{3}$$

Diese Sicherheitskapazität hängt von den Zeilen-Konvexkombinationen $\widehat{\widehat{\mathcal{W}}}$ und $\widehat{\widehat{\mathcal{V}}}$ ab.

Beispiel 1. Gegeben seien die folgenden Kanalmatrizen.

$$w(\cdot|\cdot, s_1) = \begin{pmatrix} 0.1 & 0.9 \\ 0.7 & 0.3 \\ 0.8 & 0.2 \end{pmatrix}, \qquad w(\cdot|\cdot, s_2) = \begin{pmatrix} 0.2 & 0.8 \\ 0.85 & 0.15 \\ 0.9 & 0.1 \end{pmatrix}$$

$$v(\cdot|\cdot, s_1) = \begin{pmatrix} 0.25 & 0.75 \\ 0.4 & 0.6 \\ 0.6 & 0.4 \end{pmatrix}, \qquad v(\cdot|\cdot, s_2) = \begin{pmatrix} 0.3 & 0.7 \\ 0.45 & 0.55 \\ 0.65 & 0.35 \end{pmatrix}$$

[3] Moritz Wiese, Janis Nötzel, and Holger Boche. A Channel under Simultaneous Jamming and Eavesdropping Attack – Correlated Random Coding Capacities Under Strong Secrecy Criteria. IEEE Transactions on Information Theory, 62(7):3844–3862, July 2016.

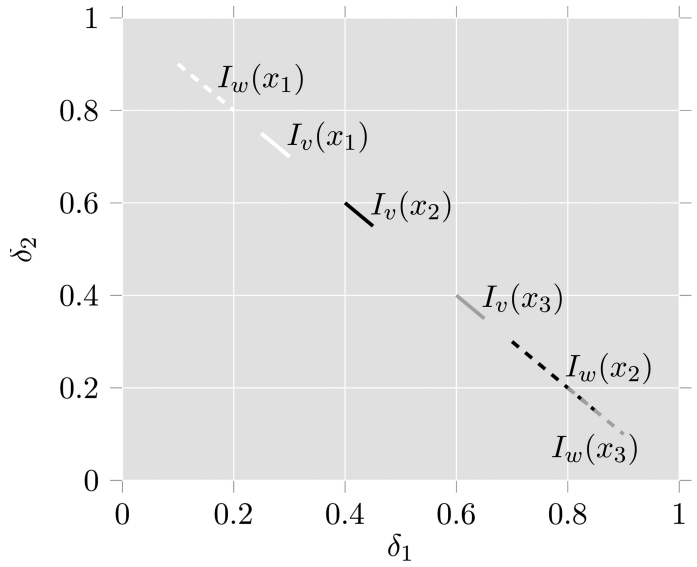

Abbildung 1: Konvexe Hüllen $\mathcal{I}_w(x)$ und $\mathcal{I}_v(x)$ für das Beispiel

Es lässt sich direkt überprüfen, dass dieser AVWC die starke degradierte Eigenschaft erfüllt.

$$\bar{W} = \alpha w(\cdot|\cdot, s_1) + (1-\alpha) w(\cdot|\cdot, s_2) = \begin{pmatrix} 0.2 - 0.1\alpha & 0.8 + 0.1\alpha \\ 0.85 - 0.15\alpha & 0.15 + 0.15\alpha \\ 0.9 - 0.1\alpha & 0.1 + 0.1\alpha \end{pmatrix},$$

$$\bar{V} = \beta v(\cdot|\cdot, s_1) + (1-\beta) v(\cdot|\cdot, s_2) = \begin{pmatrix} 0.3 - 0.05\beta & 0.7 + 0.05\beta \\ 0.45 - 0.05\beta & 0.55 + 0.05\beta \\ 0.65 - 0.05\beta & 0.35 + 0.05\beta \end{pmatrix}.$$

Die konvexen Hüllen des legitimierten Kanals ($\bar{W}$) und des Abhörerkanals ($\bar{V}$) sind in **Abbildung 1** illustriert. Die Sicherheitskapazität $C_S^{\text{ran}}(\mathcal{W}, \mathcal{V})$ dieses AVWC kann angegeben werden als $C_S^{\text{ran}}(\mathcal{W}, \mathcal{V}) \approx 0.3$ Bits pro Kanalbenutzung, mit $p_X(0) = p_X(2) = 0.5$, $p_X(1) = 0$, $\alpha = 0.5$, $\beta \approx 1$. Im Gegensatz korrespondieren die Kanäle

$$\bar{\bar{W}} = \begin{pmatrix} 0.2 & 0.8 \\ 0.8 & 0.2 \\ 0.8 & 0.2 \end{pmatrix} \qquad \bar{\bar{V}} = \begin{pmatrix} 0.25 & 0.75 \\ 0.4 & 0.6 \\ 0.65 & 0.35 \end{pmatrix}$$

mit dem besten Kanal zum Abhörer und dem schlechtesten Kanal zum legitimierten Empfänger, falls der Kanaleingang nicht-kausal bei dem Störsender bekannt ist. Für diesen Fall kann die Sicherheitskapazität des AVWC berechnet werden zu $\widehat{C}_S^{\text{ran}}(\mathcal{W}, \mathcal{V}) \approx 0.26$ Bits pro Kanalbenutzung, mit $p_X(0) = p_X(1) = 0.5$, $p_X(2) = 0$. Das zweite Eingangssymbol wird in dem Fall von nicht-kausaler Seiteninformation bezüglich des Kanaleingangs beim Störsender benutzt, anstelle

des dritten Eingangssymbols, das bei dem Fall ohne Nebeninformation benutzt wird.

Ein möglicher Ansatz, um die Zusammenarbeit zwischen dem Störsender und dem Lauscher zu bekämpfen, könnte die Möglichkeit sein, den Kanal zwischen dem Störsender und dem Lauscher zu symmetrisieren. Dabei erwarten wir, dass die Random-Code-Sicherheitskapazität geringer ist als im Fall ohne Zusammenarbeit, da die Optimierung in Bezug auf die Eingangsverteilung über alle Eingangsverteilungen erfolgt, die den Kanal zwischen Störsender und Lauscher symmetrieren. Daher erwarten wir ein ähnliches Verhalten wie beim AVC mit Beschränkungen, bei dem wiederum die optimalen Eingangsverteilungen für die Fälle mit und ohne Einschränkungen unterschiedlich sein können. Wir betrachten dies jedoch als offene Frage.

5. Zellulare Kommunikationssysteme und drahtlose Zugangsnetze

5.1 Mehrnutzer-Kommunikationssysteme mit Unsicherheit über die gemeinsame Verteilung der Fading-Kanäle

Ein entscheidendes Problem bei drahtlosen Datenübertragungen ist Schwund des Signals über den Kanal (engl. channel fading). Diese Dämpfung geschieht zufällig und wird mithilfe von Zufallsvariablen modelliert. Daraus ergibt sich folgendes Systemmodell. Das Empfangssignal ist gegeben durch

$$\boldsymbol{A} = \boldsymbol{H}\boldsymbol{M} + \boldsymbol{N}, \tag{4}$$

wobei $\boldsymbol{M}$ das gesendete Signal, $\boldsymbol{H}$ der Kanalschwund (Fading) und $\boldsymbol{N}$ das additive Gaußsche Rauschen sind. Die Übertragung geschieht mit einer Übertragungsrate R. Die Kanalkapazität wird mit C bezeichnet.

Bei der stochastischen Kanalmodellierung wird klassischerweise zwischen Slow-Fading (langsamem Schwund) und Fast-Fading (schnellem Schwund) unterschieden. Bei Ersterem ist der Fading-Koeffizient (annähernd) konstant über die Dauer einer Symbolübertragung. Bei Fast-Fading hingegen ändert sich $\boldsymbol{H}$ während der Übertragung.

Durch die Dämpfung (Fading) kommt es zu starken Performance-Einbußen und es ist bekannt, dass im Falle von Slow-Fading keine fehlerfreie Übertragung möglich ist[4], da die Wahrscheinlichkeit besteht, eine sehr starke Dämpfung ($\boldsymbol{H}$ nahe Null) während einer Übertragung zu erfahren. Die Wahrscheinlichkeit, dass die erreichte Übertragungsrate R für die fehlerschutzcodierte (FEC) Übertragung geringer ist als die instantane Kanalkapazität C, wird als *Ausfallwahr-*

[4]E. Biglieri, J. Proakis, and S. Shamai, „Fading channels: information-theoretic and communications aspects,“ IEEE Trans. Inf. Theory, vol. 44, no. 6, pp. 2619–2692, 1998.

scheinlichkeit (engl. outage probability) bezeichnet. Im Falle von Mehrantennensystemen mit n Empfangsantennen und Maximum-Ratio-Combining am Empfänger ist diese Ausfallwahrscheinlichkeit ε gegeben durch

$$\varepsilon = \mathbb{P}\left(R < C\right) = \mathbb{P}\left(\sum_{i=1}^{n} |\boldsymbol{H}_i|^2 < \frac{2^C - 1}{\xi}\right) , \tag{5}$$

wobei $\boldsymbol{H}_i$ das Fading zwischen Sender und Antenne i beschreibt und ξ das Signal-zu-Rausch-Verhältnis (SNR).

Aus (5) ist offensichtlich, dass die Ausfallwahrscheinlichkeit von der Wahrscheinlichkeitsverteilung der Fading-Koeffizienten abhängt. Neben den Randverteilungen spielt aufgrund der Summe auch die gemeinsame Verteilung eine entscheidende Rolle. In der Praxis ist es gut möglich, die Randverteilungen an den einzelnen Antennen zu messen. Allerdings besteht eine Unsicherheit über die gemeinsame Verteilung. Im Rest dieses Abschnitts werden Forschungsergebnisse diskutiert, welche Grenzen der Ausfallwahrscheinlichkeit für Unsicherheit über die gemeinsame Fading-Verteilung beschreiben.

Basierend auf den Ergebnissen von[5] werden in [BES/JOR2] Grenzen für die ε-Outage Capacity, also die maximale Übertragungsrate, für welche die Ausfallwahrscheinlichkeit höchstens ε beträgt, hergeleitet. In [BES/JOR6] werden diese Ergebnisse genauer für den Spezialfall Rayleigh-Fading untersucht und die Ausfallwahrscheinlichkeit bestimmt. Diese ist in **Abbildung 2** dargestellt. Neben den Grenzen (Best Case und Worst Case) sind die Fälle von unabhängigen und ko-monotonen Kanälen dargestellt. Das erste interessante Ergebnis ist, dass der Worst Case nicht mit dem ko-monotonen Fall übereinstimmt. Allerdings haben beide Fälle die gleiche Diversity von eins, welche als Steigung der Kurven für hohe SNR in der Abbildung abgelesen werden kann. Im Gegensatz dazu ist die Diversity im Fall von n unabhängigen Kanälen gleich n. Dies bedeutet aber auch, dass die Ausfallwahrscheinlichkeit für endliche n immer größer als Null ist und daher keine vollständig fehlerfreie Kommunikation garantiert werden kann[6]. Ein überraschendes Ergebnis ist, dass im besten Fall eine fehlerfreie Kommunikation ($\varepsilon = 0$) möglich ist. Es existiert ein SNR-Grenzwert, für welchen die Ausfallwahrscheinlichkeit auf genau Null sinkt. In **Abbildung 2** ist dies durch ein senkrechtes Abfallen der Best-Case-Kurve erkennbar.

Dieses Ergebnis zeigt, dass es möglich ist, mit einer geringen Antennenanzahl fehlerfrei über Slow-Fading-Kanäle zu übertragen, wenn die einzelnen Kanäle eine bestimmte Abhängigkeitsstruktur erfüllen. Die Eigenschaften der gemein-

[5] R. Wang, L. Peng, and J. Yang, „Bounds for the sum of dependent risks and worst Value-at-Risk with monotone marginal densities," Financ. Stochastics, vol. 17, no. 2, pp. 395–417, Apr. 2013.

[6] D. Tse and P. Viswanath, Fundamentals of Wireless Communications. Cambridge University Press, 2005.

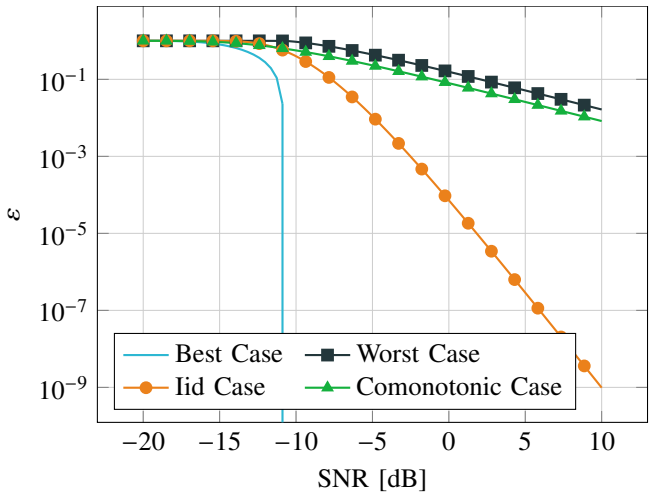

Abbildung 2: Ausfallwahrscheinlichkeiten für $n = 5$ abhängige Rayleigh-Fading-Kanäle mit einer Übertragungsrate $R = 0.5$ (Abbildung 3 in [BES/JOR6])

samen Verteilungen und zugrundeliegenden Abhängigkeitsstrukturen werden näher in [BES/LIN/JOR1] untersucht. Für zukünftige Systemdesigner ist es daher eine interessante Fragestellung, wie diese gemeinsamen Verteilungen in realen Kommunikationssystemen erzeugt werden können. Eine mögliche Schlüsseltechnologie könnten dabei Reconfigurable Intelligent Surfaces (RIS) sein [7]. Die hergeleiteten Ausdrücke für das Best-Case-Szenario können dann als Richtlinie genutzt werden um die aktuelle System-Performance mit der Bestmöglichen zu vergleichen.

Auf der anderen Seite kann der Worst Case genutzt werden, um Kommunikationssysteme robust zu entwerfen. Dabei legt man die Parameter so aus, dass das System selbst im schlimmsten Fall noch gemäß den Anforderungen funktioniert. Dies ist besonders für sicherheitsrelevante Anwendungen von großer Bedeutung. Ein Beispiel aus der Nachrichtentechnik ist die Datenübertragung, welche von einer dritten Partei abgehört wird. Es ist möglich, spezielle Kommunikationsstrategien zu verwenden um Abhörsicherheit auf der Übertragungsschicht (engl. physical layer security) zu ermöglichen. Grenzen solcher Verfahren bei Szenarien, in denen eine Unsicherheit über die gemeinsame statistische Verteilung der Übertragungskanäle zu legitimiertem Empfänger und Abhörer besteht, werden in [BES/JOR3] und [BES/JOR4] untersucht.

[7] M. Di Renzo, M. Debbah, D. Phan-Huy et al.„Smart Radio Environments Empowered by Reconfigurable AI Meta-Surfaces: an Idea Whose Time Has Come,“ in EURASIP Journal on Wireless Comunications and Networking, vol. 2019, no. 1, p. 129, Dec. 2019.

5.2 Maschinelles Lernen in Kommunikationssystemen

Das maschinelle Lernen wird in den letzten Jahren in unterschiedlichen Bereichen erfolgreich angewendet, wo es kein zugrundeliegendes Modell gibt, das zu komplex ist, oder es keine analytische einfache Lösung gibt, z.B. in Mustererkennung, Verarbeitung natürlicher Sprache, sowie in Kommunikationssystemen sowie in vielen anderen Anwendungen außerhalb der Kommunikationstechnik. Einige erfolgreiche Beispiele des maschinellen Lernens in Kommunikationssystemen sind:

- MIMO-Kanalschätzung durch das überwachte Lernen,
- Transceiver-Design mit dem Autoencoder oder mit überwachtem und bestärkendem Lernen für den nichtlinearen Kanal (z.B. Glasfaserkanäle),
- Ressourcenallokation für die V2X-Kommunikation mit überwachtem und bestärkendem Lernen.

Wir sind davon überzeugt, dass bessere und faszinierende Anwendungen des maschinellen Lernens für die Kommunikation zu erwarten sind und wir streben an, unseren Beitrag dazu zu leisten.

Mit einem Deep Neural Network (DNN) kann eine beliebige Funktion mit hochdimensionalem Input und Output approximiert werden. Wenn wir genug Daten über diese Funktion haben, können wir zufällig initialisiertes DNN trainieren, um die Funktion zu approximieren, auch wenn es keine analytische Form der Funktion gibt. Im einfachsten Fall (das überwachte Lernen) sind der Input und der entsprechende Output bekannt. Man kann mit dem überwachten Lernen das DNN so trainieren, dass der Output des Netzes den “richtigen”, d.h. gewünschten Output reproduziert. Ein Beispiel: Man überträgt ein Symbol über einen nichtlinearen Glasfaserkanal. Nach dem Empfang des Symbols muss der Empfänger entscheiden, welches Symbol aus allen möglichen Symbolen gesendet ist. Wir trainieren ein DNN, das das empfangene Symbol auf das richtige gesendete Symbol abbildet. Die Entscheidungsregionen sind in **Abbildung 3** dargestellt. Man kann beobachten, dass die Entscheidungsregionen schwierig analytisch zu bestimmen sind, weil das Phasenrauschen mit der Amplitude nichtlinear vergrößert ist.

Wenn der “richtige” Output unbekannt ist, kann man bestärkendes Lernen statt überwachtem Lernen verwenden. Im oben genannten Beispiel ist die Optimierung des Senders dieser Fall, weil der Kanal unbekannt ist. Um den Sender zu optimieren, können wir die gesendeten Symbole zufällig variieren. Danach trainieren wir den Sender so, dass Symbole, die einen hohen Störabstand aufweisen, in Zukunft häufiger auftauchen (in anderen Worten, das gute Ergebnis wird “bestärkt”). Der Sender wird auf diese Weise Schritt für Schritt optimiert. Am Ende

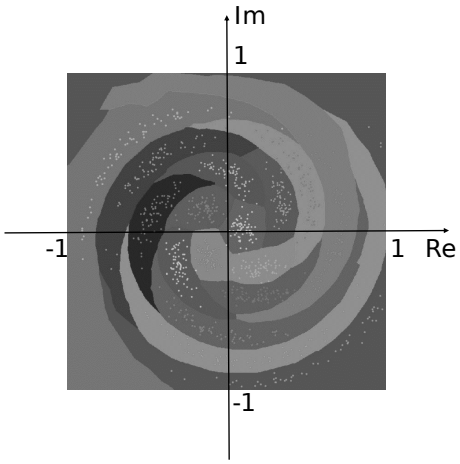

Abbildung 3: Die von einem DNN definierten Entscheidungsregionen eines Glasfaser-Empfängers unter dem SNR von 15 dB [PEN1]

haben wir das Ergebnis, wie **Abbildung 3** zeigt: Symbole mit höheren Amplituden haben größeren Abstand zwischeneinander, um das hohe Phasenrauschen zu kompensieren [PEN1].

Wir sind sicher, dass das maschinelle Lernen noch mehr Potential für die Kommunikationssysteme hat. Mit überwachtem und bestärkendem Lernen können wir komplizierte Kommunikationssysteme optimieren, deren Komplexität keine analytische Lösung ermöglicht.

5.3 Einführung in Multi-Armed Bandits (MAB)

Multi-Armed Bandits stellen k Slot-Maschinen (Spielautomaten mit einem Hebel) dar, die jeweils zufällige Auszahlungen entsprechend ihrer Zufallsvariablen ausgeben, deren Parameter (wie der Mittelwert) dem Spieler nicht bekannt sind. In jeder Runde muss sich der Spieler für eine der Slotmaschinen oder einen der k Arme des Multi-Armed Bandits entscheiden, den er spielt. Daraufhin wird entsprechend der unbekannten Zufallsvariablen eine Realisierung generiert und dem Spieler angezeigt. Das Ziel des Spielers ist es, seine kumulative Auszahlung über die begrenzte Anzahl an Runden zu maximieren.

Da der Spieler in den Runden am Anfang nur ein beschränktes Wissen über die Auszahlung der Maschinen hat, muss er abwägen, ob er nun die seiner Erfahrung nach beste Maschine i spielen soll oder lieber eine andere Maschine j spielt, die möglicherweise besser sein kann als die Maschine i mit $i \neq j$. Diese Situation wird auch als Exploitation-Exploration Dilemma bezeichnet. MAB-Algorithmen (wie der upper-confidence-bound (UCB1) Algorithmus und das Thompson-Sampling) werden eingesetzt, um Exploitation und Exploration

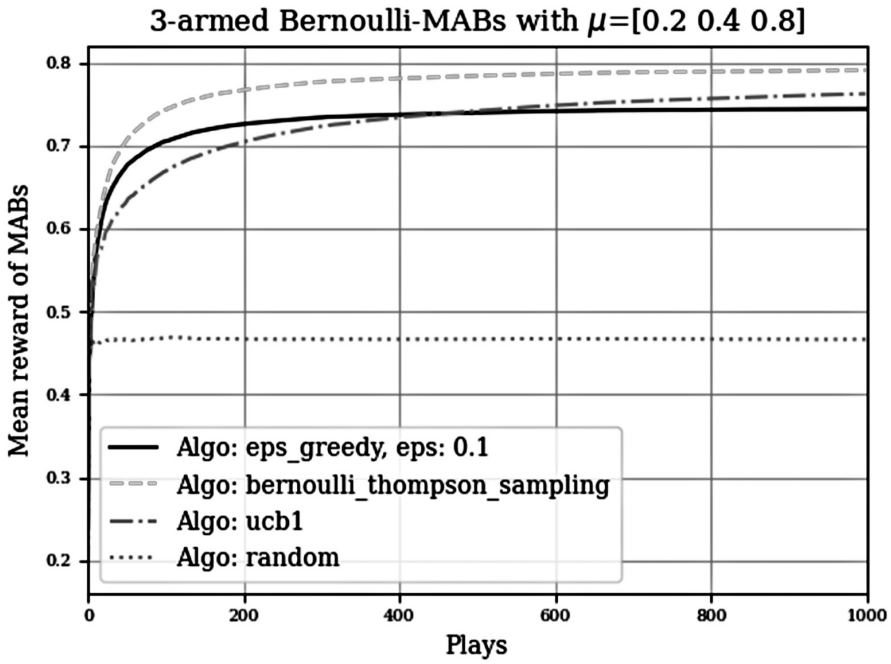

Abbildung 4: Multi-Armed Bandit mit drei Armen und Bernoulli-verteilten Zufallsvariablen $\mu = [0.2, 0.4, 0.8]$

anzupassen und auszugleichen. **Abbildung 4** zeigt Simulationen von Multi-Armed Bandits mit drei Armen, deren Auszahlungen bernoulliverteilt mit Mittelwerten $\mu = [0.2, 0.4, 0.8]$ sind. Die durchschnittlichen Auszahlungen der MABs (Englisch: mean reward of MABs) über die Anzahl der Runden (Englisch: plays) von vier unterschiedlichen Algorithmen (ϵ-greedy [8], Thompson Sampling (TS)[9], UCB1[10], Random) wurden hier dargestellt. Obwohl hier (in dieser Konstellation) nun das Thompson Sampling sich als bester Algorithmus erweist, muss das nicht immer der Fall sein. Die optimale Wahl des Algorithmus ist abhängig vom Anwendungsfall und von den Zielkriterien.

Dieses Standard-MAB-Modell lässt sich nun auch auf das Ressourcenallokationsproblem in WLAN-Systemen anwenden. Der Spieler im WLAN-System ist der Router und die Arme des Multi-Armed Bandits sind die unterstützten WLAN-Kanäle des Routers. Das Ziel dieses Modells könnte dann die Ratenoptimierung oder die Minimierung der Ausfallwahrscheinlichkeit in n Runden sein oder sogar eine Kombination aus beidem. Abhängig davon, welche Parame-

[8] Sutton, R. S., Barto, A. G. (2018). Reinforcement Learning: An Introduction. The MIT Press.

[9] Thompson, William R. On the Likelihood that One Unknown Probability Exceeds Another in View of the Evidence of Two Samples. Biometrika, 25(3–4):285–294, 1933

[10] Auer, P., Cesa-Bianchi, N., Fischer, P. Finite-Time Analysis of the Multiarmed Bandit Problem. Machine Learning 47, 235–256 (2002). https://doi.org/10.1023/A:1013689704352

ter vorhanden sind und welche Ziele verfolgt werden, kann das Standard-MAB-Modell erweitert und angepasst werden.

Die Multi-Play-Erweiterung erlaubt dem Spieler, in jeder Runde mehrere Arme zu ziehen. Hier müssen jedoch noch Kosten berücksichtigt werden, die für den Zug eines Armes aufkommen, damit nicht einfach in allen Runden alle Arme gespielt werden. Diese Erweiterung ist insofern für uns interessant, weil wir zum einen nun über unterschiedliche Parameter optimieren können und zum anderen auch innerhalb eines Parameters kombinieren dürfen. Zum Beispiel können wir damit die Nutzung einer höheren Bandbreite eines Kanals und die Übertragung über mehrere Kanäle untersuchen.

Es gibt noch eine große Anzahl an anderen Erweiterungen des MAB-Modells, die sowohl für die Ressourcenallokation in drahtlosen Netzwerken als auch für andere Gebiete interessant sein werden. Wir freuen uns auf eine aufregende und interessante Reise in die MAB-Dimension.