GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Gesamtvorhabensbezogener Teil

A. Hauptziel des Projektes

Das übergeordnete Vorhabenziel des Projekts *Code-basierte Physical-Layer Security für Terahertz-MIMO-Kommunikation (CERTAIN)* besteht darin, ausgehend von einer fundierten informationstheoretischen Basis Physical-Layer-Security (PLS) Sicherheitsverfahren für THz Multiple Input Multiple Output (MIMO) Kommunikationssysteme im Internet of Things (IoT) Kontext zu entwerfen und informationstheoretisch zu bewerten, konkret algorithmisch zu implementieren und numerisch zu analysieren, und schließlich im Rahmen von THz-Kanalmessungen und THz-MIMO-Wiretap-Demonstratoren experimentell zu validieren.

B. Förderpolitische Ziele

Das Projekt CERTAIN orientiert sich hierbei in seiner Ausrichtung am ressortübergreifenden Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt 2015–2020“. Hierbei werden sowohl die Bereiche Kommunikationssysteme als auch IT-Sicherheit adressiert. Zugleich bezieht sich das Projekt CERTAIN auf die aktuelle Hightech-Strategie 2025 der Bundesregierung „Forschung und Innovation für die Menschen“ bezüglich der konkreten Handlungsfelder „Sicherheit“ sowie „Wirtschaft und Arbeit 4.0“. Im Projekt CERTAIN konnte der Nachweis erbracht werden, dass durch das innovative Zusammenwirken von grundlegenden Sicherheitskonzepten auf der physikalischen Schicht mit breitbandiger, zukunftsweisender THz-MIMO-Übertragungstechnik neue PLS Lösungen sehr energieeffizient und recheneffizient implementierbar sind, aber trotzdem inhärente Sicherheit gewährleisten.

C. Publikationen und Patente

Seit Projektstart erfolgte Veröffentlichungen und Patentanmeldungen:

Journalartikel

[1] A. Bereyhi, S. Asaad, R. R. Müller, R. F. Schaefer, G. Fischer, and H. V. Poor, “Securing Massive MIMO Systems: Secrecy for Free with Low-Complexity Architectures,” *IEEE Transactions on Wireless Communications*, vol. 20, no. 9, pp. 5831-5845, Sep. 2021.

[2] M. Bloch, O. Günlü, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer, “An Overview of Information-Theoretic Security and Privacy: Metrics, Limits and Applications,” *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 1, pp. 5-22, Mar. 2021.

[3] S. Asaad, Y. Wu, A. Bereyhi, R. R. Müller, R. F. Schaefer, and H. V. Poor, “Secure Active and Passive Beamforming in IRS-Aided MIMO Systems,” *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1300-1315, 2022.

Abschlussbericht CERTAIN

Konferenzveröffentlichungen

[4] S. Asaad, Y. Wu, A. Bereyhi, R. R. Müller, R. F. Schaefer, and H. V. Poor, “Joint Active and Passive Secure Precoding in IRS-Aided MIMO Systems,” in *Proc. IEEE Global Communications Conference*, Madrid, Spain, Dec. 2021, pp. 1-6.

[5] R. Schulz, O. Günlü, R. Elschner, R. F. Schaefer, C. Schmidt-Langhorst, C. Schubert, and R. F. H. Fischer, “Semantic Security for Indoor THz-Wireless Communication,” in *Proc. 17th International Symposium on Wireless Communication Systems*, Berlin, Germany, Sep. 2021, pp. 1-6.

[6] A. Bereyhi, S. Asaad, C. Ouyang, R. R. Müller, R. F. Schaefer, and H. V. Poor, “How Should IRSs Scale to Harden Multi-Antenna Channels?,” in *Proc. IEEE Sensor Array and Multichannel Signal Processing Workshop*, Trondheim, Norway, June 2021, pp. 276-280.

[7] O. Günlü, M. Bloch, R. F. Schaefer, and A. Yener, “Secure Joint Communication and Sensing,” in *Proc. IEEE International Symposium on Information Theory*, Espoo, Finland, June 2022, pp. 844-849.

[8] O. Günlü, M. Bloch, R. F. Schaefer, and A. Yener, “Secure Integrated Sensing and Communication for Binary Input Additive White Gaussian Noise Channels,” in *Proc. IEEE 3rd international Symposium on Joint Communications & Sensing*, Seefeld, Austria, Mar. 2023, pp. 1-6.

[9] O. Günlü, R. Fritschek, and R. F. Schaefer, “Concatenated Classic and Neural (CCN) Codes: ConcatenatedAE,” in *IEEE Wireless Communications and Networking Conference*, Glasgow, United Kingdom, Mar. 2023, pp. 1-6.

Patentanmeldungen

[10] O. Günlü, R. Fritschek , and R. F. Schaefer, “*Methods and systems for data transfer via a communication channel,”* LU502737B1 (filed 2022, granted 2024), EP4333310A1 (filed 2023).

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Abschlussbericht CERTAIN

Zuwendungsempfänger: Technische Universität Dresden (Prof. Dr.-Ing. Rafael Schaefer)	**Förderkennzeichen:** 16KIS1242
Vorhabensbezeichnung: „Code-basierte Physical-Layer Security für Terahertz-MIMO-Kommunikation (CERTAIN)“ Teilvorhaben: „Informationstheoretische Analyse sicherer Terahertz-MIMO-Kommunikation“	
Laufzeit des Vorhabens: 01.10.2020 – 31.12.2023	

Projektpartnerbezogener Teil

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) unter dem Förderkennzeichen **16KIS1242** gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

1. Anteil zur Erreichung des Hauptziels

In CERTAIN wurde ein abhörsicheres, drahtloses PLS-THz-MIMO-Übertragungskonzept basierend auf informationstheoretischen Erkenntnissen entworfen und schließlich in einem praktischen Demonstrator umgesetzt (siehe auch Abbildung 1). Dazu wurde in CERTAIN ein fundiertes THz-MIMO-Kanalmodell entwickelt und informationstheoretisch analysiert (federführend TU Dresden). Dieses Kanalmodell ermöglichte es, Verfahren für Sicherheit auf der physikalischen Schicht durch Kombination von Methoden der codierten Modulation und sendeseitiger Vorverarbeitung zur Ansteuerung der Elemente des MIMO-Antennenarrays für die Übertragung im THz-Bereich gezielt zu entwickeln (federführend Uni Ulm). Abschließend wurde eine praktische Implementierung und experimentelle Validierung mittels THz-Wiretap-Demonstrator durchgeführt (federführend Fraunhofer HHI). Dadurch schlägt CERTAIN eine innovative Brücke von theoretischen Grundlagen-Erkenntnissen zu PLS für den THz-MIMO-Kanal über praktisch realisierbare und ressourcenarm implementierbare Codier-/Verarbeitungsverfahren hin zu einem Echtzeit-Wiretap-Demonstrator.

Abbildung 1: Zeitlicher und logischer Ablauf von CERTAIN.

Die TU Dresden war federführend im ersten Teil und hat schwerpunktmäßig das THZ-MIMO-Kanalmodell für die sichere Übertragung entwickelt und informationstheoretisch analysiert. Die gewonnenen Erkenntnisse und Ergebnisse haben die Entwicklung von PLS-Verfahren im zweiten Teil erlaubt, welche schließlich die Entwicklung eines entsprechenden Demonstrators ermöglicht haben. Die TU Dresden war in diesen Teilen ebenfalls involviert, federführend wurden diese Aktivitäten aber von der Uni Ulm bzw. dem Fraunhofer HHI vorangetrieben.

Die Projektlaufzeit erstreckte sich vom 01.10.2020 bis zum 31.12.2023. Gegenüber der ursprünglichen Zeitplanung, mit Realisierung oben genannten Aktivitäten innerhalb von 36 Monaten, wurde in erster Linie aufgrund von Verzögerungen in der ersten Phase des Projekts bei der Entwicklung des Kanalmodells und der informationstheoretischen Analyse die Gesamtprojektlaufzeit bis Ende Dezember 2023 verlängert.

2. Wissenschaftlich-technische Ergebnisse und andere wesentliche Ereignisse

2.1 Kanalmodell

Wir betrachten einen Wiretap Kanal mit drahtlosen THz-Kanälen vom Sender (Alice) zum legitimierten Empfänger (Bob) also auch dem Abhörer (Eve). Der Kanal zwischen Alice und Bob ist modelliert als $Y = H_{AB}X + N_{AB}$ wobei H_{AB} der Kanalkoeffizient und N_{AB} das unabhängige, komplexe, additive Gaussche Rauschen ist. Analog modellieren wir den Kanal zwischen Alice und Eve als $Z = H_{AE}X + N_{AE}$ wobei H_{AE} der Kanalkoeffizient und N_{AE} das unabhängige, komplexe, additive Gaussche Rauschen ist.

Bei einer typischen drahtlosen THz-Kommunikation in Innenräumen werden mehrere Strahlen auf verschiedenen Wegen von einem Sender zu einem Empfänger geleitet und erfahren dabei unterschiedliche Abschwächungen und Verzögerungen. Aufgrund der unterschiedlichen Winkel erfahren die Pfade unterschiedliche Gewinne, die von der Antennenausrichtung und der Richtwirkung abhängen. Darüber hinaus erfährt jeder Strahl, abhängig von der Trägerfrequenz f_c und der Weglänge d, einen Freiraum-Wegverlust gemäß

$$H_{fspl(f)} = \left(\frac{c_0}{4\pi f_c d}\right)^2$$

wobei c_0 die Lichtgeschwindigkeit ist. Im Allgemeinen erleiden reflektierte Strahlen im freien Raum einen größeren Pfadverlust aufgrund einer größeren Pfadlänge im Vergleich zur Line-of-Sight (LOS) Kommunikation. Darüber hinaus führt der Reflexionsverlust zu einer weiteren Dämpfung des Signals. Für die THz-Kommunikation können viele gängige Baumaterialien nicht als glatte Oberflächen betrachtet werden; daher muss auch der Verlust aufgrund von Streuung an rauen Oberflächen berücksichtigt werden. Wenn die Antennen entlang des LOS-Pfades ausgerichtet sind, erfahren die reflektierten Pfade bei der drahtlosen THz-Kommunikation aufgrund der Winkelunterschiede deutlich geringere Gewinne, was die Unterschiede in den Signalstärken im Gegensatz zur drahtlosen Kommunikation deutlich erhöht. Daher sind die reflektierten Pfade in unseren Szenarien vernachlässigbar und wir betrachten nur den dominierenden LOS-Pfad. Die empfangenen Signalstärken von Bob P_B und Eve P_E sind dann

$$P_B = P_A G_A G_B \left(\frac{c_0}{4\pi f_c d_{AB}}\right)^2$$

$$P_E = P_A G_A G_E \left(\frac{c_0}{4\pi f_c d_{AE}} \right)^2$$

wobei P_A die mittlere Sendeleistung, G_A, G_B und G_E die entsprechenden Antennengewinne für Alice, Bob und Eve sind.

Die additiven Rauschterme N_{AB} und N_{AE} folgen einer Normalverteilung mit Mittelwert 0 und Rauschvarianzen $\sigma^2_{N_{AB}} = \sigma^2_{N_{AE}} = N$. Die Signal-zu-Rauschverhältnisse (SNR) für Bob und Eve ergeben sich damit zu

$$SNR_{AB} = \frac{P_B}{N} \text{ und } SNR_{AE} = \frac{P_E}{N}.$$

In einem MIMO System mit mehreren Sende- und Empfangsantennen gelten nun die oben aufgeführten Betrachtungen zwischen jeder Sende- und jeder Empfangsantenne.

2.2 Informationstheoretische Analyse

Basierend auf informationstheoretischen Grundlagen wurden in der Literatur mehrere Sicherheitskriterien definiert, unter anderem schwache und starke Sicherheit. In CERTAIN betrachten wir jedoch die sogenannte semantische Sicherheit, die das stärkste Sicherheitskriterium darstellt [1].

Wir bezeichnen die Dekodierfehlerwahrscheinlichkeit von Bob mit $\varphi \in [0, 1]$ und den semantischen Zielsicherheitslevel mit $\delta \in [0, 1]$. Die zu übertragende Nachricht sei M. Enc sei der Encoder mit einer möglichen Realisierung g und Dec ein entsprechender Dekodierer. Dann ist der semantische Sicherheitslevel gegeben durch

$$\left(Pr[Dec(Z^n) = Enc(M)] - Pr[g = Enc(M)] \right).$$

Es wurde gezeigt, dass ein semantischer Zielsicherheitslevel von δ impliziert, dass die mittlere Fehlerwahrscheinlichkeit von Eve gegeben ist als

$$\bar{e}_E \geq 1 - \delta - \frac{1}{2^b}$$

wenn Eve versucht, nur b Informationsbits der ursprünglichen Nachricht M zu rekonstruieren [2]. D.h. ein kleinerer Wert von δ impliziert eine höhere Sicherheit. Dies gibt uns eine operationelle Bedeutung von δ, so dass die praktischen Auswirkungen vom gewählten Sicherheitslevel klar ersichtlich sind.

Das Sicherheitskriterium der semantischen Sicherheit wurde für alle folgenden Betrachtungen angenommen. Die Sicherheitskapazität beschreibt dann die maximale Übertragungsrate, mit der Alice zu Bob fehlerfrei übertragen kann bei zeitgleichem Einhalten des gewählten Sicherheitslevels. Die Sicherheitskapazität für den SISO Fall, d.h. mit einer Sende- und einer Empfangsantenne ist gegeben durch

$$C_S = \left(1 + SNR_{AB}\right) - log_2\left(1 + SNR_{AE}\right)$$

während sich der MIMO Fall zu

$$C_S = \left[\det det\left(I + SNR_{AB}\right) - log_2 \det det\left(I + SNR_{AE}\right)\right]$$

ergibt. Die Maximierung über alle möglichen Sendestrategien, d.h. insbesondere des sogenannten Precodings am Sender.

Bei diesen Untersuchungen hat sich herausgestellt, dass insbesondere die Anzahl der Empfangsantennen am nicht-legitimierten Abhörer einen großen Einfluss haben. Mit steigender Anzahl von Empfangsantennen kann der Abhörer mehr Signalleistung vom Sender „aufsammeln“, welches sich sofort in einer Degradierung der informationstheoretisch maximal erreichbaren Übertragungsrate zwischen dem Sender und dem legitimierten Empfänger widerspiegelt. Dies ist ein völlig neues Verhalten, welches sich zum vorher betrachteten SISO-Fall mit nur einer Sende- und Empfangsantenne grundlegend unterscheidet. Im SISO-Fall ist die maximale Signalleistung, die der Abhörer „aufsammeln“ kann, durch den Kanal vom Sender zum Abhörer gegeben, während im MIMO-Fall der Abhörer die aufgesammelte Leistung durch mehrere Empfangsantennen weiter steigern kann.

2.3 Kanalunkenntnis und feindliche Attacken

Auf diesen gewonnenen Kenntnissen aufbauend lag der weitere Fokus auf die Untersuchung des Einflusses von Kanalunkenntnis und feindlichen Attacken. Es wurden informationstheoretische Modelle entwickelt, um diesen Einfluss zu charakterisieren und zu analysieren. Die folgende Abbildung visualisiert das gewählte Modell für die Kanalunkenntnis.

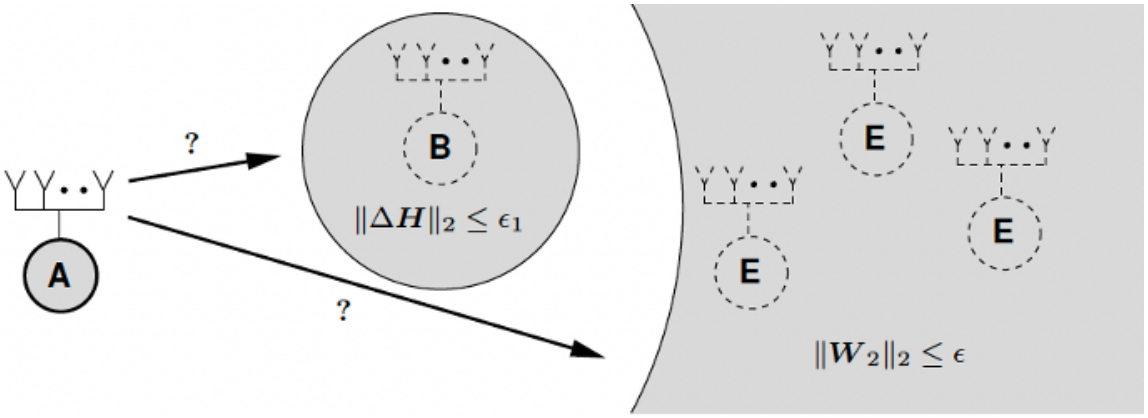

Abbildung 2: Modellierung von Kanalunkenntnis.

Hierbei wurde angenommen, dass der Kanal von Alice (A) zum legitimierten Empfänger Bob (B) einer additiven Unsicherheit unterliegt. Dies ist motiviert durch praktische Limitierungen, bei denen z.B. eine Kanalschätzung nur mit bestimmter Auflösung erfolgen kann, so dass um den geschätzten Kanal eine additive Unsicherheit / Ungenauigkeit bestehen bleibt. Die Kanalunsicherheit zu Eve (E) wurde wie folgt modelliert: Eve wird dem Sender keine Kanalkenntnisse (via Feedback etc.) mitteilen, so dass die Unsicherheit hier maximal ist. Wir können lediglich annehmen, dass Eve sich außerhalb einer gewissen (Schutz-)zone befindet, so dass die maximale Empfangsleistung für Eve durch einen gewissen Wert begrenzt ist. Insbesondere ist angenommen, dass der größte Eigenwert der Kanalmatrix den Wert nicht überschreitet. Diese Modellierung erlaubte es, weitere informationstheoretische Untersuchungen durchzuführen und informationstheoretische Größen, wie z.B. die Kapazität, zu charakterisieren.

Ist über die Art möglicher feindlicher Attacken, wie z.B. durch Jamming-Angriffe, nichts weiter bekannt, können diese ebenfalls durch das oben beschriebene Modell erfasst werden. Jamming-Angriffe auf die Kommunikation zwischen dem Sender und dem legitimierten Empfänger werden den Kanal ebenfalls in einer unbekannten Art und Weise stören, so sich der unbekannte, gestörte Kanal in der Umgebung des ursprünglich geschätzten Kanals befinden wird. Dies zeigt die Generalität und Anwendbarkeit des oben beschriebenen Modells auch für diesen Fall. Weitere, spezialisierte Attacken auf die legitimierte Kommunikation sollen im weiteren Verlauf des Projekts weiter untersucht werden.

Für Kanalunkenntnis und feindliche Attacken ist der Einfluss der Empfangsantennen am Abhörer noch signifikanter als im Fall der perfekten Kanalkenntnis. Eve kann mit steigender Anzahl von Empfangsantennen nicht nur mehr Sendeleistung aufsammeln, auch hat die Anzahl direkten Einfluss auf die Unsicherheitsregionen. Wie oben beschrieben ist die Unsicherheit über Eve dadurch modelliert, dass der größte Eigenwert der Kanalmatrix den Wert nicht überschreiten darf. Je mehr Empfangsantennen Eve jedoch hat, desto größer wird auch hier der Einfluss. Im schlimmsten Fall (worst case) sammelt Eve auf jeder Empfangsantenne den maximalen Wert von Signalleistung ein.

Diese ganzen Betrachtungen haben als Motivation gedient, robuste Codierungsverfahren zu analysieren und zu entwickeln mit dem Ziel, eine sichere Übertragung auch in diesen Fällen zu realisieren. Dies wird detailliert in den nächsten Abschnitten beschrieben und diskutiert.

2.4 Codierungsvefahren basierend auf Techniken des maschinellen Lernens

Kanalcodierung ist entscheidend für die zuverlässige Übertragung von Nachrichten über störungsbehaftete oder nichtlineare Medien wie Luft oder optische Fasern. Praktische Kanalcodes zielen darauf ab, gesendete Nachrichten mit geringer Komplexität und niedriger Blockfehlerrate (BLER) bei vorgegebenen Code-Raten und Blocklängen wiederherzustellen [3,4]. Obwohl es kapazitätsnahe Codes wie Polarcodes [5] für bestimmte Kanäle gibt, erfordert das praktische Code-Design Anpassungen an verschiedene Blocklängen, Raten, Kanalparameter und Komplexitätsbeschränkungen.

Tiefe neuronale Netzwerke wurden als alternative Encoder-Decoder-Paare für die Fehlerkorrektur vorgeschlagen [6,7,8,9] um das Code-Design zu automatisieren, Anpassungen an Kanalmodelländerungen zu ermöglichen und BLER und Komplexität gegenüber klassischen Codes zu verbessern. Allerdings wird das Training neuronaler Codes für große Blocklängen aufgrund des exponentiellen Anstiegs der Anzahl von Codewörtern und der erforderlichen Größe der Netzwerke unpraktisch [6].

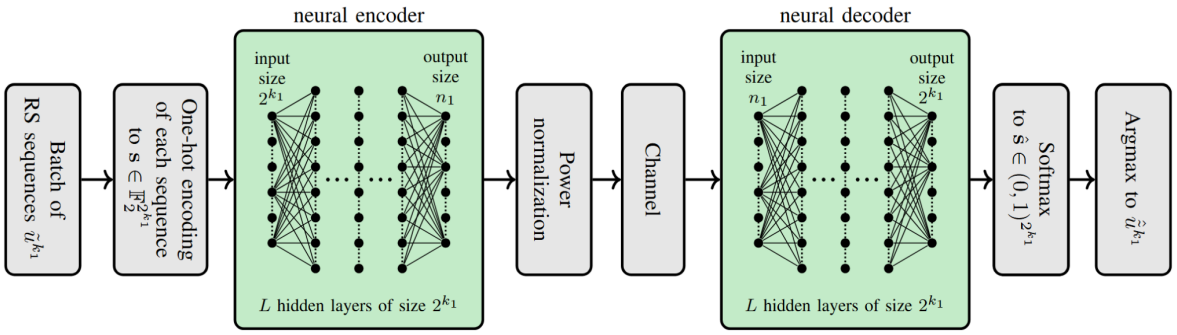

Abbildung 3: Vorgeschlagene Codestruktur.

Um diese Herausforderungen zu bewältigen, haben wir ein Konkatinationsschema vorgeschlagen, das die Code Dimension neuronaler Codes erweitert und gleichzeitig praktikabel bleibt. Durch die Verkettung eines inneren neuronalen Codes mit einem äußeren klassischen Code, insbesondere einem Reed-Solomon (RS) Code, können wir größere Blocklängen erreichen, ohne die Komplexität erheblich zu erhöhen. Dieser Ansatz nutzt die Vorteile sowohl neuronaler als auch klassischer Codes und führt zu verbesserten BLER-Leistungen und einer höheren Robustheit gegenüber Kanalmodelländerungen. Jedes Symbol des RS-Codeworts, repräsentiert durch $\log_2(q) = k_1$bits, wird unter One-Hot-Encoding in dasselbe neuronale Netzwerk eingespeist, wodurch das Netzwerk effektiv mehrfach genutzt wird. Das bildet einen verketteten Code mit Blocklänge $n = n_2 * n_1$ und Code Dimension $k = k_2 * \log_2(q)$, wobei n_2,k_2 die Parameter des äußeren RS-Codes über F_q sind und n_1,k_1 die Parameter des inneren neuronalen Codes. Der innere neuronale Encoder ordnet den One-Hot-kodierten Eingabevektor $s \in F_2^{2^{k_1}}$ einem Ausgangssymbol $\tilde{x} \in R^{n_1}$ zu, mittels einer parametrischen Funktion f_θ. Diese Funktion besteht aus einer Sequenz von affinen Transformationen und nichtlinearen Aktivierungsfunktionen und bildet ein neuronales Netzwerk mit den Parametern θ. Der neuronale Decoder g_θ ist ähnlich aufgebaut und liefert Werte, die durch eine Softmax-Aktivierungsfunktion als Wahrscheinlichkeiten interpretiert werden können. Wie schon angemerkt, verwenden wir One-Hot-Encoding und die kategoriale Kreuzentropieverlustfunktion, die sich auf die Minimierung der Blockfehlerrate statt der Bitfehlerrate konzentriert, um die neuronalen Netzwerke zu trainieren. Das ist vorteilhaft, da es die Optimierung mit dem Ziel der Fehlerkorrektur auf Blocks anpasst, also die Wahrscheinlichkeit von Nachrichten-Decodierungsfehlern in Blocks zu minimieren. Das steht im Kontrast zu anderen Ansätzen, welche die Binärentropieverlustfunktionen verwenden, bei der das neuronale Netz so optimiert wird das nur die Bitfehlerrate minimiert wird und nicht die Blockfehlerrate. Ein weiterer Vorteil unseres Ansatzes ist, dass wir einen Schwellenwert für Konfidenzwerte für die Wahrscheinlichkeit eines bestimmten dekodierten Symbols definieren können. Dies erfolgt über die Softmax Funktion, und wir können so Symbole identifizieren, die so unzuverlässig sind, i.e. den Wahrscheinlichkeitsschwellwert unterschreiten, dass der äußere RS Code sie als Auslöschung behandelt. Dies ermöglicht es uns, die Fehlerkorrektur sowie die Auslöschkorrekturfähigkeiten von RS-Codes zu nutzen und somit die Gesamtfehlerleistung weiter zu verbessern.

Wir haben Simulationen durchgeführt, um die Leistung der verketteten klassischen und

neuronalen (CCN) Codes zu bewerten. Wir verglichen einen Standard-Autoencoder (AE) neuronalen (7,4) Code mit unseren CCN-Codes, die unter Verwendung eines äußeren RS-Codes und eines inneren neuronalen Codes konstruiert wurden. Durch die Verkettung eines äußeren (255,223) RS-Codes über F_{2^8} mit einem inneren neuronalen (12,8) Code erreichten wir einen (225*12,223*8) CCN-Code mit einer ungefähren Code-Rate von $R \approx 0,583$, ähnlich dem Referenzcode. Die BLER-Leistung dieses CCN-Codes über einem AWGN Kanal zeigte erhebliche Verbesserungen gegenüber dem kleinen neuronalen Code.

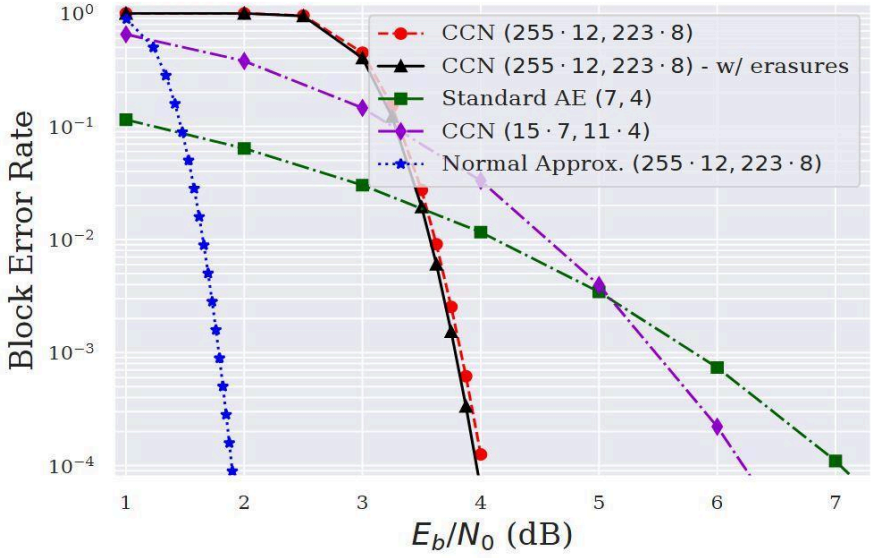

Abbildung 4: BLER-Vergleich für den AWGN-Kanal zwischen dem CCN-Code und dem Referenzcode.

Abbildung 4 zeigt die BLER-Leistung der CCN-Codes im Vergleich zum Referenzcode. Bei einer BLER von 10^{-4} erzielt der CCN-Code einen E_b/N_o-Gewinn von etwa 3,1 dB gegenüber dem Referenzcode. Darüber hinaus bietet die Verwendung von Symbol-Auslöschungschwellwerten im Output des neuronalen Decoders, kombiniert mit einem RS-Decoder für Fehler und Auslöschungen, zusätzliche Leistungsgewinne.

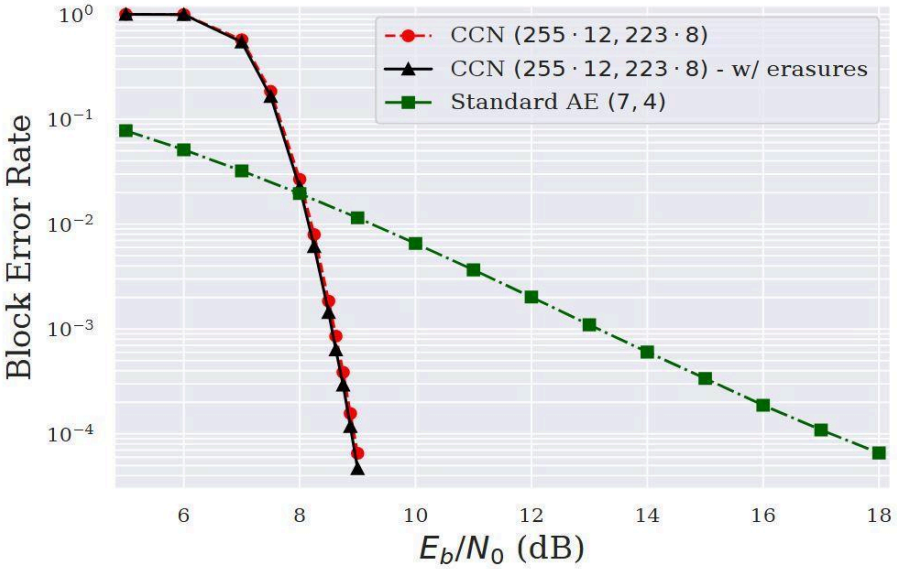

Abbildung 5: Simulation im Rayleigh Kanal-Modell.

Wir haben auch die Robustheit der CCN-Codes gegenüber Kanalmodelländerungen untersucht, indem wir die Codes über einen Rayleigh-Fading-Kanal und einen Burst-Kanal simulierten. Für den Rayleigh Kanal nahmen wir einen Block power constraint an und weiterhin, dass keine Kanalzustandsinformationen bei den neuronalen Encoder und Dekoder bekannt sind. Die CCN-Codes, die ursprünglich für den AWGN-Kanal trainiert wurden, zeigten auch in diesem Szenario erhebliche Leistungsverbesserungen gegenüber dem Referenzcode. Bei einer BLER von 10^{-4} wurde ein E_b/N_0-Gewinn von etwa 8,3 dB erzielt. Dies zeigt die Fähigkeit der CCN-Codes, sich an veränderte Kanalbedingungen anzupassen.

Zusätzlich haben wir einen Burst-Kanal modelliert, um die Auswirkungen von zeitlich korrelierten Fehlern zu untersuchen. Dies ist besonders wichtig für Anwendungen, bei denen Fehler in Clustern auftreten können, wie z. B. in drahtlosen Netzwerken mit Interferenzen. Die CCN-Codes bewiesen eine hohe Robustheit gegenüber Burst-Fehlern und übertrafen den Referenzcode signifikant mit einem 6,1 dB E_b/N_0 Gewinn.

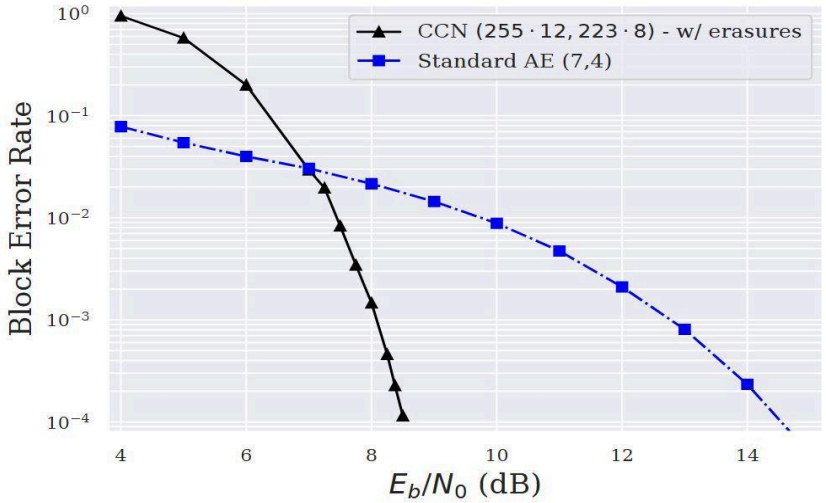

Abbildung 6 :Simulation im Burst-Kanal-Modell.

3. Fazit und Ausblick

Im Rahmen des Projekts CERTAIN ist es gelungen, Physical-Layer-Security Verfahren für THz-MIMO-Kommunikationssysteme zu entwerfen, informationstheoretisch zu bewerten, algorithmisch zu implementieren und abschließend mittels eines THz-MIMO-Wiretap-Demonstrators experimentell zu validieren.

Das Projekt ist aus Sicht der TUD erfolgreich verlaufen. Die durchgeführten Forschungsarbeiten im Teilvorhaben erforderten die im Projektantrag abgeschätzten Ressourcenaufwände und es konnten alle wesentlichen Aufgaben des Arbeitsplans erfolgreich bearbeitet werden. Die Ressourcenplanung und -aufwände waren in vollem Umfang angemessen, da die Arbeiten mit weniger Ressourcen sowohl im Umfang als auch im gesteckten Zeitrahmen ansonsten nicht erfolgreich durchgeführt hätten werden können.

Im Rahmen von CERTAIN trug die TU Dresden dazu bei, die Sichtbarkeit der Forschungsergebnisse durch Publikationen zu erhöhen. Damit geht auch eine Stärkung von Dresden und Sachsen als Forschungsstandardort einher. Die Ergebnisse und aufgebaute Expertise haben wichtige Impulse und Einflüsse auf Nachfolgeaktivitäten gegeben. Hierbei sind insbesondere die vom BMBF geförderten Projekte 6G-ANNA (16KISK103) und 6G-life (16KISK001K) zu nennen.

CERTAIN konnte in allen geplanten Punkten erfolgreich abgeschlossen werden.

Referenzen

[1] M. Bellare, S. Tessaro, and A. Vardy, „Semantic Security fort he Wiretap Channel," in *Advances in Cryptology*, Springer, Aug. 2012, pp. 294-311.

[2] Z. Utkovski, P. Agostini, M. Frey, I. Bjelakovic, and S. Stanczak, „Learning Radio Maps for Physical-Layer Security in the Radio Access," in *Proc. IEEE International Workshop on Signal Processing Advances in Wireless Communications*, Cannes, France, July 2019, pp. 1-5.

[3] S.Lin and D. J. Costello, „*Error Control Coding,*" Pearson, 2nd edition, 2004.

[4] R. G. Gallager, „*Information Theory and Reliable Communication*," John Wiley & Sons, 1968.

[5] E. Arikan, „Channel Polarization: A Method for Constructing Capacity-Achieving Code for Symmetric Binary-Input Memoryless Channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051-3073, July 2009.

[6] M. V. Jamali, H. Saber, H. Hatami, and J. H. Bae, „ProductAE: Toward Training Larger Channel Codes Based on Neural Product Codes," in *Proc. IEEE International Conference on Communications*, Seoul, Republic of Korea, 2022, p. 3898-3903.

[7] Y. Jiang et al., „Turbo Autoencoder: Deep Learning Based Channel Codes for Point-to-Point Communication Channels," in *Advances in Neural Infomation Processing Systems*, vol. 32, 2019.

[8] A. V. Makkuva et al., „Ko Codes: Inventing Nonlinear Encoding and Decoding for Reliable Wireless Communication via Deep-Learning," in *International Conference on Machine Learning*, PMLR, 2021.

[9] S. Cammerer et al., „Trainable Communication Systems: Concepts and Prototype," *IEEE Transactions on Communications*, vol. 68, no. 9, pp. 5489-5503, Sep. 2020.

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Kurzbericht CERTAIN

1. Hauptziel des Projektes

Das übergeordnete Vorhabenziel des Projekts *Code-basierte Physical-Layer Security für Terahertz-MIMO-Kommunikation (CERTAIN)* besteht darin, ausgehend von einer fundierten informationstheoretischen Basis Physical-Layer-Security (PLS) Sicherheitsverfahren für THz Multiple Input Multiple Output (MIMO) Kommunikationssysteme im Internet of Things (IoT) Kontext zu entwerfen und informationstheoretisch zu bewerten, konkret algorithmisch zu implementieren und numerisch zu analysieren, und schließlich im Rahmen von THz-Kanalmessungen und THz-MIMO-Wiretap-Demonstratoren experimentell zu validieren.

2. Ablauf

In CERTAIN wurde ein abhörsicheres, drahtloses PLS-THz-MIMO-Übertragungskonzept basierend auf informationstheoretischen Erkenntnissen entworfen und schließlich in einem praktischen Demonstrator umgesetzt. Dazu wurde in CERTAIN ein fundiertes THz-MIMO-Kanalmodell entwickelt und informationstheoretisch analysiert. Dieses Kanalmodell ermöglichte es, Verfahren für Sicherheit auf der physikalischen Schicht durch Kombination von Methoden der codierten Modulation und sendeseitiger Vorverarbeitung zur Ansteuerung der Elemente des MIMO-Antennenarrays für die Übertragung im THz-Bereich gezielt zu entwickeln. Abschließend wurde eine praktische Implementierung und experimentelle Validierung mittels THz-Wiretap-Demonstrator durchgeführt. Dadurch schlägt CERTAIN eine innovative Brücke von theoretischen Grundlagen-Erkenntnissen zu PLS für den THz-MIMO-Kanal über praktisch realisierbare und ressourcenarm implementierbare Codier-/Verarbeitungsverfahren hin zu einem Echtzeit-Wiretap-Demonstrator.

Die TU Dresden war federführend im ersten Teil der Arbeiten und hat schwerpunktmäßig das THZ-MIMO-Kanalmodell für die sichere Übertragung entwickelt und informationstheoretisch analysiert. Die gewonnenen Erkenntnisse und Ergebnisse haben die Entwicklung von PLS-Verfahren im zweiten Teil erlaubt, welche schließlich die Entwicklung eines entsprechenden Demonstrators ermöglicht haben. Die TU Dresden war in diesen Teilen ebenfalls involviert, federführend wurden diese Aktivitäten aber von der Uni Ulm bzw. dem Fraunhofer HHI vorangetrieben.

Die Projektlaufzeit erstreckte sich vom 01.10.2020 bis zum 31.12.2023. Gegenüber der ursprünglichen Zeitplanung, d.h. der Realisierung der oben genannten Aktivitäten innerhalb von 36 Monaten, wurde in erster Linie aufgrund von Verzögerungen in der ersten Phase des Projekts bei der Entwicklung des Kanalmodells und der informationstheoretischen Analyse die Gesamtprojektlaufzeit um drei Monate bis Ende Dezember 2023 verlängert.

3. Wesentliche Ergebnisse

Ein Konkatinationsschema wurde vorgeschlagen, das die Code Dimension neuronaler Codes erweitert und gleichzeitig praktikabel bleibt. Das System besteht aus einer Verkettung eines inneren neuronalen Codes mit einem äußeren klassischen Code, insbesondere einem Reed-Solomon (RS) Code und ermöglicht größere Blocklängen, ohne die Komplexität erheblich zu erhöhen. Das Verfahren wurde umfassend informationstheoretisch analysiert. Die Vorteile neuronaler als auch klassischer Codes können so genutzt werden, im Ergebnis erhält man verbesserte BLER-Leistungen und höhere Robustheit gegenüber Kanalmodelländerungen. Abschließend wurde das Verfahren implementiert und konnte mittels eines THz-MIMO-Wiretap-Demonstrators experimentell validiert werden.

Die im Rahmen von CERTAIN erzielten Ergebnisse und die aufgebaute Expertise haben wichtige Impulse und Einflüsse auf Nachfolgeaktivitäten gegeben. Hierbei sind insbesondere

die vom BMBF geförderten Projekte 6G-ANNA (16KISK103) und 6G-life (16KISK001K) zu nennen.

Das Projekt ist aus Sicht der TUD erfolgreich verlaufen. Es konnten alle wesentlichen Aufgaben des Arbeitsplans erfolgreich bearbeitet werden. Die Ressourcenplanung und -aufwände waren angemessen, die Arbeiten hätten mit weniger Ressourcen sowohl im Umfang als auch im Zeitrahmen nicht erfolgreich durchgeführt werden können.

Seit Projektstart erfolgte Veröffentlichungen und Patentanmeldungen:

Journalartikel

[1] A. Bereyhi, S. Asaad, R. R. Müller, R. F. Schaefer, G. Fischer, and H. V. Poor, “Securing Massive MIMO Systems: Secrecy for Free with Low-Complexity Architectures,” *IEEE Transactions on Wireless Communications*, vol. 20, no. 9, pp. 5831-5845, Sep. 2021.

[2] M. Bloch, O. Günlü, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer, “An Overview of Information-Theoretic Security and Privacy: Metrics, Limits and Applications,” *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 1, pp. 5-22, Mar. 2021.

[3] S. Asaad, Y. Wu, A. Bereyhi, R. R. Müller, R. F. Schaefer, and H. V. Poor, “Secure Active and Passive Beamforming in IRS-Aided MIMO Systems,” *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1300-1315, 2022.

Konferenzveröffentlichungen

[4] S. Asaad, Y. Wu, A. Bereyhi, R. R. Müller, R. F. Schaefer, and H. V. Poor, “Joint Active and Passive Secure Precoding in IRS-Aided MIMO Systems,” in *Proc. IEEE Global Communications Conference*, Madrid, Spain, Dec. 2021, pp. 1-6.

[5] R. Schulz, O. Günlü, R. Elschner, R. F. Schaefer, C. Schmidt-Langhorst, C. Schubert, and R. F. H. Fischer, “Semantic Security for Indoor THz-Wireless Communication,” in *Proc. 17th International Symposium on Wireless Communication Systems*, Berlin, Germany, Sep. 2021, pp. 1-6.

[6] A. Bereyhi, S. Asaad, C. Ouyang, R. R. Müller, R. F. Schaefer, and H. V. Poor, “How Should IRSs Scale to Harden Multi-Antenna Channels?,” in *Proc. IEEE Sensor Array and Multichannel Signal Processing Workshop*, Trondheim, Norway, June 2021, pp. 276-280.

[7] O. Günlü, M. Bloch, R. F. Schaefer, and A. Yener, “Secure Joint Communication and Sensing,” in *Proc. IEEE International Symposium on Information Theory*, Espoo, Finland, June 2022, pp. 844-849.

[8] O. Günlü, M. Bloch, R. F. Schaefer, and A. Yener, “Secure Integrated Sensing and Communication for Binary Input Additive White Gaussian Noise Channels,” in *Proc. IEEE 3rd international Symposium on Joint Communications & Sensing*, Seefeld, Austria, Mar. 2023, pp. 1-6.

[9] O. Günlü, R. Fritschek, and R. F. Schaefer, “Concatenated Classic and Neural (CCN) Codes: ConcatenatedAE,” in *IEEE Wireless Communications and Networking Conference*, Glasgow, United Kingdom, Mar. 2023, pp. 1-6.

Patentanmeldungen

[10] O. Günlü, R. Fritschek , and R. F. Schaefer, “*Methods and systems for data transfer via a communication channel,”* LU502737B1 (filed 2022, granted 2024), EP4333310A1 (filed 2023).