D. Reinhardt, H. Langweg, B.C. Witt, M. Fischer et al. (Hrsg.): Sicherheit 2020,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Göttingen 2020 41

Passive Angriffe auf kanalbasierten Schlüsselaustausch

Kompromittierung der Zufallsquelle unter Verwendung deterministischer Kanalmodelle

Paul Walther, Rober Knauer, Thorsten Strufe [1]

Abstract: Im Bereich der Physical Layer Security stellt der Schlüsselaustausch auf Basis von Kanalreziprozität eine effiziente Methode der Schlüsselaushandlung dar. Eine zentrale Annahme ist, dass die gemessenen Kanaleigenschaften ein geteiltes Geheimnis darstellen, worauf die Schlüsselgenerierung basiert. In dieser Arbeit wird diese Grundannahme angegriffen, in dem mit Hilfe von deterministischen Kanalmodellen und dem Wissen über Raumgeometrie und Terminalpositionen diese Kanaleigenschaften approximiert werden. Es wird eine Methodik entwickelt, um derartige Angriffe zu bewerten und auf Basis des *Kunisch-Pamp* Modells werden Approximationen durchgeführt. Die Resultate zeigen, dass die rekonstruierten Kanaleigenschaften trotz nicht-optimaler Voraussetzung sehr stark mit den tatsächlichen korrelieren und dies einen validen Angriffsvektor darstellt.

Keywords: Schlüsselaustausch; PhySec; Angriff; CRKG

1 Einleitung

Physical Layer Security (PhySec) stellt energieeffizient kryptographische Primitive bereit, deren Sicherheit informationstheoretisch beweisbar ist [BB11]. Ausgehend von Ahlswedes Quellenmodell [AC93] ist der Schlüsselaustausch, basierend auf Kanalreziprozität (Channel Reciprocity based Key Generation, CRKG), ein Primitiv zur Ableitung symmetrischer Schlüssel. Hierbei wird der reziproke Funkkanal zwischen zwei Kommunikationsteilnehmern als gemeinsame Entropiequelle für die Schlüsselgenerierung verwendet. Eine der Grundannahmen dieses Prozesses ist, dass die charakteristischen Eigenschaften dieses reziproken Kanals bereits ein geteiltes Geheimnis darstellen: basierend auf Jakes Streuungstheorem wird davon ausgegangen, dass alle weiteren Funkterminals, die weiter als eine halbe Wellenlänge entfernt sind, abweichende Kanalcharakteristika messen und damit keine Informationen erhalten, die ihnen helfen können, den generierten Schlüssel zu erraten.

Orthogonal dazu wurden durch umfangreicher Messstudien und Analysen immer exaktere und leistungsfähigere Kanalmodelle für Funkkanäle entwickelt, z.B. das IEEE Ultraweitband Modell [MFP03] oder das Modell von Kunisch und Pamp [KP02].

[1] TU Dresden, Datenschutz und Datensicherheit, {vorname.nachname}@tu-dresden.de
Diese Arbeit wurde mit Unterstützung des Bundesministerium für Bildung und Forschung (BMBF) im Rahmen des Projektes "5G NetMobil"(Förderkennzeichen: 16KIS0689) erstellt.

doi:10.18420/sicherheit2020_03

In der vorliegenden Arbeit werden diese beiden Felder zusammengeführt und daraus ein Angriff auf CRKG entwickelt. Basierend auf Messungen im Vorfeld und Kenntnissen über die Raumgeometrie und aktuellen Terminalpositionen während des Schlüsselaustausches werden mit Hilfe des deterministischen Kanalmodells von Kunisch und Pamp die Charakteristika des Funkkanals zwischen legitimen Kommunikationspartnern rekonstruiert und damit die Kanalimpulsantworten zwischen beiden Parteien geschätzt. Basierend auf einer hinreichend genauen Rekonstruktion kann ein Angreifer die Schlüsselgenerierung parallel ausführen und potentiell den gleichen Schlüssel ableiten.

Die Resultate zeigen, dass das gewählte Kanalmodell in der Lage ist Kanaleigenschaften zu rekonstruieren, die denen des legitimen Kanals ähnlich sind. Dadurch stellt dieser Ansatz einen validen Angriffsvektor dar.

Es werden die folgenden Beiträge gemacht:

- Vorstellung eines Angriffsansatzes basierend auf deterministischen Kanalmodellen
- Entwicklung einer geeigneten Methodik zur Bewertung eines derartigen Angriffs
- Umsetzung und Analyse des Konzept auf Basis des *Kunisch-Pamp* Kanalmodells

Abschnitt 2 gibt aktuelle Angriffskonzepte zu CRKG wieder. In Abschnitt 3 werden das System- und das Angreifermodell beschrieben. Abschnitt 4 beschreibt die entwickelte Methodik und Abschnitt 5 legt die Realisierung und erreichten Resultate dar. Abschließend fasst Abschnitt 6 zusammen und gibt einen Ausblick auf weitere Fragen.

2 Stand der Wissenschaft

CRKG unterliegen einige sehr starke Systemannahmen, was zu einer Vielzahl darauf in der Literatur vorgeschlagener passiver, wie aktiver Angriffe geführt hat. Die folgende Auswahl beschreibt die Kernideen, die die Grundlagen der unterschiedlichen Angriffe bilden.

In [EKY11] stellten die Autoren in Frage, ob die Kanaleigenschaft mit steigender Entfernung tatsächlich dekorrelieren. Hierbei konnten nicht vernachlässigbare Korrelationen selbst bei Entfernungen von mehreren Wellenlängen festgestellt werden. Die Autoren entwickeln daraus jedoch keinen erfolgreichen Angriff. Döttling et al. schlugen einen sogenannten *reradiation side-channel attack* vor [Dö10]. Da diesem Angriff zahlreiche und mitunter gleichfalls starke Annahmen zu Grunde liegen, welche in lediglich vereinfachten Szenarien überprüft wurden, erscheint dieses Szenario wenig praxisrelevant. In [Ja09] wurden die Veränderungen von RSSI-Werten in diversen statischen und dynamischen Szenarien untersucht. Sie zeigen, dass in statischen Umgebungen die Varianz der Messwerte sehr gering ist, was darauf schließen ließe, dass Approximationen praktisch möglich wären.

Bezüglich aktiven Angriffen ist die Arbeit [JZ15] von Jin und Jeng erwähnenswert: durch die Injektion von bekannten Signalen in den Messvorgang sollten die Eingangswerte der Schlüsselgenerierung manipuliert werden. In [Eb12] wurde dieser Ansatz erweitert, so dass

entweder bekannte Signale zur Schlüsselgenerierung genutzt wurden oder der Austausch behindert wurde. Beide Angriffe sind aktiver Natur und betrachten ausschließlich RSSI-Werte. Kürzliche Arbeiten schlagen für CRKG die Nutzung der Kanalimpusantworten vor, die strikt mehr Information – und dem Vernehmen nach mehr Entropie als RSSI-Werte enthalten. Die hier vorgestellten Angriffe lassen sich auf diese Schlüsselgenerierung also nicht anwenden.

3 Systemmodell und Angreifermodell

Das **Systemmodell** geht von Innenraum-Funkkommunikation im Ultraweitband (UWB) Bereich aus. Die Kanaleigenschaften werden in Form von Kanalimpulsantworten (Channel Impuls Response - CIR) aufgezeichnet, wobei die charakteristischen Eigenschaften durch die im UWB deutlichen Mehrwegekomponenten bereitgestellt werden.

Dem **Angreifermodell** liegt ein praktisch orientierter Ablauf des Angriffes zugrunde, was zwei unterschiedliche Phasen definiert, in denen sich der Angreifer unterschiedlich verhält. Die Grundidee des Angriff kann folgendermaßen beschrieben werden:

Phase 1 - Vorbereitung Ein lokaler Angreifer kann in dem Raum, in dem die zukünftige Kommunikation des Schlüsselaustausches stattfinden wird, beliebige aktive Messungen vornehmen, z.B. bzgl. der Raumgeometrie oder Referenzmessungen von Kanalimpulsantworten mit bekannten Terminalpositionen.
Auf Basis dieser Messungen wird eine repräsentative Darstellung des Funkkanals durch den Angreifer entwickelt.

Phase 2 - Angriff Während des eigentlichen Angriffs auf die Zufallsquelle der Schlüsselgenerierung werden die Informationen aus der Vorbereitung mit denen der aktuellen Kommunikation kombiniert, um die Schlüsselgenerierung zu kompromittieren. Hierzu muss sich der Angreifer nicht in der Nähe befinden und theoretisch weder aktiv noch passiv mit den berechtigten Kommunikationspartner interagieren . Auf Basis der in Phase 1 gewonnen Repräsentation wird versucht die Messwerte der legitimen Kommunikationspartner zu rekonstruieren. Im Übrigen wird davon ausgegangen, dass außer den Positionen der Terminals keine weiteren Informationen vorliegen.

Beide Phasen sind in der Praxis problemlos realisierbar, wobei der Angreifer über keinerlei besondere Ressourcen bzgl. verwendeter Technik, Rechenaufwand oder Zeit verfügen muss. Vor allem die zweite Phase stellt besonders wenig Anforderungen an den Angreifer, da Positionsdaten einfach erhoben werden können (z.B. physische Nähe oder auch visuell durch Fenster oder Überwachungskameras).

Aus praktischer Sicht wäre es natürlich sinnvoll, Daten aufzuzeichnen, die mit diesem Schlüssel verarbeitet wurden, um ein höher gelegenes Ziel des Angreifers zu realisieren. Für die vorliegenden Angriff auf den Schlüsselaustausch ist das aber nicht notwendig.

4 Methodik

Methodisch muss zwischen zwei Komponenten unterschieden werden: zu einem ist relevant, welches **Kanalmodell** der Angreifer verwendet und zum anderen mit welcher **Metrik** der Erfolg des jeweiligen Modells gemessen wird.

Kanalmodell Hauptkriterium der Modellwahl ist der Determinismus des Modells, damit aus bekannten Positionen bidirektional eindeutige CIRs berechnet werden können. Daher sind bekannte randomisierte Kanalmodelle, wie das Saleh-Valenzuela Modell [SV87] oder das IEEE UWB Channel Model [MFP03] für den vorliegenden Fall ungeeignet.

Im Bereich der deterministischen Kanalmodelle hat sich das Modell von Kunisch und Pamp bewährt [KP02]. Da es primär für die Beschreibung von Funkkanälen in Gebäuden entworfen wurde, entspricht es genau dem verwendeten Systemmodell.

Das *Kunisch-Pamp*-Modell hat eine Vielzahl an Parametern — die Wichtigsten für den vorliegende Fall sind die Geometrie des Raumes und die Positionen der Funkterminals. Laut Angreifermodell ist die Raumgeometrie bekannt, so dass die Terminalpositionen die einzigen freien Simulationsparameter sind. Die weiteren Modellparameter werden entweder festgelegt oder an Hand von Messungen optimiert. Eine wichtige Einschränkung ist, dass dieses Modell in der gegenwärtigen Realisierung nur rechteckige Räume unterstützt.

Metriken Um die rekonstruierten Kanaleigenschaften mit den gemessenen zu vergleichen, muss eine Metrik mit folgenden Eigenschaften gefunden werden:

Hohe Trennschärfe Die Hauptaufgabe der Metrik ist eine klare Unterscheidung zwischen “ähnlichen” und “unähnlichen” Kanalimpulsantworten. Die CIRs für gleiche Positionen sollten also einen hohen Wert dieser Metrik erzielen, während CIRs an unterschiedliche Positionen niedrige Werte erzielen sollten.

Normalisierung Laut den Annahmen von CRKG sind die reziproken Eigenschaften von Kanalimpulsantworten die einzelnen Mehrwegecluster und deren Eigenschaften [Ja09]. Explizit ausgeschlossen wird die absolute Stärke der Impulsantwort, die variieren kann. Daher sollten Unterschiede in den absoluten Werten ignoriert, besser noch kompensiert werden.

Zeitsynchronität Da die lokalen Terminals nicht zeitlich synchronisiert sind, muss die verwendete Metrik robust gegenüber zeitlichen Verschiebungen sein.

Die Haupteigenschaft hierbei ist eine hohe Trennschärfe der Metrik, da dies das Hauptziel ist. Die beiden weiteren Eigenschaften sind grundsätzlich durch zusätzliche Vorverarbeitungsschritte erreichbar — da zusätzliche Verarbeitungsschritte im Sinne von Komplexitätsreduktion und Fehleranfälligkeit nicht optimal sind, ist eine Metrik, die diese Eigenschaften implizit hat, zu bevorzugen.

Durch die Grundidee des Signalvergleichs bieten sich für diese Metrik besonders an:

Mean Squared Error Der klassische MSE [SS07] ist weder robust gegen Unterschiede der Verstärkung noch gegen zeitliche Verschiebung. Daher wird die in [MBS98] vorgestellte Variante verwendet, die normalisiert:

$$m_1(g,h) = \min_{\beta} \frac{\|\vec{g} - \beta\vec{h}\|^2}{\|\vec{g}\|^2} = 1 - \left(\frac{\vec{g}^T \vec{h}}{\|\vec{g}\|\|\vec{h}\|} \right)^2$$

Korrelationskoeffizient Für den vorliegenden Fall ist der Korrelationkoeffizient definiert als

$$m_2(g,h) = \frac{\sum_{k=0}^{N-1} g[k]h[k] - N\bar{g}\bar{h}}{\sqrt{\sum_{k=0}^{N-1}(g[k]-\bar{g})^2 \sum_{k=0}^{N-1}(h[k]-\bar{h})^2}}$$

mit

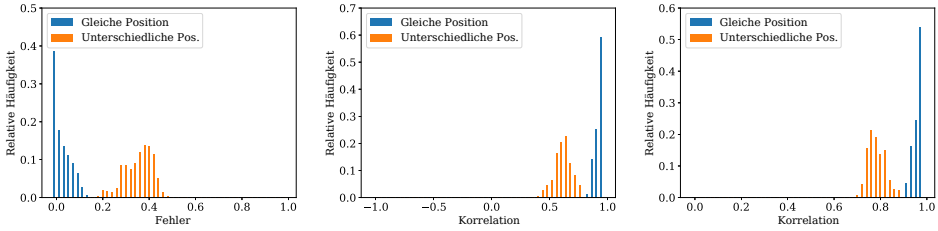
$$\bar{g} = \frac{1}{N}\sum_{k=0}^{N-1} g[k] \qquad \bar{h} = \frac{1}{N}\sum_{k=0}^{N-1} h[k]$$

Er ist normalisierend, aber anfällig für zeitliche Verschiebungen.

Kreuzkorrelation Wird die klassische Kreuzkorrelation (siehe [Mi16, p. 393]) auf Basis der Energien der Impulsantworten normalisiert, dann stellt deren Maximum eine Metrik dar, die sowohl normalisierend als auch robust gegen zeitliche Verschiebungen ist.

$$m_3(g,h) = \max_k \frac{r_{gh}(k)}{\sqrt{E_g E_h}} = \max_k \frac{\sum_{i=-\infty}^{\infty} g[i]h[i-k]}{\sqrt{\sum_{i=0}^{n_g-1} g[i]^2 \sum_{i=0}^{n_h-1} h[i]^2}}$$

Als Voruntersuchung wurden diese 3 Metriken auf alle in Kapitel 5.1 beschriebenen Messungen angewandt, um deren Eigenschaften zu untersuchen. Die Abbildung 1 zeigt die unterschiedlichen Metriken angewandt auf die verfügbaren Kanalimpulsantworten.



(a) m_1 : Mean Squared Error (b) m_2 : Korrelationskoeffizient (c) m_3 : Kreuzkorrelation

Abb. 1: Resultate der verschiedenen Metriken m_1, m_2 und m_3.

Aus der Abbildung 1 ist ersichtlich, dass alle drei Metriken die notwendige Trennung erreichen. m_1 und m_2 mussten hierfür zusätzlich bzgl. der zeitlichen Verschiebung der

einzelnen Realisierungen optimiert werden. Das heißt, dass m_3 bei geringem algorithmischen Aufwand die gleiche Trennschärfe erreicht. Tabelle 1 fasst diese Eigenschaften zusammen.

Metrik	Trennung	Normalisierung	Synchronisation
m_1: MSE	ja, mit Vorverarbeitung	ja	nein
m_2: Korrelationkoeffizient	ja, mit Vorverarbeitung	ja	nein
m_3: Kreuzkorrelation	ja	ja	ja

Tab. 1: Eigenschaften der betrachteten Metriken

Auf Basis dieser Voruntersuchung wird für die Evaluation die Metrik m_3 basierend auf der Kreuzkorrelation verwendet.

5 Umsetzung und Resultate

Nachfolgend werden die Realisierungen des Angriffes und die erzielten Resultate dargelegt.

5.1 Messungen

Um die praktische Realisierbarkeit des Angriffs zu zeigen und die dabei erzielbaren Resultate zu analysieren, wurden dem Systemmodell folgend umfassende Messungen von UWB Kanalimpulsantworten vorgenommen. Um für den Innenraum typische Messwerte zu generieren, wurden die Messungen in einem Büroraum durchgeführt. Der Raum und die entsprechenden Terminalposition sind in Abbildung 2 abgebildet.

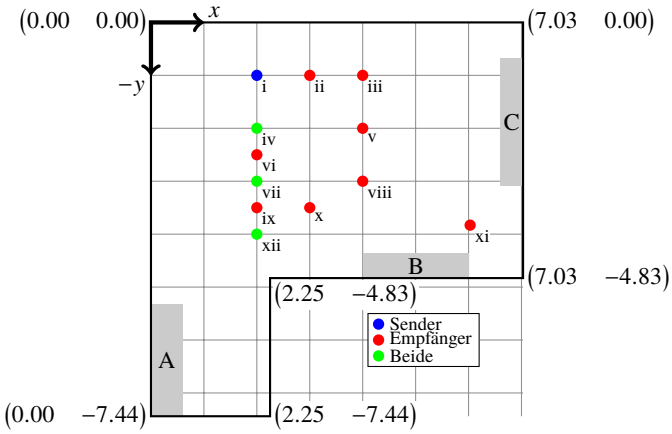


Abb. 2: Die Messumgebung mit der Raumgeometrie, den Terminalpositionen i–xii und den Hindernissen A–C. Alle Koordinaten in Metern.

Für die in Tabelle 2 aufgelisteten Kombinationen von Terminalpostionen wurden jeweils zwischen 1014 und 1112 Kanalimpulsantworten aufgezeichnet.

#	Sender	Empfänger	#	Sender	Empfänger	#	Sender	Empfänger
1	i	xi	7	i	x	13	iv	ii
2	i	iv	8	i	viii	14	vii	xi
3	i	vi	9	i	v	15	vii	ii
4	i	vii	10	i	iii	16	xii	xi
5	i	ix	11	i	ii	17	xii	ii
6	i	xii	12	iv	xi			

Tab. 2: Testläufe mit jeweiligen Positionskombinationen

Die Messungen wurden mit Hilfe von Decawave EVB1000 UWB Evaluation Boards durchgeführt, da diese durch ein Abtastintervall von $\Delta\tau = 2ns$ sehr feingranulare CIRs bereitstellen. Entsprechend der Definitionen von UWB wurden die Messungen im $4\,GHz$ Band mit einer Bandbreite von $500\,MHz$ durchgeführt. Um innerhalb der Kanalkohärenzzeit des Kanals zu bleiben, wurden die einzelnen Impulsantworten mit einem Abstand von $\Delta t = 200\,ms$ aufgezeichnet. Hierbei liefern die Transceiver pro CIR $N = 1016$ Werte, womit eine einzelne Messung eine Länge von $\approx 2\mu s$ hat.

Die komplexen Impulsantworten $g(\tau)$ wurden vorab in reellwertige umgewandelt, indem der Betrag gebildet wurde $|g(\tau)| = \sqrt{\Re(g(\tau))^2 \quad \Im(g(\tau))^2}$, da die Phase keine signifikante Reziprozität liefert [Wa18].

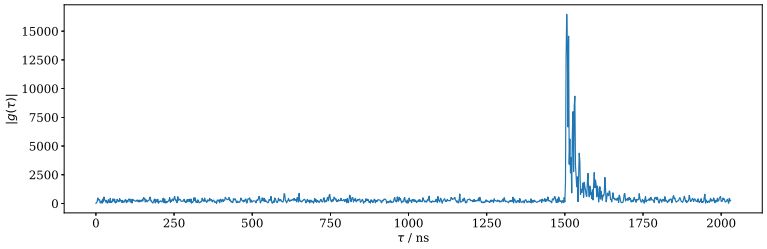


Abb. 3: Beispielhafte reellwertige Kanalimpulsantwort aus dem Messlauf #2

Abbildung 3 zeigt eine beispielhafte Kanalimpulsantwort. Da messtechnisch bedingt ein Großteil der Messungen Rauschen beinhaltet, wurde an Hand des Rauschlevels die Messung auf den “interessanten” Teil zugeschnitten.

5.2 Simulation und Optimierung

Basierend auf dem Angriffskonzept wurden für die Messungen Simulationen auf Basis des gewählten Kanalmodells durchgeführt.

Die Parameter des Modells sind in zwei Klassen unterteilt: zum einen *feste Parameter*, deren Werte durch die Umgebung vorgegeben sind (z.B. Raumgeometrie, Basisband, . . .). Zum anderen *optimierte Parameter*, deren Werte auf Basis der Referenzmessungen durch Bayes’sche Optimierung bestimmt wurden [Sh15].

Tabelle 3 zeigt die Modellparameter mit entsprechenden Werten/Wertebereichen .

Optimierte Parameter		**Feste Parameter**	
Parameter	Wertebereich	Parameter	Wert
K	Virtuelle Quellen	f	$4\,GHz$
d_0	$0,5\,d_{LOS} - 1,5\,d_{LOS}$	f_s	$500\,MHz$
α	$2,0 - 3,0$	n	$2\,ns$
G_{MP}	$-25\,dB - -10\,dB$	G	$120\,db$
$G_{MP,LOS}$	$-15\,dB - 0\,dB$	β	1.2
γ	$9\,ns - 13\,ns$		

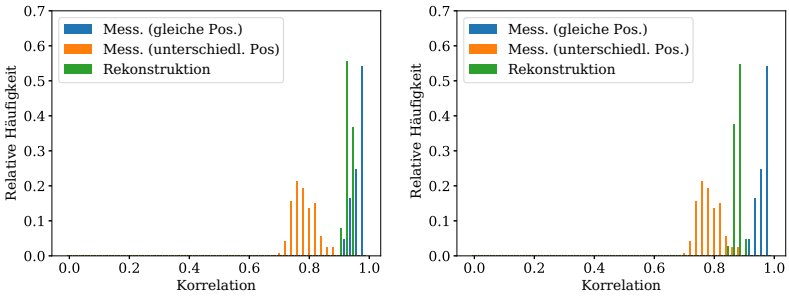
Tab. 3: Modellparameter des *Kunisch-Pamp* Kanalmodells.

Für die Optimierung wurden 2 unterschiedliche Strategien verfolgt:

Individuelle Optimierung Hierbei wurden die Modellparameter für die Simulation eines Testlaufes mit Messwerten ausschließlich aus diesem Messlauf optimiert. Das vorrangige Ziel dieser Optimierung ist die allgemeine Machbarkeit der Signalrekonstruktion zu zeigen und zu belegen, dass das gewählte Kanalmodell ein geeigneter Kandidat dafür ist.

Angreiferorientierte Optimierung Die Testläufe $R = 1, 12, 14, 16$ stellen mögliche Angreiferpositionen dar. Bei diesem Optimierungsansatz wurden ausschließlich Messungen dieser 4 Messungen verwendet, um die Modellparameter zu optimieren. Der Fokus dieser Optimierung ist die Praxisrelevanz des beschriebenen Angriffs.

5.3 Resultate



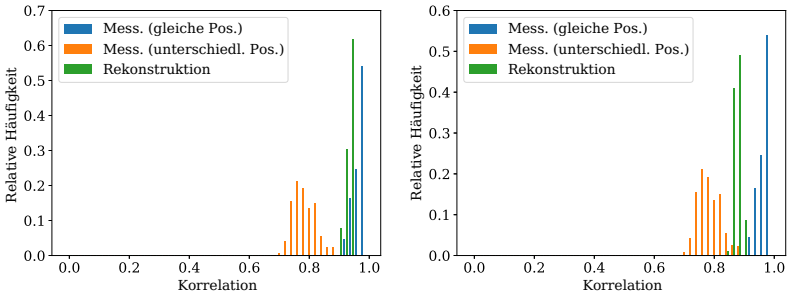
(a) Bester Testlauf #15, $\bar{c} = 0.936$ (b) Schlechtester Testlauf #16, $\bar{c} = 0.883$

Abb. 4: Bestes und schlechtestes Ergebnis der individuellen Optimierung.

Im Kontext der individuellen Optimierung konnten die folgenden Resultate erzielt werden. Abbildung 4 zeigt die Histogramme des besten als auch des schlechtesten Testlaufs. Hierbei wurden die physischen Messungen jeweils mit den rekonstruierten Signal mit der gewählten Metrik ausgewertet. Das Histogramm zeigt die relativen Häufigkeiten der Metrik-Resultate.

Die Bedeutungen der einzelnen Modellparameter können der Veröffentlichung [KP02] entnommen werden.

Nachdem dem Kanalmodell realistisches Rauschverhalten hinzugefügt wurde, konnten die Resultate nochmals verbessert werden. Die erreichten durchschnittlichen Kreuzkorrelationen konnte auf bis zu $0,941$ erhöht werden. In den Abbildungen 5 sind erneut die besten und schlechtesten Testläufe für diese Optimierung zu sehen.



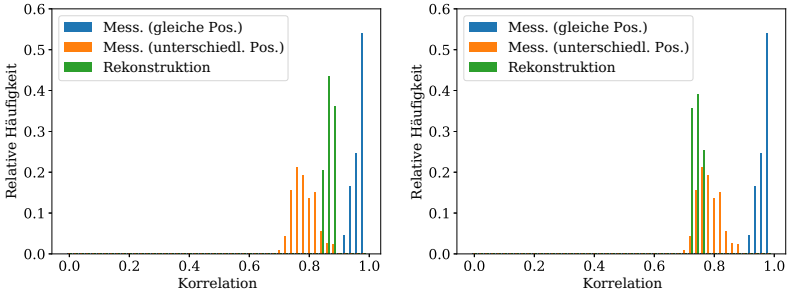
(a) Bester Testlauf #10, $\bar{c} = 0.941$ (b) Schlechtester Testlauf #16, $\bar{c} = 0.883$

Abb. 5: Bestes und schlechtestes Ergebnis der individuellen Optimierung mit Rauschen.

Diese Werte zeigen, dass das Modell grundsätzlich geeignet ist, UWB Kanalimpulsantworten auf Basis von Raumgeometrie und Terminalpositionen zu approximieren.

Aufbauend auf diesen Erkenntnissen wurde nun die **angreiferorientierte Optimierung** durchgeführt, welche ausschließlich die Testläufe $R = 1, 12, 14, 16$ zur Optimierung verwendet und anschließend CIRs für alle Positionen approximiert (siehe Abbildung 6).

Abbildung 7 zeigt die Mittelwerte aller Optimierungen im Vergleich.



(a) Bester Testlauf #13, $\bar{c} = 0.874$ (b) Schlechtester Testlauf #5, $\bar{c} = 0.748$

Abb. 6: Bestes und schlechtestes Ergebnis der angreiferorientierten Optimierung mit Rauschen.

6 Zusammenfassung und Ausblick

In dieser Arbeit wurde eine der Grundannahmen von CRKG angegriffen: dass die Entropiequelle als Grundlage der Schlüsselgenerierung nur den legitimen Kommunikationspartnern

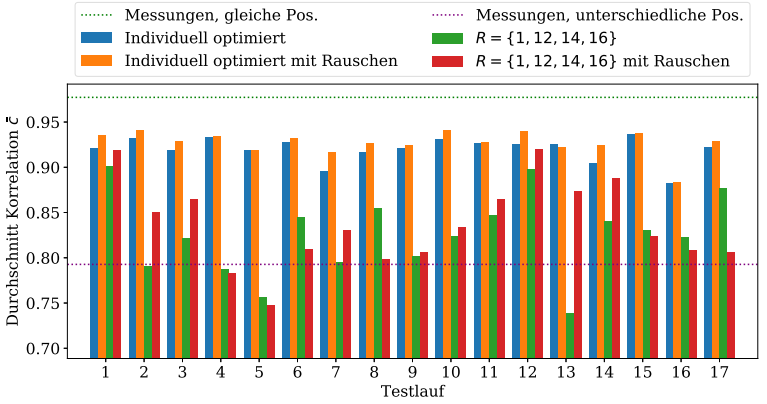


Abb. 7: Zusammenfassung aller Optimierungen und Testläufe

zur Verfügung steht. Ausgehend vom UWB Kontext wurden mit Hilfe des deterministischen *Kunisch-Pamp* Kanalmodells, optimiert durch Vorabmessungen des Angreifers, die der Schlüsselgenerierung zu Grunde liegenden Messungen approximiert.

Die Resultate zeigen deutlich, dass das gewählte Kanalmodell für deterministische Vorausberechnungen von Kanalimpulsantworten geeignet sind: die individuell optimierten Rekonstruktionen erreichen für alle angegriffenen Testläufe eine Kreuzkorrelation im Bereich von $0,93 - 0,94$, was deutlich über dem durchschnittlichen Wert für unterschiedliche Positionen von $0,79$ liegt. Weiterhin liegt es nur 3 Prozentpunkte unter dem durchschnittlichen Wert für gleiche Positionen von $0,97$ und über der empirischen unteren Schranke für gleiche Position von $0,89$. Das heißt, dass ein Großteil der in der Impulsantworten enthaltenen Informationen deterministisch vorausberechnet werden konnten. Berücksichtigt man die weiteren Verarbeitungsschritte, besonders die *Information Reconciliation* [BB11] und deren Methodik mit zusätzlichem Informationsabfluss kann von erfolgreichen Schlüsselberechnung auf Basis dieser Simulation ausgegangen werden.

Bemerkenswert für das Angriffsszenario ist, dass für die deterministische Simulation der Impulsantworten lediglich 4 Messungen des Angreifers nötig sind und der Angreifer *keine perfekten Informationen über den Raum* haben muss. Die vorliegenden Resultate konnten erzielt werden, obwohl der verwendete Raum *nicht* den Anforderungen des Kanalmodells entspricht. Es ist zu erwarten, dass eine entsprechende Erweiterung des Kanalmodells für beliebige Räume eine deutliche Verbesserung der Rekonstruktion bringt.

Für eine finale Bewertung des Angriffs muss die Auswirkung der Annäherung noch konkreter abgeschätzt werden. Dies könnte darüber stattfinden, die Transinformation zwischen Simulation/Messwerten mit der der reziproken Messungen in Verhältnis zu stellen. Da eine analytische Berechnung nicht praktikabel scheint arbeiten wir derzeit daran, geeignete Entropie- oder Transinformationsschätzer zu finden.

Literaturverzeichnis

[AC93] Ahlswede, R.; Csiszar, I.: Common Randomness in Information Theory and Cryptography. I. Secret Sharing. IEEE Transactions on Information Theory, 39(4):1121–1132, 1993.

[BB11] Bloch, Matthieu; Barros, Joao: Physical-Layer Security: From Information Theory to Security Engineering. Cambridge University Press, 2011.

[Dö10] Döttling, Nico; Lazich, Dejan; Müller-Quade, Jörn; de Almeida, Antonio Sobreira: Vulnerabilities of wireless key exchange based on channel reciprocity. In: International Workshop on Information Security Applications. Springer, S. 206–220, 2010.

[Eb12] Eberz, Simon; Strohmeier, Martin; Wilhelm, Matthias; Martinovic, Ivan: A practical man-in-the-middle attack on signal-based key generation protocols. In: European Symposium on Research in Computer Security. Springer, S. 235–252, 2012.

[EKY11] Edman, Matthew; Kiayias, Aggelos; Yener, Bülent: On passive inference attacks against physical-layer key extraction? In: Proceedings of the Fourth European Workshop on System Security. ACM, S. 8, 2011.

[Ja09] Jana, Suman; Premnath, Sriram Nandha; Clark, Mike; Kasera, Sneha K; Patwari, Neal; Krishnamurthy, Srikanth V: On the effectiveness of secret key extraction from wireless signal strength in real environments. In: Proceedings of the 15th annual international conference on Mobile computing and networking. ACM, S. 321–332, 2009.

[JZ15] Jin, Rong; Zeng, Kai: Physical layer key agreement under signal injection attacks. In: 2015 IEEE Conference on Communications and Network Security (CNS). IEEE, S. 254–262, 2015.

[KP02] Kunisch, J.; Pamp, J.: Radio Channel Model for Indoor UWB WPAN Environments. Bericht IEEE P802.15-02/281, IEEE 802.15.3a, 2002.

[MBS98] Morgan, D.R.; Benesty, J.; Sondhi, M.M.: On the evaluation of estimated impulse responses. IEEE Signal Processing Letters, 5(7):174–176, jul 1998.

[MFP03] Molisch, Andreas F; Foerster, Jeffrey R; Pendergrass, Marcus: Channel models for ultrawideband personal area networks. IEEE wireless communications, 10(6), 2003.

[Mi16] Mitra, S.K.: Signals and Systems. Oxford Series in Electrical and Computer Engineering. Oxford University Press, 2016.

[Sh15] Shahriari, Bobak; Swersky, Kevin; Wang, Ziyu; Adams, Ryan P; De Freitas, Nando: Taking the human out of the loop: A review of Bayesian optimization. Proceedings of the IEEE, 104(1):148–175, 2015.

[SS07] Sharif, Zaiton; Sha'ameri, Ahmad Zuri: The Application of Cross Correlation Technique for Estimating Impulse Response and Frequency Response of Wireless Communication Channel. In: 2007 5th Student Conference on Research and Development. IEEE, 2007.

[SV87] Saleh, A. A. M.; Valenzuela, R.: A Statistical Model for Indoor Multipath Propagation. IEEE Journal on Selected Areas in Communications, 1987.

[Wa18] Walther, Paul; Janda, Carsten; Franz, Elke; Pelka, Mathias; Hellbrück, Horst; Strufe, Thorsten; Jorswieck, Eduard: Improving Quantization for Channel Reciprocity based Key Generation. In: 2018 IEEE 43rd Conference on Local Computer Networks (LCN). 2018.