Dr.-Ing. Rafael F. Schaefer; Prof. Dr. Holger Boche; Prof. H. Vincent Poor

"Secure Communication under Channel Uncertainty and Adversarial Attacks"

Kurzfassung

Beweisbar sichere Kommunikation über Kanäle mit Abhörern, geht das denn? Diese Frage ist, unter idealisierten Annahmen bezüglich der Kanäle und Abhörer, bereits 1975 von Aaron Wyner von den Bell Labs positiv beantwortet worden. Wyners Annahme, dass die Kanäle perfekt bekannt sind und die Abhörer nur lauschen, sind in realen Kommunikationssystemen nicht erfüllt. Was passiert nun bei nicht perfekt bekannten Kanälen und noch schlimmer, bei Abhörern, die das Kommunikationssystem aktiv angreifen? Diese, seit 1975 offene, Fragestellung wird in der Arbeit beantwortet. Es wird die Kapazität der sicheren Übertragung von Nachrichten zum legitimierten Empfänger über Abhörkanäle mit aktiven Abhörern und Angreifern vollständig charakterisiert. Hierbei wird die Sicherheit, der für den legitimierten Empfänger bestimmten Nachrichten, durch eine geeignete Kodierung garantiert, die es nur dem legitimierten Empfänger erlaubt, die Nachricht zu ermitteln. Alle Abhörer, selbst bei Anwendung von beliebig großen klassischen oder Quantencomputern, werden über die Natur der Nachricht im Unklaren gelassen. In der Arbeit werden optimale Codierungsverfahren entwickelt und die für die Angreifer besten Strategien charakterisiert. Für die sichere Übertragung treten völlig neue Phänomene, wie zum Beispiel Superaktivierung, auf. Durch Nutzung von zwei orthogonalen Kanälen, die jeweils für die sichere Kommunikation völlig nutzlos sind, können durch optimale gemeinsame Kodierung doch sicher Nachrichten übertragen werden. Ein solches Verhalten kann für normale Nachrichtenübertragung niemals auftreten, d.h. dieses Verhalten ist eine zentrale Eigenschaft der sicheren Nachrichtenübertragung. Die Arbeit bildet eine Basis für den Entwurf zukünftiger Kommunikationssysteme mit sicherer Kommunikation.

Laudatio

Seit Jahrtausenden werden zur vertraulichen Übertragung von Nachrichten kryptographische Verfahren eingesetzt, die durch mathematische Formeln und einen geheimen Schlüssel gesteuert werden. Die Sicherheit dieser Verschlüsselungsverfahren gerät aber ins Wanken, wenn man davon ausgeht, dass Quantencomputer eingesetzt werden, um Lösungen für die verwendeten mathematischen Probleme zu berechnen oder einfach alle Möglichkeiten Schlüssel oder Texte in überschaubarer Zeit zu testen.

Eine Alternative hierzu bilden Verfahren, die in dem heute auszuzeichnenden Beitrag von Schäfer, Boche und Poor beschrieben werden und deren Sicherheit zudem beweisbar ist. Die Methode des Zahlenwurms von Claude Shannon, der die Nachricht mit einer einmaligen Zufallsfolge verknüpft, wird auf der physikalischen Schicht des Übertragungskanals angewendet, am besten eines drahtlosen Übertragungskanals, der einerseits besonders abhörgefährdet ist, andrerseits aber viele Störungen und ein starkes Rauschsignal aufweist: die vertrauliche

Nachricht wird im Rauschen versteckt, d.h. Rauschen hat auch positive Seiten! Der Sender überlagert der Nachricht ein Rauschen, auf dem Kanal wird sie zusätzlich durch Rauschen gestört und evtl. versucht ein Angreifer, die Nachrichtenübertragung zu stören, indem er ein Störsignal ausstrahlt. Kann der Empfänger die Nachricht hoch erfolgreich empfangen? Wie groß ist die Übertragungskapazität des vertraulichen Übertragungskanals? Die Betrachtung dieser Probleme erfolgte bisher unter der Annahme, dass der Zustand des Übertragungskanals bekannt ist. Dies ist in der Praxis aber nicht möglich, da er sich dynamisch ändert. Hierfür haben Schäfer, Boche und Poor einen zukunftsweisenden Beitrag geliefert. Einerseits ist er ein Übersichtsbeitrag, der kurz und prägnant, aber vollständig die bisherigen Entwicklungen auf dem Gebiet der Informationstheorie-basierten Übertragungssichert beschreibt, andrerseits bedeutet er aber einen großen Fortschritt in Richtung von Realisierungsmöglichkeiten, da darauf verzichtet wird, den Kanal in jedem Moment zu kennen. Stattdessen wird von einer „Unbestimmtheit“ des Kanals ausgegangen und diese Unkenntnis akzeptiert.

Außerdem besticht der Beitrag durch eine ausgezeichnete Darstellung, bei der der Leser Schritt für Schritt die Entwicklungen und Ergebnisse nachvollziehen kann. Jedem Entwickler auf dem Gebiet der Informationssicherheit, Informationstheorie oder Nachrichtentechnik wird dieser Beitrag dringend empfohlen, um sich für die informationstheorie-basierte vertrauliche Nachrichtenübertragung begeistern zu lassen.

Univ.-Prof. Dr. Karl Christoph Ruland

Dr.-Ing. Rafael F. Schaefer

Technische Universität Berlin

Rafael F. Schaefer received the Dipl.-Ing. degree in electrical engineering and computer science in 2007 from the Technische Universität Berlin, Germany and the Dr.-Ing. degree in electrical engineering in 2012 from the Technische Universität München, Germany. From 2007 until 2010 he was a Research and Teaching Assistant at Technische Universität Berlin and from 2010 until 2013 at Technische Universität München. From 2013 until 2015 he was a Post-Doctoral Research Fellow at Princeton University. Since December 2015 he has been an Assistant Professor at Technische Universität Berlin. He was a recipient of the VDE Johann-Philipp-Reis Prize in 2013. He received the best paper award of the German Information Technology Society (ITG-Preis) in 2016. He was one of the exemplary reviewers of the IEEE COMMUNICATION LETTERS in 2013. He is currently an Associate Member of the IEEE Information Forensics and Security Technical Committee. He is the General Chair of the Symposium on Information Theoretic Approaches to Security and Privacy at IEEE GlobalSIP 2016. Among his publications is the recent book: Information Theoretic Security and Privacy of Information Systems (Cambridge University Press). He is a member of VDE-ITG and IEEE.

Prof. Dr. Holger Boche

Technische Universität München

Holger Boche received the Dipl.-Ing. and Dr.-Ing. degrees in electrical engineering from the Technische Universität Dresden, Germany, in 1990 and 1994, respectively.

He graduated in mathematics from the Technische Universität Dresden in 1992. From 1994 to 1997, he did Postgraduate studies in mathematics at the Friedrich- Schiller Universität Jena, Germany. He received his Dr. rer. nat. degree in pure mathematics from the Technische Universität Berlin, Germany, in 1998. In 1997, he joined the Heinrich-Hertz-Institut (HHI) für Nachrichtentechnik Berlin, Germany. Starting in 2002, he was a Full Professor for mobile communication networks with the Institute for Communications Systems, Technische Universität Berlin. In 2003, he became Director of the Fraunhofer German-Sino Lab for Mobile Communications, Berlin, Germany, and in 2004 he became the Director of the Fraunhofer Institute for Telecommunications (HHI), Berlin, Germany. Since October 2010 he has been with the Institute of Theoretical Information Technology and Full Professor at the Technische Universität München, Germany. Since 2014 he has been a member and honorary fellow of the TUM Institute for Advanced Study, Munich, Germany. He was a Visiting Professor with the ETH Zurich, Switzerland, during the 2004 and 2006 Winter terms, and with KTH Stockholm, Sweden, during the 2005 Summer term. Prof. Boche is a Member of IEEE Signal Processing Society SPCOM and SPTM Technical Committee. He was elected a Member of the German Academy of Sciences (Leopoldina) in 2008 and of the Berlin Brandenburg Academy of Sciences and Humanities in 2009. He received the Research Award Technische Kommunikation from the Alcatel SEL Foundation in October 2003, the Innovation Award from the Vodafone Foundation in June 2006, and the Gottfried Wilhelm Leibniz Prize from the Deutsche Forschungsgemeinschaft (German Research Foundation) in 2008. He was co-recipient of the 2006 IEEE Signal Processing Society Best Paper Award and recipient of the 2007 IEEE Signal Processing Society Best Paper Award. He was a recipient of the VDE Johann-Philipp-Reis Prize in 2013. He received the best paper award of the German Information Technology Society (ITG-Preis) in 2016.

He is the General Chair of the Symposium on Information Theoretic Approaches to Security and Privacy at IEEE GlobalSIP 2016. Among his publications is the recent book Information Theoretic Security and Privacy of Information Systems (Cambridge University Press). He is a member of VDE-ITG and a fellow of IEEE.

Prof. H. Vincent Poor

Princeton University

H. Vincent Poor (S'72, M'77, SM'82, F'87) received the Ph.D. degree in electrical engineering and computer science from Princeton University in 1977. From 1977 until 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990 he has been on the faculty at Princeton, where he is currently the Michael Henry Strater University Professor of Electrical Engineering.

During 2006-16 he served as Dean of Princeton's School of Engineering and Applied Science. He has also held visiting appointments at several other institutions, most recently at Cambridge and Stanford. His research interests are in the areas of information theory, stochastic analysis and statistical signal processing, and their applications in wireless networks and related fields such as smart grid. Among his publications in these areas is the recent book Mechanisms and Games for Dynamic Spectrum Allocation (Cambridge University Press, 2014).

Dr. Poor is a Member of the U. S. National Academy of Engineering and the U. S. National Academy of Sciences, and is a Foreign Member of Academia Europaea and the Royal Society. He is also a Fellow of the American Academy of Arts and Sciences, and of other national and international academies. He received a Guggenheim Fellowship in 2002 and the IEEE Education Medal in 2005. Recent recognition of his work includes the 2014 URSI Booker Gold Medal, the 2015 EURASIP Athanasios Papoulis Award, the 2016 John Fritz Medal, and honorary doctorates from Aalborg University, Aalto University, HKUST, and the University of Edinburgh.