Störungstolerante Datenauthentifizierung für drahtlose Kommunikation

Obaid Ur-Rehman · Natasa Zivic

Störungstolerante Datenauthentifizierung für drahtlose Kommunikation

Springer Vieweg

Obaid Ur-Rehman
Lehrstuhl für Digitale
Kommunikationssysteme
Universität Siegen
Siegen, Deutschland

Natasa Zivic
Fakultät Digitale Transformation
Hochschule für Technik, Wirtschaft und
Kultur Leipzig
Leipzig, Deutschland

ISBN 978-3-031-41751-1 ISBN 978-3-031-41752-8 (eBook)
https://doi.org/10.1007/978-3-031-41752-8

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über https://portal.dnb.de abrufbar.

Dieses Buch ist eine Übersetzung des Originals in Englisch „Noise Tolerant Data Authentication for Wireless Communication“ von Obaid Ur-Rehman, publiziert durch Springer Nature Switzerland AG im Jahr 2018. Die Übersetzung erfolgte mit Hilfe von künstlicher Intelligenz (maschinelle Übersetzung). Eine anschließende Überarbeitung im Satzbetrieb erfolgte vor allem in inhaltlicher Hinsicht, so dass sich das Buch stilistisch anders lesen wird als eine herkömmliche Übersetzung. Springer Nature arbeitet kontinuierlich an der Weiterentwicklung von Werkzeugen für die Produktion von Büchern und an den damit verbundenen Technologien zur Unterstützung der Autoren.

Planung/Lektorat: Axel Garbers
Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Nature Switzerland AG und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Gewerbestrasse 11, 6330 Cham, Switzerland

Das Papier dieses Produkts ist recycelbar

Vorwort

Mit der schnellen Entwicklung und der Vereinfachung der Erstellung und Verteilung digitaler Inhalte über das Internet ist das Teilen digitaler Daten zu einem allgegenwärtigen Teil unseres täglichen Lebens geworden. Dies beinhaltet Daten in Form von digitalem Multimedia wie Text, Audio, Video und Bilder. Gleichzeitig gab es ein enormes Wachstum bei den Methoden, die Authentizität und Authentifizierungsmethoden von Daten, die über moderne Kommunikationsnetzwerke übertragen werden, sowie die gespeicherten Daten zu kompromittieren.

Standard-Authentifizierungsmechanismen sind sehr empfindlich und nicht robust gegenüber jeglichen Modifikationen. Selbst eine einzige Bit-Modifikation wird die Daten nach dem Scheitern des Authentifizierungstests beim Empfänger unbrauchbar machen. Meistens ist ein Wiederholung möglich, und die Daten können von der Quelle erneut übertragen werden. Manchmal existiert jedoch eine solche Wiedermöglichkeit nicht, z. B. im Falle einer Satellitenübertragung. In solchen Fällen besteht die Notwendigkeit, dass solche Datenauthentifizierungsmechanismen verwendet werden, die nicht nur in der Lage sind, unbeabsichtigte Modifikationen zu tolerieren, sondern auch bestimmte Modifikationen zu identifizieren, zu lokalisieren und wenn möglich zu korrigieren.

Dies wird durch die Verwendung einiger neuer Algorithmen für die Datenauthentifizierung ermöglicht, die mit Techniken zur Vorwärtsfehlerkorrektur zusammenarbeiten, so dass geringfügige Modifikationen oder Fehler nicht nur toleriert, sondern auch so weit wie möglich korrigiert werden. Dies hängt von vielen Faktoren ab, wie z. B. der Fehlerkorrekturfähigkeit der von der störungsresistenten Authentifizierungsmethode verwendeten Vorwärtsfehlerkorrekturcodes und auch der Störungsresistenzfähigkeit der Authentifizierungsschemata. Es besteht natürlich die Gefahr, dass die Sicherheit durch die Zulassung einer höheren Robustheit beeinträchtigt werden könnte. Einige der in diesem Buch diskutierten geräuschresistenten Authentifizierungsmethoden haben die Fähigkeit, die Robustheit mit bestimmten Parametern des Schemas zu konfigurieren.

Dieses Buch ist in sieben Kapitel gegliedert. Die ersten vier Kapitel führen das Hintergrundmaterial ein, das benötigt wird, um die nächsten drei Kapitel zu verstehen. Die letzten drei Kapitel basieren auf den Ergebnissen der

Forschungsarbeit, die die Autoren während ihrer Arbeit an der Universität Siegen, Deutschland, durchgeführt haben.

Kap. 1 führt die Grundlagen der Datenauthentifizierung in Anwesenheit von Modifikationen ein. Daten, die an der Quelle erzeugt werden, können auf viele Arten von Quelle zu Senke modifiziert werden. Dies beinhaltet absichtliche und unbeabsichtigte Modifikationen, wobei die ersteren ernster sind, aber auch den letzteren sollte Aufmerksamkeit geschenkt werden.

Kap. 2 behandelt die Eigenschaften eines drahtlosen Kommunikationskanals und wie die Datenübertragung durch den Kanal beeinflusst wird. Mit dem ständig steigenden Einsatz moderner Geräte mit Internetverbindung wird immer mehr Daten über den drahtlosen Kanal zusätzlich zum standardmäßigen verkabelten Kanal übertragen. Verschiedene Mittel zur Bekämpfung der durch die Kommunikation über einen drahtlosen Kanal eingeführten Datenkorruption werden in dem Kapitel vorgestellt.

Kap. 3 diskutiert die Notwendigkeit robuster Authentifizierungsmechanismen. Diese Authentifizierungsmechanismen, im Gegensatz zu den Standard-Datenauthentifizierungsmechanismen, sind tolerant gegenüber bestimmten Modifikationen. Einige dieser Mechanismen sind so konzipiert, dass sie einige Bit-Modifikationen tolerieren, während andere zusätzlich auch die modifizierten Datenpartien korrigieren können, indem sie Vorwärtsfehlerkorrekturcodes als Teil der Authentifizierung verwenden. Störungstolerante Authentifizierung mit speziell entworfenen Nachrichtenauthentifizierungscodes sowie digitales Wasserzeichen wird in dem Kapitel diskutiert.

Kap. 4 führt die digitalen Wasserzeichentechniken zur Authentifizierung von Multimediadaten ein. Digitales Wasserzeichen, seine Klassifizierung und Eigenschaften werden diskutiert.

Kap. 5 diskutiert zwei digitale Wasserzeichentechniken zur Datenauthentifizierung in Anwesenheit von Rauschen. Die in diesem Kapitel diskutierten Wasserzeichentechniken haben die Fähigkeit zur störungstolerante Datenauthentifizierung sowie zur Fehlerkorrektur. Die diskutierten Techniken verwenden duale Wasserzeichen, bei denen die Fähigkeit zur Erkennung von modifizierten Standorten erlangt wird. Die zusätzliche Verwendung von Vorwärtsfehlerkorrekturcodes verleiht den Techniken die Fähigkeit, einige Modifikationen zu korrigieren. Dies ist nützlich, wenn die Modifikationen unbeabsichtigt erfolgen, z. B. durch Kanalrauschen.

Kap. 6 behandelt eine Methode zur Bildauthentifizierung mit einer modifizierten Methode zur Bildauthentifizierung basierend auf Standard-Nachrichtenauthentifizierungscodes und Kanalcodes. Die diskutierte Methode teilt das Bild in wichtige Teile, die als Region of Interest bezeichnet werden. Durch die Authentifizierung der Region of Interest mit der Soft-Input-Decryption-Methode und die Verwendung der authentifizierten Teile als Feedback für das Decodieren wird das Ergebnis der Kanaldecodierung zusätzlich zur störungstoleranten Authentifizierung verbessert.

Kap. 7 diskutiert zwei störungstolerante Datenauthentifizierungsalgorithmen, die auf geräuschtoleranten Nachrichtenauthentifizierungscodes basieren. Diese

Codes basieren selbst auf Standard-Nachrichtenauthentifizierungscodes. Die diskutierten Methoden haben die Fähigkeit, Modifikationen zu erkennen und auf Blockebene zu lokalisieren. Es kann eine Blockgröße definiert werden, die die Granularität der Modifikationslokalisierung steuert. Diese Algorithmen haben auch die inhärente Fähigkeit zur Fehlerkorrektur. Wenn die Modifikationen die erlaubten Grenzen überschreiten und über die Fehlerkorrekturfähigkeit der Vorwärtsfehlerkorrekturcodes hinausgehen, werden die Modifikationen als Fälschungen kategorisiert.

Siegen, Deutschland — Obaid Ur-Rehman
Leipzig, Deutschland — Natasa Zivic

Danksagungen

Dieses Buch basiert auf der Forschungsarbeit, die wir, die Autoren, am Lehrstuhl für Datenkommunikationssysteme an der Universität Siegen, Deutschland, durchgeführt haben. Wir möchten die Beiträge unserer ehemaligen und gegenwärtigen Kollegen am Lehrstuhl anerkennen, denn ohne ihre Unterstützung wäre dieses Buch nicht möglich gewesen. Wir möchten insbesondere den folgenden Personen für ihre Unterstützung aufrichtig danken.

Unser erster und vorrangiger Dank gilt Christoph Ruland, der nicht nur der Vorsitzende des Lehrstuhls für Datenkommunikationssysteme ist, sondern auch der Doktorvater beider Autoren war. Er hat uns die Umgebung zur Verfügung gestellt, die wir für die Arbeit an den in dem Buch diskutierten Forschungsthemen benötigten. Er hat uns auch unterstützt, indem er uns ermöglicht hat, an der internationalen Zusammenarbeit mit der Universität Shanghai, China, zu arbeiten. Die während der Zusammenarbeit ausgetauschten Forschungsideen haben eine Grundlage für bestimmte fortgeschrittene Themen gebildet, die in dem Buch diskutiert werden.

Zweitens möchten wir auch unserem ehemaligen Kollegen Amir Tabatabaei danken, der mit uns an mehreren störungstoleranten Datenauthentifizierungsschemata kooperiert und zusammengearbeitet hat. Wir danken ihm besonders für seine Unterstützung bei der Sicherheitsanalyse der Algorithmen.

Last but not least möchten wir auch unseren Kooperationspartnern, Frau Chen Ling und Professor Wenjun Zhang, danken, die wir zunächst während des Forschungsprojekts zur störungstoleranten Videoauthentifizierung mit der Universität Shanghai kennengelernt haben. Durch verschiedene Interaktionen und Diskussionen während der Zusammenarbeit haben wir gemeinsam an vielen interessanten Ideen im Bereich des digitalen Wasserzeichens zur Authentifizierung von Videostreams gearbeitet.

Am wichtigsten möchten wir auch unseren Familien für ihre Geduld danken, während wir an dem Buch gearbeitet haben.

Inhaltsverzeichnis