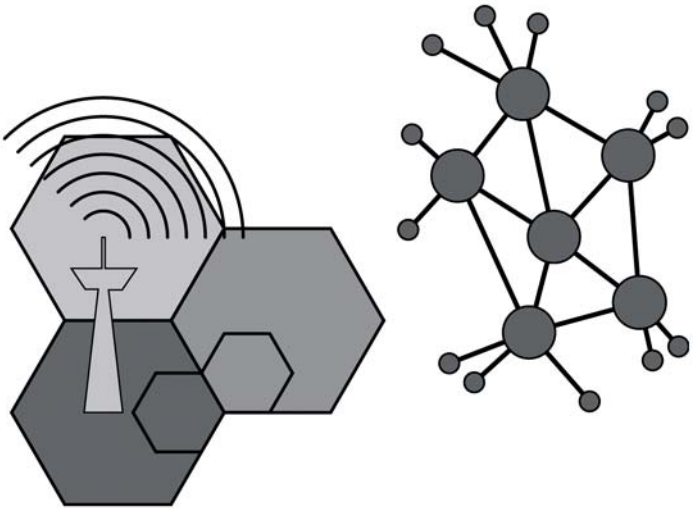
UNIVERSITÄT SIEGEN
Institut für Digitale Kommunikationssysteme

Forschungsberichte

Band 36 Herausgeber: Univ.-Prof. Dr. Christoph Ruland



Matthias Schneider

Verifikation von Zeitinformationen in drahtlosen Kommunikationssystemen

2018

SHAKER VERLAG

Verifikation von Zeitinformationen in drahtlosen Kommunikationssystemen

DISSERTATION
zur Erlangung des Grades eines Doktors
der Ingenieurwissenschaften

vorgelegt von
Dipl. Ing. Matthias Schneider
geb. am 10.11.1967 in Siegen

eingereicht bei der Naturwissenschaftlich-Technischen Fakultät
der Universität Siegen
Siegen 2017

1. Gutachter: Univ.-Prof. Dr. rer. net. Christoph Ruland
2. Gutachter: Univ.-Prof. Dr.-Ing. Horst Bessai
Vorsitzender: Univ.-Prof. Dr.-Ing. Dietmar Ehrhardt

Tag der mündlichen Prüfung: 09. November 2017

UNIVERSITÄT SIEGEN

Institut für
Digitale Kommunikationssysteme

Forschungsberichte

Herausgeber: Univ.-Prof. Dr. Christoph Ruland

Band 36

Matthias Schneider

Verifikation von Zeitinformationen in drahtlosen Kommunikationssystemen

SHAKER VERLAG

Aachen 2018

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Zugl.: Siegen, Univ., Diss., 2017

Printed in Germany.

ISBN 978-3-8440-5722-5
ISSN 1614-0508

Shaker Verlag GmbH • Postfach 101818 • 52018 Aachen
Telefon: 02407 / 95 96 - 0 • Telefax: 02407 / 95 96 - 9
Internet: www.shaker.de • E-Mail: info@shaker.de

Vorwort

Die vorliegende Arbeit entstand im Rahmen meiner Tätigkeit als Mitarbeiter am Lehrstuhl für Digitale Kommunikationssysteme der Universität Siegen.

Mein besonderer Dank gilt meinem Doktorvater Herrn Univ.-Prof. Dr. rer. nat. Christoph Ruland für die Möglichkeit der Durchführung und die Betreuung dieser Dissertation.

Weiterhin danke ich Herrn Univ.-Prof. Dr.-Ing. Horst Bessai für die Übernahme des Koreferats. Seine Anregungen und Hinweise lieferten einen wertvollen Beitrag zur Fertigstellung dieser Arbeit.

Herrn Univ.-Prof. Dr.-Ing. Dietmar Ehrhardt danke ich für die Bereitschaft, der Promotionskommission vorzusitzen und für das Interesse, das er meiner Arbeit entgegengebracht hat.

Ferner gilt mein Dank all meinen Kollegen, die mich seit 1998 etappenweise am Lehrstuhl begleitet haben, für das angenehme und heitere Arbeitsklima und die stets konstruktive Zusammenarbeit über diese lange Zeit hindurch.

Abschließend gilt ein ganz persönlicher Dank meiner Familie und meinen Eltern für die fortwährende Unterstützung und Motivation in den vergangenen Jahren.

Siegen, im Dezember 2017

Matthias Schneider

Zusammenfassung

Die Synchronisation von Uhren ist in industriellen, privaten und öffentlichen Kommunikationsnetzen von elementarer Wichtigkeit. Alle Server und Endgeräte müssen in einem Netzwerk direkten Zugriff auf die aktuelle Systemzeit haben, damit zum Beispiel Zeitstempel korrekt generiert und auf ihre Gültigkeit geprüft werden können. Die Verteilung der aktuellen Systemzeit kann mit unterschiedlichen Technologien erfolgen. So können in drahtlosen Zeitverteildiensten gleichzeitig Zeitinformationen an viele Millionen Teilnehmer gesendet werden. Zu dieser Kategorie von Kommunikationsnetzen zählen Zeitzeichendienste, Navigationssysteme und auch Datendienste, wie die Funkrundsteuertechnik. In allen Kommunikationsnetzen wird die Systemzeit regelmäßig an alle User verteilt. Hierbei spielte die Datensicherheit bisher nur eine untergeordnete Rolle. Mögliche Schäden durch Angriffe auf Zeitverteildienste wurden in der Vergangenheit meist vernachlässigt. Jedoch besteht die Gefahr von Hackerangriffen.

Der Fokus dieser Dissertation liegt auf der Verifikation von Zeitinformationen in drahtlosen Kommunikationssystemen. Zunächst werden unterschiedliche Zeitverteilsysteme untersucht und eine Sicherheitsanalyse durchgeführt. Als Ergebnis der Sicherheitsanalyse wird ein Katalog von Sicherheitsanforderungen für drahtlose Zeitverteildienste definiert und darauf aufbauend ein Verifikationsverfahren für Zeitinformationen vorgestellt, dass auf dem Vergleich zwischen einer physikalischen und einer logischen Differenzzeit basiert. Für die physikalische Differenzzeit wird die Zeit zwischen zwei korrekt aufeinanderfolgend empfangenen Zeitzeichen in einem Empfänger gemessen. Diese physikalische Differenzzeitmessung erfolgt mit einem oder mehreren Digitalzählern. Hierbei wird das Taktsignal für die Digitalzähler direkt aus dem modulierten Empfangsdatenstrom zurückgewonnen. Die logische Differenzzeit wird aus den Zeitinformationen in den Zeitzeichen berechnet. Über den direkten Vergleich von physikalischer und logischer Differenzzeit wird die Verifikation der Zeitinformationen durchgeführt. Ist das Ergebnis des Vergleichs zwischen der physikalischen und der logischen Differenzzeit gleich „Null“ oder kleiner als ein zuvor definierter Grenzwert, so ist die Verifikationsprüfung der zuletzt empfangenen Zeitinformation erfolgreich.

Das hier vorgestellte Verifikationsverfahren für Zeitinformationen in drahtlosen Kommunikationssystemen wurde so konzipiert, dass die Verifikation der empfangenen Zeitinformation alleine im Empfänger erfolgt. Somit muss nur die Firmware im Empfänger um die Funktionalität des Verifikationsverfahrens erweitert werden. Dies ermöglicht die Integration des Verifikationsverfahrens in alle drahtlosen und drahtgebundenen Zeitverteilsysteme, in denen ein kontinuierliches Taktsignal für die physikalische Differenzzeitmessung aus dem modulierten Empfangssignal extrahiert werden kann.

Als Testimplementierungen für das Verifikationsverfahren wurde je ein Laborprototyp für den Zeitzeichendienste DCF77 und die Funkrundsteuertechnik entwickelt. Mit diesen Prototypen konnte abschließend das Verhalten des hier vorgestellten Verifikationsverfahrens in zwei realen Zeitverteilsystemen einem Praxistest unterzogen werden.

Abstract

Synchronization of clocks in industrial, private and public communication networks is very important. All servers and devices in a network must have direct access to an accurate system time, because the accurate system time has to be available for the generation and verification of time stamps. The current system time can be distributed using different technologies. Wireless time distribution services are an opportunity to send time information to millions of users. This category of communications networks includes time distribution services, navigation systems, and data services, such as radio ripple control technology. By now, data security has played only a subordinate role. Potential damage caused by attacks on time distribution services has been disregarded in the past. However, there is a risk of hacker attacks. Various publications show possible attacks on wireless time distribution systems.

The focus of this dissertation is the verification of time information in wireless communication systems. First, different time distribution systems were investigated and a safety analysis was performed. As a result of the security analysis, a catalogue of security requirements for these systems was defined.

The verification method presented in this dissertation is based on the comparison between a physical and a logic time difference. For the physical time difference, the time between two correctly received time signals is measured in the receiver. One or more digital counters realize this physical differential time measurement. The clock signal for the digital counters is recovered directly from the modulated received data stream. The logical difference time is calculated from the time information contained in the time signals.

The verification of the time information is realized by a direct comparison of physical and logical difference time. If the result of the comparison between the physical and the logical difference time is equal to "zero", or less than a previously defined threshold, the verification check for the last received time information was successful.

The verification method for time information in wireless communication systems presented in this dissertation has been designed in such a way that the received time information can be verified completely at the receiver side. Thus, only the firmware in the receiver has to be extended by the functionality of the verification method. The verification method can be integrated into all time distribution systems that allows the extraction of a continuous clock signal for the physical difference time measurement directly from the modulated received signal.

Finally, the verification procedure was tested with two laboratory prototypes for the time signal service DCF77 and the radio ripple control technology. These prototypes present the behaviour of the verification method in two different real time distribution systems.

Inhaltsverzeichnis