

---

# **Technologien für die intelligente Automation**

Technologies for Intelligent Automation

Band 10

**Reihe herausgegeben von**

inIT - Institut für industrielle Informationstechnik  
Lemgo, Deutschland

Ziel der Buchreihe ist die Publikation neuer Ansätze in der Automation auf wissenschaftlichem Niveau, Themen, die heute und in Zukunft entscheidend sind, für die deutsche und internationale Industrie und Forschung. Initiativen wie Industrie 4.0, Industrial Internet oder Cyber-physical Systems machen dies deutlich. Die Anwendbarkeit und der industrielle Nutzen als durchgehendes Leitmotiv der Veröffentlichungen stehen dabei im Vordergrund. Durch diese Verankerung in der Praxis wird sowohl die Verständlichkeit als auch die Relevanz der Beiträge für die Industrie und für die angewandte Forschung gesichert. Diese Buchreihe möchte Lesern eine Orientierung für die neuen Technologien und deren Anwendungen geben und so zur erfolgreichen Umsetzung der Initiativen beitragen.

Weitere Bände in der Reihe <http://www.springer.com/series/13886>

---

Mohammad Elattar

# Reliable Communications within Cyber-Physical Systems Using the Internet (RC4CPS)

Mohammad Elattar  
Institut für industrielle Informationstechnik  
Hochschule Ostwestfalen-Lippe  
Lemgo, Germany

ISSN 2522-8579                      ISSN 2522-8587 (electronic)  
Technologien für die intelligente Automation  
ISBN 978-3-662-59792-7              ISBN 978-3-662-59793-4 (eBook)  
<https://doi.org/10.1007/978-3-662-59793-4>

Springer Vieweg

© Springer-Verlag GmbH Germany, part of Springer Nature 2020

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer Vieweg imprint is published by the registered company Springer-Verlag GmbH, DE part of Springer Nature.

The registered company address is: Heidelberger Platz 3, 14197 Berlin, Germany

# Abstract

An important requirement to realize cyber-physical systems (CPSs) in critical infrastructures such as power grids is communication reliability where such reliability is usually measured in terms of communication service unavailability. With this regard, applications proposed for smart grids have reliability requirements of 99-99.9999%. To achieve this, most power utilities rely on dedicated networks and/or leased lines. The alternative for such solutions is the Internet which represents a global, cost-effective network for CPSs that span large geographical areas. Unfortunately, the reliability of today's Internet is inadequate and varies over time. A widely adopted approach in other domains to enhance reliability utilizes mainly redundancy in terms of communication paths and transmitted data. However, this requires knowledge about the topology to ensure disjointness of used paths, which is difficult in case of the Internet. Even with such knowledge, most of the available multipath (MP) communication protocols are throughput-oriented or proposed for dedicated networks and, therefore, cannot be utilized directly. Nevertheless, MP communication is still expected to improve the communication reliability of the Internet.

In this dissertation, data duplication and dynamic MP selection during runtime when using multiple end-to-end (e2e) paths are proposed to improve the communication reliability for Internet-based CPSs. With this regard, the problem of paths selection is formulated as an optimization problem to select the minimum number of e2e paths and limit the redundant data by the needed reliability. The multiple e2e paths are realized using different access internet service providers and MP communication protocols. In addition, real world measurements to investigate the reliability gains of MP communication in the Internet were conducted. The obtained results proved the existence of e2e paths that traverse completely different networks and, consequently, are likely to be disjoint. They also showed that the concurrent unavailability of different subsets of paths with two and three paths was 0%. Those results motivated proposing the Reliable Multipath Communication for Internet-based CPSs (RC4CPS) approach. It is an e2e approach that utilizes the inherent redundancy of the Internet and the concept of MP communication protocols to improve reliability. It also provides online monitoring and dynamic MP selection that considers the diversity and unavailability probability of e2e paths to maximize the reliability gains. RC4CPS was first implemented in MATLAB for initial evaluations and, then, using the iPRP (Parallel Redundancy Protocol for IP Networks) MP transport protocol. The resulting protocol, called iPRP-RC4CPS, incorporates the RC4CPS features and extends the original iPRP implementation, proposed for dedicated WAN networks, to support the Internet. The evaluation results carried out using both implementations of RC4CPS in the Internet indicated the ability of iPRP-RC4CPS to achieve 0% unavailability while selecting the minimum number of e2e paths.

# Zusammenfassung

Eine wichtige Voraussetzung für die Realisierung von cyber-physischen Systemen (CPS) in kritischen Infrastrukturen wie Stromnetzen ist die Kommunikationszuverlässigkeit. Die Zuverlässigkeit wird üblicherweise im Hinblick auf die Nichtverfügbarkeit von Kommunikationsdiensten gemessen. In diesem Zusammenhang haben die für Smart Grids vorgeschlagenen Anwendungen Zuverlässigkeitsforderungen von 99-99,9999%. Um diese zu erreichen, sind die meisten Energieversorger auf dedizierte Netze und/oder Mietleitungen angewiesen. Die Alternative für solche Lösungen ist das Internet, das ein globales, kosteneffektives Netzwerk für CPS darstellt, die große geographische Gebiete umfassen. Leider ist die Zuverlässigkeit des heutigen Internets unzureichend und variiert im Laufe der Zeit. Ein weit verbreiteter Ansatz in anderen Bereichen zur Verbesserung der Zuverlässigkeit verwendet Redundanz in Bezug auf Kommunikationspfade und übertragene Daten. Dies erfordert jedoch Kenntnisse über die Topologie des Netzwerks, um die physische Trennung der verwendeten Pfade sicherzustellen, was im Falle des Internets schwierig ist. Selbst mit diesem Wissen sind die meisten der verfügbaren Multipath (MP) -Kommunikationsprotokolle durchsatzorientiert oder für dedizierte Netzwerke entwickelt worden und können daher nicht direkt verwendet werden. Dennoch wird erwartet, dass MP-Kommunikation die Kommunikationszuverlässigkeit des Internets verbessern wird.

In dieser Dissertation werden Datenduplikation und dynamische MP-Auswahl zur Laufzeit bei Verwendung mehrerer end-to-end-Pfade (e2e) vorgeschlagen, um die Kommunikationszuverlässigkeit für internet-basierte CPS zu verbessern. In dieser Hinsicht wird das Problem der Pfadauswahl als ein Optimierungsproblem formuliert, um die minimale Anzahl von e2e-Pfaden auszuwählen und die redundanten Daten durch die erforderliche Zuverlässigkeit zu begrenzen. Die e2e-Pfade werden unter Verwendung verschiedener Internetdiensteanbieter und MP-Kommunikationsprotokolle realisiert. Darüber hinaus wurden reale Messungen zur Untersuchung der Zuverlässigkeitsgewinne der MP-Kommunikation im Internet durchgeführt. Die erhaltenen Ergebnisse beweisen die Existenz von e2e-Pfaden, die völlig unterschiedliche Netzwerke durchlaufen und folglich wahrscheinlich physisch getrennt sind. Sie zeigten auch, dass die gleichzeitige Nichtverfügbarkeit von verschiedenen Kombinationen aus 2 und 3 Pfaden 0% betrug. Diese Ergebnisse motivierten den Ansatz des Reliable Communication for Cyber-Physical Systems (RC4CPS) vorzuschlagen. RC4CPS ist ein e2e-Ansatz, der die inhärente Redundanz des Internets und das Konzept der MP-Transportprotokolle nutzt, um die Zuverlässigkeit zu verbessern. Es bietet eine Online-Überwachung und eine dynamische MP-Auswahl, die die Pfaddiversität und die Wahrscheinlichkeit der Nichtverfügbarkeit berücksichtigt, um die Zuverlässigkeitsgewinne zu maximieren. RC4CPS wurde in MATLAB für erste Auswertungen und dann unter Verwendung des iPRP-MP-

Transportprotokolls (Parallel Redundancy Protocol for IP-Networks) implementiert. Das resultierende Protokoll, das als iPRP-RC4CPS bezeichnet wird, enthält die RC4CPS-Funktionen und erweitert die ursprüngliche iPRP-Implementierung, die für dedizierte WAN-Netzwerke entwickelt wurde, um den Einsatz im Internet zu unterstützen. Die Auswertungsergebnisse, die unter Verwendung beider Implementierungen von RC4CPS im Internet durchgeführt wurden, zeigen die Fähigkeit von iPRP-RC4CPS, 0% Nichtverfügbarkeit zu erreichen, während die minimale Anzahl von e2e Pfaden ausgewählt wurde.

# Contents

<b>1</b>	<b>Introduction</b> .....	<b>1</b>
1.1	Motivation.....	3
1.2	Structure of the Thesis.....	5
<b>2</b>	<b>Research Description</b> .....	<b>7</b>
2.1	Problem Description.....	7
2.2	Research Objectives and Questions.....	8
2.3	Contributions.....	11
<b>3</b>	<b>State of the Art</b> .....	<b>13</b>
3.1	Introduction to the Main Concepts.....	13
3.1.1	CPSs and Associated Literature to Reliability Analysis and Requirements.....	13
3.1.2	Relationship to Other Networked Systems .....	14
3.1.3	Internet Communication Reliability .....	15
3.2	Approaches for Improving Communication Reliability for CPSs.....	17
3.3	Approaches for Improving Communication Reliability in Other Domains.....	19
3.4	MP Communication Protocols .....	20
3.5	Research Gap in the Literature.....	23
<b>4</b>	<b>Technological Background</b> .....	<b>27</b>
4.1	Data Communication Networks .....	27
4.2	Impact of Communication Network Deficiencies .....	31
4.3	Middleboxes.....	33
4.3.1	Firewalls .....	34
4.3.2	Network address translators.....	35
4.4	Communication Networks for CPSs .....	36
4.5	MP Communication .....	38
4.6	Smart Grid Applications.....	39
<b>5</b>	<b>Reliable Multipath Communication for Internet-based CPSs (RC4CPS) – Concept</b> .....	<b>43</b>
5.1	System Model.....	43
5.2	Optimization Formulation for MP Selection.....	45
5.2.1	MP Diversity.....	45
5.2.2	MP Future Unavailability .....	46
5.2.3	MP Selection.....	47
5.3	Architecture for RC4CPS.....	48



5.4	Online Procedures for MP Selection .....	50
5.5	Initial Monitoring for Model Selection (IMMS) .....	51
<b>6</b>	<b>Characterizing Internet Paths Diversity and Unavailability .....</b>	<b>53</b>
6.1	End-systems Selection.....	53
6.2	Data Sets .....	53
6.2.1	Traceroute Data Set .....	54
6.2.2	Ping Data Set .....	54
6.3	Diversity Evaluation of Internet Paths .....	54
6.3.1	Measurement Setups.....	54
6.3.2	Measurement Results.....	56
6.4	Unavailability Evaluation of Internet Paths .....	59
6.4.1	Measurement Setups.....	59
6.4.2	Measurement Results.....	61
6.5	Limitations of Measurements.....	64
<b>7</b>	<b>Online Monitoring and Prediction.....</b>	<b>67</b>
7.1	Modeling e2e Path Unavailability Using Markov Chains.....	67
7.1.1	Path Traces .....	68
7.1.2	Gilbert Model .....	68
7.1.3	Extended Gilbert Model.....	69
7.1.4	General Markov Chain Model .....	71
7.1.5	Hidden Markov Chain Model.....	72
7.2	Accuracy of Path Models .....	73
7.3	Impact of Frequency and Type of Probing Packets.....	74
7.4	Comparison Test .....	77
<b>8</b>	<b>Implementation Considerations.....</b>	<b>79</b>
8.1	Assumptions for Utilizing RC4CPS.....	79
8.2	Requirements for implementing RC4CPS.....	80
8.2.1	Active Multihoming.....	80
8.2.2	Approach Layer in the OSI Model.....	80
8.2.3	Data Duplication .....	80
8.2.4	Path Selection .....	81
8.2.5	Compatibility with Middleboxes .....	81
8.2.6	Fairness.....	81
8.2.7	Open-source Development .....	81
8.3	Evaluation of MP Protocols .....	82
8.3.1	Transport layer.....	82
8.3.2	Application Layer and Session Layer.....	85
8.3.3	Selected MP protocol Candidate for RC4CPS.....	87
<b>9</b>	<b>Confidence Interval for MP communication Unavailability .....</b>	<b>89</b>

9.1	CI Estimation Methods.....	89
9.1.1	CI Using Parametric Approach.....	90
9.1.2	CI Using Non-parametric Approach.....	90
9.2	Sample Data for MP Unavailability .....	91
<b>10</b>	<b>Implementation and Evaluation of RC4CPS Using MATLAB.....</b>	<b>95</b>
10.1	Block Diagram of the Implementation.....	95
10.2	Evaluation .....	96
10.2.1	Evaluation Setup 1 .....	97
10.2.2	Results of Evaluation Setup 1 .....	97
10.2.3	Evaluation Setup 2.....	101
10.2.4	Scenarios and Results of Evaluation Setup 2.....	101
10.3	Discussion .....	110
10.3.1	MP Diversity Estimation .....	110
10.3.2	MP Unavailability Prediction .....	111
<b>11</b>	<b>Implementation and Evaluation of RC4CPS Using iPRP MP Transport Protocol.....</b>	<b>113</b>
11.1	Introduction.....	113
11.2	Protocol Description.....	113
11.2.1	Path Matching.....	114
11.2.2	Protocol Function Blocks.....	115
11.2.3	iPRP Header .....	116
11.2.4	Duplicate Discard Mechanism.....	117
11.3	iPRP implementation.....	117
11.3.1	Architecture .....	118
11.3.2	Session-information links and structures .....	120
11.3.3	Packet handling.....	121
11.4	iPRP-RC4CPS.....	122
11.4.1	iPRP limitations .....	123
11.4.2	Overview of modifications to iPRP .....	125
11.5	Path-selection daemon.....	128
11.5.1	Path monitoring: .....	128
11.5.2	Attributes Calculation .....	130
11.5.3	MP Selection.....	131
11.5.4	MP Reconfiguration.....	131
11.6	Evaluation .....	131
11.6.1	Redundancy and Overhead of iPRP and iPRP-RC4CPS .....	132
11.6.2	Measurements in Lab Environment .....	133
11.6.3	Measurements in the Internet.....	139

**12 Conclusion and Future Work..... 149**  
    12.1 Conclusion..... 149  
    12.2 Future Work ..... 151

**Appendix ..... 153**

**Appendix A: Detailed Diversity and Unavailability Results..... 153**

**Appendix B: Detailed Results for the Comparison Test ..... 163**

**Appendix C: Algorithms ..... 166**

**Appendix D: iPRP-RC4CPS Files and Functions..... 173**

**List of Tables..... 176**

**List of Figures ..... 179**

**References ..... 182**

# Abbreviations

5G	5th Generation
ACK	Acknowledgment
AGC	automatic generation control
AM	Attributes Matrix
AMI	Advanced Metering Infrastructure
AMPTCP	Augmented MPTCP
ANS	Autonomous System Number
API	Application Programming Interface
AS	Autonomous System
ASN	Autonomous System Number
CAN	Controller Area Network
CC	Congestion Control
<i>cc</i>	Correlation coefficient
CCC	Coupled Congestion Control
CDF	Cumulative Distribution Functions
CI	Confidence Interval
CMT/RP-SCTP	Resource Poolingenabled CMT-SCTP
CMT-SCTP	Concurrent Multipath Transfer SCTP
CPS	Cyber-physical System
cTCP	Concurrent TCP
CWAMPTCP	Congestion Window Adaptation MPTCP
DA	Distribution Automation
DARPA	United States Defense Advanced Research Projects Agency
DAR-SCTP	Dynamic Address Reconfiguration SCTP
DBAS	Deployable Bandwidth Aggregation System
DCC	Data and Control Center
DE	Diversity Estimator
DNP3	Distributed Network Protocol 3
DR	Demand Response
DSM	Demand-side management
DSR	Dynamic Source Routing
DTLS	Datagram Transport Layer Security Session
e2e	End-to-end
E2EMPT	End-to-End Multipath Transfer
ECN	Explicit Congestion Notification
EGM	Extended Gilbert model
EtherCAT	Ethernet for Control Automation Technology
FEC	Forward Error Correction
FIP	Factory Instrumentation Protocol
FMTCP	Fountain-Code-Based MPTCP
FPS-SCTP	Forward Prediction Scheduling SCTP
FTP	File Transfer Protocol
G-DBAS	Green DBAS

HMM	Hidden Markov Model
i.i.d.	Independent and identically distributed
IA	Inter-arrival
ICD	iPRP Control Daemon
ICMP	Internet Control Message Protocol
IED	Intelligent Electronic Device
IMD	iPRP Monitoring Daemon
IMMS	Initial Monitoring for Model Selection
IND	iPRP Network subcloud Discriminator
IP	Internet Protocol
IPC	Interprocess Communication
IPD	iPRP Path-selection Daemon
iPRP	The Parallel Redundancy Protocol for IP Networks
iPRP_CAP	iPRP capability message
IRD	iPRP Receiver Daemon
ISD	iPRP Sender Daemon
ISP	Internet Service Provider
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LG	Looking Glass
LIA	Linked Increases Algorithm
LISP	Locator/Identifier Separation Protocol
LTE	Long-Term Evolution
M&E	Monitoring & Estimation
M/TCP	Multipath Transmission Control Protocol
M2M	Machine-to-Machine
MAP/EPA	Manufacturing Automation Protocol/Enhanced Performance Architecture
MC	Markov Chain
MP	Multipath
MPLS	Multiprotocol Label Switching
MPLOT	Multi-Path LOss-Tolerant
MP RTP	Multipath RTP
MPTCP	Multipath TCP
MPTCP-SPA	MPTCP Slow Path Adaptation
MPTS-AR	Multipath Transport System Based on Application-Level Relay
MTC	Machine-Type Communication
M-TCP	Multipath TCP
MuniSocket	Multiple Network Interface Socket
NAN	Neighborhood-area Network
NASPI	The North American Synchro-Phasor Initiative
NAT	Network Address Translator
NC-MPTCP	Network Coding Based MPTCP
NCC	Network Coordination Centre
NGMN	Next Generation Mobile Networks
NSP	Network service provider
OLIA	Opportunistic Linked Increases Algorithm
OPERETTA	Optimal Energy Efficient Bandwidth Aggregation System
OS	Operating system

OSI	Open System Interconnection
PC	Personal computer
PDU	Protocol data unit
PLC	Programmable logic controller
PMTUD	Path MTU Discovery
PMU	Phasor Measurement Unit
PROFIBUS	PROcessField Bus
PROFINET	Process Field Net
PRP	Parallel Redundancy Protocol
PRR	Ping-Receive Routine
PSN	Probe sequence number
PSockets	Parallel Sockets
PSR	Ping-Send Routines
PSW	Pattern start window
pTCP	Parallel TCP
PUM	Path Usage Method
PW	Pattern window
QoS	Quality of Service
QoS-MPTCP	QoS-oriented MPTCP
RC4CPS	Reliable Multipath Communication for Internet-based CPSs
RI2N/UDP	UDP-based Redundant Interconnection with Inexpensive Network
RIPE	Abbreviated from French for "European IP Networks"
R-M/TCP	Rate-based M/TCP
RMTP	Reliable Multiplexing Transport Protocol
RON	Resilient Overlay Network
RP	Resource Pooling
RT	Real-time
RTP	Real-Time Transport Protocol
RTT	Roundtrip time
RTU	Remote terminal unit
SCADA	Supervisory Control and Data Acquisition
SC-MPTCP	Systematic Coding MPTCP
SCTP	Stream Control Transmission Protocol
SDN	Software-defined Networking
SN	Sequence Number
SNSID	Sequence-Number-Space ID
SR	Selection Routine
SSR	Subflow Sender Reports
TCP	Transmission Control Protocol
TTL	Time-to-Live
UC	Unavailability Calculator
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
UP	Unavailability Predictor
VN	Virtual node
WAN	Wide Area Network

WASA	Wide Area Situational Awareness
WAVSM	Wide-area Voltage Stability Monitoring
WRR	Weighted Round-Robin
WSN	Wireless Sensor Network