Daphne Tuncer · Robert Koch
Rémi Badonnel · Burkhard Stiller (Eds.)

LNCS 10356

Security of Networks and Services in an All-Connected World

11th IFIP WG 6.6 International Conference
on Autonomous Infrastructure, Management, and Security, AIMS 2017
Zurich, Switzerland, July 10–13, 2017, Proceedings

ifip

also developed by scimago: SCIMAGO INSTITUTIONS RANKINGS

SJR Scimago Journal & Country Rank Enter Journal Title, ISSN or Publisher Name

Home Journal Rankings Country Rankings Viz Tools Help About Us

Lecture Notes in Computer Science

COUNTRY

Germany

Universities and research institutions in Germany

Media Ranking in Germany

SUBJECT AREA AND CATEGORY

Computer Science
- Computer Science (miscellaneous)

Mathematics
- Theoretical Computer Science

PUBLISHER

Springer Verlag

H-INDEX

415

PUBLICATION TYPE

Book Series

ISSN

03029743, 16113349

COVERAGE

1937, 1955, 1973-2021

INFORMATION

Homepage

How to publish in this journal

lncs@springer.com

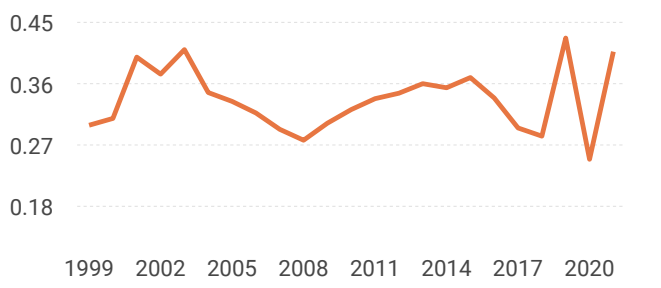
SCOPE

This distinguished conference proceedings series publishes the latest research developments in all areas of computer science.

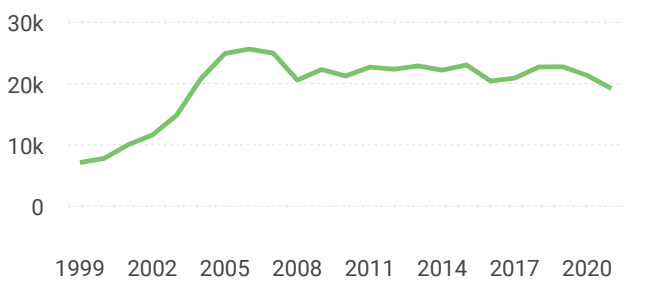
Join the conversation about this journal

Quartiles

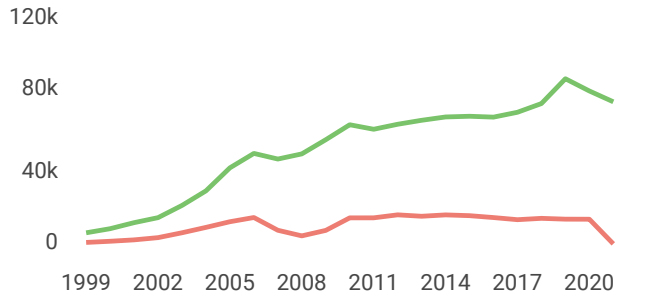
SJR



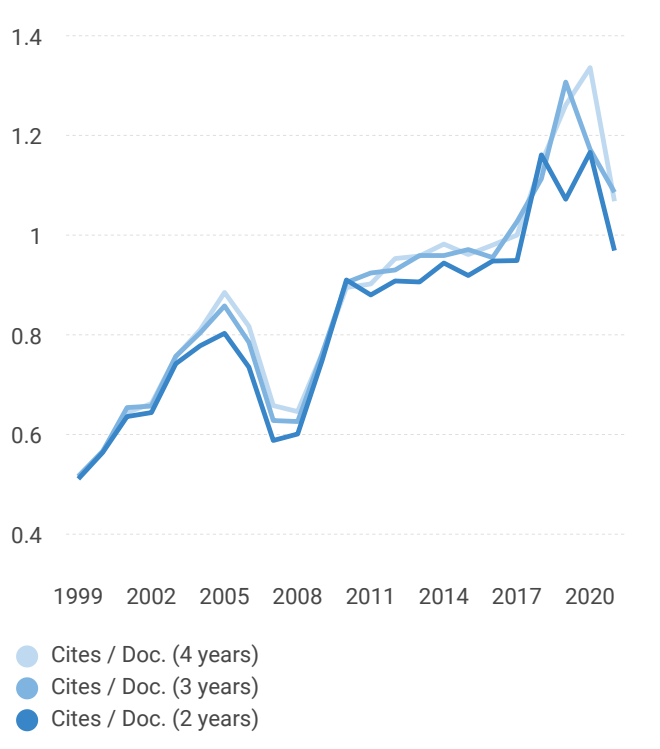
Total Documents



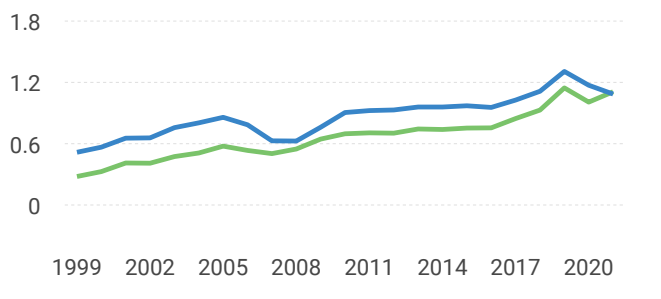
Total Cites Self-Cites



Citations per document

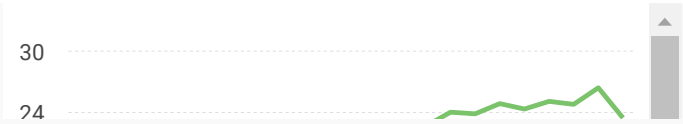


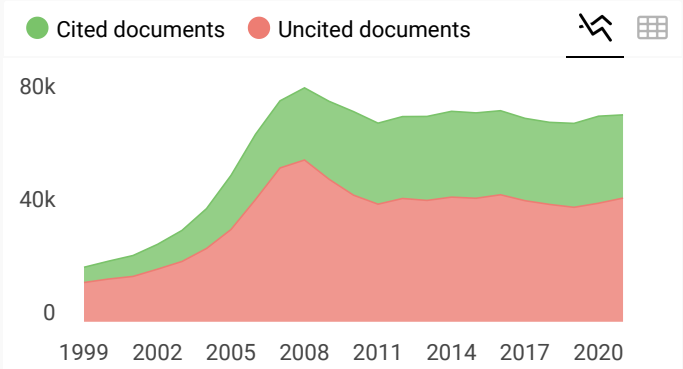
External Cites per Doc Cites per Doc

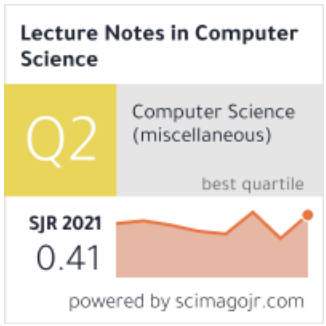


% International Collaboration

Citable documents Non-citable documents







← Show this widget in your own website

Just copy the code below and paste within your html code:

<a href="https://www.scimag

SCImago Graphica

Explore, visually communicate and make sense of data with our **new data visualization tool**.

Metrics based on Scopus® data as of April 2022

Vladimir Zyubin 1 year ago

4 Feb 2022: Thank you for your site. But why does your journal quartile data not match the original Scopus data for LNCS? You calculated Q3-Q4, but according to Scopus (https://www.scopus.com/sources.uri) the current quartile of the journal is Q2.

reply

SCImago Team

Melanie Ortiz 1 year ago

Dear Vladimir, Thank you for contacting us.
As you probably already know, our data come from Scopus, they annually send us an update of the data. This update is sent to us around April / May every year.
The calculation of the indicators is performed with the copy of the Scopus database provided to us annually. However, the methodology used concerning the distribution of

Lecture Notes in Computer Science **10356**

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison
Lancaster University, Lancaster, UK
Takeo Kanade
Carnegie Mellon University, Pittsburgh, PA, USA
Josef Kittler
University of Surrey, Guildford, UK
Jon M. Kleinberg
Cornell University, Ithaca, NY, USA
Friedemann Mattern
ETH Zurich, Zurich, Switzerland
John C. Mitchell
Stanford University, Stanford, CA, USA
Moni Naor
Weizmann Institute of Science, Rehovot, Israel
C. Pandu Rangan
Indian Institute of Technology, Madras, India
Bernhard Steffen
TU Dortmund University, Dortmund, Germany
Demetri Terzopoulos
University of California, Los Angeles, CA, USA
Doug Tygar
University of California, Berkeley, CA, USA
Gerhard Weikum
Max Planck Institute for Informatics, Saarbrücken, Germany

More information about this series at http://www.springer.com/series/7411

Daphne Tuncer · Robert Koch
Rémi Badonnel · Burkhard Stiller (Eds.)

Security of Networks and Services in an All-Connected World

11th IFIP WG 6.6 International Conference
on Autonomous Infrastructure, Management, and Security, AIMS 2017
Zurich, Switzerland, July 10–13, 2017
Proceedings

Springer Open

Editors
Daphne Tuncer
University College London
London
UK

Rémi Badonnel
LORIA - Inria
Villers-lès-Nancy
France

Robert Koch
Universität der Bundeswehr München
Neubiberg
Germany

Burkhard Stiller
University of Zurich
Zurich
Switzerland

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-60773-3 ISBN 978-3-319-60774-0 (eBook)
DOI 10.1007/978-3-319-60774-0

Library of Congress Control Number: 2017943842

LNCS Sublibrary: SL5 – Computer Communication Networks and Telecommunications

© The Editor(s) (if applicable) and The Author(s) 2017. This book is an open access publication.
Open Access This book is licensed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.
The images or other third party material in this book are included in the book's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the book's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.
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, express 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.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2017) is a single-track event targeted at junior researchers and PhD students in network and service management and security. It features a range of sessions including conference paper presentations, hands-on lab courses, and educational keynotes. One of the key goals of AIMS is to offer junior researchers and PhD students a dedicated place where they can discuss their research work and experience, receive constructive feedback from senior scientists, and benefit from practical hands-on sessions on emerging technologies. By putting the focus on junior researchers and PhD students, AIMS acts as a complementary piece in the set of international conferences in the network and service management community, providing an optimal environment for in-depth discussions and networking.

AIMS 2017 — which took place during July 10-13, 2017, in Zürich, Switzerland, and was hosted by the University of Zürich — was the 11th edition of a conference series on management and security aspects of distributed and autonomous systems. It followed the already established tradition of an unusually vivid and interactive conference series, after successful events in Munich, Germany, in 2016, Ghent, Belgium, in 2015, Brno, Czech Republic, in 2014, Barcelona, Spain, in 2013, Luxembourg, Luxembourg, in 2012, Nancy, France, in 2011, Zürich, Switzerland, in 2010, Enschede, The Netherlands, in 2009, Bremen, Germany, in 2008, and Oslo, Norway, in 2007.

AIMS 2017 focused on security of networks and services in an all-connected world. To address these challenges, solutions for the design, monitoring, configuration, and protection of the next generation of networked systems in an efficient, secure, and smart manner are investigated. The theme is reflected in the technical program with papers presenting novel approaches and evaluation studies for the security management of rich network services and environments. AIMS 2017 was organized as a 4-day program to encourage the active participation of and interaction with the audience. The program consisted of technical sessions for the main track and PhD sessions, interleaved with three lab sessions and two keynotes.

The lab sessions offered hands-on experience in the topics of security and advanced network management techniques, and were organized in on-site labs preceded by short tutorial-style teaching sessions. The first lab session was run by Martin Drašar (Masaryk University, Czech Republic) and focused on an introduction to security games. The second lab session was supervised by Thomas Bocek and Moritz Schneider (University of Zürich, Switzerland) and presented how to program smart contracts. Finally, the last session was held by Salvatore Signorello (University of Luxembourg, Luxembourg) and Jérôme François (Inria, France) and explored P4, the emerging high-level data plane programing language and its applicability to packet processors.

The keynotes were presented by two experts in their domain: Marcel Waldvogel (University of Konstanz, Germany), who discussed “Getting Rid of IoT Insecurity,” and Matthias Bossardt (KPMG, Switzerland), who shared his view with the audience on “Cyber Security Challenges – A Business Perspective.”

The technical program consisted of six sessions, divided into three full-paper sessions and three short-paper sessions. The three full-paper sessions covered technical presentations on the themes of: (1) Security Management, (2) Management of Cloud Environments and Services, and (3) Evaluation and Experimental Study of Rich Network Services. They included a total of eight full papers, which were selected after a thorough reviewing process out of 24 submissions. Each paper received at least three independent reviews. The three short-paper sessions included 11 short papers. These covered PhD research papers on the themes of "Methods for the Protection of Infrastructure and Services," and "Autonomic and Self-Management Solutions" as well as six short presentations on the topic of "Security, Intrusion Detection, and Configuration."

During all the PhD research presentations, doctoral students had the opportunity to present and discuss their research ideas, and more importantly to obtain valuable feedback from the AIMS audience about their PhD research work. All PhD research proposals included in this volume describe the current state of these investigations, including well-defined research problem statements, proposed approaches, and an outline of emerging and promising results achieved to date.

The present volume of the *Lecture Notes in Computer Science* series includes all papers presented at AIMS 2017 as defined within the overall final program. It demonstrates again the European scope of this conference series, since most of the accepted papers originate from European research groups. In addition, by hosting two tracks specifically dedicated to research proposals, AIMS 2017 stayed true to its defined DNA of a conference with a strong educational goal, focusing especially on issues and challenges associated with the security of networks and services.

The editors would like to thank the many people who helped to make AIMS 2017 such a high-quality and successful event. Firstly, many thanks are extended to all authors who submitted their contributions to AIMS 2017, and to the lab session speakers as well as the keynote speakers. The great review work performed by the members of the AIMS Technical Program Committee as well as additional reviewers is greatly acknowledged. Thanks also to Thomas Bocek and Martin Drašar for organizing the lab sessions. Additionally, many thanks are extended to the local organizers for handling logistics and hosting the AIMS 2017 event.

Finally, the editors would like to express their thanks to Springer, especially Anna Kramer, for the smooth cooperation in finalizing these proceedings. Additionally, special thanks go to the AIMS 2017 supporters, University of Zürich UZH, Communication Systems Group CSG, Research Institute for Cyber Defense and Smart Data CODE, München, Germany, and the European FP7 NoE FLAMINGO under Grant No. 318488.

May 2017

Daphne Tuncer
Robert Koch
Rémi Badonnel
Burkhard Stiller

Organization

General Chair AIMS 2017

Burkhard Stiller	University of Zürich, Switzerland

Technical Program Committee Co-chairs

Daphne Tuncer	University College London, UK
Robert Koch	Universität der Bundeswehr München, Germany

Labs Co-chairs

Martin Drašar	Masaryk University, Czech Republic
Thomas Bocek	University of Zürich, Switzerland

Publications Co-chairs

Rémi Badonnel	LORIA, Inria, France
Burkhard Stiller	University of Zürich, Switzerland

Local Chair

Barbara Jost	University of Zürich, Switzerland

Publicity Chair and Web Master

Corinna Schmitt	University of Zürich, Switzerland

AIMS Steering Committee

Anna Sperotto	University of Twente, The Netherlands
Pavel Čeleda	Masaryk University, Czech Republic
Filip De Turck	Ghent University - iMinds, Belgium
Rémi Badonnel	LORIA, Inria, France
Aiko Pras	University of Twente, The Netherlands
Burkhard Stiller	University of Zürich, Switzerland
Robert Koch	Universität der Bundeswehr München, Germany

Technical Program Committee

Alexander Clemm	Huawai, USA
Alexander Keller	IBM Global Technology Services, USA

Alva L. Couch	Tufts University, USA
Anandha Gopalan	Imperial College London, UK
Anna Sperotto	University of Twente, The Netherlands
Bertrand Mathieu	Orange Labs, France
Bruno Quoitin	Université de Mons, Belgium
Burkhard Stiller	University of Zürich, Switzerland
Daniele Sgandurra	Imperial College London, UK
David Hausheer	Otto-von-Guericke Universität Magdeburg, Germany
Filip De Turck	Ghent University - iMinds, Belgium
Gabi Dreo Rodosek	Universität der Bundeswehr München, Germany
Guillaume Doyen	Troyes University of Technology, France
Isabelle Chrisment	TELECOM Nancy, Université de Lorraine, France
Jan Kořenek	Brno University of Technology, Czech Republic
Jérôme François	Inria Nancy Grand Est, France
Joan Serrat	Universitat Politècnica de Catalunya, Spain
Jürgen Schönwälder	Jacobs University Bremen, Germany
Kurt Tutschku	Blekinge Institute of Technology, Sweden
Lisandro Zambenedetti Granville	UFRGS, Brazil
Mario Golling	Universität der Bundeswehr München, Germany
Martin Barrère	Imperial College London, UK
Mauro Tortonesi	University of Ferrara, Italy
Michelle Sibilla	Paul Sabatier University, France
Olivier Festor	INRIA Nancy Grand Est, France
Pavel Čeleda	Masaryk University, Czech Republic
Philippe Owezarski	LAAS-CNRS, France
Rashid Mijumbi	Waterford Institute of Technology, Ireland
Rémi Badonnel	Telecom Nancy, Université de Lorraine, France
Ricardo Schmidt	University of Twente, The Netherlands
Roberto Riggio	CREATE-NET, Italy
Steven Latré	University of Antwerp, iMinds, Belgium
Thomas Bocek	University of Zürich, Switzerland

Additional Reviewers

Detailed reviews for papers submitted to AIMS 2017 were undertaken by the Technical Program Committee as listed above and additionally by the following reviewers:

Messaoud Aouadj, Jeremias Blendin, Remi Cogranne, Ariel Dalla-Costa, Muriel Franco, Borislava Gajic, Christian Jacquenet, Christian Koch, Radek Krejci, Genaro Longoria, Christian Mannweiler, Hassnaa Moustafa, Tan Nguyen, Leonhard Nobach, Vinícius Schaurich, and Eder John Scheid.

Keynotes

Getting Rid of IoT Insecurity

Marcel Waldvogel

University of Konstanz, Distributed Systems Group, Universitätsstr. 10/229,
78457 Konstanz, Germany
Marcel.Waldvogel@uni-konstanz.de

Abstract. The Internet-of-Things (IoT) is already everywhere, but even then, there is still much more to come. Right now, IoT security is a mess, chaotic, unsustainable, and unmanageable. To prevent this is going to remain like this, and that these devices will continue to risk or endanger increasing amounts of our and everybody's lives, we need coordinated actions by manufacturers, vendors, integrators, ISPs, and customers.

But it is the researchers, you, who need to make a long-term difference: how to create blueprints, on which new products may be based, which may include design for privacy, security, manageability, while not overwhelming the users is probably the biggest challenge of them all.

This talk will present three examples, which clearly outlines the challenges, describes open problems, and proposes a coherent framework, into which your next solutions hopefully will fit.

Cyber Security Challenges – A Business Perspective

Matthias Bossardt

Lead Partner for Cyber Security, KPMG Switzerland, Zürich, Switzerland
mbossardt@kpmg.com

Abstract. This keynote will shed light on real world challenges that companies face when dealing with cyber threats on a global scale. In global organizations and where cyber security has to scale to hundred thousands of employees, contractors, suppliers, and clients as well as thousands of business processes and applications, understanding the organization's risk exposure and implementing effective protection measures is very complex.

And the plethora of challenges related to the (Industrial) Internet-of-Things and managing cyber security becomes a daunting task. To secure an organization, understanding human behavior and mastering organizational change is as important as implementing security technology. This talk will discuss those security capabilities needed in an organization and it will highlight those topics that can benefit greatly from additional research.

Lab Sessions

Hacking your Way to Safety – A Beginner's Guide to Security Games

Martin Drašar

CSIRT-MU, Masaryk University, Brno, Czech Republic
drasar@ics.muni.cz

Abstract. Maintaining infrastructure security or hardening a system is never a simple task. Nor it is a one-click operation. Often it requires the adoption of attacker's mindset to identify correctly weak spots or to even understand that a threat is imminent. This, however, is not possible without acquiring a large body of knowledge, which is usually dispersed around the Internet or available only as dry technical reports. While the process of assembling these bits of information may appeal to somebody, a majority will prefer something more entertaining. Security games are one such approach.

This lab is aimed at beginners and will serve as a brief introduction to hacking as a way to better understand computer security. It will discuss available learning resources and focus mostly on security games: why, which, where, and how to play them for maximum benefit? It will also give participants an opportunity to try out some of these games in a guided manner. These games will be executed both locally as virtual machines on attendees' laptops and remotely in a virtual sandbox environment [1]. Attendees will also be asked to participate in a survey regarding skill self-assessment and effectiveness of knowledge transfer, which fosters further research as presented in [2].

References

1. Kourill, D., Rebok, T., Jirsik, T., Čegan, J., Drasar, M., Vizvary, M., Vykopal, J.: Cloud-based Testbed for Simulation of Cyber Attacks. In: IFIP/IEEE Network Operations and Management Symposium. NOMS 2014, Krakow, Poland, May 2016
2. Ykopal, J., Bartak, M.: On the Design of Security Games: From Frustrating to Engaging Learning, In: USENIX Workshop on Advances in Security Education. ASE 2016, Austin, Texas, USA, August 2016

Programming Smart Contracts

Thomas Bocek and Moritz Schneider

University of Zürich UZH, Department of Informatics IfI, Communication Systems Group CSG, Binzmühlestrasse 14, 8050 Zürich, Switzerland
bocek@ifi.uzh.ch, moritz.schneider3@uzh.ch

Abstract. Blockchains and smart contracts have gained a lot of attention. Public blockchains are considered secure and exist without centralized control. As one of the most prominent blockchain examples, Bitcoin has the potential to disrupt financial services. However, the blockchain technology is applicable to a wider range of application domains, such as smart contracts, public registries, registry of deeds, or virtual organizations.

Another prominent blockchain example, Ethereum, which is considered a general approach for smart contracts, is the second biggest public blockchain with respect to market capitalization. A smart contract in Ethereum [1] is written in the language Solidity [2]. These contracts allow not only sending and receiving funds, but since Solidity its a Turing-complete language, it allows for the definition of any kind of rules.

The introduction of this lab session will address the history and an overview of blockchains as well as their categorization. Blockchain basics are explained in terms of basic building blocks and how they work, including the essential consensus mechanisms. Thus, the Solidity language is introduced in terms of syntax and main constructs, combined with simple code snippets and examples [3]. The audience will compile and deploy a simple smart contract with the goal to familiarize itself with the language and the development environment. Furthermore, the lab shows on the basis of Ethereum smart contracts how to create your own tokens or cryptocurrency [4]. The tokens or cryptocurrency initiator can create initial tokens that can be transferred to any address.

References

1. Homestead Release: ethereum. https://www.ethereum.org/. Accessed May 1, 2017
2. Solidity. http://solidity.readthedocs.io. Accessed May 1, 2017
3. Contract examples for Ethereum. https://github.com/fivedogit/solidity-baby-steps. Accessed May 1, 2017
4. Create your own crypto-currency with Ethereum. https://www.ethereum.org/token. Accessed May 1, 2017

Programming Data Planes in P4 – A High-level Language for Packet Processors

Salvatore Signorello[1] and Jérôme François[2]

[1] SnT, University of Luxembourg, Luxembourg, and LORIA, University of Nancy, Nancy, France
[2] MADYNES Team at INRIA, Nancy Grand-Est, France
salvatore.signorello@uni.lu, jerome.francois@inria.fr

Abstract. This lab will introduce the audience to the P4 language [1], providing them with the knowledge necessary to develop and prototype their own research ideas in P4. The lab starts by providing an overview of the research that led to the emergence of the language and by illustrating the P4 language consortium objectives and related ongoing activities. Additionally, the lab explains the P4 language programming model and introduces an open source development environment [2], which can be used to write and test P4 programs on a single machine. The presented software toolset includes a P4 front-end compiler, a P4 software target, and the Command Line Interface (CLI) used to program this target at run-time. Finally, the lab interactively presents the language's syntax and main constructs.

Throughout the entire lab, simple P4 code snippets and examples are written, compiled, and executed by the participants. Furthermore, full assignments of increasing complexity are proposed to strengthen the understanding of the programming model and of the main language constructs. More in detail, simple tasks, like the definition of a custom encapsulation protocol and the implementation of an access control list, help the audience to familiarize itself with the definition and the parsing of new protocols and with the definition of the control flow of a P4 program. While more complex assignments, like the implementation of a port-knock firewall, are meant to explore advanced language constructs, which can be used to implement stateful network functions.

References

1. Bosshart, P., Daly, D., Gibb, G., Izzard, M., McKeown, N., Rexford, J., Schlesinger, C., Talayco, D., Vahdat, A., Varghese, G., Walker, D.: P4: Programming Protocol-independent Packet Processors. Comput. Commun. Rev. **44**(3), 87–95
2. P4. http://p4.org/join-us

Contents

Security Management

Making Flow-Based Security Detection Parallel 3
Marek Švepeš and Tomáš Čejka

A Blockchain-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts 16
Bruno Rodrigues, Thomas Bocek, Andri Lareida, David Hausheer, Sina Rafati, and Burkhard Stiller

Achieving Reproducible Network Environments with INSALATA 30
Nadine Herold, Matthias Wachs, Marko Dorfhuber, Christoph Rudolf, Stefan Liebald, and Georg Carle

Management of Cloud Environments and Services

Towards a Software-Defined Security Framework for Supporting Distributed Cloud 47
Maxime Compastié, Rémi Badonnel, Olivier Festor, Ruan He, and Mohamed Kassi-Lahlou

Optimal Service Function Chain Composition in Network Functions Virtualization 62
Andrés F. Ocampo, Juliver Gil-Herrera, Pedro H. Isolani, Miguel C. Neves, Juan F. Botero, Steven Latré, Lisandro Zambenedetti, Marinho P. Barcellos, and Luciano P. Gaspary

Evaluation and Experimental Study of Rich Network Services

An Optimized Resilient Advance Bandwidth Scheduling for Media Delivery Services 79
Maryam Barshan, Hendrik Moens, Bruno Volckaert, and Filip De Turck

The Evaluation of the V2VUNet Concept to Improve Inter-vehicle Communications 94
Lisa Kristiana, Corinna Schmitt, and Burkhard Stiller

Towards Internet Scale Quality-of-Experience Measurement with Twitter 108
Dennis Kergl, Robert Roedler, and Gabi Dreo Rodosek

Short Papers: Security, Intrusion Detection, and Configuration

Hunting SIP Authentication Attacks Efficiently 125
Tomáš Jansky, Tomáš Čejka, and Václav Bartoš

MoDeNA: Enhancing User Security for Devices in Wireless Personal and Local Area Networks 131
Robert Müller, Marcel Waldvogel, and Corinna Schmitt

Flow-Based Detection of IPv6-specific Network Layer Attacks 137
Luuk Hendriks, Petr Velan, Ricardo de O. Schmidt, Pieter-Tjerk de Boer, and Aiko Pras

Towards a Hybrid Cloud Platform Using Apache Mesos 143
Noha Xue, Hårek Haugerud, and Anis Yazidi

Visual Analytics for Network Security and Critical Infrastructures 149
Karolína Burská and Radek Ošlejšek

Preserving Relations in Parallel Flow Data Processing 153
Tomáš Čejka and Martin Žádník

Ph.D. Track: Autonomic and Self-Management Solutions

SmartDEMAP: A Smart Contract Deployment and Management Platform . . . 159
Markus Knecht and Burkhard Stiller

Optimizing the Integration of Agent-Based Cloud Orchestrators and Higher-Level Workloads 165
Merlijn Sebrechts, Gregory Van Seghbroeck, and Filip De Turck

Ph.D. Track: Methods for the Protection of Infrastructure and Services

Situational Awareness: Detecting Critical Dependencies and Devices in a Network 173
Martin Laštovička and Pavel Čeleda

A Framework for SFC Integrity in NFV Environments 179
Lucas Bondan, Tim Wauters, Bruno Volckaert, Filip De Turck, and Lisandro Zambenedetti Granville

Multi-domain DDoS Mitigation Based on Blockchains 185
Bruno Rodrigues, Thomas Bocek, and Burkhard Stiller

Author Index 191

Evaluation and Experimental Study of Rich Network Services

The Evaluation of the V2VUNet Concept to Improve Inter-vehicle Communications

Lisa Kristiana[1,2(✉)], Corinna Schmitt[1], and Burkhard Stiller[1]

[1] Communication Systems Group CSG, Department of Informatics IfI, University of Zürich, Binzmühlestrasse 14, 8050 Zurich, Switzerland
{kristiana, schmitt, stiller}@ifi.uzh.ch
[2] The Department of Informatics, National Institute of Technology, Bandung 40124, Indonesia
lisa@itenas.ac.id

Abstract. Due to the high mobility behavior in inter-vehicle communications (IVC), packet forwarding among vehicles becomes an important issue. For IVC in a traditional packet forwarding setting, it was observed that the ratio between packets received and the packets transmitted is often very low, sometimes less than 50%. This ratio is highly influenced by the environment, especially by road topologies and obstructions (*e.g.*, buildings or overpasses). Further influences encompass the number of driving vehicles on streets offering burdens for the IVC as well as serving as relay candidates. In order to improve IVC this paper introduces a Vehicular-to-Vehicular Urban Network (V2VUNet) to overcome inevitable obstructions and frequent network changes by selecting the best relay candidate. The V2VUNet implemented was evaluated in an IVC with the focus on three-dimensional road topologies including overpasses with a different number of driving lanes. The result shows that the developed V2VUNet provides about 30% better packet transmission performance compared to traditional packet transmission in IVC.

1 Introduction

Inter-vehicle networks as a part of Vehicular Ad-hoc Network (VANET) are expected to support communications with multiple participating vehicles [3]. Thus, information exchanges in a vehicular network communication require stable and reliable connections. During packet transmissions and receptions the communication path has to be maintained in any cases. For IVC in a traditional packet forwarding setting, it was observed that the Packet Delivery Ratio (PDR) as the indicator of network performance is often less than 50% due to path failures [19]. These path failures are mainly caused by the road topology complexity of the environment, such as overpass constructions and buildings at intersection roads [9].

For inter-vehicle communications, a position-based forwarding scheme is generally used, since it offers an advantage of not relying on packet broadcasting in its routing mechanisms. Since position information is already made available, the approach proposed in this paper, the Vehicular-to-vehicular Urban Network (V2VUNet), emphasizes in filtering unnecessary participant nodes [18] and predicting the routing path based on

© The Author(s) 2017
D. Tuncer et al. (Eds.): AIMS 2017, LNCS 10356, pp. 94–107, 2017.
DOI: 10.1007/978-3-319-60774-0_7

the position information and on the calculated direction information [17]. Therefore, the packet forwarding scheme is expected to become more efficient. In this research work, the packet forwarding is tested in two types of road environment models. The first type is the cross road model and the second type is the parallel road model. Both types reflect the three-dimensions cases with three coordinate axes x, y, and z. The advance beyond state-of-the-art in this three-dimensional area is determined by the z axis, which in many of VANET scenarios is rarely included. In addition, the three-dimensional case in VANET is significantly influenced by objects placed between signal transmitting devices. These objects can be a building or an overpass. Therefore, it is important to investigate the packet forwarding in these three-dimensional environments. Besides a better performance, the packet forwarding scales best in case of non-safety or non-real-time applications, which can be considered as delay constraint. Thus, delays are evaluated here as a less significant characteristic.

Another relevant aspect today is the use of Multiple Input Multiple Output (MIMO) technology in Inter-vehicle Communication (IVC). MIMO is a method to increase the radio link capacity and becomes a promising solution, since it increases the number of transmitted data by embedding multiple transmitters and receivers [15]. This method is useful to be implemented in a non-safety application, such as for infotainment, since it requires high data rates and large amount of data interchanges. However, as this work in this paper here focuses on the network layer, MIMO is better to be evaluated in the data link layer.

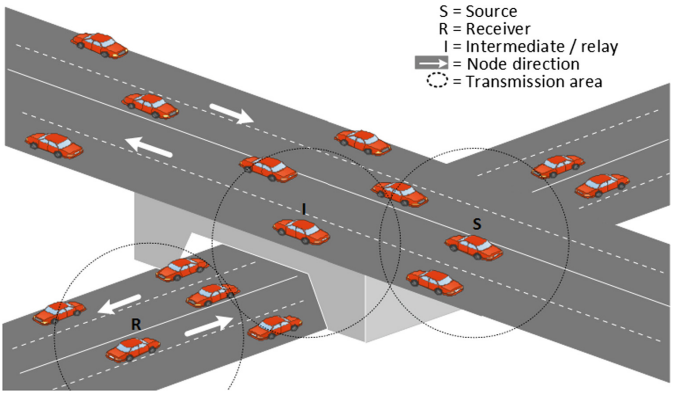


Fig. 1. Inter vehicle communication in a three-dimensional road topology

In previous works as shown in [17, 18], the evaluation of network performance of each approach is compared to a traditional location-based routing. This paper ensues to evaluate both forwarding approaches in V2VUNets by implementing various size of packets, different network densities, and speed of vehicles. The remainder of this paper is organized as follows: Sect. 2 describes related work of the packet forwarding model used. Section 3 introduces the key idea of the vertical angle forwarding scheme being part of a V2VUNet. Additionally, the evaluation of the V2VUNet is discussed in Sect. 4, followed by the summary and future work in Sect. 5.

2 Related Work

Successful communication requires an efficient packet forwarding. Packet forwarding is considered as efficient, when the packet is broadcasted with a smaller probability of errors. Packet forwarding for non-safety applications refers to numerous size of data and is assumed to be distributed at a high rate [1–3]. Therefore, dealing with frequent topology changes in IVC's behavior, the packet forwarding is based on the method of forwarding [2, 5–7]. The first idea is to avoid collision in a dense network [8], thus, the packet forwarding is designed to reduce the number of relay candidates by restricting the area of transmission [18]. The second idea is to predict the direction of relay candidates by calculating the relative direction of a relay and by selecting the candidate that has the same direction with the destination's direction [17]. It is obvious that the relay having the same direction with the destination increases the possibility to prolong the duration of a connection between communicating vehicles. Thus, in a large city environment with its road topology and traffic complexity [5], both approaches will be evaluated to perform a reliable data transmission in VANETs, more specifically in IVC. The two concepts of packet forwarding in IVC are studied in a survey that shows relevant literatures [4–7, 16]. While the first concept follows an angle-based forwarding approach, the second concept is defined as direction-based forwarding approach.

2.1 Angle-Based Forwarding

An angle-based forwarding mechanism utilizes angle measurement to reduce the area of transmission. The idea of implementing angle is to locate relay candidates within the transmission range of a sender *S*. Thus, under the assumption that the location coordinate of a receiver *R* is known, the imaginary line is drawn in order to scale the angle as shown in Fig. 2. The angle-based forwarding mechanism selects one of the relay candidates as the intermediate relay based on the location where it has the smallest angle calculation respect to an imaginary line [11, 12]. As illustrated in Fig. 2, *S* selects node *C* as the relay node since *C* has the smallest angle value. The advantage of this mechanism suits on the dense network because of the efficient route path in terms of time [12, 13]. The comparison of existing angle forwarding schemes has been done in [21].

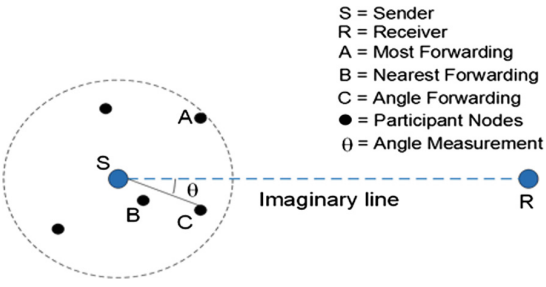


Fig. 2. Angle forwarding scheme

2.2 Direction-Based Forwarding

In IVC, vehicles are assumed to move on a predefined path such a straight or intersection road. Thus, vehicles can have heterogeneous directions depend on the road types. In order to cover route loss due to the 'free' movement of vehicles, the direction-based forwarding mechanism involves direction as a weight value to determine the next relay node. The direction has a dynamic value since it depends on the road topology and time-based factor. The direction value is calculated based on the sender and receiver position as illustrated in Fig. 3.

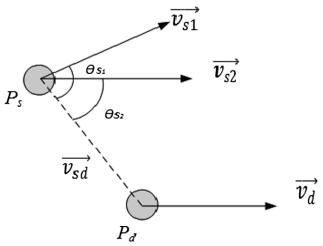


Fig. 3. A relative direction of a vehicle

3 V2VUNet Concept

The concept used in V2VUNet is an enhancement of the selection method in order to find the best relay node of available candidates [1, 4]. Previous work of V2VUNet determines the area restriction of transmission [18] and the path prediction [17]. Both area restriction and path prediction schemes in V2VUNet utilize the angle measurement on the same road level, *i.e.*, Horizontal Relative Angle (HRA) measurement and different road levels *i.e.*, Vertical Relative Angle (VRA) measurement. The implementation of V2VUNet in this work is performed to compare each algorithm in various parameters.

3.1 Area Restriction Scheme

In the area restriction scheme, the V2VUNet operates in two steps. The first step is to define the HRA with value of 30°, which is intuitively based on the width of a road in two-dimensional area and the closest distance between two vehicles. The second step is to adjust HRA based on the available relay candidates position. If the number of relay candidates is more than one, then the V2VUNet algorithm selects the relay based on the smallest value of HRA. The algorithm for the area restriction scheme is shown as in Algorithm 1 (cf. Fig. 4). The previously mentioned two steps are also applied in a three-dimensional area. Similar to HRA, VRA will be first defined as 30°, which is indicated as the preliminary angle value based on the transmission range. This 30° value is then increased gradually as part of the searching mechanism.

Algorithm 1

1. $S \leftarrow$ sender node
2. $R \leftarrow$ receiver node
3. I all neighboring nodes of S
4. $\theta_{x,max} \leftarrow$ maximum boundary of the horizontal angle
5. $\theta_{z,min} \leftarrow$ minimum boundary of the vertical angle
6. $\theta_{z,max} \leftarrow$ maximum boundary of the vertical angle
7. $\theta_x \leftarrow$ horizontal angle made by n to s
8. $\theta_z \leftarrow$ vertical angle made by n to s
9. $i_{filtered} \leftarrow$ only i that is within $[-\theta_{x,max}, \theta_{x,max}]$ and $[-\theta_{z,min}, \theta_{z,max}]$
10. $d \leftarrow$ distance from *ifiltered* to R, $nexthop \leftarrow arg_{min}$ (d)

Fig. 4. Area restriction algorithm

3.2 Path Prediction Scheme

In this scheme, the HRA is used to predict the direction of relay candidates. The prediction algorithm is designed to overcome the disconnection possibility due to the transmission coverage in two-dimensional area. In case of VRA, the algorithm is designed to encounter the disconnection due to obstruction by the overpass. Furthermore, HRA and VRA in this scheme use the relative direction of each vehicle. This relative direction provides the actual direction in three-dimensional scheme. The path prediction scheme is shown in Algorithm 2 (cf. Fig. 5).

Algorithm 2

1. $s \leftarrow$ sender node, at position of p_s and orientation of v_s
2. $i \leftarrow$ all neighboring nodes of s, at position of p_i and orientation of v_i
3. $\theta_{solid} \leftarrow$ threshold of the solid angle for all i
4. $v_{si} = |p_s - p_i|$
5. $\theta_{si} = \text{atan}\,(||v_s \times v_{si}||\,,\, ||v_s \cdot v_{si}||)$
6. $i_{filtered} \leftarrow i$ with θ_{si} within $[-\theta_{Solid}, \theta_{solid}]$
7. $d \leftarrow$ distance from $i_{filtered}$ to R
8. next hop $\leftarrow$ argmin (d)

Fig. 5. Path prediction algorithm

For the sake of a precise prediction, the direction that is used in V2VUNet algorithm determines a relative direction since the direction of each vehicle is measured in vehicle's current position. This relative direction is changed whenever a vehicle changes its position as illustrated in Fig. 3. Thus, the traditional direction calculation cannot be implemented in this prediction as it is done in [17]. Those two proposed algorithms are expected to provide a network performance as indicated by high PDR and low end-to-end (E2E) delays. In order to compare all algorithms implemented in this work, Table 1 shows a short description of each scheme and all related factors.

Table 1. Comparison of angle, area restricted, and path prediction forwarding algorithms

Factor	Angle-based forwarding	Area restriction	Path prediction
Coordinate location	*x*-, and *y*-axis	*x*-, *y*-, and *z*-axis	*x*-, *y*-, and *z*-axis
Weight value	HRA	HRA and VRA	HRA and VRA
Relative direction	No	No	Yes
Routing based	Greedy	Greedy	Greedy
Road topology	2D intersection, highway	3D intersection, 3D parallel	3D intersection, 3D parallel

As the first factor in this comparison table the coordinate location describes the coordinate axis which is used in measuring the current location of a node. The second factor is the weight value which determines the angle schemes, HRA for two-dimensional area and VRA for three-dimensional area. The third factor is the relative direction which is added in the path prediction algorithm in order to improve the calculation of the location coordinate. This relative direction factor is suitable when nodes move randomly and is useful to indicate the current direction of a node. Greedy routing is used in all algorithms because greedy routing uses the distance factor to do packet forwarding. Basically the greedy approach work best the many routing protocol mechanisms [10]. The last factor that influences all forwarding schemes is the road topology, which becomes the main idea of forwarding packet improvement. The angle-based forwarding scheme is used in two-dimensional intersection, where the direction factor becomes an important value, and in the highway, where the speed of a vehicle is highly considered. However, it is necessary to consider about the complexity of a road topology. Thus, the area restriction and path prediction schemes raise the three-dimensional road topology indicated as three-dimensional intersection (*i.e.*, cross road) and parallel roads.

As previously mentioned in the introduction section, this work evaluates and compares the area restriction and path prediction schemes as the improvement of traditional greedy routing.

4 Performance and Evaluation

The simulation in this work aims to validate the theoretical analysis of the proposed algorithms in IVC. Two simulation scenarios of a road environment with parallel and cross road topology are selected. In parallel road topology, the difference in vehicles' direction is more extreme than in a cross road topology. In a parallel topology, there are less chance that one vehicle can meet another vehicle once they pass each other. In a cross road topology, there is a segment of the road that is under another segment of the road, which could potentially contributes to disconnection at particular moment.

In order to obtain a realistic city environment, typical parameters for the influencing factors are chosen as shown in Table 2. The Network Simulator-3 (NS-3.25) [14] is used to simulate wireless technologies (*i.e.*, IEEE 802.11p), the routing protocol (*i.e.*, Greedy Perimeter Source Routing (GPSR) [10]), the mobility, the road topology, and

the network density. The IEEE 802.11p is a well known technology since it is designed to cope the frequent topology changing in IVC. During 200 s of simulation time, each vehicle is expected to run under and on the overpass in the first case, and on the different road level in the second case. *S*, *R*, and *I* are placed randomly both on two different road levels and SUMO [20] is used to generate the realistic mobility of each vehicle. Moreover, the number of *S* and *R* are generated equally, which means a 10-vehicle network contains of 5 senders and 5 receivers. The simulation area covers an environment which involves crossing and parallel overpass scenarios (c.f. Fig. 1) in order to show many cases in three-dimensional area.

In previous works, these two algorithms have not been evaluated over various packet sizes, thus, the packet size for the first evaluation is varied from 1–10 kB, especially for non-safety applications: a half page of unformatted email is 1 kB, one typical HTML webpage is 30 kB, 1 min of near-CD quality audio as MP3 or a 2048 × 1536 (4 megapixel) JPEG photo is 1 MB, to evaluate the size of packet that can be successfully transmitted in two algorithms. However, this simulation focuses only on transmitting email, with the size of the packet from 1 to 10 kB.

The first result (cf. Fig. 6) shows the PDR of all algorithms when different packet sizes are applied. This performed evaluation simulates 40 vehicles that move with an average speed of 40 km/h. The V2VUNet area restriction algorithm gives 20% better PDR compared to the greedy forwarding scheme which in the figure is indicated as No V2VUNet. V2VUNet area restriction also shows 10% better compared to V2VUNet-path prediction scheme. The showed PDR in overall algorithms decreases as the packet size increases, which indicates that more participating vehicles and simulation time are required to successfully complete the packet forwarding mechanism. V2VUNet indicates that HRA and VRA weight values have significant impacts in packet transmission.

Table 2. Parameter Settings

Parameter	Unit
Transmission range IEEE 802.11p	Up to 300 m
Routing protocols	GPSR
Number of vehicles	20–100
Simulation area	500 m × 500 m
Upper road height	20 m
Vehicle velocity	30–70 km/h
Packet size	1 kB–10 kB
Simulation time	200 s
Number of driving lanes	4
DSRC data rates	6 Mbps

The second result shows the E2E delay of all algorithms (cf. Fig. 7) when different data sizes are applied. The E2E delay increases as the packet size increases. This is because more time are required to transmit packet with bigger size. The E2E delay of 200 ms (highest delay) is indicated by path prediction scheme. This is because the path finding mechanism in the V2VUNet path prediction scheme requires more time

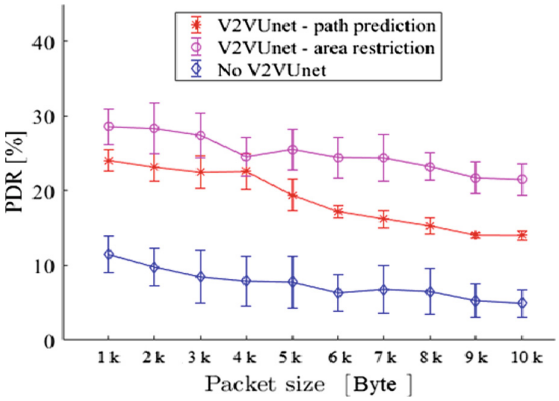


Fig. 6. Evaluation of a packet delivery ratio

compared to the area restriction mechanism. In overall E2E delay results, the traditional forwarding scheme provides lowest delay compared to other two algorithms. This is because the traditional forwarding scheme does not need an additional mechanism to perform packet forwarding.

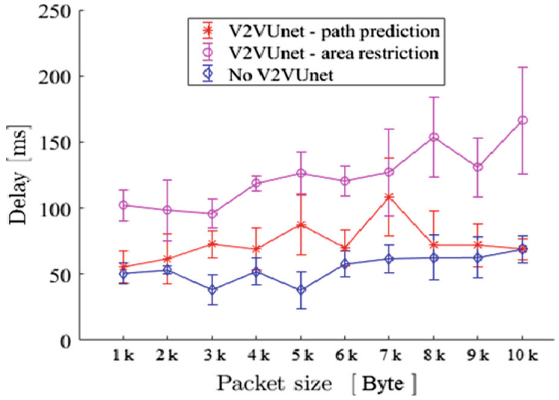


Fig. 7. Evaluation of end-to-end delays

The third set of results shows PDR of all algorithms in various number of participating vehicles in cross road scenario (cf. Fig. 8). These various number of vehicles are used to evaluate V2VUNet schemes when dealing with the network density and network speed. The V2VUNet-path prediction and V2VUNet-area restriction shows 10% and 20% better PDR, respectively, compared to a greedy forwarding without V2VUNet. As the network density grows, the PDR decreases in all forwarding schemes. From all simulation trials that have been performed, the highest PDR that can be achieved is about 40%. This is due to the path failure that occurs when the communicating vehicles are under the overpass. This path failure cannot be avoided since

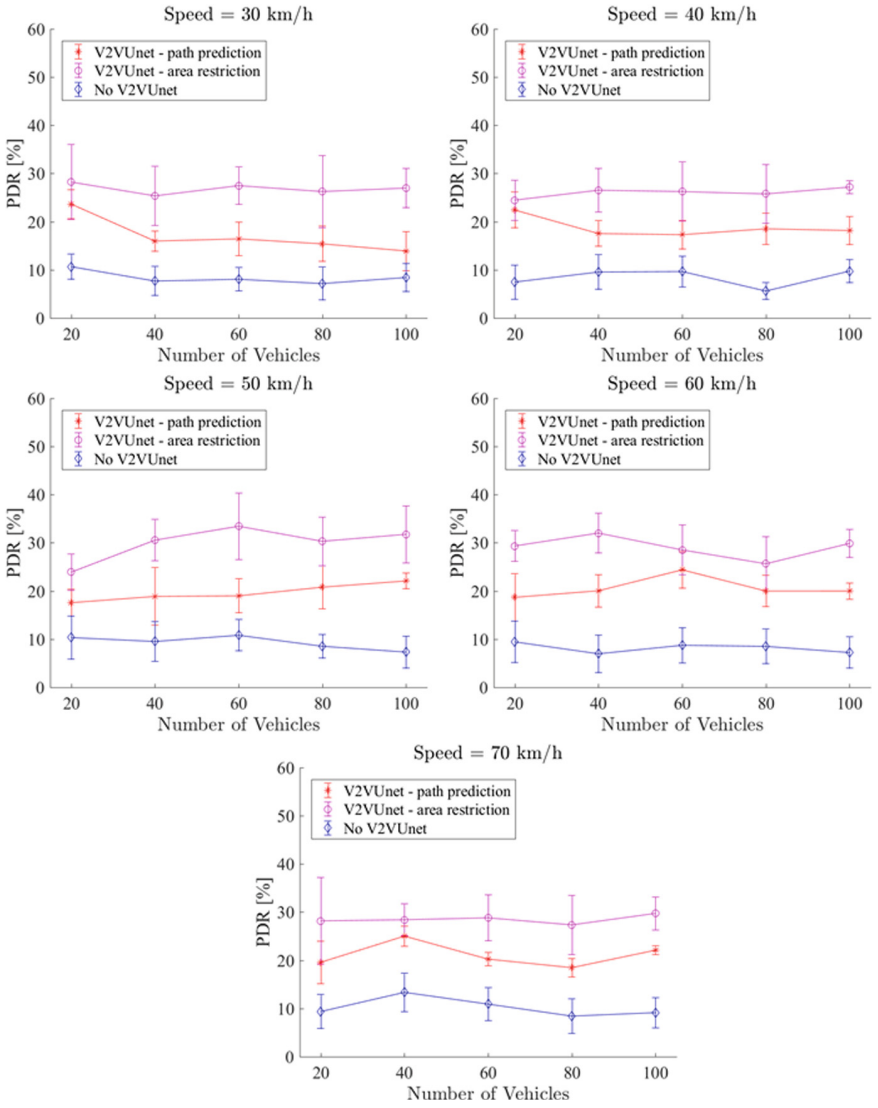


Fig. 8. Evaluation of packet delivery ratios for varying numbers of vehicles and vehicle speeds

the overpass disturbs the transmission, thus it will never reach 100% of PDR. The network density with 60–80 vehicles shows the maximum 40% result at speed 50 km/h. This indicates that 60 vehicles with 30 pairs of S and R are the 'best' condition where the packet transmission is performed.

However, in high speed mobility (*i.e.* 50 km/h–70 km/h), the PDR reaches higher results compared to PDR in low speed mobility (*i.e.*, 30 km/h and 40 km/h). The main reason for this is that in higher speed mobility, the path reconstruction is even more possible than maintaining the old path. In this case, V2VUNet area restriction scheme

provides PDR 10% higher compared to V2VUNet path prediction forwarding scheme. This is caused by the overpass construction which blocks the packet transmission, thus, it becomes difficult to complete path finding process.

The fourth set of results shows E2E delays of all algorithms when various number of participating vehicles are involved in a cross road scenario (cf. Fig. 9). This E2E delay reaches 350 ms at 70 km/h speed. The high E2E delay can be caused by two reasons: the first reason is that the intermediate node which moves in the opposite direction (*e.g.*, vehicle that changes its direction or turns back), has impact to the searching mechanism. Thus, the mechanism starts to find a new path and the transmission is delayed because of this reason. The second reason is that the connections between two vehicles are interrupted or discontinued, when one of the vehicles is located under the overpass. However, the E2E delays decrease for mobility with higher speeds *i.e.* 50 km/h–70 km/h. The similar explanation as in the PDR can also be applied to explain the E2E delays. The required period of time to find a new path is less than in the mobility with low speeds (*i.e.*, 30 km/h and 40 km/h). In overall results, the

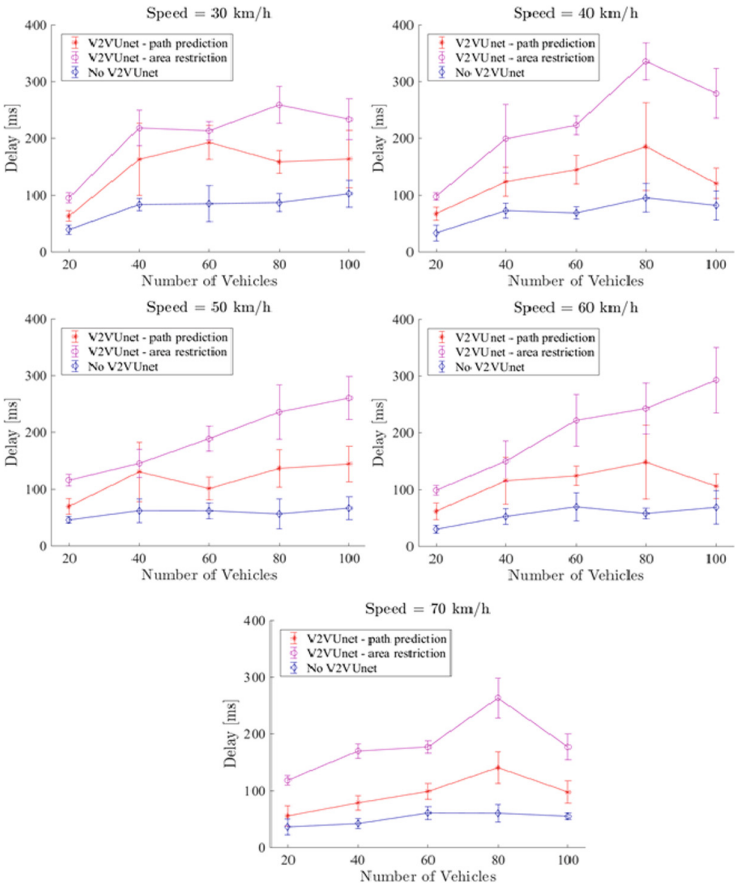


Fig. 9. Evaluation of end-to-end delays for varying numbers of vehicles and vehicle speeds

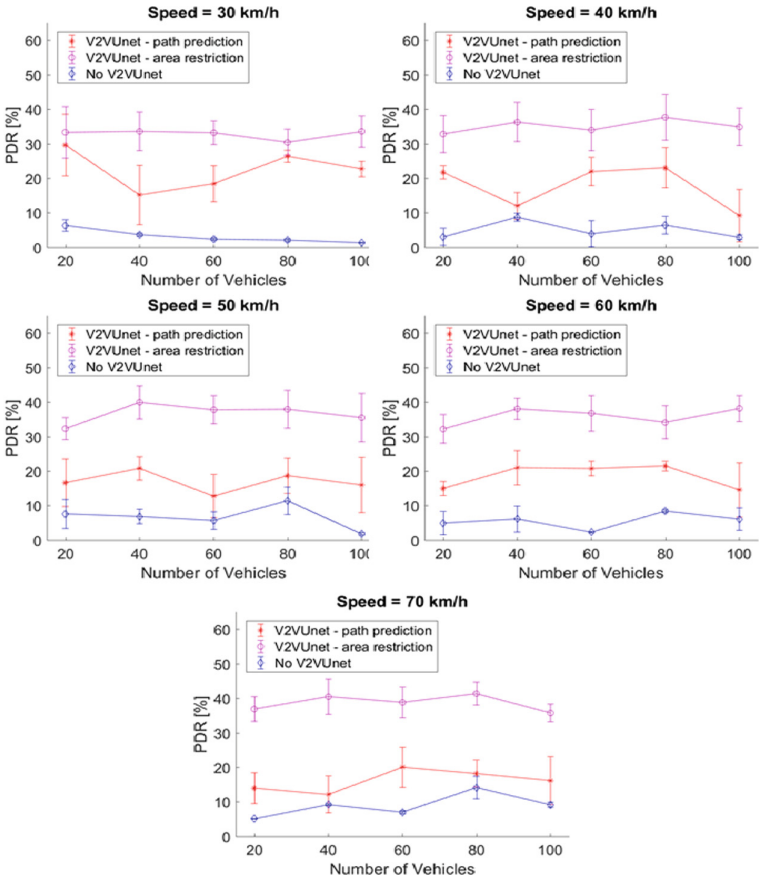


Fig. 10. Evaluation of packet delivery ratios for varying numbers of vehicles and vehicle speeds

E2E delays are considered as drawbacks in order to obtain better PDR by applying V2VUNet. Thus, this becomes an open question.

The fifth set of results in Fig. 10 shows the evaluation of PDR in the parallel road scenario. Here, the path prediction scheme reaches 40%. When compared to other schemes, PDR of the path prediction is found to be the highest because in parallel road scenarios the direction of vehicles is predictable *i.e.*, either in the same direction or opposite direction. Thus, in the parallel scenario, path prediction scheme works well in predicting the relay candidate's direction. In overall, the PDR decreases accordingly to number of participating nodes. This is because of the collision due to the network density.

The sixth set of results shows E2E delays (cf. Fig. 11) in the parallel road scenario. The traditional greedy routing shows the lowest delay compared to other scheme because the scheme does not include additional searching mechanism as previously mentioned. However, the path prediction scheme shows reasonable E2E delays of 50 ms as the prediction mechanism works well in the parallel road scenario.

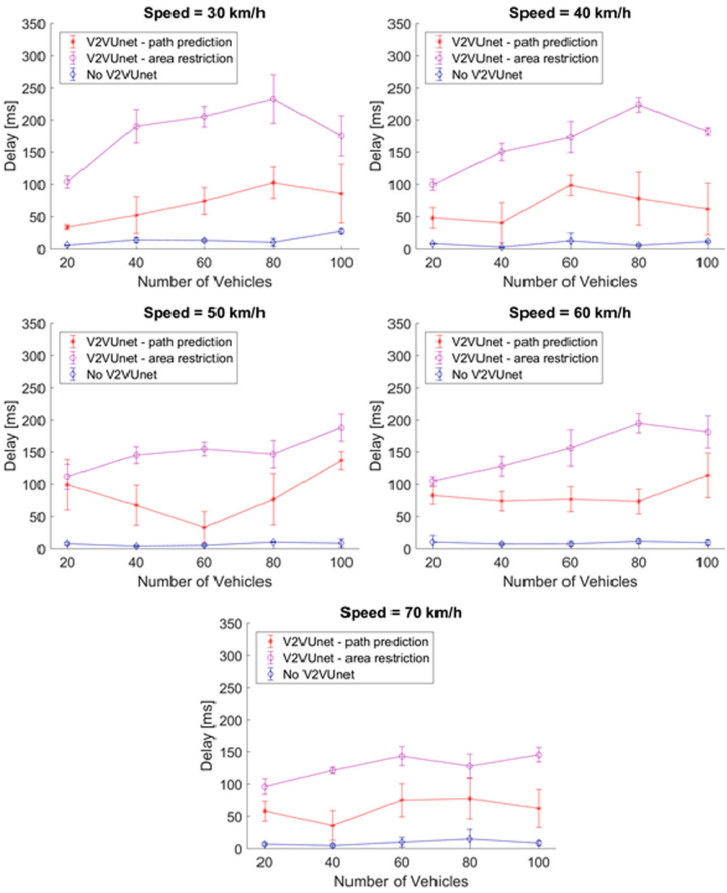


Fig. 11. Evaluation of end-to-end delays for varying numbers of vehicles and vehicle speeds

5 Summary and Future Work

This work covers and ensues the evaluation of V2VUNet through a three-dimensional road topology in a large city. Important parameters of V2VUNet have been evaluated: packet size, speed, and number of vehicles. The V2VUNet takes into account HRA and VRA as additional weight values, which are applied in area restriction and path prediction algorithms. The network performance as indicated by PDR and E2E delay values shows to be reliable in non-safety applications. The PDR in an overall performance shows that V2VUNet provides 20% better result compared to traditional routing algorithms. However, the E2E delays in the overall evaluations are slightly higher than for traditional routing algorithms. Thus, these E2E delays are considered to determine the trade-off in V2VUNet, even though a non-safety application is assumed to be a delay tolerant scheme. Additionally, the path prediction scheme is less suitable to be adopted in the cross scenario, however, it performs better in the parallel scenario. Thus,

it can be concluded that the V2VUNet path prediction works better in the parallel scenario, since the direction of vehicles is homogeneous. The V2VUNet area restriction performs better in the cross scenario, since it restricts the number of relay candidates.

Further research in improving V2VUNet, the area restriction, and path prediction concept can be performed for any position-based routing scheme, where the distance and direction indicate the influencing weight value. The combination of these two schemes will be considered as a hybrid scheme, thus, both algorithms in V2VUNet are expected to improve the packet forwarding scheme depending on the use case.

References

1. Mauve, M., Scheuermann, B.: VANET Convenience and Efficiency Applications, VANET Vehicular Applications and Inter-Networking Technology, pp. 81–105. Wiley, Hoboken (2010)
2. Aoki, M., Fujii, H.: Inter-vehicle communication: technical issues on vehicle control application. IEEE Commun. Mag. **34**(10), 90–93 (2002). New York, NY, U.S.A. doi:10.1109/35.544327
3. Papadimitratos, P., La Fortelle, A.D., Paristech, M., Evenssen, K., Asa, Q.: Vehicular communication systems: enabling technologies, applications, and future outlook on intelligent transportation. IEEE Commun. Mag. **47**(11), 84–95 (2009). New York, NY, U.S.A. doi:10.1109/MCOM.2009.5307471
4. Jerbi, M., Senouci, S.M., Meraihi, R., Ghamri-Doudane, Y.: An improved vehicular ad-hoc routing protocol for city environments. In: IEEE International Conference on Communications, New York, N.Y, U.S.A., pp. 3972–3979, June 2007. doi:10.1109/ICC.2007.654
5. Tavakoli, R., Nabi, M.: TIGeR: a traffic-aware intersection-based geographical routing protocol for urban VANETs. In: IEEE 77th Vehicular Technology Conference (VTC Spring), New York, N.Y., U.S.A., pp. 1–5, June 2013. doi:10.1109/VTCSpring.2013.6692786
6. Lin, Q., Li, C., Wang, X., Zu, L.: A three-dimensional scenario oriented routing protocol in vehicular ad-hoc networks. In: IEEE Vehicular Technology Conference (VTC), New York, N.Y., U.S.A., pp. 1–5, June 2013. doi:10.1109/VTCSpring.2013.6691848
7. Wang, H., Tan, G.Z., Yang, J.X.: An improved VANET intelligent forward decision-making routing algorithm. J. Netw. **7**(10), 1546–1553 (2012)
8. Mohimani, G.H., Ashtiani, F., Javanmard, A., Hamdi, M.: Mobility modeling, spatial traffic distribution, and probability of connectivity for sparse and dense vehicular ad-hoc networks. IEEE Trans. Vehicular Technol. **58**(4), 1998–2007 (2009). New York, N.Y., U.S.A. doi:10.1109/TVT.2008.2004266
9. Walfisch, J., Bertoni, H.: Theoretical model of UHF propagation in urban environments. IEEE Trans. Antennas Propag. **36**(12), 1788–1796 (1988). New York, N.Y., U.S.A. doi:10.1109/8.14401
10. Karp, B., Kung, H.T.: GPSR: greedy perimeter stateless routing for wireless network. In: International Conference on Mobile Computing and Networking (MobiCom), pp. 243–254. ACM, New York, August 2000. doi:10.1145/345910.345953
11. Spachos, P., Toumpakaris, D., Hatzinakos, D.: Angle-based dynamic routing scheme for source location privacy in wireless sensor network. In: IEEE Vehicular Technology Conference (VTC), New York, N.Y., U.S.A., pp. 1–5, May 2014. doi:10.1109/VTC-Spring.2014.7022833

12. Banka, R.K., Xue, G.: Angle routing protocol: location aided routing for mobile ad-hoc networks using dynamic angle selection. In: IEEE Premier International Conference for Military Communications (MILCOM), New York, N.Y., U.S.A., vol. 1, pp. 501–506, October 2001. doi:10.1109/MILCOM.2002.1180493
13. Huang, C., Chiu, Y., Wen, C.: Using hybrid angle/distance information for distributed topology control in vehicular sensor networks. Sensors **14**(11), 20188–20216 (2014). Basel, Switzerland, doi:10.3390/s141120188
14. NS3. https://www.nsnam.org/. Accessed 28 Jan 2017
15. Moser, S., Behrendt, L., Slomka, F.: MIMO-enabling PHY layer enhancement for vehicular ad-hoc networks. In: IEEE Wireless Communications and Networking Conference Workshops (WCNCW), New York, N.Y., U.S.A., pp. 142–14 (2015). doi:10.1109/WCNCW.2015.7122544
16. Kristiana, L., Schmitt, C., Stiller, B.: Survey of angle-based forwarding methods in VANET communications. In: IEEE Wireless Days (WD), Toulouse, France, pp. 1–3, March 2016. doi:10.1109/WD.2016.7461505
17. Kristiana, L., Schmitt, C., Stiller, B.: Predictive forwarding scheme in three-dimensional vehicular communication scenarios. In: International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT), Avignon, France, pp. 1–6, May 2017
18. Kristiana, L., Schmitt, C., Stiller, B.: V2VUNet - a filtering out concept for packet forwarding decision in three-dimensional inter-vehicular communication scenarios. In: IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), New York, N.Y., U.S.A., pp. 1–6, September 2016. doi:10.1109/PIM-RC.2016.7794600
19. Kolici, V., Oda, T., Spaho, E., Barolli, L., Ikeda, M., Uchida, K.: Performance evaluation of a VANET simulation system using NS-3 and SUMO. In: IEEE 29th International Conference on Advanced Information Networking and Applications Workshops (WAINA), New York, N.Y., U.S.A., pp. 348–353, March 2015. doi:10.1109/WAINA.2015.121
20. Simulation of Urban MObility, SUMO. http://www.dlr.de/ts/en/desktopdefault.aspx/tabid-9883/16931_read-41000/. Accessed 16 Mar 2017
21. Kristiana, L., Schmitt, C., Stiller, B.: Survey of angle-based forwarding methods in VANET communications. In: IEEE Wireless Days, New York, N.Y., U.S.A., pp. 1–3, March 2016. https://doi.org/10.1109/WD.2016.7461505

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

Author Index

Badonnel, Rémi 47
Barcellos, Marinho P. 62
Barshan, Maryam 79
Bartoš, Václav 125
Bocek, Thomas 16, 185
Bondan, Lucas 179
Botero, Juan F. 62
Burská, Karolína 149

Carle, Georg 30
Čejka, Tomáš 3, 125, 153
Čeleda, Pavel 173
Compastié, Maxime 47

de Boer, Pieter-Tjerk 137
de O. Schmidt, Ricardo 137
De Turck, Filip 79, 165, 179
Dorfhuber, Marko 30

Festor, Olivier 47

Gaspary, Luciano P. 62
Gil-Herrera, Juliver 62
Granville, Lisandro Zambenedetti 179

Haugerud, Hårek 143
Hausheer, David 16
He, Ruan 47
Hendriks, Luuk 137
Herold, Nadine 30

Isolani, Pedro H. 62

Jansky, Tomáš 125

Kassi-Lahlou, Mohamed 47
Kergl, Dennis 108
Knecht, Markus 159
Kristiana, Lisa 94

Lareida, Andri 16
Laštovička, Martin 173
Latré, Steven 62
Liebald, Stefan 30

Moens, Hendrik 79
Müller, Robert 131

Neves, Miguel C. 62

Ocampo, Andrés F. 62
Ošlejšek, Radek 149

Pras, Aiko 137

Rafati, Sina 16
Rodosek, Gabi Dreo 108
Rodrigues, Bruno 16, 185
Roedler, Robert 108
Rudolf, Christoph 30

Schmitt, Corinna 94, 131
Sebrechts, Merlijn 165
Stiller, Burkhard 16, 94, 159, 185
Švepeš, Marek 3

Van Seghbroeck, Gregory 165
Velan, Petr 137
Volckaert, Bruno 79, 179

Wachs, Matthias 30
Waldvogel, Marcel 131
Wauters, Tim 179

Xue, Noha 143

Yazidi, Anis 143

Žádník, Martin 153
Zambenedetti, Lisandro 62

© The Editor(s) (if applicable) and The Author(s) 2017. This book is an open access publication.
Open Access This book is licensed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this book are included in the book's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the book's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

Ads by Google

Stop seeing this ad Why this ad?

Lecture Notes in Computer Science

COUNTRY

Germany

Universities and research institutions in Germany

SUBJECT AREA AND CATEGORY

Computer Science
- Computer Science (miscellaneous)

Mathematics
- Theoretical Computer Science

PUBLISHER

Springer Verlag

H-INDEX

356

PUBLICATION TYPE

Book Series

ISSN

03029743, 16113349

COVERAGE

1937, 1955, 1973-2020

INFORMATION

Homepage

How to publish in this journal

lncs@springer.com

Ads by Google

Stop seeing this ad

Why this ad?

SCOPE

This distinguished conference proceedings series publishes the latest research developments in all areas of computer science.

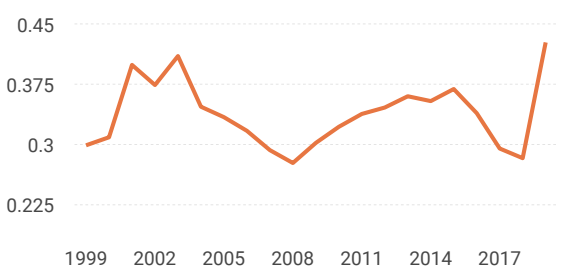
Join the conversation about this journal

Ads by Google
Stop seeing this ad | Why this ad?

Quartiles

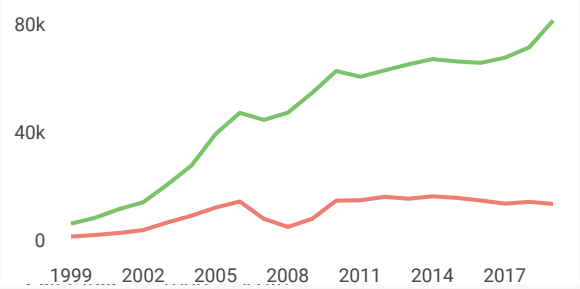
Ads by Google
Stop seeing this ad | Why this ad?

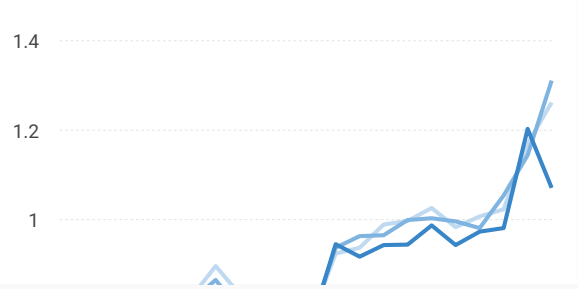
SJR

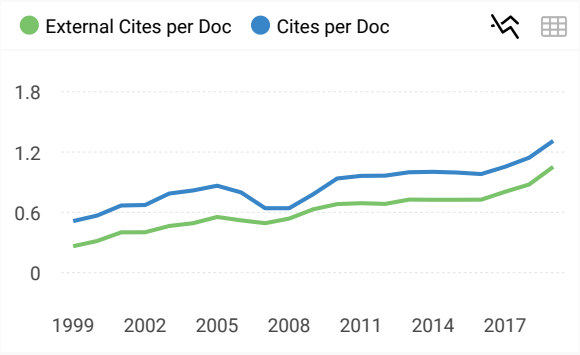


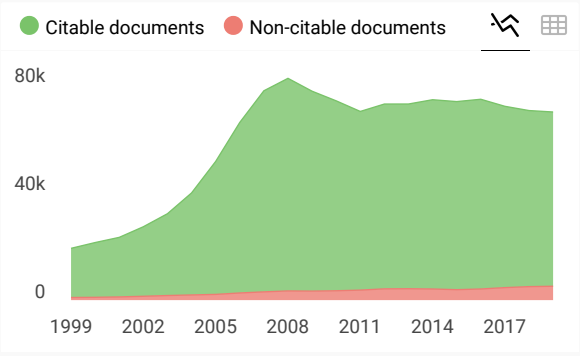
Citations per document

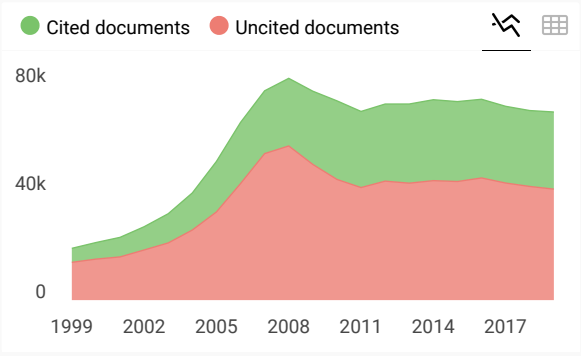
Total Cites | Self-Cites

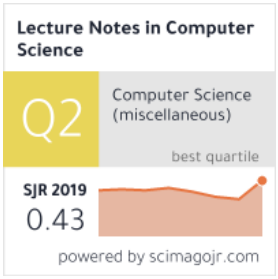












← Show this widget in your own website

Just copy the code below and paste within your html code:

<a href="https://www.scimag

Ads by Google
Stop seeing this ad
Why this ad?

Metrics based on Scopus® data as of April 2020

W **Win Lei** 3 months ago

LNCS is Q2 and how about LNAI?
According to the LNCS homepage, LNAI is a topical subseries of LNCS focusing on artificial intelligence.
I would like to know that can we call LNAI is also Q2?