MUSAB A. ALTURKI

CONTACT INFORMATION

email	musab.alturki@gmail.com
phone	+1 (215) 470-7611
Online profiles	LinkedIn: lnkd.in/CYGMTh Google Scholar: goo.gl/UaXfZB DBLP: dblp.org/pid/150/2827

RESEARCH INTERESTS

Formal methods for program verification, specification and design of distributed and concurrent programming languages and systems, and for analysis of security properties.

EDUCATION

2006-2011 University of Illinois at Urbana-Champaign

Ph.D. in Computer Science

Urbana, IL, USA · Department of Computer Science

- *Dissertation:* Rewriting-based Formal Modeling, Analysis and Implementation of Real-Time Distributed Services
- *Committee:* José Meseguer (Chair), Gul Agha, Carl A. Gunter, Grigore Rosu, Jayadev Misra (UT Austin)
- *Description:* Developed novel rewriting-based methods and tools for formally specifying distributed services, analyzing their properties and building correct-by-construction implementations.

2003-2005 University of Illinois at Urbana-Champaign

M.Sc. in Computer Science

Urbana, IL, USA · Department of Computer Science

- *Thesis:* A Rewriting Logic Approach to the Semantics of Orc
- *Advisor:* José Meseguer
- *Description:* Developed a provably correct, efficiently executable formal semantics of Orc applied to an online auction case study.

1997-2002 King Fahd University of Petroleum and Minerals

B.Sc. in Computer Science

Dhahran, Saudi Arabia · Information & Computer Science Department

First Honors · GPA: 3.98 (Cumulative) and 4.0 (Major), both on a 4.0 scale

PROFESSIONAL EXPERIENCE

2018–Present Senior Research Engineer

RV Inc.

Runtime Verification Inc. · Urbana, IL, USA

- Formal modeling and verification of safety and liveness properties in state-of-the-art decentralized consensus protocols
- Statistical model checking of resilience of blockchain protocols against selective reveal attacks

2011–2019 Assistant Professor

KFUPM

King Fahd University of Petroleum and Minerals · Dhahran, Saudi Arabia

- Teaching introductory and advanced courses in computer science

- Conducting research in formal methods, programming languages and security
- Service through the development of courses and research programs, and contribution to the professional society

2017–2018 Visiting Research Scholar

UPenn

UNIVERSITY OF PENNSYLVANIA · Philadelphia, PA, USA

- Investigating formal methods for the design and analysis of secure cyber-physical systems and protocols
- Host: Andre SCEDROV, Chair of the Mathematics Department, Professor of Mathematics, Professor of Computer and Information Science

2013–2017 Assistant Dean of Research

KFUPM

KING FAHD UNIVERSITY OF PETROLEUM AND MINERALS · Dhahran, Saudi Arabia

- Strategic planning of research programs and activities
- Development and monitoring of research policies and regulations
- Administration of research grant applications, evaluations and operations
- Supervision of research support system development, including “Abhathi”, an enterprise research management system
- Management of four different units having a total of 20 employees

Summer 2008 Research Engineer Intern

DoCoMo Labs

DOCOMO USA LABS · Palo Alto, CA, USA

- Developed a framework based on Real-Time Maude for formal software specification and analysis including verification of non-functional timing properties of mobile software systems

2007–2011 Research Assistant

UIUC

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN · Urbana, IL, USA

- Developed formal methods and tools for the specification, analysis and implementation of real-time, distributed services
- Developed methods and tools for statistical analysis and model-checking of probabilistic systems, including analysis of resilience against DDoS and amplification attacks

2006–2007 Graduate Research Assistant

NCSA

NATIONAL CENTER FOR SUPERCOMPUTING APPLICATIONS · Urbana, IL, USA

- Investigated specifying role-based and attribute-based access control mechanisms using XML-based policy languages (such as XACML), and formally verifying their security properties using Margrave
- Extended the encryption techniques in the open-source Bouncycastle cryptography API in Java for secure e-mail and web services with a novel, two-staged identity-based encryption scheme

2002–2003 Database Developer and Administrator

KFUPM

KING FAHD UNIVERSITY OF PETROLEUM AND MINERALS · Dhahran, Saudi Arabia

- Developed and maintained a complete enterprise Microsoft SQL Server system for part-time job management, along with a dynamic, ASP-based web application front-end

2002–2003 Graduate Assistant

KFUPM

KING FAHD UNIVERSITY OF PETROLEUM AND MINERALS · Dhahran, Saudi Arabia

- Researched new network designs for VoIP applications and extensively analyzed them through deep OPNET simulations
- Taught introductory computer science labs in Java

Summer 2001 System Analyst Intern

Aramco SAUDI ARAMCO · Dhahran, Saudi Arabia

- Managed various Sun Solaris 2.6/2.8 machines, configured production Sun SSP's and Clusters, and developed automation scripts in Perl

REFEREED PUBLICATIONS

Statistical Model Checking of RANDAO's Resilience to Pre-computed Reveal Strategies

October 2019 Proceedings of the 1st Workshop on Formal Methods for Blockchains, October 11, 2019, Porto, Portugal
Musab A. ALTURKI and Grigore ROSU

Towards a Verified Model of the Algorand Consensus Protocol in Coq

October 2019 Proceedings of the 1st Workshop on Formal Methods for Blockchains, October 11, 2019, Porto, Portugal
Musab A. ALTURKI, Jing CHEN, Victor LUCHANGCO, Brandon MOORE, Karl PALMSKOG, Lucas PENA and Grigore ROSU

Resource-Bounded Intruders in Denial of Service Attacks

June 2019 Proceedings of the 32nd IEEE Computer Security Foundations Symposium, June 25–28, 2019, Hoboken, NJ, USA
Abraão. URQUIZA, Musab A. ALTURKI, Max KANOVICH, Tajana BAN KIRIGIN, Vivek NIGAM, Andre SCEDROV and Carolyn TALCOTT

A Multiset Rewriting Model for Specifying and Verifying Timing Aspects of Security Protocols

March 2019 Foundations of Security, Protocols, and Equational Reasoning - Essays Dedicated to Catherine A. Meadows, Lecture Notes in Computer Science, volume 11565, pp 192–213, Springer
Musab A. ALTURKI, Tajana BAN KIRIGIN, Max KANOVICH, Vivek NIGAM, Andre SCEDROV and Carolyn TALCOTT

Statistical Model Checking of Distance Fraud Attacks on the Hancke-Kuhn Family of Protocols

Oct. 2018 Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy (CPS-SPC@CCS'18), Toronto, ON, Canada, pp 60–71, ACM
Musab A. ALTURKI, Max KANOVICH, Tajana BAN KIRIGIN, Vivek NIGAM, Andre SCEDROV and Carolyn TALCOTT

Program Comprehension through Reverse-engineered Sequence Diagrams: A Systematic Review

June 2018 Journal of Software: Evolution and Process, Volume 30, Issue 11, e1965, Wiley
Taher A. GHALEB, Musab A. ALTURKI, Khalid ALJASSER

A Symbolic Rewriting Semantics of the COMPASS Modeling Language

Aug. 2017 IEEE 18th International Conference on Information Reuse and Integration, San Diego, CA, USA
Musab A. ALTURKI

Implementing the Observer Design Pattern as an Expressive Language Construct

Nov. 2015 The International Conference on Software Engineering Advances, Barcelona, Spain
Taher A. GHALEB, Khalid ALJASSER, Musab A. ALTURKI

Towards Formal Verification of Orchestration Computations Using the $\mathcal{K}$ Framework

June 2015 Proceedings of the 20th International Symposium on Formal Methods (FM'15), Oslo, Norway, Lecture Notes in Computer Science, Volume 9109, pp 40–56, Springer
Musab A. Alturki, Omar Alzuhaibi

Executable Rewriting Logic Semantics of Orc and Formal Analysis of Orc Programs

March 2015 Journal of Logic and Algebraic Methods in Programming: Special Issue on Automated Specification and Verification of Web Systems, Volume 84, Issue 4, pp 505–533, Elsevier
Musab A. Alturki, José Meseguer

Sparse Single-hidden Layer Feedforward Network for Mapping Natural Language Questions to SQL Queries

Sep. 2014 Proceedings of the 24th International Conference on Artificial Neural Networks (ICANN'14), Hamburg, Germany, Lecture Notes in Computer Science, Volume 8681, pp 241–248, Springer
Issam H. Laradji, Lahouari Ghouti, Faisal Saleh, Musab A. Alturki

Stable Availability under Denial of Service Attacks through Formal Patterns

April 2012 Proceedings of Fundamental Approaches to Software Engineering (FASE'12), Tallinn, Estonia, Lecture Notes in Computer Science, Volume 7212, pp 78–93, Springer
Jonas Eckhardt, Tobias Mühlbauer, Musab A. Alturki, José Meseguer, Martin Wirsing

PVeStA*: A Parallel Statistical Model Checking and Quantitative Analysis Tool*

Aug. 2011 Proceedings of Algebra and Coalgebra in Computer Science (CALCO'11), Winchester, UK, Lecture Notes in Computer Science, Volume 6859, pp 386–392, Springer
Musab A. Alturki, José Meseguer

Dist-Orc*: A Rewriting-based Distributed Implementation of Orc with Formal Analysis*

April 2010 Proceedings of the International Workshop on Rewriting Techniques for Real-Time Systems (RTRTS'10), Longyearbyen, Norway, Electronic Proceedings of Theoretical Computer Science, Volume 36
Musab A. Alturki, José Meseguer

Model-Checking DoS Amplification for VoIP Session Initiation

Sep. 2009 Proceedings of the European Symposium on Research in Computer Security (ESORICS'09), Saint Malo, France, Lecture Notes in Computer Science, Volume 5789, pp 390–405, Springer
Ravinder Shankesi, Musab A. Alturki, Ralf Sasse, Carl A. Gunter, José Meseguer

Probabilistic Modeling and Analysis of DoS Protection for the ASV Protocol

Sep. 2009 Proceedings of the International Workshop on Security and Rewriting Techniques (SecReT'08), Pittsburgh, PA, USA, Electronic Notes in Theoretical Comp. Sci., Volume 234, pp 3–18, Elsevier
Musab A. Alturki, José Meseguer, Carl A. Gunter

Formal Specification and Analysis of Timing Properties in Software Systems

March 2009 Proceedings of Fundamental Approaches to Software Engineering (FASE'09), York, UK, Lecture Notes in Computer Science, Volume 5503, pp 262–277, Springer

Musab A. ALTURKI, Dinakar DHURJATI, Dachuan YU, Ajay CHANDER, Hiroshi INAMURA

PBES*: A Policy Based Encryption System with Application to Data Sharing in the Power Grid*

March 2009 Proceedings of ACM Symposium on Information, Computer and Communications Security (ASIACCS'09), pp 262–275, Sydney, Australia, 2009, ACM
Rakesh BOBBA, Himanshu KHURANA, Musab A. ALTURKI, Farhana ASHRAF

Reduction Semantics and Formal Analysis of Orc Programs

May 2008 Proceedings of the International Workshop on Automated Specification and Verification of Web Systems (WWV'07), Venice, Italy, Electronic Notes in Theoretical Comp. Sci., Volume 200-3, pp 25–41, Elsevier
Musab A. ALTURKI, José MESEGUER

Real-time Rewriting Semantics of Orc

July 2007 Proceedings of the 9th International ACM SIGPLAN Conference on Principles and Practice of Declarative Programming (PPDP'07), pp 131–142, Wroclaw, Poland, 2007, ACM
Musab A. ALTURKI, José MESEGUER

ISSUED PATENTS

METHODS, COMPUTER READABLE MEDIA, AND SYSTEMS FOR COMPILING CONCISE EXPRESSIVE DESIGN PATTERN SOURCE CODE

September 2019 Patent US010437572, USPO 2019
Taher A. GHALEB, Khalid ALJASSER, Musab A. ALTURKI

PENDING PAPERS

Improving Test Coverage through an Executable Formal Model of the Beacon Chain

2019 Musab A. ALTURKI, Denis BOGDANAS, Chris HATHHORN, Daejun PARK and Grigore ROSU

INVITED TALKS

Statistical Model Checking and Quantitative Analysis of Security Protocols

Dec. 2017 Protocol eXchange Meeting, National Cryptologic Museum,
Annapolis Junction, MD, USA

An Introduction to Rewriting Logic and the Maude Tool

June 2016 PL Club Seminar Series, University of Pennsylvania,
Philadelphia, PA, USA

Research Ethics

April 2015 University of Dammam,
Dammam, Saudi Arabia

Rewriting-based Formal Modeling and Analysis of Timed Distributed Services

Oct. 2011 CS Seminar Series, Carnegie Mellon University – Qatar,
Doha, Qatar

Rewriting Semantics and Formal Analysis of Orc Programs

Jan. 2010 Formal Methods Seminar, University of Texas,
Austin, TX, USA

CONFERENCE TALKS

Statistical Model Checking of RANDAO's Resilience to Pre-computed Reveal Strategies

Oct. 2019 The 1st Workshop on Formal Methods for Blockchains (FMBC'19)
Porto, Portugal

Towards a Verified Model of the Algorand Consensus Protocol in Coq

Oct. 2019 The 1st Workshop on Formal Methods for Blockchains (FMBC'19)
Porto, Portugal

Resource-Bounded Intruders in Denial of Service Attacks

June 2019 The 32nd IEEE Computer Security Foundations Symposium (CSF'19)
Hoboken, NJ, USA

A Multiset Rewriting Model for Specifying and Verifying Timing Aspects of Security Protocols

March 2019 Catherine Meadows Festschrift Symposium
Fredericksburg, VA, USA

Statistical Model Checking of Distance Fraud Attacks on the Hancke-Kuhn Family of Protocols

Oct. 2018 The 2018 Workshop on Cyber-Physical Systems Security and PrivaCy (CPS-SPC @ CCS'18)
Toronto, ON, Canada

Statistical Model Checking of Guessing and Timing Attacks on Distance-bounding Protocols

July 2018 The 15th Workshop on Foundations of Computer Security (FCS'18)
Oxford, UK

A Symbolic Rewriting Semantics of the COMPASS Modeling Language

Aug. 2017 IEEE 18th International Conference on Information Reuse and Integration (IRI'17)
San Diego, CA, USA

Towards Formal Verification of Orchestration Computations Using the $\mathbb{K}$ Framework

June 2015 The 20th International Symposium on Formal Methods (FM'15)
Oslo, Norway

PVeStA*: A Parallel Statistical Model Checking and Quantitative Analysis Tool*

Aug. 2011 Algebra and Coalgebra in Computer Science (CALCO'11)
Winchester, UK

Probabilistic Modeling and Analysis of DoS Protection for the ASV Protocol

Sep. 2009 The International Workshop on Security and Rewriting Techniques (SecReT'08)
Pittsburgh, PA, USA

Formal Specification and Analysis of Timing Properties in Software Systems

March 2009 Fundamental Approaches to Software Engineering (FASE'09)
York, UK

TEACHING

Lecturer — Theory and Design of Programming Languages · Graduate
Fall 2014, Fall 2015, Fall 2016 · KFUPM, Saudi Arabia

Lecturer — Principles of Programming Languages · (Under)graduate
Fall 2012, Fall 2013 · KFUPM, Saudi Arabia

Lecturer — Theory of Computation · Undergraduate
Spring 2012 · KFUPM, Saudi Arabia

Lecturer — Formal Methods and Models in Software Engineering · Undergraduate
Fall 2011 · KFUPM, Saudi Arabia

Lecturer — Introduction to Computing I & II · Undergraduate
2011 – 2013 · KFUPM, Saudi Arabia

Teaching Assistant — Introduction to Computing I & II – Lab · Undergraduate
Fall 2002, Spring 2003 · KFUPM, Saudi Arabia

RESEARCH GRANTS (ACADEMIA)

2014-2017 — $50,000 · Internal Funding Grant (KFUPM)

- "Symbolic Model Checking of CML Specifications" (Principal investigator)

2013-2014 — $20,000 · Junior Faculty Grant (KFUPM)

- "Formal Specification and Verification of Service Compositions in Orc Based on Rewriting Logic" (Principal investigator)

Summer 2013 — $10,000 · British Council Post-doctoral Summer Program (through KFUPM)

- "Rewriting Semantics of the COMPASS Modeling Language" (Principal investigator)

DISSERTATION

Title — "Rewriting-based Formal Modeling, Analysis and Implementation of Real-Time Distributed Services"

Summary — My dissertation develops formal specification, simulation, prototyping, and analysis techniques and tools for distributed software services, based on rewriting logic, the Maude system, and the theory of Orc, with the overall goal of improving the reliability of *Internet software*, a class of distributed systems based on Internet-accessible software components. The dissertation focuses on two fundamentally important aspects of Internet software systems: (1) functional correctness of service compositions through reachability and model checking analysis (the web-based tool MOrc) , and (2) availability of services (Quality-of-Service properties) through probabilistic modeling and statistical model checking and quantitative analysis (the client-server tool PVeStA). The notion of *stable availability* in cloud-based services, which guarantees a level of service regardless of how heavy a DDoS attack is, is introduced and defined through formal patterns.

SOFTWARE AND PUBLIC REPOSITORIES

Algorand — Developed 2019 · A formalization of the Algorand consensus protocol using the Coq proof assistant
https://github.com/runtimeverification/algorand-verification

RANDAO — Developed 2018 · A probabilistic rewriting model of Randao-based random number generation schemes with statistical model checking https://github.com/runtimeverification/rdao-smc

MOrc — Developed 2009-2011 · An online, web-based system for specifying and verifying service compositions, consisting of an interactive JQuery-based front-end and a PHP back-end powered by Maude
http://www.ccse.kfupm.edu.sa/~musab/morc

PVeSta — Developed 2010-2011 · An efficient parallel statistical model checking and quantitative analysis tool written in Java
http://maude.cs.uiuc.edu/tools/pvesta

IB-MKD — Developed 2007-2008 · An open-source implementation of a novel policy-based encryption system as a modified Java Bouncycastle Library and its S/MIME and CMS Processors

CAAC — Developed 2001-2002 · A web-based, database-driven enterprise application for managing student part-time-job applications and processes

HONORS AND AWARDS

2014	*Distinguished Service Award* · College of Computer Science and Eng., KFUPM
2008	*Scholarship Award* · King Abdullah Scholar Award for Excellence in Research
2003	*Scholarship Award* · Higher Education Scholarship Award for Graduate Studies
2002	*First Honors* · First Honors Award in Computer Science
1997	*First Place* · Prince Muhammad bin Fahd's Award for Scientific Excellence

SELECTED PROFESSIONAL ACTIVITIES

Graduate Student Supervision

Turki Alhazmi · A formal system for computable financial contracts (Spring 2018)

Shadi Alhaj · A rewriting logic formalization of regular string transformations and formal analysis of transformation expressions (Spring 2017)

Omar Alzuhaibi · A Formal Semantics of Orc using the $\mathcal{K}$ Framework and Formal Verification of Orc Programs (Fall 2016)

Taher Ghaleb · Improved Reverse Engineering Technique for Program Comprehension with Effective Sequence Diagrams (Spring 2016)

PC and Review Board Membership

FTSCS 2012–2015 · International Workshop on Formal Techniques for Safety-Critical Systems

SIMULTECH 2013, 2012 · International Conference on Simulation and Modeling Methodologies, Technologies and Applications

SCP 2017, 2019 · Science of Computer Programming Journal

JLAMP 2017 · Journal of Logical and Algebraic Methods in Programming

FAC 2011 · Formal Aspects of Computing Journal

JCS 2010 · Journal of Computer Security

AMAST 2008 · International Conference on Algebraic Methodology and Software Technology

Professional Affiliation

ACM 2014–present · Professional Member

SKILLS

Programming	C/C++, Java, OCaml, Haskell, Perl, Bash, LaTeX
Web	Javascript, JQuery, PHP, HTML5, CSS
Verification	Maude, $\mathcal{K}$, Coq, Isabel/HOL, Java Modeling Language (JML), NuSMV, CVC4, Z3
Languages	Fluent in both Arabic (native language) and in English

October 22, 2019