Curriculum vitae

Name: David Miguel Sanan Baena

Date: July 2017

Surname: Sanan Baena Name: David Miguel
Birthday: 22-06-1977

Current Position
Position: Senior Research Fellow.
Entity/ Organism: Nanyang Technological University (Since February 2015)
Faculty, School or Institute: School of Computing Science and Engineering.

Telephone: +6597946419
Fax:
email: sanan@ntu.edu.sg

Academic Training

Degree	University	Grade	Year
Degree in Computer Engineering	University of Malaga	B	2003
Research Master in Computer Engineering	University of Malaga	A	2006
PhD in Computer Engineering	University of Malaga	A with Honors	2009

University teaching

Course	Hours	Degree	Year
Abstract Data Types	30	Computer Science	2008/2009
Abstract Data Types	30	Computer Science	2008/2009
Declarative Programming	60	Computer Science	2007/2008

Lines of Research: Embedded systems verification. Specification and verification of partitioning and separating microkernels. Hardware Verification. Analysis and verification of software using the model checking technique for programs that uses external APIs. Verification of properties over dynamic structures with multi-level temporal logics. Sensor Networks Verification.

Postdoctal Experience

- Postdoc at University of Malaga. From Dec 2009 to May 2011. Extension of LTL with mu-calculus for the spatial and temporal verification of programs using complex data structures.
- Postdoc at Singapore University of Technology and Design. From Jun 2011 to Jun 2012. Application of model checking techniques to the verification of sensor networks software.
- Postdoc at Trinity College Dublin. From July 2012 to December 2013. Modelling and verification of a separation microkernel by means of theorem proving.
- Postdoc at National University of Singapore. From January 2014 to January 2015. Machine code verification by means of theorem proving.
- Postdoc at Nanyang Technological University. From February 2015. Separation Micro-kernel and Hardware verification by means of theorem proving.

Non-Achademic Experience

- AtLinks/Thomson/Novasoft. From October 2002 to November 2004.
  Development of embedded software for landline phone terminals.
  Development of backend software for managing public phone terminals.

Scientist-Technique Publications

Refereed Journals

1. Yongwang Zhao, David Sanan, Fuyuan Zhang and Yang Liu. Refinement-based Specification and Security Analysis of Separation Kernels. IEEE Transactions on Dependable and Secure Computing. doi:10.1109/TDSC.2017.2672983
2. Zhe Hou, David Sanan, Alwen Tiu, Rajeev Gore, Ranald Clouston. Separata: Isabelle Tactics for Separation Algebra. Archive of Formal Proofs, November 2016. ISSN: 2150-914x
3. Zhe Hou, David Sanan, Alwen Tiu, Liu Yang. A Formal model for the SPARCv8 ISA and Proof of Non-Interference for the Leon3 Processor. Archive of Formal Proofs, October 2016. ISSN: 2150-914x
4. Yongwang Zhao, David Sanan, Fuyuan Zhang, Yang Liu. Formal Specification and Analysis of Partitioning Operating Systems by Integrating Ontology and Refinement. IEEE Transactions on Industrial Informatics 12(4):1321-1331. (2016)
5. Maria del Mar Gallardo, David Sanan. Verification of Complex Dynamic Data Tree with Mu-Calculus. Automated Software Engineering 20(4):569-612 (2013)
6. Maria del Mar Gallardo, Christophe Joubert, Pedro Merino, David Sanan. A model-extraction approach to verifying concurrent C programs with CADP. Science of Computer Programming 77(3): 375-392 (2012)
7. Maria del Mar Gallardo, Pedro Merino, David Sanan. Model Checking Dynamic Memory Allocation in Operating Systems. Journal of Automated Reasoning 42: 229 – 264 (2009)
8. Pedro de la Camara, Maria del Mar Gallardo, Pedro Merino, David Sanan. Checking the Reliability of Socket Based Communication Software.International Journal on Software Tools for Technology Transfer 11:359 – 374 (2009)
9. Maria del Mar Gallardo, Christophe Joubert, Pedro Merino, David Sanan. Web Services for Accessing Explicit State Space Verification Tools. Ercim News 73:40-40 (2008)
10. Sergio Contreras, Maria del Mar Gallardo, Pedro Merino, David Sanan, Javier Rivas, Joaquin Torrecilla. Validating complex telecommunication software. Ercim News 66:62-63 (2006)
11. Pedro de la Camara, Maria del Mar Gallardo, Pedro Merino, David Sanan. Model Checking Software with Well-Defined APIS: The Socket Case. EASST Newsletters 11:31-34 (2005)

Refereed Conferences

1. Shang-Wei Lin, Jun Sun, Hao Xiao, Liu Yang, David Sanan, Henri Hansen. FiB: Squeezing Loop Invariants by Interpolation between Forward and Backward Reachability. TBA. The 32nd IEEE/ACM International Conference on Automated Software Engineering. October 30 – November 3, 2017. Urbana-Champaign, Illinois, USA.
2. Hou Zhe, David Sanan, Alwen Tiu, Liu Yang. Proof Tactics for Assertions in Separation Logic. 8th International Conference on Interactive Theorem Proving (ITP). 26-29 September 2017. Brasilia, Brazil.
3. David Sanan, Yongwang Zhao, Zhe Hou, Fuyuan Zhan, Alwen Tiu, Liu Yang. CSimpl: a Framework for the Verification of Concurrent Programs using Rely-Guarantee. 23rd International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS). 24-29 April 2017. Uppssala Sweden.
4. Wilayat Khan, David Sanan, Alwen Tiu. VeriFormal an Executable Formal Model of a Hardware Description Language. 2nd Singapore Cyber Security R&D Conference. 19 -20 February 2017.
5. Zhe Hou, David Sanan, Alwen Tiu, Liu Yang, Koh Chuen Hoa. An Executable Formalization of the SPARCv8 Instruction Set Architecture: A Case Study for the Leon3 Processor. 21st Internation Symposium on Formal Methods. LNICS 9995:388 – 405. November 9-11, 2016. Limassol Cyprus.
6. Yongwang Zhao, David Sanan, Fuyuan Zhang, Yang Liu. Reasoning About Information Flow Security of Separation Kernels with Channel-Based Communication. 22nd International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS). 14-21 October 2016 Eindhoven, The Netherlands.
7. David Sanan, Yang Liu, Yongwang Zhao, Zhenchang Xing, Mike Hinchey. Verifying FreeRTOS' Cyclic Doubly LInked List Implementation: From Abstract Specification to Machine Code. 20th International Conference on Engineering of Complex Computer Systems. ICECCS 2015. 9-12 December 2015. Gold Coast, Australia.
8. Yongwang Zhao, Zhibin Yang, David Sanan, Yang Liu. Based Formalization of Safety-Critical Operating Systems Standards - An Experience Report on ARINC 653 using Event-B. 26th IEEE International Symposium on Software Reliability Engineering. ISSRE 2015. 2-5 November 2015. Gaithersburg, MD, USA.
9. David Sanan, Andrew Butterfield, Mike Hinchey. Separation Kernel Verification: the XtratuM Case Study. 6th Working Conference on Verified Software: Theories, Tools, and Experiments. VSTTE 2014. 17 – 18 July 2104. Vienna Austria.
10. Andrew Butterfield, David Sanan, Mike Hinchey. Formalisation of a Separation Micro-Kernel for Common Criteria Certification. 18th International Conference on Data Systems In Aerospace (DASIA 2013). 3-5 June 2014. Warsaw, Poland.
11. Andrew Butterfield, David Sanan, Mike Hinchey. Towards Formal Verification of a Separation Microkernel. 17th International Conference on Data Systems In Aerospace (DASIA 2013). 14-16 May 2013. Porto, Portugal.
12. Manchun Zheng, Jun Sun, David Sanan, Yang Liu, Jin Song Don, Yu Gu. State Space Reduction for Sensor Networks using Two-level Partial Order Reduction.

14th International Conference on Verification, Model Checking, and Abstract Interpretation. January 20-22 2013. Rome, Italy.
13. Manchun Zheng, Jun Sun, David Sanan, Yang Liu, Jin Song Don, Yu Gu. Towards Bug-free Implementations for Wireless Sensor Networks. 9th ACM Conference on Embedded Networked Sensor Systems. 01-04 November 2011. Seattle USA.
14. Maria del Mar Gallardo, David Sanan. Verification of Dynamic Data Tree with mu-calculus Extended with Separation 8th IEEE International Conference on Software Engineering and Formal Methods (SEFM 2010). 13-18 September 2010. Pisa, Italy.
15. Maria del Mar Gallardo, Pedro Merino, David Sanan. Model Checking Dynamic Data Structures in Operating Systems. XVII Conference on Concurrent and Distributed Systems. 10-12 June 2009. Sagunto, Valencia.
16. Maria del Mar Gallardo, Pedro Merino, David Sanan. Model Checking C Programs with Dinamyc Memory Allocation. VIII Conference on Programming and Languages. 7 – 10 October 2008. Gijon, Spain.
17. Maria del Mar Gallardo, Pedro Merino, David Sanan. Model Checking C Programs with Dinamyc Memory Allocation. 32nd IEEE International Computer Software and Applications Conference. 28 July – 01 Aug. 2008. Turku Finland.
18. Maria del Mar Gallardo, Pedro Merino, David Sanan. Automatic verification of C programs with dynamic memory allocation. XVI Conference on Concurrent and Distributed Systems. JCSD 2008. 11 – 13 June 2008. Albacete, Spain.
19. Maria del Mar Gallardo, Christophe. Joubert, Pedro Merino, David Sanan. On the Fly model checking for C programs with extended CADP in FMICS-jETI. 12th IEEE International Conference on Engineering Complex Computer Systems. 10 -14 July 2007. Auckland New Zeland.
20. Maria del Mar Gallardo, Christophe Joubert, Pedro Merino, David Sanan. C.OPEN and ANNOTATOR: tools for On-the-Fly model checking C programs. 14th international SPIN workshop Lecture Notes in Computer Science. 4595. Pags. 268-273. 1-3 July 2007. Berlin Germany.
21. Maria del Mar Gallardo, Pedro Merino, David Sanan. C.OPEN, a tool for analyzing C code in CADP. XV Conference on Concurrent and Distributed Systems. 6-8 June 2007. Malaga, Spain.
22. Maria del Mar Gallardo, Pedro Merino, David Sanan. Extending CADP for analyzing C code. 5th International Workshop on Modelling, Simulation, Verification and Validation of Enterprise Information Systems (MSVVEIS 2007). 12 – 16 June 2007. Funchar, Portugal.
23. Maria del Mar Gallardo, Christophe Joubert, Pedro Merino, David Sanan. On-the-fly API influence analysis of software. 2nd International Conference on Science and Technology. 21 – 23 March 2007. Malaga, Spain – Tanger Marruecos.
24. Maria del Mar Gallardo, Pedro Merino, David Sanan. Towards Model Checking C Code with OPEN/CÆSAR. 5th International Workshop on Modellling, Simulation, Verification and Validation of Enterprise Information Systems. 23 - 27 May 2006. Paphos, Cyprus.
25. Pedro de la Camara, Maria del Mar Gallardo, Pedro. Merino, David. Sanan. SocketMC: A tool to verify C code. 13th Conference on Concurrent and

Distributed Systems. 13 – 16 September 2005. Granada, Spain.
26. Pedro de la Camara, Maria del Mar Gallardo, Pedro Merino, David Sanan. Model Checking Software with well-defined APIs: The Socket case. 10th International Workshop on Formal Methods for Industrial Critical Systems. 5 – 6 September 2005. Lisbon, Portugal.

Researching experience

R&D Proyects Participation

Securify: A Compositional Approach of Building Security Verified Systems. At Nanyang Technological University. From 06/02/2015 to date. Main researcher: Pr. Srikanthan Thambipillai.

Research and Development in the Formal Verification of System Design and Implementation. 9011102033. At National University of Singapore. From 21/01/2014 to 05/02/2015. Main researcher Pr. Jin Song Dong.

Method and Tools for On-Board Software Engineering. ESTEC CONTRACT No. 4000106016. At Trinity College Dublin. From 01/07/2012 to 31/12/2013. Main researcher: Pr. Andrew Butterfield.

Enhancing Reliability for Cyber-Physical Systems. At Singapore University of Technology and Design. From 01/06/2011 to 30/06/2012. Main researcher: Pr. Sun Jun.

Techniques to Improve Internet Services Quality on Mobile Telephony. At University of Malaga. From 2008 to 2011. Main researcher: Pr. Pedro Merino.

Reliable Software Composition in Ubiquitous Environments. TIN2008-05932. At University of Malaga. From 2009 to 2011. Main researcher: Pr. Ernesto Pimentel.

CAReSS. Construction and adaptation of reliable services in Software. TIN2007-67134. At University of Malaga. From 2007 to 2008. Main researcher: Pr. Ernesto Pimentel.

DSDM: Model Driven Software Development. TIN2005-25886-E. At University of Malaga. From 2006 to 2008. Main researcher: Pr. Antonio Vallecillo.

SELF: Agile Formalisms in Software Engineering. CICYT TIN 2004-7943-C04-01
At University of Malaga. From 2005 to 2007. Main researcher: Pr. Ernesto Pimentel.

Stream: Formal Software tools. A multi-paradigm Approach. CICYT TIC2001-2705-C03-02. At University of Malaga. From 2001 to 2004. Main researcher: Pr. Ernesto Pimentel.

Research Grants

Research staff training Pre-doctoral grant from the Ministry of science and innovation Reference: BES-2005-10282 From 01/08/2005 to 31/07/2009

Research staff training Pre-doctoral grant from the Ministry of science and innovation. Reference: TIN2004-07943-C04-01. From 01/12/2004 to 31/07/2005

Grant within the contract between University of Malaga and Malaga Transport Consortium. Reference: nº 8.006/3140. From: 01/08/2009 to 31/10/2009

Grant within the contract between ATLINKS ESPAÑA S.A. and University of Malaga. Reference: 8.06/47.2188. From 01/11/2003 to 31/10/2004