CURRICULUM VITÆ

Massimo Merro

Professor in Computer Science

1 General information

Address:

Department of Computer Science, University of Verona,
Strada le Grazie 15, 37134 Verona (Italy)
Phone: (+39) 045 802 7992
E-mail: massimo.merro@univr.it
Web: http://profs.scienze.univr.it/∼merro/

Birthday and birthplace:
June 9, 1970; Messina (Italy).

Qualifications and positions:

- *Full Professor* in Computer Science at University of Verona (2018-);
- *National Habilitation to Full professorship* in Computer Science, SSD INF01 - Informatica (2013);
- *Associate Professor* in Computer Science at University of Verona (2006-2018);
- *Assistant Professor* in Computer Science at University of Verona (2002-2006);
- *Research Fellow* at the Laboratoire des Méthodes de Programmation, Institute d'Informatique Fondamentale, Ecole Polytechnique Fédérale de Lausanne, Switzerland (2002);
- *Research Fellow* at the School of Cognitive and Computing Science, University of Sussex, UK (2000-2002).

Diplomas:

- *PhD in Computer Science*, with full marks and honours, École Nationale Supérieure des Mines de Paris at Sophia-Antipolis, France (2000). Thesis title: "Locality in the π-calculus and applications to distributed objects". Funded by a 18 months *TMR Marie Curie Research Training Grant*.
- *Master (Laurea) degree cum Laude* in Computer Science, University of Pisa, Italy (1996). Thesis title: "Priorities in Statecharts".

Research interests:

- Semantic foundations of cyber-physical systems and IoT systems.
- Formal security analysis of cyber-physical systems and IoT systems.
- Formal verification of complex systems via semantic techniques and static analysis.
- Semantic foundations of programming languages for concurrent, distributed, and mobile systems.

2 Research activity

The research activity of Dr. Merro has focussed on the semantic foundations of *concurrent, distributed and mobile systems*. More recently, Dr. Merro turned his attention to *wireless systems*, embracing both semantic foundations and formal verification of ad-hoc networks protocols. Dr. Merro is also working on the semantic foundations of the *Internet of Things*, paying particular attention to provide solid bases for the formal verification of the security of such systems, and, more generally, of the security of *cyber-physical systems*.

Models for Concurrent Languages

Papers [54, 50, 15, 43] study a variant of Milner's π-calculus, called Local π, as a core model for *concurrent and/or distributed programming languages*, such as Pierce and Turner's *Pict*, Fournet and Gonthier's *Join*, and Boudol's *Blue*. Those papers show that Local π retains much of the expressive power of the π-calculus. Papers [54, 15] study the semantic theory of Local π, focusing on *bisimulation-based* behavioural equivalences. In [52] special processes, called *equators*, are investigated. Equators have been proposed by Honda to model equivalence relations over channel names. Paper [53] studies the relationship between equators and the *fusions* of names, in the style of Parrow and Victor's *Fusion calculus*. In their work, Parrow and Victor argued that Fusion calculus is strictly more expressive than π-calculus. Paper [53] shows that this is not the case by providing a fully abstract encoding of (an asynchronous variant of) Fusion calculus into (an asynchronous variant of) π-calculus.

Semantics of Concurrent Languages

Modern programming languages achieve concurrency through multithreading, which translates into true parallelism on multicore hardware. Thus, writing complex and correct multithreaded software is essential to exploit the full computing power of current and future hardware; it is also a natural choice for web services; cloud computing, avionics, aerospace and car industry. However, synchronisation has a cost; *data races* lead to subtle and non-repeatable bugs. languages.

To prevent concurrency errors, programmers need to obey a *locking discipline*. Annotations that specify that discipline, such as Java's `@GuardedBy`, are already widely used. Papers [29, **?**] provide the first formalisation of the semantics of `@GuardedBy`, building on an operational semantics for a small concurrent fragment of a Java-like language. These two papers precisely identify when such annotations are actual guarantees against data races. The results in [29, **?**] have been used to extend the Julia static analyser to check and infer `@GuardedBy` annotations in arbitrary Java code. This work is at the core of the Joint Project named "Static Analysis for Multithreading", where Dr. Merro is the principal investigator.

Semantics of Distributed Object-oriented Languages

Papers [51, 17] solved an open problem in Cardelli's distributed object-oriented programming language *Obliq*. In this setting, Cardelli proposed that *object migration* can be derived from two other primitives, *cloning* and *aliasing*, by performing one after the other. In concurrent and distributed programs, it is important that certain state changes may happen transparently from the point of view of the rest of the system. Ensuring that the implementation of such state changes is in fact transparent can be a difficult task since the programmer must, in principle, anticipates all possible execution scenarios. Thus, the open issue was whether object migration in Obliq is transparent to object's clients, and how that could be formally proved.

Following Cardelli's original semantics, papers [51, 17] give a formal semantics for (an appropriate abstraction of) Obliq. The language is equipped with a standard notion of program equivalence defined in terms of "may convergence". The correctness of migration is then formalised by means of a simple equation saying that the behaviour of a migrating object must be preserved after migration. Surprisingly, this equation is not valid in Cardelli's semantics. Some counterexamples show that object-migration is not transparent to object's clients. As a solution, papers [49, 16, 43] provide an amended variant of the original semantics of Obliq in Local π, and present a formal proof of the desired equation for a wide class of Obliq programs.

Semantics of Distributed and Mobile Languages

Dr. Merro has worked on algebraic models for distributed programming languages supporting code mobility, such as $D\pi$ (Hennessy and Riely 1998) and *Ambients* (Cardelli and Gordon 1998). In calculi with code mobility, one of the major open problems was to define an appropriate notion of labelled bisimilarity based on some standard contextual behavioural equivalence. Papers [48, 11] define a labelled bisimilarity for an extension of *Safe Ambients* (Levi and Sangiorgi 1999). The main result is that, in such setting, the labelled bisimilarity is both sound and complete with respect to a standard contextual equivalence. Characterisations of contextual equivalences in higher-order languages are rare and notoriously hard, in particular in the presence of private names. The result appeared in [48, 11] is the first one for process calculi with code mobility. Then, Dr. Merro focussed on type theory, working on the definition of appropriate type systems to control code mobility in Ambient calculi [47, 46, 13]. This knowledge has then been used to extend Dπ with a typed semantics theory [45, 14]. Finally, the work in [48, 11] has been refined in [44, 42, 12] to provide a bisimulation-based semantic theory of the original Ambient calculus of Cardelli and Gordon.[1]

Foundations of Wireless Systems

Many technical challenges have emerged in the design of robust and secure wireless networks. This because wireless communications brings a dynamic aspect into the digital environment and extends security-related requirements.

Papers [40, 9] proposed the first process calculus for *mobile* ad hoc networks, providing a semantics theory and a labelled characterisation of a standard contextual equivalence.[2] This model has been subsequently extended in [39, 7] with a discrete notion of time to provide a proper formalisation of *communication collisions*, a well-known problem in wireless systems which has a strong impact on communication performance. Papers [32, 4] extend and generalise the work in [7] by providing a fully abstract characterisation of a standard contextual equivalence in terms of a non-trivial labelled bisimilarity.[3]

Formal Verification of Protocols for Ad Hoc Networks

Most of the analyses of protocols for wireless networks are usually based on discrete-event simulators (e.g., ns-2, Opnet and Glomosim). However, different simulators often support different models of the MAC physical-layer yielding different results. On the other hand, formal analysis techniques allow to screen protocols for flaws and to exhibit counterexamples to diagnose them.

Many protocols for wireless networks rely on a common notion of time among the devices at MAC layer. The correctness of *clock synchronization protocols* is quite unexplored and many attacks in wireless systems consist in preventing node synchronization. Paper [33] does *statistical model-checking* to verify the gMAC protocol, a clock synchronization protocols proposed within the EU Project QUASIMODO. The main result is that the protocol fails to correctly synchronise nodes, when considering lossy communication.

Gossip protocols are at the intermediate Gossip layer which is responsible for insertion of new messages, forwarding of current messages and deletion of old messages. Paper [35] defines a simple probabilistic timed process calculus equipped with a simulation theory to compare probabilistic protocols that have similar behaviour up to a certain probability. This theory is then used to prove a number of algebraic laws which revealed to be very effective to evaluate the performance of gossip networks with and without communication collisions.

Ad hoc networks rely on multi-hop wireless communications where nodes have essentially two roles: (i) acting as end-systems and (ii) performing routing functions. *Ad hoc routing protocol* are fundamental to determine the appropriate paths on which data should be transmitted in a wireless network. In papers [31, 23] the performances of the AODV routing protocol and its 15-years-later variant DYMO are compared, in terms of route established, by applying statistical model-checking.

[1] In the VQR 2004-2010 national evaluation, both papers [12, 11] have been evaluated as "excellent" (score 1).
[2] In the VQR 2004-2010 national evaluation, paper [9] has been evaluated as "excellent" (score 1).
[3] Paper [32] got the DisCoTec 2013 best paper award.

The main result is that, in contradiction with a recent result by Höfner and McIver, Dymo performs better than AODV on networks of significant size.

Security Aspects of Wireless Systems

Ad hoc routing protocols are exposed to several kinds of attacks. Thus, many "secured" versions of routing protocols have been proposed to work in an adversarial setting. However, security protocols are notoriously difficult to get right. Paper [37] applies model-checking techniques on two secure ad hoc routing protocols: ARAN and endairA. The analysis found two different attacks on ARAN.

In the last 30 years, several efforts have been made to prevent unauthorized information flow in multilevel computer systems. The seminal idea of non-interference (Goguen and Meseguer 1982) aims at assuring that information can only flow from low levels to higher ones. The first taxonomy of non-interference-like properties has been uniformly defined and compared by Focardi and Gorrieri. Papers [36, 34, 5] extend and generalise Gorrieri and Martinelli's tGNDC property to perform a *semantic security analysis* on three well-known *key management protocols* for wireless sensor netorks: μTESLA, LEAP+ and LiSP. The analysis found two replay attacks in the last two protocols.

Trust Management (TM) is a general approach to specifying and interpreting security policies, credentials, and trusting relationships. In highly dynamic setting a formal treatment of trust management revealed to be quite challenging. Papers [38, 6] proposes a security-based process calculus for mobile ad hoc networks which relies on an abstract *behaviour-based multilevel trust model*. Communication in the calculus are safe with respect to the security levels of the involved parties. In particular, *safety despite compromise* is ensured: compromised nodes cannot affect the rest of the network. A *non-interference* result is also proved in terms of information flow.

Semantic and Security Foundations of IoT Systems and Cyber-Physical Systems.

In the Internet of Things (IoT) paradigm, smart objects interact among themselves and with the physical environment by exchanging physical and logical data. The current research on IoT is mainly focusing on practical applications such as the development of enabling technologies, ad hoc architectures, semantic web technologies, and cloud computing. However, there is a lack of research on the modelling and the validation of IoT systems through formal methodologies. Papers [30, 3] proposes a fully abstract semantic theory for a process calculus of systems/devices in the context of the Internet of Things. Security issue concerning IoT platforms to automatically develop IoT apps are investigated in [18]. Given their ability to be potentially upgraded with external code, IoT systems may acquire disruptive potentiality that could lead to serious repercussions. This is even more evident in *cyber-physical systems* (CPSs) where system failure would be extremely costly and threaten not only the systems environment, but also the existence of the organisation that operates the system or, ultimately, even human life. Papers [26, 1] propose a hybrid process calculus for modelling and reasoning on cyber-physical systems. The paper provides the first compositional bisimulation-based behavioural semantics to compare different CPSs. Papers [19] provides a reachability result for a non-trivial class of linear CPSs, *i.e.*, CPSs whose physical processes can be expressed in terms of linear differential equations. Paper [25, 20] relies on the formal semantics for CPSs developped in [26], focussing on a formal treatment of both integrity and DoS attacks to physical devices (sensors and actuators) of CPSs, paying particular attention to the timing aspects of these attacks. This step is essential to develop formal and automated analysis techniques to be made available to the "practitioners" for checking the security of their CPSs. First attempts to provide a security of formal verification of non-trivial CPSs can be found in [22, 21].

2.1 Editorial boards

- Editor of *Open Computer Science*, `http://www.degruyter.com/view/j/comp` (2015-);
- Review Editor of *Frontiers in ICT, Computer and Network Security*, (2014-) `http://journal.frontiersin.org/journal/ict/section/computer-and-network-security`;

- Associate Editor of *Mobile Information Systems*, (2014-)
  `https://www.hindawi.com/journals/misy/`;

2.2 Program committes

- 20° *Italian Conference on Theoretical Computer Science (ICTCS'19)*, Como, Italy, 2019.
- 14° *International Conference on Embedded Software* (EMSOFT'17), Seoul, South Korea, 2017.
- 36° *IFIP International Conference on Formal Techniques for Distributed Objects, Components and Systems* (FORTE'16), Heraklion, Crete, 2016.
- 43° *International Colloquium on Automata, Languages and Programming* (ICALP'16) – Track B: Logic, Semantics, Automata and Theory of Programming, Rome, Italy, 2016.
- 42° *International Colloquium on Automata, Languages and Programming* (ICALP'15) – Track C: Foundations of Networked Computation: Models, Algorithms and Information Management, Kyoto, Japan, 2015.
- 38° *International Colloquium on Automata, Languages and Programming* (ICALP'11) – Track C: Foundations of Networked Computation: Models, Algorithms and Information Management, Zurich, Switzerland, 2011.
- 4° *International Conference on Frontier of Computer Science and Technology* (FCST'09), Shanghai, China, 2009.
- 2° *International Workshop on Formal Methods for Wireless Systems* (FMWS'09), Bologna, Italy, 2009.
- 2° *International Meeting on Membrane Computing and Biologically Inspired Process Calculi* (MeCBIC'08), Iasi, Romania, 2008.
- 1° *International Workshop on Formal Methods for Wireless Systems* (FMWS'08), Toronto, Canada, 2008.
- 17° *International Conference on Concurrency Theory* (CONCUR'06), Bonn, Germany, 2006.
- 10° *International Workshop on Expressivity in Concurrency* (EXPRESS'03), Marseilles, France, 2003.
- 9° *International Workshop on Expressivity in Concurrency* (EXPRESS'02), Brno, Czech Republic, 2002.

2.3 Qualifications and awards

International:

- The paper [CHM13] got the best paper award at the Federated Conference Event *DisCoTec* 2013.
- PhD at École Nationale Suprieure des Mines de Paris in Sophia-Antipolis, France, with mention "*Trés honorable avec félicitations du jury*" (2000).
- 18 months *TMR Marie Curie Research Training Grant* (1998).

National:

- In the VQR 2004-2010 national evaluation, the following papers:
  - M. Merro and F. Zappa Nardelli. Behavioural Theory for Mobile Ambients. Journal of the ACM 52(6):961-1023, 2005
  - M. Merro and M. Hennessy. A Bisimulation Semantic Theory of Safe Ambients. ACM Transactions on Programming Languages and Systems 28(2):290-330, 2006
  - M. Merro. An Observational Theory for Mobile Ad Hoc Networks (full version). Information and Computation 207(2):194-208, 2009

  have been all evaluated as "excellent" (score 1).
- In the VQR 2011-2014 national evaluation, the following papers:
  - M. Merro, F. Ballardin and E. Sibilio. A Timed Calculus of Wireless Systems. Theoretical Computer Science 412(47): 6585-6611, 2011.
  - M. Merro and E. Sibilio. A calculus of trustworthy ad hoc networks. Formal Aspects of Computing 25(5):801-832, 2013.

  have been all evaluated "very good" (score 0.7).

2.4 Research projects since year 2000

- Joint Project 2017 titled "Security Static Analysis for Android Things", funded by University of Verona, for Euro 164.318, from 01.01.2018 to 31.12.2020 (*Principal Investigator*).
- Joint Project 2011 titled "Static Analysis for Multithreading", founded by the University of Verona, for Euro 135.083, from 01.01.2013 to 30.06.2015 (*Principal Investigator*).
- National Italian PRIN Project 2010-2011 named "Security Horizons", from 01.02.2013 to 01.02.2016 (*Investigator*).
- EU project VII PQ (2011-2013) "SPaCIoS: Secure Provision and Consumption in the Internet of Services" (*Investigator*).
- EU project VII PQ (2009-2011); "AVANTSSAR: Automated ValidatioN of Trust and Security of Service-oriented ARchitectures" (*Investigator*).
- National Italian PRIN Project 2007 named "SOFT: Security-Oriented Formal Techniques" (*Investigator*).
- National Italian PRIN Project 2005-2006 named "Formal Verification by Abstract Interpretation" (*Investigator*).

2.5 Supervision of research students and fellows

- Research Fellow, Dr. Michele Pasqua. Title of the project: *Security Static Analysis for Internet of Things*, University of Verona, 2019-2020.
- Research Fellow Dr. Fabio Mogavero. Title of the project: *Formal Verification of Cyber-Physical System Security*, University of Verona, 2018.
- PhD student, Dr. Andrei Munteanu. Thesis title: *Formal Security Verification of Cyber-Physical Systems*. University of Verona, 2018-2020.
- PhD student Dr. Eleonora Sibilio. Thesis title: *Formal Methods for Wireless Systems*. Università degli Studi di Verona, 2011.

- External PhD student Dr. Leckraj Nagowah. Thesis title: *Formal Methods for Securing IoT Systems*. University of Mauritius, Moka, 2017-.
- Visiting PhD student Dr. Mojgan Kamali, Abo Akademi University, Turku, Finland. Project title: Statistical model checking of ad hoc routing protocols. Sep-Dec 2016.
- Research Fellow Dr. Damiano Macedonio. Project title: *Formal Verification of Wireless Network Protocols*, Università degli Studi di Verona, 2011-2013.
- Research Fellow of 12 months to be assigned. Project title: *Formal Tools for Cyber-Physical System Security*, Università degli Studi di Verona, July 2017.

3 Publications

Bibliometrics:

The following data are extracted by *Elsevier's Scopus* database as to September 2019:

- papers: 55
- citations: 840 (707, excluding self citations)
- h-index: 18 (17, excluding self citations)
- g-index: 25 (25, excluding self citations)
- authors/paper: 2.3.

The following data are extracted by *Google Scholar* database as to September 2019:

- documents: 60
- citations: 1509
- h-index: 23
- g-index: 25
- authors/paper: 2.3.

In the following lists of papers, alphabetical order for authors means equal contribution in the paper. On the contrary, when the alphabetic order is not respected, the first author gave a major contribution.

International journals:

[1] R. Lanotte, M. Merro and S. Tini. A Probabilistic Calculus of Cyber-Physical Systems. Accepted for publication in *Information and Computation*, 40 pages.

[2] R. Lanotte, M. Merro and S. Tini. Equational Reasonings in Wireless Network Gossip Protocols. *Logical Methods in Computer Science*, 14(3):1-47, 2018.

[3] R. Lanotte and M. Merro. A Semantic Theory of the Internet of Things, *Information and Computation*, 259(1):72-101, 2018.

[4] A. Cerone, M. Hennessy, M. Merro. Modelling MAC-Layer Communications in Wireless Systems. *Logical Methods in Computer Science*, 11(1), paper 18, 1–59, 2015.

[5] D. Macedonio and M. Merro. A semantic analysis of key management protocols for wireless sensor networks. *Science of Computer Programming*, 81:53-78, 2014.

[6] M. Merro and E. Sibilio. A Calculus of Trustworthy Ad Hoc Networks. *Formal Aspects of Computing* 25(5):801-832, 2013.

[7] M. Merro, F. Ballardin and E. Sibilio. A Timed Calculus for Wireless Systems. *Theoretical Computer Science* 412(47):6585-6611, 2011.

[8] M. Merro. An Observational Theory of the CPS-calculus. *Acta Informatica* 47(2):111-132, 2010.

[9] M. Merro. An Observational Theory for Mobile Ad Hoc Networks (full paper). *Information & Computation* 207(2):194-208, 2009.

[10] R. Fuzzati, M. Merro and U. Nestmann. Distributed Consensus, Revisited. *Acta Informatica* 44(26):377-425, 2007.

[11] M. Merro and M. Hennessy. A Bisimulation-based Semantic Theory of Safe Ambients. *ACM Transactions on Programming Languages and Systems* 28(2):290-330, 2006.

[12] M. Merro and F. Zappa Nardelli. Behavioural Theory for Mobile Ambients. *Journal of the ACM* 52(6):961-1023, 2005.

[13] M. Bugliesi, S. Crafa, M. Merro and V. Sassone. Communication and Mobility Control in Boxed Ambients. *Information & Computation* 202(1):39-86, 2005.

[14] M. Hennessy, M. Merro and J. Rathke. Towards a behavioural theory of access and mobility control in distributed systems. *Theoretical Computer Science* 322(3):615-669, 2004.

[15] M. Merro and D. Sangiorgi. On asynchrony in name-passing calculi. *Mathematical Structures in Computer Science* 14(5):715-767, 2004.

[16] M. Merro, J. Kleist and U. Nestmann. Mobile Objects as Mobile Processes. *Information & Computation* 177(2):195-241, 2002.

[17] U. Nestmann, H. Hüttel, J. Kleist and M. Merro. Aliasing Models for Mobile Objects. *Information & Computation* 175(1):3-33, 2002.

International conferences and symposia:

[18] M. Balliu, M. Merro and M. Pasqua. Securing cross-app interactions in IoT platforms. In *32th IEEE Computer Security Foundations Symposium (CSF'19)*, IEEE Computer society, pp. 319-334, 2019.

[19] R. Lanotte, F. Mogavero and M. Merro. On the decidability of linear bounded periodic cyber-physical systems. In *22nd ACM International Conference of Hybrid Systems: Computation and Control (HSCC 2018)*, pp. 87-98, ACM Press, 2019.

[20] R. Lanotte, M. Merro and S. Tini. Towards a formal notion of impact metric for cyber-physical attacks. In *14th International Conference on integrated Formal Methods (iFM 2018)*, Volume 11023 of Lecture Notes in Computer Science, pp. 296-315, Springer, 2018.

[21] A. Munteanu, R. Muradore, M. Merro and P. Fiorini. On cyber-physical attacks in bilateral teleoperation systems: An experimental analysis. In *1st IEEE International Conference on Industrial Cyber-Physical Systems (ICPS-2018)*, pp. 159-166, IEEE Industrial Electronics Society, 2018.

[22] R. Lanotte, M. Merro and A. Munteanu. A Modest Security Analysis of Cyber-Physical Systems: A Case Study. In *38th IFIP WG 6.1 International Conference on Formal Techniques for Distributed Objects, Components, and Systems (FORTE'18)*. Volume 10854 of Lecture Notes in Computer Science, pp. 58-78, Springer, 2018.

[23] M. Kamali, M. Merro and A. Dal Corso. AODVv2: performance vs. loop freedom. In *44th International Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM'18)*. Volume 10706 of Lecture Notes in Computer Science, pp. 337-350, Springer, 2018.

[24] R. Lanotte, M. Merro and S. Tini. Compositional weak metrics for group key update. In *42nd International Symposium on Mathematical Foundations of Computer Science (MFCS'17)*. Volume 83 of LIPIcs series, pp. 72:1-27:16, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017.

[25] R. Lanotte, M. Merro, R. Muradore and L. Viganò. A Formal Approach to Cyber-Physical Attacks. In *30th IEEE Computer Security Foundations Symposium (CSF'17)* IEEE Computer society, pp. 436-450, 2017.

[26] R. Lanotte and M. Merro. A Calculus of Cyber-Physical Systems. In *11th International Conference on Language and Automata Theory and Applications (LATA'17)*. Volume 10168 of Lecture Notes in Computer Science, pp. 115-137, Springer, 2017.

[27] R. Lanotte, M. Merro and S. Tini. Weak Simulation Quasimetric in a Gossip Scenario. In *37th IFIP WG 6.1 International Conference on Formal Techniques for Distributed Objects, Components, and Systems (FORTE'17)*. Volume 10321 of Lecture Notes in Computer Science, pp. 139-155, Springer, 2017.

[28] R. Lanotte, M. Merro and S. Tini. Compositional weak metrics for group key update. In *42nd International Symposium on Mathematical Foundations of Computer Science (MFCS'17)*. To appear on LIPIcs, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik.

[29] M.D. Ernst, D. Macedonio, M. Merro and F. Spoto. Semantics for Locking Specifications. In *8th NASA Formal Methods Symposium (NFM'16)*. Volume 9690 of Lecture Notes in Computer Science, pp. 355-372, Springer, 2016.

[30] R. Lanotte and M. Merro. A Semantic Theory of the Internet of Things (extended abstract). In *18th IFIP International Conference on Coordination Models and Language (COORDINATION'16)*. Volume 9686 of Lecture Notes in Computer Science, pp. 157-174, Springer, 2016.

[31] A. Dal Corso, D. Macedonio and M. Merro. Statistical Model Checking of Ad Hoc Routing Protocols in Lossy Grid Networks. In *7th NASA Formal Methods Symposium (NFM'15)*. Volume 9058 of Lecture Notes in Computer Science, pp. 112-126, Springer, 2015.

[32] A. Cerone, M. Hennessy and M. Merro. Modelling MAC-Layer Communications in Wireless Systems. In *15th IFIP International Conference on Coordination Models and Language (COORDINATION'13)*. Volume 7890 of Lecture Notes in Computer Science, pp. 16-30, Springer, 2013.

[33] L. Battisti, D. Macedonio and M. Merro. Statistical Model Checking of a Clock Synchronization Protocol for Sensor Networks. In *5th IPM International Conference on Fundamentals of Software Engineering (FSEN'13)*. Volume 8161 of Lecture Notes in Computer Science, pp. 168-182, Springer, 2013.

[34] D. Macedonio and M. Merro. A Semantic Analysis of Wireless Network Security Protocols. In *4th NASA Formal Methods Symposium (NFM'12)*. Volume 7226 of Lecture Notes in Computer Science, pp. 403-417, Springer, 2012.

[35] R. Lanotte and M. Merro. Semantic Analysis of Gossip Protocols for Wireless Sensor Networks. In *22nd International Conference on Concurrency Theory (CONCUR'11)*. Volume 6901 of Lecture Notes in Computer Science, pp. 156-170, Springer, 2011.

[36] F. Ballardin and M. Merro. A Calculus for the Analysis of Wireless Network Security Protocols. In *7th Workshop on Formal Aspects in Security and Trust (FAST'10)*. Volume 6561 of Lecture Notes in Computer Science, pp. 206-222, Springer, 2011.

[37] D. Benetti, M. Merro and L. Viganò. Model Checking Ad Hoc Network Routing Protocols: ARAN vs. endairA. In *8th IEEE Conference on Software Engineering and Formal Methods (SEFM'10)*, IEEE Computer Society Press, pp. 191-202, 2010.

[38] M. Merro and E. Sibilio. A Calculus of Trustworthy Ad Hoc Networks. In *6th International Workshop on Formal Aspects in Security and Trust (FAST'09)*. Volume 5983 of Lecture Notes in Computer Science, pp. 157-172, Springer, 2010.

[39] M. Merro and E. Sibilio. A Timed Calculus for Wireless Systems. In *3rd International Conference on Fundamentals on Software Engineering (FSEN'09)*. Volume 5961 of Lecture Notes in Computer Science, pp. 228-243, Springer, 2010.

[40] M. Merro. An Observationl Theory for Mobile Ad Hoc Networks. In *23rd International Conference on the Mathematical Foundations of Program Semantics (MFPS'07)*. Electronic Notes in Theoretical Computer Science 173:275-293, Elsevier, 2007.

[41] M. Merro and C. Biasi. On the observational theory of the CPS-calculus. In *22nd International Conference on the Mathematical Foundations of Program Semantics (MFPS'06)*. Electronic Notes in Theoretical Computer Science 158:307-330, Elsevier, 2006.

[42] M. Merro and F. Zappa Nardelli. Behavioural Theory for Mobile Ambients. In *3rd International Conference on Theoretical Computer Science (IFIP TCS 2004)*, pp. 549-562, Kluwer, 2004.

[43] U. Nestmann, R. Fuzzati and M. Merro. Modeling consensus in a process calculus. In *14th International Conference on Concurrency Theory (CONCUR'03)*. Volume 2761 of Lecture Notes in Computer Science, pp. 399-414, Springer, 2003.

[44] M. Merro and F. Zappa Nardelli. Bisimulation proof techniques for mobile ambients. In *30th International Colloquium on Automata, Languages, and Programming (ICALP'03)*. Volume 2719 of Lecture Notes in Computer Science, pp. 584-598, Springer, 2003.

[45] M. Hennessy, M. Merro and J. Rathke. Towards a Behavioural Theory of Access and Mobility Control in Distributed System. In *6th International Conference on the Foundations of Software Science and Computation Structures (FOSSACS'03)*. Volume 2620 of Lecture Notes in Computer Science, pp. 282-297, Springer, 2003.

[46] M. Bugliesi, S. Crafa, M. Merro and V. Sassone. Communication Interference in Mobile Boxed Ambients. In *22th International Conference on the Foundations of Software Technology and Theoretical Computer Science (FST&TCS'02)*. Volume 2556 dof Lecture Notes in Computer Science, pp. 71-84, Springer, 2002.

[47] M. Merro and V. Sassone. Typing and Subtyping Mobility in Boxed Ambients. In *13th International Conference on Concurrency Theory (CONCUR'02)*. Volume 2421 of Lecture Notes in Computer Science, pp. 304-320, Springer, 2002.

[48] M. Merro and M. Hennessy. Bisimulation Congruences in Safe Ambients. Conference record of *29th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'02)*. Volume 37(1), pp. 71-80, ACM Press, 2002.

[49] M. Merro, J. Kleist and U. Nestmann. Local π-Calculus at work: Mobile Objects as Mobile Processes. In *1st IFIP International Conference on Theoretical Computer Science (IFIP TCS'00)*. Volume 1872 of Lecture Notes in Computer Science, pp. 390-408, Springer, 2000.

[50] M. Merro. Locality and Polyadicity in Asynchronous Name-passing Calculi. In *3rd International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'00)*. Volume 1784 of Lecture Notes in Computer Science, pp. 238-251, Springer, 2000.

[51] H. Hüttel, J. Kleist, M. Merro e U. Nestmann. Aliasing Models for Object Migration. In *5th International EURO-PAR'99 - PARALLEL PROCESSING Conference*. Volume 1685 of Lecture Notes in Computer Science, pp. 1353-1368, Springer, 2000.

[52] M. Merro. On Equators in Asynchronous Name-passing Calculi without Matching. In *6th International Workshop on Expressiveness in Concurrency (EXPRESS'99)*. Electronic Notes in Theoretical Computer Science 27:57-70, Elsevier, 1999.

[53] M. Merro. On the Expressiveness of Chi, Update, and Fusion calculi. In *5th International Workshop on Expressiveness in Concurrency (EXPRESS'98)*. Electronic Notes in Theoretical Computer Science 16(2):133-144, Elsevier, 1998.

[54] M. Merro and D. Sangiorgi. On Asynchrony in Name-passing Calculi. In *25th International Colloquium on Automata, Languages and Programming (ICALP'98)*. Volume 1443 of Lecture Notes in Computer Science, pp. 856-867, Springer, 1998.

[55] A. Maggiolo-Schettini e M. Merro. Priorities in Statecharts. In *5th Workshop on Analysis and Verification of Multiple-Agent Languages (LOMAPS'96)*. Volume 1192 of Lecture Notes in Computer Science, pp. 404-429, Springer, 1996.

PhD thesis:

[43] M. Merro. Locality in the pi-calculus and applications to distributed objects. *École Nationale Supérieure des Mines de Paris*. October 2000.

4 Teaching activity

Dr. Merro has 17 years of experience in university-level undergraduate and graduate teaching in Computer Science, at University of Verona, with responsibility of courses in the field of: Programming, Formal Languages, Programming Language for Distributed Systems, Network Programming, and Network Security. More precisely,

4.1 Courses

Undergraduate:

- *Automata Theory*, 20h, University of Sussex, UK, (2000-2002)
- *Network and Distributed Programming*, 60h, Univ. Of Verona (2003-2013)
- *Man-machine interaction*, 20h, Faculty of Literature and Philology, University of Verona (2004-2005)
- *Basics in Informatics*, 24h, University of Verona (2006-2009)
- *Object-Oriented Programming*, 60h, University of Verona (2009-2010).

Graduate:

- *Concurrent and Mobile Languages*, 60h, University of Verona (2003-2009)
- *Semantics ans Static Analysis of Programming Languages*, 56h, University of Verona (2010-)
- *Network Security*, 52h, University of Verona (2013-).

4.2 Stages, bachelor and master theses supervision

Dr. Merro has supervised (and revised) several industrial and academic stages, bachelor theses, and master theses. A number of these works have given rise to publications in international conferences or symposia. In particular:

- paper [21] exends and generalises soem of the results appeared in the master thesis of Andrei Munteanu.
- paper [31] extends and generalises some of the results obtained during the the stage and the bachelor thesis of Alice Dal Corso; some preliminary work was done during the stages of students Marco Campion and Giacomo Annaloro;
- paper [33] extends and generalises some of the results obtained during the stage and the bachelor thesis of Luca Battisti;
- paper [34] relies on some preliminary results obtained during the master thesis of Mattia Tirapelle.
- paper [36, 7] extends and generalises some of the results obtained during the stage and the bachelor thesis of Francesco Ballardin.
- paper [37] relies on the results appeared in the master thesis of Davide Benetti; Benetti's master thesis got a prize from Clusit (Associazione Italiana per la Sicurezza Informatica) in 2010;
- paper [41] extends and generalises some of the results of the master thesis of Corrado Biasi.

5 Institutional activity

- Coordinator of the PhD Program in Computer Science of Verona (2016-);
- President of the self-evaluation commission for the high quality of the master course in Computer Science and Engineering (2016-2019);
- Member of *Giunta del Consiglio di Dipartimento in Informatica di Verona*, (2009-2015 and 2019-);
- Member of *Collegio dei Docenti del Dottorato in Informatica di Verona*, (2003-);
- President of *Commissione Didattica, Laurea in Informatica ed Informatica Multimediale, Facoltà di Scienze MMFFNN dell'Università di Verona*, (2006-2013);
- Member of *Commissione Didattica del GRIN*, (2008-2011);
- Vice President of *Corso di Laurea in Informatica della Facoltà di Scienze MMFFNN dell'Università di Verona*, (2006-2012).