Curriculum Vitae:

First Name: Angelo
Last Name: TROINA
Place and Date of Birth: Wolfsburg (D), 09/08/1979
Address: Dipartimento di Informatica, Largo B. Pontecorvo 3, 56127 Pisa, Italy
E-mail: troina@di.unipi.it
Home Page: http://www.di.unipi.it/~troina

1. Education:

Master Degree in Computer Science at the University of Bologna (Italy)
with Distinction (110 mark over 110 cum laude)
Title of the thesis:
"Un Approccio Algebrico Probabilistico all'Analisi di Proprietà di Sicurezza di Sistemi Crittografici" ("A probabilistic Algebraic Approach for the Analysis of Security Properties of Cryptographic Systems")
Advisor: Prof. Roberto Gorrieri
Date: October 2002

Currently a Ph.D. Student in Computer Science at the University of Pisa.
Ph.D. degree expected by June 2006.
Title of the thesis: Probabilistic Timed Automata for Security Analysis and Design
Supervisor: Prof. Andrea Maggiolo Schettini

1.1. Schools attended:

April 2005
" Spring School on Security", Marseille, France.

September 2004
"Foundations of Security Analysis and Design" (FOSAD04), Bertinoro (FC), Italy.

September 2003
"Advanced School on Mobile Computing", Pisa, Italy.

March 2003
"Bertinoro International Spring School" (BISS'03), Bertinoro (FC), Italy.

2. Research Activity:

2.1. Research Fields of Interest:

- Formal Description Techniques of Concurrent Systems
- Formal Modeling and Verification of Real-Time and Probabilistic Systems
- Foundations of Security Analysis and Design
- Systems Biology

2.2. Research Activity – A brief report

While some system properties can be studied in a non-timed and non-probabilistic setting, others, such as quantitative security properties, system performance and reliability properties, require a timed and probabilistic description of the system. My research activity focused on methods for formal modeling and specification of probabilistic timed systems, and on algorithms for the automated verification of their properties. The models considered describe the behavior of a system in terms of time and probability, and the formal specification languages used are based on extensions of timed automata, Markov decision processes and probabilistic replacement rules.

These techniques are applied in two main fields: (1) Security Analysis and (2) Systems Biology.

Security Analysis

In multilevel systems it is important to avoid unwanted indirect information flow from higher levels to lower levels, namely the so called *covert channels*. Initial studies of information flow analysis were performed by abstracting away from time and probability. It is already known that systems that are considered to be secure may turn out to be insecure when time or probability are considered. Recently, work has been done in order to consider also aspects either of time or of probability, but not both.

In [17] a concept of weak bisimulation for Probabilistic Timed Automata is given, together with an algorithm to decide it. This model is used for describing and analyzing a probabilistic non-repudiation protocol in a timed setting.

In [13,7] a general framework is proposed, which is based on Probabilistic Timed Automata, where both *probabilistic* and *timing covert channels* can be studied. A Non-Interference security property and a Non Deducibility on Composition security property are defined. They allow expressing information flow in a timed and probabilistic setting, and they can be compared with analogous properties defined in settings where either time or probability or none of them are taken into account. This permits a classification of the properties depending on their discerning power.

In [18,16,8] the assumption of perfect cryptography is relaxed and a new probabilistic equivalence of messages exchanged in a communication protocol is introduced. The methodology takes to the definition of a probabilistic notion of secrecy.

In [14] a probabilistic model is defined for the analysis of a Non-Repudiation protocol which guarantees fairness without resorting to a trusted third party, by means of a probabilistic algorithm. The PRISM model checker is used for estimating the probability for a malicious user to break the non-repudiation property.

The *NRL Pump* protocol defines a multilevel secure component whose goal is to minimize leaks of information from high level systems to lower level systems, without degrading average time performances. In [15,9] a probabilistic model for the NRL Pump is defined and the FHP-murϕ probabilistic model checker is used to estimate the capacity of a probabilistic covert channel in the NRL Pump.

In [12] a model of Parametric Probabilistic Transition Systems is developed, where probabilities associated with transitions may be parameters. Techniques are proposed to find instances of parameters that satisfy a given property and instances that either maximize or minimize the probability of reaching a certain state.

Systems of Data Management Timed Automata (SDMTAs) are networks of communicating timed automata with structures to store messages and functions to manipulate them. In [5] the decidability of reachability for SDMTAs is proved. As an application, the Yahalom protocol is modeled and analyzed.

Systems Biology

In the last few years people became aware that biological processes can be described using means originally developed by computer scientists to model systems of interacting components. This permits simulation of system behaviour and verification of properties. Among the many formalisms that have been applied to biology there are, for instance, Petri Nets, Hybrid Systems, and the pi-calculus. Moreover, some new formalisms have been proposed to describe biomolecular and membrane interactions and some models based on probabilities have been successfully used to develop simulators for biochemical systems.

In [10,6,2] a probabilistic calculus for biomolecular interaction (in particular for enzymatic activity) is introduced. The calculus is based on a set of rewrite rules whose application depends on a probability. As an alternative to Gillespie's one, an interpretation algorithm and a formal semantics are given for the calculus, and their compatibility is proven. A prototype implementation of the interpreter for the calculus is developed, which permits to follow the evolution of a biomolecular system. The formal semantics, given as a transition system, permits to verify properties of a system by model checking.

In [1,4] a new calculus is introduced, which is suitable to describe microbiological systems and their evolution. The calculus is used to model interactions among bacteria and bacteriophage viruses, and to reason on their properties.

2.3. Publications:

Journals:

[1] R. Barbuti, S. Cataudella, A. Maggiolo-Schettini, P. Milazzo, A. Troina. " A Calculus of Looping Sequences for Modelling Microbiological Systems". Fundamenta Informaticae, vol. 72, pp. 1-15, 2006.

[2] R. Barbuti, S. Cataudella, A. Maggiolo-Schettini, P. Milazzo, A. Troina. "A Probabilistic Model for Molecular Systems". Fundamenta Informaticae, vol. 67(1-3), pp. 13-27, 2005.

Conferences and Workshops Proceedings:

[3] R. Lanotte, A. Maggiolo-Schettini, P. Milazzo, A. Troina. "Modeling Long-running Transactions with Communicating Hierarchical Timed Automata". 8th IFIP Int. Conference on Formal Methods for Open Object-Based Distributed Systems (FMOODS'06), Springer LNCS, Bologna, Italy, June, 2006.

[4] R. Barbuti, A. Maggiolo-Schettini, P. Milazzo, A. Troina. "A Calculus of Looping Sequences for Modelling Microbiological Systems". 14th Int. Workshop on Concurrency Specification and Programming (CS&P'05), Warsaw University 511/2005, pp. 29-40, Ruciane-Nida, Poland, 2005.

[5] R. Lanotte, A. Maggiolo-Schettini, A. Troina. "Timed Automata with Data Structures for Distributed Systems Design and Analysis". 3nd Int. Conference on Software Engineering and Formal Methods (SEFM'05), IEEE Computer Society Press, pp. 44-53, Koblenz, Germany, September 2005.

[6] R. Barbuti, A. Maggiolo-Schettini, P. Milazzo, A. Troina. "An Alternative to Gillespie's Algorithm for Simulating Chemical Reactions". 3rd Int. Workshop on Computational Methods in Systems Biology (CMSB'05), pp. 167-178, Edinburgh, Scotland, April 2005.

[7] R. Lanotte, A. Maggiolo-Schettini, A. Troina. "A Classification of Time and/or Probability Dependent Security Properties". 3rd Int. Workshop on Quantitative Aspects of Programming Languages (QAPL'05), Elsevier ENTCS, Edinburgh, Scotland, April 2005, to appear.

[8] A. Troina, A. Aldini, R. Gorrieri. "Towards a Formal Treatment of Secrecy against Computational Adversaries". 2nd Int. Workshop on Global Computing (GC'04), Springer LNCS 3267, pp. 77-92, February 2005.

[9] R. Lanotte, A. Maggiolo-Schettini, S. Tini, A. Troina, E. Tronci. "Automatic Covert Channel Analysis of a Multilevel Secure Component". 6th International Conference on Information and Communications Security (ICICS'04), Springer LNCS 3269, pp. 249-261, Malaga, Spain, October 2004.

[10] R. Barbuti, S. Cataudella, A. Maggiolo-Schettini, P. Milazzo, A. Troina. "A Probabilistic Calculus for Molecular Systems". 13th Int. Workshop on Concurrency Specification and Programming (CS&P'04), Caputh, Germany, September 2004.

[11] R. Lanotte, A. Maggiolo-Schettini, S. Tini, A. Troina. "Verification of Hybrid Automata by Synthesis and Refinement". 13th Int. Workshop on Concurrency Specification and Programming (CS&P'04), Caputh, Germany, September 2004.

[12] R. Lanotte, A. Maggiolo-Schettini, A. Troina. "Decidability Results for Parametric Probabilistic Transition Systems with an Application to Security". 2nd Int. Conference on Software Engineering and Formal Methods (SEFM,04), IEEE Computer Society Press, pp. 114-121, Beijing, China, September 2004.

[13] R. Lanotte, A. Maggiolo-Schettini, A. Troina. "Information Flow Analysis for Probabilistic Timed Automata". 2nd Int. Workshop on Formal Aspects in Security and Trust (FAST'04), Springer IFIP 173, pp. 13-27, Toulouse, France, August 2004.

[14] R. Lanotte, A. Maggiolo-Schettini, A. Troina. "Automatic Analysis of a Non-Repudiation Protocol". 2nd Int. Workshop on Quantitative Aspects of Programming Languages (QAPL,04), Elsevier ENTCS 112, pp. 113-129, Barcelona, Spain, March 2004.

[15] R. Lanotte, A. Maggiolo-Schettini, S. Tini, A. Troina, E. Tronci. "Automatic Analysis of the NRL Pump". Proceedings of the MEFISTO Project 2003 (Formal Methods for Security and Time), Elsevier ENTCS 99, pp. 245-266, 2004.

[16] A. Troina, A. Aldini, R. Gorrieri. "Approximating Imperfect Cryptography in a Formal Model". Proceedings of the MEFISTO Project 2003 (Formal Methods for Security and Time), Elsevier ENTCS 99, pp. 183-203, 2004.

[17] R. Lanotte, A. Maggiolo-Schettini, A. Troina. "Weak Bisimulation for Probabilistic Timed Automata and Applications to Security". 1st Int. Conference on Software Engineering and Formal Methods (SEFM,03), IEEE Computer Society Press, pp. 34-43, Brisbane, Australia, September 2003.

[18] A. Troina, A. Aldini, R. Gorrieri. "A Probabilistic Formulation of Imperfect Cryptography". 1st IFIP WG 1.7 Int. Workshop on Issues in Security and Petri Nets (WISP'03), Eindhoven, the Netherlands, June 2003.

3. Teaching Activity:

2004
Teaching assistant for the course "Metodologie di Programmazione" ("Programming Methods"). Corso di Laurea in Informatica, University of Pisa.

4. Research Projects:

2003
He was involved in the project “Metodi formali per la sicurezza e il tempo” ("Formal Methods for Security and Time") (MEFISTO), funded by the Italian Ministry for Education.

2005-2009
He is involved in the project Automata: from Mathematics to Applications (AutoMathA), founded by the European Science Foundation.

5. Workshops and Conferences attended:

September 2005
" 3th International Conference on Software Egineering and Formal Methods (SEFM'05)", Koblenz, Germany. Where he presented [5].

April 2005
" 8th European Joint Conference on Theory And Practice of Software (ETAPS'05)", Edinburgh, Scotland. Where he presented [7].

October 2004
"6th International Conference on Information and Communications Security (ICICS04)", Malaga, Spain. Where he presented [9].

September 2004
"Concurrency Specification and Programming Workshop (CS&P04)", Caputh, Germany. Where he presented [11].

June 2004
"Dimacs Workshop on Security Analysis of Protocols", Piscataway (NJ), USA.
Where he presented a preliminary version of [8].

March 2004
"7th European Joint Conference on Theory And Practice of Software (ETAPS'04)", Barcelona, Spain. Where he presented [14].

November 2003
MEFISTO Project final Workshop, Pisa, Italy.
Where he presented [15].

June 2003
"1st IFIP WG 1.7 Int. Workshop on Issues in Security and Petri Nets (WISP,03)", Eindhoven, the Netherlands. Where he presented [18].

April 2003
1st Workshop of the MEFISTO Project, Salerno, Italy.

6. Reviewing Activity:

Workshop and Conferences:

- International Workshop on Constructive Methods for Parallel Programming (CMPP)
- International Workshop on Practical Applications of Stochastic Modelling (PASM)
- International Workshop on Views On Designing Complex Architectures (VODCA)
- International Workshop on Security Issues with Petri Nets and other Computational Models (WISP)
- International Static Analysis Symposium (SAS)
- International ACM Conference on Computer and Communications Security (CCS)
- International IEEE Computer Security Foundations Workshop (CSFW)
- International Colloquium on Automata, Languages and Programming (ICALP)
- International Conference on "Foundations of Software Science and Computation Structures (FOSSACS)
- International Conference on Software Engineering Research, Management and Applications (SERA)

Journals:

- Information Processing Letters
- Theoretical Computer Science