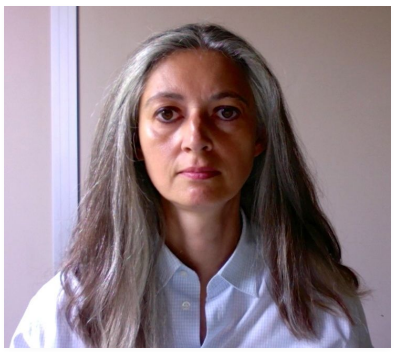
International Conference on Wireless, Intelligent, and Distributed Environment for Communication (WIDECOM 2019)

Keynotes and Tutorials

Keynote Speaker I



Dr. Elena Pagani, Associate Professor, Computer Science Department, Università degli Studi di Milano, Italy, and Associate Researcher at the Institute for

IMPORTANT DATES

Submission of papers:
Sept 20, 2018 (Closed)

Acceptance notification:
Sept. 30, 2018 (Notified)

Camera-ready papers:
Nov. 15, 2018

Conference date:
Feb. 11-13, 2019

Informatics and Telematics of the National Research Council in Pisa, Italy

Title: From WSNs to VANETs: paradigms, technologies and open research issues for challenged networks

Abstract

Wireless technologies are going to revolutionize countless aspects of daily life, touching issues ranging from smart cities to opportunistic networks, from smart vehicles to Industry 4.0. At the base of all these applications, there is the requirement of implementing communication services amongst devices possibly with scarce resources and also mobile. The purpose of this talk is to analyze the paradigms for mobile ad hoc networking and the characteristics of these infrastructures, to discuss the state of the art of the technologies and solutions available to implement them, and to highlight the research aspects that are still open.

Biography

Dr. Elena Pagani received her Master degree in Computer Science from the Università degli Studi di Milano, Italy, in 1992. From 1992 to 1993, she had a grant of the National Research Council (CNR) for the Telecommunication Research Project (Progetto FinalizzatHerMy Ph.D. Thesis concerned ``Primitives for Reliable Group Communication in Distributed Systems with Mobile Hosts'', advisors Prof. Francesco Tisato and Prof. Gian Paolo Rossi of the Computer Science Department of the Università degli Studi di Milano, and Prof. Mario Gerla of the Computer Science Department of the UCLA. From october 1999, she was an Assistant professor at the Computer Science Department of the Università degli Studi di Milano. Since march 2006, she has been an Associate professor in that same department.

Keynote Speaker II

Dr. Francesco Bruschi, Assistant professor, Computer Science Department, Università degli Studi di Milano, Italy

PAPERS PUBLISHED IN –

Springer Series 'LNDECT'

PAPERS INDEXED IN –

EI Compendex
MetaPress
ISI Proceedings
Springer link
SCOPUS

EXTENDED VERSIONS IN –

International Journal of Space-Based and Situated Computing (IJSSC), Inderscience
International Journal of Grid and Utility Computing (IJGUC)
Internet of Things Engineering Cyber Physical Human Systems
Elsevier

Title: Making sense(s) of smart contracts in a connected world

Abstract

Smart contracts are digital, executable, self-enforcing descriptions of commitments between parts. They were first envisioned in 1994 by Nick Szabo and recently, blockchain based platforms such as Ethereum, with their very strong guaranties of untampered, deterministic execution, seem to offer an ideal medium for their deployment. Among the main applications of smart contracts are the automatization of interactions such as bets, collaterals, prediction markets, insurances. One of the main issues that arise in extending the domain of smart contracts regards provisioning reliable information on the blockchain (the so called "oracle problem"). In this talk, we will consider the challenges that emerge when using IoT sensors and devices as information providers for smart contracts.

Biography

Dr. Francesco Bruschi was born in Milan on January 12, 1975. In 2000 he obtained his degree in Electronics Engineering at the Politecnico di Milano, with a thesis titled "A functional approach to VLIW testing". In 2001 he obtained a sponsorship from Siemens ICN for his doctoral studies. In 2004 he received his Ph.D. degree from the Politecnico di Milano, with a thesis titled "Methodologies and tools for the design of digital systems with programmable components and hardware/software interaction". Since 2004 he is an assistant professor at the Department of Electronics and Information of the Politecnico di Milano.

Tutorial Speaker I

Alessandro De Piccoli, PhD student, Computer Science Department, Università degli Studi di Milano, Italy

Title: High Speed Cryptography

Abstract

In today's communications, cryptography is increasingly crucial to ensure the confidentiality of the exchange of data, whether they are related to commercial transactions or simply information. Exploiting the recent optimization of the product between polynomials, especially those having binary coefficients, it is possible to improve the implementation of cryptography algorithms. In fact, when implementing a cryptographic algorithm, efficient operations have high relevance both in hardware and software. Since a number of operations can be performed via polynomial multiplication, the arithmetic of polynomials over

finite fields plays a key role in real-life implementations. Through new techniques, we can save time and memory, allowing fast encryption/decryption operations, but also faster cryptanalysis. At the same time, this technique may be used by researchers to prevent attacks such as side-channel, and timing attacks. The aim of this tutorial is to provide an introductory guide to the mathematical aspects of high- speed cryptography techniques for computer science researchers.

Tutorial Speaker II

Dr. Kaushal Shah, Assistant Professor at CGPIT, Uka Tarsadia University, Gujarat, India

Title: Understanding the key pre-distribution aspect of linear wireless sensor network

Abstract

There is a set of applications in wireless sensor networks that forms a particular topology through specific placements of sensor nodes. This set is known as linear infrastructure or one- dimensional network. Applications of such networks are subway tunnel or pipeline monitoring and perimeter surveillance. These applications often demand critical security concerns. Distribution of symmetric keys for such networks is different from those that are planner and are widely studied. By considering requirements for such linear infrastructure in detail, we observe that connectivity is an important issue as capturing a single node disrupts the entire network's services. Therefore, we propose a new measure of connectivity that produces the optimal results with acutely lightweight key pre-distribution schemes (KPS). We also show the theoretical analysis of our proposed scheme and prove how it produces optimal results with lesser storage requirements as compared to other schemes. The performance analysis shows that the proposed KPS requires lesser number of keys per node (O(1) constant storage), as compared to the other existing schemes in the literature to provide the same level of connectivity.

Tutorial Speaker III

Dr. Michela Ceria, Postdoctoral Fellow, Computer Science Department, Università degli Studi di Milano, Italy

Title: Efficient cryptographic algorithms for securing passwords

Abstract

Nowadays, there are several real-life applications that require authentication and so the use of passwords: e-mails, online banking, mobile phones, and so on. A server retaining our passwords must ensure them the highest possible level of security from attacks (e.g. dictionary attacks and brute force attacks), also taking into consideration that the average user is not able to generate a strong password with a suitable number of entropy bits (the average password entropy was estimated at 40.54 bits) and that more than one user likely employ the same password for the same kind of service. This problem can be addressed by means of cpu-and memory-intensive algorithm that slow attackers down. In this talk, we will give an overview of main password hashing algorithms such as Argon2, Catena, Lyra2, Makwa, yescrypt, explaining their main features and instances.

CONTACT US

E-
Mail: widecom2019@easychair.org