Keynote Speakers
TrustCom 2011

Access Control in Distributed Systems:
Merging Theory with Practice

Prof. Ivan Stojmenovic, University of Ottawa, Canada

Ivan Stojmenovic received his Ph.D. degree in mathematics. He held regular and visiting positions in Serbia, Japan, USA, Canada, France, Mexico, Spain, UK (as Chair in Applied Computing at the University of Birmingham), Hong Kong, Brazil, Taiwan, and China, and is Full Professor at the University of Ottawa, Canada and Adjunct Professor at the University of Novi Sad, Serbia. He published over 250 different papers, and edited seven books on wireless, ad hoc, sensor and actuator networks and applied algorithms with Wiley. He is editor of over dozen journals, editor-in-chief of IEEE Transactions on Parallel and Distributed Systems (from January 2010), and founder and editor-in-chief of three journals (MVLSC, IJPEDS and AHSWN). Stojmenovic is one of about 300 computer science researchers with h-index at least 40 and has >10000 citations. He received three best paper awards and the Fast Breaking Paper for October 2003, by Thomson ISI ESI. He is recipient of the Royal Society Research Merit Award, UK. He is elected to IEEE Fellow status (Communications Society, class 2008), and is IEEE CS Distinguished Visitor 2010-12. He received Excellence in Research Award of the University of Ottawa 2009. Stojmenovic chaired and/or organized >60 workshops and conferences, and served in >200 program committees. He was program co-chair at IEEE PIMRC 2008, IEEE AINA-07, IEEE MASS-04&07, EUC-05&08-10, AdHocNow08, IFIP WSAN08, WONS-05, MSN-05&06, ISPA-05&07, founded workshop series at IEEE MASS, ICDCS, DCOSS, WoWMoM, ACM MobiHoc, IEEE/ACM CPSCom, FCST, MSN, and is/was Workshop Chair at IEEE INFOCOM 2011, IEEE MASS-09, ACM MobiHoc-07&08.

Summary
Access control ensures that only authorized users have access to data and services. This problem becomes challenging in distributed systems, where coordination of activities by a central authority might not be possible or could be resource demanding. Attribute Based Encryption (ABE) is a recent cryptographic primitive which is being used for access control. We address some contemporary access control problems in distributed systems such as mobile ad hoc networks, vehicular networks, smart grids and cloud computing. Each of these applications has different constraints and requirements. We show how ABE and different variants of it can be tailored to suit the specific needs of the above applications.
Power Management in Embedded Systems: Clusters of Satellites as a Case Study

Prof. Daniel Mossé, University of Pittsburgh, USA

Daniel Mossé is Professor and Chair of the Computer Science Department at the University of Pittsburgh, USA. The current major thrusts of his research are real-time and embedded systems, power management issues, and networks (wireless and security), bridging the gap between the operating systems and networking research fields. He has published approximately 200 papers worldwide in these topics. Typically funded by NSF and DARPA, his projects combine theoretical results and actual implementations. He received a BS in Mathematics from the University of Brasilia in 1986, and MS and PhD degrees in Computer Science from the University of Maryland in 1990 and 1993, respectively. Dr. Mossé received the Provost's Innovation in Education Grant/Award in 2007 for redesigning the Introductory Programming course for non-majors. He received the Tina and David Bellet Teaching Excellence Award in 2006 (One of two among over 500 faculty members in the School of Arts and Sciences). Dr. Mossé has served on PCs and as PC chair for most major IEEE- and ACM-sponsored real-time conferences. In 2011, he is co-chair of the International Green Computing Conference and General Co-Chair for the International conference on Embedded and Real-Time Computing Systems.

Summary

Embedded systems have gone from being microcontroller-based, small-footprint and single-application systems to modern multi-tasked distributed systems, wirelessely networked, managing multiples devices, and with more resources. Still, many of these systems are deployed in harsh environments and out-of-reach locations, which makes wireless deployment an attractive if not the only option. Therefore, changing batteries would be time and resource consuming. In this talk, we explore techniques for saving power/energy in modern embedded systems, from the perspective of multiple devices in a single embedded platform composed of a cluster of such platforms. As a case study, we use a coalition of small satellites that will be deployed in the near future as part of the F6 DARPA program; as a fractionated spacecraft, satellites coordinate actions in a cluster, but require high levels of power management due to the very nature of the environment where they are deployed. The cluster is heterogeneous and allows for a rich platform for power saving techniques.
Fault Detection in Cloud Computing Systems

Prof. Yi Pan, Georgia State University, USA

Yi Pan is the chair and a professor in the Department of Computer Science and a professor in the Department of Computer Information Systems at Georgia State University. Dr. Pan received his B.Eng. and M.Eng. degrees in computer engineering from Tsinghua University, China, in 1982 and 1984, respectively, and his Ph.D. degree in computer science from the University of Pittsburgh, USA, in 1991. He is also a guest professor of many universities including Tsinghua University and Beijing University. Dr. Pan's research interests include parallel and distributed computing, optical networks, wireless networks, and bioinformatics. Dr. Pan has published more than 100 journal papers with 40 papers published in various IEEE journals. In addition, he has published over 100 papers in refereed conferences (including IPDPS, ICPP, ICDCS, INFOCOM, and GLOBECOM). He has also co-authored/co-edited 34 books (including proceedings) and contributed several book chapters. His pioneer work on computing using reconfigurable optical buses has inspired extensive subsequent work by many researchers, and his research results have been cited by more than 100 researchers worldwide in books, theses, journal and conference papers. He is a co-inventor of three U.S. patents (pending) and 5 provisional patents, and has received many awards from agencies such as NSF, AFOSR, JSPS, IISF and Mellon Foundation. His recent research has been supported by NSF, NIH, NSFC, AFOSR, AFRL, JSPS, IISF and the states of Georgia and Ohio. He has served as a reviewer/panelist for many research foundations/agencies such as the U.S. National Science Foundation, the Natural Sciences and Engineering Research Council of Canada, the Australian Research Council, and the Hong Kong Research Grants Council. Dr. Pan has served as an editor-in-chief or editorial board member for 15 journals including 5 IEEE Transactions and a guest editor for 10 special issues for 9 journals including 2 IEEE Transactions. He has organized several international conferences and workshops and has also served as a program committee member for several major international conferences such as INFOCOM, GLOBECOM, ICC, IPDPS, and ICPP. Dr. Pan has delivered over many keynote speeches at international conferences. Dr. Pan is an IEEE Distinguished Speaker (2000-2002), a Yamacraw Distinguished Speaker (2002), a Shell Oil Colloquium Speaker (2002), and a senior member of IEEE. He is listed in Men of Achievement, Who's Who in Midwest, Who's Who in America, Who's Who in American Education, Who's Who in Computational Science and Engineering, and Who's Who of Asian Americans.

Summary

Cloud computing is an increasingly important solution for providing services deployed in dynamically scalable cloud networks. In cloud-based networks, services may be virtualized with details abstracted and hidden. Here, some servers are active and available, others busy or heavily loaded, and still others offline for various reasons. Therefore, in order to provide an effective control scheme and parameter guidance for service conditions and cloud resources, failure detection is essential to meet user service expectations. Effective failure detection is a fundamental factor in addressing possible performance bottlenecks in providing virtual service. It is imperative to design and implement an acceptable failure detector (FD) for cloud-based networks. Most existing FD schemes used in traditional networks do not automatically adjust their detection service parameters for dynamic network conditions. Given that cloud-based networks are dynamic and unexpected, we explore FD properties with relation to actual and automatic fault-tolerant cloud-based network systems, so as to find a general non-manual analytical method to self-tune corresponding parameters to satisfy various user requirements. Based on this general self-tuning method, we will report a dynamic and automatic Self-tuning Failure Detector schemes and discuss possible improvements over existing FD schemes. In this talk, we will also report experimental results which are carried out to compare Quality of Service (QoS) metrics of several adaptive FDs. We will show that our newly designed FD scheme has good performance and can
automatically adjust corresponding parameters to satisfy different user requirements. Such a self-tuning FD scheme can be significantly beneficial in dynamic cloud-based environments since it does not involve any human intervention and are fully automatic.
Intelligence in Cyber-Physical-Social Spaces

Prof. Zhaohui Wu, Zhejiang University, China

Zhaohui Wu is a Professor of the College of Computer Science and Technology at Zhejiang University, China. He is a Vice-President of Zhejiang University and the Director of the Institute of Computer System and Architecture. He received the Ph.D. degree from Zhejiang University in 1993. From 1991 to 1993, he was with the German Research Center for Artificial Intelligence (DFKI) as a joint Ph.D. student. He was a visiting professor of the University of Arizona. He is a member of the IT Expert Committee for the National 863 program, a senior member of the IEEE, a standing council member of China Computer Federation. His research interests include intelligent system, semantic grid, and ubiquitous embedded systems. Prof. Wu has authored 4 books and more than 100 refereed papers. He is on the editorial boards of several journals, and has served as PC member for various international conferences.

Summary

Physical things and the human society have formed into the world we live in. With the advent of ubiquitous sensing, future social networks are becoming cyber-physical, combining measured elements of the physical world. The convergence of computational and physical processes as well as human's social behaviors exhibits a variety of complicated characteristics, which leads to a lot of challenges. This talk will explore the intelligence issues in Cyber-Physical-Social Systems. Trends and challenges will be reviewed, and potential applications will be discussed. We will also give a brief introduction of our group’s work attempting to address these challenges.
TRUSTIE: Design of a Trustworthy Software Production Environment

Prof. Huaimin Wang, National University of Defense Technology, China

Huaimin Wang received his Ph.D. in computer science from National University of Defense Technology (NUDT). He is a Chang Jiang Scholars Program Professor of Ministry of Education, Distinct Young Scholar of NSFC, assembly member of Department of Information Science of NSFC and Fellow of CCF. As the Vice Dean of School of Computer Science and Technology of NUDT, he has worked as the director of several grand research projects, including “Internet-based Virtual Computing Environment (iVCE)” (funded by 973 Program), “Trustworthy Software Production Tools and Integration Environment” (funded by 863 Program), and “Research on Trustworthy Software Technology” (funded by NSFC). He has published more than 100 research papers on international conferences and journals of related research field and has been awarded National Awards for Science and Technology in 2003. His current research interests include distributed system and middleware, Internet computing, trustworthy computing and software engineering.

Summary

Internet fundamentally changes the model of software development, the demands of software quality, and the process of software resource sharing. Internet-based environment for trustworthy software production is recognized as a key topic of software engineering in both academic and software industry. In this paper, the concepts and models of trustworthy software are introduced which dominate the design of Trustie environment. Trustie provides trustworthy software components sharing by an evolving software repository, and provides collaborative software development in a customizable development platform powered by a software production line framework. Finally the layered practices of research and application based on Trustie preliminarily demonstrate the effectiveness as well as the promising future of this environment.
Summary
This tutorial is organized as follows: First, the Pauli matrices and their properties are introduced. Second, a mathematical definition for the block Jacket matrices is presented. Then, the block Jacket matrices with size 2x2 are investigated. Following resultants of the 2x2 block Jacket matrices, a general approach for any size block Jacket matrix is investigated in detail. Then, several special cases are investigated. After that, we extend the fast construction approach for the block Jacket matrices to higher dimension case. Especially, a brief description on 3-D block Jacket matrices is presented. To decompose high order factorable block Jacket matrices, a fast block inverse Jacket transform is proposed. The proposed decomposition algorithm is very helpful in encoding, sequence signal processing, and information processing. Finally, properties of the block Jacket matrices are discussed.
Defending Against Large-Scale and Coordinated Attacks in the Ubiquitous Environments

Dr. Yang Xiang, Deakin University, Australia

Dr. Yang Xiang is currently with School of Information Technology, Deakin University, Australia. He received his PhD in Computer Science from Deakin University. His research interests include network and system security, distributed systems, and wireless systems. In particular, he is currently leading in a research group developing active defense systems against large-scale distributed network attacks and new Internet security countermeasures. Dr. Xiang has published more than 100 research papers in international journals and conferences, most of them are IEEE/ACM journals/conferences, such as IEEE Transactions on Parallel and Distributed Systems, IEEE Journal on Selected Areas in Communications, and IEEE Transactions on Forensics and Information Security. Dr. Xiang is the co-founder of the International Conference on Network and System Security (NSS). He has served as Program Chair for about 10 international conferences such as ICA3PP 11, IEEE TrustCom 11, IEEE/IFIP EUC 11, IEEE HPCC 10/09, IEEE ICPADS 08, and NSS 10/09/08/07. He has been PC member for about 50 international conferences such as IEEE ICC, IEEE GLOBECOM, SECRIPT, Malware, and IEEE ICPADS. He has served as the guest editor for ACM Transactions on Autonomous and Adaptive Systems, Computer Communications (Elsevier), Future Generation Computer Systems (Elsevier), Journal of Network and Computer Applications (Elsevier), and Concurrency and Computation: Practice and Experience (Wiley). He is on the editorial board of Journal of Network and Computer Applications (Elsevier).

Summary

Ubiquitous computing is an exciting paradigm shift where technology becomes virtually invisible in our lives. Through decades of development, we have seen the tremendous trend of moving desktop or laptop computers to invisible computers that are sensible and networked locally and globally. We are fast moving towards a cyber integrated world with innovative applications of embedded cyber physical objects and systems. In the increasingly interconnected world, threats to our daily lives can come from unexpected sources and universal directions. Criminals and terrorists have recognised the value of leveraging the ubiquitous computing environments to facilitate the commission of crimes. It is revealed that there has been a shift in trend in cybercrime that organised cybercriminal activities are on the rise and with large-scale profit-driven incentives. The cybercriminals typically launch different forms of large-scale and coordinated attacks, causing huge financial loss and potential life hazard. In this talk, we report two innovative approaches to defend against large-scale and coordinated attacks in the ubiquitous environments: 1) Inferring the cybercrime’s intent through network traffic classification to enable the early warning of potential attacks; and 2) Profiling the large-scale and coordinated cyber attacks through both microscopic and macroscopic modelling to provide better control of such attacks. These approaches are effective in finding weak symptoms caused by the attacks thus can successfully defend against the large-scale and coordinated attacks at their early stages.
Quality-of-Service and Traffic Scheduling of Wireless Multimedia Applications

Prof. Geyong Min, University of Bradford, UK

Dr. Geyong Min is a Reader in Computer Networking in the Department of Computing at the University of Bradford, UK. He received the PhD degree in Computing Science from the University of Glasgow, UK, and the BSc degree in Computer Science from Huazhong University of Science and Technology, China. He joined the University of Bradford, UK, as a Lecturer in 2002, was promoted to a Senior Lecturer in 2005 and became a Reader in 2007. His research interests include Next Generation Internet, Wireless Communications, Multimedia Systems, Information Security, Ubiquitous Computing, Modelling and Performance Engineering.

His recent research has been supported by UK EPSRC, Royal Society, Royal Academy of Engineering, and European FP, and industrial partners including Motorola Ltd, Lucent Technologies, IBM, INMARSAT, and InforSense Ltd. He has published over 200 research papers in prestigious international journals, including IEEE Transactions on Communications, IEEE Transactions on Wireless Communications, IEEE Transactions on Computers, IEEE Transactions on Parallel and Distributed Systems, and IEEE Network, and in reputable international conferences, such as ICDCS and IPDPS. He was the recipient of the Best Paper Awards from IEEE AINA’2007, ICAC’2008, IEEE CSE’2009 and TrustCom’2010.

Dr. Min is an Editorial Board member of 9 international journals and serves as the Guest Editor for 18 international journals. He has chaired/co-chaired 30 international conferences /workshops and served as the committee member of 150 professional conferences/workshops. He was awarded the Outstanding Leadership Awards from IEEE International conferences CIT’2010, ScalCom’2010, ICESS’2010, ScalCom’2009, HPCC’2008 and one Outstanding Service Award from ISPA’2006.

Summary

Differentiated Quality-of-Service (QoS) is an important requirement of wireless multimedia networks. The hybrid scheduling mechanism that integrates the fundamental traffic scheduling schemes in a hierarchical manner is a promising strategy for QoS differentiation of multimedia applications. However, the interdependent relationship among multiple traffic flows significantly increases the complexity and poses more challenges for modelling the hybrid scheduling mechanism. Many measurement studies have convincingly demonstrated that the realistic multimedia traffic exhibits noticeable self-similar nature (i.e., scale-invariant burstiness and large-lag correlation).

In this talk, we will report the heterogeneous traffic models for multimedia communication networks, and then present the analytical performance models of the hybrid scheduling schemes in the presence of multi-class self-similar traffic. The accuracy of the analytical models is validated through extensive comparison between the analytical results and those obtained from simulation experiments of the actual system subject to the real-world multimedia applications. To illustrate its applications, the analytical model is adopted as an efficient tool to study the issues of resource management and call admission control in the hybrid scheduling system subject to specific QoS constraints. Finally, we will present the emerging issues and future directions of analytical modelling of multimedia communication networks.
Privacy, Identity and Trust in Context-Aware Mobile Services

Dr. Valtteri Niemi, Nokia Fellow

Valtteri Niemi received a PhD degree in Mathematics from the University of Turku, Finland in 1989. After serving in various positions in Univ of Turku, he was an Associate Professor in Mathematics at the University of Vaasa, Finland, during 1993-97. He joined Nokia Research Center (NRC), Helsinki, Finland, in 1997. He has contributed in several roles for Nokia research in wireless security area, including cryptological aspects. In 2008, he moved to the new NRC laboratory in Lausanne, Switzerland, where his main focus was on privacy-enhancing technologies. He was nominated as a Nokia Fellow in January 2009. Starting from beginning of 2011, Valtteri is leading the Security and Networking Protocols team in the Radio Systems laboratory of NRC (in Helsinki). He participated 3GPP SA3 (security) standardization group from its beginning and during 2003-2009 he was the chairman of the group. Before 3GPP, Dr. Niemi took part in ETSI SMG 10 for GSM security specification work. He has published around 50 scientific articles and he is a co-author of four books and more than 20 patents.

Summary

Mobile services are increasingly utilizing context information, e.g. user location. There is an intriguing interplay between privacy, identity, security and trust in this domain. In the talk, technologies are presented that can help in managing this interplay. Several technologies have also been tested in trials carried out recently by Nokia Research Center in Lausanne, Switzerland. We take a look at some key results obtained from these trials. Examples of used technologies are pseudonym management for location privacy purposes, usage control for protection of privacy-sensitive context data and secure multiparty computations for minimizing the amount of needed information exchange.