TCS Special on Stabilization, Safety and Security

Call for Papers

Journal of Theoretical Computer Science

Special Issue on

Stabilization Safety and Security

Tentative schedule: Submission December 2008, Referee process until April 2009, Final versions August 2009.

Self-Stabilization is the property of a system, component, process or object to right itself no matter how severely its state variables, including memory, message buffers, and registers, are corrupted. Self-stabilization is most interesting for distributed and concurrent systems, because local detection of a faulty condition is problematic.

During previous symposia on the topic (1989, 1995, 1997, 1999, 2001, 2003, 2005, 2006, 2007) influential research has been presented covering such topics as algorithmic techniques, formal methodologies, model theoretic questions, and compositionality.

Beyond the theory, self-stabilization is a guiding principle in many network protocols (in fact, a number of Internet and LAN protocols are self-stabilizing or very nearly so). Recent applied research has succeeded in demonstrated self-stabilizing, hardware, operating systems and file systems and in implementing protocols for routing, reprogramming, and synchronizing nodes in sensor networks. These examples show how the principles of self-stabilization can be used to implement lightweight solutions to the problems of fault tolerance in practical systems.

Recent interest of the field is in the design and development of fault-tolerant distributed systems with self-* properties, such as self-stabilizing, self-configuring, self-organizing, self-managing, self-repairing, self-healing, self-optimizing, self-adaptive, and self-protecting areas of algorithmic techniques, formal methodologies, model theoretic issues, and composition techniques. All these areas are essential to the understanding and maintenance of self-* properties in fault-tolerant distributed systems. Research in distributed systems is now at a crucial point in its evolution, marked by the importance of dynamic systems such as peer-to-peer networks, large-scale wireless sensor networks, mobile ad hoc networks, robotic networks, etc. Moreover, new applications such as grid and web services, banking and e-commerce, e-health and robotics, aerospace and avionics, automotive, industrial process control, etc. have joined the traditional applications of distributed systems.

Now, more than ever, the theory of self-stabilization has tremendous impact in these areas. Last two years, the scope of the symposium was expanded to cover all safety and security related aspects of self-* systems. The symposium solicits contributions on all these aspects from theoretical contributions, to reports of the actual experience of applying the principles of self-stabilization to static and dynamic systems. Topics of interest include, but are not limited to:

Stabilization

- self-stabilizing systems
- self-managed, self-assembling, autonomic and adaptive systems
- self-optimizing and self-protecting systems
- self-* abstractions for implementing fundamental services in static and dynamic distributed systems
- impossibility results and lower bounds for self-* systems
- application of stabilizing algorithms and techniques in dynamic distributed systems
- data and code stabilization
- algorithms for self-* error detection/correction
- models of fault-tolerant communication
- stochastic, physical, and biological models to analyze self-* properties

Safety

- safety critical systems
- trust models and specifications
- semantics of trust, distrust, mistrust, over-trust, cheat, risk and reputation
- trust-related security and privacy
- reliable and dependable systems
- fault-tolerant algorithms and systems, hardware redundancy, robustness, survivable systems, failure recovery
- program maintenance for safety preservation
- peer-to-peer networks, sensor networks, MANETs, and wireless mesh networks
- self-* properties and their relation with classical fault-tolerance
- safety of election systems

Security

- security of network protocols
- security of sensor and mobile networks protocols
- secure architectures, frameworks, policy, intrusion detection/awareness
- proactive security
- security protocols for self-* systems
- peer-to-peer networks, sensor networks, MANETs, and wireless mesh networks
- security of election systems

Guest Editors:

Shlomi Dolev, Ben-Gurion University, dolev@cs.bgu.ac.il

Sandeep Kulkarni, Michigan State University, sandeep@cse.msu.edu

Andre Schiper, Ecole Polytechnique Federale Lausane, andre.schiper@epfl.ch