Workshop Co-Chairs

Mohamed Eltoweissy
Virginia Tech, USA

Mohamed Younis
University of Maryland
Baltimore County, USA

Publicity Co-Chairs

Denis Gračanin
Virginia Tech, USA

Ahmed Safwat
Queen's University, Canada

Program Committee

First IEEE Workshop on Information Assurance in Wireless Sensor Networks (WSNIA 2005)

`http://www.csee.umbc.edu/~younis/WSNIA2005.htm`

In conjunction with

24th IEEE International Performance Computing and Communications Conference (IPCCC 2005)

`http://ipccc.org/`

April 7-9, 2005 — Phoenix, Arizona

Recently, there has been a growing interest in the potential use of wireless sensor networks (WSNs) in applications such as smart environments, disaster management, combat field reconnaissance, and security surveillance. While the initial view of the community was that WSNs will play a complementary role that enhances the quality of these applications, recent research results have encouraged practitioners to envision an increased reliance on WSNs in such critical and sensitive applications. Therefore, to realize their potential, necessary information assurance (IA) measures have to be incorporated in the design and during the operation of WSNs. IA is usually specified using attributes like integrity, authenticity, confidentiality, availability, and survivability. A defense-in-depth approach to IA involves the activities of attack and failure prevention, detection and response, as well as the refinement of these activities. The scope of defense-in-depth may start with a diameter that spans the deployed sensors to a diameter that includes the command nodes and likely beyond. It also involves assurance at, and cross-cutting, the protocol stack layers, from physical to application.

Achieving information assurance in WSNs will require non-conventional mechanisms due to many factors including: (1) sensors are significantly constrained in the amount of available resources such as energy, storage and computation; (2) sensors are expected to be deployed in very large numbers in normal as well as forbidding environments; (3) WSNs suffer from structural weakness and limited physical protection, and (4) localization of impact is complicated due to the un-tethered nature of the WSN and of the potential attackers. In addition, IA requirements may vary according to a WSN's mission defined over a multi-dimensional context, such as field of deployment (e.g., hostile versus friendly), type of application (e.g., monitoring, tracking, data collection), mode of operation (e.g., normal, exception, post-event recovery), and time.

This workshop will foster a forum for discussing and presenting recent research results on IA in WSNs. Best papers will be invited to a Special Issue of the Journal of Computer Security (`http://www.csl.sri.com/programs/security/jcs/`). Topics of interest include, although not limited to, the following:

- Fault and intrusion-tolerant architectural and operational models
- Robust routing, storage, and processing of sensed data
- Predictable MAC medium access arbitration
- IA architectures and protocols
- Vulnerabilities, attacks and countermeasures
- Monitoring and evaluation techniques
- Scalability and robust clustering techniques
- Resilient virtual infrastructures
- Autonomic IA in WSNs
- Formal representation and verification of assurance properties
- Adaptive security and assurance techniques
- Quality of service provisioning
- Metrics for measuring security, assurance and dependability
- Privacy-aware dependable operation
- Simulation and visualization environments
- Agent-based management for multi-tier WSNs
- WSNs as components of larger information grids

Prospective authors should submit their paper electronically to `toweissy@vt.edu` or `younis@csee.umbc.edu`. Papers should contain original material and not be previously published, or currently submitted for consideration elsewhere. The manuscript should not exceed 20 single-column double-space pages in MS-Word, PS or PDF font size 11 or larger. The first page should include title, authors' contact information, an abstract and five keywords. Authors should attach the abstract to their message.

Submission deadline: December 10, 2004
Decision notification: December 23, 2004
Final manuscript due: January 15, 2005