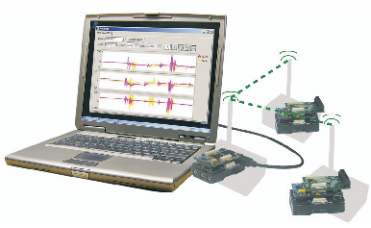
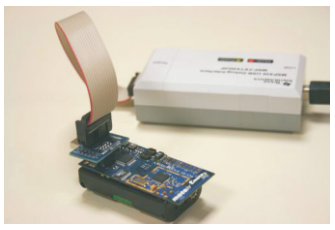
& Algorithms & Security

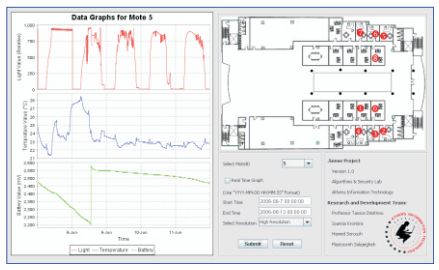
Security in Sensor Networks

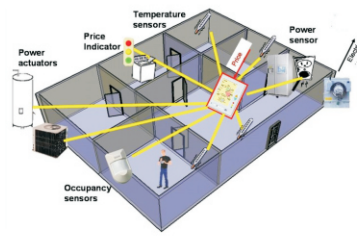




- Real time Intrusion Detection and Recovery
- Secure code dissemination for network reprogramming
- Runtime composition of middleware security services
- Security of high level protocols and services

Sensor Networks Applications





- Energy efficiency aspects in buildings
- Personalized monitoring in healthcare systems
- Ecosystem monitoring, forest fire detection and control
- Intelligent vehicles and traffic management
- Monitoring and management of ecosystems

Security in Ad-Hoc Networks

- Efficient authentication and key agreement
- Detection protocols for compromised nodes
- Intrusion detection based on neural networks and linear threshold schemes
- Intrusion response based on watermarking techniques and binary trees

“ The primary objective of the group is to bring together expertise in education, research and practice in the field of information security and algorithms. Our group members conduct research in areas spanning from the theoretical foundations of cryptography to the design and implementation of leading edge efficient and secure communication protocols. ”

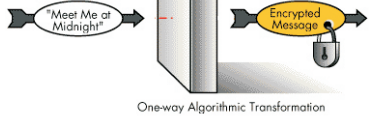
Security in Telecommunication Networks

- Security enhancements to GSM A5/I encryption
- Adaptive authentication mechanisms
- Secure mobile multimedia applications

Smart Cards and RFID Security

- Smart Identity Cards
- Key Escrow Systems
- Smart Cards for multimedia transmission
- Secure biometric template storage
- RFID protocols for user privacy and anonymity

Applied Cryptography and Computer Security



- Private and public key encryption systems
- Provable security
- Efficiency aspects of encryption systems
- Robust and light-weight cryptographic algorithms and primitives

“ The long term goal of the research activity on cryptography and security is to raise awareness of cybersecurity threats, promote safe and responsible online behavior, and help protect the national information infrastructure and individual firms (banks, organizations, etc.). To this end we cooperate closely with various Academic Institutions and the Cyber Security Lab (CyLab) of Carnegie Mellon University. ”

Contact:

Prof. Tassos Dimitriou,
Head, Algorithms & Security
Athens Information Technology,
E-mail: tdim@ait.edu.gr
Tel: +30 210 6682700, Fax: +30 210 6682703
Web: http://www.ait.edu.gr/ait_web_site/faculty/tdim/dimitriou.html

ATHENS INFORMATION TECHNOLOGY
CENTER OF EXCELLENCE FOR RESEARCH AND GRADUATE EDUCATION

TOWARDS A MORE SECURE WORLD

Our security-related efforts aim towards:

- Designing secure applications for networking and electronic commerce that can be proved secure against adversaries of various capabilities.
- Consulting and educating users, firms, etc., because security is as strong as its weakest link and the tools used to enforce security are never the weakest link.
- Accounting for new attacks through research because today’s threat environment should not be the basis for planning. Planning must look 2-5 years in the future because threats are likely to be much worse and will certainly increase in frequency.