

Sherif Khattab {*s.khattab@fci-cu.edu.eg*}

CONTACT INFORMATION

489 Horeya Street
Apt 5
Bolkley
Alexandria, Egypt

Home: (+20) 35825837
Cell (+20) 191614051
E-mail: s.khattab@fci-cu.edu.eg
WWW: www.fci-cu.edu.eg/~skhattab

TEACHING EXPERIENCE

Assistant Professor, Faculty of Computers and Information, Cairo University, August 2008-
Today

- CS495 - Undergraduate Network Security (<http://www.fci-cu.edu.eg/~skhattab/netsec/cs496>).
- CS112 - Programming-1 (Co-instructor)
- CS517 - Design and Analysis of Algorithms (Graduate).
- CS595 - Graduate Network security (<http://www.fci-cu.edu.eg/~skhattab/netsec/cs595>).

Open Education Center, Cairo University, April 2009 - Today

- 402 - Introduction to Natural Language Processing

ECCouncil University (<http://www.eccuni.us>), June 2009 - Today

- ECU521 - Ethical Hacking and Countermeasures

University of Pittsburgh, Fall 2001

- CS1541 - Computer Architecture (TA)

RESEARCH INTERESTS

- Network security.
- Fault tolerant network protocols.
- Wireless sensor networks.
- Delay-tolerant networks.
- Operating systems.
- Distributed systems.

EDUCATION

University of Pittsburgh, Pittsburgh, Pennsylvania USA

Ph.D. in Computer Science, August 2008
M.Sc. in Computer Science, April 2004

- Advisors: Rami Melhem and Daniel Mossé
- GPA 3.98

Cairo University, Giza, Egypt

B.Sc., Computer Engineering, July 1998

- GPA 3.83

PUBLICATIONS

- Sameh Gobriel, Sherif Khattab, Daniel Mossé, and Rami Melhem, **On Link-Quality Estimation and Fault-tolerant Aggregation in Wireless Sensor Networks**, in *GlobeCom* 2009.
- Sherif Khattab, Daniel Mossé, and Rami Melhem, **Jamming Mitigation in Multi-Radio Networks: Reactive Proactive?**, in *SecureComm* 2008.
- Sameh Gobriel, Sherif Khattab, Daniel Mossé, and Rami Melhem, **GroupBeat: Wireless Sensor Networks Made Reliable**, in *IEEE MASS* 2008 (short paper).
- Sherif Khattab, Daniel Mossé, and Rami Melhem, **Modeling of the Channel-Hopping Anti-Jamming Defense in Multi-Radio Wireless Networks**, in *MOBIQUITOUS* 2008 (*acceptance rate 17%*).

- Sherif Khattab, Sameh Gobriel, Rami Melhem, and Daniel Mossé, **Live Baiting for Service-level DoS Attackers**, in IEEE INFOCOM 2008.
- Sherif Khattab, Rami Melhem, Daniel Mossé, and Taieb Znati, **Honeypot Back-propagation for Mitigating Spoofing Distributed Denial-of-Service Attacks**, in Journal of Parallel and Distributed Computing (JPDC) Special Issue on Security in Grid and Distributed Systems, Vol 66(9), p1152-1164, September 2006, Elsevier. (Extended version of SSN'06 paper).
- Sameh Gobriel, Sherif Khattab, Daniel Mossé, José Brustoloni, and Rami Melhem, **RideSharing: Fault Tolerant Aggregation in Sensor Networks Using Corrective Actions**, in *Proceedings of the Third Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON'06)*.
- José Brustoloni, Sherif Khattab, Christopher Santamaria, Brian Smyth, and Daniel Mossé, **Integrated Scheduling of Application- and Network-Layer Tasks in Delay-Tolerant MANETs**, in *Proceedings of the 49th Annual IEEE GLOBECOM conference (GLOBECOM'06)*.
- Sherif Khattab, Rami Melhem, Daniel Mossé, and Taieb Znati, **Honeypot Back-propagation for Mitigating Spoofing Distributed Denial-of-Service Attacks**, in *Proceedings of the 2nd International Workshop on Security in Systems and Networks (SSN'06) in conjunction with IPDPS 2006*, April 2006, **Best Paper Award**.
- Sherif Khattab, Daniel Mossé and Rami Melhem, **Honeybees: Combining Replication and Evasion for Mitigating Base-station Jamming in Sensor Networks**, in *Proceedings of the 14th International Workshop on Parallel and Distributed Real-Time Systems (WPDRTS'06) in conjunction with IPDPS 2006*, April 2006.
- C. Sangpachatanaruk, S. M. Khattab, T. Znati, R. Melhem, and D. Mossé, **Design and Analysis of a Replicated Elusive Server Scheme for Mitigating Denial of Service Attacks**, in *Journal of Systems and Software, Vol 73(1), p15-29*, September 2004, Elsevier.
- Sherif M. Khattab, Chatree Sangpachatanaruk, Daniel Mossé, Rami Melhem, and Taieb Znati, **Roaming Honeypots for Mitigating Service-level Denial-of-Service Attacks**, in *Proceedings of the 24th International Conference on Distributed Computing Systems (ICDCS'04)*, March 2004.
- Sherif M. Khattab, Chatree Sangpachatanaruk, Rami Melhem, Daniel Mossé, and Taieb Znati, **Proactive Server Roaming for Mitigating Denial-of-Service Attacks**, *Proceedings of the International Conference on Information Technology: Research and Education (ITRE'03)*, August 2003.
- C. Sangpachatanaruk, S. M. Khattab, T. Znati, R. Melhem, and D. Mossé, **A Simulation Study of the Proactive Server Roaming for Mitigating Denial of Service Attacks**, in *Proceedings of the 36th Annual Simulation Symposium 2003 (ANSS'03)*, March 2003.

SELECTED
PROJECTS

Security Joint work with my advisors and the NetSec (www.cs.pitt.edu/netsec) and S-CITI (www.cs.pitt.edu/s-citi) group members

- Designed and analyzed the **live baiting** algorithm for detecting Distributed Denial-of-Service Attackers using group testing theory. A preliminary version of the algorithm has been implemented in C.
- Designed and implemented in C the **server roaming** scheme for defending against Denial-of-Service (DoS) attacks. The scheme aims at dodging attacks by continuously changing the service location in a way agreed upon with legitimate clients yet unpredictable to attackers. The scheme has been evaluated in the ns-2 network simulator and I tested a prototype in a FreeBSD network. I also designed and implemented a reactive flavor of the scheme, whereby

the protected service escapes from attacked servers *after* an attack is detected.

- Designed and evaluated the **roaming honeypots** scheme for defense against denial-of-service (DoS) attacks. The scheme works by camouflaging traps for attackers within a server pool. At any point of time, a subset of the servers are authentically providing the service, while the rest are acting as traps or honeypots, in the sense that any request they receive is from an attacker and is used to blacklist the attacker's IP address. Legitimate clients are always made aware of the authentic servers so that they forward no request to the honeypots. The scheme was evaluated using the ns-2 network simulator.
- Designed and evaluated the **honeypot back-propagation** scheme to trace attack packets back to their true sources in the case that IP addresses are spoofed (forged). Attack packets are identified using the roaming honeypots scheme, that is, packets received by camouflaged honeypots are used for the traceback process. I have analyzed honeypot back-propagation mathematically and evaluated its performance using the ns-2 network simulator.
- Designed and evaluated the **honeybees** scheme to defend against radio jamming in wireless sensor networks. The scheme is designed to protect mobile base-stations from jammers by a careful combination of redundancy and evasion with the purpose of outlasting energy-constrained attackers. I evaluated the scheme using a custom-made simulator in C.
- Ported a threshold-signature Scheme from Java into C++ using the OpenSSL crypto library. (*Operating Systems class project*)
- Designed and developed the **AODV watch-dog** mechanism for mitigating the blackhole problem in wireless ad-hoc networks. The blackhole is a malicious network node that attracts traffic to pass through it, but instead of forwarding the traffic to its ultimate destination, the blackhole drops it. This work aimed at showing that a hop-by-hop routing protocol, such as AODV, is more suitable for defending against the blackhole attack than source-routing protocols, such as DSR. To this end, I designed the watch-dog mechanism, whereby legitimate nodes identify blackholes within their neighborhoods by overhearing packet forwarding (or lack thereof) events. I have evaluated the scheme in the ns-2 network simulator. (*Advanced Networks class project*)

Networks

- Designed and evaluated the **Ridesharing** scheme for fault-tolerant aggregation in wireless sensor networks. The scheme makes use of the inherent redundancy in wireless broadcast so that if a message was lost because of a communication error, sensors, which overheard the message, other than the primary recipient correct the error. The scheme was evaluated in CSIM simulator. (*Joint project with my advisors and Sameh Gabriel*)
- Conducted a simulation analysis of the *DiffServ* QoS framework in the ns-2 network simulator.
- Evaluated the *RSVP* reservation protocol using CISCO routers and the MGEN traffic generation software. (*Class project with Mansour Sharha*)
- Designed and evaluated a battery-aware replica selection algorithm in Ad-hoc networks. Evaluation was in the GlomoSim network simulator. (*Class project with Paul Brennfleck and Patrick Herron*)

Systems (Software and Hardware)

- Designed and implemented a hardware encryption/decryption circuit using the Multisim electronic-circuit simulator and a secure chat program in C.
- Developed a cycle-accurate processor simulator of an out-of-order superscalar processor with branch prediction and dynamic scheduling in C++.
- Designed and implemented a prototype of an *InternetTV* using VHDL Hardware Description Language and 8031-based system (*B.Sc. graduation project with Mahmoud Radwan and Mohammad Shahin*).

- Designed and implemented an *infrared* Wireless Communicator using an Infrared TX/RX circuit connected to serial-port interface. (*Class project with Mahmoud Radwan and Mohammad Shahin*).
- Developed a *compiler* for the Cool programming language in Java (Class project).

PROFESSIONAL
EXPERIENCE

Bosch Research and Technology Center, Pittsburgh, PA (Summer 2008), Software Engineering Intern.

- Co-developed a mode extraction tool to enhance component specification within the Software Component Technology. The tool parses engine control unit's code, extracts modes, and writes new XML specification.

Google Inc., Mountain View, CA (Summer 2007), Software Engineering Intern.

- Developed an integrated, customizable, web-based dashboard for performance monitoring of different Google applications.
- Designed a back-end MySQL database for the dashboard.

Ericsson Data Networks, Pittsburgh, PA (Summer 2006), Software Engineering Intern.

- Installed and managed HP OpenView and ServiceOn Data network-management software in an ATM network.
- Worked with the Eclipse software development environment and the P4 version control software.
- Setup a student-learning lab composed of terminal servers, edge and core network switches, and Solaris and Windows XP hosts.
- Developed dynamic web pages using Ruby and MySQL.

SamaSoft, Cairo, Egypt (1998-2001)

- Performed requirements Analysis, design, and system integration of a highway toll-gate control system.
- Developed multimedia tutoring applications in Delphi.

Giza Systems Engineering, Giza, Egypt (Summer 1997)

- Participated in operation and maintenance of a distributed information system developed for the U-17 FIFA World Championship.

COMPUTER SKILLS

- C, C++, Java, Delphi, Assembly Language (80x86), Oracle PL/SQL, PHP/MySQL, UNIX shell scripting; Unix/Linux, Windows.
- Network simulators: NS2, GlomoSim, and CSIM.

AWARDS

- Andrew Mellon Predoctoral Fellowship (2006-2007).
- USENIX Student Stipend Award to attend NSDI'05.

ACADEMIC
EXPERIENCE

University of Pittsburgh, Pittsburgh, Pennsylvania USA

Graduate Research Assistant

Summer 2002 - Spring 2006

Includes current Ph.D. research and Ph.D. level coursework.

Software TA

Spring 2002

Helping with the department's technical staff.

Teaching Assistant

Fall 2001

Computer Architecture.

Cairo University, Faculty of Computers and Informatics, Giza, Egypt

Assistant Professor
Teaching Assistant

09/2008 - now
1998 - 2001

- Taught courses: Data Structures, File Structures, Computer Networks, Operating Systems, Computer Architecture, Digital Design, C/C++, Software Engineering, Database Concepts, and Distributed Databases.
- Installed and supervised student laboratories for Oracle Designer, Oracle Developer, Power Designer, Linux networking and inter-process communication mechanisms, and CORBA.
- External Reviewer for IEEE Transactions on Wireless Communications, IEEE/ACM Transactions on Networking, Journal of Parallel and Distributed Computing, WCNC'02, DSN'04, ECRTS'04, MOBIQUITOUS'05, UbiCare'06, DASC'06, ICENCO'06, MOBIQUITOUS'07, RTSS'07, OPODIS'07, AICCSA'08, and RTAS'08.

ACADEMIC
ACTIVITIES

REFERENCES

Rami Melhem

Professor
Dept. Computer Science
6137 Sennott Square
University of Pittsburgh
Phone: 412-624-8493
Fax: 412-624-8854
melhem@cs.pitt.edu

Daniel Mossé

Professor
Dept. Computer Science
6423 Sennott Square
University of Pittsburgh
Phone: 412-624-8923
Fax: 412-624-8854
mosse@cs.pitt.edu

Taieb Znati

Professor
Dept. Computer Science
6415 Sennott Square
University of Pittsburgh
Phone: 412-624-8417
Fax: 412-624-8854
znati@cs.pitt.edu

Prashant Krishnamurthy

Associate Professor
School of Information Sciences
718 SIS Building
University of Pittsburgh
Phone: 412-624-5144
Fax: 412-624-2788
prashant@mail.sis.pitt.edu