



Achievements on ICTRDF Projects

Syed Ali Khayam

Assistant Professor

Wireless and Secure Networks Research (**WiSNet**) Lab
School of Electrical Engineering & Computer Science
National University of Sciences & Technology (NUST), Pakistan

About the speaker

- PhD (Electrical Engineering): Michigan State University (MSU), December 2006
- Assistant Professor: School of Electrical Engineering & Computer Science (SEECS), National University of Sciences & Technology (NUST), Pakistan
- Founding Director: Wireless and Secure Networks (WiSNet) Research Lab
- CEO and Co-Founder: Baltoros Limited

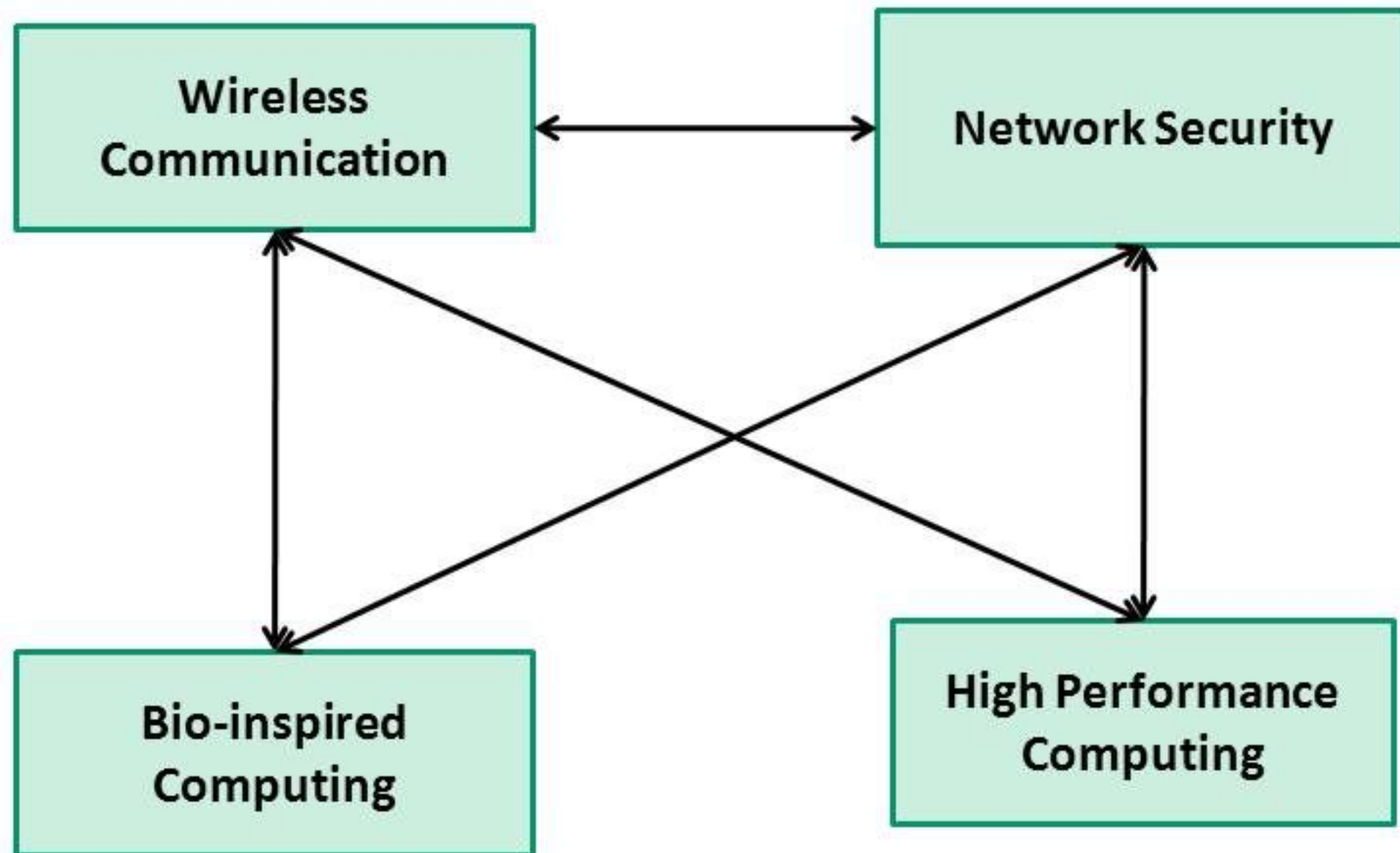


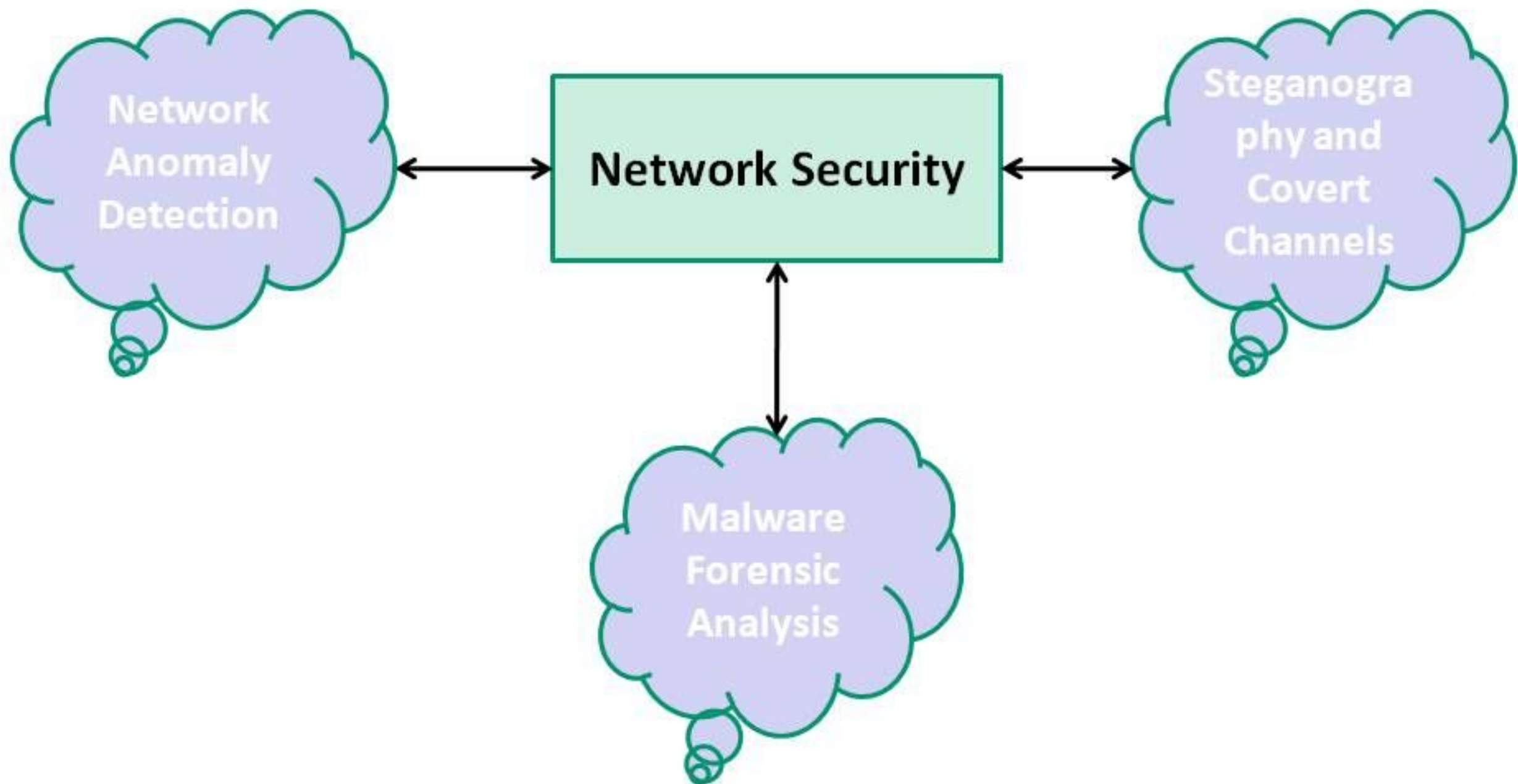
Wireless and Secure Networks Research Lab

<http://wisnet.seecs.nust.edu.pk>



About WiSNet: Focal Research Areas





Design and Development of an Open Source Network Security Solution

Co-PI: Mr. Ali Sajjad



Network-Embedded Security using In-Network Packet Marking

Co-PI: Dr. Fauzan Mirza



An Intelligent Secure Kernel for Mobile Devices

PI: Dr. Mudassar Farooq/FAST-NU



ICTRDF Funded Projects: Selected Publications



ICTRDF Funded Projects: Selected Publications

ICC 2008
INTERNATIONAL CONFERENCE ON COMMUNICATIONS

Welcome Message Committees Information for Authors/Speakers Conference Program Registrations Hotel General Information

19-23 MAY 2008
ICC 2008, BEIJING, CHINA

ICC 2008 in BEIJING
International Conference on Communications

IEEE ICC 2007 ~ 24 - 28 June 2007 ~ Glasgow

smart communications technologies for tomorrow

2008 **EVO***
www.evostar.org

Largest Conference in the Field of Genetic and Evolutionary Computation

GECCO Genetic and Evolutionary Computation Conference

2008

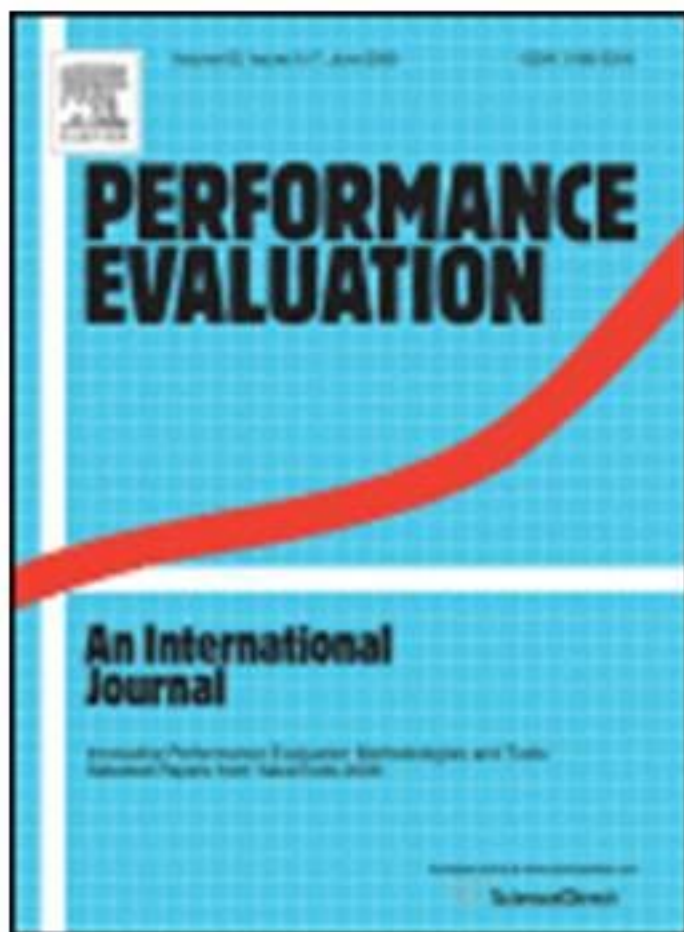
Saturday - Wednesday
July 12 - 16, 2008
Atlanta, Georgia, USA

GECCO = RWA + GA + GP + EMO + ACO + AL + EDA + GBML + GDS + ES + ...

acm

www.sigevo.org

ICTRDF Funded Projects: Selected Publications



ICTRDF Funded Projects: Students at ACM CCS 2009



Patents Filed on ICTRDF Projects



PATENTS FILED IN IPO PAKISTAN



PATENT 1 [A METHOD FOR EMBEDDED MALWARE DETECTION]

APPLICATION NO.: 210/2008 FILING DATE: 09-07-2008

APPLICANTS: NATIONAL UNIVERSITY OF SCIENCES AND TECHNOLOGY
SCHOOL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE
(NUST-SECS)
FOUNDATION FOR ADVANCEMENT OF SCIENCES AND TECHNOLOGY
(FAST /NU)
PAKISTAN NATIONAL ICT R&D FUND

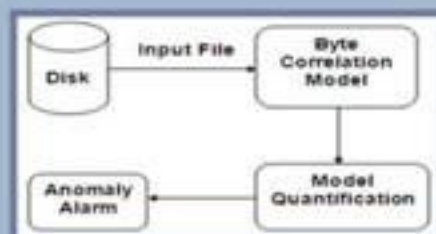
INVENTORS: M. ZUBAIR SHAFIQ
DR. MUDASSAR FAROOQ
DR. SYED ALI KHAYAM

PRIORITY DATA: 09-07-2008

TITLE: A METHOD FOR EMBEDDED MALWARE DETECTION

ABSTRACT: A METHOD FOR DETECTION OF EMBEDDED MALWARE IS FORMULATED BY ANALYZING THE CORRELATION OBSERVED IN A BENIGN FILE'S DATA. THIS CORRELATION STRUCTURE IS STATISTICALLY MODELED USING MARKOV CHAINS. FOR DETECTION OF EMBEDDED MALWARE, THE MODEL IS QUANTIFIED USING AN INFORMATION THEORETIC MEASURE AND A CLASSIFICATION THRESHOLD IS DETERMINED. UNKNOWN FILES ARE THEN CLASSIFIED USING THE CLASSIFICATION THRESHOLD.

FIGURE:



PATENT 2 [DETECTION OF TRAFFIC ANOMALIES IN A COMPUTER NETWORK]

APPLICATION NO.: 239/2008 FILING DATE: 15-07-2008

APPLICANTS: NATIONAL UNIVERSITY OF SCIENCES AND TECHNOLOGY
SCHOOL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE
(NUST-SECS)
FOUNDATION FOR ADVANCEMENT OF SCIENCES AND TECHNOLOGY
(FAST /NU)
PAKISTAN NATIONAL ICT R&D FUND

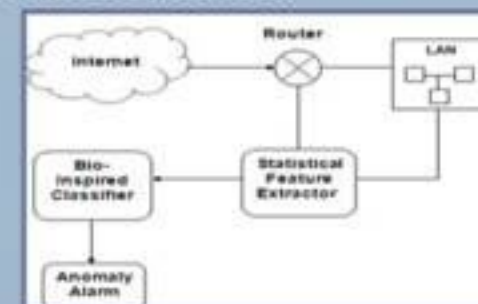
INVENTORS: M. ZUBAIR SHAFIQ
DR. MUDASSAR FAROOQ
DR. SYED ALI KHAYAM

PRIORITY DATA: 15-07-2008

TITLE: DETECTION OF TRAFFIC ANOMALIES IN A COMPUTER NETWORK

ABSTRACT: THE PRESENT INVENTION PRESENTS A SET OF INTELLIGENT STATISTICAL FEATURES WHICH CAN IMPROVE THE CLASSIFICATION ACCURACY OF A BIO-INSPIRED CLASSIFIER OPERATING ON THESE INTELLIGENT FEATURES. THE FEATURE SET ACTS AS AN INPUT TO THE BIO-INSPIRED CLASSIFIER.

FIGURE:



A total of 4 patents have been filed; 3 with IPO-Pakistan and 1 with USPTO

Achievements on ICTRDF Projects

- 4 patents filed
- 2 journal publications in 2009
- 12 conference publications in last 3 years
- Established a patent drafting cell at NUST-SEECS
- HR Development
 - 15 graduate students are supported as RAs on ICTRDF projects
 - 3 MS theses completed under ICTRDF projects; 3 more theses underway
 - 5 FYPs completed under the project; 1 FYP underway

Achievements on ICTRDF Projects

- Best Final Year Projects (FYPs) three years in a row
- First ever paper from South Asia in RAID
- First ever paper from Pakistan in ACM CCS
- First ever papers from Pakistan in the Springer Journal in Computer Virology
- Won student travel grants for RAID 2008, RAID 2009, RAID 2010
- Won the prestigious ACM Human Competitive Award 2009 (in collaboration with a FAST/NU) team

Achievements on ICTRDF Projects

- Every single student from WiSNet who wanted to pursue higher education has gotten a fully funded PhD position abroad
- WiSNet students are getting industry salaries that they ask for, not what is being offered to them

Thank you!

- Contact Information:
 - Email: ali.khayam@seecs.nust.edu.pk
 - Web: <http://wisnet.seecs.nust.edu.pk>

Full List of Publications from ICTRDF Projects in 2009

- Hassan Khan, Fauzan Mirza, Syed Ali Khayam, "Determining Malicious Executable Distinguishing Attributes and Low-Complexity Detection," accepted to *Springer Journal in Computer Virology*, October 2009.
- Ayesha Binte Ashfaq, Muhammad Qasim Ali and Syed Ali Khayam, "[Accuracy Improving Guidelines for Network Anomaly Detection Systems](#)," *Springer Journal in Computer Virology*, July 2009.
- Syed Ali Khayam and Hayder Radha, "[Comparison of Conventional and Cross-Layer Multimedia Transport Schemes for Wireless Networks](#)," *Springer Journal on Wireless Personal Communications (WPC)*, July 2009.
- Hassan Khan, Mobin Javed, Fauzan Mirza and Syed Ali Khayam, "[Evading Disk Investigation and Forensics using a Cluster-Based Covert Channel](#)," *ACM Conference on Computer and Communication Security (CCS)*, 2009.
- Muhammad Qasim Ali, Hassan Khan, Ali Sajjad, and Syed Ali Khayam, "[On Achieving Good Operating Points on an ROC Plane using Stochastic Anomaly Score Prediction](#)," *ACM Conference on Computer and Communication Security (CCS)*, 2009.
- Mobin Javed, Ayesha Binte Ashfaq, M. Zubair Shafiq, and Syed Ali Khayam, "[On the Inefficient Use of Entropy for Anomaly Detection](#)," *Recent Advances in Intrusion Detection (RAID)*, September 2009.
- Saira Zahid, Muhammad Shahzad, Syed Ali Khayam, and Muddassar Faroo, "[Keystroke-based User Identification on Smart Phones](#)," *Recent Advances in Intrusion Detection (RAID)*, September 2009.
- Hassan Khan, Yousra Javed, Syed Ali Khayam, and Fauzan Mirza "[Embedding a Covert Channel in Active Network Connections](#)," *IEEE Global Communications Conference (GlobeCom)*, December 2009.

Full List of Publications from ICTRDF Projects in 2009

- Ayesha Binte Ashfaq, Maria Joseph Robert, Asma Mumtaz, Muhammad Qasim Ali, Ali Sajjad, and Syed Ali Khayam, "[A Comparative Analysis of Anomaly Detectors under Portscan Attacks](#)," *Recent Advances in Intrusion Detection (RAID)*, September 2008.
- M. Zubair Shafiq, Syed Ali Khayam, and Mudassar Farooq, "[Embedded Malware Detection using Markov n-grams](#)," *Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, July 2008.
- M. Zubair Shafiq, Syed Ali Khayam, and Mudassar Farooq, "[Improving Accuracy of Immune-Inspired Malware Detectors using Intelligent Features](#)," *ACM Genetic and Evolutionary Computing Conference (GECCO)*, July 2008.
- Sohraab Soltani, Syed Ali Khayam, and Hayder Radha, "[Detecting Malware Outbreaks using a Statistical Model of Blackhole Traffic](#)," *IEEE International Conference on Communications (ICC)*, May 2008.
- Syed Ali Khayam, Hayder Radha, and Dmitri Loguinov, "[Worm Detection at Network Endpoints using Information-Theoretic Traffic Perturbations](#)," *IEEE International Conference on Communications (ICC)*, May 2008.
- M. Zubair Shafiq, Mudassar Farooq, and Syed Ali Khayam, "[A Comparative Study of Fuzzy Inference Systems, Neural Networks and Adaptive Neuro Fuzzy Inference Systems for Portscan Detection](#)," *European Workshop on the Application of Nature-inspired Techniques to Telecommunication Networks and other Connected Systems (EvoCOMNET)*, March 2008. (Best paper nomination)