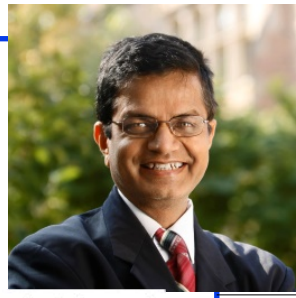
Our Research on New AI and Blockchain Techniques for Network Security



Scan this to download slides

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@wustl.edu

A talk in "CSE 591: Introduction to Graduate Studies in CSE"
October 2, 2020

These slides and a video recording of this talk are at:
http://www.cse.wustl.edu/~jain/talks/cs59120.htm

Overview

1. Why networking is important
2. Recent trends and issues in networking
3. Our Research and its Distinctions
4. Required qualifications

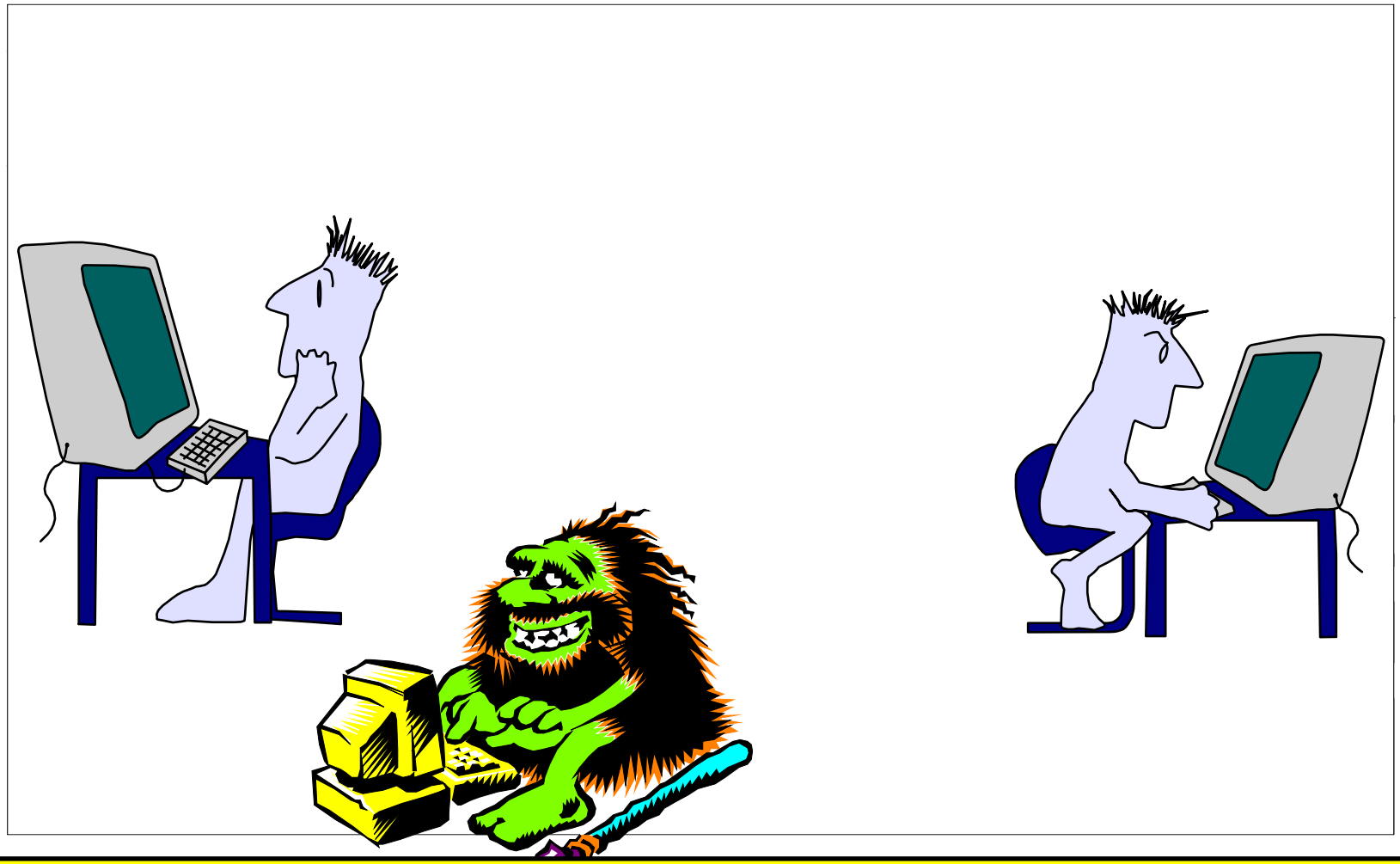
Networking is Fueling All Sectors of Economy

- Networking companies are among the most valued companies: Apple, AT&T, Samsung, Verizon, Microsoft, China Mobile, Alphabet, Comcast, NTT, IBM, Intel, Cisco, Amazon, Facebook, …

  ⇒ All tech companies that are hiring currently are networking companies
- Note: Apple became highly valued only after it switched from computing to communications (iPhone)

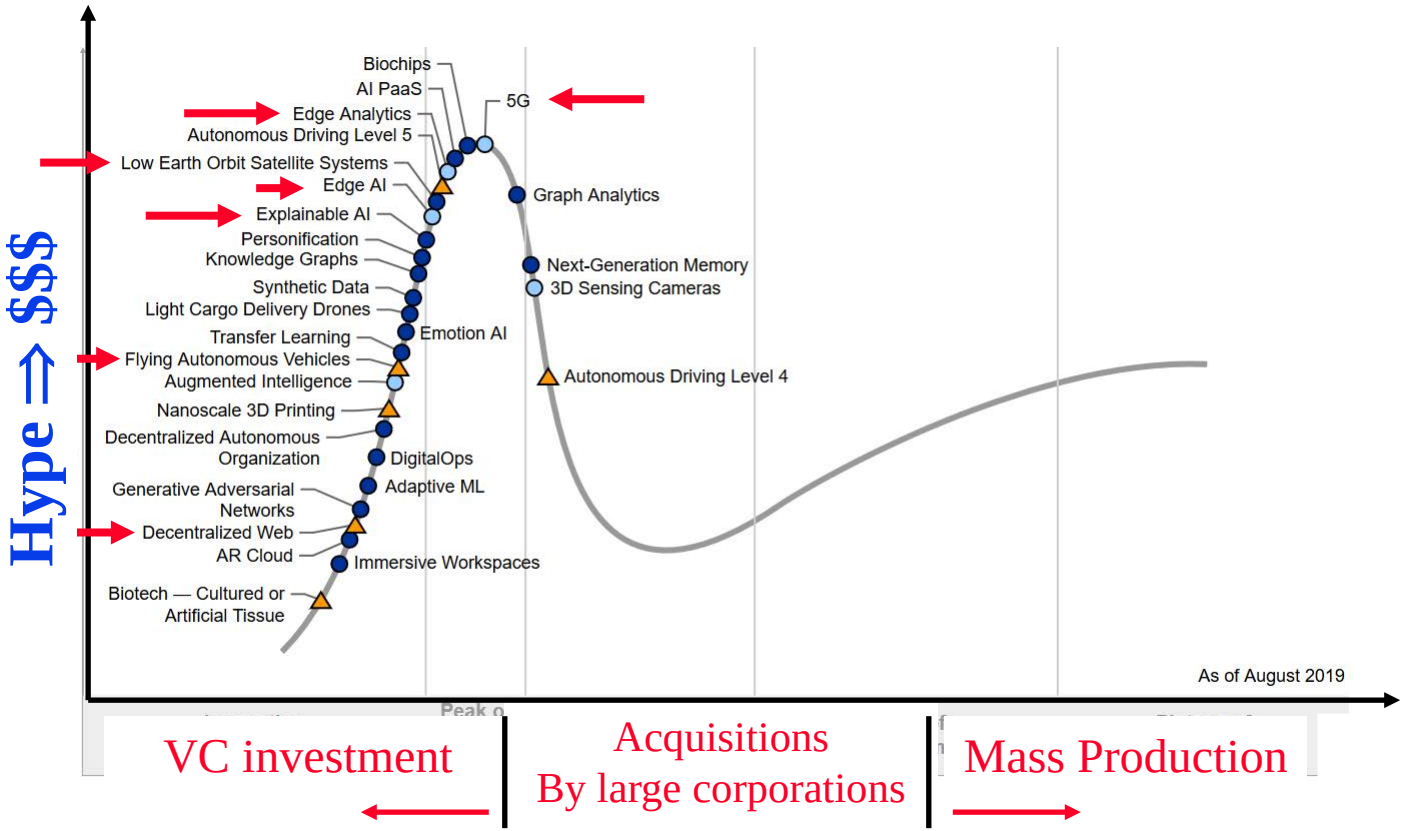
Networking = Economic Indicator

Cave Persons of 2020



Networking ⇒ Any where, Any time, Any place, Any dress, Any task

Gartner Hype Cycle of Emerging Tech 2019



Ref: B. Burke, D. Smith, "Hype Cycle for Emerging Technologies, 2019," Gartner Report G00370466, 6 Aug. 2019, 68 pp.

Current Hot Topics in Networking

1. Internet of Things (IoT)
2. IoT Security
3. Artificial Intelligence
4. Blockchains
5. Drones

Smart Everything

Smart Watch

Smart TV

Smart Car

Smart Health

Smart Home

Smart Kegs

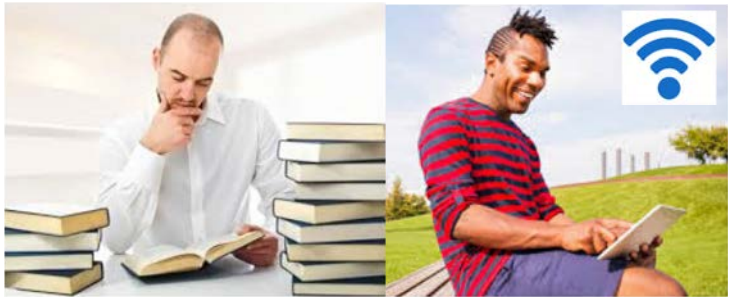
Smart Space

Smart Industries

Smart Cities

What's Smart?

- Old: Smart = Can think ⇒ Computation
  = Can Recall ⇒ Storage
- Now: Smart = Can find quickly, Can Delegate
  ⇒ Communicate = Networking
- Smart Grid, Smart Meters, Smart Cars, Smart homes, Smart Cities, Smart Factories, Smart Smoke Detectors, …



Not-Smart Smart

- Smart = Apply the latest **technology** to solve problems

Trend: Smart to Intelligent

Intelligent Clock

Intelligent TV

Intelligent Car

Intelligent Health

Intelligent Home Security

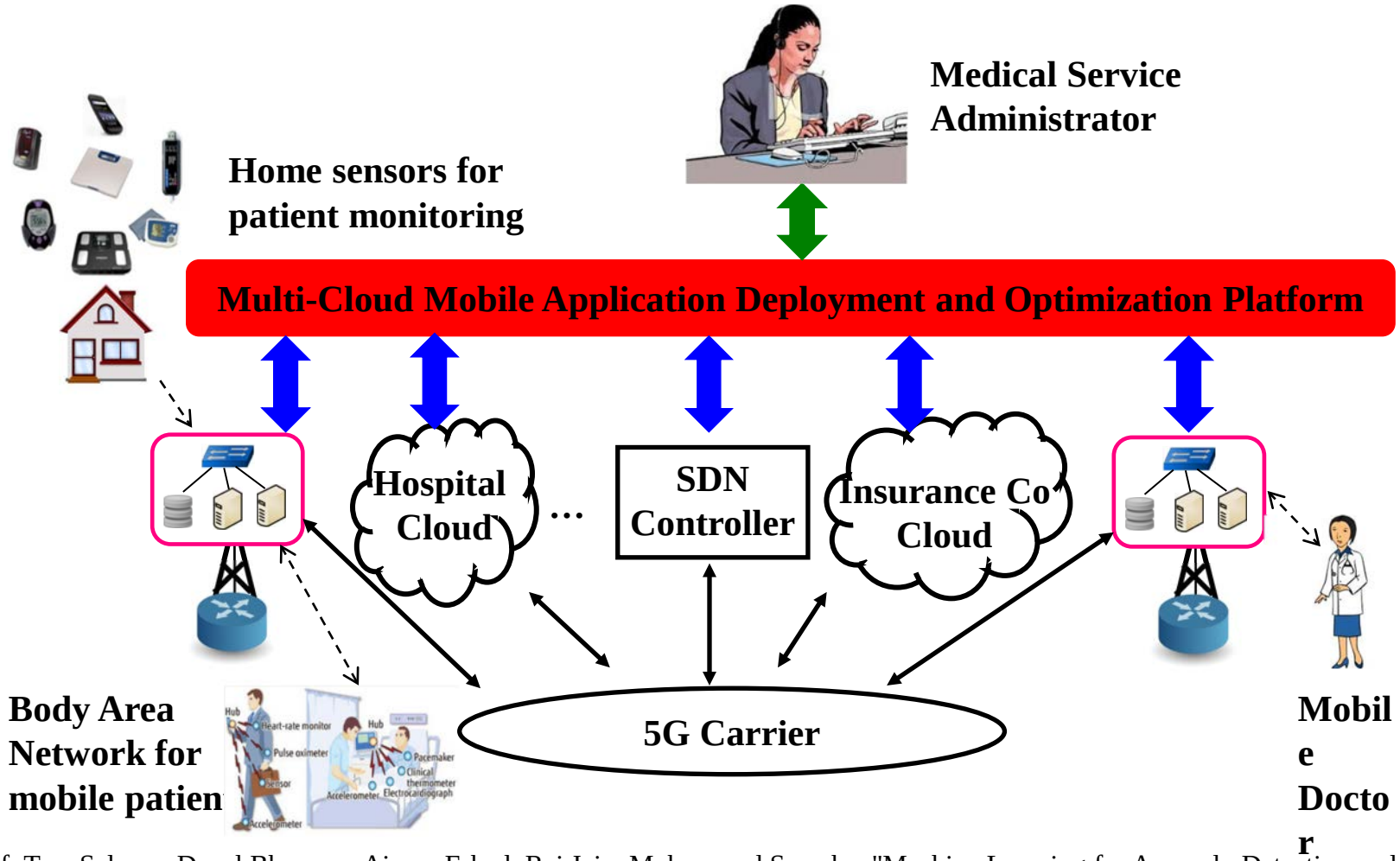
Intelligent Microwave

Intelligent Light

Amazon Alexa

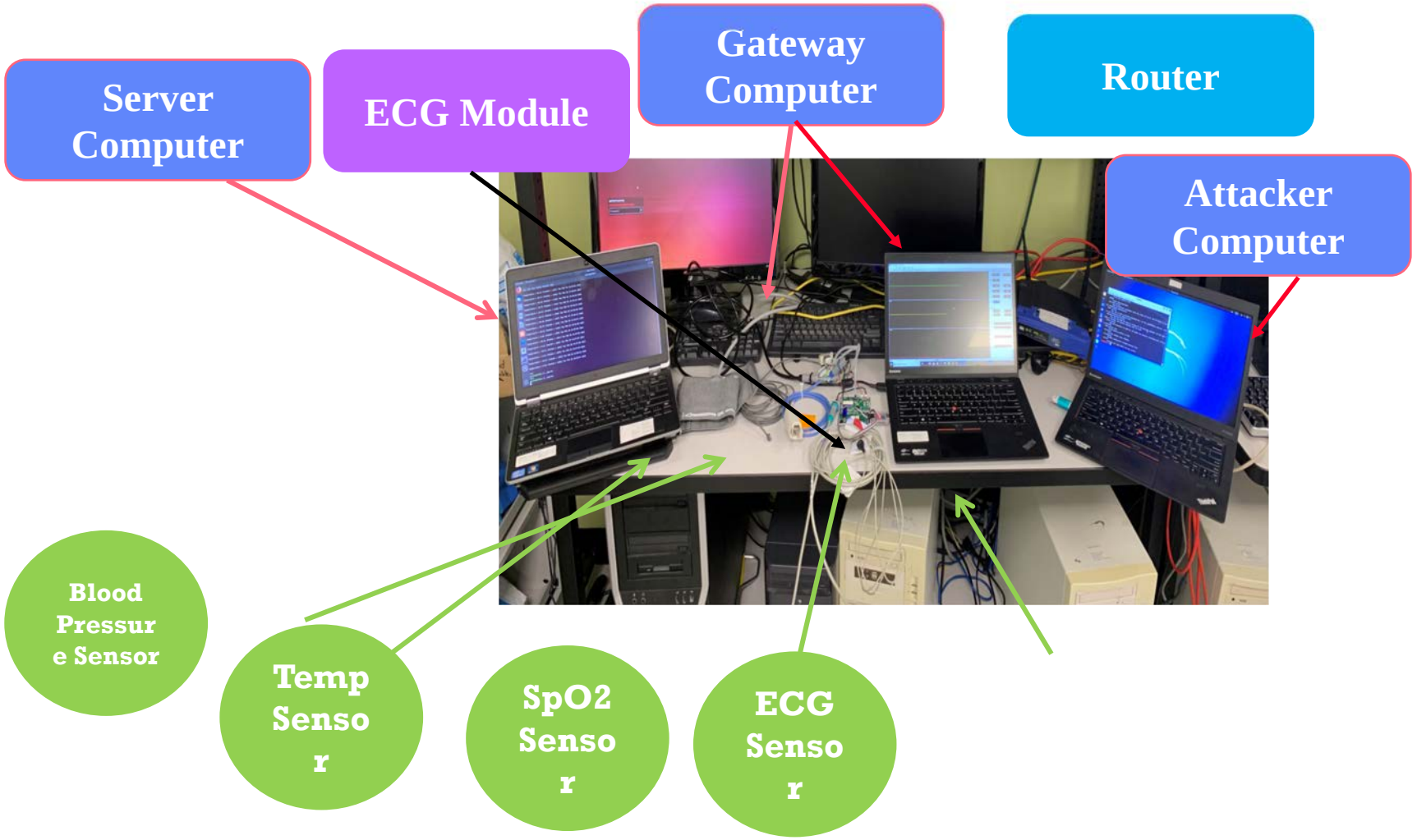
Google Assistant

Mobile Healthcare Use Case



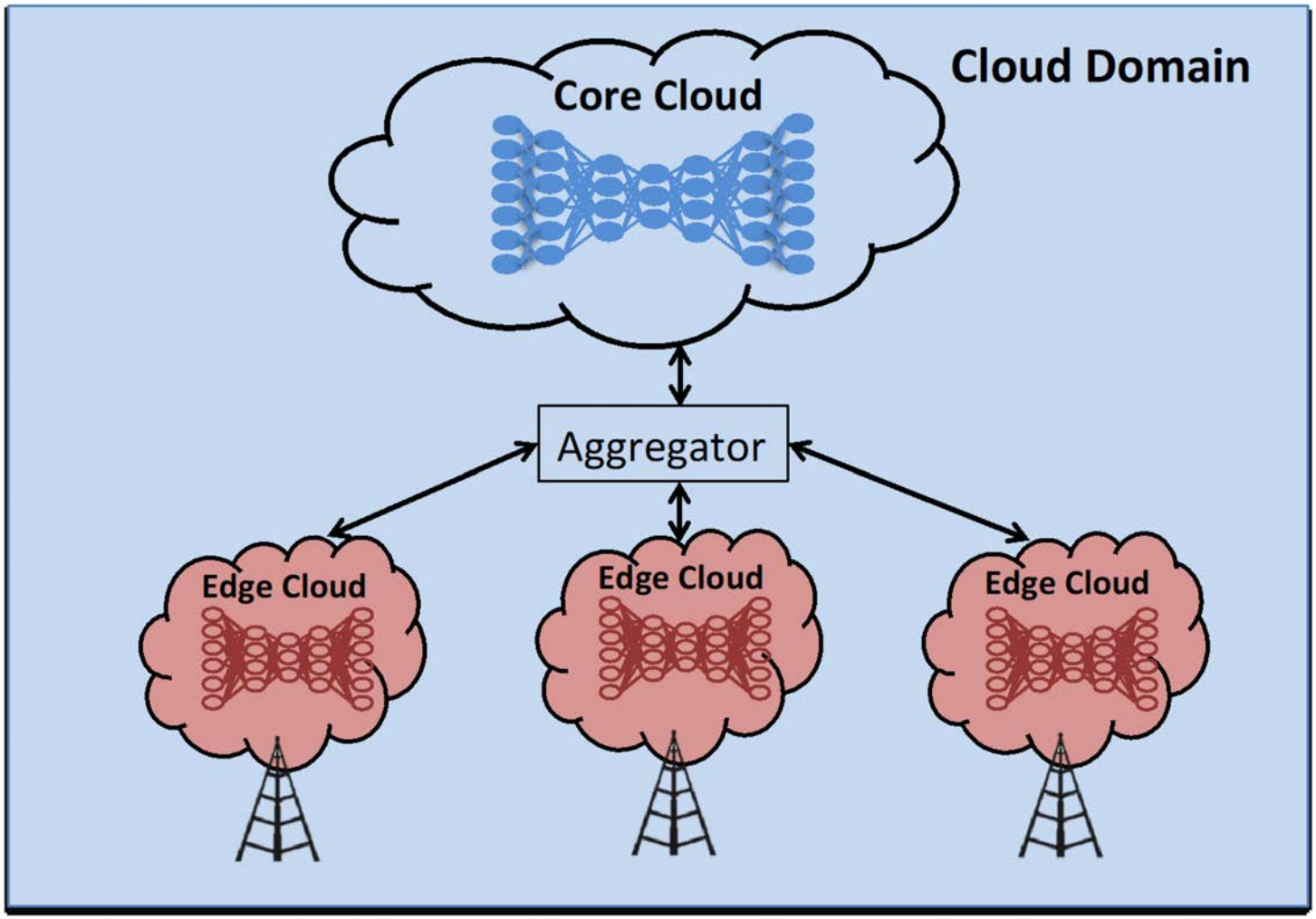
Ref: Tara Salman, Deval Bhamare, Aiman Erbad, Raj Jain, Mohammed Samaka, "Machine Learning for Anomaly Detection and Categorization in Multi-cloud Environments," The 4th IEEE International Conference on Cyber Security and Cloud Computing, June 26-28, 2017, http://www.cse.wustl.edu/~jain/papers/cscloud.htm

Hospital on Hospital on a Desk Testbed



Ref: Anar A. Hady, Ali H. Ghubaish, Tara Salman, Devrim Unal, Raj Jain, "Secure Healthcare Monitoring System using Machine Learning," Submitted.

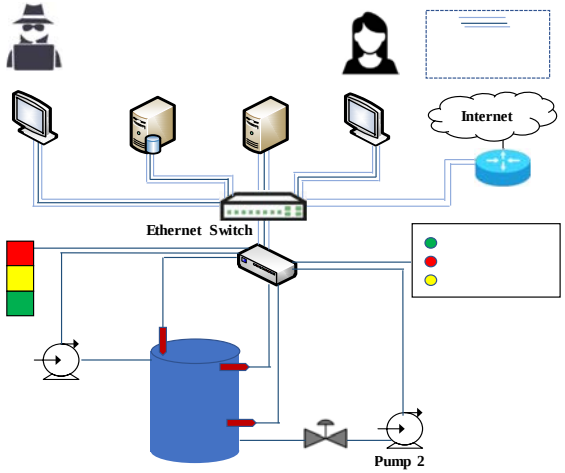
Innovations in Multi-Cloud
Hierarchical AI Model with Layer Reuse

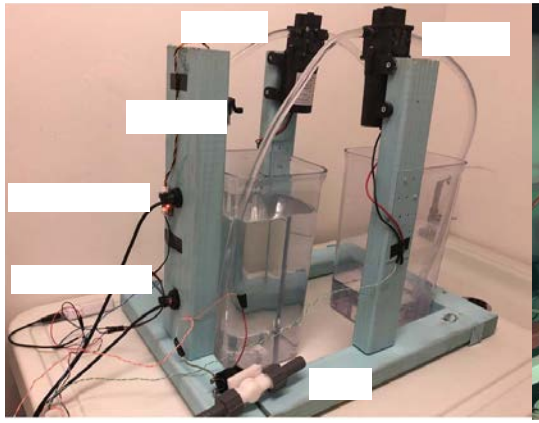


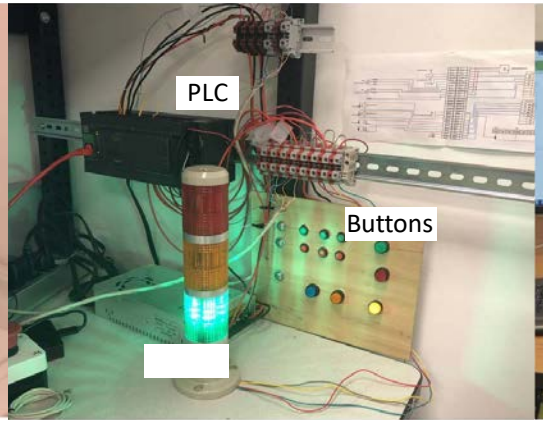
Industrial Control Systems Security

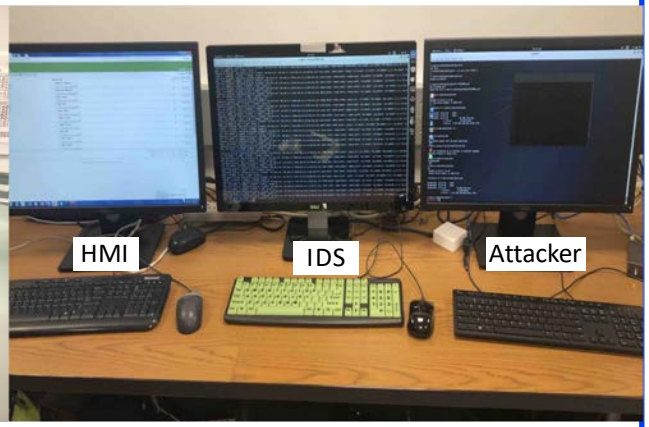
- Pre-Ethernet era networks and protocols: Modbus
- Extremely critical infrastructure
- Nation state level attacks
- Any weakness in the lifetime management, installation, or upgrades, may lead to attacks

ICS Testbed





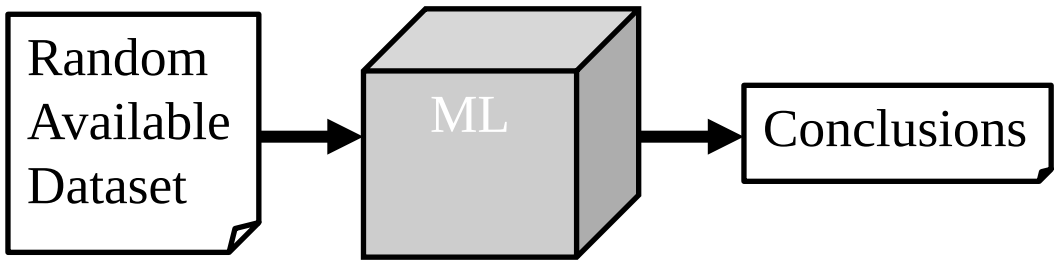




Ref: Marcio Andrey Teixeira, Tara Salman, Maede Zolanvari, Raj Jain, Nader Meskin, and Mohammed Samaka, "SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach," Future Internet 2018, 10(8), 76,
http://www.cse.wustl.edu/~jain/papers/ics_ml.htm

Machine Learning Challenges

- Machine learning is currently a black box
- ML algorithms are developed/used without domain expertise
- Data cleanliness, labeling, feature extractions, all require domain knowledge, e.g.,
  What is the distance between Port 80, Port 81, and Port 8080?
- Synthetic data is used ⇒ Garbage-In, Garbage-Out
- Results are stated without model validation.



AI for Security

- AI started with image analysis but needs to be extended for security
- Security data is very different from image data
  - Most security datasets are not representative of real world.
  - In most papers, 10-15% of the packets are attack packets
- In real-world, 1 in a billion packets is an attack packet
  - Mis-classify the attack packet ⇒ 99.9999% accuracy
  - Current metrics and methods not suitable for highly imbalanced data
- **Data imbalance** is a key issue in AI for security

1% attack =

http://www.cse.wustl.edu/~jain/talks/cs59120.htm

Trend: AI to Explainable AI

- Explainability issue
  ⇒ No idea of why the results are what they are
  Can't discover bugs in ML model implementations

Machine Learning is what only machines can do, but human cannot do and cannot explain

Ref: M. Zolanvari, M. A. Teixeira, R. Jain, "**Effect of Imbalanced Datasets on Security of Industrial IoT Using Machine Learning**," 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami FL, Nov. 9 - 11, 2018, 6 pp., http://www.cse.wustl.edu/~jain/papers/imb_isi.htm

M. Zolanvari, M. A. Teixeira, R. Jain, "**An Explainable Machine Learning Based Security Framework: A Special Case on Industrial IoT," Submitted February 2019.**

Blockchains

- Blockchain is the technology that made Bitcoin secure
- Blockchain was invented by the inventor of Bitcoin
- After Bitcoin became successful, people started looking into the technology behind Bitcoin and found:
  - Blockchain is the key for its success
  - Two complete strangers can complete a transaction/contract without a third party

Innovations in Blockchain

1. Probabilistic Blockchains (Patent Pending)

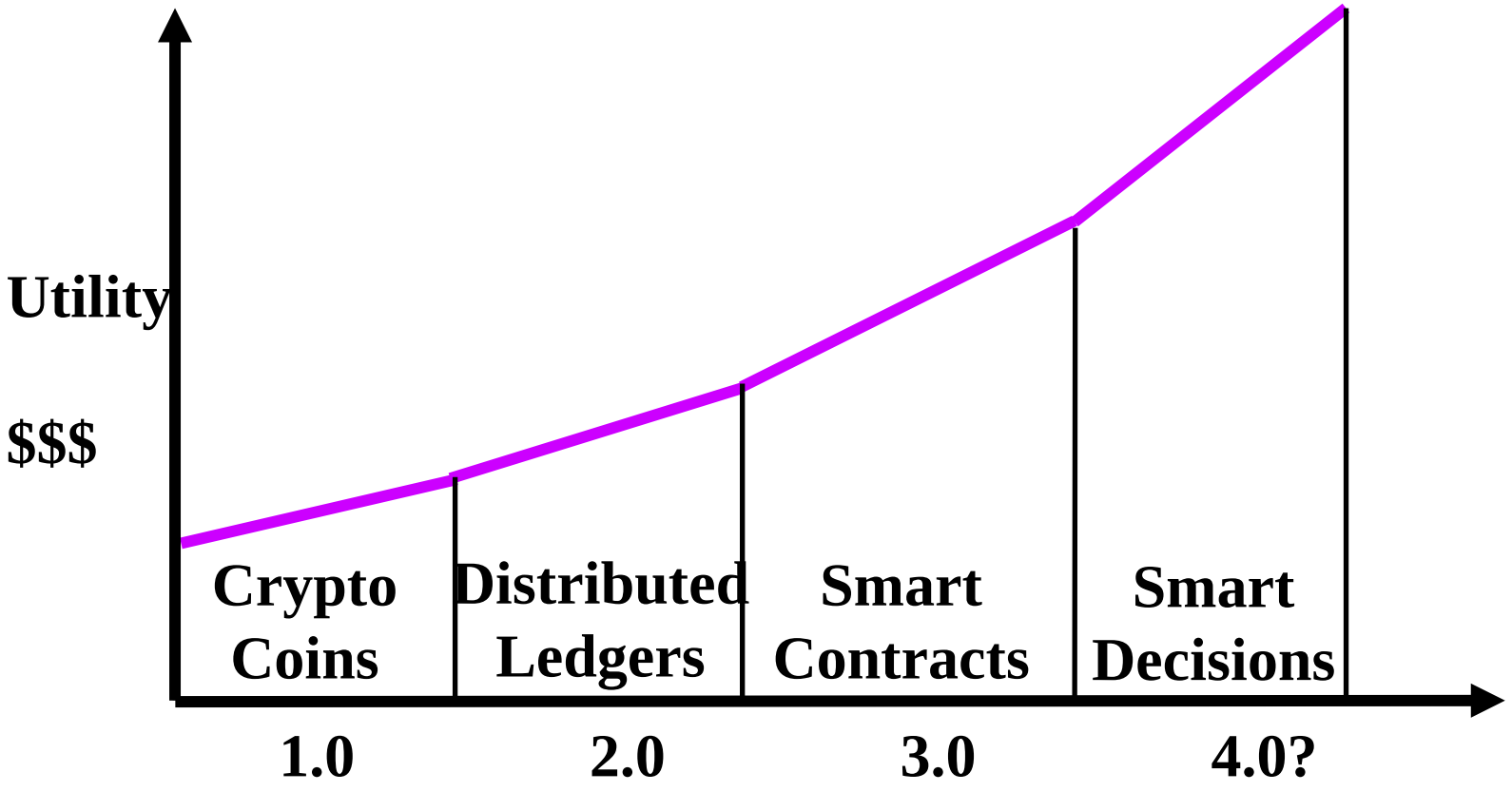
- Allows probabilistic statements:
  - I am 50% sure that this is a spam
- Uses statistics/AI to create a knowledge summary
- Good for decisions based on large number of opinions

2. Reputation Management System

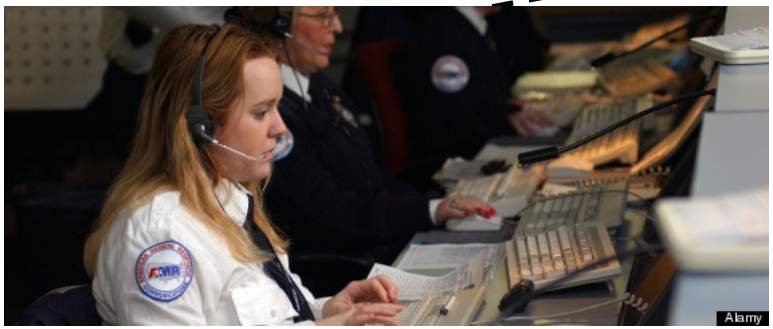
Ref: Tara Salman, Raj Jain, and Lav Gupta, "Probabilistic Blockchains: A Blockchain Paradigm for Collaborative Decision-Making," 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON 2018), New York, NY, November 8-10, 2018, 9 pp., http://www.cse.wustl.edu/~jain/papers/pbc_uem.htm

- Tara Salman, Raj Jain, Lav Gupta, "A Reputation Management Framework for Knowledge-Based and Probabilistic Blockchains," 2019 IEEE International Conference on Blockchain, Atlanta, July 14, 2019,

Blockchain Generations



Trend: Drones



Our Research Projects

1. IIoT Security: Industrial Control Systems Security
2. IoTM Security: Healthcare Security
3. Fault and Security of Datacenters using Deep Learning
4. Blockchains for Security
5. Communication using UAVs

3 Funded Research Projects

} Approved

} Pending

Techniques:

1. Machine learning and Deep Learning
2. Blockchains
3. Security
4. Networking

Key Distinction of Our Research

- Goal: Impact to the real-world DECbit congestion indication in almost all networking architectures since its invention
- Funded by industry partners: Intel, Cisco, Broadcom, Boeing, …
- Impact real-world by participating in standards organizations and industry forums: ATM Forum, IEEE Standards, American National Standards Institute (ANSI), Internet Engineering Task Force (IETF), WiMAX Forum
- Work on long term as well as short term research

Networking Courses at WUSTL

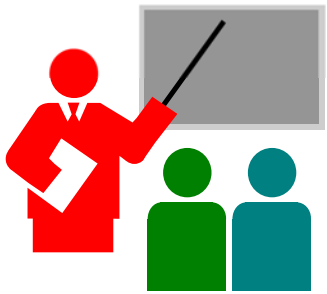
- CSE 521S: Wireless Sensor Networks
- CSE 537S: Mobile Computing
- **CSE 570: Advanced Networking**
- CSE 571: Network Security
- **CSE 574S: Wireless and Mobile Networking**
- CSE 7700: Res Seminar On Networking

CSE 473S: Introduction to Networking

Requirements

- Have 4 students working on 3 funded projects + 1 approved
- Need 1 more new Ph.D. student
- Requirements:
  - Background and interest in networking: CSE 473
  - Flexibility to work on the latest issues
  - Good communication skills
  - Machine learning (optional)
  - Preferably with a masters degree

Summary



1. Networking is the backbone of all computing
   $\Rightarrow$ Cyber age. Networking companies are leading
2. Smart $\neq$ High-Speed Computation,
   Smart $\neq$ Big Data Storage,
   Smart = Networked and Intelligent
3. We are developing new AI and Blockchain techniques for network security issues
4. Research for Impact

References: Class Recordings

- Recordings of all of my classes and talks are available on YouTube and on my website:

1. CSE 473: Introduction to Computer Networks, http://www.cse.wustl.edu/~jain/cse473-20/index.html
2. CSE 571S: Network Security, http://www.cse.wustl.edu/~jain/cse571-17/index.html
3. CSE 574S: Wireless Networks, http://www.cse.wustl.edu/~jain/cse574-18/index.html
4. CSE 567: Computer Systems Analysis http://www.cse.wustl.edu/~jain/cse567-17/index.html
5. CSE 570: Recent Advances in Networking http://www.cse.wustl.edu/~jain/cse570-19/index.html

Our Publications on ICS Security

1. M. Elnour, N. Meskin, K. Khan, R. Jain, "A Dual-Isolation-Forests-Based Attack Detection Framework for Industrial Control Systems," IEEE Access, Vol. 8, 19 February 2020, pp. 36639 - 36651, http://www.cse.wustl.edu/~jain/papers/dif.htm
2. D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, N. Meskin, "Cybersecurity for Industrial Control Systems: A Survey," Computers and Security, Elsevier, Volume 89, February 2020, Article 101677, http://www.cse.wustl.edu/~jain/papers/ics_survey.htm
3. M. Zolanvari, M. Teixeira, L. Gupta, K. Khan, R. Jain, "Machine Learning Based Network Vulnerability Analysis of Industrial Internet of Things," IEEE Internet of Things Journal, Vol. 6, Issue 4, Aug 2019, http://www.cse.wustl.edu/~jain/papers/vulnerab.htm
4. M. Zolanvari, M. Teixeira, R. Jain, "Effect of Imbalanced Datasets on Security of Industrial IoT Using Machine Learning," 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami FL, Nov. 9 - 11, 2018, 6 pp., http://www.cse.wustl.edu/~jain/papers/imb_isi.htm

Our Publications on Healthcare Security

1. Anar A. Hady, Ali Ghubaish, T. Salman, Devrim Unal, and R. Jain, "**Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study**," IEEE Access, June 2020, http://www.cse.wustl.edu/~jain/papers/hms.htm

Our Publications on Blockchains

1. T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security Services Using Blockchains:A State of the Art Survey" IEEE Communications Surveys and Tutorials, First Quarter 2019, Volume 21, Issue 1, 858-880 pp., http://www.cse.wustl.edu/~jain/papers/bcs.htm
2. T. Salman, R. Jain, L. Gupta, "A Reputation Management Framework for Knowledge-Based and Probabilistic Blockchains," IEEE 1st International Workshop on Advances in Artificial Intelligence for Blockchain (AIChain 2019), held in conjunction with the 2019 IEEE International Conference on Blockchain, Atlanta, July 14, 2019, http://www.cse.wustl.edu/~jain/papers/rpmcewa.htm
3. T. Salman, R. Jain, and L. Gupta, "Probabilistic Blockchains: A Blockchain Paradigm for Collaborative Decision-Making," 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON 2018), New York, NY, November 8-10, 2018, 9 pp., http://www.cse.wustl.edu/~jain/papers/pbc_uem.htm

Our Publications on 5G

1. J. Li, C. uo, L. Gupta, and R. Jain, "Efficient and Secure 5G Core Network Slice Provisioning Based on VIKOR Approach," IEEE Access, 15 October 2019, http://www.cse.wustl.edu/~jain/papers/vikor.htm
2. J. Li, C. uo, Jun Xu, L. Gupta and R. Jain, "Towards Efficiently Provisioning 5G Core Network Slice Based on Resource and Topology Attributes," Applied Sciences, September 2019, http://www.cse.wustl.edu/~jain/papers/5g_slice.htm
3. J. Li, M. Samaka, H. Chan, D. Bhamare, L. Gupta, C. uo, and R. Jain, "Network Slicing for 5G: Challenges and Opportunities," IEEE Internet Computing, Vol. 21, Issue 5, September 18, 2017, pp. 20-27, http://www.cse.wustl.edu/~jain/papers/slic_ic.htm [63 Citations]
4. L. Gupta, R. Jain, H. Chan, "Mobile Edge Computing - an important ingredient of 5G Networks," IEEE Softwarization Newsletter, March 2016, http://www.cse.wustl.edu/~jain/papers/mec16.htm
5. Sanjay Kumar Biswash, Artur Ziviani, R. Jain, Jia-Chin Lin, Joel J. P. C. Rodrigues, "Editorial: Device-to-Device Communication in 5G Networks," Guest Editorial, Mobile Networks and Applications, Volume 22, Issue 6, December 2017, pp. 995-997, http://www.cse.wustl.edu/~jain/papers/d2d_ed.htm

Our Publications on Machine Learning

1. M. Zolanvari, M. Teixeira, R. Jain, "Effect of Imbalanced Datasets on Security of Industrial IoT Using Machine Learning," 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami FL, Nov. 9 - 11, 2018, 6 pp., http://www.cse.wustl.edu/~jain/papers/imb_isi.htm

Our Publications on UAVs

1. M. Zolanvari, R. Jain, T. Salman, "Potential Data Link Candidates for Civilian Unmanned Aircraft Systems: A Survey," IEEE Communications Surveys & Tutorials, December 17, 2019, 28 pp., http://www.cse.wustl.edu/~jain/papers/uav_dl.htm
2. Ali Ghubaish, T. Salman, and R. Jain, "Experiments with a LoRaWAN based Remote ID System for Locating Unmanned Aerial Vehicles (UAV)," Wireless Communications and Mobile Computing, October 20, 2019, http://www.cse.wustl.edu/~jain/papers/uav_lora.htm
3. R. Jain and F. Templin, "Requirements, Challenges and Analysis of Alternatives for Wireless Datalinks for Unmanned Aircraft Systems," IEEE Journal on Selected Areas in Communications (JSAC) Special Issue on Communications Challenges and Dynamics for Unmanned Autonomous Vehicles, Vol. 30, No. 5, June 2012, pp. 852-860, http://www.cse.wustl.edu/~jain/papers/uas_jsac.htm
4. Denise S. Ponchak, Fred L. Templin, Greg Sheffield, Pedro Taboso, R. Jain, "Advancing the Standards for Unmanned Air System Communications, Navigation, and Surveillance," IEEE Aerospace Conference, Big Sky, Montana, Mar 2-9, 2019, http://www.cse.wustl.edu/~jain/papers/aerosp19.htm

Our Publications on UAVs (cont)

5. Denise Ponchak, Fred Templin, Greg Sheffield, Pedro Taboso, R. Jain, "An Implementation Analysis of Communications, Navigation, and Surveillance (CNS) Technologies for Unmanned Air Systems (UAS)," 2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC), San Diego, CA, Sep. 23-27, 2018, 10 pp., http://www.cse.wustl.edu/~jain/papers/dasc18.htm
6. M. Zolanvari, M. Teixeira, R. Jain, "Analysis of AeroMACS Data Link for Unmanned Aircraft Vehicles," 2018 International Conference on Unmanned Aircraft Systems (ICUAS), Dallas, TX, September 2018, pp. 752 - 759, http://www.cse.wustl.edu/~jain/papers/aeromacs.htm
7. Denise S. Ponchak, Fred L. Templin, Greg Sheffield, Pedro Taboso-Ballesteros, and R. Jain, "Reliable and Secure Surveillance, Communications and Navigation (RSCAN) for Unmanned Air Systems (UAS) in Controlled Airspace," 2018 IEEE Aerospace Conference, Big Sky, MT, March 3-10, 2018, 13 pp., http://www.cse.wustl.edu/~jain/papers/aerosp18.htm
8. R. Jain, Fred L. Templin, "Datalink for Unmanned Aircraft Systems: Requirements, Challenges and Design Ideas," AIAA Infotec@Aerospace Conference, Saint Louis, MO, March 2011, http://www.cse.wustl.edu/~jain/papers/uas_dl.htm

Our Publications on UAVs (Cont)

9. Ali Ghubaish, "Locating Unmanned Aerial Vehicles (UAVs)," MS Thesis, Department of Computer Science and Engineering, Washington University in Saint Louis, December 2017, 59 pp., http://www.cse.wustl.edu/~jain/theses/agms.htm

Acronyms

- 3GPP Third Generation Partnership Project
- AI Artificial Intelligence
- ANSI American National Standards Institute
- AT&T American Telephone and Telegraph
- BSS Business Support Services
- CA California
- CGNAT Carrier Grade Network Address Translator
- CSE Computer Science and Engineering
- DECbit Digital Equipment Corporation Bit
- IEEE Institution of Electrical and Electronic Engineering
- IoT Internet of Things
- ML Machine Learning
- MO Missouri
- MS Master of Science
- NFV Network Function Virtualization
- NTT Nippon Telephone and Telegraph

Acronyms (Cont)

- OpenADN Open Application Delivery Networking
- OSS Operations Support Services
- SON Self-Organizing Networks
- TV Television
- UK United Kingdom
- US United States
- VC Venture Capital
- WAN Wide Area Network
- WiMAX Worldwide Interoperability for Microwave Access
- WUSTL Washington University in St. Louis

Scan This to Download These Slides

Raj Jain
Rajjain.com

http://www.cse.wustl.edu/~jain/talks/cs59120.htm

Our Courses on YouTube

CSE567M: Computer Systems Analysis (Spring 2013),
https://www.youtube.com/playlist?list=PLjGG94etKypJEKjNAa1n_1X0bWWNyZcof

CSE473S: Introduction to Computer Networks (Fall 2011),
https://www.youtube.com/playlist?list=PLjGG94etKypJWOSPMh8Azcgy5e_10TiDw

CSE 570: Recent Advances in Networking (Spring 2013)

https://www.youtube.com/playlist?list=PLjGG94etKypLHyBN8mOgwJLHD2FFIMGq5

CSE571S: Network Security (Fall 2011),
https://www.youtube.com/playlist?list=PLjGG94etKypKvzfVtutHcPFJXumyyg93u

Video Podcasts of Prof. Raj Jain's Lectures,
https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw