Report of the NSF Workshop on Internet-of-Things (IoT) Systems

1. Introduction

This report summarizes the work of a group of contributors on important aspects in Internet-of-Things (IoT) research. The contributors met before ICCAD in San Diego, California on November 4, 2018 to discuss ideas in person. The report was completed by electronic discussion based on notes from that meeting.

The next section discusses the definition of IoT and compares IoT systems to other types of computing systems. Section 3 reviews applications domains for IoT systems. Section 4 describes research challenges and opportunities. Section 5 surveys diversity and inclusion challenges and opportunities related to IoT systems. Section 6 reviews needs for education and training related to IoT. Section 7 identifies both enabling and dis-enabling factors for IoT systems research. NSF support for this workshop is acknowledged in Section 8. This report is the creation of all the participants at the workshop; the contributors are identified in Section 9.

2. What is IoT?

Internet-of-Things is used both as a technical and marketing term. As a marketing term, it is broadly applied to many different kinds of systems. As a technical term, we can identify some key characteristics that form the core definition along with additional characteristics of some IoT systems.

IoT systems are large-scale networked embedded systems that are provide sensing, actuating, processing, and informing. The participants agreed that an IoT system has two essential characteristics:

- It senses physical quantities, both continuous and discrete.
- It operates on sensor data as a distributed computing system composed of several different types of nodes connected by wireless and/or wired networks.

Frequently found characteristics include:

- IoT networks are often designed for long operational lifetimes, whether they be in a factory or a smart city. The system needs to be maintainable and upgradeable over its entire lifetime.
- Shared computing resources can be applied to data from multiple sources. Computing resources may also be shared by several applications. Different users may have diverse views of a common set of data.
- IoT systems are built on heterogeneous architectures: multiple types of processors, networks, I/O devices, and software stacks.
- IoT systems are systems-of-systems. Their design process is complex and may not admit of a single optimum solution.
- The IoT system often makes use of public standards for communication and information access, although not every node or link must make use of such public standards. For example, many IoT systems do not use the Internet Protocol to connect to some nodes at the extreme edge.
- An IoT system performs a consequential physical act---the sensor system may be involved in actions that directly affect safety, health, and comfort.
- Actuation (*e.g.*, by solenoid or human) is common.

- A significant component of its operation occurs autonomously, although human-in-the-loop supervisory operation is common.
- The IoT system may be formed as an Internet of cyber-physical systems that perform real-time control.

IoT systems research draws from several existing research communities:

- Sensor networks.
- Distributed computing.
- Embedded computing.
- Cyber-physical systems.
- Computer-aided design.
- Signal processing.
- Computer security.
- Reliability engineering.

The definition of IoT system is brought into focus by comparing it to other fields. When comparing IoT systems to cyber-physical systems, the participants identified differences in both function and performance. Functionally, cyber-physical systems feature closed-loop control while IoT systems sense but may not perform closed-loop functions. Cyber-physical systems operate at higher sample rates (IEEE IRDS puts the boundary at 1 s); IoT systems are often event-oriented, identify changes in signals that may operate at lower rates. Chemical and biological processes, for example, often need lower sample rates. A comparison of IoT systems to sensor network identified differences in architecture and scale. IoT systems put more emphasis on distributed computation. Sensor networks typically send data to cloud application while IoT systems perform in-network distributed computation. IoT system opportunities and challenges also include the huge scale made possible by the huge number of semiconductor sensors that can be manufactured, an opportunity referred to by the sensor community as the *trillion sensor world*.

IoT systems exhibit a range of important requirements:

- Function:
  - Measure and interpret signals.
  - Compare and analyze multiple signals.
- Communication:
  - Communicate for distributed computation.
  - Communicate with external applications such as the cloud or SCADA.
- Performance:
  - Keep up with signal rates.
  - Supply data to external applications at required rates.
- Power:
  - Some nodes are ultra-low power (microwatt).
  - Different nodes will have varying power requirements.
- Cost:
  - Very low cost nodes ($0.01 - $0.10) [Ral16].
  - Low total cost of ownership including purchase, installation, system integration, and maintenance.
- Safety, security, privacy:
  - Must protect data integrity, timing.

- Must ensure that data is not improperly exposed to unauthorized persons.
- Particularly important given distributed architecture, shared tenancy in some systems.

3. Application Domains

IoT systems are used in a wide range of applications. We give a few examples of specific applications for each area; many other applications are possible:

- Health care: patient monitoring, wellness [ASU18], home health care [Ray14, Wol15].
- Transportation: monitoring systems for transportation terminals, traffic monitoring systems [Xia11], vehicular monitoring [Hew14].
- Advanced manufacturing: process monitoring [Aba11], quality monitoring and analysis, maintenance prediction [Yid16], safety [Tao14].
- Conservation: energy, water [Tar12, Koo15], sewage [Gub15].
- Energy distribution: smart grid [Hub12], remote control, load balancing.
- Environment: air quality [Hon08], forest fire monitoring [Laz13, Bea17].
- Agriculture: soil monitoring [Ton13], plant analysis, harvesting and crop quality.
- Arts: interactive artwork and performance, lessons.
- Sports: athlete performance monitoring, monitoring of play and rules.

We use the term *IoT system* rather than *the Internet-of-Things* to emphasize that not these systems are not connected into a single, globe-spanning network. IoT technology is used in many application areas---health care, manufacturing, *etc.*---that require some amount of privacy.

IoT systems applications reach across many disciplines. IoT systems research should include the participation of experts in other fields: other engineering disciplines, physics, chemistry, human factors, sociology, *etc.*

4. Research Challenges and Opportunities

The participants identified several important research challenges and opportunities in IoT systems.

They strongly agreed that applications are important drivers of the IoT system design process. Applications provide important challenges that may not be apparent when the technology is viewed in isolation. A foundation of common principles should be supplemented with techniques aimed at the unique characteristics of the application.

Participants also strongly agreed that IoT research should work to break down silos in system standards [Rab17]. IoT research should build upon existing knowledge bases in system-level design, sensor networks, CPS, and other fields---*don't reinvent the wheel*. Devices, networks, and applications should be able to interoperate effectively. Interoperability is especially important given the long lifetimes of many IoT systems: components may fail, new hardware capabilities will emerge, software standards will evolve, new capabilities will be desired by users.

IoT systems research is a convergent challenge that encompasses both physics-oriented engineering (mechanical, civil, electrical, chemical, aeronautical) and computation-oriented engineering. These disciplines have very different views of modeling---discrete *vs*. continuous is just one example. IoT systems research should bridge these disciplines and evolve a world view that is useful to all component disciplines. A practitioner does not need a detailed knowledge of all component disciplines, but a basic working knowledge of some key concepts provided by the participating disciplines is essential to the design of successful IoT systems.

Security, safety, and privacy are important characteristics for IoT systems. Security and safety cannot be considered as separate design activities when dealing with computationally-intensive physical systems [Wol18, Sch17].

Many devices in IoT systems must operate on limited amounts of power. Power limitations may come from the limited availability of wiring to deliver power or from environmental characteristics. Ultra-low power devices---devices that consume microwatts while performing useful operations---are an important challenge for IoT systems. The design of ultra-low power devices introduces challenges in circuits and devices, architecture, power management, and design methodologies. Devices may also have energy limitations, or they may be limited in energy use within a given time period (such as under energy-harvesting conditions). The operation duty-cycle of these devices may be limited and IoT systems may become networks of intermittently powered and intermittently connected computing devices.

Many IoT systems will make use of machine learning. A significant fraction of machine learning---both inference and training---will be performed at the edge due to constraints on communication bandwidth, power, latency, and privacy [Lih18]. Providing formal guarantees for recall/precision, security, safety, and privacy is a research challenge [Hua17] Machine learning methods adapted to distributed systems and ultra-low power devices present a significant challenge and research opportunity.

IoT systems research is a new field of opportunity for CAD and system-level design. Design-oriented research should leverage, enhance, and extend distributed/SW/SoC/HW design methodologies and tools [Swa18]. Challenges include formal models for specification, synthesis for translation between abstraction layers, and compilation/synthesis tools for automating the design process. IoT system design processes must go beyond hardware/software co-design to take into account both physical and cyber characteristics.

IoT systems often operate as human-in-the-loop systems. System design taking into account human interactions along with distributed computation and ultra-low power operation provide important research challenges. IoT platforms should support collaboration and cooperation.

Many IoT systems exhibit shared tenancy: several applications may share data from a common pool of sensors; applications may share the network and distributed computing platform. Shared tenancy introduces new challenges: security, safety, and privacy; performance and latency management; power management [Bon18].

5. Diversity and Inclusion

IoT application areas cut across societal needs and applications. As a result, IoT systems provide an opportunity to broaden participation and create more inclusive communities of designers and users. Reaping the benefits of IoT technology will require inter-disciplinary, inter-institutional, cross-cultural, and inter-regional solutions. Inclusion should continue to be a mandate for research efforts in IoT systems.

Some IoT systems research efforts could target potential solutions for disadvantaged groups---for example, IoT systems to aid people with physical or cognitive disabilities. The relatively low cost of experimental systems for IoT also makes this technology a good candidate for institutions with limited resources. IoT offers the potential to help bridge the digital divide by providing services directly related to the community and its needs.

Ensuring the participation of underrepresented groups may be facilitated by funding research efforts for application areas of particular interest to those groups or at institutions that serve those groups. Such targeted efforts may provide added incentives to enter the IoT systems field.

Including researchers and students from underrepresented groups helps to provide role models that encourage additional participation. IoT system architectures will influence the degree to which access to and control of these systems is centralized. This will influences how the benefits and (e.g., privacy) costs of these systems accrue to their diverse users and owners vs. those most adept at centralizing and controlling power.

6. Education and Training

Given the pervasive application of IoT systems, education and training at all levels should take into account IoT technologies and their underlying core scientific and mathematical principles. IoT systems education and training should occur at the professional level, graduate and undergraduate education, and K-12. Properly chosen examples of IoT systems can promote community and family participation.

Professional training will help workers and managers in the field to make better use of sensors and IoT systems in their fields of endeavor. Professional seminars, short courses, online videos, and conferences are all important mechanisms for delivering IoT systems knowledge to professionals.

Graduate education in IoT systems is clearly interdisciplinary---VLSI, embedded computing, sensor networks, signal processing, control. Not all institutions will have concentrated expertise in all these areas; inter-institutional efforts can help to provide the necessary knowledge to a wider range of institutions. Both theoretical and application-oriented courses and projects are important.

Undergraduate education in IoT systems can leverage existing academic disciplines: embedded computing, networking, signal processing and controls, machine learning. Case studies will help educators inject IoT material into their courses. Case studies can include application descriptions, hardware and software platforms, and simulation frameworks. Some IoT-centric courses should be developed; IoT material should also be added to existing courses. Given the wide range of engineering disciplines who will make use of IoT technology---mechanical, chemical, electrical, civil---all disciplines should introduce some basic IoT-oriented knowledge into their curricula.

IoT is very well suited to K-12 education because it is about tangible and touchable objects. Younger students can learn by play and use IoT concepts to help them understand the physical world. At the high school level, CS/CE/EE kits that teach the fundamentals of IoT. Universities need to help train K-12 teachers on IoT fundamentals. The two groups should work together to identify opportunities to introduce important concepts and how best to convey the required knowledge.

Maker spaces---common places with facilities such as 3D printers---provide a valuable service at all levels, from professional education through K-12. Students from different disciplines come together and exchange ideas. Learning-by-doing is an important educational tool and very well suited to many IoT applications. Graduate and undergraduate students can help to mentor users of maker spaces.

7. Enabling and Dis-Enabling Factors

The participants identified several enabling factors for effective IoT research. They also identified some dis-enabling factors that could inhibit effective research in the field.

Effective interdisciplinary research requires breaking down silos. Shared infrastructure is an important enabling mechanism for IoT system research. Dataset and benchmark creation can have

high impact but is very challenging. How does the field create and maintain testbed data sets? How many domains? How can a good set of candidate domains select? Funding agencies should encourage the creation of such data sets by providing funding for their creation and maintenance.

Reference platforms may be very useful. Such platforms are often built from open-source hardware and software. How can researchers and practitioners be encouraged to develop open-source platforms? Possible domains for such reference platforms include edge computing, safety and security, and complex applications.

Shared experimental platforms are challenging to design and maintain but can allow more groups to experiment in complex domains. Experimental platforms may consist of physical equipment and simulated setups in various combinations. Such platforms require up-front effort to design a platform that can be safely and effectively shared; they also require continuing funding for maintenance and operation. Some experimental platforms may be of interest to companies who do not have the financial resources to build a complete experimental facility or who may not have the time required to build such a facility from scratch. Corporate users introduce some privacy and data security issues but may also provide a useful funding source for these environments.

Applications with human interactions may have broad impact.

Conferences are an important venue for sharing knowledge. Companies, universities, and K-12 institutions may all make use of conferences, although no single conference is likely to fully satisfy all these diverse communities. Several mechanisms can be used to discuss IoT systems: new meetings can be created; IoT tracks can be formed in existing meetings. Discussion and exploration in the communities should be encouraged to decide the best way to develop forums for IoT systems research, practice, and education.

Research/knowledge silos were identified as a key dis-enabling-factor to the creation and deployment of effective IoT systems. Silos are everywhere, especially in academia. Funding agencies can use funding leverage to help break down existing silos and discourage the creation of new silos. Research outcomes---publications, patents, design utilization, *etc.*---can help funding agencies to incentivize researchers and practitioners to practice interdisciplinary, effective creation of IoT systems.

8. Acknowledgments

This workshop was sponsored by the National Science Foundation under award 1833276.

9. Contributors

Contributors:

Jacob Abraham	jaa@cerc.utexas.edu
Ali Ahmadinia	aahmadinia@csusm.edu
Baris Aksanli	baksanli@sdsu.edu
Ganapati Bhat	gmbhat@asu.edu
Abhjit Chatterjee	abhijit.chatterjee@ece.gatech.edu
Xiang Chen	xchen26@gmu.edu
Yiran Chen	yiran.chen@duke.edu
Robert Dick	dickrp@umich.edu
Kevin Fu	kevinfu@umich.edu
Luis Garcia	garcialuis@g.ucla.edu
Mohsen Imani	moimani@ucsd.edu
Takahide Inoue	tinoue@citris.org

Ryan Kastner	kastner@ucsd.edu
Srinivas Katkoori	katkoori@mail.usf.edu
Young Soo Kim	ykim@fsmail.bradley.edu
Eugene Lee	eugene@ieee.org
Anthony Lopez	anthl10@uci.edu
Andrew Lukefahr	lukefahr@iu.edu
Tukila Mitra	tulika@comp.nus.edu.sg
Miroslav Pajic	mp275@duke.edu
Nikshep Patil	nikshep.patil@gmail.com
Kishore Ramachandran	rama@gatech.edu
Nafiul Rashid	nafiulr@uci.edu
Tajana Rosing	tajana@ucsd.edu
Patrick Schaumont	schaum@vt.edu
Jenna Wu	jenna@kneron.us
Jishen Zhao	jzhao@eng.ucsd.edu
Hao Zheng	haozheng@usf.edu
Han Zou	hanzou@berkeley.edu

Workshop committee:

Dong Ha, Virginia Tech
Howard Shrobe, MIT
Mohammad Al Faruque, UC Irvine
Ryan Kastner, UCSD
Jack Stankovic, University of Virginia
Shuvra Bhattacharyya, University of Maryland
Robert Dick, University of Michigan
Li Shang, University of Colorado
Saibal Mukhopodhyay, Georgia Tech
Marilyn Wolf, Georgia Tech (chair)

References

[Aba11] Abad, A., Paynabar, K., and Jin, J. (2011) "Modeling and Analysis of Operators Effect on Process Quality and Throughput in Mixed Model Assembly Systems," *ASME Transactions, Journal of Manufacturing Science and Engineering*, Vol. 133, 021016-1~9.

[ASU18] ASU Elab Group, *OpenHealth System*, https://sites.google.com/view/openhealth-wearable-health/home

[Bea17] E. Beachly, C. Detweiler, S. Elbaum, and B. Duncan, "Uas-rx interface for mission planning, fire tracking, fire ignition, and real-time updating," in IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR)., 2017.

[Bon12] Bonomi, Flavio, et al. "Fog computing and its role in the internet of things." *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*. ACM, 2012.

[Gub13] Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." *Future generation computer systems* 29.7 (2013): 1645-1660.

[Hew14] He, Wu, Gongjun Yan, and Li Da Xu. "Developing vehicular data cloud services in the IoT environment." *IEEE Transactions on Industrial Informatics* 10.2 (2014): 1587-1595.
[Hon08] Honicky, Richard, et al. "N-smarts: networked suite of mobile atmospheric real-time sensors." *Proceedings of the second ACM SIGCOMM workshop on Networked systems for developing regions*. ACM, 2008.
[Hua17] Huang, Xiaowei, et al. "Safety verification of deep neural networks." *International Conference on Computer Aided Verification*. Springer, Cham, 2017.
[Hub12] T. Hubert, S. Grijalva, "Advanced Modeling for Residential Electricity Optimization in Dynamic Pricing Environments", *IEEE Transactions on Smart Grid, Special Issue on Intelligent Buildings and Home Energy Management*, December, 2012.
[Koo15] Koo, Dan, Kalyan Piratla, and C. John Matthews. "Towards sustainable water supply: Schematic development of big data collection using internet of things (iot)." *Procedia engineering*118 (2015): 489-497.
[Laz13] Lazarescu, Mihai T. "Design of a WSN platform for long-term environmental monitoring for IoT applications." *IEEE Journal on emerging and selected topics in circuits and systems* 3.1 (2013): 45-54.
[Lih18] Li, He, Kaoru Ota, and Mianxiong Dong. "Learning IoT in edge: deep learning for the internet of things with edge computing." *IEEE Network* 32.1 (2018): 96-101.
[Rab17] Video "Swarm 2.0. The Living Network of Everyone and Everything," Jan Rabaey, Keynote at Lenaro Connect 2017 < https://www.youtube.com/watch?v=NHnUygY9rj8/ >
[Ral16] P. Ralston, D. Fry, S. Suko, B. Winters, M. King and R. Kober, "Defeating counterfeiters with microscopic dielets embedded in electronic components," in *Computer*, vol. 49, no. 8, pp. 18-26, Aug. 2016.
[Ray14] Ray, Partha P. "Home Health Hub Internet of Things (H 3 IoT): An architectural framework for monitoring health of elderly people." *Science Engineering and Management Research (ICSEMR), 2014 International Conference on*. IEEE, 2014.
[She13] Sheng, Zhengguo, et al. "A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities." *IEEE Wireless Communications* 20.6 (2013): 91-98.
[Swa18] Swarm Lab, https://swarmlab.berkeley.edu
[Tao14] Tao, Fei, et al. "IoT-based intelligent perception and access of manufacturing resource toward cloud manufacturing." *IEEE Trans. Industrial Informatics* 10.2 (2014): 1547-1557.
[Tar12] Muhammad Umer Tariq, Hasan Arshad Nasir, Abubakr Muhammad and Marilyn Wolf, "Model-driven performance analysis of large scale irrigation networks," in *Proceedings, ICCPS 2012*, IEEE, 2012.
[Ton13] TongKe, Fan. "Smart agriculture based on cloud computing and IOT." *Journal of Convergence Information Technology* 8.2 (2013).
[Sch17] P. Schaumont, "Security in the Internet of Things: A Challenge of Scale," Design Automation and Test in Europe (DATE 2017), Lausanne, CH, March 2017.
[Wol15] Marilyn Wolf, Mihaela van der Schaar, Honggab Kim, and Jie Xu, "Caring analytics for adults with special needs," *IEEE Design & Test*, 32(5), October 2015, pp. 35-44.
[Wol18] M. Wolf and D. Serpanos, "Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems," in *Proceedings of the IEEE*, vol. 106, no. 1, pp. 9-20, Jan. 2018. doi: 10.1109/JPROC.2017.2781198
[Yid16] Yildirim M., Xu A.,and Gebraeel N., "Sensor Driven Condition-Based Generator Maintenance Scheduleing Part 2: Algorithms and Validation ", *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 4263-4271, 2016.