Internet of Everything (IoE) focus area

Core faculty: Tom Lee (EE, lead), Philip Levis (CS), Mark Horowitz (EE), Daniel Boneh (CS), Amin Arbabian (EE), Juan Rivas (EE), Boris Murmann (EE)

The exponential scaling of communications networks generally and wireless networks specifically raises the reasonable question of how much longer this trend might be sustained. In trying to discern the outlines of credible futures it is useful to trace the past evolution of wireless. Although history is not destiny, it is nonetheless often true that established and recurrent patterns from the past can serve as a reasonable basis for extrapolations into the future.

The network architecture of Marconi’s spark telegraph mirrored that of the land-based telegraph that it extended, and on which it was modeled. Its station-to-station topology was an artifact of its reliance on a consumer-unfriendly Morse code signaling mode that consequently inhibited both the network’s growth rate and ultimate reach. At its peak, the Marconi system achieved kiloscale connectivity, ultimately managing to interconnect of the order of 10 thousand nodes.

The emergence of station-to-people broadcasting in the 1920s disrupted in the purest sense of this much-overused term. The engineers who created the underlying enabling technologies were as surprised as Marconi at what they had unleashed. The astonishing speed with which broadcasting took off is evident in the very use of the word broadcasting: Engineers struggled to describe a phenomenon that was already approaching escape velocity, and ultimately were forced to appropriate this word from farmers, to whom it still means the spreading of seeds. Today, the most popular television programs are viewed by the order of 10 million people. That is, the 3-order-of-magnitude increase in connectivity accompanying the transition from station-to-station to station-to-people extended the reach of networks to the megascale.

Today, of course, we enjoy 24/7 people-to-people communications. This year, the number of mobile subscriptions will actually surpass the number of humans on the planet (this historic crossover may have in fact already occurred). In round numbers, then, the transition to people-to-people cellular enabled yet another 3-order-of-magnitude jump in connectivity, to the gigascale.

This historical pattern of multiple order-of-magnitude increases in connectivity occasioned by enlarging the circle of conversants stimulates thinking about how one might produce the next such jump, to the terascale. Since, as has been famously observed by Alan Kay and others, the best way to predict the future is to invent it, the IoE focus area begins with the assumption that of the order of $10^{12}$ objects will be connected to each other and to humans, say, by 2035. Working backwards from that assumed future eventuality, we identify what needs to be done today to enable that terascale future. The research tasks that form the core activities within the IoE focus area are informed by identification of both the barriers that need to be overcome, as well as the enabling technologies that need to be developed. What follows is a representative sampling of relevant research derived from that thinking.
Wireless power delivery (lead: Lee, with Arbabian and Rivas)

A terascale network presents a multitude of novel scaling challenges. One of the most prominent is how to supply power to a trillion client devices. Batteries will certainly be part of the solution, but the sheer size of a terascale network presents difficulties. The environmental problems associated with battery production and disposal, as well as the diligence and labor required to replace dead batteries may substantially limit their deployment.

Energy-harvesting methods are an area of active research, both at Stanford and elsewhere, and energy harvesting will certainly be among a portfolio of technologies that address the power problem, particularly well below milliwatt power levels. However, limitation to the sub-milliwatt regime unfortunately precludes many potentially compelling applications. Some higher power needs could be practically fulfilled by conventional hard-wired power supplies, but untethered devices are more versatile. Consequently, a process of elimination compels us to consider wireless power delivery (including for recharging battery-powered devices), for power levels of the order of 10mW to perhaps 100mW (subject to biological safety considerations).

Assuming an aperture constraint of a few centimeters, coupled with an assumed separation of approximately 100m between router and client, frequencies in the range of about 30GHz present a satisfactory balance between enabling narrow beamwidths and possessing acceptable propagation physics. Given that the 24-24.25GHz band is globally available, our initial research is focused on that ISM band. Sub-activities within this research task include development of high-efficiency, CMOS-compatible millimeter-wave RF-to-DC conversion devices and circuits, and low-cost, CMOS-based beamforming architectures intended to support both power delivery and massive MIMO (MMIMO) communications.

![Figure 1. Notional system architecture showing router/basestation supplying power to client IoE devices, in addition to performing the usual communications functions.](image-url)
Circuits, devices and architectures for securing the IoE (lead: Levis and Boneh, with Lee)

A terascale network would present by far the largest network “attack surface” in human history. If the same methods used to secure today’s Internet are used to secure the IoE, we can expect seriously negative outcomes. Somewhat ominously, the current rush to bring IoE products to market has resulted in many products lacking even the most basic protections. Solutions are needed urgently.

The IoE presents an opportunity for a fresh start, for a way to build in security without the legacy burden that constrains current practice. Typical malware payloads are denominated in kilobytes, and have remained roughly constant in size over the history of malware. Anti-malware programs, on the other hand, weigh in at hundreds of megabytes and continue to grow in size. This growing asymmetry is a symptom of a failed approach: The response is not convergent with the threat.

Reliance on software-only solutions is part of the problem. There are a few simple hardware-based strategies that can materially improve security in the IoE era. One of these is to use a processor architecture that prevents the classic “overflow exploit” from succeeding.

Another is the use of an analog random-number generator (ARNG) in crypto engines. All-digital RNGs suffer from the weakness that they can be spoofed readily. An analog RNG, on the other hand, can be constructed in a way that facilitates verification that the ARNG is indeed the source of the random numbers. For example, an ARNG will be affected by supply voltage and temperature in a way that would be cumbersome for an all-digital method to emulate. Furthermore if the ARNG resides on a separate chip, physical verification at low cost is readily provided. Wireless interrogation and/or powering of the ARNG can facilitate testing and verification. We are developing simple (and thus readily inspected and verified), low power ARNGs as adjuncts to IoE client devices as part of an overall security strategy that attacks the problem at a combined hardware, firmware and software level. No approach can achieve 100% security, but a multidisciplinary strategy may reduce the vulnerabilities to an acceptable level at low cost.

Field-programmable things array (FPTA) (lead: Lee, with Horowitz)

The stresses of the terascale expose other potential problems: There may not be enough engineers on the planet to design anything other than an infinitesimal percentage of a trillion devices within the assumed time frame of a decade or two. And even if there were enough engineers, the NRE associated with designing and fabricating a large number of different mask sets would quickly make the enterprise uneconomical.

One strategy for closing the gap and producing more favorable economics is to develop better CAD tools to act as a “workforce multiplier.” It is hoped that an order-of-magnitude reduction in the number of engineer-dollars per design could be achieved this way. That optimism derives from the recognition that IoE devices will share a common core of capabilities: Sensing, computing, communicating and actuating. That high-level similarity can be exploited to reduce the time and cost expended to produce a family of designs.

The effectiveness of that approach can be multiplied many times over by producing a fabric that explicitly acknowledges in its hardware architecture the insight that many IoE devices will share
that high-level similarity. The result of pursuing that line of thought is the field-programmable things array (FPTA):

![Field-programmable things array (FPTA) block diagram.](image)

**Figure 2.** Field-programmable things array (FPTA) block diagram.

Just as today’s FPGA offerings span a range of capabilities and costs, FPTAs would similarly comprise a family of a relatively small number of devices. Mask and design costs could then be amortized over a very large number of units, making it possible to produce devices at low cost in a short time. The field programmability not only allows deferral of personalizing a given device, it also allows post-fabrication upgrades to respond to bugs and security threats on a dynamic basis. The FPTA would embed within it “best practices” for security, freeing the designers from having to become experts in this specialized field. The FPTA would shift much of the design burden away from the relatively scarce hardware engineer, to the far more numerous software engineer, thus producing a better “impedance match” between problem and solution.

**Closing thoughts**

The vastness of the *Internet of Everything* makes it impossible for any one university to solve all relevant problems. That said, we have consciously chosen to address first the most conspicuous impediments to getting to the terascale, and to devise research activities intended to remove those impediments. Solving the problems of powering, securing and designing a trillion devices would have the highest impact of all the IoE activities we’ve identified. We acknowledge that conspicuous by its absence is any discussion about specific applications for the *IoE*. We will revise our list as research proceeds and the opportunities (and needs) presented by particular applications (e.g., biosensing) become more prominent.

**Affiliated faculty**

Recognizing the vast scope of “everything”, the *IoE* focus group includes a number of affiliated faculty spanning multiple engineering and science departments at Stanford including, but not limited to: Tom Kenny (MechE), Roger Howe (EE), Andrea Goldsmith (EE), Shan Wang (MS&E/EE), Kunle Olukotun (CS) and Greg Kovacs (EE).