The Human Intranet – Where Swarms and Humans Meet

Jan M. Rabaey
EECS Department
University of California
Berkeley
jan@eecs.berkeley.edu

***Abstract*— A *Human Intranet* is envisioned as an open scalable platform that seamlessly integrates an ever-increasing number of sensor, actuation, computation, storage, communication and energy nodes located on, in, or around the human body acting in symbiosis with the functions provided by the body itself. This may fundamentally alter the ways humans operate, and interact with the physical world around them. It all starts with concepts that find their roots in the Internet of Things (IoT) and swarm technologies.**

Keywords—IoT, Swarms, Human-Machine interfaces, Body-Area networks

I. INTRODUCTION

There's no question about it—IoT is happening as we speak, and is radically transforming the information technology platform. In the last decade or so, the cloud has emerged as the keeper, transformer, and interpreter of all data, and mobile devices, such as smartphones, have changed how we enter, access, and interact with information. The IoT adds yet another layer to the onion, providing an extremely high-bandwidth channel between the cyberworld (represented by the cloud) and the physical and biological world in which we live, giving birth to terms such as *cyberphysical* [1] and *cyberbiological* systems. For the first time, we can engineer systems that tightly interweave the "real" physical and "imaginary" cyber worlds, often blurring the boundary between the two.

Much has been written about the effects and possible applications of the IoT, covering virtually every aspect of society: industrial and home automation, mobility, energy and the environment, agriculture, safety and security, health and wellness, art, and social interaction. However, the nature of many of the applications envisioned is hampered by the "IoT" name itself. It conjectures an image of many devices connected through a vast network to a "centralized" cloud that acquires and acts on that data. Although this picture might work well for some functions, it misses a great number of scenarios and could act as a hurdle for adopting other functions.

Instead, imagine a world permeated with connected smart devices with sensory, actuation, compute, and storage capabilities. Some might be static devices, while others might move around rapidly—such as those carried by humans or mounted on cars or drones. In such an environment, applications would form by opportunistically marshaling the resources available to them at a given time and place. Such a distributed system is called a *swarm* [2,3], a term that captures the organic nature of cyberphysical and cyberbiological applications better than the Internet-centric IoT concept.

While swarms might consist entirely of non-biological entities (such as clusters of cars on the freeway, or bands of drones in the sky), often they intimately involve one or more humans. In fact, some of the highest-impact uses of the sensory swarm might relate to how humans interact with the physical world around them (and the cyberworld beyond), how they interact with their fellow human beings, and ultimately how they monitor and introspect themselves.

While the proliferation of communication and data processing devices (such as laptops and smartphones) has profoundly changed our interaction patterns, nothing has similarly changed our means of processing inputs (sensory) and outputs (actuation). Many of these interactions are still funneled through a limited set of means (such as displays, headphones, keyboards, touch panels) integrated in a single device. The swarm could change all of this.

Consider the evolution of the smartphone. Over the past decade, it has continuously been accumulating additional functionality in terms of connectivity options and sensory capabilities. Yet trying to integrate all of these into a single device limits both the user experience as well as the application scope. For example, many meaningful signals, such as ECG, are impossible to acquire in a single handheld device. This motivates the various efforts on disaggregating the phone into an ensemble set of separate but connected components, such as watches, bangles, glasses, contact lenses, earpods, and other wearable devices.

In this scenario, which researchers at the Berkeley Wireless Research Center have dubbed the "unPad" [4], the personal communication device is no longer a single entity; it becomes a collection of devices aggregated in true swarm fashion in an organic and opportunistic way. Some of those components can be carried on the person, while the augmented environment around us might provide others. Given the broad diversity of sensory and actuation interfaces offered by advanced technology, these unPads would offer an experience that's substantially richer than what our five natural senses and traditional motor functions (speech, motion) can offer. The

978-3-9815370-4-8/DATE15/©2015 EDAA

potential is huge—think empowered humans in an enhanced world. The nascent field of brain-machine interfaces offers just a glimpse into what's possible [5].

Realizing this potential requires overcoming a number of barriers, many of which are similar to those the swarm is facing, yet may even be more challenging—not only technologically but also in terms of the economical and sociological aspects. In this paper, we will identify some of these challenges and discuss potential solutions.

II. Human Intranet Principles

The transformational opportunity offered by wearable devices has certainly not escaped the industry—or the press [6,7]. Yet the technological solutions being forwarded today bear an eerie resemblance to last decade's sensor-net scenario. Many devices are single-purpose gadgets connecting in a point-to-point link to a smartphone and are only compatible with devices of the same company—again, a true stovepipe model.

Imagine, in contrast, a Human Intranet realized as an open, scalable platform that seamlessly integrates an ever-increasing number of sensor, actuation, computation, storage, communication, and energy nodes located on, in, or around the human body acting in symbiosis with the functions provided by the body itself. The traditional set of senses and interactions is to be augmented by a set of new capabilities, some of which might be hard to even imagine today. Added functionality might be *extrospective* —that is, dealing with the external world around us— or *introspective* —including monitoring, intervention, interaction, and augmentation of human operation. The scope of this *Human Intranet* is not solely confined to the human body, but includes all devices and functions that are within the human's influence sphere at a given point in time. This means that any tool or object that moves with or is carried by a person (such as a bicycle, car, drill, or exoskeleton) is considered a wearable device, and hence is an inherent part of her/his Intranet. Like the swarm, the Intranet develops organically as a heterogeneous mesh of connected nodes (wired or wireless), collaborating to deliver services in a guaranteed way, notwithstanding the stringent environmental, energy, and size constraints.

Again, the vision of body-area networks is certainly not new [8]. Yet the vast majority of the proposed approaches rely either on point-to-point connections or dedicated star networks serving only a single purpose. For the transformative potential to be realized, we need to take a fresh look and harness Metcalf's law. For this, devices must be seamlessly "insert-able" and interfaces must be seamlessly combinable, all while the interaction with the environment is maintained independent of the available connectivity options. In addition, given the personal nature of the information being acquired and transmitted, as well as the potentially life-threatening effects of indiscriminate or malicious actuation/stimulation, any solution should provide rock-solid reliability, safety and security guarantees, in stark contrast to current practice.

To get an idea of what an Intranet might look like, consider the neuro-prosthesis system shown in Figure 1. A network of sensors measure neural activity as related to motor function (using either on-skull EEG or implanted neuro-electrodes). The information is transmitted through a combination of wireless and wired connections to one or more control modules ("hubs"), which translate the intent into actual control signals driving an exoskeleton or a prosthetic device. Those hubs, an evolved version of the smartphone, also support telemetry and direct interfacing with the surrounding environment. Additional sensors could measure EMG signals at various muscle groups or collect tactile feedback from the exoskeleton.

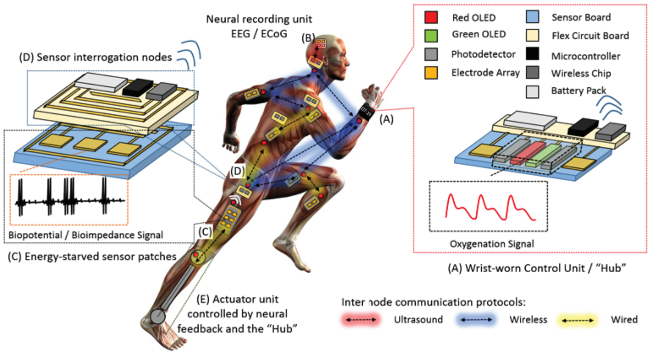

Figure 1. An example Human Intranet configuration targeting a neuro-prosthesis application. An exoskeleton is operated based on information obtained from distributed sensors acquiring neural and other biometric signals. A body-spanning network distributes both information and energy.

This system features many of the properties that are typical for Human Intranet applications: (1) It's distributed over the entire body; (2) It integrates a collection of diverse devices including sensing, actuation, processing and storage; (3) It combines energy-starved (battery-less) devices with energy-rich battery-operated nodes (for example, an evolved smartphone); (4) It exploits a broad range of communication strategies (both wired and wireless), not only for information but also for energy delivery. (5) It provides high-capacity, low-latency connectivity to the surrounding augmented environment. (6) It must be continuously operational for extended periods of time—although the amount of activity may vary dynamically over time.

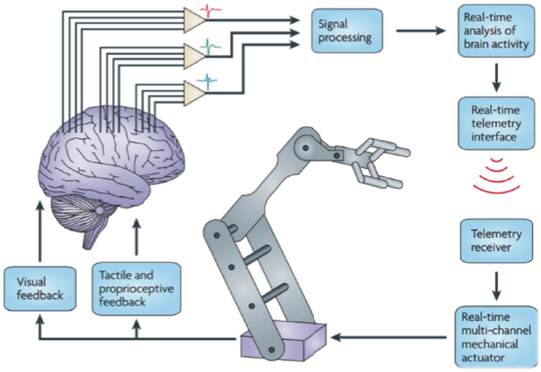
Signal processing
Real-time analysis of brain activity
Real-time telemetry interface
Telemetry receiver
Real-time multi-channel mechanical actuator
Visual feedback
Tactile and proprioceptive feedback

Figure 2. Block diagram of neuro-prosthetic system.

A schematic diagram of the system in shown in Fig. 2, illustrating both its closed-loop operation as well as the tight interplay between wearables and biological functions. It also highlights the various forms of processing that are involved.

Many similar scenarios can be envisioned including humans immersed in virtual reality or augmented environments.

III. Human Intranet Challenges

To realize the Human Intranet, a number of technological challenges need to be overcome, some of which I discuss here.

A. Integrate Energy and Information Distribution

Energy sparsity is one of the central challenges in constructing the Human Intranet. While some nodes (hubs) might have a sizable energy reservoir in the form of batteries or energy-harvesting capability, others might not have any storage and thus would require remotely provided energy when information is requested.

Paralleling, in a sense, the human nervous and arterial systems, network nodes collaborate to form a hierarchical and adaptive mesh that delivers both information and energy. Network links exploit a broad range of connectivity mechanisms, including wired and wireless, electromagnetic, resistive, capacitive, inductive, acoustic, and optical—the choice of which is determined by the local context, that is the location and accessibility of the individual nodes. Using again the biological analogy, a majority of the links are static serving steady-state needs; however, in response to a specific event (similar to a pain impulse), resources can be funneled towards the area of need. For example, a number of nodes may collaborate to beam energy to power a passive sensor node.

The evolved smartphone plays an essential role in this scenario as a hub node. It serves as a bridge to the surrounding world with a diverse set of broadband communication capabilities (5G and beyond). While providing major computation and data storage capacity, it also serves as an energy reservoir for the rest of the Intranet. Devoid of many of its user interface functions of today, its form factor could become really small, rendering it unobtrusive. A believable model of such a hub is presented in a series of videos, called "A Day Made of Glass," created by Corning Glass [9].

B. Distribute System Intelligence

The Human Intranet operates in a dynamic world, subjective to both slow evolution and extremely fast changes in needs, activity, conditions, and composition—both in the surrounding environment and in the Intranet itself. Therefore, the Human Intranet should be constructed as an adaptive and evolutionary system that combines local decision making with centralized global learning and optimization performed in hub nodes. This approach, in which intelligence is both global and distributed, is essential to address issues of latency and single points of failure, while avoiding the trap of many distributed entities with limited knowledge trying to address a global issue.

The central hub nodes are the perfect location to perform long-range and global functions such as feature extraction on the incoming signal stream, sensor fusion, advanced machine learning to extract patterns, and to establish overall operational patterns. Yet, trying to compress all intelligence in the centralized hubs leads to longer response times and brittleness. For instance, beam forming of energy requires tight synchronization, which is hard to establish in a centralized fashion. The same holds for tight control loops. Hence, empowering some of the sensor nodes with ultra low-energy data processing capabilities is of essence.

C. Ensure Fail-Safe Operation

Given the often life-critical nature of its applications, basic or partial functionality of the Human Intranet must be retained under all circumstances, even when resources fail or are insufficient, during system overload, or during denial-of-service attacks. Fail-safety must be built-in from the ground up and should be an inherent property of the basic components and their compositions. Approaches to address this include:

- Baselining: an essential design principle is that every critical function must be able to fall back into a safe mode, whenever resources (energy, communciation, bandwidth) fail or are insufficient. The safe mode should in fact be the default condition, with extra functionality only being added when resources are available. In addition, it should be ensured that this fail-safe mode is reachable from any given state.
- Adaptive and reconfigurable network strategies: One of the prime defense mechanisms in nature (e.g. the brain) against failure or external interference is the capability to remap functions dynamically, and to use the inherent redundancy in the system to reconfigure the system on the fly. This should be an inherent property of the organic nature of the Intranet as envisioned.
- Redundancy: For this adaptive paradigm to really function, it is essential that the Intranet embraces redundancy. Networking and compute resources are to be made available in excess of what any application may need. This is in contrast to the dedicated point-to-point solutions of today, which tend to be brittle and highly sensitive to any failure that may occur. On the other hand, providing redundancy in an energy-starved environment may prove to be challenging.

D. Develop a Human Firewall

Given the personal nature of the information being acquired and transmitted as well as the potentially life-threatening effects of indiscriminate or malicious actuation/stimulation, any solution should provide rock-solid safety and security guarantees. That security and privacy is an extremely hard problem in any distributed system is a well-known fact. Many of the concerns raised in the general networking setting apply equally to the Human Intranet. Yet, the very nature of the Intranet offers some mechanisms that may help to make the problem (more) tractable:

- There is no excuse: every single link in the Intranet should be encrypted. Ultra low-energy design makes this a real possibility.
- This requires a secret and unique way of generating private keys. An attractive solution to this problem is to derive the keys from locally observed features. The Human

Intranet concept offers unique opportunities in that respect, as a number of biomarkers that can be easily collected on the body are unique to that particular human (as proposed by [e.g. 10]). An interesting avenue is hence to explore which biometric body parameters can lead to a "best" combination that is easily constructed on different parts of the body, yet is hard to observe from the outside.

- One of the main challenges of the Human Intranet - weak signal levels on the communication links - can be turned into an opportunity. As demonstrated in [11], it is possible to create a virtual "cloak" through the deliberate generation of noise to spoof eavesdroppers. As the generated noise can be considered "self-interference", it is relatively simple to remove by the internal network nodes.

The integareted set of mechanisms described above – which we have jointly labeled the Human Firewall [12] – can help to ensure that private data circulating in the network remains secure and that the network is protected from external intrusions.

IV. Some High Order Bits

Turning the enumerated Human Intranet concepts into reality requires a broad range of collaborating technologies and solutions that reside at the all layers of the system stack, ranging from devices to circuits, networks and systems. In addition, the Human Intranet paradigm raises a broad range of issues that transcend technology and relate to all aspects of human behavior (including sociology, psychology, privacy, security, and legality). The best way to address these issues is to start the discussion now, when the technologies are still in their infancy.

Acknowledgments

This article is the result of many discussions with a broad group of people—in particular, my colleagues at the Berkeley Wireless Research Center (Elad. Alon, Ana Arias, Robert. Brodersen, Ali Niknejad, Borivoje Nikolic, Vladimir Stojanovic, John Wawrzynek, and Paul. Wright), the Berkeley Ubiquitous Swarm Lab (Bernhard Boser, Bjoern Hartman, Edward Lee, John Kubiatowicz, Eric Paulos, Kris Pister, Claire Tomlin), and the Center for Neural Engineering and Prosthetics (Jose Carmena and Michel Maharbiz). The gracious support of the member companies and funding sources of these centers is gratefully acknowledged.

References

[1] E. Lee, *Cyber Physical Systems: Design Challenges*, tech. report UCB/EECS-2008-8, University of California, Berkeley, EECS dept., 2008.

[2] J. Rabaey, "The Swarm at the Edge of the Cloud," *Proc. 2011 Symposium on VLSI Circuits*, 2011, pp. 6–8.

[3] E. Lee, Ed et al, "The Swarm at the Edge of the Cloud," Design & Test, IEEE , vol.31, no.3, pp.8-20, June 2014.

[4] "The unPad and e-wallpaper", https://bwrc.eecs.berkeley.edu/research/unpad-and-ewallpaper.

[5] J.M. Carmena, "Advances in Neuroprosthetic Learning and Control," *PLoS Biology*, vol. 11, no. 5, 2013; doi:10.1371/journal.pbio.1001561.

[6] B Wasik, "Why Wearable Tech Will Be as Big as the Smartphone," *Wired,* 17 Dec. 2013; www.wired.com/2013/12/wearable-computers/all.

[7] Times Magazine, "Never offline," September 2014.

[8] R. Lauwereins, "Design Technology for Integrated Information and Communication Systems," Competence Center on Circuit Design (CCCD) Workshop, Lund, October 2002, www.es.lth.se/cccd/images/Workshop2002-Lauwereins.pdf.

[9] Corning Glass, "A Day Made of Glass", http://www.corning.com/ADayMadeofGlass/Videos/index.aspx.

[10] M. Li, S. Yu, J.. Guttman, W. Lou and K. Ren, "Secure Ad-Hoc Trust Initialization and Key Management in Wireless Body Area Networks," ACM Transactions on Sensor Networks (TOSN), 2013.

[11] G. Shyamnath et al., "They Can Hear Your Heartbeats: Non-Invasive Security for Implantable Medical Devices," ACM SIGCOMM, 2011; http://dl.acm.org/citation.cfm?id=2018438.

[12] G. Slack, "The Last Firewall," *Berkeley Engineer*, Spring 2014, pp. 8–11.