The Internet of Things... of All Things

A spendthrift refrigerator, a garrulous cellphone, and a loafing automobile, there's a new technology in town everyone's talking about.

By George Hurlburt

DOI: 10.1145/2845143

Mark Weiser envisioned the technology in the early 1990s. As it evolved, people gave it different names: ubiquitous computing, pervasive computing, and ambient computing. Today, we call it the Internet of Things (IoT), a term RFID pioneer Kevin Asthon claims to have coined in 1999. Today, the IoT sits atop the 2015 Gartner Hype Curve for emerging technology. And yet, there is no universally accepted definition of what the "Internet of Things," or a "thing" actually is.

Wikipedia defines the IoT as "the network of physical objects or 'things' embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure." According to Gartner, the IoT is the "network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment." The European Research Cluster on IoT (IERC) gives a slightly different definition, describing it as "a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities, use intelligent interfaces, and are seamlessly integrated into the information network."

THE MODEL

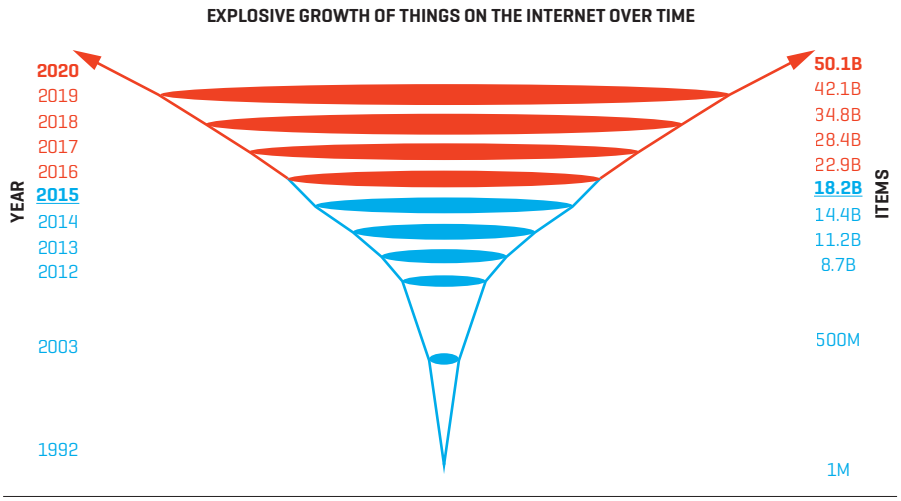
Despite the lack of a clear definition, the technology itself, according to its Gartner status, is very well hyped. The few facts that are known about the IoT, perhaps, justify the hype. The "things" exceeded the number of people on the planet in 2008. By 2025, their number is expected to reach 50 billion (see Figure 1). Its economic impact will be equally massive: The IoT is expected to yield around $11.1 trillion worth of world-wide business annually by 2025, representing a major technology fueled shift in the global economy.

The IoT model involves sensing, thinking, and acting, usually occurring iteratively in that order. The IoT already contains a myriad of sensors, and more are being added every day. Sensor data requires some form of processing, which constitutes the thinking phase of the model. The processed data, then, initiates some type of action.

Humans possess five primary senses: vision, sound, taste, smell, and touch. In addition to these, and independent of them, humans can also

Image by Chesky / Shutterstock.com

Figure 1. The Internet of Things: An explosion of connected possibilities.



detect balance, motion, temperature, humidity, pressure, itch, pain, relative location of body parts, muscle tension, stretching, thirst, hunger, chemicals in the bloodstream, magnetism, and perhaps even time. The IoT can sense everything a human can sense, but also far more.

Sensing. Sensors in the IoT (see Figure 2) can read the entire electromagnetic spectrum ranging from the slowest, low-energy subsonic waves to the fastest energetic cosmic rays. Thus, it can sense frequencies that humans cannot: subsonic and ultrasonic waves, radio waves, microwaves, X-rays, infrared, ultraviolet, and all other forms of ionizing radiation. It can capture audible sounds (hearing) and visible light (sight). Specialized sensors can yield "snapshots," or dynamic streams of information—both audio and video—suitable for human consumption.

Other sensors in the IoT (see Figure 2), many of which are microminiaturized, detect all manner of physical phenomena: motion, direction, acceleration, velocity, rotation, tilt, yaw, roll, pitch, pressure, force, load, torque, position, compression, tension, stretch, strain, vibration, presence, proximity, temperature, humidity, moisture, chemical and gas composition, electrical and magnetic fields, radiation, frequency, flow, leaks, levels, duration, and time—you name it.

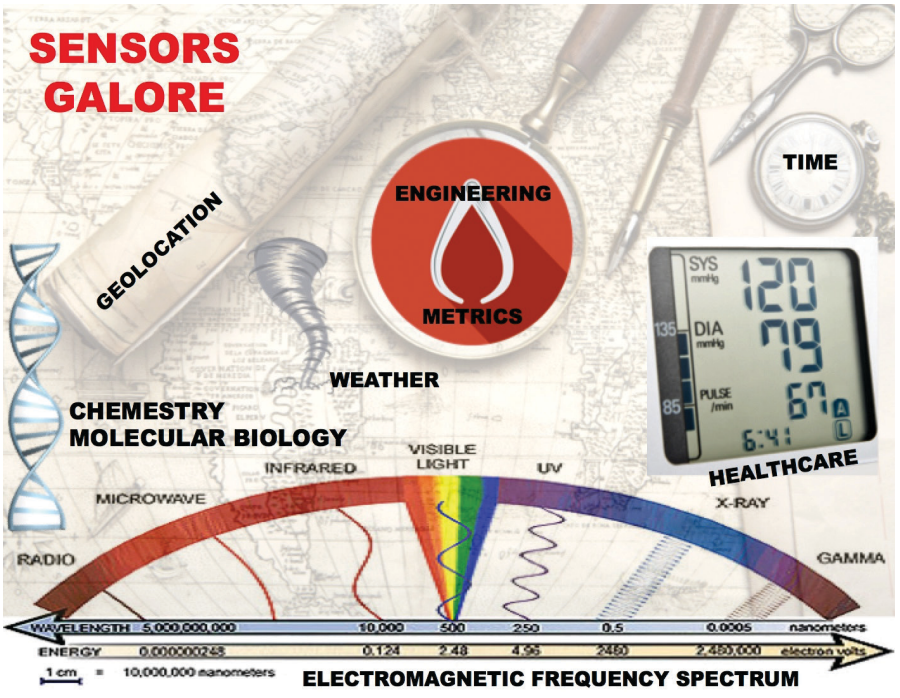
In brief, if a quantity can be measured, there is likely a suitable sensor for it in the IoT. This means the IoT will rapidly become an all-sensing instrument greatly augmenting, yet far exceeding, the range of human nervous sensation. The sensory reach of the IoT is a key aspect of its potential value.

Thinking. Hunger triggers a signal indicating a need to eat. The sensation is transmitted to the brain, which, in turn, interprets the relative urgency of the situation. As urgency increases, the brain transmits interrupt signals that tend to override any other activities. This form of selective processing involves organizing and managing the myriad simultaneous sensory signals hitting the brain at any point in time.

The human brain is a scale-free network of some 100 billion nodes (neurons) with some 100 trillion (10^{14}) connections. It is roughly 73 cubic inches in size. Currently, some 7.3 billion instances of the brain exist, with untold trillions of human-to-human connections [1]. IBM's Watson has 32 core-processors with billions of possible wired connections. It has multiple instances and currently occupies a space equal to three large pizza boxes [2]. In 2011, the Internet was a scale-free network of an estimated 13.5 billion indexed nodes and trillions of connections. The Internet has only one instance, and it spans the entire globe.

Computation has a long way to go before it rivals the human brain. The secret is in the compactness of the brain, which leads to superior wetware computational efficiency borne of connection proximity. This suggests the IoT will be superior to the brain only when its nodes can connect as fast as neural communication Despite Moore's Law, the human brain will clearly hold the advantage for some time to come. This reality refutes some

Figure 2. Sensors galore.



of the high-profile AI doomsday predictors. That is not to say, however, the IoT cannot run amok and create disasters on its own. As we shall examine, that possibility does exist.

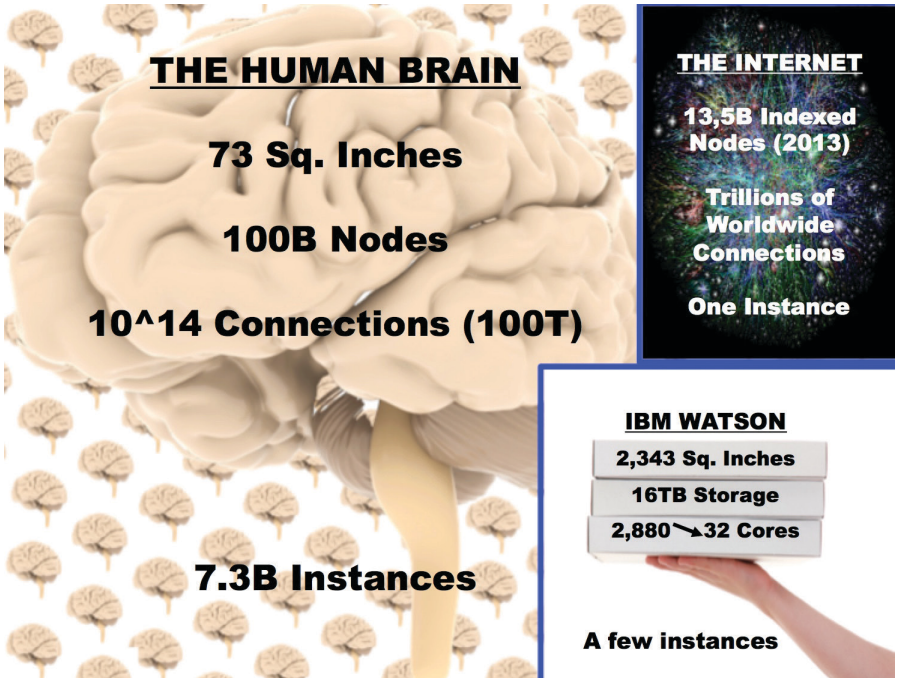
Perhaps the IoT is not the sophisticated computational system many suppose it to be. Indeed, specialized processing is required to handle the output from various devices. Consider the devices that take advantage of various frequencies in the electromagnetic spectrum. These include: Doppler, planar array, monopulse, continuous wave and ballistic radars, light detecting and ranging (LIDAR/LADR) systems, IR and UV sensors, frequency modulated, amplitude modulated and short-wave radio, television, ground proximity system (GPS) satellites, Wi-Fi, mobile devices, and X-ray systems. These devices help humans orient themselves in space, communicate with one another, diagnose diseases, assess various situations, and isolate objects outside direct sensory perception. While these devices may help humans understand and assess situations, in themselves, they do not possess sufficiently profound knowledge to trigger all but the simplest of actions.

This is not to say software is simplistic. In fact, when federated, software forms complex interdependent networks where cause and effect are only indirectly related. This poses a real computational challenge for the IoT. The design and testing of highly interactive sensor-fed software in systems, systems of systems, and, eventually, networks of networks requires deep knowledge of network dynamics. In such networks, the ever-present potential of rigid lockup or a descent into chaos exists, characteristic of complex adaptive systems. Moreover, in the presence of mammoth corporation-halting hacks and ubiquitous malware, there is an immediate urgency for applied systems dynamics and the mathematics they entail.

The level of software interaction, influenced by constant sensor-bombardment, also represents a persistent big data issue. When the inputs are straightforward sensor readings, the volume and velocity aspects of big data apply. Unfortunately, inputs come from many sources in addition to sensor, such as allied software packages in the federation, alien sensors, and human operators. This brings variety into the mix, and the associated semantics calls for veracity. Thus, it is not surprising some forms of dynamic ontology is becoming necessary to deal with abstractions not only within systems, but to disambiguate the software that drives them.

If the IoT is to eventually fulfill the dream of a fail-safe computational powerhouse, network dynamics will have to come into play. In fact, the IoT, by its very nature, represents a large networked system. Interconnected smart homes, buildings, cities and infrastructure grids, autonomous land vehicles and drones, all manner of connected wearables, and integrated health informatics systems are clearly within the realm of networked systems. One issue will obviously be how to place bounds on such immense networks—to preserve security and integrity if not for other reasons—while also allowing necessary information to be shared among them as they begin to overlap into interconnected networks of networks. The IoT, most likely, will not become the singular all-encompassing entity many seem to expect, but rather an amalgam of loosely coupled unique instances.

Figure 3. A comparison of the area, nodes, connections, and instances of the human brain, the Internet, and IBM Watson.



Even the most autonomous of systems need to be told where to deliver their human or systemic payload.

Acting. This brings us to acting. Following our earlier discussion, the meaning of this stage of the model should be fairly evident. If the term "acting," however, becomes "interacting," many additional factors come into play.

While some firmly believe the IoT is all about autonomy, in fact, that is not the case. Consider the example of a smart home. Ideally, it should maintain a constant humidity and tempera-

ture via its servomechanisms. Lights and appliances should turn on and off according to a timetable of events. The lawn would be watered when sensors indicate the need. In reality, however, extreme weather can exceed a system's thermal limits, servomechanisms can fail, schedules vary widely, and water restrictions might draw large fines. Thus, the homeowner is required to spend time and energy regularly interacting with the smart home. Variables outside the realm of the home are constantly at work, requiring some level of ongoing system tweaking.

An autonomous drone in human occupied airspace provides an example on a larger scale. The Next Generation (NEXT GEN) Air Traffic Control system will hardly be autonomous. While many control actions of the human controllers will be transmitted as digital text messages that are readable by onboard systems, humans, nevertheless, remain firmly in control. In the case of autonomous aircraft, the air traffic controller will be in direct contact with the drone's operator, even if the drone is largely flying semi- autonomously.

The famous Google autonomous vehicle, now declared street-legal for testing in California, must still have emergency breaking and steering systems to allow human engineers to override the Bayesian Network controlling the vehicle in case of a pending emergency during road tests [3]. It is highly likely, as road and weather sensors emerge in grid fashion to better inform vehicles of conditions ahead, human over-rides will also be required in the larger infrastructure.

The IoT will be superior to the brain only when its nodes can connect as fast as neural communication .

While perhaps simplistic, these examples illustrate an important point. Sensors may well fuse with programmable, perhaps even self-organizing software, in the IoT. At the end of the day, however, these devices are built to augment human activity and will inevitably require some level of human intervention. Even the most autonomous of systems need to be told where to deliver their human or systemic payload. When confronted with dangerous or unforeseen situations, they will require some form of human decision-making, especially in the design and testing phases, but likely throughout the life cycle. Rapidly changing environmental variables are too plentiful for any other alternative.

CONCLUSION

The IoT human-machine interface requires a multi-disciplinary approach. Not only are computer scientists and software developers needed, but subject matter experts from many fields must also be fully engaged. Nor is it purely up to the neurologists, cognitive psychologists, and anthropomorphic experts to shape the interfaces. Engineers, chemists, and physicists must engage in designs best suited to the intended purpose. Most importantly, functional subject matter experts such as doctors, architects, city planners, forensics people, and many others—including skilled crafts people—must contribute their knowledge to assure a given IoT system accomplishes its purpose. Despite its name, the IoT is not the sole prudence of the computer scientist. Rather, each instance will require a dedicated cross-discipline community working collaboratively under common visions to make the IoT truly effective.

Figure 4. Where the smart IoA stuff will be.

References

[1] Zimmer, C. 100 trillion connections: New efforts probe and map the brain's detailed architecture. *Scientific American*. January, 2011.

[2] Marks, P. Watson in your pocket: Supercomputer gets its own apps. *New Scientist* 222, 2967 (2014), 17–18

[3] Linert, P. Google driverless test cars to have steering wheels, brakes. *Insurance Journal*. May, 2015.

Biography

George Hurlburt is chief scientist at STEMCorp, a nonprofit that works to further economic development via adoption of network science and to advance autonomous technologies as useful tools for human use. He is engaged in health informatics and course development. He sits on the editorial board of *IT Professional* and is a member of the Board of Governors of the Southern Maryland Higher Education Center.