Evolution of the Internet of Things

September 2014

From Connected to Intelligent Devices

INTRODUCTION

The Internet of Things, or IoT, has recently become a strategic priority for organizations in all industries and all parts of the world. As a concept, it is used to describe an ongoing megatrend under which connectivity and intelligence are being added to various physical objects that have traditionally been both unconnected and unintelligent. By adding more and more parts of this "physical-first" domain to the digital universe, organizations can finally expose detailed and accurate data from their previously opaque assets, operations, and end products. In essence, the IoT will turn every industry into a digital industry.

In these early days, IoT deployments typically follow designs that rely more on the connectivity, rather than intelligence, part of the equation. Despite being often labelled as "smart", many of the IoT devices themselves actually tend to be relatively unsophisticated, capturing data through sensors and delivering them to a cloud backend either directly or over a gateway. In such setups, the system's intelligence resides predominantly on the cloud level, and the edge devices are capable of very little processing.

This old way of doing this could be best described as the connected device paradigm. It has proven critical in enabling the IoT to take off, but it should not be seen as the end of evolution for the connected world. There is much more to come.

Table of Contents

ABIresearch®

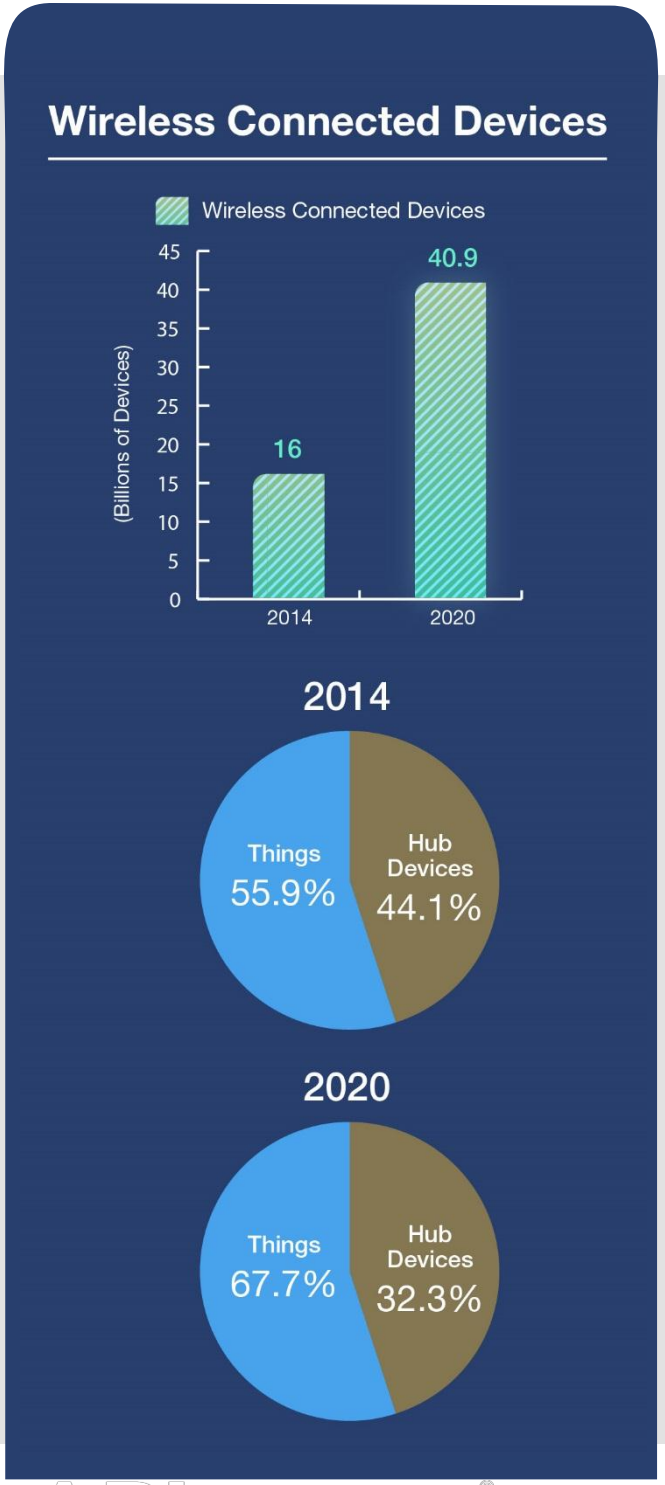
With this whitepaper, ABI Research and Camgian Microsystems seek to explore the potential for a paradigm shift—moving from merely connected to truly intelligent devices—and the benefits it can bring for tomorrow's connected enterprises and other organizations.

THE INTERNET OF THINGS IN BRIEF

ABI Research estimates that there will be more than 16 billion wireless connected devices in active use at the end of 2014. As an installed base, that is about 20% larger than a year earlier. The market size is set to continue its rapid expansion over the rest of the decade, with 40.9 billion active devices forecasted for the end of 2020. The current size and the future growth of the IoT can be best understood by analyzing the composition of this global device pool.

As of 2014, smartphones, PCs, gateways, and other high-performance "hub" devices still account for 44% of the number, but by end-2020 their relative share will have dropped to 32%. On the flipside of this trend, sensor nodes and accessory devices—or "Things", which generally connect with and feed data to such hubs—will increase their share of the installed base from 56% to 68%. In other words, 75% of the connected world's 25-billion-device expansion between today and the end of this decade can be said to come from the IoT.

Importantly, the Things have certain characteristics that make them challenging to deploy and manage. More often than not, they have restrictively compact form factors and need to operate unplugged in difficult locations, so getting them efficiently connected and powered is not an easy feat. Furthermore, as these devices tend to serve business-critical tasks, with direct and even irrevocable implications for the physical world, they need to be also secure and reliable. All this means that inadequately designed devices and poorly planned network architectures can quickly prove counter-productive for the deploying organization.



THE PARADIGM SHIFT: FROM CONNECTED TO INTELLIGENT

As discussed earlier, the first phase of the IoT has been built around the premise that the device's role in the architecture is to serve as a dumb data trap, whereas the actual smarts in the system are kept on the cloud level. This is the *connected device paradigm*. For players involved in the IoT, it has been more of a necessity than a choice. The connectivity problem simply has been solved before the computing problem, so it has made sense to design the early systems in this manner.

Advances to computing, however, are making other types of designs more viable than they have been in the past. This, in turn, is making the available architecture choices more nuanced and allowing pioneering organizations to enhance their products and other physical assets in whole new ways. As a result, the industry is now on the verge of the *intelligent device paradigm*. It comes with three main advantages:

- **Communication Latency**: Handling more processing at the network's edge reduces latency from the device's actions. Use cases that are highly time-sensitive and require immediate analysis of, or response to, the collected sensor data are, in general, unfeasible under cloud-centric IoT architectures, especially if the data are sent over long distances.

- **Data Security**: By and large, sensitive and business-critical operational data are safer when encrypted adequately on the endpoint level. Unintelligent devices transmitting frequent and badly secured payloads to the cloud are generally more vulnerable to hacking and interception by unauthorized parties. Additionally, many enterprises may need to secure and control their machine data on the edge level for compliance reasons.

- Communication Latency
- Data Security
- Total Cost of Ownership

- **Total Cost of Ownership**: Perhaps most significantly, the paradigm shift can reduce the IoT systems' total cost of ownership, or TCO. Intelligent devices are usually more expensive than less sophisticated alternatives, but their TCO over a long service life can be substantially lower. The following two sections of this whitepaper will focus on demonstrating the TCO advantages for a deploying organization.

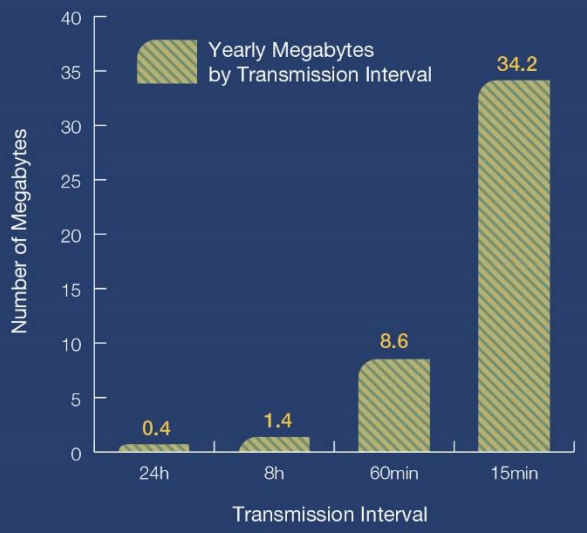
REDUCED DATA FOOTPRINT

Regarding the TCO savings, the ability to handle data closer to the source reduces the associated bandwidth and backend-storage requirements. This is achieved by prolonging the intervals at which the network's devices transmit data, without compromising the objectives of data analysis. Smarter devices make it possible to prompt more complex actions based on the data, as well as to "triage" the data at the source, in order to determine which readings should be sent on for further analysis.

To illustrate, let's assume three device profiles that differ by their transmission intervals. Profile A transmits data four times an hour (*i.e.,* every 15 minutes) and profile B once an hour (every 60 minutes), while profile C transmits three times a day (every 8 hours) and profile D once a day (every 24 hours). Each transmission event delivers 1024 bytes (*i.e.,* 1 kilobyte) of data to the cloud.

As the chart on the right shows, the profile with the highest interval, profile A, will accumulate 35,040 kilobytes—34.2 megabytes—of data over one year of usage. For profile B, the data will amount to 8.6 MBs, while profile C will see 1.4 MBs and profile D just 0.4 MBs. For an enterprise that runs a network of hundreds or even thousands of devices, operating an indiscriminately high-interval profile starts, therefore, adding up quickly in bandwidth and storage costs. Viewed within the context of the global installed base reaching 40.9 billion by 2020, the advantages of distributed intelligence as a means to manage the data footprint are quite compelling.

Yearly Megabytes by Transmission Interval



Now, it is worth bearing in mind that such profiles are highly dependent on the use case of the devices. It would be unrealistic to expect that a time-sensitive use case like, for instance, crowd management could rely on the same interval as a more long-term one, such as predictive maintenance of enterprise assets. However, since already relatively modest tweaks to the intervals can result in large savings over time, moving from, say, profile A to B, or C to D, would make a big difference to the IoT network's TCO.

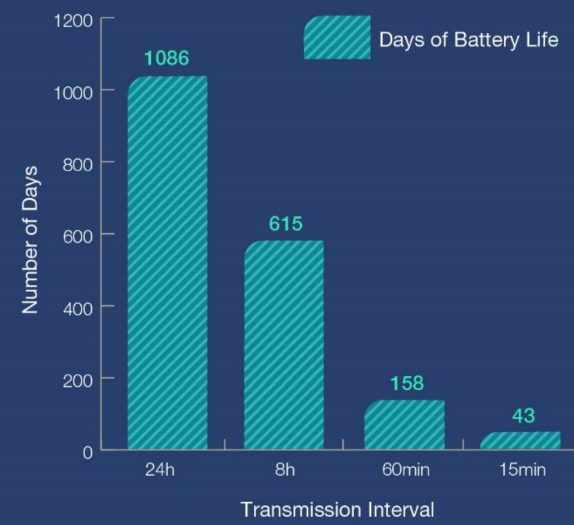
REDUCED POWER FOOTPRINT

Besides cutting down the volumes of transmitted data, the optimization of transmission intervals represent similar—and often even more valuable—benefits in the form of reduced power footprint. Since processing data is, by and large, less consuming on the battery than sending data, IoT-driven organizations can make their device networks more power-efficient by adopting edge intelligence, when it makes sense for the use case.

For the purpose of this quantification exercise, let's assume that the batteries powering the IoT network's wirelessly connected devices have a rated capacity of 6600 mAh, with self-discharge derating this level by 6%. The average current draw while the device is awake is 140 mA with data transmission and 30 mA without transmission. The current draw during the device's sleep mode is 0.135 mA.

These parameters would give profile A, with a transmission interval of 15 minutes, an average current draw of 6.4 mA, which translates into 43 days of battery life. For profile B, the respective figures are 1.7 mA and 158 days of battery life, whereas profile C achieves 0.4 mA and 615 days. Profile A, which transmits data just daily, sees an average current draw of 0.2 mA, allowing it to run on the same battery for 1,085 days—or nearly 3 years.

Days of Battery Life by Transmission Interval



Again, moving from one profile extreme to another is seldom possible, but even fairly modest changes to the intervals can bring large operational gains. This is of particular significance if the deployed devices tend to be located in remote or otherwise hard-to-reach places, considering that asset maintenance is a pronouncedly labor-intensive activity. The more life the enterprise can squeeze out of a single battery, the cheaper it is to run an extensive IoT network. As is the case with data footprint, customizing the profiles to match the deployment's actual needs allows multiplying ToC savings.

CONCLUDING REMARKS

It should be stressed that no single architecture alone can address all possible IoT use cases in a satisfying manner. The cloud will inevitably remain an integral part of the technological landscape also in the future. In the meantime, at the network's edge, the endpoint is not the only part of the connectivity chain that can enable distributed computing and intelligence. The next generation of switches, routers, and gateways should be also considered part of this evolution.

The result, most probably, will be that the IoT will reshape the cloud as a concept into something more local and decentralized than what we are used to. Instead of relying on few vast and geographically dispersed datacenters, the cloud of the IoT era may well be made of multiple small, internetworked cloud clusters and thin clients. They can be local (city-level) or even hyper-local (neighborhood-level), depending on where and when the data ultimately need to be processed.

The key takeaway from all this is that organizations betting on the IoT are finally starting to have real technology choices when planning their approaches. For some of them, the connected device paradigm is still the right one, while for others the most viable way forward is to gear their work toward the intelligent device paradigm.

Moreover, this whitepaper has approached the paradigm shift namely from the practitioner's viewpoint, assessing what benefits it has with regard to individual IoT strategies. That aspect, however, is only one side of the story. Further impetus to the change will come from the pressure that the diversification of connected devices is putting on the companies supplying the end products and associated services.

The cloud architectures underpinning today's smartphones, tablets, and other traditional hub devices are based on the premise that all devices have reasonably short lifespans. The revenue from sold devices pays for the cloud's operating costs, and no device overstays its welcome from the cost perspective. Even if the cloud expenditure overshoots from what was originally planned, the economics can be restored with the next generation of devices.

The longer replacement cycles of IoT products alter these datacenter economics, making the cloud/device equation much more unpredictable. The suppliers can truly end up between a rock and a hard place, if they commit to years of cloud support without knowing reliably how large device revenues they can count on in the future. This factor will, by no means, affect all IoT categories, since there are several of them in which the retirement rates will be less of an issue. Yet at the same time, in many parts of the market, the suppliers will need to put a lot of thought into their business plans, for the cited reasons. By taking advantage of the intelligent device paradigm, they can mitigate the involved long-term risks.

And finally, by distributing intelligence to the edge, the suppliers can open up whole novel product segments that would not otherwise be possible. The shift will be especially important when it comes to making machines and other equipment more autonomous in their operation. For example, unmanned aerial vehicles and various other types of newer robotic machines rely on advanced environmental sensing and a certain level of contextual awareness to perform their tasks effectively and safely.

For this “Internet of Robotic Things,” as ABI Research refers to it, the connected product paradigm is seldom viable, given the fundamental need of these products to sense and interact with their dynamic surroundings with low latency. This cannot be achieved without distributing intelligence to the device level or, alternatively, across a bigger fleet or swarm of robot nodes, depending on the product characteristics.

To conclude, it will be fascinating to follow where the new, “edgier” IoT will take us over the next few years. At least the first signs of the described paradigm shift have been promising, and we at ABI Research and Camgian Microsystems cannot wait to find out what’s next.

Published September 4, 2014

249 South Street
Oyster Bay, NY 11771 USA
Tel: +1 516-624-2500
Fax: +1 516-624-2501
http://www.abiresearch.com/contact/analyst-inquiry/

ABIresearch®