Internet of Things.
Ambient Energy Harvesting

Mikko Lampi

Abstract—The aim of this paper is to compare the physical needs and the energy requirements of processing and communication of the Internet of Things nodes. After demonstrating the hard limits this paper aims to compare relevant energy harvesting methods and select the most likely candidates for IoT use. The three conclusions this paper aims to prove are that for true IoT systems wires will not work, batteries are not sufficient and there are ambient energy solutions that will solve these problems.

I. INTRODUCTION

Internet of Things (IoT) as a term is a bit nebulous and many commercial operators have added their own interpretation of it to the full semantic field of the name. As a term Internet of Things was probably first coined by Kevin Ashton in 1999 [1]. The basic definition of giving an abstract view of a sea of measurement nodes or distributed actuators using Internet like technologies like IP addresses and both stateful and stateless access and routing that is immune and adaptable to the actual physical track the data has to travel.

This initial definition creates a nice dividing line between the current definition of IoT and the pre-1999 solutions built by IBM, Motorola and others. Those older systems were used in smart toasters and controllable lamps, but all of them were connected to a network that had it’s own addressing scheme or was only addressable from the local application that controlled the system.

The RFID people from Kevin Aston’s Auto-ID Center bought into this mix the concept of IP addressable nodes that are not continuously connected, but only transmit data or receive commands when they happen to get in range of an active transmitter. Unfortunately this also further muddies the waters as many IoT RFID devices use their own addressing based on the Electronic Product Codes (EPC) [2] to identify their nodes.

There are other definitions that both overlap and extend the IoT definition both from database manufacturers and distributed network designers. To be able to meaningfully address the power needs of IoT devices, we will have to limit the scope a little.

II. TAXONOMY OF DIFFERENT IoT INSTALLATIONS

Most of the internet of things solutions and ideas rotate around the concept of nodes that can measure and/or control physical things. This yields to a model where we can divide the different installations into different sizes to be able to comprehend their power and data communications needs. Size here means both the number of the nodes and the size of the network needed to connect them.

A. Trivial

1-10 sensors or actuators

- Up to 10 meters of cable, Fits into a briefcase
- All power from the central unit
- All data on the same cables

These kind of installations can be both temporary or permanent. They can be found in portable measurement systems and last generation automobile systems. These are also common in EEG installations and heart rate monitoring. Nodes are powered from the central unit and data communications are done using the same cabling as the power. Controller Area Network (CAN) [3] protocol is an example of this kind of system. Nodes are easy to identify visually and they are often within arms reach of the central unit. Cabling can and is often done with pre-made cables of fixed width.

B. Classic

10-100 sensors or actuators

- 80 m cable reel, can be carried, but not for long
- Power can come from a central system or from local sources
- Data can still use copper, but it is getting hard to do so reliably.

Cabling starts becoming an issue here. It is unlikely that we can use ready made cables so every cable pull from node to node has to be made with cables of at least four strands and a possible protective metallic covering. Each end of the cables needs a connector. This leads to a situation where even a very conservative estimate of 1-5% error rate on connector making means we have at least five broken connectors at start. Also many connectors like RJ-45 type solutions have some form of springs and locks which have a relatively high Mean Time Between Failures (MTBF) value but the sheer number of connections means the probability of problems start rising rapidly.

Data communications over the same cables that move power is still a possibility, but compromises are needed. If the data is high speed (Ethernet) the single cable pull might be limited to 80 m maximum length, and if the data is slow even one kilometer is possible (RS-485).

Even though data cabling is starting to get problematic, getting power cabling to nodes is still possible. This is still limited by the fact that every connector adds around 1 ohm of
resistance and this will degrade the maximum length of cable segments even further if a lot of nodes are on the same cable.

Nodes usually are addressed with some kind of numbering scheme that can be extended to be compatible with IP or is directly IPv4 or IPv6 based.

C. True IoT

100-1M sensors or actuators
- A truckload of RJ-45 cable
- Even pulling power from nearby AC sockets would fill the rooms with transformers
- Data cabling would be a routing nightmare

These kinds of installations solve a myriad or currently hard or impossible to crack problems. Placing a temperature, moisture and CO2 sensor at every wall and and at three heights would create a sensor network that could be used to effectively drive a predicting and stabilizing air conditioning systems. Putting a light sensor and a current sensor on each lamp could make it possible to manage the light effectively an intelligently and brighten and dim it depending on surrounding light conditions. Placing sensors under floor tiles would make it possible to know where people are and adapt the buildings systems to users. This list can go on, but the main point is that the number of sensors bypasses thousands and starts shooting towards millions.

Probability of multiple critical cabling failure almost a certainty at installation time. Connector wear and physical aging will disconnect nodes continuously due to simple MTBF probability. Also the network grows so large that it easily crosses buildings and power grids, creating problems with different ground potentials. Which leads to further complications on installation and during maintenance.

From this we can safely come to the first conclusion that True IoT can not be done using wires. Neither the data nor the power can be transferred over copper wires or we will be limited to systems that in the end resemble the Classic installation.

The next task is to evaluate the power needs of the processing nodes and the data communication to get a rough framework in which we can evaluate our options for power solutions.

III. POWER REQUIREMENTS OF IoT

Powering the IoT nodes is a hedge of compromises. Complex local processing means there is less need for costly data traffic. High speed data traffic means the processing can be done elsewhere but the cost of using the fast wireless long range data connection becomes high.

If the nodes have to shout long distances the energy cost goes up, if the nodes can be chained or used as a mesh network the energy needs can be distributed between multiple units, and the individual distances stay short, but the cost in units and cost in maintenance shoots up.

First we must look at the processing elements and get a rough list of different options. We are ignoring the additional components on the motherboard and the sensors as they fall beyond the scope of this paper. They are expected to be chosen so that they need only a fraction of the power the main cpu/controller needs. Aim is to get an order of magnitude list of power usage costs.

A. Processing per Watt

The example processors are chosen as being typical members of their class. The i7 represents the uncompromising high execution power solution group. The Atom is for the most execution power without drastic compromises. The ARM represents the best division between energy consumption and execution power and the Microchip micro controller represents the systems where energy efficiency is everything and execution efficiency comes always second.

<table>
<thead>
<tr>
<th>Processor</th>
<th>Clock Speed</th>
<th>Power Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel Core i7 2600</td>
<td>3400 MHz</td>
<td>95 W [4]</td>
</tr>
<tr>
<td>Intel Atom D425</td>
<td>1800 MHz</td>
<td>10 W [5]</td>
</tr>
<tr>
<td>OMAP 3430 ARM Cortex 8</td>
<td>650 MHz</td>
<td>0.383 W [6]</td>
</tr>
<tr>
<td>Microchip PIC18F86J60</td>
<td>42 MHz</td>
<td>0.032 W [7]</td>
</tr>
<tr>
<td>Smart sleep</td>
<td></td>
<td>0.000024 W [8]</td>
</tr>
</tbody>
</table>

It is clear the high power processors can be used only on short bursts to do their work. The ARM comes as a middle of the road solution on energy. The sleep or smart sleep functionality of micro controllers is something the more classical processors do not have. It means the unit powers down and stops execution and clocks, but leaves a small bit of logic active on ports which can wake the processor up in fraction of a second to continue execution when something interesting or noteworthy happens.

B. Communication per Watt

The communication solutions also yield easily to five distinct classes. The 3G offers most range and speed but with a considerable cost.

<table>
<thead>
<tr>
<th>Communication</th>
<th>Throughput</th>
<th>Power Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>3G</td>
<td>384 kbps</td>
<td>2 W [9]</td>
</tr>
<tr>
<td>GPRS</td>
<td>24 kbps</td>
<td>1 W [10]</td>
</tr>
<tr>
<td>WiFi</td>
<td>10 Mbps</td>
<td>32-200 mW [11]</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>1 Mbps</td>
<td>2.5-100 mW [12]</td>
</tr>
<tr>
<td>Zigbee</td>
<td>250 kbps</td>
<td>1 mW [13]</td>
</tr>
</tbody>
</table>

Unfortunately as the power needs diminish also the protocols become less and less tested. Zigbee is the clear winner on power and speed, but the IEEE 802.15.4 is very young and has a lot to prove in company of solutions like WiFi and GPRS.

IV. HOW CAN WE POWER IoT?

To remain true to the concept of IoT the power source has to be limited in size. When the number of nodes runs to millions the size and security of the power sources becomes an issue. Due to the problems of getting rechargeable batteries
with modern a chemistry in AAA size or smaller, the example solutions have been chosen among the AA sized units.

On the other hand we can not scale up all that much as a large battery is a serious fire hazard. If we have millions of large batteries distributed around a building they would be a dangerous source of both heat and airborne chemicals when exposed to open fire. Also some batteries (Li-Ion) can explode and shower the neighborhood with molten shrapnel and chemicals when heated by fire. This limits the size of the battery considerably.

Some batteries have a self discharge current. This means that even when nothing is connected to the battery is will slowly empty itself. This is most notable with rechargeable batteries. This also makes a hard limit on how long a battery can be in service no matter the load from the IoT node.

<table>
<thead>
<tr>
<th>Type</th>
<th>Energy</th>
<th>Self discharge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classic battery</td>
<td>1.5 V 4.2 Wh</td>
<td>0 Wh per month</td>
</tr>
<tr>
<td>NiMH battery</td>
<td>1.2 V 0.96 Wh</td>
<td>0.03 Wh per month</td>
</tr>
</tbody>
</table>

The two obvious choices left out are LiIon batteries and fuel cells. LiIon is excluded primarily because of safety. Current LiIon batteries are too dangerous embedded into structures and buildings in large numbers. Also they have a much worse self discharge current. So they will be left out in favor of NiMH batteries.

Micro fuel cells are a very promising technology for IoT devices that need a lot of power, but the fuel cells are still very experimental and hard to get a hold of. Without verifiable numbers and example installations they had to be left out as all numbers would have been pure guesswork.

A. Expected lifetimes

Let us start with the three most likely options: an ARM processor, a 8-bit micro controller and a 8-bit controller using the smart sleep. All three are using Zigbee (1 mW) for data communications which will be added to their power requirement numbers. They are powered by the best energy source the 4.2 Wh single use battery. The power values for the 1:10 smart sleep cycle are calculated expecting a one to ten ratio of sleep and activity.

OMAP 3430 ARM 4.2 Wh / 0.384 W = 0.5 d
PIC18F86J60 4.2 Wh / 0.033 W = 5 d
PIC18F86J60-1:10 4.2 Wh / 0.000124 W = 3-4 y

From these numbers we can see that event the very best battery and the very best controller solution with the very best timing still means that a million IoT nodes will need a maintenance visit every three years. Changing one million batteries, or even just ten thousand batteries every three years is infeasible. No matter the processor technology, no matter the algorithmic solutions and no matter the wireless solution we have to come to the second important conclusion that True IoT can not be built using batteries.

V. AMBIENT ENERGY HARVESTING

The only road forwards is that the True IoT nodes have to be able to feed themselves. They have to be able to gather sufficient energy for operation and data communications from around themselves.

From the earlier calculations we can conclude that the low end of power usage for a IoT node that remains useful is at 124 µW. This means the node sleeps for a second and is activated by an outside trigger for processing and data communications that will not last longer than one tenth of a second. We need to find ambient power sources that can fulfill this energy requirement.

A. Small solar cell outdoors

A small solar cell installed outdoors can easily give 150 mW [14]. It will need a battery to survive nighttime or cloudy days.

It has to be installed into a visible place that is free from shadow. This means it will have to survive different weather conditions from snow to direct rain and withstand dust accumulation. Also a solar cell is shiny and in many countries it tends to get stolen as it has to be installed into a visible position.

B. Small indoor solar cell

Solar cells in inside use are often overlooked as toys or completely ignored. A small unit in unfavorable angle to an incandescent lamp can create 51 µW [15]. If we install three of these we hit our power target of 124 µW. This is very promising.

On the other side we can not guarantee that the lamps will be on all the time. So we will have to install some kind of battery or capacitor that charges from the solar cell and powers the IoT node when lamps are off.

This might lead to considerable problems in buildings that become empty for longer periods of time. For example during a summer holiday.

C. Magnetic coupling with a nearby power line

A very simple power source is to gather energy from power lines that are embedded inside walls. They offer high power when the IoT node is directly on top of the power line. This solution can easily feed even a high power processor. Unfortunately this solution suffers from the square distance law. Even a small increase of distance from them power line reduces drastically the power available for the magnetically coupled node.

Also rather unexpectedly this solution suffers from a version the same problem as the indoors solar cells. The power line gives energy to the coupled IoT node only when some other device for example a lamp is using power from the line. If the lamp or device is switched off or not connected there is no energy flow and so the IoT node can not get any energy. Even when paired with a battery a magnetically coupled unit might run out of energy during a summer holiday when all devices and lamps are turned off.
D. Harvesting radio signals

Most of the available radio signals need a huge antenna to be gathered efficiently. That naturally is not a realistic option for an IoT device. The most realistic case is a smallish (10x5 cm antenna) 10 m from WiFi antenna. This gives roughly 4 µW if the base station is transmitting continuously. This is not enough unless we either go up with the signal strength or use a really large antenna.

If we go up in size of the antenna we also start creating shadows behind us where the WiFi signal is weaker for other listeners. This becomes quickly a problem when the number of IoT nodes goes up. It is also hard to create a design that won’t create problems for other IoT nodes by dampening their transmissions. Even though there are some products on offer that might be used for IoT power use, it seems the solution is not feasible with the current processor technology.

E. Magnetic capture of vibration

A very promising technology is the magnetic capture of vibration. The principle is simple. A magnet is hung from a spring or similar structure and placed inside a coil. When the magnet vibrates due to outside forces it will create alternating current in the coil surrounding it. An example installation produced from a 0.85 mm movement over 180 µW [16] of power. This fulfills the requirement set earlier nicely. This kind of energy harvesting has been used to power measurement systems in bridges. The vibration created by trucks passing powered the measurement nodes in the bridge. It can also be used in tall buildings to gather energy for operations from the swaying of the building in wind. Unfortunately this kind of energy capture usually needs moving parts that can wear out over time. The stiffer and more robust the moving parts the stronger the energy has to be that moves them. This limits the applicability of this technology somewhat.

F. Piezo capture of vibration and strain

Piezoelectric elements can capture energy both from vibration and compression. A Human walking over a large piezoelectric plate can easily produce 8 W [17] during the passing. If we expect the human to pass the plate in half a second producing 4 J and our energy needs derived from 124 µW are 0.446 J per hour leads to conclusion that we need one human every 9 hours to pass the plate to keep the IoT device running. This is a very reasonable expectation. As there is so much excess energy available from the piezoe plate it is logical to pair the plate with a small NiMH battery. This can be kept topped from the element to compensate for the self discharge current. Leading to a system that can survive even summer holidays or long times without any people in the building.

G. Thermoelectric (pellet) capture

In thermoelectric capture the idea is to gather energy from a temperature difference or more specifically heat flow. The elements are small and the output is a simple DC current. As an example Seiko wristwatch produced 22 µW @ 1.5 °C from human body heat [18]. Scaling that up by 10x or 10x temperature difference we can easily get 220 µW which compares favorably with our target of 124 µW. This would be continuous power. Unfortunately buildings are usually designed to minimize places where there can be heat flow between large temperature differences. So finding places where there units can be positioned will prove troublesome.

H. Air movement

Air movement does not need to be gathered with large and visible propellers. Piezoelectric wind turbines can gather energy from passing air rather innocuously. This kind of turbine can be inside ventilation ducts and it can gather energy from the random air current inside building. A small piezoelectric wind turbine can easily get 200 µW [19] from random air movements. Leaving sufficient extra energy to keep a battery topped.

Currently available models are designed for larger energies and are unfortunately bigger than a AA battery, but there is no reason why the technology could not be scaled down and some manufacturers seems to be experimenting with the small turbines.

I. Conclusions

In the first part we concluded that the true IoT can not be built using wires. Both the sheer mass of cabling needed and to multiple problems with physical connectors can cable building make that option too costly and impractical.

In the second part we conclude that even the best processors and best batteries could give us just a few years of usage time. This also is impractical and would limit the installations to Classical systems with limited number of nodes. So another means of energy has to be found for the IoT nodes.

In the third part we demonstrate multiple ambient energy harvesting solutions and list their power output and their problems. From these it becomes evident that ambient vibration and light are the most likely sources to use for true IoT devices.

Next logical step would be to build a demonstration system to measure the power output from vibration and light sources and to gather better insight into how these kind of systems operate and what are their limitations in true IoT use.

References


