SILVAIR

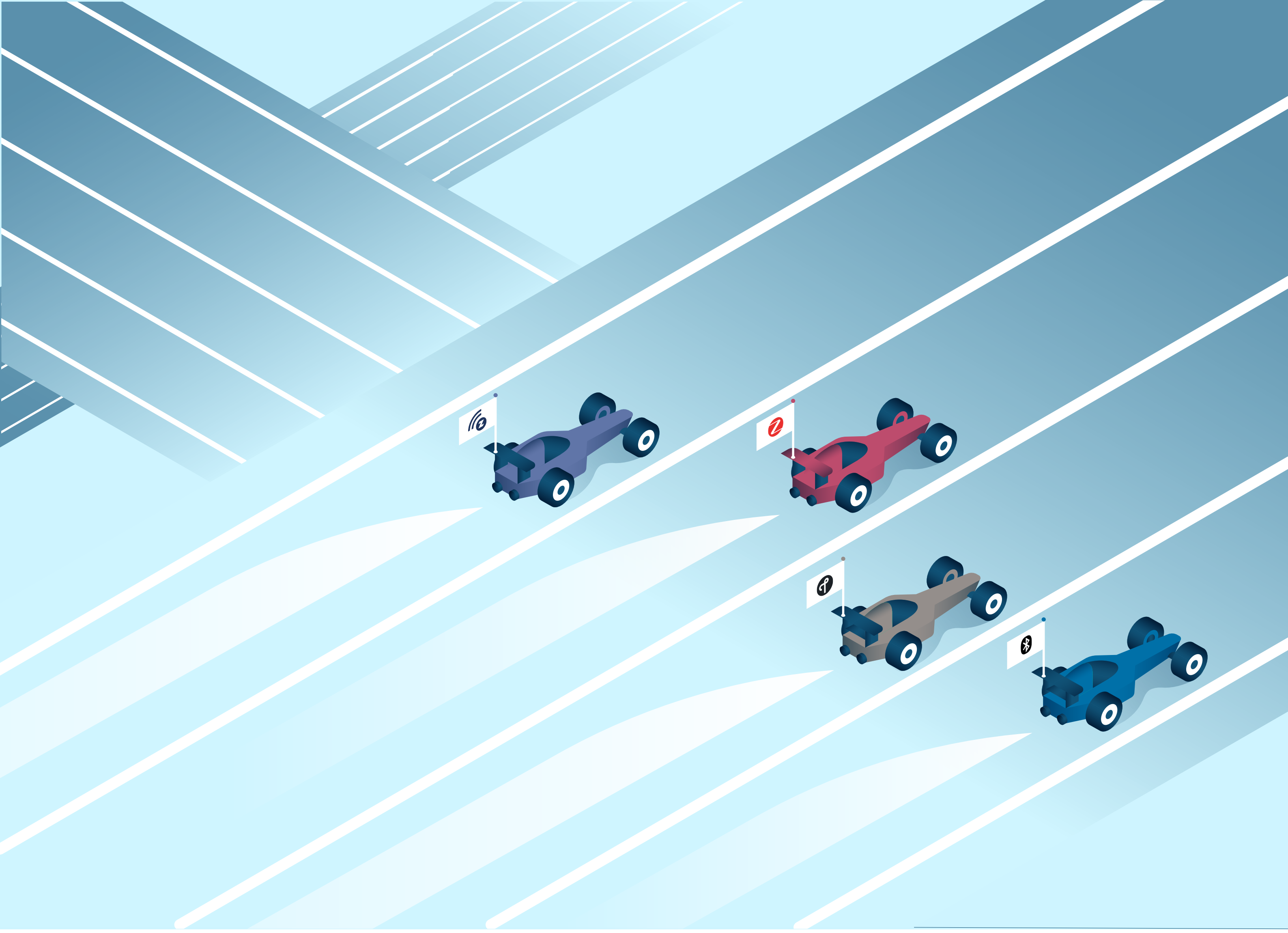
A tale of five protocols

The ultimate guide to the IoT wireless communication landscape

Ebook

Revision **3.0**
February 2018

Table of Contents



1 Introduction: In pursuit of interoperability

Companies venturing into the IoT market are facing some difficult choices. One of the crucial decisions they need to make relates to the wireless communication technology their future smart products will employ.

At the most basic level, the IoT is all about connectivity. The idea is that countless numbers of smart devices are able to communicate seamlessly, producing massive benefits across all aspects of our lives and having a remarkable impact on our society. The reality, however, is still far from that concept. At this early stage of market development, the **Internet of Things is heavily fragmented and lacks interoperability**. A recent **report** from McKinsey Global Institute predicts that the global economic impact of the IoT could reach even up to **$11.1 trillion** per year by 2025, representing **11%** of the entire world economy. But at the same time, it identifies several major obstacles on the road to this IoT promised land. Topping the list is the problem of varying standards which prevent devices and systems from communicating with each other. According to the report, interoperability is required to capture roughly 40% – and in some cases, **as much as 60%** – of the potential value across IoT applications. The matter of interoperability does not revolve solely around connectivity protocols. Barriers also include lack of standard data formats or common software interfaces. **Yet, getting smart devices to talk to one another and interoperate is an elementary need that must be met to make the connected world a reality.**

A number of wireless communication technologies have attempted to dominate the smart home and connected building automation market, but so far none has emerged as a clear leader in this race. Each brings certain attributes to the table, and each approaches the challenge of interoperability in its own way. In fact, the differences between them are often so fundamental that drawing a direct comparison is virtually impossible. And while it's still uncertain whether all the specific needs of various industries and environments can be addressed by a single universal connectivity solution, only the fittest will survive, eventually becoming the global standards for the IoT. This will benefit vendors and end users alike, contributing to further market growth and accelerating mass adoption of connected products.

This situation mirrors the challenges faced by the technology industry in the early days of networking. A number of competing protocols proliferated back then, including IBM's SNA, Xerox' XNS, Novell's IPX/SPX, Apple's AppleTalk and many others, but it was TCP/IP that emerged as the protocol of choice for most networking applications, eventually becoming basically synonymous with the technical definition of the Internet. Without agreed-upon protocols and standards, the Internet and the World Wide Web would not have become what they are today.

With the Internet of Things, history is repeating itself, although on an incomparably larger scale. Eventually, the "things" of the IoT will also learn to communicate with each other, but until that happens, **device makers are forced to make bets in an immature environment**. This creates both certain complications and risks, as well as big opportunities. Some of the communication technologies will inevitably fade away over time, forcing all the companies utilizing them to retool and switch to other solutions, in the meantime withdrawing their products from the market. But those who bet on the winning horse will enjoy all the benefits of being ahead of the curve.

So which of the available communication protocols is most reliable? Which offers the most for manufacturers of smart products, and has the greatest potential to survive the standards war, eventually becoming the go-to technology to connect the IoT? These are some of the questions we will try to answer here. We feel that we've learned several important lessons that we can share on this matter, since we also had to face the same exact dilemma, being fully aware of how significant the consequences of our decision would be. Wireless connectivity is behind everything we do, so we have put an enormous effort to ensure that we know each of the available solutions inside out, and that we are able to identify all of their strengths and weaknesses in particular applications.

Our goal is not to promote one or another communication technology. Our goal is to **make everything connectable**, and interoperability is the only way to get there. So our guide to wireless communication protocols is, in fact, a guide to interoperability. Hopefully, these resources will prove valuable to manufacturers who are aching to get into the exciting market of connected devices, but still hesitate, being unsure of which technology to embrace.

2 Can we talk?

First things first. What are communication protocols and why do we need them to make our homes and offices smart? Simply put, **a protocol is a set of predefined rules that are followed by two or more devices in a network** to establish reliable communication and successfully exchange data between each other. For the Internet of Things to become a reality, an enormous part of this communication has to be wireless, and so a wide range of machine-to-machine wireless connectivity technologies have emerged over the past years. Features most of them have in common include **low energy and low bandwidth requirements**, as this radically extends battery life and allows multiple devices to be used within a limited space. With radio being a shared medium, frequency bands are very scarce resources. In order to accommodate many devices in a given frequency band, the requirement for them to be low bandwidth is extremely important.

Since many popular radio protocols have numerous overlapping qualities, at first glance it might seem that all of them basically do the same job. But as we already mentioned, there are fundamental differences between them. Some wireless communication technologies do completely different things than the other ones, and were developed with different goals and assumptions in mind. This becomes clear once we look at how they relate to the **OSI reference model**.

The International Organization for Standardization (ISO) developed the Open Systems Interconnection (OSI) model back in the 80s to provide a framework for the coordination of communications standards development. To this day, it remains the **primary reference model for network communication**. The OSI framework breaks the network communication process down into a manageable hierarchy of seven layers. Each of them has a specific function and deals with clearly defined tasks, interfacing with the layers located directly below and above it. The 7-layer OSI reference stack looks as follows:

Application

Presentation

Session

Transport

Network

Data Link

Physical

The name of each layer tells a bit about the types of services provided there. We won't describe all these services and tasks at this point; the OSI model has been around for ages and there is plenty of detailed information about it all over the Internet. However, we will keep returning to the above stack in this document, explaining where on the OSI model a particular connectivity solution operates, and what consequences this entails both for end users and manufacturers. That's because the OSI model is where the fundamental differences between individual protocols originate from.

Some of the standards aspiring to connect the IoT define only a small part of the 7-layer OSI reference model, while relying on other available technologies to take care of the remaining aspects of communication. Others go all the way from the physical layer up to the application layer. By itself, this does not make any of them better or worse. What it means is that they are often based on completely different principles, and this is something one should be aware of when trying to answer the question **"which technology will be the best one for my application?"**. Another important thing is that there is no perfect technology. Different applications have different requirements, and there is no one-size-fits-all solution.

Back to the OSI, in order to better visualize this 7-layer concept and how the protocols fit into this model, you can think of it as a framework for communication between humans. This might not be something we pay any attention to, but two persons who want to communicate with each other must share certain clearly specified rules. Just like protocols. Similarly as in the OSI reference model, these rules can be easily broken down into a number of layers. Starting from the lowest one, i.e. the physical layer, humans also need what can be called a physical infrastructure for their communication. In the case of verbal communication, this would include such mediums as voice or sound in general. Human speech organs would also fit somewhere in the lower part of the OSI layer, and as we move towards the top, our communication rules would become more narrow, specifying phones, phonemes, words with their various meanings, grammatical structures, and so on. On top of the OSI model sits the application layer. Applying our loose verbal communication metaphor, the application layer is where context differentiation happens. It is the awareness of who we are, where we are, what we do, etc. that enables seamless contextual communication and exchanging messages in such a way that both parties involved in the process understand a given message exactly the same, and are capable of either relaying it further without any loss in meaning, or taking relevant actions based on the information learned from the other party. This is exactly what we want to achieve when pairing devices with each other for communication and data exchange purposes. To make this contextual conversation happen, **smart devices also need to know what they are, what actions they can take, what states they can be in, how they can be adjusted**, and so forth.

Each of the layers is important and each defines tasks that are integral part of the communication process. They enable communication between devices sharing the same protocol by providing necessary network management and maintenance, security, data exchange, etc. Nevertheless, **it is the application layer that is the key to interoperability**. If the application layer is not defined, devices simply won't be aware of the context of communication, and will never understand each other unless this is somehow agreed between vendors of particular products. This explains why the problem of interoperability relates not only to situations where two devices employing different protocols can't communicate. The thing is that **even if they share the same protocol, they still might not be able to interoperate** if that particular protocol doesn't define the topmost layer of the OSI model.

The more watchful market participants are becoming increasingly aware of how significant the application layer is in overcoming the interoperability challenge that the IoT is facing today. A number of initiatives have recently shown up that aim to address this problem right at the top layer of the OSI model. These include IoTivity or AllJoyn (now merged under one project led by the Open Connectivity Foundation), transport layer agnostic frameworks that sit on top of existing wireless technologies to enable communication across the boundaries of product brands, platforms or connection types. It might be too early to determine whether this is the right approach, especially considering the fact that these solutions are still under development. We'll certainly review them at some point but first let's take a closer look at the most common wireless communication standards of today's IoT.

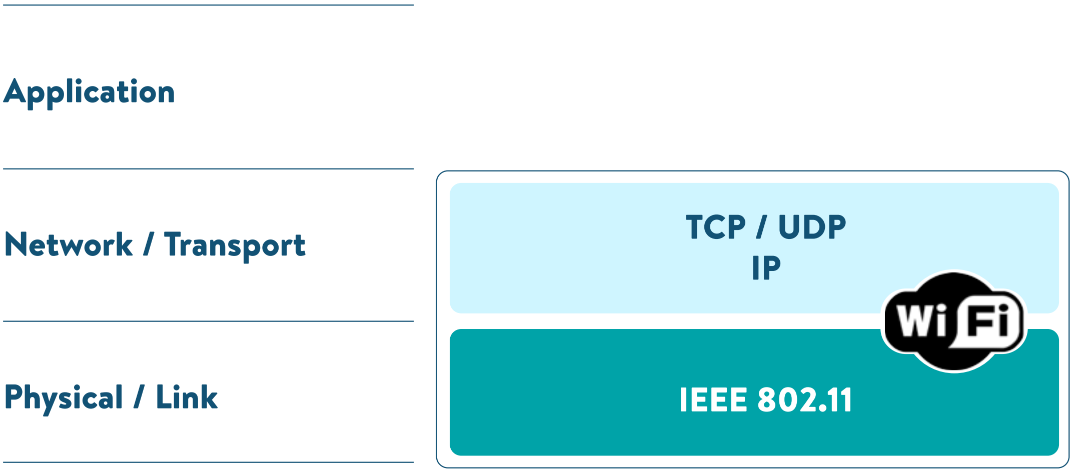
3 Why not Wi-Fi?

MARKET POSITION

What else could we start with but Wi-Fi, a true connectivity classic, and arguably the most globally recognized wireless networking technology. According to the Wi-Fi Alliance, the standard carries roughly a **half of all Internet traffic** for billions of users. It is most commonly used to provide computers, smartphones and tablets with quick and reliable Internet access, but it can theoretically connect any two devices to enable the exchange of data between them. **Widely used in private homes, offices and public spaces the world over, Wi-Fi might seem to be perfectly positioned to take the early IoT market by storm**. And while the dust is far from settling in the IoT communication standards war, this powerful technology is clearly nowhere near the top of the list of today's hottest connectivity solutions for the Internet of Things. So what went wrong? Let us break it down for you.

OSI MODEL

The Wi-Fi technology is based on the family of wireless networking standards IEEE 802.11x. They define only the first two layers of the OSI reference model – the physical layer and the data link layer. As far as the network and transport layers are concerned, Wi-Fi typically relies on other standard protocols, such as UDP or TCP (for transport) and IPv4 or IPv6 (for networking). Let's see what this arrangement looks like on a simplified version of the OSI model:



Application

Network / Transport

Physical / Link

TCP / UDP
IP

IEEE 802.11

Wi-Fi is a powerful and reliable wireless connectivity solution that the technology industry has successfully relied on for many years. The 802.11 has emerged as a global communication standard because it offered numerous excellent features, and was continually developed and improved by the Institute of Electrical and Electronics Engineers (IEEE). As a result of these efforts, multiple versions of 802.11 were developed over time, with 802.11n being the most commonly used in today's homes and offices. **A Wi-Fi network has a star topology, which means that all its nodes connect directly to the central hub, e.g. a wireless router**. With this arrangement, devices can be added and removed from the network without disrupting its entire structure and flow of data. Designed for rapid exchange of high data volumes over reasonable distances, Wi-Fi does that job just perfectly. Basic parameters, such as range or data transfer rate, vary between different 802.11 flavors, but a typical wireless router is usually enough to provide a decent network coverage for a standard apartment. In larger buildings, more access points or signal extenders can be deployed to increase coverage. As for the throughput, some versions of the 802.11 standard have the limit of 11 or 54 Mb/s, but the commonly used 802.11n is capable of transmitting **hundreds of megabit per second**, and 802.11ac is even faster. These numbers certainly look impressive, as the throughput of other wireless connectivity solutions for the IoT is expressed in kb/s rather than Mb/s. On top of that, one of Wi-Fi's major strengths is the ubiquity of 802.11 infrastructure across the globe. The fact that it is commonly integrated into new laptops, smartphones and tablets is also extremely relevant from the perspective of IoT applications.

TOPOLOGY

RANGE

DATA RATE

The features mentioned above is what made Wi-Fi the default technology for enabling wireless Internet access in our lives. It can easily transport high-definition video streams and its throughput limits are usually way higher than the needs of an average user. But the IoT is a completely different thing than the good ol' Internet. The thing is that **Wi-Fi's impressive data transfer rate is overkill for typical smart home/office applications** where instead of data-heavy content, devices broadcast simple commands (e.g. on/off), state-change signals or only tiny bits of information (e.g. sensor data). While such overcapacity is not an issue by itself, there is a cost for this enormous throughput. Being a high-bandwidth communication standard, Wi-Fi is extremely power intensive. This is a big problem in the resource-scarce IoT world where multiple devices are supposed to operate without any wires. In the case of several other connectivity solutions, coin batteries can keep simple wireless devices running for impressive periods of time. But building a battery-powered Wi-Fi device that could operate for any reasonable time with decent responsiveness is virtually impossible. The power-hungriness is

POWER CONSUMPTION

obviously not a big deal if a particular device is permanently connected to power supply, but for all those applications where battery-powered operation is a must (e.g. sensors in remote places), Wi-Fi is just not capable of delivering a reasonable performance.

SINGLE POINT OF FAILURE

Further limitations arise from the topology of a Wi-Fi network. Reliance upon a central gateway to handle all the traffic has one major drawback – **once a hub fails, individual nodes of the network cannot communicate with each other**, essentially making the entire network inoperable. Of course you don't expect your hub to go down all that often, but once it does it can cause some huge problems – especially in commercial settings. Not to mention that replacing a broken hub requires network administrators to rebuild the network configuration from scratch.

COMPATIBILITY WITH SMARTPHONES

On a positive note – as already mentioned, Wi-Fi can be found in every new smartphone or laptop on the market. Out of all communication protocols aspiring to connect the IoT, **only Wi-Fi and Bluetooth have this advantage of being natively integrated into our phones**, making them ultimate controllers for our smart environments. However, in the case of Wi-Fi this potential cannot be fully realized. Even though a smartphone and a Wi-Fi enabled smart device use the same language to communicate, this communication is not direct as it always goes through the network's central access point. This is why Wi-Fi devices cannot use proximity sensing features that have become a trademark of the Bluetooth technology.

ONBOARDING

Given that virtually every potential customer has a Wi-Fi enabled phone, one could assume that setting up a Wi-Fi network of smart devices would be a piece of cake. Unfortunately, this part is a bit tricky. Before a smart device can be added to a Wi-Fi network, it has to know the network's password. This is easy when you want to connect a laptop or a smartphone, but gets hard when your device has no keyboard and no screen. It might seem that a smartphone could do the job, after all it also speaks Wi-Fi – so why not use it to tell the device what the password is? This doesn't seem like a bad idea, but the problem is that the device has to be networked with the phone first, which brings us back to where we started from. Manufacturers use various methods to make this setup process manageable, yet each of them introduces additional complexity and has certain drawbacks. The setup process is one of the biggest problems of the Wi-Fi technology, since flawless user experience is a must if we want to see e.g. traditional lighting systems replaced by smart multi-service lighting networks one day. To address this challenge, some of the vendors have gone so far as to add microUSB ports to their smart Wi-Fi devices solely for configuration purposes. While this effectively solves the setup issues, we are not convinced that light switches with USB ports is where we want the IoT to take us.

INTEROPERABILITY

In the introduction to our guide, we kept emphasizing that interoperability tops the list of challenges which need to be addressed for the IoT to realize its full potential. So what does Wi-Fi offer in this regard? Not that much, unfortunately. As we already mentioned, Wi-Fi does not define the application layer, which means that machine-to-machine communication is basically impossible unless companies manufacturing two particular devices work in close cooperation to precisely define how they can communicate. Wi-Fi is often mistakenly considered interoperable, since we use it all the time to successfully enter into all kinds of interactions with each other. But all these interactions can happen only because there are humans on both ends of the process. Setting up a Skype conversation is what can be described as adding an ad-hoc application layer to the Wi-Fi based communication. Humans can do it by choosing the right tools and coordinating the entire process by themselves. “Things” can’t handle that, and for this reason Wi-Fi is a standard which by itself does not ensure any interoperability in the world of connected devices.

Finally, there is the price factor that always needs to be taken into consideration by manufacturers. Wi-Fi modules are relatively pricey, and although differences have decreased recently, they still remain 50% to 100% more expensive than some of the competing radio modules commonly used in connected devices. This is not something that can be easily ignored when drawing up mass production plans.

Now we need to emphasize that some of the disadvantages mentioned above apply to the majority of the leading communication technologies, just to mention the hub-based topology or the complicated setup process. But what really disqualifies Wi-Fi as the ultimate connectivity solution for the IoT is its power-hungriness. Despite numerous impressive features, it just cannot efficiently support wireless devices, such as sensors or controllers, which are an important part of what the IoT is expected to become.

FUTURE DEVELOPMENTS

It must be noted, however, that the Wi-Fi Alliance is aware of these shortcomings, and is making some efforts to address them. In 2016, the new IEEE 802.11ah standard was introduced. It promised to eliminate many of the limitations that legacy 802.11 technologies struggle with in the resource-scarce IoT space. While some had really high hopes for the “ah” flavor, marketed under the brand name Wi-Fi HaLow, we were skeptical from the moment it was announced. ABI Research **didn’t seem to be sold** on its success either, predicting that only 11 million chipsets would be shipped by 2020. Compare this to more than **100 million ZigBee chips** that GreenPeak Technologies (now part of Qorvo) shipped into the smart home market by September 2015, and you’ll get the idea just how pessimistic ABI Research is on the future of 802.11ah. Don’t forget that GreenPeak was one of many suppliers of ZigBee modules over that time, and that demand for low-power radios is expected to be significantly higher between 2016 and 2020 than it was in the previous years.

Why no love for 802.11ah? A number of reasons, really. While the new sub-GHz Wi-Fi implementation does solve certain major problems of previous 802.11 standards by introducing an extended range and lower power consumption, there are multiple other roadblocks on its path to market success, just to mention the lack of peer-to-peer communication, the requirement for an access point device which becomes the network’s single point of failure, the complicated setup process, or the lack of advanced security features such as key management. Plus, it is just a transport layer, which means that 802.11ah still isn’t able to ensure interoperability even within its own ecosystem - especially considering the fact that its frequency spectrum is not harmonized across the globe. And being an entirely new radio standard it isn’t compatible with all those Wi-Fi routers already present at millions of households and offices across the globe, suddenly making Wi-Fi’s biggest advantage irrelevant. When it comes to IoT applications, 802.11ah certainly is a big improvement over the previous 802.11 technologies, but what it offers is just too little, too late to make any serious impact. And the market seems to share these concerns as Wi-Fi HaLow has not seen much uptake since its debut. There is much more talk these days about yet another Wi-Fi standard, IEEE 802.11ax, which will deliver significantly better spectral efficiency, especially in a congested radio environment. Operating on both 2.4GHz and 5.0GHz frequency band, it is expected to provide backward compatibility with legacy Wi-Fi standards, while at the same time ensuring stunning data rates. It isn't technically ready for commercial release yet, although a number of 802.11ax routers were recently revealed at CES 2018. Some say it will be the most popular Wi-Fi standard of the next decade, offering enormous advantages over e.g. 802.11ac. We say this new flavor is still not a technology that could drive decentralized, information-centric building automation networks that support ultra low power devices and do not have the vulnerability of single points of failure.

That said, there are multiple scenarios where Wi-Fi – even without these IoT-focused improvements mentioned above – can still get the job done really well in the Internet of Things. If you are a manufacturer of a device which needs a reliable connection with the cloud rather than with a dense network of other smart devices, and your product needs to be connected to some sort of power supply anyway, and you manage to find a way to overcome setup challenges to make this process sufficiently intuitive and user-friendly, and you don't care all that much about the price of a radio module since it constitutes only a tiny part of your product price anyway, then Wi-Fi could potentially be the best available solution for you. Otherwise, you should think twice. Wi-Fi is an excellent technology for performing data-heavy activities, such as streaming video content, and it is likely to single-handedly cover this small fraction of the IoT space where such processes are required. But when it comes to smartening our homes and offices, there are simply more suitable solutions out there, the ones that were designed specifically to address the challenging needs of the IoT. In another chapter, we'll take a look at one of them.

4 Riding the Z-Wave

Z-Wave is one of the flagship home automation technologies of the past decade. It's a low-power wireless communication protocol developed to provide end users with an efficient and reliable method to remotely control a wide range of devices and systems. For manufacturers, Z-Wave offers a cost-effective and easy-to-implement solution for making their products smart and connected.

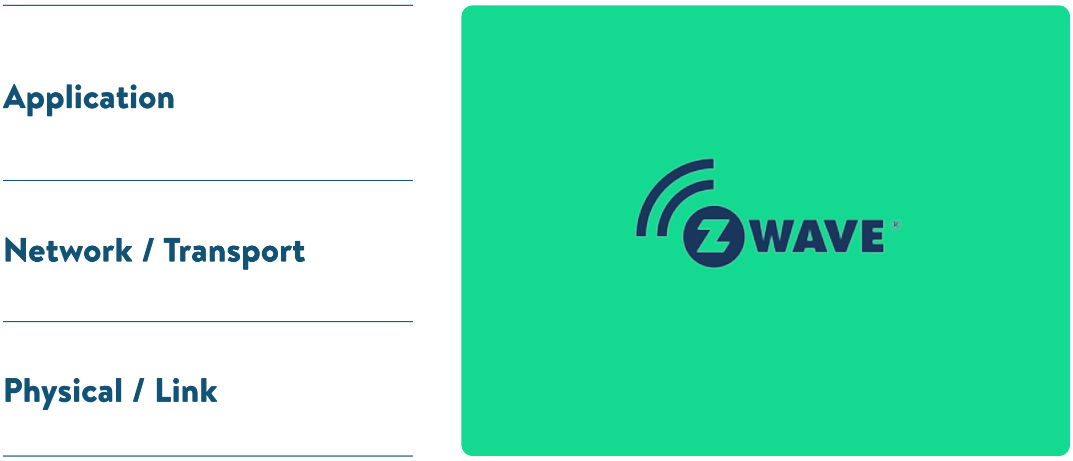
Z-Wave was introduced to the market in 2003 by Zensys, a company acquired five years later by Sigma Designs which licenses the technology and remains the primary supplier of Z-Wave chips. Addressing all the most important needs of the emerging smart home segment, it has become the leading international wireless standard for control and automation in a residential environment. **With more than 1,300 certified devices on the market today**, and approximately **35 million compatible units in circulation**, it is certainly a mature and proven technology. However, its strong market position is now being challenged by a number of solutions that claim to be better suited for the applications it was intended for.

MARKET POSITION

This impressive market penetration might be Z-Wave's biggest strength in the race for dominance among wireless communication protocols. For customers, it means the largest selection of interoperable devices for controlling and monitoring their homes. For manufacturers, it creates an opportunity to deliver products that can easily become part of already deployed smart environments, thereby improving their chances of market success. One could expect that the enormous installed base of Z-Wave devices would create a snowball effect enabling the solution to dominate the entire building automation segment, particularly now when adoption is gaining momentum and the number of connected products on the market is increasing rapidly. However, it must be remembered that technologies come and go, and a strong market presence does not make any solution immortal. What matters in the long run, particularly in the technology industry, is whether a given technology can survive the test of time by adjusting its capabilities to constantly evolving consumer requirements. Fifteen years is a long time, especially for such a fledgling market as home automation. A lot has changed since Z-Wave made its debut, so **the question whether it still remains a reasonable solution for customers and manufacturers is certainly a valid one**.

As mentioned, Z-Wave's strong market presence benefits customers by allowing them to choose from a wide variety of products when expanding or building their smart homes. They can enjoy this freedom of choice not only because of the exceptionally high number of products on the market, but also because of Z-Wave's very unique feature, its **unmatched cross-vendor interoperability**. A quick glance at the simplified OSI model explains it all:

OSI MODEL



Simple as that, **Z-Wave covers all of the layers of the primary reference model for network communications, from the physical layer up to the application layer**. We already know how important the application layer is in overcoming the problem of interoperability in the IoT. Within its own ecosystem, Z-Wave does not have this problem. Unlike the vast majority of leading wireless connectivity solutions, the protocol ensures full interoperability between different branded products based upon it. This wouldn't be possible without defining the **application layer**, but also without the **strong standard** and certification program established by the Z-Wave Alliance. Interoperability is one of the keys to Z-Wave's market success, especially that the protocol also ensures a **complete backwards compatibility** with all previous versions, another unique feature considering its relatively long history.

INTEROPERABILITY

To achieve this, certain sacrifices had to be made along the way, though. A lot of effort was put to ensure that the protocol keeps evolving and its capabilities are enhanced as the time goes by, but the ambitious goal of maintaining backwards compatibility made it impossible to introduce any radical changes. As a result, Z-Wave remains **based on concepts that were developed more than a dozen years ago**.

TOPOLOGY

One of these concepts is the mesh network topology. Z-Wave was designed in such a way as to allow individual nodes to forward messages until they reach their ultimate destination. Significantly extending the range of a wireless network, even today mesh networking is viewed as essential for enabling reliable coverage in building automation. When it comes to mesh, Z-Wave was way ahead of numerous other technologies. Bluetooth, for example, didn't enable such a topology until mid-2017. **Z-Wave has been successfully routing messages over mesh networks for years, although there are certain limitations as to how this communication is handled**.

RANGE

First of all, a Z-Wave network is capable of routing messages via up to 4 repeating nodes. This alone limits potential applications to the smart home environment, since commercial premises and office spaces in particular often require a wider network coverage. With a typical indoor range of Z-Wave modules nearing 40m, a mesh network with a 4-hop limit allows for transmitting data over reasonable distances, providing coverage just sufficient for an average apartment, but **way below the needs of an entire office building or a vast industrial facility**.

SCALABILITY

Furthermore, a **Z-Wave network can have up to 232 nodes, although smaller numbers are recommended to prevent saturation**. While this seems like more than enough for an average smart home enthusiast, it is, again, a serious barrier for a connected office environment where countless devices, sensors and controllers should work in concert to provide real benefits, particularly with regard to energy management. But even in the residential environment, the above limit might soon turn out to be insufficient. **Gartner predicts that within a couple of years there could be more than 500 smart devices in a typical home**, a number that Zensys could not have predicted when designing Z-Wave's architecture almost fifteen years ago.

ROUTING

Z-Wave uses **source-based routing** which means that a device initiating the message generates a complete route through the mesh network to the recipient. Before this can happen, routing tables need to be built. This is done using a device called primary controller which analyses the entire network to come up with optimal routes between its nodes. This **source-routed topology is efficient and reliable as long as the network arrangement remains unchanged**. But if one of the nodes fails, e.g. a bulb burns out or a mobile device moves out of range, the network's topology needs to be rediscovered and routing tables must be updated. The healing procedure takes a while (up to 1-2 hours), and the whole network remains down until it's over. It is recommended to run it regularly during night hours. For some customers this won't be much of a problem, but the fact that your smart ecosystem cannot be operational 24/7 might be an issue in many scenarios and environments. In the more recent versions of Z-Wave, so-called explorer frames were introduced that can be used to solve the problem of missing nodes without initiating the lengthy network healing procedure. However, it has been reported that they often cause the entire network to freeze for roughly a minute. From a perspective of the end user not expecting such enormous delays, this could be a highly irritating experience.

SECURITY

In its early days, Z-Wave was widely considered insecure. A number of successful attempts to break the protocol strongly contributed to this reputation, although it must be noted that some of these vulnerabilities were caused by poor implementations rather than Z-Wave's architecture. Over time, a lot of effort was made to improve the overall security level. As a result, the latest generations of chips feature the government grade data encryption standard AES 128 which requires that a one-time key, commonly referred to as a nonce, is sent along with every message.

This does have certain implications, though. **Balancing security and convenience is a common challenge for technology vendors these days**, but Z-Wave had to pay a particularly high price for ensuring that the exchanged data is protected well enough. While making the entire network significantly more secure and preventing packet replay attacks, the requirement to transport a nonce along with each transmitted message multiplies the communication effort. Before a command can be sent, a nonce request must be transmitted first, and once it is confirmed by the receiver, a nonce itself can be sent which also requires confirmation from the receiving device. Only after all these steps have taken place, the sender can transmit the message, and the receiver can perform a relevant action. Optimized for exchanging small data packets, typical for home automation applications, **Z-Wave offers data rates of 9.6, 40 and 100 kbit/s**, depending on the generation of chips. It is therefore very slow, even compared to other low-power communication protocols. After applying all the necessary security measures, which significantly increase the volume of network traffic, end users often have to struggle with latency issues. In some applications this won't really matter, but there are numerous scenarios where delays go far beyond any acceptable levels. This is one of the reasons why Z-Wave failed to succeed as a reliable solution for lighting control systems where synchronous operation of a set of bulbs requires multiple data exchanges between each of the nodes and the controller.

DATA RATE

LATENCY

It is important to realize that these latency issues stem directly from the architecture of the Z-Wave protocol. In general, all of the leading wireless connectivity solutions for the IoT provide a similar level of security. But Z-Wave had to make particularly big sacrifices with regard to efficiency and user experience in order to reach that level.

What Z-Wave does have in common with the vast majority of wireless communication technologies is that **a central hub must be deployed within a Z-Wave network in order to enable end users to control it with a smartphone**. This is because the protocol is not directly supported by smartphones or tablets, a feature which remains the exclusive privilege of Bluetooth and Wi-Fi.

COMPATIBILITY WITH SMARTPHONES

One last thing that needs to be mentioned regarding the Z-Wave communications model is that the protocol uses an **8-bit checksum with a relatively simple algorithm** to verify the integrity of data exchanged between individual nodes. This is often regarded as one of the major weaknesses of this connectivity standard. With an enormous number of data packets running over larger mesh networks, a weak checksum might not be able to prevent an occasional erroneous transmission leading to a totally unexpected behavior of a smart device. In practice, this means that a light bulb can turn on when not asked to. Or a water valve might open just like that. To address this, a stronger checksum has recently been made available to increase the network's reliability in some more sensitive applications - such as smart door locks - but the market still remains full of devices that come with a not-so-exciting pinch of unpredictability.

INTEGRITY OF EXCHANGED DATA

All of this shows that Z-Wave is certainly not an ideal communication technology for applications that require 100% reliability and efficiency. It also doesn't seem to be ready to deal with the challenges of the future. Things have progressed a long way since it was developed, and it's now showing clearly visible signs of aging despite the fact that the Z-Wave Alliance is putting some effort to keep up with the rapidly evolving IoT reality. An example of these efforts is the **decision made in late 2016** when the Alliance Board of Directors voted to mandate all devices receiving Z-Wave Certification to include a new, more advanced security framework (S2). This decision came into force in April 2017, and according to the Z-Wave Alliance, the new security framework *virtually removes the risk of devices being hacked while they are included in the network*. Z-Wave devices can now be authenticated using a QR or pin-code, and the new security architecture implements the reliable Elliptic Curve Diffie-Hellman (ECDH) key-agreement scheme. Improving Z-Wave's security comes as an important move towards enabling the protocol to be used in professional applications, but there is so much more to be done before it can become a suitable solution for commercial spaces. Also, the recently introduced improvements disable what we earlier called Z-Wave's biggest advantage, i.e. its uncompromised backward compatibility. Fixing Z-Wave's security required introduction of some radical changes to its architecture. As a result, don't expect the latest generation of Z-Wave devices to interoperate with legacy ones. This means the protocol's biggest asset is now lost.

That said, it still remains a perfectly decent solution for smart home enthusiasts who will often be satisfied with their smart home experience despite some of the flaws mentioned above, mainly because their connected environments are relatively small. An average homeowner can enjoy numerous benefits delivered by a smart network of Z-Wave devices, and live through occasional lags or lengthy network maintenance activities. And a random node of a home network performing a random operation once in a blue moon probably won't cause any major disaster anyway. But for these reasons, we wouldn't recommend Z-Wave for those more sensitive applications, such as home security, and certainly not for any type of commercial or industrial purposes.

As far as manufacturers of smart devices are concerned, each of them needs to decide whether this is the market they want to target, and whether this is the kind of user experience they want to deliver. An important question to be answered is whether the unmatched market penetration is a good enough incentive to stick to a solution that has its best years already behind it.

But if Z-Wave's best years are already gone, what the future has in store for this technology and customers using it? This is a very relevant question concerning the fact that 2017 brought some groundbreaking news in this regard. It all started in July 2017 when Sigma Designs published a remarkable **press release** that went quite unnoticed by the market. It informed that the company's BoD had engaged a financial advisor *to assist in its exploration of strategic alternatives that may enhance stockholder value*. Already at that time, Sigma Designs admitted that further moves could include *restructuring, a sale of the company or certain product lines, or other possible transactions*. In October, **another press release** was issued, this time informing about restructuring activities that were supposed to refocus operating expenses and accelerate the return to profitability. Finally, in December the **news broke out** that Silicon Labs - one of the world's leading chipmakers - was acquiring Sigma Designs in what was yet another M&A deal announced in the semiconductor industry in recent time.

What does this mean for Z-Wave? Only time will tell. Some say it's the the start of a new era, others say it's the beginning of the end. Acquiring Sigma Designs will theoretically allow Silicon Labs to produce an ultimate multi-protocol SoC monster featuring Z-Wave, Bluetooth, ZigBee and Thread all at once. But there are multiple problems with such multi-protocol designs that ultimately reduce their usefulness in many of IoT applications. Supporting a wide range of protocols makes much more sense in the case of gateway devices than for system-on-chip solutions. Considering that Z-Wave is not keeping up with today's expectations, let alone future IoT developments, another aspect of that acquisition might be crucial for Silicon Labs. By acquiring Sigma Designs, the semiconductor giant acquires a considerable customer base for its chips. And who knows, maybe one day it will want to convert it into a more future-proof wireless technology. Z-Wave's well-designed and deep application layer could theoretically be decoupled from the underlying radio technology and merged with a more effective mean of wireless data transport. This could be an interesting development opening new opportunities for Z-Wave.

This entire last year's drama shows exactly why global open standards are the future of communication in the IoT. With Sigma Designs remaining practically the only vendor offering chips and stacks for Z-Wave, the protocol - despite its considerable market success - is more of a proprietary solution than an open standard. And just like with every proprietary technology, its fate depends on a number of business factors that affect the entity holding the rights to it. No one will ever acquire truly open standards such as Wi-Fi or Bluetooth, or take them down as part of restructuring efforts. Of course, no technology is guaranteed to last forever. But in the case of a fully open standard, one can be sure that if a particular technology vanishes, it is because of technological reasons. Not because of business-related ones.

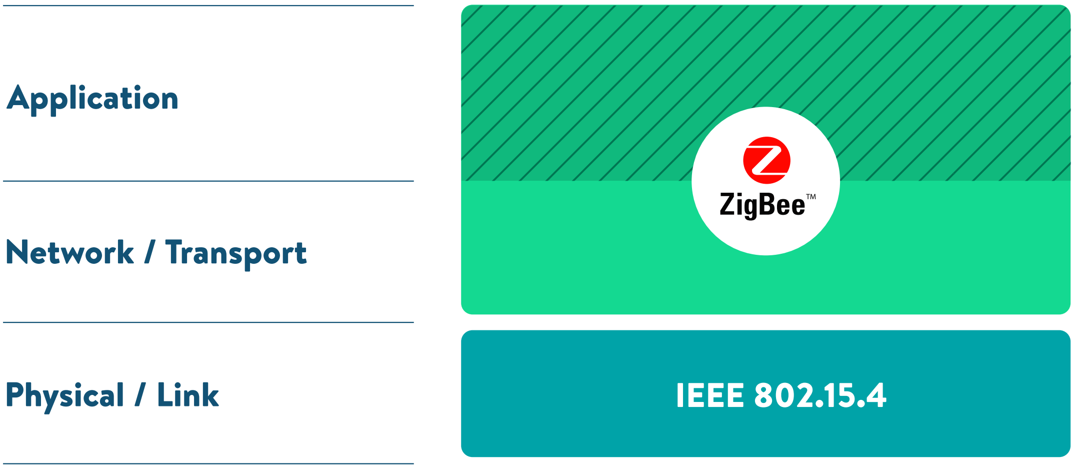
5 ZigBee – is the sting still sharp?

So you already know that riding the Z-Wave might not get you too far if you are a customer or manufacturer looking for a totally predictable wireless communication technology that can be relied upon 24/7. Such a ride can be fun, for sure, but sometimes you just need a rock-solid solution for your applications. The initial excitement that usually accompanies early building automation experiences eventually fades, and what matters in the end is **reliability and a flawless UX**. Now we'll take a look at a machine-to-machine wireless communication protocol that comes pretty close to delivering just that. Being one of the leading contenders in the race for dominance among building automation connectivity standards, **ZigBee has to be on the radar of every company** gearing up for entering the IoT market. Let's see what it has to offer.

MARKET POSITION

Along with Z-Wave, ZigBee is one of the most widely deployed wireless communication technologies in today's smart homes. Both of these standards have an equally long history. The development of ZigBee started in the late 90s, but it wasn't until 2004 that its first specification was published by the ZigBee Alliance. Since then, ZigBee and Z-Wave have been competing with each other, trying to attract early adopters of smart building automation solutions. Both are low-power, low-bandwidth wireless protocols optimized for remote monitoring and control. Both use mesh network topology and target similar applications, although for a number of reasons Z-Wave has failed to reach beyond the residential market, while ZigBee did have a fair amount of success also in commercial and industrial environments. Both technologies might seem almost identical in terms of functionality, but there are certain important differences between them. As usually, the OSI model is where it all begins.

OSI MODEL



CHIP VENDORS

Built on top of the IEEE's physical radio specification 802.15.4, ZigBee's protocol stack defines the network, transport and application layers of the OSI model. The IEEE's 802.15.4 standard is supported by multiple silicon vendors, including the biggest brands in the industry, which creates a **healthy competition environment that naturally benefits their clients**. In the case of Z-Wave, the market is nowhere near as competitive, since the lion's share of these modules are supplied by a single chipmaker. Although Sigma Designs finally decided, following its multi-year monopoly, to grant a license to manufacture Z-Wave chips to another company (Mitsumi), such a drastically low number of technology vendors remains a serious risk for manufacturers. It is also the major reason why Z-Wave is still widely considered a proprietary solution. This is not the case with ZigBee, though, as the technology **meets all the most important requirements to be called an open global standard**.

TOPOLOGY

Within the network/transport layer of the simplified OSI model shown above, ZigBee specifies data routing and forwarding rules that constitute the foundation of its mesh network architecture. While the protocol does support other topologies, it is the mesh networking capability that was the key to ZigBee's market success. Contrary to Z-Wave, which employs a **source-based routing scheme**, ZigBee uses **destination-based routing** to deliver packets to individual nodes of the network. This solves some of the problems that Z-Wave keeps struggling with, making a ZigBee network way more robust, resilient and flexible. Mobile controllers frequently changing their location, burnt-out smart bulbs, or any other devices that suddenly go down for whatever reason are not a problem for ZigBee, as its self-healing network can quickly reroute data packets to ensure they reach destination should any of the nodes fail.

SCALABILITY

RANGE

LATENCY

Another important feature of a ZigBee network is its impressive scalability. Capable of supporting up to **65,000 nodes**, it can provide **enormous coverage despite relatively low range of individual modules** (10-20m indoors). This number dwarfs the 232-node limit that applies to Z-Wave networks, although it should be treated with a certain amount of skepticism. Implementations featuring a four-digit number of nodes have been reported to face significant problems with maintaining smooth network operation. Latency issues tend to occur even in the case of much smaller deployments,

DATA RATE

INTERFERENCE

which is not that surprising considering the fact that **ZigBee's maximum data rate is 250 kbit/s**. Yes, that's significantly faster than what Z-Wave offers, and it might seem more than enough for transmitting simple commands or state-change signals typical for smart building automation. But with a huge number of data packets traveling back and forth over a larger mesh network, the entire system might eventually become clogged, especially considering ZigBee's relatively **low spectral efficiency**. Things get even worse when there is a strong interference produced by other radios. Being a single-channel solution, ZigBee is not always able to effectively combat interference that is common in the **crowded 2.4GHz** band shared by the protocol with such ubiquitous technologies as Wi-Fi or Bluetooth.

That said, ZigBee's data rate still looks absolutely reasonable in the vast majority of building automation applications, at least the ones we can think of today. The future is a different story, though. Analysts predict there will be a myriad of smart devices all around us within a couple of years, and that an enormous scale of connected environments is something that smart manufacturers should start preparing for today. Even in the resource-scarce IoT space, **data rates higher than 250 kbit/s are possible and eventually will be needed**. Bluetooth, for example, is already capable of providing a rate of 2 Mbit/s while being even more energy-efficient than ZigBee, so significantly faster solutions are available even for those manufacturers who want to have their simple smart devices running on coin cells or not requiring any power supply due to energy-harvesting capabilities.

FUTURE DEVELOPMENTS

At some point, ZigBee's throughput limit might become a serious barrier for further development of its ecosystem. The IEEE's 802.15.4 standard, which defines the physical layer of the ZigBee protocol stack, restricts the data rate to 250 kbit/s, and only the IEEE can introduce any adjustments in this regard. Should higher data rates become a necessity, the ZigBee Alliance will have to enter into lengthy negotiations with the Institute of Electrical and Electronics Engineers. The outcome of these talks cannot be predicted, as the IEEE has its own interests and goals. This is where the bodies overseeing protocols like Bluetooth or Z-Wave are in a much more comfortable position. Both of these communication technologies define every single layer of the OSI model, and thus all decisions regarding any aspect of communication are in the hands of a single organization.

MULTICASTING

In addition to mesh networking, **ZigBee also supports multicasting, which means that messages can be distributed to a specified group of network nodes in a single transmission**. However, the technology has been optimized primarily for unicast communications, and there are some important limitations as to how it manages multicasting. To prevent latency issues, **a maximum of 9 multicast messages can be broadcast over a 9-second period**. There are applications where this is clearly insufficient, and smart lighting is a perfect example. Smooth dimming is one of the must-have features for manufacturers of lighting controls. Whenever a smart dimmer is being used, it keeps sending relevant commands to a certain group of lamps so that they can instantly respond by adjusting their brightness to its current position. From the network operation perspective, this is nothing but constant multicasting where just a slight dimmer movement requires multiple multicast transmissions. Zig-Bee's limit of 9 multicast messages per a 9-second period can therefore be reached very quickly, making the dimmer completely useless for the next couple of seconds. Explaining to customers why they can't dim their lights the way they always used to might be quite a challenge for the manufacturers of ZigBee-powered lighting controls.

SECURITY

In terms of security, ZigBee provides a wide range of advanced measures to ensure that the data exchanged between smart devices is protected well enough. With a 128-bit AES algorithm used for data encryption and authentication, and three types of keys used to manage security, end users should have not much to worry about. However, every now and then we can hear some disturbing news about security issues found in ZigBee-enabled devices. This is what happened in mid-2015 when Cognosec **demonstrated** at the Black Hat USA conference how certain vulnerabilities in ZigBee products can be exploited. They related mainly to unsecure initial pairing key transport used when a new device joins the network.

In the statement issued by the ZigBee Alliance, the organization admits that *the hack described by Cognosec is an old one that exists for any system using an open key exchange when joining the network*, adding that it affects many different technologies, not just ZigBee-based devices. One might wonder why this vulnerability still exists if it has been known for a long time, and this is how the ZigBee Alliance explains it: *Security has to fit the application, and schemes are dictated by the resources at hand. It is very hard to enter a 16-digit passphrase into a light bulb when there is no keyboard or monitor. If a scheme is too expensive, too difficult to install, or too time-consuming – consumers won't apply it.* We wouldn't dare to argue with that. We've already mentioned that **balancing security and ease of use is a common challenge in the technology industry**, and that the process of adding new smart devices to an existing network is something that almost all of the leading wireless connectivity solutions struggle with. Bluetooth is in a particularly comfortable situation here, and soon we'll explain why.

The majority of security problems with ZigBee networks have nothing to do with the protocol itself. Despite being able to exploit certain vulnerabilities, even Cognosec admits in its report that *the features provided by the ZigBee standard can be considered as very strong and robust*. The problem is that manufacturers are not obliged to implement all of them in their products. The **ZigBee Alliance does not require device makers to adopt the entire specification**. Instead, they are given the freedom to choose those mechanisms that are needed for their applications. As a result, they often implement only a minimum set of security features required to pass the certification procedure, and such poor implementations is where vulnerabilities usually can be found.

All in all, despite these few shortcomings mentioned above, we must admit we do like how ZigBee handles network communication. With its reliable mesh architecture, it certainly is a powerful and mature technology, one that can support certain professional applications - although its limited scalability eliminates more complex deployments. Still, we would totally agree with its market slogan, *Wireless control that simply works*, if not for one little detail – way too often, ZigBee devices do NOT work with each other. How is that possible?

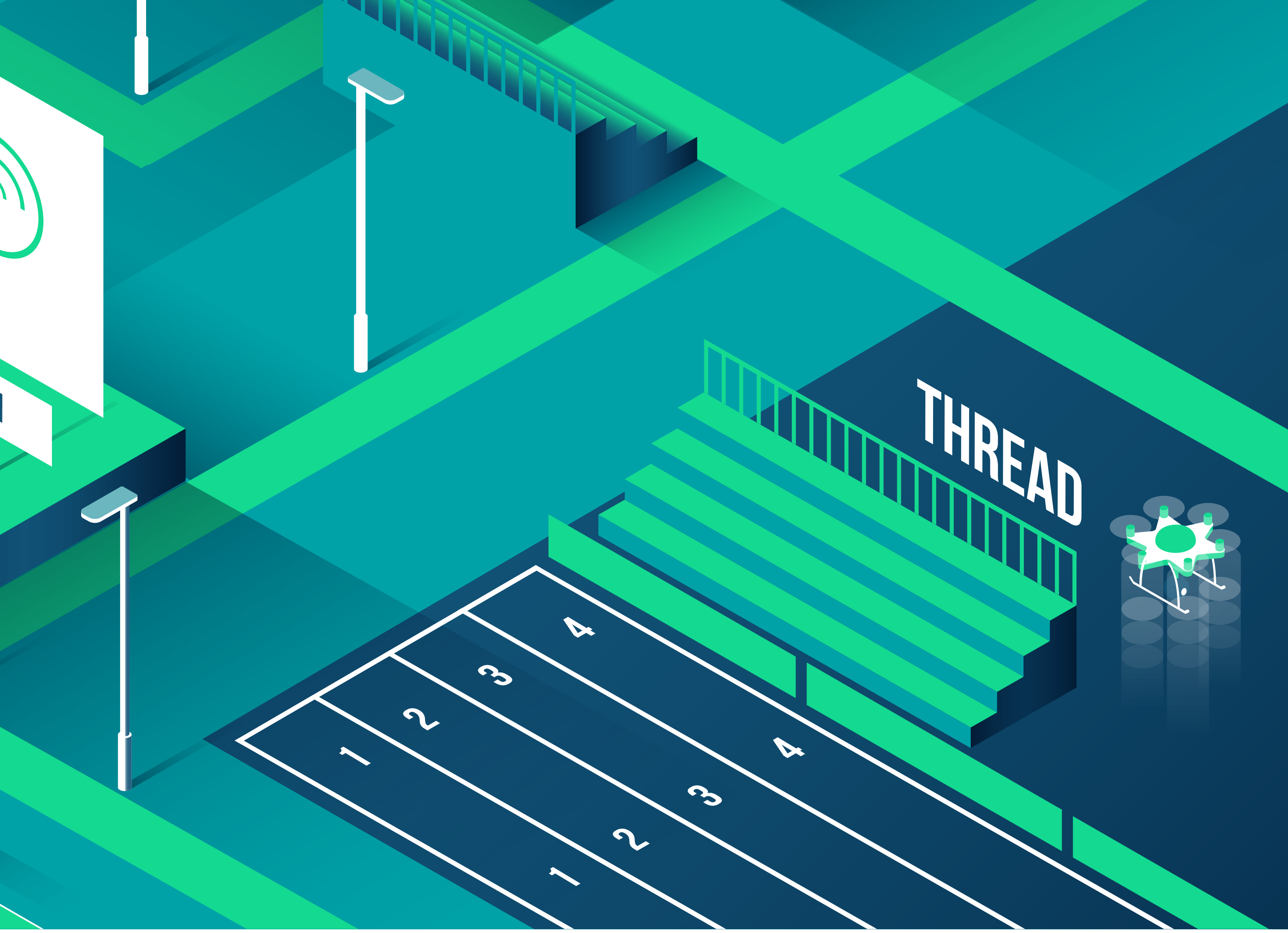
INTEROPERABILITY

If you look at our simplified OSI model again, you'll notice a question mark in the upper right corner of ZigBee's protocol stack. This is because of some serious confusion that is happening at the application layer of this particular communication technology. In order to make it easier for manufacturers to implement ZigBee into their products, and to lay the foundation for cross-vendor interoperability, the **ZigBee Alliance has established a number of standardized application profiles, such as the Home Automation profile or the Light Link profile**. Each of them precisely specifies the pattern of communication between smart devices representing a particular category of products. The Alliance's certification program verifies whether a given product is fully compliant with the relevant profile, ensuring that devices sharing the same profile can talk to each other even if they were manufactured by different vendors. At first glance, this seems like a reasonable idea. But similarly as in the case of certain security mechanisms, device makers were given the freedom to choose whether or not to adopt these pre-developed profiles. And for various reasons, many of them exercised this freedom by building their own proprietary solutions. This is where the ZigBee ecosystem turned into the Wild West of connectivity, with a bunch of application profiles that are not compatible with each other, and a sea of products that are not compatible with almost anything else.

So if you pick two random ZigBee devices off the shelf, chances are they won't be able to talk to each other. One of them might be employing the certified Light Link profile, and the other one could be using the Home Automation profile. Or one of them could be a proprietary solution capable of communicating only with other devices under the same brand. Interoperability was Z-Wave's major strength, but this is clearly where ZigBee's biggest weakness lies. As much as we like ZigBee's network architecture, the ZigBee Alliance completely **failed to address the problem of technological fragmentation**. With interoperability being the single most important challenge faced today by the IoT, how is a protocol that can't ensure interoperability within its own ecosystem supposed to make every thing connected in our homes and offices?

Aware of how significant the problem of interoperability is for the ZigBee ecosystem, in late 2015 the ZigBee Alliance **announced** ratification of ZigBee 3.0, which builds on and unifies the application profiles that had previously been developed, such as Light Link or Home Automation. This was followed by the introduction, in January 2017, of **Dotdot**. It is a rebrand and expansion of the Zigbee Cluster Library which was previously the foundation of ZigBee's application layer. Dotdot is a transport layer agnostic solution so it can potentially be used with different types of radio technologies. The ZigBee Alliance has some ambitious plans regarding Dotdot, calling it *the universal language for the IoT*. For now it seems more like a universal language for ZigBee devices, which is already quite an achievement considering all interoperability problems ZigBee has been facing throughout its lifetime. With multiple ZigBee-based proprietary solutions already in the market, standardization of the protocol's application layer won't produce instant benefits for confused consumers, but in a long run this should improve the overall interoperability within the ZigBee ecosystem.

The decision to launch Dotdot as a separate brand might have other interesting consequences. If it proves successful as an application layer solution, Dotdot could potentially outlive the ZigBee protocol itself. We'll return to this at the end of the next chapter, after we get familiar with another wireless technology that has recently been navigating towards Dotdot. As for the ZigBee & Dotdot setup, with the former technology being responsible for data transfer issues and the latter handling tasks within the application layer, it seems a step forward from where ZigBee previously was. However, this duo still remains a solution that is based on the 802.15.4 physical infrastructure with its single-channel transmission, hub-dependent topology and not-so-impressive data rate. If you ask us, we believe this is simply not enough for ambitious IoT applications of the future. And the pressure on ZigBee ramps up with the recent debut of a very similar low-power wireless communication technology which also happens to be based on the 802.15.4 standard. But that's a story for another chapter.



5 THREADing the way through a connected home

Wireless communication protocols reviewed by us so far have been around for quite a while. All of them were introduced to the market when expectations and hype surrounding the IoT and connected spaces were nowhere near as big as they are today. What's more, certain product categories did not even exist back in the days when ZigBee, Z-Wave or Wi-Fi were designed and developed, with smart lighting being a perfect example of a segment that has come a long way from non-existence to being one of the hottest smart building automation solutions over just a couple of years. While we still cannot be sure what a smart home or smart office will look like 10 years from now, at this point we at least have a rough idea of what to expect – and we **do** **expect** a **lot**.

As you've already noticed, each of those more mature m2m communication technologies has its weaknesses. This is hardly surprising if you consider the above. But quite obviously, the wireless connectivity landscape is not some sort of a dinosaur reserve. There are juvenile predators out there, and one of them has recently attracted particularly strong attention. Let us introduce you to Thread, **a newcomer to the communication standards war**.

The Thread Group was launched in July 2014 with a goal of creating **a simple, secure and low-power network for the home and its connected products**. One year later, technical specifications and documentation were made available to members of the organization to let them start building connected products based on Thread. From the very beginning, **the protocol has been positioned as a connectivity solution designed strictly for the home automation segment**. This might seem like a less ambitious approach than the one taken by e.g. the ZigBee Alliance, but it certainly makes sense. Narrowing the target market should allow the Thread Group to provide a standard that is perfectly engineered to address the needs of a very specific group of customers. And reaching these customers should not be an overwhelming task considering that the organization is backed by some of the most recognized technology firms in the world, including a bunch of the leading chip manufacturers.

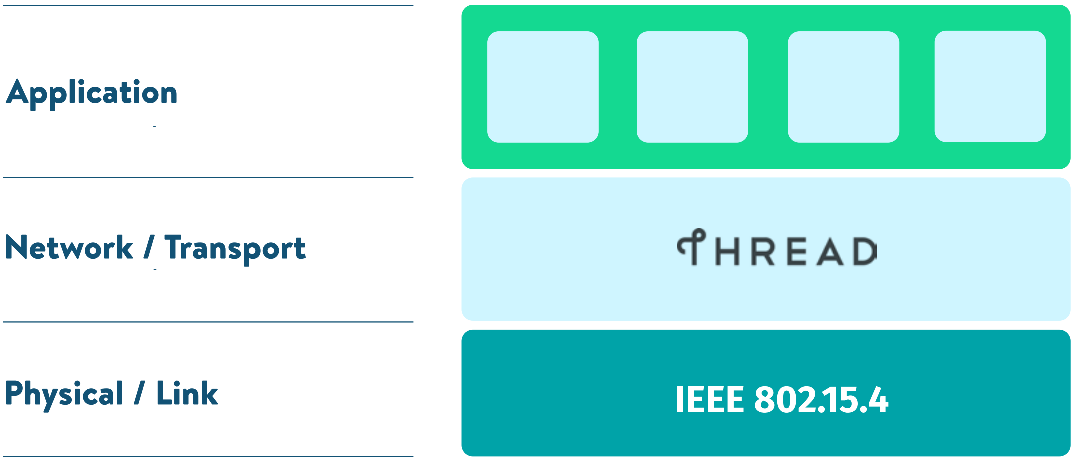
MARKET POSITION

On the downside, arriving to the IoT party much later than several importants competitors obviously has certain implications. Technologies like ZigBee or **Z-Wave had more than a decade to establish market presence and build some level of customer awareness**. As a result, both can be found in more than 1,000 certified devices, enabling wireless connectivity for millions of products that are already in circulation. The Thread Group officially launched Thread in July 2015, with the certification program announced in November same year. The first wave of Thread devices was supposed to debut soon after that, but now it's early 2018 and there are two such products available on the market. Not two thousand, not two hundred, but two. These are Nest Guard and Nest Detect. What's worse, they are not even *Thread Certified* products. They are *Thread Ready*. What is the difference? Just recently, the Thread Group **expanded its test program** to include the *Thread Ready* designation for specific applications. The move is highly controversial and could have a profound impact on the future of this technology. While the T*hread Ready* concept makes it easier for manufacturers to implement some of the features of Thread-based networking, it is likely to fragmentize the market even further and might simply break the standard. That's because *Thread Ready* products won't have to include all of the core Thread features, and won't have to be recognized by *Thread Certified* devices. This all seems like the ZigBee history repeating over and over again. Is lowering the entry barrier for manufacturers worth it? We believe it's not, because we do believe in interoperability. And the entire *Thread Ready* program looks to us like a desperate attempt to keep Thread hot despite the fact that things have been progressing glacially slow so far.

Good news is that several Thread-supporting SoCs have recently been launched by semiconductor companies, which is a condition that has to be met before a wireless technology can make any sort of market impact. Nevertheless, Thread has lost a lot of its traction since the big announcements made in 2014. But to be honest, it's hard to blame the Thread Group for this epic delay. This is what often happens with similar initiatives – which really shows just how complicated and challenging the entire wireless environment is. Time is money, though, and time also means the market share. Competing standards are working on big improvements all the time, just to mention the adoption of the Bluetooth mesh specification which took place in mid-2017.

That said, with the IoT-driven building automation technologies still at the beginning of the technology adoption curve, it seems there is enough space and time for a new technology to succeed – as long as it is able to effectively address the industry's major challenges. Is Thread that kind of contender? Let's begin with a simplified OSI model:

OSI MODEL



Let us quickly explain what is going on in here. **Thread runs on top of the well-known radio standard IEEE 802.15.4**, the same that forms the basis of every ZigBee network. The protocol itself defines only the network and transport layers of the OSI model, addressing such issues as routing, commissioning or security. **It does not cover the application layer, as it was designed to work with a variety of different application layer protocols**. Now what does this all mean in practice? Let's break it down, starting from the bottom of the OSI model.

DATA RATE

SCALABILITY

Being based on the 802.15.4 physical infrastructure, Thread adopts **all its strengths and weaknesses** that we've mentioned when reviewing the ZigBee standard. The former include reliable radio performance, reasonable range and support for low-power applications. As for the weaknesses, the 802.15.4 is a single-channel solution with a maximum data rate of 250 kbit/s. It is therefore not surprising that a Thread network becomes saturated when it reaches **approximately 200 nodes**. This has to be a bit disappointing considering that Thread made its debut almost a year after Gartner predicted that a typical family home might soon accommodate more than 500 smart devices. Whether or not Gartner's forecast will turn out accurate, 200 nodes is really unimpressive. Thread has the ambition of becoming the go-to technology for connecting and controlling a smart home with all its appliances and systems, including such applications as lighting, energy management, security, climate control, etc. If you try to count all of the nodes of such a network, you'll quickly realize that Gartner's predictions are not as exaggerated as they might seem at first glance. So the question remains how Thread is going to handle those extensive sensor-driven implementations. And again, we need to mention that just like the ZigBee Alliance, the Thread Group does not have any direct control over the 802.15.4 which is maintained solely by the IEEE.

At the same time, it should be noted that Thread's reliance on the 802.15.4 standard is not as strong as in the case of ZigBee. Therefore, it doesn't seem impossible to have its networking mechanisms implemented on top of a different type of radio. In certain scenarios, this could enable the Thread Group to overcome some of the current limitations of the IEEE's 802.15.4 technology.

TOPOLOGY

On top of the 802.15.4, Thread delivers a self-healing, secure, IP-based mesh networking solution that allows end users to easily bridge their devices to the Internet so that they can access a variety of cloud services. The **IPv6 connectivity** is enabled by 6LoWPAN, a technology for sending and receiving IPv6 packets over the 802.15.4 radio, which is one of the major advantages that Thread has over ZigBee. Thread introduces important improvements also with regard to the onboarding process, i.e. the act of adding a new device to the network. We've already emphasized how challenging this issue is, and how various technologies struggle with it (remember Wi-Fi switches with microUSB ports solely for configuration purposes or security holes in initial pairing key transport that were found in ZigBee implementations?). Thread standardizes this process by enforcing manufacturers to attach numeric code labels onto their products that are later used by end users during onboarding. This might not be the most convenient procedure, but it does make commissioning more secure and manageable than what we got used to when working with 802.15.14 networks in the past.

ONBOARDING

Moving to the top of the OSI model, we finally get to the application layer. As an **application layer agnostic technology**, Thread leaves this space completely empty. Support for different application layers has been promised by the Thread Group, so we can expect gradual integration with certain existing solutions. However, this concept leaves us a bit confused about how the Thread Group plans to address the problem of interoperability. With the application layer being key to interoperability, individual application frameworks supported by Thread won't be able to communicate. Ad the fact that Thread is an IP-based standard does not help much, either. By itself, IP connectivity enables seamless communication only when there is a human being on both sides of the process, selecting the right tools for specific needs. Devices cannot do this and thus they cannot talk to each other unless they are given very specific instructions on how to organize this process. This is what the application layer is needed for.

INTEROPERABILITY

There is one more important thing that needs to be mentioned with regard to the topmost layer of the OSI model. Communication protocols that define the application layer also define the rules for cooperation between different companies using a particular technology. This means that a manufacturer of e.g. Bluetooth light switches does not need to enter into any kind of agreement with a manufacturer of Bluetooth bulbs in order to launch a product that controls these bulbs. By deciding to employ Bluetooth or Z-Wave, each producer automatically agrees to become part of a broad ecosystem where devices from different vendors can interoperate without any legal restrictions. **Thread does not define the application layer and the rules for communication between devices, and so the legal framework for potential cross-vendor interoperability is also missing**. This is a strictly business problem, and manufacturers of certain types of devices need to figure out by themselves how to deal with it.

BUSINESS AGREEMENTS

With Thread being such an immature technology, it's really hard to guess at this point what its future is going to look like. At first, it seemed like a natural successor of the ZigBee standard, building upon the solid (but not too exciting anymore) foundation of the 802.15.4 technology, while introducing certain important improvements in such critical areas as security or commissioning. Things got even more interesting when the Thread Group announced that 802.15.4 devices already in circulation would be able to start running Thread via a simple software upgrade, which means that a part of ZigBee's considerable installed base could theoretically switch to Thread. And while we've heard from chip vendors that the Thread stack is pretty heavy and thus can be handled only by the latest generation of 802.15.4 modules, Thread's capability of snatching some of ZigBee deployments could sound like a real challenge for the ZigBee ecosystem. On the other hand, the ZigBee Alliance and

FUTURE DEVELOPMENTS

the Thread Group **announced launching a friendly cooperation** to enable the ZigBee Cluster Library to run over Thread networks already in mid-2015. Since then, the cooperation between the Thread Group and the ZigBee Alliance has strengthened even further, with members of both organizations demonstrating prototypes that run the ZigBee application profiles on Thread networks **in late 2016**. If that's not enough, in December 2017, the Zigbee Alliance and the Thread Group announced the availability of the Dotdot specification over Thread's IP network. Could Dotdot become a default application layer for devices running on Thread? To be honest, we like the Thread+Dotdot combo much better than the ZigBee+Dotdot one. From a technological perspective, ZigBee has no advantages over Thread in terms of wireless data transfer efficiency. It has a number of market advantages, but market position is not what makes a wireless solution capable of dealing with future IoT challenges. Still, such patchwork solutions don't come without certain drawbacks.

If you look at Dotdot-over-Thread, these are two separated layers, two different technologies with different requirements. Yes, they can be tied together, but there is always a price to pay. This might be the commissioning process, which in such case has to be performed separately for the application layer and the transport layer. Or configuration/maintenance complexities resulting from the fact that you need different sets of tools for adjusting core networking features and for adjusting the way devices interact with each other at the application layer. That said, the Dotdot-over-Thread arrangement is probably the most capable solution you can currently built on the 802.15.4 radio. This doesn't mean it's the best low-power connectivity option for the IoT. But combined with a strong support from major chipmakers, this should be enough to make some sort of a market impact. It will be interesting to see how the Thread-Zigbee love story evolves, and what role Thread will play in the IoT without its own application layer. It will be even more interesting to see how this close cooperation will affect ZigBee. Assuming that Thread finally establishes some market presence, manufacturers will need really good reasons to choose Dotdot-over-ZigBee instead of Dotdot-over-Thread. And it's hard to imagine that the ZigBee Alliance isn't aware of this. If you ask us, we feel like both the launch of Dotdot and the constantly strengthening cooperation between the Zigbee Alliance and the Thread Group shows one thing - that ZigBee is just getting old. And that the ZigBee Alliance is now focusing its marketing activities on the application layer (Dotdot) because this is where it might be successful in the future IoT. As a mean of wireless data transfer, ZigBee is just not efficient enough to meet the enormous expectations accompanying the connected revolution. While not perfect, Thread is hands down better.

Is it good enough for high-density networks often found in commercial spaces? This seems doubtful, since the underlying 802.15.4 standard is not dealing with heavy network traffic efficiently enough. In applications like building automation, a wireless technology needs to handle large-scale, sensor-packed networks. We expect these networks to constantly collect and analyze large amounts of data, while at the same time ensuring wire-like responsiveness of critical systems, such as the connected lighting infrastructure. This just seems too much for Thread unless some deep changes are introduced into the architecture of the 802.15.4 technology. And nothing is known about the IEEE's plans in this regard. Despite this fact, and despite its initial focus on the residential segment, the Thread Group at some point announced its intention to expand Thread beyond the connected home. The body plans to overcome the challenges awaiting in the commercial environment by adding extensions to the existing specification. Issues to be addresses include enterprise commissioning options and support for large subnets. The latter should enable some degree of scalability but is this going to be enough considering how quickly the 802.15.4 standard is ageing today? We won't find out until the extensions are published. And there is no official information on when this could happen. It's been almost two and half years since the Thread specification was published, and there are still no products on the shelves. How much time will pass between commercial extensions are adopted and the first professional Thread deployment shows up? And where the IoT is going to be at that time? We don't even dare to guess. And the fact that these commercial extensions are needed shows that Thread is not capable of supporting professional applications in its current shape.

There are multiple scenarios that could possibly unfold for Thread over the coming months - or perhaps years - that will determine its future position in the IoT market. We do appreciate the enhancements it introduced to make the 802.15.4 a more viable choice for manufacturers and customers alike, but at the same time we are disappointed with limitations that apply to Thread due to its reliance on this particular radio technology. And we certainly are concerned about interoperability issues, as Thread doesn't bring much to the table to solve them. In fact, the recently launched Thread Ready program suggests that interoperability isn't on the Thread Group's priority list at all. It seems the market will just have to wait and see how things continue to evolve, particularly with regard to Thread's certification program, application layer policy, extensions for commercial use cases, and complicated relations with the ZigBee technology.

6 Bluetooth: a technology in transition

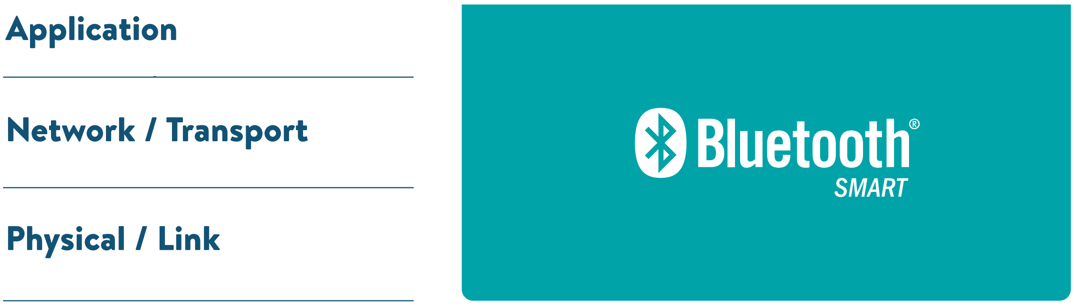
The history of the original Bluetooth standard started back in 1994, which makes such dinosaurs as ZigBee or Z-Wave look pretty young. One might wonder why such an ancient technology is even being considered for all these innovative IoT applications. After all, when reviewing Z-Wave, we concluded that this 15-year-old solution has failed to keep up with the rapid evolution of the IoT – so how could Bluetooth be a viable choice if it was first developed before the term "Internet of Things" was even coined? A short answer is that **Bluetooth of today is something completely different than Bluetooth of the past.**

The original Bluetooth, known as Bluetooth Classic, was designed as a short-range, cable-replacement technology for point-to-point communications. Initially, the main goal was to synchronize data between mobile phones, but the standard quickly became a default technology for wireless data exchange between personal computing equipment (mobile phones, PCs, PDAs) and various peripherals (headsets, cordless keyboards and mice, printers and such). Devices could form a tiny personal area network (PAN) called piconet, where a single central device would coordinate the activity of up to 7 active peripherals. Bluetooth Classic certainly did the job it was intended for, although we've all probably had some mixed experiences with it. Especially in its early days, the user experience was far from ideal, the process of pairing devices would sometimes end up being a bit frustrating, and the transfer of data would drain the battery very quickly. But that's past.

Fast forward to 2010, the Bluetooth Core Specification version 4.0 is released, introducing Bluetooth Low Energy (BLE), more commonly known as Bluetooth Smart. This is where the story of Bluetooth in the Internet of Things really begins. Bluetooth Smart was **designed specifically to address the needs of a new generation of smart devices**, many of which are battery-powered and thus require fast connection times and efficient power management to reduce unnecessary energy consumption. This extended Bluetooth's usefulness to a whole new range of products, ultimately making it a go-to technology for all kinds of wearables. And while Bluetooth Classic still remains part of the Bluetooth Core Specification, it doesn't have much use in the IoT universe – so let's forget about it for a while. Whenever we mention the name of Bluetooth from now on, we'll mean Bluetooth Smart.

Interestingly, even though almost 8 long years have passed since Bluetooth Smart made its debut, there is still a lot of confusion in the market about what it is capable of, and what applications it fits. And rarely is it even considered an option for smart home or smart office environments. There are reasons for that, and we'll try to explain both what these reasons are, and where the Bluetooth technology stands at the moment. Traditionally, the simplified OSI model is what we'll begin with.

OSI MODEL



Pretty much like Z-Wave, Bluetooth covers all of the layers of the primary reference model for network communications, from the physical layer up to the application layer. So the Bluetooth Special Interest Group (SIG), the body which oversees the development and licensing of Bluetooth, has the rare privilege of being able to introduce any modifications to the standard directly and independently. This allows the SIG to respond to market developments and customer needs in a timely manner, **making Bluetooth way more agile than other leading wireless communication technologies**. We'll get back to the SIG later on, now let's focus on the protocol itself.

Out of all low-power, low-bandwidth communication standards, **Bluetooth has the best radio**. Period. This might seem like a bold statement so we're certainly open to discussion, but the facts really do speak for themselves. And why is the radio performance so important? Because of what the IoT is expected to become. Even today, when we think of e.g. commercial smart lighting systems of the future, one thing is certain - we need to think big. A smart office building of the future is a different story than a smart home of the future. And if Gartner predicts 500 smart nodes in a smart home, then how many smart nodes we should be prepared for in a smart office building? Thousands of them, including LEDs, occupancy sensors, photosensors, and looking even further ahead - potentially also all the smart components of e.g. the HVAC infrastructure. To get prepared for that, we need a technology that can provide extremely fast and reliable transmission of data, even in a network with thousands of nodes.

POWER CONSUMPTION

LATENCY

But what exactly influences the speed and efficiency of transmission? First off, the data rate. This one is pretty obvious. **Data transfer rate is one of the crucial parameters for extensive mesh networks**. The higher it is, the faster data packets reach their destination – freeing up radio waves, minimizing the occurrence of radio packet collisions, and preventing network saturation. A higher data rate means lower duty cycle, which directly translates into longer battery life - and Bluetooth's support for sleepy nodes (devices that spend most of their time in sleep mode, wake up only to quickly perform their task, and then go back to sleep again), simple smart "things" such as sensors or switches can keep running on tiny coin cells for years. But above all, a higher data rate means **lower latency and better responsiveness** – something that is critically important e.g. for lighting control systems. Especially in the commercial environment, latency must be kept close to none. LEDs simply *must* respond immediately to occupancy sensors' detection of presence. And they must respond instantly to on/off/dim commands sent from wireless switches. Commercial smart lighting won't take off unless such a seamless, no-latency communication can be provided.

DATA RATE

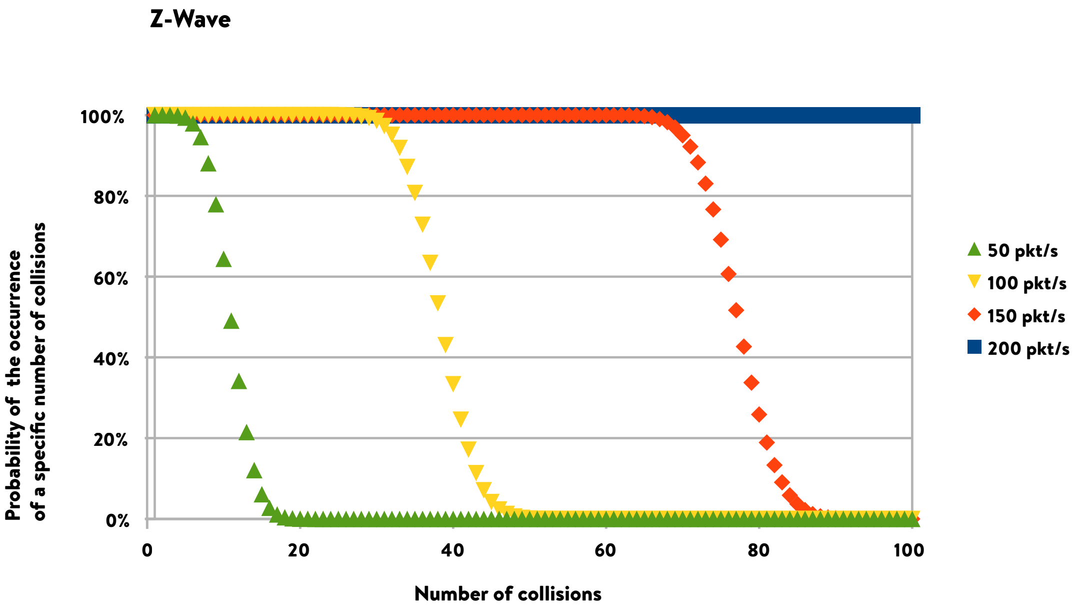
SPECTRAL EFFICIENCY

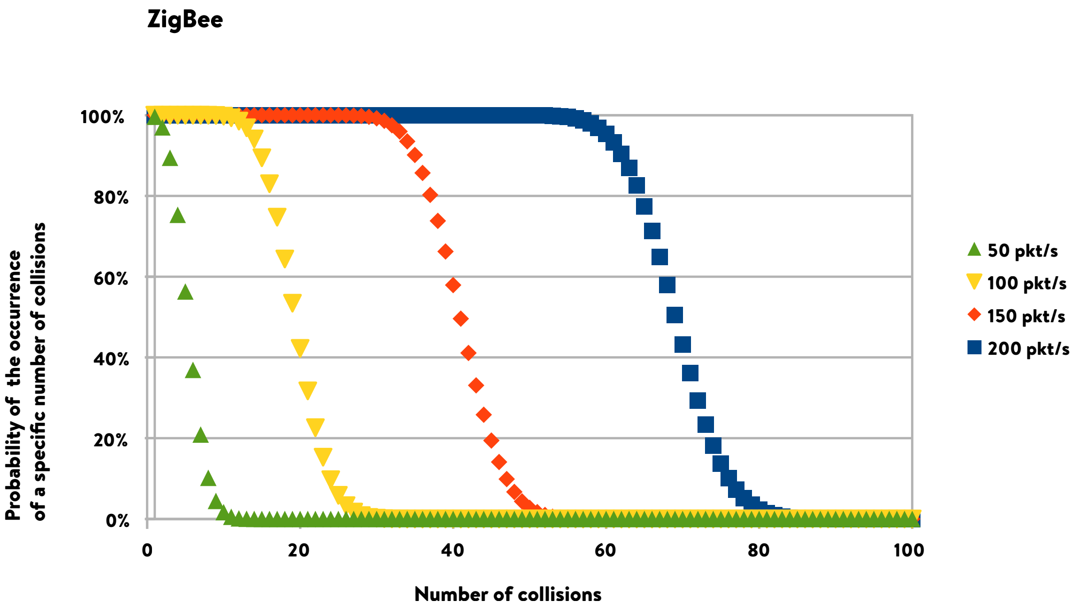
In terms of network robustness, Bluetooth Smart is head and shoulders above the rest. The secret to its performance is the fact that the protocol has been **optimized to transport very large amounts of very small data packets**. Exactly what is needed in IoT applications. First of all, it is capable of transferring data with a rate of **1 Mbit/s** (and higher, but we'll get to that later on). With its maximum throughput of a mere 100 kbit/s, Z-Wave can offer only one-tenth of Bluetooth's data rate. All of the 802.15.4 radios, including ZigBee and Thread, are also significantly less efficient in this regard, as their maximum data rate amounts to 250 kbit/s. As for data packets' size, it must be remembered that each data packet includes **payload and overhead**. The former is the essential data carried within a packet – the core message that is conveyed so that other network nodes can act upon it. The overhead is all the additional information that is required to make the message reach its destination. This includes security mechanisms, certain networking procedures, potentially also some sort of routing data (if a routing technique is applied). Radio communication requires overhead for effective, secure communications and interoperability. It ensures that appropriate encryption and authentication measures are applied, and that the integrity of transmitted data is maintained. So on the one hand, overhead must be capacious enough to ensure reliable and safe communication, but on the other hand we want to keep it as small as possible – since the size of overhead obviously affects the size of the entire data packet which, as already said, must remain low to minimize collisions. Just another example of contradictions typical for the resource-scarce IoT environment. Unfortunately, most of wireless protocols are loaded with overhead. This makes messages occupy massive time slots on a given frequency, which is the easiest way to saturate such dense networks as commercial smart lighting systems. Bluetooth again stands out from the rest here, proving that proper network design can minimize overhead and improve the overall network performance, while not compromising on security or manageability.

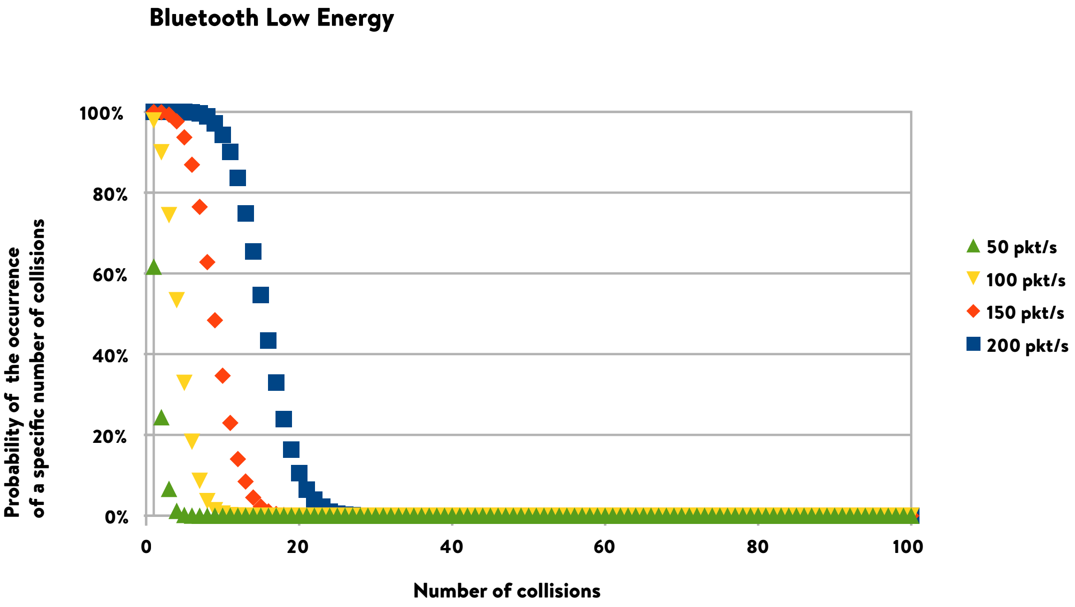
With both payload and overhead kept under very strict limits, Bluetooth's message occupies less than 400µs in the shared radio spectrum. This means that more than 2,500 such messages can theoretically be sent over a period of 1 second. As mentioned, Bluetooth has been optimized for transporting large amounts of very small packets, so it doesn't make much sense to compare these numbers to Wi-Fi which has been designed with completely different assumptions in mind. But even other low-power protocols pale in comparison. **It takes less than 4 ms to transmit a message within a ZigBee network, which is approximately 10 times more than in the case of Bluetooth**. Where does this enormous difference come from? First, the data packet of ZigBee is roughly 2 times larger than

Bluetooth's. Second, the maximum data rate of all 802.15.4 radios is 250 kbit/s, compared to Bluetooth's rate of 1 Mbit/s. All these numbers add up, having significant impact on real throughput, and determining whether a high-density smart lighting network deployed in a commercial environment can provide a satisfactory performance.

When analyzing different wireless data transmission technologies, we started examining how many packets could be sent per second over networks powered by different types of low-power communication protocols before the packet collision rate becomes a problem. This was first done by means of a theoretical simulation, and then verified in practice with statistical measurements. One of the simulations carried out by us analyzed the probability of occurrence of specific numbers of collisions, depending on the number of data packets generated each second by the network. We've performed it for each of the leading low-power wireless communication technologies of that time, i.e. ZigBee, Z-Wave and Bluetooth. The obtained results can be seen in the following charts:







A quick glance at these charts shows that Bluetooth packets are significantly more resistant to collisions, even when there are hundreds of them circulating across the network. In the case of Z-Wave, for example, networks generating 200 packets per second are basically certain to be saturated all the time. It must be noted, however, that these simulations did not take into account the full spectrum of technological factors contributing to performance of a particular network, such as certain collision prevention mechanisms used by the abovementioned technologies. They also did not take into consideration multiple factors that affect network performance in real-life environment, just to mention radio interference. However, they did provide us with a solid foundation for further analysis. They also did reinforce our faith in Bluetooth as the **best available radio for high-density commercial mesh networks**.

INTERFERENCE

Another very relevant feature of Bluetooth Smart, which makes the communication process even more robust, is the **adaptive frequency hopping scheme**. It allows the signal to **hop dynamically between the 40 available channels**, avoiding the noisy ones and selecting those that ensure a quick and successful delivery. This is particularly important considering the fact that Bluetooth utilizes the same 2.4GHz spectrum as numerous other radio technologies, including Wi-Fi, ZigBee or Thread, but also such appliances as microwave ovens, baby monitors or cordless phones. Still, Bluetooth's 2.4GHz band is a bit of a downside. While the standard has the tools to effectively counteract interference problems, the 2.4GHz signal weakens faster than a sub-GHz signal as radio waves travel through walls and other obstacles.

RANGE

That said, the **range of the Bluetooth radio is way better than most people think**. Bluetooth is still widely considered an ultra-low range communication technology, the one just about sufficient to handle wireless data exchange between a laptop and a cordless mouse. But with Bluetooth Smart, manufacturers may choose to optimize range to ensure a reliable data exchange over incomparably higher distances. Example? After applying certain software and hardware solutions to a standard Bluetooth module, we've managed to significantly increase its reach, while ensuring full compliance with the core Bluetooth specification and the RF radiation exposure regulations. Operating at +10dBm Tx power and with -98dBm Rx sensitivity, such tweaked modules provided a 108dB link budget that translates to **a line-of-sight range of up to 500m**. Inside buildings, this value will obviously be much lower and dependent on many factors, yet it still remains impressive.

BLUETOOTH EVOLUTION

Now if you compare the above characteristics with what other low-bandwidth standards have to offer, you'll see why we claim that the Bluetooth radio is superior to any other technology available on the market. And in terms of network robustness and resilience, this gap keeps widening. In December 2016, the SIG adopted the latest core specification of Bluetooth, introducing **Bluetooth 5**. With a maximum data rate of 2 Mbit/s, it can be twice as fast as the previous version of Bluetooth, which means that even lower duty cycle, latency and energy consumption are becoming achievable. Furthermore, its range has increased up to 4x versus the previous standard. Even without these enhancements Bluetooth was hands down the best low-power radio, but Bluetooth 5 takes things even further, leaving other major competitors far behind - especially that none of them has revealed plans of similar improvements regarding their physical infrastructure anytime soon. The vast majority of devices still rely on the previous generation of Bluetooth SoCs, and the transition to Bluetooth 5 will certainly take some time. But it has already begun and will be progressing, allowing the Bluetooth radio to step up to a much higher weight class. What is particularly important, Bluetooth 5 comes with backward compatibility so new chipsets will be able to communicate with the older ones.

But of course it is not all about the radio. We mentioned earlier that Bluetooth traditionally wasn't even considered an option in more complex IoT applications. How could that be if the Bluetooth transport offers such an outstanding set of features? The answer lies in the middle part of the simplified OSI model shown above, with network being the key word.

Despite being developed specifically to address the challenges of the rapidly evolving IoT market, Bluetooth Smart was engineered to support relatively simple hub-and-spoke networks. And that's just not enough to enable a contextual, dynamic, sensor-driven environment that we'd like to see in our connected homes, let alone offices or factories. Mesh networking is an essential topology for numerous applications, particularly the ones that require extended range or peer-to-peer communication. Smart lighting, and smart building automation in general, are perfect examples. Therefore, it is not surprising that all of the usual suspects in the low-bandwidth category (Z-Wave, ZigBee, Thread) route messages over mesh networks.

TOPOLOGY

For a long time, Bluetooth did not support mesh topology and almost no one thought this could be possible. Except for several companies which started working on their proprietary mesh solutions powered by Bluetooth Low Energy. Silvair was one of them, and transforming the single-hop BLE topology into a robust multi-hop, peer-to-peer network was a huge effort that required overcoming multiple complex challenges. But with the outstanding features of the underlying Bluetooth Low Energy radio, it turned out that our proprietary mesh system could be a powerful and rock-solid backbone even for large-scale, sensor-driven networks. Moreover, it performed surprisingly well in one of the most challenging IoT applications, i.e. connected lighting.

These few proprietary Bluetooth mesh solutions that started showing up did not really matter from the market perspective, though. Proprietary systems aren't worth much in general as they can never solve the problem of interoperability, the IoT's biggest roadblock to mass adoption. They are also never as reliable and secure as open standards developed in a collaborative effort between multiple companies and experts. Still, these early attempts proved that Bluetooth can successfully relay messages over mesh networks. And they looked so promising that in early 2015, the Bluetooth SIG announced the formation of the Mesh Working Group. Its goal was to standardize mesh networking support and draw up relevant specifications. Companies that had earlier developed their pioneering proprietary mesh systems joined the group, along with technology industry giants and chip vendors. Together, they tried to work out the most efficient and robust architecture for Bluetooth mesh networking. This took quite some time but in July 2017, Bluetooth mesh specifications were finally adopted and officially published. With a total of almost 1,000 pages, this isn't a casual evening read. But it dives very deep into the roots of problems that wireless technologies are struggling with in the Internet of Things. Bluetooth mesh networking is a complex technology. It requires a significant development effort from stack vendors, probably bigger than in the case of any other low-power radio. But to solve complex challenges, you usually need some complex tools. And Bluetooth mesh specifications seem to deliver a very powerful toolkit. What's inside? A number of very innovative concepts that have not yet been applied to low-power wireless standards.

Bluetooth mesh is very different from other mesh technologies we've discussed so far. The communication process follows a different set of paradigms. One of them relates to how messages are propagated through the network. Both in source-based routed networks (Z-Wave) and destination-based routed ones (ZigBee, Thread), each message is propagated along a specific path by hopping from one node to another until it reaches its destination. Bluetooth mesh uses an approach called managed flooding. Each message is broadcast to every device in range, and relaying nodes push it deeper into the network by broadcasting it, again, to all devices within their reach. This way, a given message gets relayed across the entire network, and relevant nodes respond to it as soon as they receive it.

At first glance, traditional routing looks like a more elegant and efficient approach. But in multiple challenging applications, the managed flooding technique offers distinct advantages. It doesn't require sophisticated routing tables, advanced network management, or complicated and time consuming emergency network healing procedures for re-routing data packets that encounter some sort of an obstacle. This means managed flooding requires less memory and less processing power. At the same time, it is a highly reliable technique – mainly because of how simple it is. It maximizes the efficiency of wireless data transmission by reducing the overhead for conveying routing information. As a result, it allows for keeping the size of data packets as small as possible – which is critically important in high-density sensory networks. Finally, managed flooding provides stronger resistance to interferences and obstructions. Since messages are propagated simultaneously along multiple paths, they are able to reach their recipients even if a number of things go wrong along the way – e.g. when many of these paths become blocked at the same time for whatever reason.

The managed flooding approach is accompanied by the publish-subscribe paradigm which ensures robust multicast communications within Bluetooth mesh networks. Network nodes can be configured to subscribe to a set of group addresses, or to publish messages to a set of group addresses. This is a radical departure from the precisely routed messaging known from previous wireless technologies. Just like the managed flooding approach, this model supports very efficient message transmission in large-scale commercial networks.

The communication paradigms introduced by Bluetooth mesh are in line with the Information Centric Networking (ICN) concept. Networking experts say this is where the entire Internet will be heading in order to deal with constantly increasing traffic volume caused by proliferation of applications like mobile video or cloud computing. The ICN is an approach to evolve the Internet infrastructure and support this growth by introducing uniquely named data as a core Internet principle. Moving away from a host-centric paradigm, the ICN model doesn't care that much about senders, recipients, addresses. Instead, named information is its focal point, making data independent from location, storage or application. In Bluetooth mesh networking, this is realized through a fully decentralized architecture with no single points of failure. With its publish-subscribe paradigm, Bluetooth mesh moves away from a host-centric architecture, while allowing for highly efficient multicast communications. Data generated by intelligent sensors becomes addressable information. Since addresses of individual nodes don't matter, sensor data is the focal point - other nodes subscribe to it and respond accordingly. This approach seems to be solving a number of problems that other technologies are dealing with in complex mesh networks. Device replacement is one of such problems. In Bluetooth mesh, whenever a broken lamp needs to be replaced, a new device only has to be re-subscribed to the same groups as the previous one. There is no need to change anything in the configuration of all sensors that interact with it.

These innovative communication concepts, coupled with extremely efficient wireless transfer capabilities of the BLE radio, is what makes Bluetooth mesh networks so robust and scalable. In addition to its impressive scalability, Bluetooth mesh also introduces additional measures that help confine heavy network traffic in extremely dense, large-scale commercial implementations. One of them is the concept of subnets. With a single mesh network capable of accommodating more than 4,000 subnets, Bluetooth mesh should be able to cover any building automation system we could possibly imagine today. Furthermore, Bluetooth mesh can use three different frequencies, which means that available raw radio resources are significantly larger than in the case of protocols operating on a single frequency. Also, the source may repeat each message three times as a recommended option drastically improving network reliability in those high-density implementations.

Considering everything that was stated above, we expect Bluetooth mesh standard to have a transformative impact on the smart building automation segment and the entire IoT. Well, unless it fails to address the challenge of interoperability - as is the case with the vast majority of wireless technologies.

INTEROPERABILITY

So how does the Bluetooth SIG plan to handle this challenge? The first condition is already met, since Bluetooth covers all of the layers of the OSI model, including the application layer. In BLE, interoperability was addressed by defining profiles for individual applications and types of devices. In Bluetooth mesh, this is addressed by introducing an impressive library of mesh models. From the perspective of the application layer, the Mesh Model Specification is the key part of Bluetooth mesh networking technology. Its first revision focuses heavily on smart lightning, although it also introduces multiple generic models that can be used in other applications. Why such a focus on luminaires? Because commercial smart lighting is a perfect application for the mesh topology. Not only is it one of the most challenging segments of the entire IoT, but also the one which opens enormous opportunities that could generate huge benefits on a global scale, particularly with regard to energy efficiency. Furthermore, lights are everywhere and they are already powered. So depending how you look at it, a lighting control system may be the goal itself or may just be the initial step to develop more services that are based on a mesh-connected infrastructure. And Bluetooth has some real superpowers when it comes to enabling value-added IoT services (we'll get back to this later).

Future revisions of Bluetooth mesh networking are expected to introduce more models that will be specifically designed to support different applications. But just looking at how Bluetooth mesh addresses typical challenges awaiting in the connected lighting segment, one can tell that the Bluetooth SIG takes things seriously. The Mesh Model Specification covers all sorts of lighting control scenarios and needs, from switch-based operation and smooth dimming capabilities to advanced sensor-driven lighting control strategies, such as occupancy sensing or daylight harvesting.

Still, a rigorous certification program is a must if the SIG doesn't want to end up where the ZigBee Alliance did at some point. The first wave of Bluetooth mesh enabled devices is on its way to the market, so soon we'll be able to verify whether this new technology can provide cross-vendor interoperability. What is encouraging, though, is that so far the Bluetooth SIG has placed great emphasis on ensuring full interoperability between devices bearing the Bluetooth logo. It seems that supporting the application layer has always been a natural direction for the SIG – this is why you can blindly grab any Bluetooth headset off the store shelf without having to wonder whether or not it will work with your phone. You just know it will, and this is the confidence end users should have with every type of smart product on the market. Also, the focus that the Bluetooth SIG has put on the Mesh Model Specification seems to be proving that cross-vendor interoperability between connected devices powered by Bluetooth mesh will be ensured.

BEACONS

That's all about the OSI model, but that's not all about the Bluetooth radio. While the most popular radio protocols aspiring to connect the IoT have a fair amount of overlapping qualities, there are several value-added features that only Bluetooth can provide. The beacon capability is one of them. Using Bluetooth's proximity sensing, beacons can make smartphones perform certain actions whenever the user is close to a given smart device. This enables a wide array of unique applications, from location-based push notifications that open up entirely new possibilities in retail marketing, to accurate positioning services that can be used e.g. to guide passengers at the airport to their gates. What's particularly important is that adding several lines of code to a software stack is all that is needed to equip a Bluetooth-powered smart device with the beacon functionality. Each Bluetooth module is natively equipped with proximity sensing capabilities, so there is no reason why e.g. beacon-enabled lighting fixtures should be more expensive than "standard" connected fixtures.

COMPATIBILITY WITH SMARTPHONES

ONBOARDING

That proximity sensing is possible due to the fact that a smart device and a smartphone can communicate directly with each other. And this might actually be the biggest single advantage that Bluetooth mesh has over its competitors. Out of all wireless communication technologies used in the IoT, only Bluetooth and Wi-Fi are natively supported by virtually all smartphones, tablets and laptops on the market. But apart from being completely unsuitable for the vast majority of IoT applications, Wi-Fi pushes all messages through an access point, anyway. Direct communication happens only with Bluetooth. This produces very significant benefits from the user experience perspective, since a phone app is all that is needed to build, configure and control a network of connected devices. Thanks to this direct connectivity, Bluetooth provides the end user with what could be called a Remote Display and a Remote Keyboard for each smart device, no matter how small or simple it is. One of the major benefits resulting from this is the simplicity of the commissioning process. With other protocols, manufacturers often have to come up with the wildest ideas to facilitate adding a new device to the existing network. With Bluetooth, the entire procedure can be made simpler, more intuitive and safer.

COST

But if Bluetooth offers so much goodness, there has to be a price to pay for that, you might think. And you'll be right. But it's not about the financial cost of chipsets, as Bluetooth modules are among the cheapest ones on the market. That price comes in the form of complexity. While smartening a device requires the manufacturer to make quite a lot of effort regardless of the technology it decides to embrace, it’s a bit more difficult to implement Bluetooth than to implement one of the other leading wireless communication protocols. On the other hand, that’s quite a universal rule. More sophisticated and powerful solutions are usually more difficult to understand and master.

So this is Bluetooth, a technology in transition. Following the recent adoption of Bluetooth mesh networking specifications, it finally seems to have everything that is needed to introduce new quality to low-bandwidth communications in the IoT. Time will tell what applications will be addressed in future revisions, but Bluetooth mesh networking seems to be well prepared to address an extremely wide range of use cases. As far as connected lighting is concerned, no wireless technology has ever been so deep and comprehensive. With Bluetooth’s global interoperability and strong market presence, its well-tuned lighting control framework should finally enable widespread adoption of connected lighting systems. And if this scenario becomes reality, Bluetooth mesh networking - through smart LEDs - will get a chance to be deployed in commercial buildings across the entire globe. This would be a pretty comfortable position for a solution which aspires to become a go-to technology for the Internet of Things.

7 And the winner is...

So there you have it, the closing chapter of the Tale of Five Protocols. Who is the winner in this race? As already stated in one of the opening paragraphs, there is no one-size-fits-all solution. But once you break it all down into these tiny technical and practical details, identifying the technology that is going to work best for you and your customers should not be all that difficult.

The omnipresent Wi-Fi is a great and totally reliable protocol, but there is an extremely limited number of applications for it in the Internet of Things. Your router is where it belongs, and leaving it there is the best thing you can do.

The good old Z-Wave deserves a fair amount of respect for handling wireless data transfer in the early years of the IoT era, but this is really the right moment to say farewell. Yes, there have been some improvements introduced to it, but no matter how much you improve your favorite scooter – you just won't win a Nascar race with it. And to be honest, we wouldn't bet a dime on Z-Wave's future considering the recent ownership turmoil that we addressed when describing this technology.

ZigBee is, in fact, the first wireless system on our list that might deserve your attention. It is not a SpaceX rocket by any means, but if you're into some relatively simple solutions, it might work for you just fine. It is a bit rusty, but it did manage to grow out of certain past issues. It keeps developing, it has a strong market presence, and a fair number of limitations on top of it all. But if they don't bother you and – more importantly – your customers, then go ahead and try out how it meets your not-too-sophisticated wireless needs. Just do yourself a favor and don't put it into you smart lighting devices or other building automation solutions. Don't expect it to handle heavy traffic or ensure low-latency performance in more complicated scenarios. This is a simple solution for simple tasks, and this is where it should be used.

Thread looks interesting, we have to admit. It is well positioned to address some of the challenges of today's IoT. It is backed by some big technology companies, which isn't without significance. And there are further improvement on its roadmap that should make it even more interesting at some point in the future. But if you're building a professional product today, it does take a lot of courage to think about Thread. There are just so many question marks. Why there are no products so long after the adoption of specification? When can we expect much-needed commercial extensions that could enable professional deployments? Why is the Thread ecosystem being diluted with the controversial Thread Ready program? If you can figure it all out and the answers don't seem scary for you, then you probably understand this wireless landscape way better than we do. We are bold but not crazy - we'll be keeping an eye on Thread, that's for sure. But at the same time we'll stay away from it as far as our wireless solutions are concerned.

And the last contender, Bluetooth. With its complicated history and even more complicated branding, this could be the most confusing technology out of all wireless systems reviewed by us here. How could that Bluetooth from my headset enable adaptive lighting networks? Isn't Bluetooth 5 the best version of the standard? So why is there so much noise about Bluetooth mesh? We keep hearing these questions over and over again, but this doesn't change the fact that Bluetooth is currently the most powerful low-power technology for the Internet of Things. Based on our experience with all leading wireless standards, no other radio can provide such a complete set of capabilities that meet the needs of the most advanced applications. Add to this the recently added support for mesh topology, the innovative information-centric approach, the Bluetooth SIG's focus on cross-vendor interoperability, and the outstanding value-added services that can be provided on top of Bluetooth mesh networks - and it becomes clear why Bluetooth emerges as the indisputable winner. It has made an enormous technological leap over the last couple of years, and it's hard to imagine that something could prevent the Bluetooth SIG from maintaining that IoT-oriented course. For all sorts of more demanding implementations - and smart lighting in particular - there is simply no better wireless technology at the moment. If you're into such solutions, Bluetooth mesh networking is where you should start. Development will be a challenge, but the rewards will be huge ■

Silvair is a provider of flexible lighting firmware packages that can be easily integrated into a variety of LED lighting and sensor devices. Optimized for professional applications, lighting models developed by Silvair support sensor and switch-based lighting functionalities and basic to advanced lighting control scenarios. In addition, Silvair provides a full-stack lighting control platform for commissioning and managing connected lighting systems in commercial spaces.

For more information about our solutions, visit **www.silvair.com**

Twitter **LinkedIn**

Author: **Szymon Rzadkosz** (Silvair)
Editorial design & illustrations: **Jerzy Nosek** (Silvair)
Technical consultancy: **Szymon Slupik** (Silvair)

The information provided in the study was prepared by Silvair, Inc. This is for information purposes only and should not be relied on for any other purpose. This study does not in any way represent advice or recommendations.
We make no representation (whether explicit or implicit) or warranty regarding the suitability, accuracy or completeness of the information in the study. Matters that may affect third parties are not addressed in the study, and any liability is therefore hereby expressly excluded. Any reliance third parties choose to make on the information is a matter of their judgement exclusively and independently. Furthermore, we are under no duty to update or revise the study in any way.

SILVAIR

www.silvair.com