White Paper

WP_001

Smart Home Gateways

Version 1.0

Issue Date: 2017-01-23

This white paper discusses the challenges and opportunities presented with the new smart appliance market and how control of all the different technologies can be centralized through a smart hub.

Bridgetek Pte Limited (BRTChip)
178 Paya Lebar Road, #07-03 Singapore 409030
Tel : +65 6547 4827 Fax : +65 6841 6071
Web Site: http://brtchip.com

Table of Contents

1 Introduction

Smart home, smart appliances, home automation and IoT, etc. are increasingly common terms in today's world, but what is it?

For most the terminology refers to the control and monitoring of sensors and appliances remotely and it is the remote control or networked element which typically defines the device as being smart or not. Although not totally restricted to the home, this and commercial properties (e.g. hotels) is where the volume market is perceived to be with applications covering lighting, heating control, security, and entertainment. As this is an emerging market (that has been emerging for some years) there is a certain disparity in technologies used by different appliance providers.

Within this white paper will be a discussion on the different technologies and protocols used to realize a smart device, with a view on how the different technologies can be brought together to function in an integrated installation through the use of IoT hubs or gateways.

2 The Hardware Transport Layer

The hardware or physical transport layer is technology used to bridge between an appliance and the control device. This may be a physical connection such as Ethernet or RS485, but is increasingly being handled by a wireless connection. While cabling is simpler and potentially more secure, it does not lend itself so well to installation in an older building, while a wireless solution just requires a power supply.

2.1 Cabled connections

Cables are great for short runs and new installations. Typically a cabled installation will use either RS485 or Ethernet as the protocol associated with each technology allowing for addressing individual nodes on the network.

2.1.1 RS485

This is a popular protocol for cameras, particularly for controlling the pan, tilt or zoom features of a camera installation. It has the potential to offer more security than a wireless link as it is physically connected point to point and cable runs can be relatively long, up to 1200m. Additionally the RS485 protocol allows for addressing different nodes on a network such that multiple devices can be accessed. Data rates supported by RS485 are typically up to 1Mbyte/s which should be perfectly adequate for the typically short data bursts used in many smart appliance communications.

2.1.2 Ethernet

Ethernet offers a lot of the same benefits as RS485, plus a few others. The key additional benefit being that power may be transmitted over the same cable run, thus solving a potential issue with powering the smart device such as a motor to control opening / closing shutter blinds.

Data rates are also high (typically 10/100Mbps) with Ethernet, and suitable for transfer of video data in security camera applications.

Ethernet cable runs may be readily available in commercial buildings whilst residential properties will still require new wiring to be installed if selecting this technology.

2.2 Wireless connections

Wireless connectivity also comes in a variety of forms with many consumers being more familiar with terms such as WiFi or Bluetooth than the cabled alternatives. The obvious benefit of wireless over cabled is in the cost and ease of installation – no cables to route.

2.2.1 WiFi

WiFi is already available in many homes via the router that connects the home to the wider internet. It is a technology that is widely used in smart TVs as well as on tablets, phones and other portable devices.

From a consumer perspective the technology is relatively easy to use. No manual paring is required and with DHCP, an IP address for each device may be obtained automatically.

Another advantage of WiFi is the ability to control devices while away from home via internet routers which is not necessarily the case for other shorter range wireless or cabled technologies.

Many gateway technologies will bridge from WiFi to the technology used by the local smart device thus enabling low power devices with a short wireless range to be accessed remotely.

Base standard	IEEE802.11
Frequency	2.4GHz / 5.0 GHz
Range	35m
Number of Slaves	Based on IP addresses
Data rate	54Mbps – 600Mbps
TX Power	-

Table 1: Wi-Fi

2.2.2 BLE

Low Energy Bluetooth is a lower power version of Bluetooth developed with IoT in mind and is ideal for connecting devices that may be running off batteries such as home security sensors. The technology does rely on users "pairing" devices to establish a communications link, although this is a relatively simple and fast process that should only need to be done once.

Although the specification does not specify a maximum number of devices that can be paired it seems a practical limit in the 10's should be achievable with decent data rates and a connection distance of >100m.

Another advantage of the Low energy variant of Bluetooth is the ability to add 128 bit AES encryption for data security.

The Bluetooth standard is now at Bluetooth 5, with Low Energy clauses being introduces at version 4. The standard is based on IEEE802.15.1.

Base standard	IEEE802.15.1
Frequency	2.4GHz
Range	>100m
Number of Slaves	Undefined (typically 10's)
Data rate	1Mbit/s
TX Power	15mA

Table 2: BLE

2.2.3 ZigBee

ZigBee is another popular standard based (IEEE802.15.4) wireless mesh technology for home automation and has been around for a long time. It is a low power option designed to be low cost with home automation in mind. The protocol allows for the connection of many thousands of devices at distances up to 100m and with data encryption support.

At present there are 3 basic specifications within the ZigBee standard – ZigBee PRO, ZigBee RF4CE and ZigBee IP

The standard is used globally; however different regions / markets operate at different frequencies. EU and Japan use 868MHz, while the US uses 915MHz. A third 2.4GHz ISM band is also available in the standard and is the most popular as it is available worldwide.

Base standard	IEEE802.15.4
Frequency	2.4GHz
Range	10 - 100m
Number of Slaves	240 physical nodes each able to address a further 240 device (in theory)
Data rate	Up to 250kpbs
TX power	~20mA

Table 3: ZigBee

2.2.4 Z-Wave

Z-Wave is a low frequency (900MHz) RF connection for smart devices. The benefits of the low frequency solution are claimed to include less interference and hence a stronger more reliable signal between the device and controller. As a smart home will inevitably have many obstacles such as walls, doors and furniture to penetrate, the longer wavelength from Z-Wave should perform better.

Base standard	Proprietary – but since open sourced
Frequency	900MHz
Range	30m
Number of Slaves	232 devices
Data rate	Up to 100kbps
TX power	23mA

Table 4: Z-Wave

2.2.5 Thread

Thread is another low power wireless solution aimed at connecting up to 250 devices around the home. It offers an open standard to encourage developer adoption and connects devices through a mesh network for increased robustness as any broken node in the mesh can be redirected. This solution is also built around the IEEE802.15.4 standard that ZigBee uses and as such is aimed at applications with lower data rates e.g. 250kbps.

Base standard	IEEE802.15.4
Frequency	2.4GHz
Range	100m but uses routers to extend reach
Number of Slaves	Up to 250
Data rate	Up to 250kbps
TX Power	-

Table 5: Thread

2.2.6 NFC

Near Field Communication or NFC typically requires a physical token or smart phone to activate a device by being in close proximity to it. In a smart application it may be used to power on lights or unlock doors / computer apps or share data such as photos between devices when the user is present. It is relatively short range and designed for one to one connection.

Base standard	ISO/IEC 18000-3
Frequency	13.56MHz
Range	0.1m
Number of Slaves	1
Data rate	Up to 420kbps
TX Power	-

Table 6: NFC

2.2.7 IrDA

IRDA represents the Infrared Data Association and provides wireless connectivity via an infrared link. The connectivity is for short range applications and does require line of sight between controller and device. This sort of technology is likely to be found in TV, Blu-ray players, cameras etc. A key feature of this technology is the low bit error rate making it very efficient.

Base standard	-
Frequency	1.1Mhz
Range	1m
Number of Slaves	1
Data rate	~1.2Mbps (115.2 kbps in low power spec)
TX Power	-

Table 7: IrDA

2.2.8 433/315MHz RF

RF at lower frequencies of either 433MHz or 315MHz are unlicensed and popular in control and sensor modules used by the maker market in applications such as Arduino shields. They are typically used in short range applications and have the advantage over IrDA in that they do not require line of sight to communicate. Some example applications may include a remote control for opening / closing a blind or shutter when data encryption or security is not a concern.

Base standard	-
Frequency	433 / 315 MHz
Range	100m
Number of Slaves	1
Data rate	-
TX Power	-

Table 8: 315/433Mz RF

3 The software transport Layer

In addition to the hardware layer for device communication being fragmented across various technologies, so too are the software APIs to control the various smart devices.

Not only do the different wireless solutions have different underlying protocols but the different smart appliance technologies often also have unique function calls too.

This may make some sense to the engineering community as they try to add features to distinguish their solutions from a competitor's solution, but for the consumer that only wants to switch a light on or off, it seems an unnecessary complication.

For example if a user buys a HUE lightbulb from Philips and they buy the HUE tap and install the HUE app on their phone they are essentially locked into HUE technology. What happens when the lightbulb fails (it will at some point in time)? Either the user replaces with HUE technology, assuming it is still available at a reasonable cost or transfers to another vendors solution where they may also have to acquire new controllers and apps for their smart device.

This is a significant barrier to adoption of this new technology which in the absence of a global standard for all smart devices is best resolved with a smart gateway hub that accesses multiple technologies.

4 The User Interface

The user interface to access a smart device comes in a variety of forms.

4.1 Mechanical

The most basic interface is a mechanical button. This is perfectly adequate for simple on/off functionality such as required for controlling power to devices or controlling the opening or closing of a blind/shutter.

4.2 Touch panel / smart phone

The next step is the mobile phone application. This allows consumers to interact with their smart technologies via a familiar portable device either at home or away. This is a huge advance from a basic mechanical button as the user can read sensor data and accurately set control parameters such as temperature or time settings in a heating system.

Smart phone apps typically rely on visual and touch interaction and are often supplied free with the devices and are therefore a cheap alternative to dedicated controllers but cannot really ever replace the dedicated controller especially in safety and security applications where it is not acceptable for the smart appliance to be inaccessible due to a discharged battery of the phone and its owner being away from home and not contactable.

4.3 Audio

Relatively new to the market is the addition of voice activated controllers. Philips HUE are bringing a new voice activated hub to the market for their devices, and Amazon have their Alexa and echo dot devices which can access the internet or control a growing selection of 3rd party smart devices. Siri, Cortana, or Hey Google offer voice control for the smartphone apps which will further increase the number of voice activated options.

4.4 Gesture Control

Gesture control is another mechanism that users may employ to interact with their technology. This can come in two forms, the first being similar to a Wii game controller where motion is detected by the movement of a ”wand” or hand gestures picked up by a camera. Movement up/down could control the volume of an audio device while left and write could scroll through a music collection.

The second class of gesture control relates back to the touch panel or smart phone app where a swipe or “drawn” letter on the display could operate as a shortcut to a predefined function.

5 Device and Data Security

A further technological challenge in the smart appliance is the security of the appliance data. It is widely recognized that for the technology to be successful the consumer must have confidence that the appliance is secure and any personal data cannot be hacked.

Security solutions are being developed in a number of forms – software encryption with 128 bit AES being common as well as dedicated security ICs.

6 Gateways and Hubs

Bridgetek and a few other companies have not attempted to recreate or force a new standard on the market. Instead the solution taken by these companies is to embrace all the distinct technologies and offer a common control interface and bridge to the various standards out there.

One smart controller hub can deliver a fixed or portable device that remains in the home (unlike a smart phone) and offers a common interface to multiple similar devices e.g. different manufacturer's light bulbs using either ZigBee or BLE.

Also by accessing all the smart technologies through a centralized point it extends the integration of light, power and security by enabling a simpler one stop location for coordinating when lights and security need to be enabled / disabled and gathers consolidated statistics of energy usage.

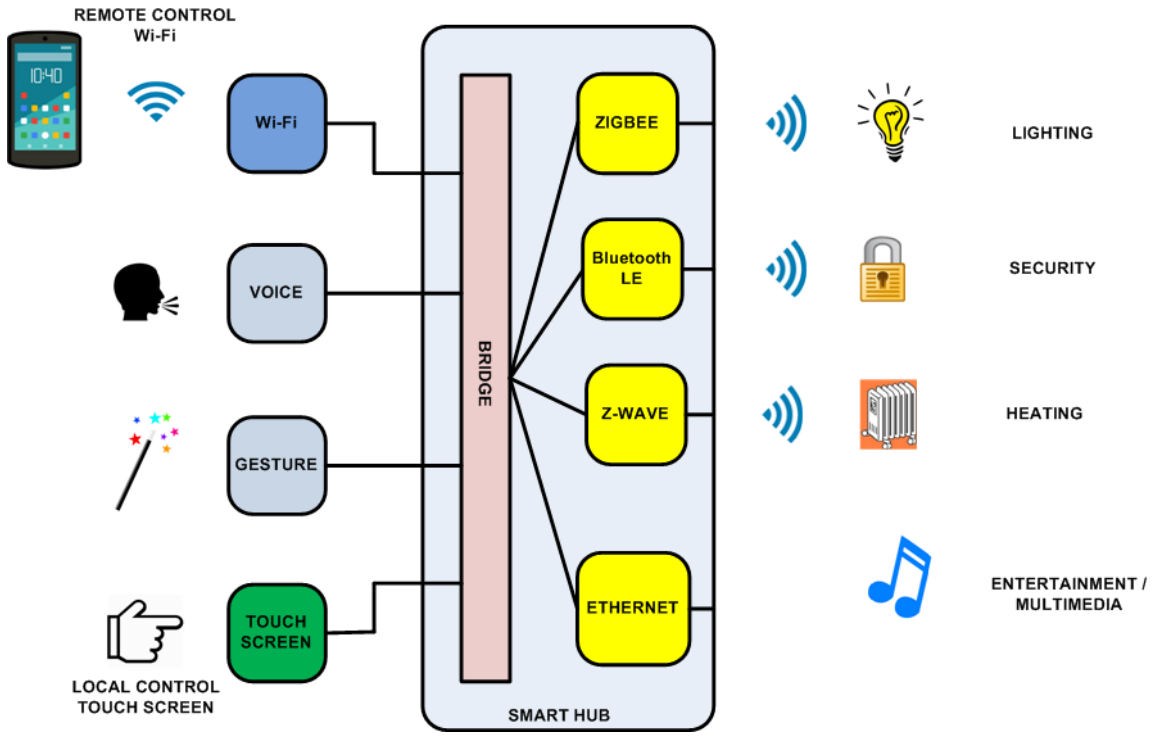

Figure 1: Smart Hub

7 Conclusion

Smart home integration requires many elements, smart appliances, smart controllers, low power and data security to name but a few.

Despite all these new devices being brought to market through different technologies, it is reasonable to assume that eventually one or two technologies will win out. Remember the lessons of history with BETAMAX vs VHS video recorders. The technology with the better content will ultimately win before itself being superseded by better technology.

However before that time comes there is a definite need to embrace all the different technologies that are applied to different market segments and consolidate the user interface into something smart that controls all aspects of the smart home and not just individual applications.

To this end we should expect to see more IoT gateways and hubs appearing on the market to support the smart appliances.

8 Contact Information

Head Quarters – Singapore

Bridgetek Pte Ltd
178 Paya Lebar Road, #07-03
Singapore 409030
Tel: +65 6547 4827
Fax: +65 6841 6071

E-mail (Sales) sales.apac@brtchip.com
E-mail (Support) support.apac@brtchip.com

Branch Office – Taipei, Taiwan

Bridgetek Pte Ltd, Taiwan Branch
2 Floor, No. 516, Sec. 1, Nei Hu Road, Nei Hu District
Taipei 114
Taiwan, R.O.C.
Tel: +886 (2) 8797 5691
Fax: +886 (2) 8751 9737

E-mail (Sales) sales.apac@brtchip.com
E-mail (Support) support.apac@brtchip.com

Branch Office - Glasgow, United Kingdom

Bridgetek Pte. Ltd.
Unit 1, 2 Seaward Place, Centurion Business Park
Glasgow G41 1HH
United Kingdom
Tel: +44 (0) 141 429 2777
Fax: +44 (0) 141 429 2758

E-mail (Sales) sales.emea@brtichip.com
E-mail (Support) support.emea@brtchip.com

Branch Office – Vietnam

Bridgetek VietNam Company Limited
Lutaco Tower Building, 5th Floor, 173A Nguyen Van Troi,
Ward 11, Phu Nhuan District,
Ho Chi Minh City, Vietnam
Tel : 08 38453222
Fax : 08 38455222

E-mail (Sales) sales.apac@brtchip.com
E-mail (Support) support.apac@brtchip.com

Web Site

http://brtchip.com/

Distributor and Sales Representatives

Please visit the Sales Network page of the Bridgetek Web site for the contact details of our distributor(s) and sales representative(s) in your country.

Appendix A – References

Document References

RS485 - https://en.wikipedia.org/wiki/RS-485

Ethernet - https://en.wikipedia.org/wiki/IEEE_802.3

BLE - https://www.bluetooth.com/

ZigBee - http://www.zigbee.org/

WiFi – http://www.IEEE.org/

Thread – http://threadgroup.org/

NFC - http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/

IrDA - http://www.irda.org/

Acronyms and Abbreviations

Terms	Description
BLE	Bluetooth Low Energy
IoT	Internet of Things

Appendix B– List of Tables & Figures

List of Tables

List of Figures

Appendix C – Revision History

Document Title: WP_001 Smart Home Gateways
Document Reference No.: BRT_000064
Clearance No.: BRT#056
Product Page: http://brtchip.com/m-smarthome/
Document Feedback: Send Feedback

Revision	Changes	Date
1.0	Initial Release	2017-01-23