Cano, J.; Berrios, V.; Garcia, B.; Toh, C. (2018). Evolution of iot: An industry PErsPEctivE. IEEE Internet of Things Magazine. 1(2):2-7. https://doi.org/10.1109/IOTM.2019.1900002

Evolution of IoT: An Industry Perspective

Juan Carlos Cano*, Universitat Politecnica de Valencia, SPAIN
Victor Berrios, ZigBee Alliance, USA
Ben Garcia, Z-Wave Alliance & Silicon Labs, USA,
Chai K. Toh, National Tsing Hua University, Taiwan & GLG Group USA
corresponding author, email: jucano@disca.upv.es

Abstract

Mobile ad hoc networks have evolved since the early 1990s. Until now, it has been over two decades. However, its unique concept of wireless device-to-device networking has now ballooned into a major technology and industry revolution with applications impacting the many facets of our lives. In fact, it has paved the way for Internet of Things (IoT) and Smart Cities. In this paper, the evolution of IoT through mobile ad hoc networks is discussed and its penetration into defense, society, and industries through ZigBee, Z-Wave, and other technologies is revealed. Finally, a discussion is made on IoT architecture, connectivity, cloud, analytics, and its implications on the realization of future smart cities.

1. Introduction

The Internet in the early days was largely an interconnection of routers (packet switches) via copper wires, which was later replaced by co-axial cables and subsequently optical fibers. The invention of packet switching by Paul Baron has opened doors to transmit information in digital forms, in a distributed manner, globally. This surpasses the telecommunication voice network which at that time, primarily carried voice traffic. The work of Drs. Vint Cerf and Rob Khan on TCP/IP has further enabled the Internet to carry traffic end-to-end in a reliable manner, providing data error handling, flow and congestion control. With the creation of the Internet, and subsequently the WWW by Tim Berners Lee, there is an explosion of data traffic and Internet users. In fact, data traffic has now surpassed voice traffic, and the Internet is commonly used for a variety of applications, from business transactions, social networks (such as Facebook and Twitter), to emails, cloud storage (Google Cloud), and personal multimedia entertainment from Netflix.

The idea of an mobile ad hoc network was born in the early 1990s. This field was first worked on Toh [1 – 3], Perkins [4], and then Johnson [5]. In [1, 2], an all-wireless device-to-device network known as wireless ad hoc networks (tree and mesh topology) or also known as mobile ad hoc networks were introduced. Perkins was working on Mobile IP [4], which was based on a wireless extension (star topology) of the wired Internet. Johnson was also working on Mobile IP solution. However, both Perkins and Johnson subsequently moved to work fully on mobile ad hoc networks, with each proposing their own routing protocols [6][5]. The first practical wireless ad hoc network [2][3][4] was

implemented in 1998, using Lucent WaveLAN WiFi 802.11 2.4GHz radios, and with several laptops running Linux OS and the associativity-based ad hoc routing protocol (invented in early 1990s). In that work, it was demonstrated that realizing ad hoc networks is possible, and existing RPC/UDP/TCP/IP applications, such as FTP/TELNET/RLOGIN and HTTP web-based client-server multimedia applications can be supported transparently. Since then, mobile ad hoc networks have moved out of the myth and hype era. Research on mobile ad hoc networks has blossomed and is now approaching 25 years, which is remarkable.

The push has been significantly attributed to its remarkable potential applications. It was initially designed for distributed anytime anywhere computing but had later evolved into:

- Sensor wireless networking,
- Smart home wireless networks,
- Disaster rescue networks,
- Defense battlefield networks,
- Mobile phone peer networks,
- Smart street lights networks,
- UAV communication networks,
- Vehicular ad hoc networks, etc.

Currently, mobile ad hoc networks have paved the way for IoT, with even wider spread of use in smart homes, industry and environmental sensing applications, disaster rescue operations, defense communication networks, and for smart cities. As shown in Fig. 1., mobile ad hoc networks have evolved into IoT and smart cities, and it is still evolving despite in existence for over 20 years.

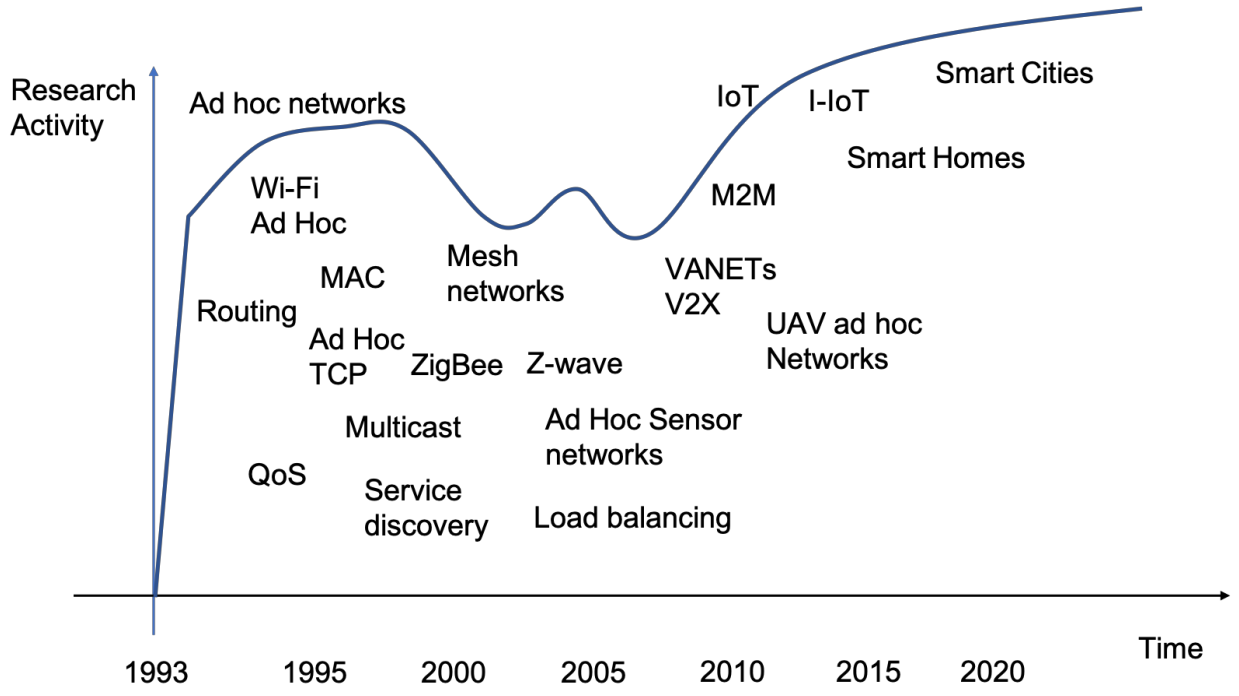


Figure 1: Ad Hoc Networks Research Evolution into Internet of Things (IoT)

2. Research Activity

2.1 Scale and Research Areas: While early research on mobile ad hoc networks was focused on routing (ref survey paper), it then went on to other areas of the 7-layer protocol stack (see Fig.1), such as media access, auto-address configuration, power issues, transport, multicasting, session, application and security.

In academia, a search on Google Scholar reveals that over 2.13Million published articles with key words related to ad hoc networks (see Table 1). In addition, the USA NSF alone has spent over $500Million over a 30 years period (since 1997) on research projects related to ad hoc mobile networks (see Table 1). Most of the research are still in pursuit by universities, and also from national laboratories. American defense industries have been active in this field too, sponsoring over $2Billion dollars of projects to enhance battlefield operations and war fighting capabilities (see Table 1). Defense agencies from Europe and Asia have collectively spent billions. All these have clearly shown the scale and importance of ad hoc mobile networks for the last 30 years.

Table 1: (a) Number of papers published with key word ad hoc networks (July 2018), (b) National Science Foundation (USA) projects related to ad hoc networks, and (c) some major defense spending on mobile ad hoc networks

1a. Number of papers published with key word ad hoc networks (July 2018)	
Keywords used in Google Scholar Search	No of articles founded by Google Scholar
Ad hoc networks	2.13 Million
Mobile Ad hoc networks	1.5 Million
Wireless ad hoc networks	1.12 Million
Vehicular ad hoc networks	179,000
1b. National Science Foundation (USA) projects related to ad hoc networks	
No. of NSF projects awarded in the area of ad hoc wireless networks (1996 – now)	Total Estimated Awards Amount (USD)
3000+	Over $500M
1c. Highlight of some major defense spending on mobile ad hoc networks	
Some Major Defense Research Programs on Ad Hoc Networks	Project Estimated Value (USD)

DARPA Ad Hoc Networking Gateway	$155M
DoD WIN-T Phase 1, 2, 3 respectively	$75M, $346M, $475M
US Special Ops Tactical ad hoc radios	$390M

3. Evolution of IoT Connectivity

3.1 Wi-Fi Ad Hoc

Early work [1 – 3] by industries on mobile ad hoc networks was based on WiFi. WiFi is an IEEE 802.11 standard at 2.4GHz. It is a WLAN standard. WiFi radios can transmit more than 100 meters in radio range, with transmission power typically of 1mWatts. Since its inception, several variations of 802.11 standards have evolved (see Table 2).

Table 2: IEEE 802.11 standards

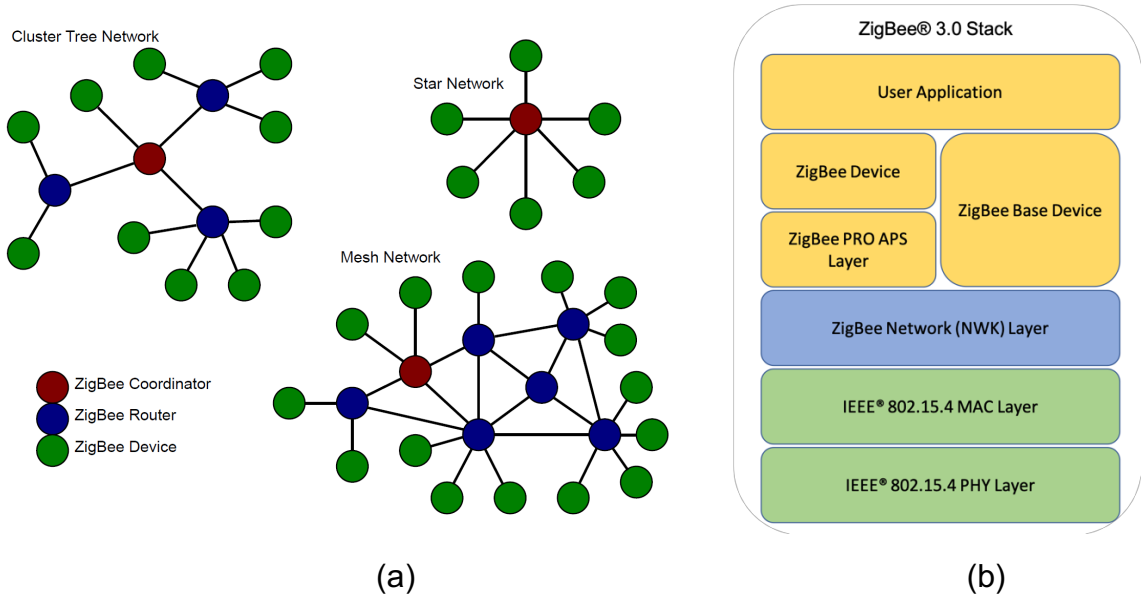
IEEE 802.11	Operating frequency	Date Rate	Transmission Range
IEEE 802.11a	5GHz	6-54Mbps	120m
IEEE 802.11b	2.4GHz	1-11Mbps	140m
IEEE 802.11g	2.4GHz	6-54Mbps	140m
IEEE 802.11n	2.4/5GHz	288M-600Mbps	250m
IEEE 802.11ac	5GHz	346M-3.466Gbps	-
IEEE 802.11ad	60GHz	Up to 6.7Gbps	-
IEEE 802.11ah	900MHz	Up to 347Mbps	-
IEEE 802.11aj	45/60GHz		-
IEEE 802.11ax	2.4/5GHz	Up to 10.53Gbps	-
IEEE 802.11ay	60GHz	Up to 20Gbps	100m
IEEE 802.11az	60GHz		-

3.2 ZigBee Technology

The ZigBee Alliance [7] was established by industries in 2002 with the purpose of providing a standard mesh network specification and complimentary application layer standards for the IoT. Its wide-ranging global membership collaborates to create and evolve universal open standards for the IoT.

“ZigBee PRO” is the Alliance’s flagship network standard, designed to connect and facilitate interoperability between smart devices with a very low-cost, very low-power-consumption, two-way, wireless communications solution. The ZigBee PRO stack architecture is made up of a set of blocks called layers (see Fig. 2b). Each layer performs a specific set of services for the layer above. A data entity provides a data transmission service and a management entity provides all other services. Each service entity exposes an interface to the upper layer through a service access point (SAP), and each SAP supports a number of service primitives to achieve the required functionality.

ZigBee PRO forms low-power ad hoc wireless networks using intermediate, routing capable nodes (coordinator and routers) to route and relay data hop-by-hop, using automatically discovered and maintained routes (see Fig. 2a). A coordinator is used as a central controller to initiate and manage network-wide services. As shown in Fig. 2b, IEEE 802.15.4 standard defines the two lower layers: (a) physical (PHY) layer and (b) medium access control (MAC) sub-layer. ZigBee Alliance builds on this foundation by providing the network (NWK) layer and the framework for the application layer. The application layer framework consists of application support sub-layer (APS) and ZigBee device objects (ZDO).



(a) (b)

Figure 2: (a) ZigBee architecture and topology, showing the presence of coordinator, routers, and end devices, and (b) ZigBee 3.0 protocol stack.

ZigBee PRO is the underlying network technology that supports full-stack interoperable devices implementing the ZigBee 3.0 or ZigBee Smart Energy Application Standards. These standards leverage the self-forming and self-managing capabilities of the ZigBee PRO network to provide application level device definitions, device discovery, binding and command-response capabilities to end-products. Table 3 below summarizes a few key features of the ZigBee 3.0 Standard.

Applications of ZigBee include wireless light switches, home energy monitors, connection of home appliances (such as thermostat), manufacturing and production automation, smart metering, smart grid monitoring, etc.

To complement its network and application standards, the Alliance offers its ZigBee Certified products program, which ensures that quality, interoperable ZigBee devices are available for ecosystem developers, service providers and their customers. The ZigBee Alliance is committed to ensuring that quality ZigBee products are available throughout the value chain. As of mid-2018, there were over 2600 certifications issued by the ZigBee Alliance. There are 2000+ ZigBee-compliant products on the market. Companies that

produce products complying to ZigBee 3.0 standards include: Samsung, Valeto, Themis, Toshiba, Kroger, Volare, Signify, etc.

Table 3: (a) ZigBee 3.0 Standard Specification, and (b) Z-Wave Technical Specification.

3a. ZigBee Specification	**Parameter**
Network Protocol	ZigBee PRO 2015 (or later)
Network Topology	Self-forming, Self-Healing Mesh
Network Device Types	Coordinator (routing capable), router, end devices, ZigBee green power device
Network Size	Up to 65,000 nodes
Radio Technology	IEEE 802.15.4 – 2011
Frequency Band / Channels	2.4 GHz (ISM Band) 16 channels (2 MHz wide)
Data Rate	250 Kbps
Security Models	Centralized and distributed
Encryption Support	AES-128 at network layer AES-128 available at application layer
Power Output	1-100mW
No. of Channels	16
Communication Range	Up to 300 meters (line of sight) Up to 75 – 100 meters (indoor)
Low Power Support	Sleeping end devices ZigBee green power devices (energy harvesting)
3b. Z-Wave Specification	**Parameter**
Data Rate	40Kbps (more recent up to 100Kbps)
Power Output	-24 to 6 dBm
No. of Channels	1-3 channels
Transmit Frequency	868 & 869 MHz (EU) 908 & 916 MHz (USA) 919 & 921 MHz (AU/NZ/BR) 919 – 926 MHz (JP/TW/KR/SG)
Routing	Source Routing with dynamic route resolution
Security	128bit AES encryption
Devices supported	Up to 232

3.3 Z-Wave Technology

Z-Wave, a standard first developed by Zensys Inc., and has recently been acquired by Silicon Labs Inc. The Z-Wave technology has made several evolutions since its creation.

In 2003, the 100 series chipset became available and later in 2005 200 series was released, with the ZW0201 chip offering a high-performance low-cost solution. In March 2013, Z-Wave Plus, called 500 Series, was released, featuring improved wireless range and battery life as well as four times the memory size of previous chips.

The prime application for Z-Wave is smart homes, where the protocol is widely used for connecting door locks, smoke detectors, home appliances, and remote controls. It is designed to provide reliable, low-latency transmission of small data packets, and is optimized for the smart home application through a few other features, including a communication distance that can cover most residences, which is at 40 meters on the 500 Series chip and will expand. Z-Wave devices link up to form a wireless mesh network where data can be relayed hop-by-hop from one device to another.

Interoperability is another key feature of Z-Wave, which allows Z-Wave device hardware and software to work together, so users may operate their entire smart home from one smart home application. With interoperability built-in at the application layer, all Z-Wave devices from various brands and vendors are backward and forward compatible and work together in a home or building.

Z-Wave operates in the 800-900MHz band, and hence does not suffer from much interference unlike the 2.4GHz ISM band, and Z-Wave PHY and MAC layers are defined by ITU-T G9959 [8] recommendation. See Table 3 for details on the Z-Wave specification. Z-Wave uses AES-128 for symmetrically encrypted communications (AES CBC-MAC and AES-OFB) for access control devices, but in 2015, Security 2 (S2) was added as an enhancement to Z-Wave Security by hardening the enrollment and authentication of new devices into the network through adding out-of-band key exchanges. In April 2017, the latest security framework, Security 2 (S2), was made mandatory for all Z-Wave certified devices.

By securing communications between end devices and the hub or gateway, S2 effectively reduces the risk of Z-Wave devices being hacked while they are operating in a network. Common attacks such as man-in-the-middle, replay, and brute force are virtually powerless against the S2 framework through implementation of the industry-wide accepted AES-128 encryption standard. The use of QR or pin-codes on the devices uniquely differentiates them so they can be added to a particular network with ease.

Z-Wave also released the SmartStart protocol, which enables the pre-configuration of devices to the network by security dealers and installers prior to installation which dramatically reduces time spent on-site, thereby reducing costs and maximizing ROI for dealers and integrators. With SmartStart, devices are pre-configured to the network so that devices only need to be physically mounted and powered on which reduces installation time and costs.

The next generation of Z-Wave's technology platform is under development and has been unveiled to the public. Z-Wave 700 series will include numerous performance and technological enhancements in energy-efficiency and RF performance to power the

context-aware smart home. Z-Wave 700-Series is a long range, low power and future-proof hardware platform with integrated software tools and building blocks enabling a whole new generation of Z-Wave sensor devices.

As of 2018, there are more than 100 million interoperable Z-Wave devices in the market representing 70 percent of the smart home market in the U.S., with over 2,500 Z-Wave products certified by the Z-Wave Alliance. The Z-Wave Alliance [9] is a consortium of companies in the space creating these devices, who are focused on the continued interoperability and expansion of Z-Wave devices.

3.4 Long-Range Low Power – LORA and Sigfox

While both ZigBee and Z-Wave provide coverage of up to 300m per radio hop, they are not meant for long range low power wireless networks. This explains why LORA [10] and Sigfox [11] were introduced. LORA is led by Semtech Inc. and LORA radios work at the unlicensed ISM bands of 868MHz and 915MHz and has a further transmission range of up to 10Km. LORA is designed for IoT and M2M networks. Sigfox, on the other hand, is also a proprietary low power, low data rate, long range wireless technology operating at 868MHz/902MHz. Both LORA and Sigfox exhibit star network topology and are suitable for smart grid and smart metering applications.

3.5 Sensor Networks for the Environment

While home appliances may or may not have sensors, sensor networks used for the environment have gained popularity. They are used to measure air quality, humidity, noise, earthquakes, etc. With the push for a greener living environment, more government agencies are stepping up to provide accurate distributed environmental sensing. Sensors are distributed around the observed area and data are continuously collected and relayed to the control station for processing. For ease of deployment, most sensors use wireless communications to relay sensor data. Hence, sensor networks are another form of mobile ad hoc networks, but with less mobility. The issues addressed here are:

- low power protocols
- low bandwidth situations
- data aggregation methods, and
- how to design large scale operational and distributed sensor networks.

Sensor networks can be used for various verticals, such as agricultural, transport, health, rescue operations, etc. Sensors can also be mounted on moving objects such as buses, motorbikes, bicycles, etc., to collect sensor data in various locations, enabling distributed coverage of the area to be sensed.

3.6 V2X Networks for Transport

Mobile ad hoc networks have also given birth to vehicular ad hoc networks (VANETs), where cars could talk among themselves (V2V) (form a wireless network on-the-fly when in proximity), or to any roadside infrastructures (V2I). Recently, there is also V2X – effectively talking to any object or device within proximity. The IEEE 802.11p standard addresses this issue at the PHY and MAC layers, focusing on:

a. Operating frequency
b. Higher rate of mobility
c. Real-time requirements
d. Use of Alert Messages

VANETs can take the form of mesh or star topology, and communications among cars can help exchange vital data (such as location, speed, etc.) used to avoid accidents, congestion, overcome blind spots, summon for rescue operations, detect speeding or dangerous vehicles (for example, drunk drivers and criminals on-the-run) on the road, etc. It is envisaged that all future smart cars (including autonomous vehicles) will have some sort of V2X capability. Hence, ad hoc networks have impact on transportation too, in addition to numerous other applications in deployment and in use today.

The different types of mobiles ad hoc networks technology are specially addressed to the following spectrum of vertical applications:

- **WiFi Ad Hoc & Low Power Ad Hoc:**
  - Transport – VANET V2X
  - Smart Home – ZigBee, Z-Wave,
  - Smart Office,
  - Smart Buildings,
  - Smart Phone Peer Networks,
  - Disaster Rescue,
  - Smart Metering,
  - Smart Street Lights, and
  - Smart Logistics.

- **Sensors Ad Hoc:**
  - Agriculture,
  - Environmental Monitoring,
  - Factory automation – M2M,
  - Natural Disaster monitoring,
  - Health monitoring, and
  - Transport – self driving cars.

- **Tactical Ad Hoc:**

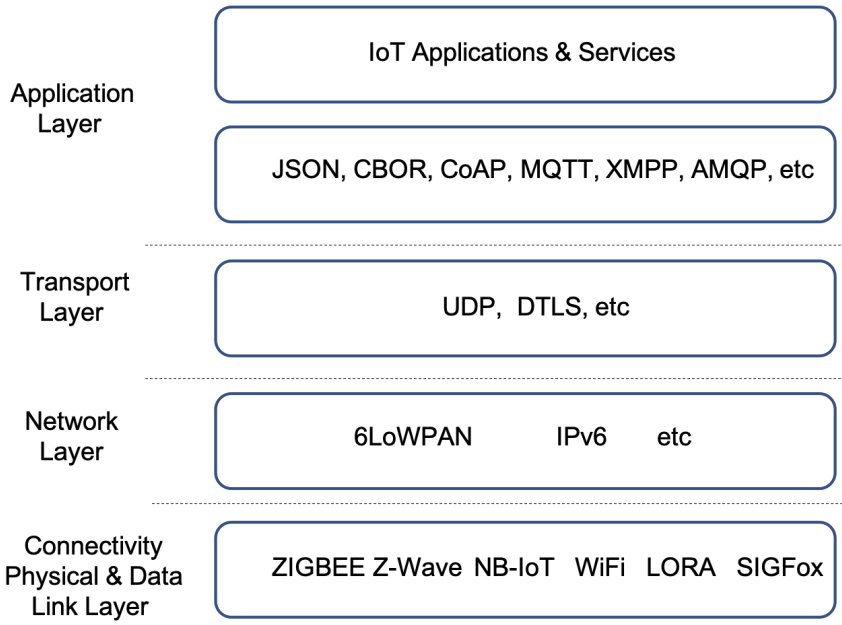
- Army tactical ad hoc radios,
- Ad hoc robots,
- UAV ad hoc,
- Explosive hopping mines, and
- Navy ship area ad hoc.

4. IoT: Market, Types & Technologies

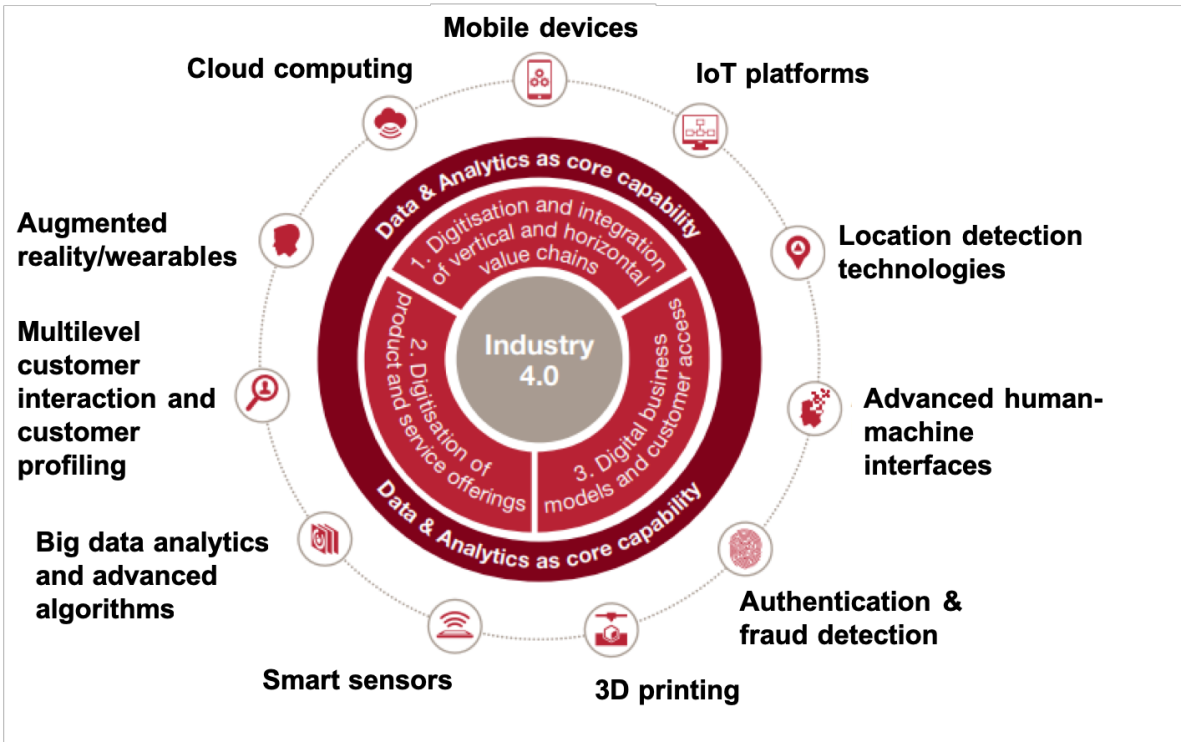
4.1 IoT Predicted Market Share: According to Intellipaat [12], $6Billion will be spent on IoT technologies from 2016 – 2021 and estimated revenue will be $13 Trillion by 2025. According to Statista, the size of IoT worldwide market would hit 2.225Trillion in 2020 and by 2025, with over 75Billion of IoT connected devices to be installed worldwide.

4.2 IoT & Connectivity: IoT is the connection of objects or any devices to the Internet. Hence, IoT needs connectivity. This connectivity is largely enabled through wireless, and in IoT, **device-to-device networking feature** derived from the earlier ad hoc networks is still a necessity. Devices and objects are characterized by low power requirements, the ability to interconnect among themselves, and eventually routed data to the core network or the Internet. Some devices are sensors, while other can be powerful devices capable of streaming large amount of data, such as real-time video.

IoT devices can be interconnected by different connectivity options, such as Bluetooth, WiFi, ZigBee, Z-Wave, NB-IoT, or cellular-IoT (see Fig. 3a) or even wired networks. IoT networks will be heterogeneous, have different devices, and they will carry different size and types of data. Eventually, our Internet of routers will be overlaid with IoT. While the Internet of routers were primarily focusing on user traffic (data and emails), **IoT is about control, intelligence, and automation** – enabling an intelligent and controllable environment. IoT paves the way for the realization of smart cities**. IoT networks can be private and public**, with each domain secured by its own administrative authority, governing whether sensor and IoT data can be shared or not.



(a)



(b)

Figure 3: (a) IoT requires device, connectivity, transport, data, and application layers, and (b) Industry 4.0 and its relation to IoT (Source: PWC report 2016 [13]).

4.3 IoT Type - NarrowBand-IoT (NB-IoT): To handle millions of sensors within a city or country, a single wireless mesh network with 100+ millions of nodes would be difficult to establish, track, and maintain. Telcos have suggested NB-IoT, where cellular base stations can provide coverage to thousands of sensors within a single radio microcell. NB-IoT was standardized in 2016 as 3GPP Release 13. It has a data rate of 25Kbps (DL-OFDMA) and 64Kbps (UL-SCFDMA) and a coverage of 164dB. NB-IoT can operate in several LTE FDD Bands (1,2,3,5,8,11,12,13,17,18,19,20,25,26,28,66,70) with a bandwidth of 180KHz. There are three possible modes of operation: (a) standalone, (b) guard band, and (c) in-band. Both Ericsson and Huawei have NB-IoT solutions on the market.

4.4 IoT Data Analytics: With IoT sensor data gathered through multiple devices, data analytics will yield greater insights into the operation and situation of an environment or system, providing a more accurate understanding of the condition and status, hence allowing fine tuning, fast response, efficient operation, greater safety and automation. Sensor data gathering takes time and different frequencies to gather, and some applications demand for real-time analytics to take place.

4.5 IoT Architecture & Protocols: The architecture basically comprises: (a) things (sensors and devices), (b) gateway, and (c) network (and/or cloud). Examples of gateways are Raspberry Pi and Intel Galileo. Sensor-to-gateway connectivity can be supported through Bluetooth, ZigBee, Z-Wave, WiFi, LORA, or Sigfox. As shown in Fig. 3a, the protocol for messaging can be based on MQTT (Message Queuing Telemetry Transport) or CoAP (Constrained Application Protocol). The gateway to cloud or Internet can be through ethernet, WiFi or even cellular connection. In terms of data flow architecture, one can view IoT as sensing and generating events, performing transport and the collection of data, transformation, processing, and storage of data, with eventual presentation and actuation.

4.6 IoT & Cloud: Recently, there were proposals on putting sensor data onto clouds, be it private or public clouds. Cloud data acquisition in an IoT cloud architecture can be achieved through the use of HTTP server, MQTT server or CoAP server. Also load balancers are used to direct traffic to respective servers in order to avoid overload. Just as web clients access HTTP servers through push-pull API, IoT devices can use the subscribe-publish API to communicate with MQTT servers residing in the cloud.

4.7 IoT Standardization Efforts – Currently, there is no one universal standard for IoT. One may ask what is there to standardize? It is really from the connectivity end, data formatting and handling ends. There is no standard on data analytics that one can use. Without a single standard, there is a need for interoperability and possibly open standards. Currently, there exist many different used cases that will demand for different IoT protocols, data formats, data handling, and interfaces. Hence, it is possible that de facto standards will exist and interoperability will be needed to cater for different IoT implementations, and used cases that have different requirements in terms of bandwidth, range, delay, etc. Issue is IoT application and used cases are too diverse and the industry efforts have been focused and segregated. This explains the current situation.

4.8 IoT Security: IoT security is multi-folded and multi-layered. Device security ensures that it cannot be tampered with. Access control ensures no unauthorized local or remote access to the IoT device. Encryption ensures sensor data cannot be read, interpreted, or copied. Finally, end-to-end security ensures that the identities of devices and collective data cannot be extracted by intruders on the IoT network.

4.9 Description of Things: Currently, each IoT device uses a specific data format in its messaging to other devices or to the hub. This format is largely dependent on the communication protocol used, such as MQTT, etc. Due to bandwidth and power constraints in devices, message size is kept short. There is no universal standard message format for all IoT devices in existence today. Lately, there were proposals on an IoT device description language, so as to universally describe content, attributes, services and attachment of things [14].

4.10 Industry IoT Solutions: Industries have been focusing on: (a) devices, (b) connectivity and protocols, (c) software platform (such as Amazon IoT), and (d) data analytics. Many are offering cloud-based IoT platform to provide device registration, connectivity, control, rapid visualization, storage and data analytics functions. In the future, greater integration of these components is necessary to fully realize the potential of IoT. Table 4 shows a list of some industry IoT products and solutions.

Table 4: Industry IoT products and solutions.

Companies	Product Type	Remarks
Amazon	Amazon IoT platform	Managed cloud platform, capable of supporting billion of IoT devices.
Microsoft	Azure IoT	Managed cloud platform
IBM	Watson IoT platform	Managed cloud host service
GE Digital	Predix platform	Industrial IoT cloud and edge platform
Google	Google Assist	Smart IoT device for home
Siemens	Mindsphere IoT OS	Industrial-IoT cloud platform
Oracle	IoT Cloud services	Managed cloud platform

4.11 Industrial IoT (I-IoT) & Smart Factories: According to Accenture, I-IoT could add $14.2Trillion to the global economy by 2020 and global market is projected to grow at 7.3% CAGR through 2020. Currently, Siemens and GE are the two major industries primarily focusing on I-IoT and both solutions involved using cloud as the data and processing platform to connect, relay, store, process, and analyze sensor data.

I-IoT has direct impact on Industry 4.0, where digitalization, self-organizing automation and predictive maintenance are essential to drive future efficient production processes and manufacturing operations of smart factories [13].

5. The Rise of Smart Cities

Singapore, London, Paris, and New York have constantly emerged as the top few smart cities of the world in recent rankings [15]. A smart city is viewed as an area of advanced civilization using the latest information and communication technologies to enhance efficiency of business operations and elevate residents' quality of life. IoT is one of the important ICT technologies to enable smart cities, along with connectivity, data analytics and artificial intelligence. Many countries have initiated smart cities projects and invested billions into the development of smart cities. For example, in China alone, more than 300 pilot smart cities projects were initiated. In Singapore, the country introduced the Smart Nation program that focuses on smart homes, smart transport, and smart health. For homes, IoT enables home automation, enhances home safety, home security, monitoring of child and elderly, and allows the efficient use of electric energy. For transportation, IoT has enabled on-demand bus or car shared ride, smart traffic lights, smart street lights, sensor-based self-driving vehicles for communal transport, etc. Finally, for smart health, sensors, artificial intelligence, and data analytics enable health specialists to predict and prescript medical treatment to patients in an advanced and timely manner, providing better healthcare. Hence, IoT, as heterogeneous as it may be, is crucial to the development of future smart cities.

6. Conclusion

Mobile ad hoc networks have provided a fundamental and important feature – that of any device-to-device communications and networking, with or without the presence of device mobility. This key feature paves the way for forming instantaneous device and sensor networks, and it is the precursor to IoT. IoT is crucial to the development of smart cities, with sensing providing data for insights and decision making, enabling smart health, smart transport, smart living and smart e-commerce. IoT will form the next important information grid hovering over the globe, which will impact billions of lives in the coming decade.

Acknowledgement

Thanks to Dr. Erwin Gianchandani of National Science Foundation Directorate for Computing and Information Science and Engineering, for providing data related to research spending on mobile ad hoc networks.

References

[1] C. Toh, "Wireless ATM and Ad Hoc Networks", Kluwer Academic Press, ISBN 0-7923-9822-X, 1996

[2] C. Toh, "A Novel Distributed Routing Protocol to support Ad Hoc Mobile Computing", IEEE International conference on Computers and Communications, 1996.

[3] C. Toh, “Ad Hoc Mobile Wireless Networks: Protocols and Systems”, Prentice Hall Pubslihers, ISBN 013-007817-4, 2001

[4] C. Perkins, “Mobile IP”, IEEE Communications Magazine, 1997.

[5] D Johnson, Y. Hu, and D. Maltz, “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks”, IETF Draft RFC 4728, 2007.

[6] C. Perkins, “Ad Hoc On Demand Distance Vector Routing”, IETF Draft, 2000.

[7] ZigBee Alliance - https://www.ZigBee.org. Accessed on March 4th, 2019.

[8] ITU-T Recommendation G9959 – “Short Range Narrow-Band Digital Radio Communication Transceivers”, 2015. Available at: https://www.itu.int/rec/T-REC-G.9959-201501-I/en. Accessed on March 4th, 2019.

[9] Z-Wave Alliance – https://z-wavealliance.org. Accessed on March 4th, 2019.

[10] LORA Alliance - https://lora-alliance.org/. Accessed on March 4th, 2019.

[11] Sigfox – http://www.sigfox.com. Accessed on March 4th, 2019.

[12] Intellipaat - “The need for universal standards in IoT” – Available at: https://intellipaat.com/blog/need-universal-standards-internet-things/. Accessed on March 4th, 2019.

[13] PWC, “Industry 4.0: Building The Digital Enterprise” – PWC report, 2016

[14] A. Khaled, S. Helal, W. Lindquist, and C. Lee – “IoT Device Description Language for the T in IoT”, IEEE Access, 2017

[15] Forbes, “The Smartest Cities in the World in 2018”, Forbes Magazine, 2018.

JUAN-CARLOS CANO (jucano@disca.upv.es) is professor and chairman of Department of Information and Computer Engineering at the Universitat Politecnica de Valencia, Spain. He earned an MSc and a Ph.D. in Computer Science from the UPV in 1994 and 2002

respectively. From 1995-1997 he worked as a programming analyst at IBM's manufacturing division in Valencia. His current research interests include Wireless Communications, Vehicular Networks, Mobile Ad Hoc Networks, and Internet of Things.

VICTOR BERRIOS is VP of Technology with ZigBee Alliance, USA. He received his BSEE from Iowa State, MSEE and MBA from Arizona State University.

BEN GARCIA, is a senior Z-wave field application engineer with Silicon Labs, which has taken over the leadership of Z-Wave Alliance from Sigma Design Inc. USA.

CHAI K. TOH (ck_away@hotmail.com) was Group CTO and Assistant Chief Executive at IDA Singapore, and VP and CTO of Singapore Power Telecom Ltd, co-leading the Singapore's Smart Nation program, IoT, data analytics, smart transport, smart utility and smart homes programs. He is an IEEE Fellow (2009) and AAAS Fellow (2009). He is

currently the Tsing Hua Honor Chair Professor of Computer Science at NTHU, Taiwan and an expert with GLG Group USA.

Figure 1: Ad Hoc Networks Research Evolution into Internet of Things (IoT)

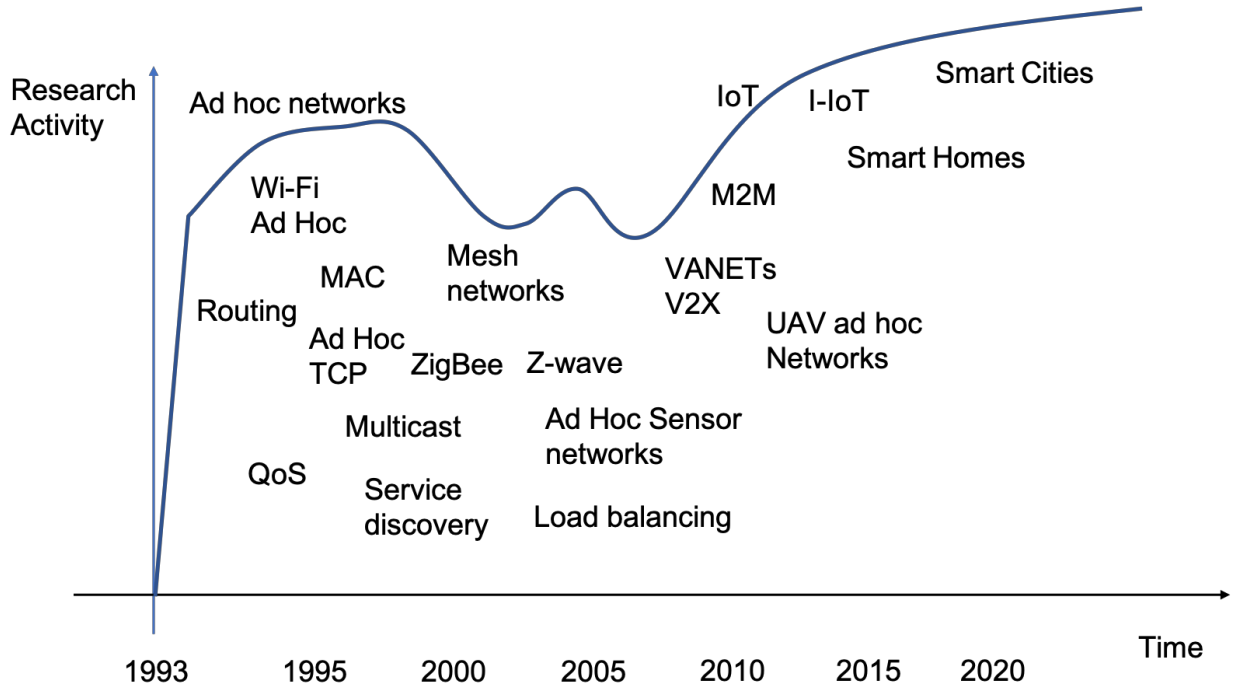


Figure 2: (a) ZigBee architecture and topology, showing the presence of coordinator, routers, and end devices.

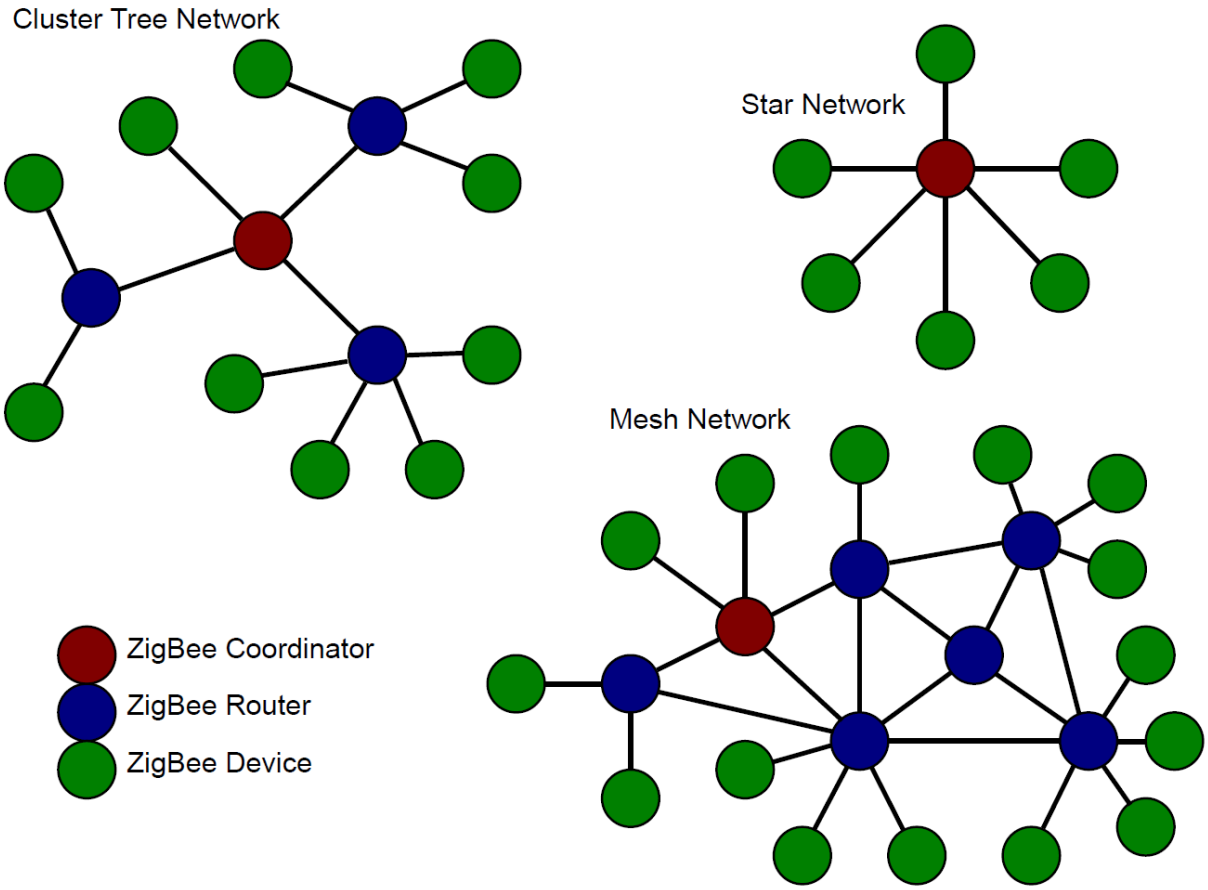


Figure 2: (b) ZigBee 3.0 protocol stack.

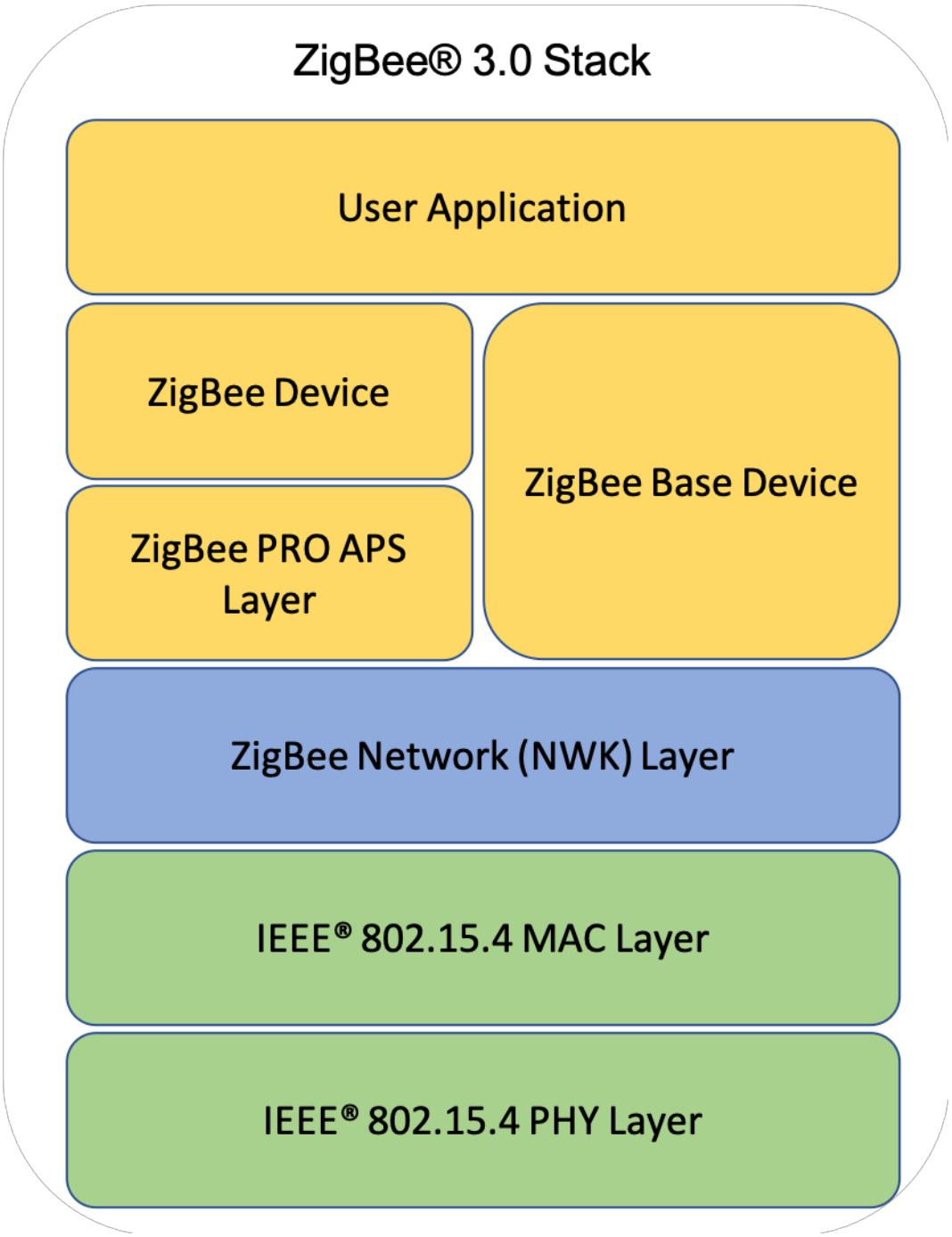


Figure 3: (a) IoT requires device, connectivity, transport, data, and application layers, and (Source: PWC report 2016 [13]).

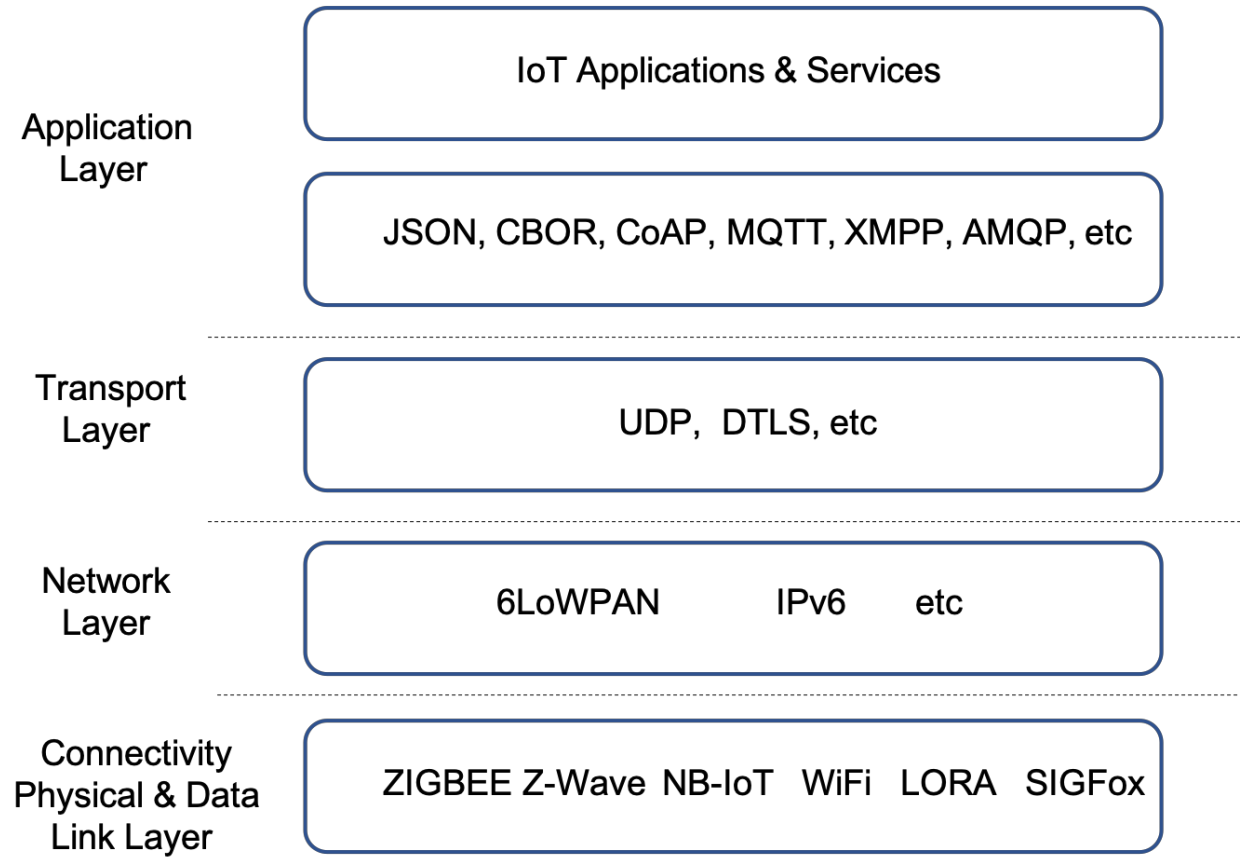


Figure 3: (b) Industry 4.0 and its relation to IoT (Source: PWC report 2016 [13]).