Comparison of 6LoWPAN and LPWAN for the Internet of Things

Article *in* Australian Journal of Electrical and Electronics Engineering · December 2017

DOI: 10.1080/1448837X.2017.1409920

2 authors:

Hayder A. A. Al-Kashoash
Southern Technical University -Iraq

Andrew H. Kemp
University of Leeds

AUSTRALIAN JOURNAL OF ELECTRICAL AND ELECTRONICS ENGINEERING, 2017
https://doi.org/10.1080/1448837X.2017.1409920

Comparison of 6LoWPAN and LPWAN for the Internet of Things

H. A. A. Al-Kashoash[a] and Andrew H. Kemp[b]

[a]Technical Institute/Qurna, Southern Technical University, Basra, Iraq; [b]School of Electronic and Electrical Engineering, University of Leeds, Leeds, UK

ABSTRACT
By 2020, 50 billion devices (things) are expected to be connected to the Internet to form the Internet of Things (IoT) world. In general, two main categories of networks are used in the IoT: short-range and long-range low-power networks. IPv6 over low-power wireless personal area networks (6LoWPAN) are considered to be a crucial network in short-range low-power networks where 6LoWPAN motes will account for the majority of short-range low-power things. Also, LoRaWAN and SigFox are two major networking landscapes and players in long-range, low-power networks or oftentimes called low-power wide area networks (LPWAN). This paper reviews and compares 6LoWPAN and LPWAN in terms of network architecture, protocol stack, applications and security. In general, LPWAN networks are more demanding in terms of node and link constraints than 6LoWPAN networks (e.g. very low payload size, very low data rate and very limited resources). Also, as yet, LPWAN networks do not have IPv6 addressing capabilities. Each network category has its unique characteristics and strengths and each category has its important role in the IoT world.

ARTICLE HISTORY
Received 28 October 2017
Accepted 17 November 2017

KEYWORDS
6LoWPAN; LPWAN; LoRaWAN; SigFox; Internet of Things

1. Introduction

The Internet of Things (IoT) is considered to be the next communication revolution and the next big challenge for the communication research community. The IoT will comprise billions of intelligent communicating devices which extend the border of the world with physical entities and virtual components (Li, Da Xu, and Zhao 2015). These things are connected to the Internet with the ability to sense status and condition, and use real-time data whilst also accessing historical data and developed algorithms, possibly triggering devices, leading to very powerful smart environments (home and building), health care, etc.

Generally, two main categories of networks are deployed in the IoT: short-range and long-range, low-power networks (Conran 2016). The short-range, low-power networks, sometimes called 'last 100 meters of connectivity' represent a large fraction of the potential number of things, e.g. IPv6 over low-power wireless personal area networks (6LoWPAN), radio frequency identification (RFID), near-field communication (NFC) and Bluetooth low energy (BLE) (Andersson 2013). 6LoWPAN is a key part of the IoT where the 6LoWPAN motes will account for the majority of the 'last 100 meters of connectivity' things (Dunlap 2011; Al-Kashoash, Hafeez, and Kemp 2017; Al-Kashoash et al. 2017). The long-range low-power networks or sometimes called low-power wide area networks (LPWAN) are designed and used for long-range communications at low-power consumption and low data rate e.g. SigFox, long-range wide area network (LoRaWAN), Wi-SUN, narrow-band IoT (NB-IoT), etc. (Nolan, Guibene, and Kelly 2016). The LPWAN devices are expected to be approximately 25% of overall IoT things (Raza, Kulkarni, and Sooriyabandara 2017). SigFox and LoRaWAN are already widely used and deployed. The SigFox network covers 29 countries over 1.7 million km^2, with 471 million devices according to the SigFox official website (SIGFOX 2017).

Both 6LoWPAN and LPWAN will play a crucial role in the IoT world where each network type has its unique characteristics and applications. Recently, many papers review, compare and evaluate different LPWAN technologies for the IoT. In Bouleogeorgos, Diamantoulakis, and Karagiannidis (2016) compare and discuss the design specifications of LPWAN technologies and their suitability for different IoT applications. In Raza, Kulkarni, and Sooriyabandara (2017) survey different LPWAN standards and technologies where they concluded that LPWAN technologies adopt similar approaches and have the same limitations and challenges. In Nolan, Guibene, and Kelly (2016) survey and evaluate SigFox and LoRaWAN for the IoT in terms of physical and MAC layers. Also, they conducted an experimental evaluation for outdoor range test estimation for SigFox technology. In Mikhaylov et al. (2016) discuss and analyse the

CONTACT H. A. A. Al-Kashoash hayderaam@stu.edu.iq

LoRaWAN technology in terms of network scalability and uplink throughput. They concluded that a base station may serve several million end nodes and the uplink channel capacity of a node depends on the distance and does not exceed 2 kbps. In Adelantado et al. (XXXX) overview the capabilities and limitations of LoRaWAN in terms of network size, reliability and network capacity. Bor, Vidler, and Roedig (2016) investigate the capacity limits of LoRaWAN where experimental results show that LoRaWAN networks can scale quite well if they use dynamic transmission parameter selection and/or multiple base stations; otherwise, they do not. However, according to our best knowledge, none of these consider and compare between 6LoWPAN and LPWAN. In this paper, we consider and compare 6LoWPAN and LPWAN (LoRaWAN and SigFox) with various aspects, e.g. network architecture, protocol stack, applications and security aspects. The constraints of LPWAN networks are more demanding than 6LoWPAN networks. LPWAN is characterised by node constraints (e.g. very low cost, very limited processing capabilities, very small memory size and very low energy consumption) and link constraints (very short payload length and very low bandwidth). Also, unlike 6LoWPAN, LPWAN nodes do not currently have IPv6 addressing capabilities. The Internet Engineering Task Force (IETF) LPWAN working group created in 2016 is working to adapt IETF defined protocols and bring IPv6 addressing to LPWAN.

The remainder of the paper is organised as follows: in Section II, we overview and compare the network architecture of 6LoWPAN and LPWAN. Section III compares the physical layer of 6LoWPAN, LoRaWAN and SigFox. The main aspects of the MAC layer for 6LoWPAN, LoRaWAN and SigFox are given in Section IV. Section V overviews and compares the upper layers and applications of 6LoWPAN and LPWAN. Section VI explains security mechanisms used in 6LoWPAN, LoRaWAN and SigFox networks. Finally, Section VII draws the conclusions.

2. Network architecture

The 6LoWPAN network architecture contains three elements: host node, router node and edge router as shown in Figure 1 (Kushalnagar, Montenegro, and Schumacher 2007). The hosts can sense the physical environment and actuate devices. The routers are intermediate nodes that forward data packets from the hosts to the edge routers or to a destination inside the 6LoWPAN network. The connection among 6LoWPAN elements is implemented via IPv6 over IEEE 802.15.4. The edge routers provide interconnection and traffic management (e.g. Neighbor Discovery (ND) and handling IPv4 interconnectivity) between 6LoWPAN network and other IP networks (typically the Internet). Sending and receiving packets between 6LoWPAN elements and IP nodes in other networks occur in an end-to-end scheme similar to any IP nodes where each 6LoWPAN element is identified by a unique IPv6 address.

The LoRaWAN and SigFox networks consist of four elements: end node (end point), gateway (base station), network server (SigFox cloud) and end user application (device application) as shown in Figure 2 (Sornin et al. 2015; Nolan, Guibene, and Kelly 2016). LoRaWAN (SigFox) network architecture is a star topology where gateways are transparent bridges between end nodes and network server. End nodes are connected to the network server by a single hop wireless communication (LoRa RF and SigFox LTN radio), while gateways are connected to the network server by backhaul (cellular, Wi-Fi, Ethernet or satellite). In LoRa and SigFox networks, the end nodes cannot communicate with each other directly as in 6LoWPAN networks. This will save energy as end

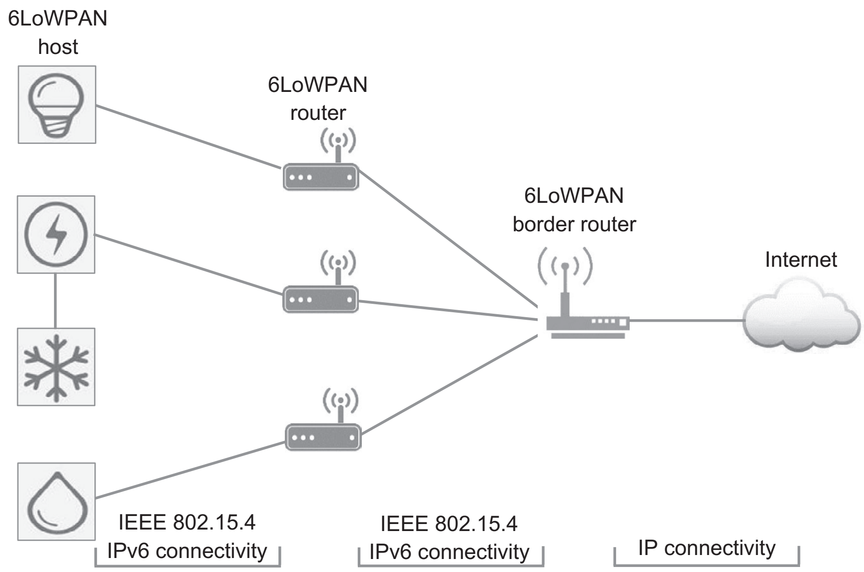

Figure 1. 6LoWPAN network architecture.

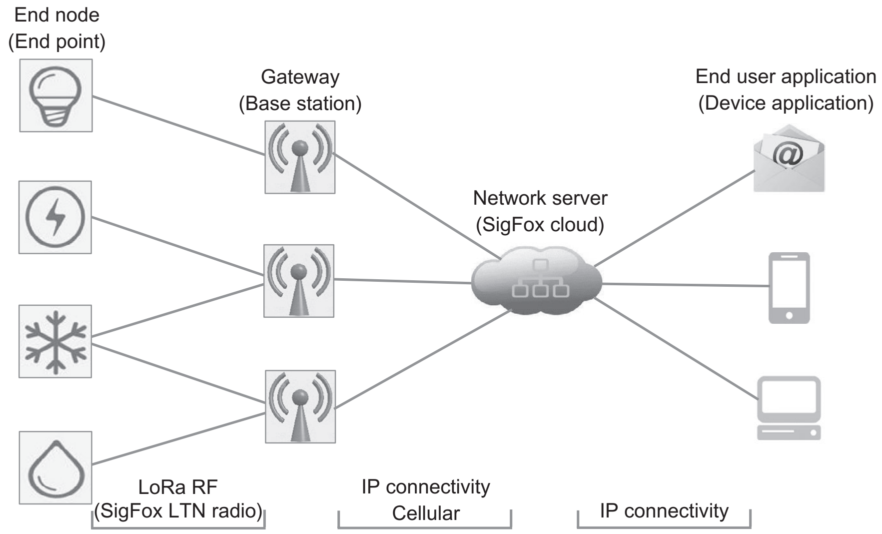

Figure 2. LoRaWAN and SigFox networks architecture.

nodes do not work as relays for forwarding messages (Marshall 2016).

The main differences between 6LoWPAN and LPWAN (LoRaWAN and SigFox) in term of network architecture are topology and distance between end nodes and intermediate nodes. In 6LoWPAN networks, host (end) node can communicate with other host nodes directly. Whereas, in LoRaWAN and SigFox, end nodes can communicate only with gateways and they cannot send packets directly to other end nodes. This organises the network as a star topology centred at the network server (SigFox cloud) as shown in Figure 2. Also, this eliminates the need for a routing topology as each end node knows where to forward its packets directly. The other main difference is the distances between end nodes and intermediate nodes. In the case of 6LoWPAN networks, the distance is 10 –100 m, whereas for LoRaWAN and SigFox, it is 5–50 km. This means that many 6LoWPAN nodes have to be distributed to cover a small area (i.e. high node density). On the other hand, a small number of base stations can cover a whole city. Other architectural considerations are host (end node) visibility and mobility. An IP node in other networks can communicate directly with a 6LoWPAN node as it has a unique IPv6 address (i.e. the host is visible to other IP nodes). However, IP nodes cannot communicate with LPWAN end nodes directly. Also, mobility in 6LoWPAN presents unique challenges to the 6LoWPAN architecture where the standard 6LoWPAN protocol stack does not support mobility (Mulligan, Huo, and Williams 2010); however, LoRaWAN and SigFox do.

3. Physical layer

At the bottom of the communication model the physical layer defines the hardware equipment, frequencies, communication medium, modulation, etc. Table 1 compares the physical layer parameters and characteristics for 6LoWPAN, LoRaWAN and SigFox networks. IEEE 802.15.4 standard (LAN/MAN-Standards-Committee et al. 2003) defines the physical layer for 6LoWPAN networks. The IEEE 802.15.4 physical layer provides the following services: activation and deactivation of radio transceiver, energy detection of the current channel, link quality indication (LQI), channel selection, clear channel assessment (CCA) and transmitting and receiving packets through the wireless channel. The 6LoWPAN physical layer parameters are shown in Table 1.

The physical layer of the LoRaWAN network is called LoRa which is a chirp spectrum modulation technique for long-range, low data rate and low-power wireless communications (Adelantado et al. XXXX). The main features of LoRa RF are low-cost, low energy consumption, secure bidirectional communications and most important, long range where a single gateway has a coverage of hundreds of square kilometres. The LoRa radio has four configuration parameters: carrier frequency, spreading factor, bandwidth and coding rate (Bor, Vidler, and Roedig 2016). These parameters allow multiplexing of signals on a single frequency and hence, increasing the network capacity and dynamic adaptation of data rates. The SigFox physical layer employs ultra narrow band technology which is the key to provide a scalable, high-capacity network and very low power consumption. The SigFox radio provides mono- and bidirectional communications over longer distances than LoRa. The SigFox radio uses frequency hopping to avoid signal interception, hence improving security and to limit the impact of interference (LinkLabs 2016). LoRa and SigFox radio parameters are also shown in Table 1.

The main features of LPWAN (LoRaWAN and SigFox) radio are long-range, very low data rate, very low power consumption, very low channel bandwidth, very low receiver sensitivity and sub-1-GHz band transceiver. On the other hand, IEEE 802.15.4 radio operates

Table 1. Physical layer parameters Of 6LoWPAN, LoRaWAN And SigFox.

Parameter	6LoWPAN	LoRaWAN	SigFox
Frequency band	2400–2483.5 MHz (worldwide) 902–929 MHz (North America) 868–868.6 MHz (Europe)	902–928 MHz (North America) 863–870 MHz and 434 MHz (Europe) 779–787 MHz (China)	902 MHz band (America) 868 MHz band (Europe)
Number of channels	16 channels for 2.4 GHz band 10 channels for 915 MHz band 1 channel for 868.3 MHz band	80 channels for 915 MHz band 10 channels for 868 MHz band and 780 MHz band	360 channels + 40 channels are reserved (not used)
Channel bandwidth	5 MHz for 2.4 GHz band 2 MHz for 915 MHz band 600 kHz for 868.3 MHz band	125 kHz and 500 kHz for 915 band 125 kHz and 250 kHz for 868 MHz band and 780 MHz band	100 Hz – 1.2 kHz
Maximum data rate	250 kbps for 2.4 GHz band 40 kbps for 915 MHz band 20 kbps for 868.3 MHz band	980 bps–21.9 kbps for 915 band 250–50 kbps for 868 MHz band and 780 MHz band	100 bps – 600 bps
Protocol data unit	6 bytes header + 127 bytes SDU	variable number of bytes header + (19 to 250) bytes	12 bytes header + (0 to 12) bytes
Channel coding	Direct Sequence Spread Spectrum (DSSS)	Chirp Spread Spectrum (CSS)	Ultra narrow band coding
Channel modulation	O-QPSK for 2.4 GHz band BPSK for 915 MHz band BPSK for 868.3 MHz band	LoRa for 915 MHz band LoRa and GFSK for 868 MHz band and 780 MHz band	BPSK and GFSK
Receiver sensitivity	−85 dBm for 2.4 GHz band −92 dBm for 915 MHz band −92 dBm for 868.3 MHz band	−137 dBm	−137 dBm
Transmission range	10–100 m	5–15 km	10–50 km
Battery lifetime	1–2 years	<10 years	<10 years

in three frequency bands with short-range, low data rate (but higher than LPWAN radio by a factor of between 5 and 2500) and low power consumption.

4. MAC layer

IEEE 802.15.4 standard defines the MAC layer for 6LoWPAN networks. The IEEE 802.15.4 defines two types of devices which can participate in the network; a full-function device (FFD), which has full levels of functionality and can serve as a coordinator, and a reduced function device (RFD) which has more limited functionality. The IEEE 802.15.4 MAC layer has the following features: beacon management, channel access, guaranteed time slot (GTS) management, frame validation, acknowledged frame delivery, association and disassociation. The IEEE 802.15.4 standard defines two types of channel access mechanism: non-beacon enabled, which uses un-slotted CSMA/CA, and beacon enabled mode where slotted CSMA/CA is used. Also, the IEEE 802.15.4 MAC layer defines four frame structures: data frame, beacon frame, acknowledgement frame and MAC command frame. The general frame format is shown in Figure 3 with the maximum MAC frame size of 127 bytes.

LoRaWAN is the MAC protocol for LoRa nodes and it is an open standard maintained by LoRa Alliance. LoRaWAN MAC protocol uses a simple ALOHA protocol as a channel access mechanism (Bardyn et al. 2016). LoRaWAN offers fully bidirectional symmetrical and secure links between end nodes and gateways. Also, LoRaWAN defines three types of devices: Class A, Class B and Class C (Sornin et al. 2015). Class A end nodes allow for bidirectional communications where each uplink transmission is followed by two short downlinks receive windows. In Class B, end nodes allow for more receive slots where nodes open extra receive widows at scheduled times. Class C nodes have nearly continuous open receive windows where nodes close only when transmitting. In general, Class C nodes use more energy and offer less latency than Class A and Class B nodes. LoRaWAN MAC protocol supports a payload ranging from 19 bytes to 250 bytes with protocol overhead ranging from 12 bytes to 28 bytes depending on regional specifications (LoRa-Alliance-Technical-committee 2016). The physical and MAC message format is shown in Figure 4 where PHDR is the physical header, CRC is cyclic redundancy check, MHDR is MAC header, FHDR is frame header, FPort is port field and MIC is message integrity code. The length of preamble field is variable and depends on LoRaWAN regional parameters and

Physical header			MAC header						MAC Payload	MAC header
Octets: 4	1	1	2	1	0/2	0/2/8	0/2	0/2/8	variable	2
Preamble	Start frame delimiter	Frame length	Frame control	Sequence number	Destination PAN identifier	Destination address	Source PAN identifier	Source address	Payload	Frame check sequence

Figure 3. IEEE 802.15.4 physical and MAC frame format (LAN/MAN-Standards-Committee et al. 2003).

Octets: *	*	*	1	7 – 22	0 – 1	*	4	*
Preamble	PHDR	PHDR_CRC	MHDR	FHDR	FPort	Frame payload	MIC	CRC**

* the length is variable ** this field is for uplink packet only

Figure 4. LoRaWAN message format (Sornin et al. 2015).

modulation scheme, e.g. in Europe and China regions, the preamble length is 8 symbols for LoRa modulation and 5 bytes for GFSK modulation and in America region, it is 8 symbols for LoRa modulation. For more information about regional parameters, please refer to (LoRa-Alliance-Technical-committee 2016). The symbol duration (T_s) is not constant and depends on bandwidth (BW) and the selected spreading factor (SF) where $T_s = 2^{SF}/BW$. The length of many fields in LoRa messages is variable and depends on regional parameters. For more information, please refer to LoRa-Alliance-Technical-committee (2016), and Sornin et al. (2015).

SigFox is not an open protocol and there is little information available about it. In general, SigFox MAC protocol uses the ALOHA protocol as a wireless channel access mechanism (Raza, Kulkarni, and Sooriyabandara 2017). SigFox MAC can send up to 14 messages per day. The format of uplink and downlink frames is shown in Figure 5. The length of SigFox MAC frame (overhead plus payload) ranges from 14 bytes to 29 bytes for uplink frames and from 20 bytes to 28 bytes for downlink frames.

5. Upper layers and applications

The 6LoWPAN protocol stack defines an adaptation layer which is located between the network layer and the MAC layer to enable transmission of IPv6 packets over an IEEE 802.15.4 link. The adaptation layer has three main functions: IPv6 header compression, IPv6 fragmentation and reassembly, and routing. As the IEEE 802.15.4 frame overhead is 25 bytes without security support (which needs an additional 21 bytes), the remaining frame size at the MAC layer is 102 bytes without security and 81 bytes with security support. For an IPv6 header of 40 bytes and a UDP header of 8 bytes, there is only a maximum 54 bytes for application payload. Therefore, IPv6 header compression is very important to reduce overhead and increase application payload space. RFC 6282 (Hui and Thubert 2011) defines how to compress the IPv6 and UDP headers efficiently using improved header compression (IPHC) and next header compression (NHC) methods.

IEEE 802.15.4 defines the maximum transmission unit (MTU) of 127 bytes, while IPv6 requires packet transmission with MTU of 1280 bytes. To address this apparent contradiction, the next major function of the adaptation layer is IPv6 fragmentation and reassembly. When an IPv6 packet does not fit into a single IEEE 802.15.4 data frame, the packet is divided into fragments each of which is sent over a single IEEE 802.15.4 frame. When all fragments are received at the destination, the IPv6 packet is reassembled and delivered up to the network layer. RFC 4944 (Montenegro et al. 2007) specifies how an IPv6 packet is divided into a FRAG1-type fragment and a number of FRAGN-type fragments. FRAG1 contains the IPv6 compressed header and part of the payload, while FRAGN fragments are sent subsequently and contain the remaining payload. Besides the above two functions, the adaptation layer supports the 'mesh-under routing' scheme to forward packets inside the 6LoWPAN network.

After the implementation of the adaptation layer in the 6LoWPAN architecture, it is possible to take routing/forwarding decisions either in the network layer or in the adaptation layer. Generally, routing protocols in 6LoWPAN can be divided into two categories: 'mesh-under' and 'route-over' (Chowdhury et al. 2009). With the mesh-under scheme, the adaptation layer performs the packet routing and forwarding over multiple hops based on the 6LoWPAN header or the IEEE 802.15.4 link layer address. In the route-over, all routing decisions are taken in the network layer and packets are forwarded to the final destination using IPv6 addresses. One of the important routing protocols for 6LoWPAN networks is the IPv6 routing protocol for low-power and lossy networks (RPL) (Winter et al. 2012) which was developed by the RoLL working group to meet the requirements and challenges of low-power and lossy networks (LLNs). RPL is a distance vector routing protocol which organises the network as a Directed Acyclic Graph (DAG) routed at the sink. It constructs the network topology by using an objective function which defines how routing metrics are computed to obtain a Rank value. The Rank value represents a nodes' position in the graph and the node selects

Uplink frame

Bits: 19	29	32	0 – 96	16 – 40	16
Preamble	Frame synch	Dev ID	Payload	Msg Auth. Code	FCS

Downlink frame

Bits: 91	13	32	0 – 64	16	8
Preamble	Frame synch	ECC	Payload	Msg Auth. Code	FCS

Figure 5. SigFox frame format (Zuniga and Ponsard 2016).

its parent based on the Rank. RPL is expected to be the standard routing protocol for 6LoWPAN networks.

As yet, LoRaWAN and SigFox networks do not support IPv6. Thus, they do not have an adaptation layer as in 6LoWPAN architectures. The constraints of LPWAN networks are more demanding than 6LoWPAN networks (e.g. very low payload length and very low data rate). So, it is a challenge for the 6LoWPAN fragmentation and compression mechanisms to be used for enabling IPv6 over LPWAN. Now, the IETF LPWAN working group is working to bring IPv6 to LPWAN networks (Farrell 2016). With regard to routing, the LoRaWAN and SigFox networks have a star topology. A point-to-point connection exists between an end node and a gateway. So, there is no need for routing at the network layer with the existing architecture.

Connecting wireless sensor nodes to the Internet through the 6LoWPAN protocol stack makes use of most of the Internet application protocols are equally important for 6LoWPAN networks (Shelby and Bormann 2009). Also, this enables a wide range of applications where 6LoWPAN networks are applicable for home and building automation, health care automation, logistics, industrial automation, smart metering and smart grid infrastructures, environmental monitoring and vehicular automation. However, the main limitation of 6LoWPAN networks is short-range connectivity where 6LoWPAN nodes cannot be distributed over large geographical areas. The typical personal operating space (POS) of a 6LoWPAN node is from 10 to 100 m. On the other hand, LPWAN networks promise and enable very long-range devices to spread and move over wide coverage areas (Raza, Kulkarni, and Sooriyabandara 2017). LPWAN networks are an excellent candidate and suitable for IoT applications which require extended coverage areas (Bouleogeorgos, Diamantoulakis, and Karagiannidis 2016). For example, in the case of the SigFox network, a small number of base stations can cover a whole city. However, the limitation of LPWAN networks (especially SigFox) is very low data rate, e.g. the maximum number of messages per day for SigFox network is 14. Thus, LPWAN networks are not suitable for high data rate applications, e.g. real-time monitoring. Also, LPWAN networks can carry very short payload (e.g. the maximum payload of SigFox is 12 bytes). Thus, LPWAN networks are not suitable for applications that require large payload, e.g. video streaming.

6. Security

As the number of devices connected to the IoT world is increasing day by day, security becomes one of the biggest issues in the IoT. In 6LoWPAN networks, security can be handled at three layers: MAC, network and application (Hennebert and Dos Santos 2014). IEEE 802.15.4 MAC layer implements security services to achieve data encryption and authentication. IEEE 802.15.4 defines different security suites which can be mainly classified into null (no security), encryption only (AES-CTR), authentication only (AES-CBC) and encryption and authentication (AES-CCM) (LAN/MAN-Standards-Committee et al. 2003). For all security suites, the advanced encryption standard (AES) algorithm should be used. Each security suite offers a set of different security properties and guarantees where an application has to specify its security requirements and an appropriate security suite. At the network layer, IPsec protocol suite can be used to authenticate and encrypt each IP packet. Also, at the application layer, datagram transport layer security (DTLS) can be used to secure the network traffic.

LoRaWAN defines two main security keys: NwkSKey and AppSKey where each key has a length of 128 bits. The NwkSKey session key is used to provide data integrity between the end user and the network server (i.e. it is used for network layer security and checking the message validity). The AppSKey is used to provide data confidentiality between the end node and the network server or the end user application (i.e. it is used to encrypt and decrypt the application payload). The application payload is encrypted using AES-128 algorithm. In SigFox networks, the radio protocol provides a mechanism for message authentication and integrity using a unique device ID and a message authentication code (Zuniga and Ponsard 2016). Each message is signed using a key (device ID) which is flashed inside the device by a manufacturer. This ensures that the message has been generated and sent by the device with its ID in the message (VT-Networks 2016). However, SigFox does not provide an encryption mechanism to encrypt data sent in the message payload where an attacker in the middle can read the messages.

7. Conclusions

In this paper, we reviewed and compared 6LoWPAN and LPWAN network architectures. Three main elements exist in the 6LoWPAN architecture: host node, router node and edge router where network topology is organised as a DODAG routed at the edge router. While, four main elements exist in LPWAN network: end node, gateway, network server and user application with network topology organised as a star. Next, we compared between 6LoWPAN and LPWAN in terms of protocol stack. There are many differences between them in different aspects, e.g. physical layer characteristics (channel bandwidth, data rate, packet length, channel modulation, transmission range and battery lifetime), MAC layer (frame format, payload length and wireless channel access) and upper layers (LPWAN does not have an adaptation layer as in 6LoWPAN and LPWAN does not need a routing protocol, while RPL is used in 6LoWPAN as the routing protocol). After that, we compared between applications of 6LoWPAN and LPWAN networks where each network has its unique features to be used for different applications with various requirements. Finally, we compared security aspects of 6LoWPAN, LoRaWAN and SigFox where the level of security in 6LoWPAN networks is higher than LoRaWAN and SigFox as 6LoWPAN connected to the Internet through IPv6 and IEEE 802.15.4 MAC provides a variety of security suites. Also, the level of security in LoRaWAN is higher than SigFox where LoRaWAN provides encryption mechanisms which SigFox does not.

To sum up, the IoT is a huge umbrella under which are grouped a collection of technologies (e.g. 6LoWPAN, BLE, Wi-Fi, HaLow, LPWAN, Ethernet) where each technology aims to provide the best solution and lead the IoT world. IoT applications are diverse with various requirements (e.g. range, data rate, security level, power demand, latency, reliability level). Each technology has its unique key characteristics in addition to other characteristics (e.g. connectivity, coverage area, radio technology, channel capacity, power consumption, security, mobility, reliability, latency). We believe that each technology has its part in the whole IoT mission and each has its own role that compliments the other technologies roles (i.e. success of each technology supports the success of the overall IoT goal). The real long-term challenge will be the successful co-existence of all these technologies.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Adelantado, F., X. Vilajosana, P. Tuset-Peiro, B. Martinez, and J. Melia. 2016. "Understanding the Limits of LoRaWAN." arXiv.

Al-Kashoash, H. A. A., M. Hafeez, and A. H. Kemp. 2017. "Congestion Control for 6LoWPAN Networks: A Game Theoretic Framework." *IEEE Internet of Things Journal* 4 (3): 760–771.

Al-Kashoash, H. A., H. M. Amer, L. Mihaylova, and A. H. Kemp. 2017. "Optimization Based Hybrid Congestion Alleviation for 6LoWPAN Networks." *IEEE Internet of Things Journal* .

Andersson, M. 2013. Short-range Low Power Wireless Devices and Internet of Things (IoT). *Wireless Congress*. Munich.

Bardyn, J.-P., T. Melly, O. Seller, and N. Sornin. 2016. "IoT: The Era of LPWAN is Starting Now." In *42nd European Solid-State Circuits Conference (ESSCIRC)*, 25–30. Lausanne: IEEE.

Bor, M., J. E. Vidler, and U. Roedig. 2016. "LoRa for the Internet of Things."

Bouleogeorgos, A.-A. A., P. D. Diamantoulakis, and G. K. Karagiannidis. 2016. "Low Power Wide Area Networks (LPWANs) for Internet of Things (IoT) Applications: Research Challenges and Future Trends." arXiv preprint arXiv:1611.07449.

Chowdhury, A. H., M. Ikram, H.-S. Cha, H. Redwan, S. Shams, K.-H. Kim, and S.-W. Yoo. 2009. "Route-over vs Mesh-under Routing in 6LoWPAN." In *Proceedings of the International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, 1208–1212. Leipzig: ACM

Conran, M. 2016. "Internet of Things (IoT) Networking." Accessed February 19, 2017. http://networkinsight.net/2016/11/internet-of-things-iot-networking/

Dunlap, J. 2011. "From Billing and Technology Convergence to Ecosystem Convergence: Why M2M Matters to Your Business." *Pipeline: Technology for Service Providers* 8 (7): 1–3.

Farrell, S. 2016. "LPWAN Overview draft-Ietf-lpwan-overview-00." LPWAN Working Group. 1–35. IETF.

Hennebert, C., and J. Dos Santos. 2014. "Security Protocols and Privacy Issues into 6LoWPAN Stack: A Synthesis." *IEEE Internet of Things Journal* 1 (5): 384–398.

Hui, J., and P. Thubert. 2011. "Compression Format for IPv6 Datagrams Over IEEE 802.15. 4-Based Networks." IETF RFC 6282.

Kushalnagar, N., G. Montenegro, and C. Schumacher. 2007. "IPv6 over Lowpower Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals." IETF RFC 4919.

Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std. 802.15.4. 2003.

Li, S., L. Da Xu, and S. Zhao. 2015. "The Internet of Things: A Survey." *Information Systems Frontiers* 17 (2): 243–259.

LinkLabs. 2016. "SigFox Vs. LoRa: A Comparison between Technologies & Business Models." Accessed February 07, 2017. https://www.link-labs.com/blog/sigfox-vs-lora

LoRa-Alliance-Technical-committee. 2016. *LoRaWAN Regional Parameters*. Beaverton, OR: LoRa Alliance.

Marshall, B. 2016. "RF Communications and the Internet of Things – Part 5." Accessed February 07, 2017. https://www.rs-online.com/designspark/rf-communications-andthe-internet-of-things-part-5

Mikhaylov, K., J. Petaj, A. J. Arvi, and T. Haenninen. 2016. "Analysis of Capacity and Scalability of the LoRa Low Power Wide Area Network Technology," In *Proceedings of 22th European Wireless Conference*, 1–6. Frankfurt am Main: VDE.

Montenegro, G., N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks." 2007. IETF RFC 4944.

Mulligan, G., D. Huo, and C. Williams. 2010. Mobility Considerations for 6lowpan Draft-Williams-6lowpan-mob-03.txt.

Nolan, K. E., W. Guibene, and M. Y. Kelly. 2016. "An Evaluation of Low Power Wide Area Network Technologies for the Internet of Things." In *International Wireless Communications and Mobile Computing Conference (IWCMC) IEEE*, 439–444. Paphos.

Raza, U., P. Kulkarni, and M. Sooriyabandara. 2017. "Low Power Wide Area Networks: An Overview." *IEEE Comm Surveys & Tutorials* 19 (2): 855–873.

Shelby, Z., and C. Bormann. 2009. *6LoWPAN: The Wireless Embedded Internet*. Wiley.

SIGFOX. 2017. "SIGFOX Official Website." Accessed February 07, 2017. https://www.sigfox.com/

Sornin, N., M. Luis, T. Eirich, T. Kramp, and O. Hersent. 2015. *LORaWATMSpecifications*. Beaverton, OR: LoRa Alliance.

VT-Networks. 2016. "The Security Protocol of SigFox." Accessed February 07, 2017. http://vtnetworks.ie/wp-content/uploads/2016/12/Sigfox-Security.pdf

Winter, T., P. Thubert, A. Brandt, J. Hui, and R. Kelsey. 2012. "RPL: IPv6 Routing Protocol for Low-power and Lossy Networks." IETF, RFC 6550.

Zuniga, J., and B. Ponsard. 2016. *SIGFOX System Description draft-zunigalpwan-sigfox-system-description-01*. IETF.