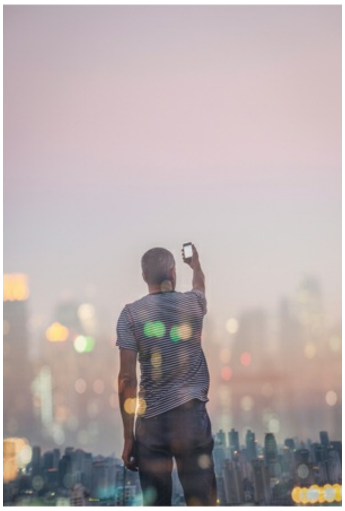
Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 13, Issue 8

Shaping the Future of IoT



By: Sanjay Khatri

New technologies and standards like LPWAN and 5G will impact the way service providers implement IoT strategies, but IoT security remains an underlying priority.

There are several driving forces that are shaping broad IoT adoption today, as well as more specific factors that are shaping the future of IoT use across every industry. For service providers specifically, these factors will significantly impact the way they implement an IoT strategy and harness IoT value.

Service providers around the world are addressing a more diverse set of business needs from their growing customer base. Their enterprise customers are requiring network connectivity for devices or assets that once before were not equipped to be connected. Vehicle fleets, vending machines, smart meters, pipelines, medical devices: these are just some of the many new assets connecting to today’s networks.

The business challenges presented by connecting billions of new devices will continue to get more complex if service providers fail to implement IoT strategies to meet their customer needs. But the industry is seeing emerging market trends and new technologies that are helping service providers address these challenges.

Service providers have played a critical role in establishing IoT today, and will continue to have a significant impact on IoT’s future — largely due to their unique ability to explore new networks, standards, and technologies that better enable IoT results for their customers.

LPWAN Adoption Will Accelerate

One of the major forces influencing service providers today is the adoption of Low Power Wide Area Networks (LPWANs). LPWAN technologies are developed specifically for IoT environments and have lower power requirements, longer range, and lower costs than traditional mobile networks such as cellular networks.

Beginning in 2017 (and accelerating in 2018 and beyond), more service providers will begin deploying LPWAN technologies to enable much greater efficiency for IoT applications that require long range and low-power capabilities. According to a 2017 Technavio report, the LPWAN market will continue to grow over the next four years and will achieve a compound annual growth rate of more than 50 percent by 2021.

In fact, we are already seeing broader testing of LPWAN technologies including EC-GSM-IoT, LTE-M and Narrow Band (NB-IoT).

It’s important to distinguish that technologies such as NB-IoT and LTE-M are licensed LPWAN technologies that run on the public cellular network. Other technologies such as LoRaWAN and Sigfox, are unlicensed technologies and are often used when public networks are unavailable, or there is a need for a dedicated network, such as on a rural farm.

While it’s true that both unlicensed and licensed LPWAN technologies are being explored in the

Not for distribution or reproduction.

market, licensed LPWAN technologies that support GSM and 3GPP standards will see greater adoption. There already are 900 mobile operators around the world that operate networks supporting those standards, covering the broadest swath of the globe where people live and businesses operate.

NB-IoT specifically is already beginning to take off globally, and industry leaders see the value of this technology as it significantly reduces the power consumption of devices, while increasing system capacity and spectrum efficiency, especially in deep-coverage areas. As a result, battery life of more than 10 years can be supported for a wide range of use cases.

One NB-IoT example comes from Australian-based service provider Optus, which completed core network trials to support NB-IoT earlier this year. Also, Etisalat was one of the first service providers in the United Arab Emirates to successfully conduct trials using NB-IoT, and it has prepared the company for reliable and secure connectivity of IoT solutions at a large scale.

As we round out 2017 and head further into the future, these adoptions will become more commonplace and are even expected to pick up in the United States.

5G: Myth or Reality?

We cannot talk about IoT without addressing 5G: a high-speed wireless standard that might – to some – seem to be an urban myth in the making. Service providers and other industry leaders have grappled with the concept of 5G, and in many cases have still yet to define what it really is.

But 2017 marks a major pivot as the industry will buckle down to determine how 5G can realistically be utilized. Earlier this year, AT&T announced 5G Evolution plans and initiatives to “expand and enhance ultra-fast internet access.” The service provider claims that it has completed initial lab trials achieving speeds up to 14 gigabits-per-second (Gbps) over a wireless connection.

Beyond AT&T, other tech companies like Intel and Qualcomm are jumping on the 5G bandwagon, and like AT&T, have announced early trials, commitments and general interest in getting ahead of 5G as a new wireless standard.

As it evolves, 5G will have major implications on the deployment of IoT — for both high-bandwidth applications like connected car low-power applications like smart meters that require greater efficiency, and everything in between.

IoT Security Remains the Underlying Priority

Regardless of how many IoT devices connect to a network, and regardless of what technologies and standards get implemented for successful IoT solution rollouts, IoT security will need to remain the underlying priority for service providers and enterprises alike.

Aside from the obvious loss of trust from customers, and a tarnished reputation, IoT security breaches are costly, regardless of company size. According to a 2017 report from Altman Vilandrie & Company, nearly half of the firms with annual revenues above $2 billion estimated the potential cost of one IoT breach would be more than $20 million.

Many IoT devices used by companies — even on secure networks — could be vulnerable if those devices are not managed properly. So how can businesses better manage all IoT devices, in an automated way, to monitor for and prevent dangerous activity?

Anyone deploying IoT solutions today needs to deploy a comprehensive IoT security solution capable of providing visibility into applications, users, protocols, and anomalies. And critical systems need to be allowed to continue operating safely, even when under attack. In addition, it is important to simplify compliance with industry or government regulations; scale cost-effectively to accommodate more IoT devices or more data; increase situational awareness and accelerate incident response; and integrate IT and OT processes. By connecting OT systems to the IT network, companies can create more value around existing IT security investments and policies.

Not for distribution or reproduction.

But no company can do IoT security alone. As service providers continue to build more robust IoT strategies, it will be critical for them to build strong ecosystem partners to tackle the security challenges that still remain on the horizon.