Xona Partners

Internet of Things: State of the Union

Xona Partners' Dr Riad Hartani, Frank Rayal and Ananda Sen Gupta provide an ecosystem reference model for Internet of Things (IoT) and a brief overview of some key challenges and evolving trends in the sector

The Internet of Things (IoT) is by definition a vast topic that encompasses multiple markets, technologies, and disciplines. It is impossible to do service to this field in a single paper, which makes our attempt to accurately characterize the market and call out important issues in this short paper particularly ambitious. Nevertheless, we lunge forward with an overview of some of our thoughts and observations while we admittedly leave many areas uncovered.

Connecting devices and 'things' to the Internet is a natural evolutionary step after two decades of focusing on connecting humans to the Internet. However, while the term 'Internet of Things' may go back to 1999, elements of IoT preceded that date. In its earlier form, the focus of IoT was on sensors and tracking devices – an example can be found in fleet tracking technologies using GPS such as Omnitracs. Early applications focused on commercial, industrial and even military sectors, illustrating the difficulty of narrowing down a precise definition of IoT's scope.

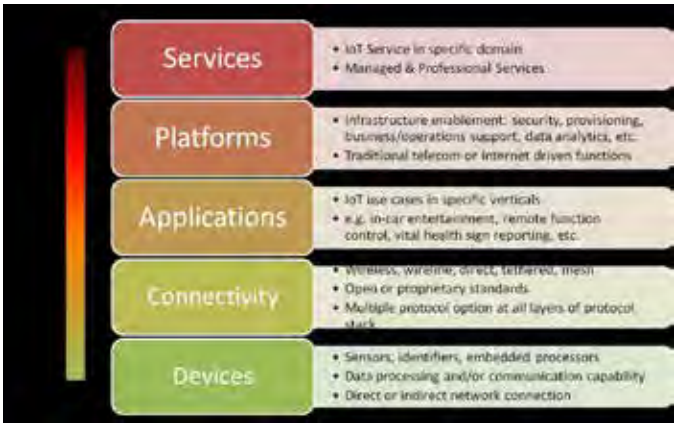
The current term for IoT is in fact, much broader than the original. The recent growth in connected consumer devices, which include wearables and connected home, health and car applications, has skewed the definition of IoT towards the consumer sector. The impetus for this change is due to the proliferation of smartphones and data services that provide connectivity to remotely controlled devices that transfer rich multimedia content. The developments in wide-area connectivity are mirrored by equally important evolution in highly scalable compute platforms for low-cost storage and data processing capabilities, which also plays a fundamental part in propelling data science applications to provide value added services that improve the business case of IoT. This is a critical point, as many IoT applications would fail on a commercial basis without the additional value derived from services that are enabled through the cloud.

Together with the promise of IoT comes a series of obstacles that combined to slow down the rate of adoption of many smart technologies. IoT applications are broad, fragmented and siloed in specific verticals where multiple competing technologies vie for prominence resulting in incompatibility. The topics of security and privacy become complex, and often requiring intervention to frame a regulatory context that provides direction for further development. From this perspective, IoT is an evolutionary process that will exhibit varying adoption rate in each silo while the market works its way through the challenges.

In this paper, we layout an ecosystem reference model for IoT and provide a brief overview of some key challenges and evolving trends that characterize each layer.

The IoT Ecosystem

To conceptually define IoT, we present a five-layer functional model



that includes devices, connectivity, applications, platforms, and services (Figure 1).

Devices: Sensors, identifiers and gateways are types of IoT devices used to collect and convey information. Devices are designed and deployed to meet the application use case requirements. They can range from simple identifiers that provide specific information on the object, to complex devices that have the ability to measure (sensors) and process data (gateways). The application, use case and deployment scenario places requirements on the device such as size, weight, power consumption, life of operation or deployment. This in turn impacts the connectivity of the device to the network. A variety of IoT devices have emerged in various business verticals, starting in the utility / energy sector to include today devices in the health, transportation, home and finance ecosystems among others.

Connectivity: Devices can be connected directly to the network, or indirectly through another similar device (mesh) or a gateway that is provisioned to support multiple devices. Connectivity can be through a number of physical media such as copper, fiber optical cable or over the air through a number of wireless technologies. One of the challenges in IoT is the proliferation of connectivity standards, which is a common symptom of the breadth and fragmentation of IoT application requirements. These standards span the entire logical protocol stack through layers 1 – 7.

Examples of connectivity would include the traditional 2.5/3/4G networks, as well as various local area solutions (Zigbee, Wi-Fi, Bluetooth, others) and low power wide area solutions (e.g. Weightless) among others.

Applications: Applications define the use case of the device and include all the necessary functions required to make use of the device for the intended purpose including the hardware and software architectures. IoT application stores are emerging with applicability to specific industry verticals, with the health wearable devices being a recent example.

Platforms: devices and connectivity requires a platform to provide a service. Platforms are used to provision devices, manage and control them. They are used for billing and fraud detection. Platforms also provide the means to customize functions and data according to the requirements of end users. From this perspective, platforms allow the IoT infrastructure to perform as required.

Services: This references the IoT service to the end-customer. The service provider leverages all the downstream elements in this value chain: platforms, applications, connectivity and devices. The service provider can be the same or different from the platform and application provider. Examples would include automotive automated diagnostic, medical geriatrics and remote power consumption optimization.

The IoT Connectivity Model

To help drive conclusions and observations on IoT development, we intersect the IoT reference model presented above with a model for data flow, which can simply be modeled by three stages: data creation, transmission, and consumption.

Data creation: Data is generated by different types of devices, as described earlier. Data has specific characteristics such as rate, volume, latency, and frequency. For example, video surveillance has high data rate whereas SCADA systems have low bit rate. Taking this example further, we note that in many SCADA applications, the latency has to be very low to accommodate specific requirements of an application such as a fault in an electric transformer that require instantaneous switching of electric current to avoid damages while there is higher tolerance to latency in video applications.

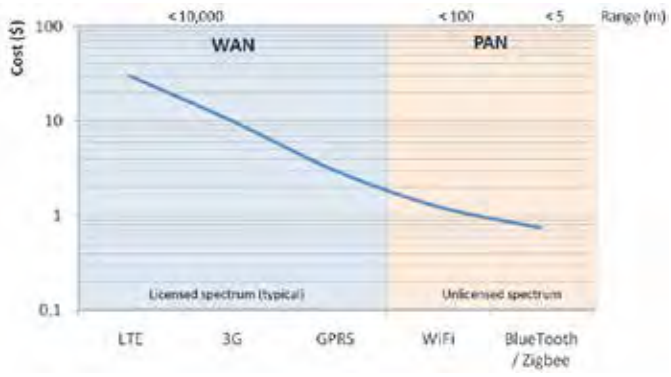
Data transmission: The characteristics data place requirements on transmission in terms of bandwidth, latency, compression, encoding, multiplexing, privacy and security. Thus, different types of pipes are used for transmission as outlined above in connectivity: GPRS, 3G, 4G, LPWA, IP, P2P, DSL, satellite, fiber, etc.

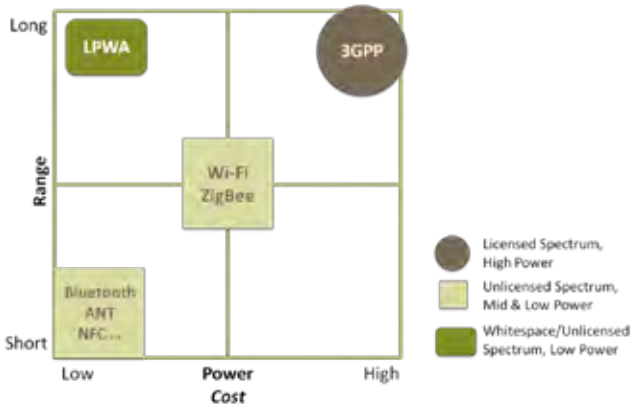
Data consumption: Data is consumed by different segments of end users according to the application. This can be through simple systems that involve the user directly interacting with device, for example, interacting with a wearable through an application on a mobile device or tablet. Alternatively, sophisticated techniques based on data sciences can be used to derive additional information, which can be used to the mutual benefit of the end user and a third party. A homeowner may install a Google Nest thermostat, which she can control remotely; however, the data can also be shared with the utility company to control temperature within certain bounds during peak hours. The intersection between the IoT and data reference models is used to develop a number of observations and conclusions on the state of the IoT market as we outline below.

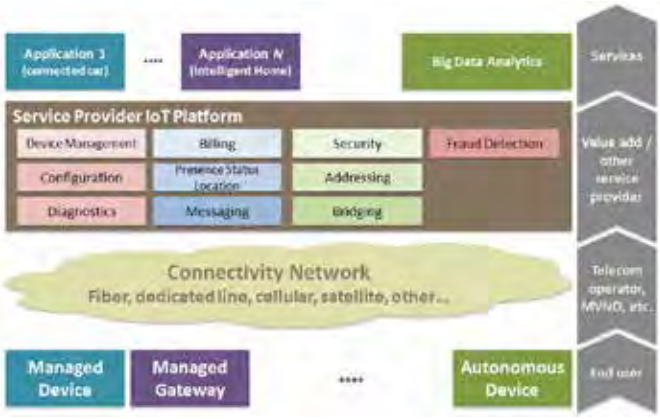
Observations on IoT Market Space

We can deploy the conceptual IoT framework above to model developments across the ecosystem layers starting with devices and connectivity and working upwards towards platforms and services.

	Xiaomi Mi Band	Fitbit Flex	Jawbone Up
Steps taken	✓	✓	✓
Calories burned	✓	✓	✓
Dstance traveled	✓	✓	✓
Active time	✓	✓	✓
Sleep time	✓	✓	✓
Sleep quality	✓	✓	✓
Map routes		✓	
Average pace		✓	
3rd party apps		✓	✓
Diet tracker			✓
Waterproof	✓	✓	✓
Bluetooth	✓	✓	
Social sharing	✓	✓	✓
Alarm	✓	✓	✓
Notifications			✓
Indicator lights	✓	✓	✓
Price	$13	$99	$79







To start, we note that the IoT use case determines requirements for devices and connectivity. Device characteristics such as size, weight, placement, mobility, power and communication characteristics as defined by the application drive the connectivity requirements. The great variety in use cases in each vertical market (for example, automotive, home, health, industry, etc.) has resulted in proliferation of connectivity standards.

1- Proliferation of connectivity standards: Connectivity standards can be divided into different categories depending on fundamental characteristics. In our model, we used the following three categories: Spectrum requirements (for wireless connectivity; devices can be connected through wireline technologies such as PLC);and range, power and cost which are highly correlated. 3GPP standards such as GPRS, UMTS and LTE are licensed band access schemes that rely on high power for long range, consequently are relatively expensive in comparison with other connectivity techniques. On the other hand, technologies such as Bluetooth are meant for short-range communications in unlicensed spectrum and are low on power consumption. Various LPWA proprietary solutions have also recently emerged, mostly in unlicensed sub-1GHz spectrum but also in some licensed bands. Wi-Fi relies on higher power and provides longer range than Bluetooth albeit at a higher cost.

In recent years, advancements in silicon technologies such as 28 and 14 nm processes have significantly reduced power consumption to allow ever-smaller devices with less battery requirements to come to market. Coupled with the maturity of smartphones, this led to a great jump in interest in wearables and personal connected devices.

2- Commoditization of devices: Devices and connectivity continue to march on a downward slope of cost reduction (Figure 2). This is essential to enable the business case for IoT applications. The challenge to device manufacturers is how to differentiate from competition. Our observation in this space is that software applications and platforms, including operating systems, are the essential leverages used by device manufacturers to differentiate (e.g. Apple/iOS, Google/Android; Samsung attempt at differentiating through Tizen, and in a similar way with Alibaba and XiaMi's own platforms design).

3- Commoditization of connectivity: Low-cost connectivity is essential to enable the business case of most applications. There are many variants of connectivity including wireline and wireless technologies.

The lowest cost wireless connectivity leverageslicense-exempt spectrum over short distance (Figure 3). Wearables, for example, leverage Bluetooth to connect with smartphones. Alternatively, some consumer devices rely on longer-range license-exempt technologies such as Wi-Fi for greater range. Central hubs for connectivity and routing are deployed to tether over longer distances for remote control and monitoring. Where mobility is required, wireless technologies in licensed spectrum can be implemented albeit at a higher cost.

4- Emergence of long-range low power wireless technologies: We see an opportunity for very long range wireless technologies that are low power, low cost and work over long range (Figure 4). Such technologies are now on the market but are yet to prove their commercial viability (for example, Neul Weightless, SigFox Ultra Narrow Band, Semtech LoRa, and On-Ramp). These technologies often assume the buildout of a parallel IoT network to the mobile network. The IoT network is operated as a private networkon a subscription model of per device/message basis for low fixed cost pricing.

5- Competition and harmonization of connectivity standards: Connectivity standards have been progressing slowly but steadily. The challenge is not really in the definition of these standards, but more in terms of the number of variety of competing and complementary standards, as well as the conflicting interests of the industrial groups behind the various standards. Although harmonization is ongoing, it is very likely that IoT solutions will face challenges

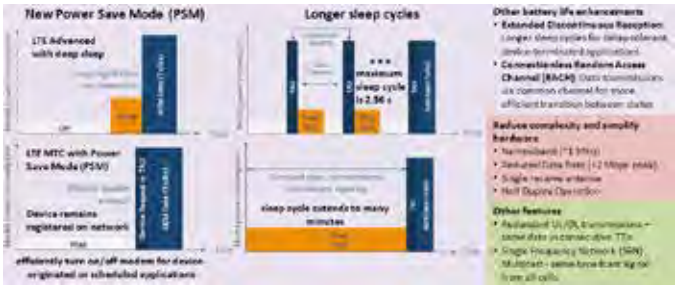
for rapid mass adoption. The development of interworking platforms with open APIs will help alleviate some of these challenges by allowing interoperability of different standards or different implementations of the same standards. This is not only the case for physical and link layer standards, but also includes aspects related to applications and services running on top of the IoT ecosystem.

6- Partnerships and alliances to win the IoT platform war: The development of IoT solutions is inherently about the development of ecosystems around offered solutions. Such ecosystemsarebuilt via tight and lose partnerships between the various industry players. The leading players will aim at controlling the ecosystem by providing a platform that would host IoT applications, and over which IoT services will be built (Figure 5). As in any platform model, such as those in smartphones and the Internet, the key is to increase the adoption of the platform. Various models are being put in place to achieve this, via the development of open source IoT connectivity and interworking software, open APIs to plug into the platforms, and SDKs to develop services on top of the platform. We foresee the emergence of fragmented alliances over the next few years, across industry verticals, with a focus on advancing specific IoT platforms, but progressively evolving towards selecting winners, as it's traditionally the case for Internet-centric business models. Various contenders are already in the game to achieve this, including the Internet platform players (Google, Apple, Amazon, etc), the lead industrial players with a specific vertical focus (e.g. GE for industrial Internet), and to some extent certain mobile operators with a strategy towards Internet-scale OTT deployment.

7- Emergence of new MNO and MVNO service models: A key dynamic of the IoT market that needs to be highlighted is that the majority of 'value' in any IoT application lies not in the simple carriage of data, but in the provision of an overall service. For example, a wide-area wireless enabled home security system represents a significant revenue opportunity for a mobile or virtual mobile operator, including revenues from device sale, installation, and monthly service fees. However, the data traffic revenue that such a solution generates is likely to be relatively small in comparison. In a similar fashion, a connected health solution would include the connectivity network as well as the platform to manage the solution, interfacing with the various stakeholders in the health solution value chain. The story is the same for many other IoT applications: the real opportunity for mobile operators lie in moving up the value stack and away from the simple provision of data carriage services. Basically, to provide IoT service, the ecosystem will be complex, multi-party and heterogeneous in nature. The mobile network operator has to provide the connectivity and IoT management for value added. IoT solution provider (either over-the-top IoT service provider or mobile service provider who offers IoT solutions) has to integrate all the components of the ecosystem for the end-to-end IoT solution.

8- Extracting value through data sciences: As businesses evolve to leverage the huge amounts of data assembled – mining and learning through such data as well as optimizing communication between those producing it and those using it brings significant opportunities around IoT business models. As such, the desired goal is to create a solid foundation architecture that is able to provide these optimal functional capabilities and a platform to overlay data science applications. This would include the various layers in the data value chain – optimized processing through an acceleration of migrations to the cloud, scalable data management leveraging big data models and the use of customized data sciences solutions for business intelligence creation. This is complemented by a fundamental re-architecture of IT models within the businesses integrating IoT models. We are now witnessing the emergence of enhanced (and new in some cases) set of machine learning and data mining algorithms, specifically focused on clustering and predictive modeling in high dimensional spaces based on imprecise, uncertain and incomplete information, efficient statistical data summarization and features extraction algorithms as well as large-scale real-time data stream management. These tools will be at the core of the processing engines being commercialized or running in open source environment, and will aim, when applied to specific industry problems, at optimizing the existing business logic and augment it with new functionalities over time.

9- Evolution to 5G: In terms of timing and mass market adoption of advanced IoT solutions, it is very likely that this will converge and overlap with the specification and rollout of the first 5G networks. It is then natural that 5G specifications will have to take into account IoT requirements, either directly or via the complementary technologies that would form the future mobile ecosystem (including evolutions of Wi-Fi, LPWA, Zigbee, etc). As such, the LTE roadmap will continue to evolve to include new features that represent a precursor to those in 5G. For example, LTE-MTC in Release 13 aims to reduce power consumption of LTE devices for IoT applications and achieve low cost points by eliminating some of the broadband features of LTE (Figure 6). On the core, backend and underlying IT infrastructure, a gradual move towards virtualization, specific functionality enablement in private/hybrid/public cloud environment, and integration of big data analysis frameworks into network data management, will start appearing. All of these aspects will in essence con-



tribute to bringing advanced IoT solutions and IoT centric business models to markets.

IoT – The Road Ahead

The IoT era has had various false starts, as far as mass adoption and progression to mainstream. The recent convergence of various trends including innovation in low power and low cost device technologies, scalable network connectivity as well as mainstream cloud and big data processing models, policies encouraging mass adoption in the transportation sector, have opened a new window for the emergence of IoT based value added services. In this paper, we took a systemic view of the IoT ecosystem which we divide into five layers and leveraged our experience with recent deployments of IoT solutions in select industry verticals, and working jointly with the various players in the IoT value chain, including device and chipset vendors, network connectivity providers, and suppliers of platforms for IoT service delivery to explore some of the most significant trends, both mid and long term, which we highlighted with implications on how the ecosystem will likely evolve and the underlying challenges and competitive positioning models that would emerge in this market. T

Managed securesite service actively monitors websites of government and private sector organizations for hacking and defacementv

With the flare-up of the regional hostilities in the physical world, the war in the virtual world has also escalated. Every day hacktivists are defacing websites to spread their message to the online world.

Not only are the hacktivists defacing websites and posting their messages on the home pages and inside pages, they immediately take screenshots and upload them to social media sites like Twitter, Facebook and Instagram. Once these posts are uploaded – they are immediately forwarded or retweeted to a large number of hashtags and groups.

Whereas in the past, website defacement message was limited in visibility, now its impact can be felt very quickly across the globe. News, Media and Government organizations are especially attractive targets as they have a very large visitor base that will immediately be affected. This phenomenon is bound to grow as the tensions in the region increase.

'Managed', a UAE based company, is a pioneer in website defacement monitoring and mitigation services, and has been providing website defacement monitoring and alerting to high-visibility companies in the region. Mr. Sameer Hussain, CEO of Managed said, "Monitoring the websites of News and Media companies is very challenging as these websites are very dynamic and have thousands of news pages and their content is always changing. Normal website defacement monitoring techniques result in a very large number of false alerts which will greatly reduce the effectiveness of the monitoring system."

Managed has created a very sophisticated algorithm for its website defacement service, coupled with Social Media monitoring, which greatly reduces the false alerts and provides actionable results to its News and Media industry clients on a timely basis – so that damage control can happen very quickly thereby minimizing the impact of the defacement.

Managed has built its Secure-Site platform to monitor and manage today's complex, dynamic and diverse online presence of high-visibility Government or private sector organizations. The SecureSite service monitors many aspects of a website, including content, uptime, performance loading and DNS servers – as well as online threats, to ensure that the right information is being delivered at the right speed with high availability. T