Internet of things (IoT) – Regulatory aspects

Trilok Dabeesing, ICT Authority

28 June 2017

IoT – Regulatory aspects

- IoT - the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.

- With IoT, we can connect billions of devices with sensors, processors and actuators over the Internet
  - It is the phase where the web meets with the physical world

- The computerisation of everything will change our profession, computer will affect the world in a direct and physical manner.

Regulatory components

- This tremendous evolution opens up the doors for great opportunities and also poses challenges that need to be overcome if we want to benefit the most from IoT

- As a regulator, there are a list of issues with this emerging technology that need to tackled
  - Security
  - Privacy
  - Frequency spectrum management
  - Certification

Security concerns with IoTs

- Mirai DDoS attack
  - The potency of Mirai did not come from an unrivalled sophistication, but instead from its simplicity!
  - A large number of Internet-connected security cameras and DVR boxes (instead of infected PCs) all around the world were hijacked to send traffic toward a target which was the Dyn domain name server
- The security paradigm is different in IoT
  - low processing and low memory devices
  - how to embed security capabilities into these type of devices
- Practical issues that need to be fixed
  - Security will need to become much more innovative to be able to successfully tackle these issues.

So why are we in this situation?

- Basically the problem is cost related.
  - A lot of IoT devices are for consumer market and the companies that are making them want to make them quick and cheap and security is not on their priority list.
  - One possibility to address this problem is to sensitise consumers about these security requirements
  - Experts have used the term “tip of the iceberg” to describe the potential threat from IoT
    - Mirai DDOS attack has caused a number of industry professionals and organisations to call for government involvement.
- security breaches can lead to physical harm to people.
  - A security breach in a connected car or a connected pacemaker can result in loss of life.
- Will Mirai lead to sweeping regulations and increased liability for the makers of connected devices?
- However, coming regulations should not stifle innovation
  - the best way forward is to ensure that technologists get involved in policy and as such the ITU is an ideal platform to do so.

Certification

- The purpose of this type approval process is to avoid
  - radio frequency interference,
  - electromagnetic incompatibility issues
  - exposition to radiation levels which are beyond acceptable safety norms.
- No standardised security framework for the different categories of IoTs for certification purposes yet.
- 70% of the IoT devices which caused the Mirai DDoS attack in the US originated from outside the US.
- Certification practices for IoT equipment at the level of individual countries would have a limited positive effect
  - International security standards for IoTs need to be quickly adopted and enforced by all countries.

Privacy perspective

- Your smart phone is, in fact, a multipurpose pocket computer that stays connected at all times and goes with you wherever you go.

- With this device, an astounding amount of personal data is generated.

- Our data is stored locally on our devices, but they are also recoded on third party cloud storage systems where large businesses can learn more about their users.

- Privacy issues and these cloud systems are also prone to security attacks and sensitive data leak into the wrong hands every day.

- And the cloud is about to get much thicker with the IoTs

Privacy perspective

- The ideal solution is to enable IoTs to be able to communicate securely among themselves through exchange of encrypted data.

- Practical issue
  - Many of the IoT devices for the consumer market transmit very little information, very short packets so that our basis crypto algorithm would not fit onto these packets

- So this is another component where different standardized features for different categories of IoTs should eventually become mandatory.

Spectrum management

- Proper spectrum management implies a good understanding of IoT connectivity technologies and the trends in IoT
  - IoT technologies differ based on how they connect to the Internet—whether by fixed, satellite, low-power-wide-area ("LPWA") networks, cellular, or other solutions.
- Example:
  - the kind of connectivity for a connected car or an industrial appliance with lots of data exchange requirements is completely different from the architecture and business model required where you need to ask a street light to be on or off once a day.

Trends in IoT

- Many IoT use-cases involve short-range uses and/or applications that can tolerate signal latency or delay.
  - Technologies such as Wi-Fi and Bluetooth may be particularly appropriate for consumer IoT services, such as health, fitness trackers, wearable or smart home devices.
  - Short range:Bluetooth low energy (Bluetooth smart); IEEE 802.11ah; IEEE 802.15.4; ZigBee; Z-Wave; etc
- The need for a technology such as LPWA is much greater in industrial IoT.
  - In these environments, the huge numbers of connected devices can only be supported if communications are efficient and power costs low. LPWAs can operate at a lower cost, with greater power efficiency.
- Long range (LPWA networks): Sigfox, Weightless, Ingenu, LoRaWAN, etc.

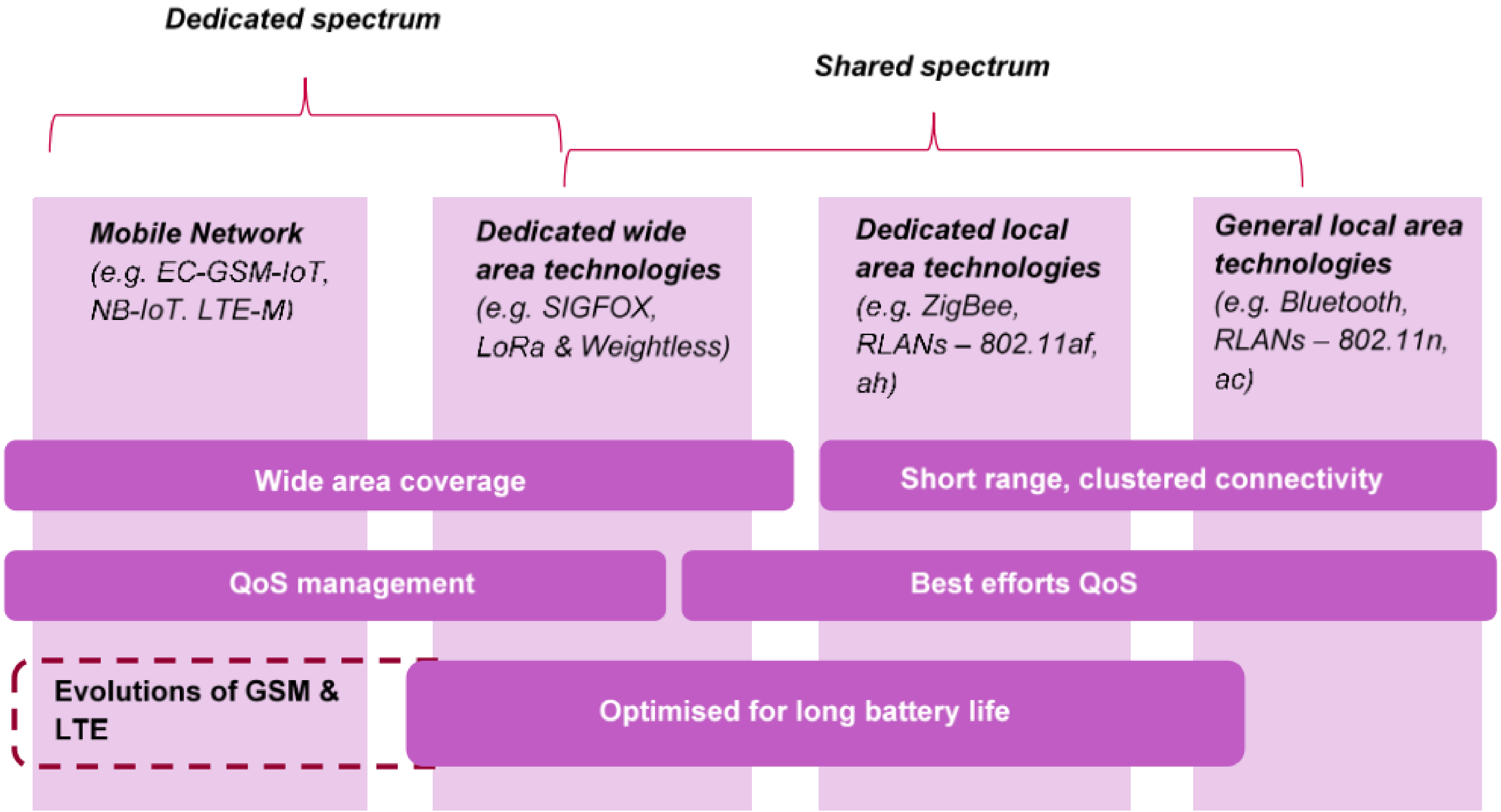
Spectrum requirements

- The bulk of the M2M market (72%) uses short-range, unlicensed connections (e.g. WiFi, Zigbee etc.),
- The wide area market is heavily reliant on cellular connectivity
  - high quality of service guarantees over wide areas, as operators are not at risk of interference and can control usage levels
- There is, therefore, a whole portfolio of different use cases and a whole range of different needs for different type of IoTs.
- In terms of spectrum requirements, provisions will have to be made within both the licence exempt frequency band and also within the licensed frequency band.

Spectrum planning

- Immediate focus
  - accommodate IoT applications within the existing licensing framework and
  - identification of candidate spectrum bands to address expected future demand.
- When it comes to the designation of particular spectrum bands to IoT applications,
  - a mix of licensing arrangements and
  - variety of spectrum bands may be required to support different IoT use cases.
- The spectrum planning approach presently under examination by the ICTA is as follows:
  - Benchmarked with the recommendations of the Radio Policy Group of the European Commission made in Nov 2016 as Mauritius is also in Region 1 of the ITU Band Plan.

Roadmap for IoT Spectrum Access



Dedicated spectrum

Shared spectrum

Mobile Network *(e.g. EC-GSM-IoT, NB-IoT. LTE-M)*

Dedicated wide area technologies *(e.g. SIGFOX, LoRa & Weightless)*

Dedicated local area technologies *(e.g. ZigBee, RLANs – 802.11af, ah)*

General local area technologies *(e.g. Bluetooth, RLANs – 802.11n, ac)*

Wide area coverage

Short range, clustered connectivity

QoS management

Best efforts QoS

Evolutions of GSM & LTE

Optimised for long battery life

Example bands				
700 MHz [1] 800 MHz [1] 900 MHz 1.8 GHz 2.1 GHz	2.5-2.69 GHz [2] 3.4-3.6 GHz [3]	169.4-169.8 MHz 410-430, 450-470 MHz [4] 862-868 MHz 868-870 MHz 870-876 MHz 915-921 MHz	863-868 MHz 868-870 MHz 870-876 MHz 915-921 MHz 2.4 GHz	2.4 GHz [5] 5 GHz [5]

Note 1: There are plans to open the 700 MHz and 800 MHz (Digital Dividend bands)

Note 2: The 2.500 - 2.690 GHz bands is open for IMT-2000 and other compatible technologies for the provision of Broadband Wireless Access (BWA) services.

Note 3: The 3.4 - 3.6 GHz band is open for BWA systems.

Note 4: The band 410 - 430, 450 - 470 falls within frequency band currently allocated to PMR / telemetry system.

Note 5: The 2.4 and 5 GHz frequency band already open and used for Bluetooth / WLAN systems.

Shared band

- Such frequencies are used on a non-interference and un-protected basis. As a result, they are mainly identified for low power devices.
- Such frequencies are already used by IoT, including the following bands: 169 MHz, 433 MHz, 863-870 MHz, 2400 to 2483.5 MHz, 5150-5350 MHz and 5470-5725 MHz.
- Permission is not needed from a regulator, just compliance to worldwide transmission specifications
  - power and ranges are defined by above Directives and Recommendation.
- In turn, the regulator offers no assurance that the band will be free from harmful interference
- The regulator is mostly concerned about non-interference. Its concerns are overcome by certifying the device, not the provider.
- Governed by
  - ECC REC70(03)
  - ICTA Directives 2005 & 2006 on BWA
- The same principle applies for M2M or IoT devices.

Licensed band

- Frequencies whose use is subject to licensing, includes:
  - frequencies allocated or identified for the implementation of public mobile networks (2G, 3G, 4G and 5G);
  - frequencies for the implementation of professional mobile radio networks (called PMR);
  - fixed service frequencies (wireless local loop, microwave);
  - frequencies of satellite services.
- Use of public mobile networks allows high data rates and ubiquitous coverage and roaming, while ensuring a managed level of quality of service, security and resilience.
- The regulatory framework does not act directly on the technology but on the spectrum resources available for the development of IoT, considering the compatibility with existing services
- In some jurisdictions, the redeployment of existing bands assigned to older technology devices are re-farmed and dedicated to new technology, such as IoT.
- Of course the downside of adopting this approach and not harmonizing this use globally is that the spectrum use becomes 'fit for purpose' – it has a narrow use in one jurisdiction.
- International spectrum harmonisation is vital for a global, affordable cellular IoT market

Practical example

- Application for the deployment of a LPWA based IoT network in the shared band will require the following licences and certifications:
  - Commercial licence
  - No spectrum licence
  - Type approval of the devices in use for customs clearance purposes
    - If the technical specifications of the devices are compliant with the requirements of REC 70 03/BWA Directives in terms of power and range, device type approval is granted
    - Otherwise applicant will also be requested to take out a ELAN apparatus licence or any other applicable engineering licence required for customs clearance

5G

- Over 12 billion IoT devices are already connected and 5G will be the real enabler for IoTs with an expected 30 billions devices connected in 2030.

- 5G is expected to be 100 times faster than 4G (150MbpS to 10Gbps) and 1/50 the latency of 4G which means that it will be 50 faster to get that data to the device.

- What does that mean?
  - For example, in self driving cars where every millisecond counts, 4G ideally needs 15 to 25 ms for one car to tell another one behind it that an emergency braking is required. That will actually drop to 1 ms with 5G and this can actually save thousands of lives.

- As the regulator we will need to closely follow up on this evolution so as to be able to plan accordingly.

Medium term plan

- A regulatory framework for licensed spectrum that facilitates the development and growth of IoT, and that does not impose service or technological restrictions that hold back innovation is required

- Medium term actions (amendments to the ICT Act)
  - The Regulator will adopt a service and technology neutral framework by reviewing the current licensing framework

  - provide the regulator with additional modern tools for spectrum management.
    - Provisions for dynamic spectrum management
    - Provisions for use of guard bands/white space under controlled conditions

Manage identification plans

- How do we find or address a device within a particular application or platform, especially if it is within a public network such as the internet?

  - Some will argue the traditional IP addresses (especially once IPv6 is broadly deployed) are a satisfactory start with sufficient governance mechanisms in place.

  - Others will argue that traditional 'telephone numbers', sometimes referred to by industry as E.164 numbers, should work when needed.

Conclusion

- A National Task Force will need to be set up
  - to assess the state of readiness of our ICT legal, regulatory and infrastructural frameworks to facilitate and enable Mauritian businesses and citizens to benefit from IoT innovations
- This assessment exercise will identify priority areas for facilitating IoT developments in the near, medium and longer term, in terms of
  - resource allocation such as spectrum needed for communications infrastructure
  - managing network security and data privacy
  - supporting the interoperability of devices and information
  - supporting Mauritian business and citizens to develop stronger digital technical capabilities to mediate their way through the increasing complexity of digital information.
  - aligning with international best practices

Thank you