Connected Living Programme

Connection Efficiency Guidelines

© GSMA 2014

GSMA IoT DEVICE CONNECTION EFFICIENCY GUIDELINES

The GSMA IoT Device Connection Efficiency Guidelines detail a set of requirements for the whole IoT ecosystem that will aid the mass deployment of efficient IoT services and applications.

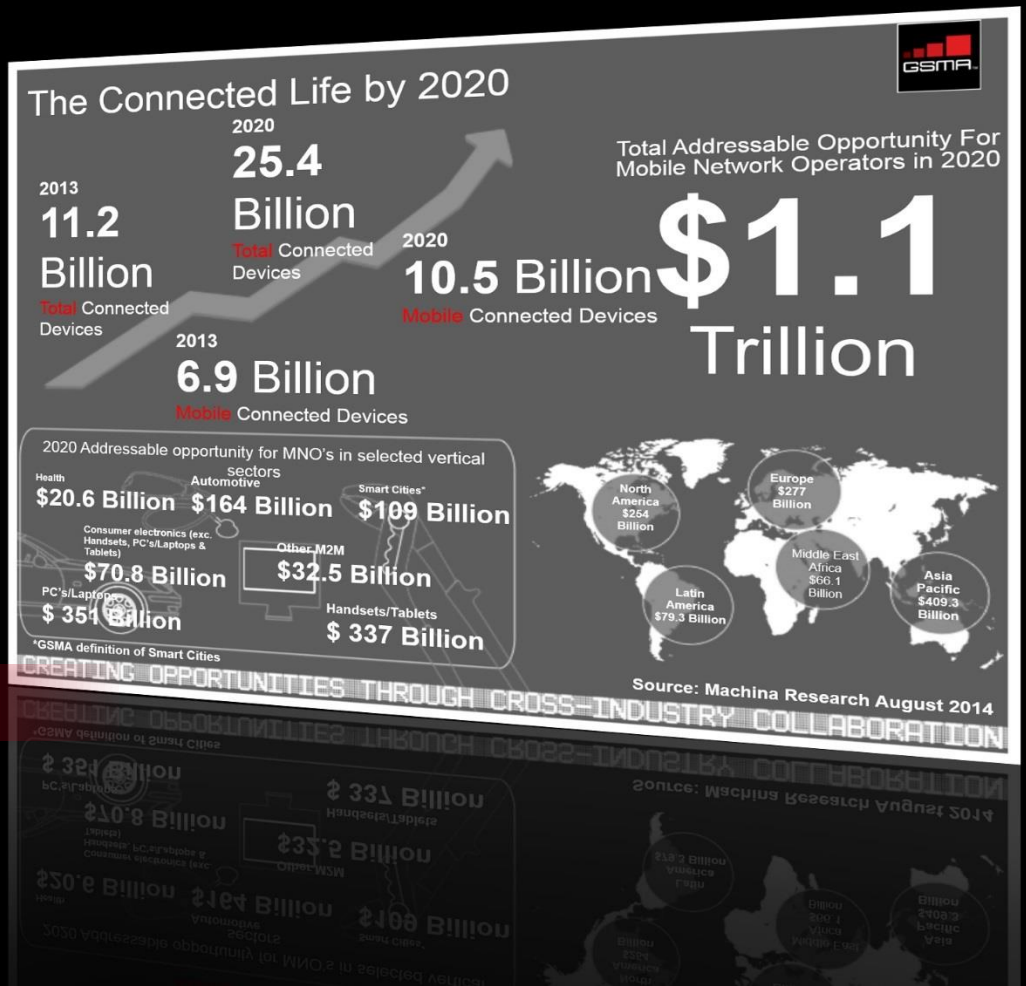
© GSMA 2014

PROBLEM STATEMENT

THE GROWTH OF IOT DEVICES AND APPLICATIONS WILL CREATE MAJOR CHALLENGES FOR THE IOT ECOSYSTEM:

- Local issues e.g. cell congestion.
- Capacity and performance problems within the core network.
- Degradation of the IoT service's performance.
- Increased power consumption of the IoT devices.

HOW CAN THIS BE AVOIDED?



© GSMA 2014

WHAT CAN GO WRONG?

#1 Local area network congestion due to poor application design

- In Mumbai all school buses are connected devices.
- When the buses are geographically distributed around the city the data traffic generated is consequently distributed across the mobile network operator's network.
- However, when the buses return to the bus depot at then end of the day the data traffic becomes concentrated onto a small number of cells within the mobile network causing network overload of these local sites. This congestion then affects all the other mobile network users in this local area.

HOW COULD THIS HAVE BEEN AVOIDED?

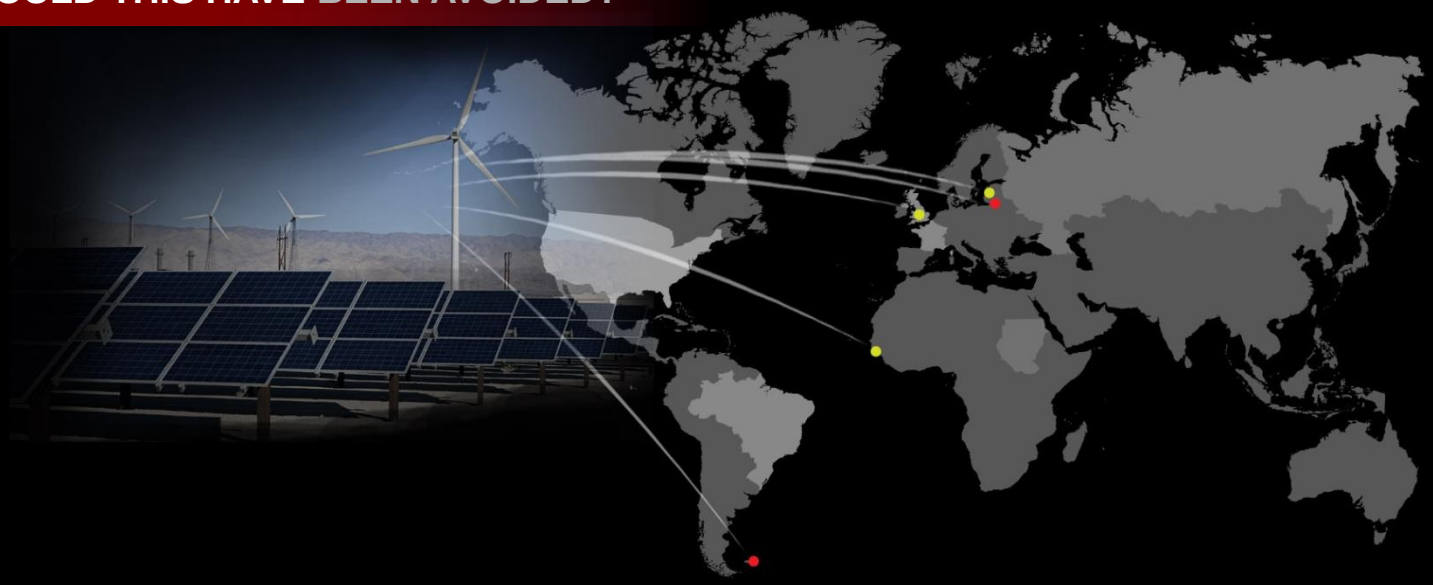
© GSMA 2014

WHAT CAN GO WRONG?

#2 Fraud due to Insecure IoT Communications Modules

- In this case, the operator's B2B customer had an installed base of 59 IoT devices used to monitor wind and solar power generation.
- A hacker had discovered the temporary public IP addresses of the IoT devices and then logged on to each device using the default username and password.
- In December 2013 17,000 fraudulent voice calls were made by the 59 IoT devices to Gambia, Latvia, Lithuania, UK and the Falkland Islands.

HOW COULD THIS HAVE BEEN AVOIDED?



© GSMA 2014

WHAT CAN GO WRONG?

#3 Network Overload due to Unintelligent Error Handing Mechanisms

- An European operator's B2B customer had an installed base of approx. 375,000 geographically fixed IoT devices (for use in the homes of consumers).
- In 2013, the customer's server suddenly and unexpectedly stopped acknowledging the status reports from the IoT devices. This error caused all of the devices to reboot every few seconds to try to re-connect to the mobile network inadvertently creating a 'denial of service' attack.
- Overall, it took this operator approximately 48 hours to completely resolve the problem which classified the event as 'critical' on their network.

HOW COULD THIS HAVE BEEN AVOIDED?

© GSMA 2014

USE OF GUIDELINES WITHIN BROADER ECOSYSTEM

- Should work with their developer partners to implement the requirements contained within the guidelines.
- Should reference the guidelines in the supply contracts they place with their developer partners.

- Should ensure that their communication modules conform to the requirements stated within the guidelines

- Should ensure their IoT services and devices conform to the requirements stated in the guidelines.
- Should reference the guidelines in the supply contracts they place with their IoT device makers

- Should ensure that their IoT device application conforms to the requirements stated within the GSMA connection efficiency guidelines.

- Should promote the use of the guidelines.
- Should make commercially reasonable efforts to reference the guidelines in the connectivity contracts they agree with their IoT Service Providers.

- Should ensure that their radio baseband chipsets conform to the requirements stated within the GSMA connection efficiency guidelines

© GSMA 2014

KEY FEATURES DEFINED WITHIN THE GUIDELINES

Network Friendly Mode

- Network Friendly Mode is a non-standardised feature of the Communications Module that polices the amount of times the Communications Module can perform IMSI attach, GPRS attach, PDP Context activation and SMS-MO in order to reduce the amount of signalling generated towards the HPLMNs HLR, SMSC or GGSN.

Radio Policy Manager

- Radio policy manager is a radio baseband chipset feature that protects the Network by performing “Connection Aggression Management” which is necessary when a device is aggressively trying to access the network following various NAS reject scenarios.

© GSMA 2014

MORE INFORMATION & HOW TO GET INVOLVED..

- **Associated Deliverable**
  An associated document containing a set of ‘common connection efficiency test cases’ will be delivered in early 2015.

- **GSMA contact:**
  Ian Smith

- **Resources:** http://www.gsma.com/connectedliving/gsma-iot-device-connection-efficiency-guidelines/

© GSMA 2014