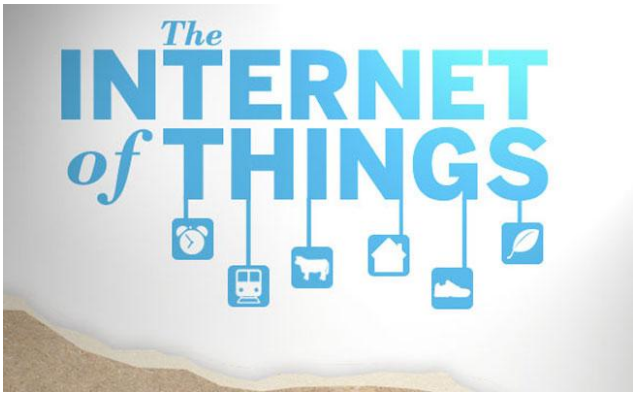
HOUSES OF PARLIAMENT
PARLIAMENTARY OFFICE OF SCIENCE & TECHNOLOGY

POSTNOTE

Number 423 December 2012

# Machine to Machine Communication




Machine to machine (M2M) communication will allow the connection of billions of 'smart' devices and enable new ways of living and working. This note examines the potential of M2M, the common infrastructure that underlies many applications and the technological barriers to implementation.

## Overview

- M2M communication technologies can improve services in industries as diverse as healthcare, transport and manufacturing.
- This will result in exceptional growth in the number of connected devices and the economic returns in the next decade.
- It will also present new challenges in the areas of data security, personal privacy and the future use of the radio spectrum.
- Government and EU initiatives like smart metering and eCall are helping to drive the implementation of this technology in the utilities and automotive sectors.
- However, challenges in the areas of competition and standardisation are hindering implementation.

## Background

The use of machines to remotely monitor systems and environments and to automate processes is not new. Such systems have been in operation since the early part of last century (e.g. weather balloons). The difference between previous systems and what is now called M2M is the ability to connect many more devices and combine previously isolated data sets in new and beneficial ways. These systems are typically designed to operate with minimal direct human interaction.

### Applications

M2M communication has existing and potential applications in the management of a 'smarter' society across multiple industrial sectors including leisure, consumer electronics, transport and logistics (POSTnote 322), retail, manufacturing, construction and agriculture. The automotive, healthcare and utilities (POSTnote 301, 372) sectors are expected to make the most use of M2M initially. Box 1 gives a case study of a current application.

The UK aims to install smart electricity and gas meters in every home and small business by 2019.[1] These meters will communicate readings to the energy supplier and provide the home owner with real-time information about their energy use. Homeowners can use this information to monitor their energy usage and suppliers can use it to better manage energy demands.

In the automotive sector eCall is an EU initiative intended to reduce the response time to road traffic accidents. Sensors in the car are activated in the event of an accident, in a similar fashion to airbags, and automatically transmit a vehicle's location and establish a voice connection with the emergency services. The European Commission has taken legislative action backed by the European Parliament to make the installation of eCall devices mandatory in all new cars by 2015.[2] However, the UK has so far not supported this because of concerns over the cost of implementation.

**Box 1. Case Study - Smart Bins**[3]

Vodafone and the waste management company Mic-O-Data have created 'smart bins'. Using a SIM card, each bin can connect via the telecommunication company's network and send daily status updates advising when they are getting full. This allows refuse collectors to plan their collections accordingly and avoid unnecessary journeys. Six thousand bins have been deployed by 25 local authorities in the Netherlands. An independent study looking at the impact of the bins in one local authority found that Groningen City Council reduced their $CO_2$ emissions by 18% and made a saving of approximately £72,000 per year.

### Growth Predictions

The forthcoming roll out of M2M in the utilities and automotive sectors is expected by some to drive adoption in other sectors. Once suitable networks are implemented and awareness of successful applications has been raised, it is expected that

other industry sectors will build on these networks and implement their own M2M systems.

Growth predictions for the number of devices that will be connected to a communications network in the next decade vary. The most widely quoted figure is from the telecommunications firm Ericsson, which predicts that there will be 50 billion[4] connected devices (M2M and other) globally by 2020. Other forecasts are more conservative, predicting only 24 billion devices by the same date (including 12bn M2M devices).[5] Despite the disparity in predicted connectivity, caused in part by varying definitions of M2M (see Box 2), the number of connected devices of all types will soon greatly outstrip the number of people connected to the internet. This will give rise to what is often referred to as the 'Internet of Things' (IoT).

The economic benefits of M2M can be measured in terms of the direct revenue generated from the development of new business models and industries, and in the savings made by improved efficiency of existing systems. Direct global revenues have been estimated to be between $948 billion and $2.5 trillion by 2020.[5]

## M2M Technologies

There are three primary components of an M2M system.

- The **sensory node** represents the outer edge of an M2M system. It may sense physical conditions in its immediate environment, such as room temperature, or it may monitor a specific process, such as energy usage.
- The **communications network** transmits data collected at the node to an end user. Data can be transmitted over a wired or a wireless network (Box 3). Which of these is used depends primarily on the geographical concentration of the devices (localised or dispersed) and the mobility (mobile or fixed location) of the nodes.[6]

**Box 2. Glossary of Terms**

- **M2M device:** Devices that are able to collect and send (or receive) data automatically to another device, machine or computer system. Technologies such as smart phones which require a large degree of human interaction are not included in this definition.
- **RFID:** Radio Frequency ID tags (POSTnote 225) are one of the enabling technologies for many M2M applications. However, as they do not generally initiate communications they are sometimes excluded from the general definition of M2M.
- **SIM card:** A subscriber identity module (SIM) is a circuit embedded in a removable plastic card. These cards contain identity and security information allowing a user to connect to their provider's network with a unique identity.
- **Protocol:** A set of instructions specifying how information is to be exchanged between devices. Well known protocols relating to the internet include TCP/IP and HTTP.
- **Standard:** A standard, or a set of standards, is not a set of specific instructions but an expected level of service or format for the output. Several different protocols can be used to achieve the same standard. However, if it becomes the norm to use a particular protocol to complete a task or deliver a certain level of service it can become 'the standard'. For example, URLs for identifying resources on the internet.

- The **back-end system** can be a single isolated database or a complex network of servers. This system may process the data sent by the node or simply store it until it is required. This system will also be responsible for sending updates and instructions to the node.

### The Communications Network

The technology for the sensory node and back-end components of M2M systems is well established. However, there are a number of alternatives available for the network component. The following factors will have differing levels of importance when selecting the most appropriate network for a particular application, but the most versatile network technology must address all of these issues.

- **Capacity –** the network must be able support the data transmission requirements of all the nodes. This will vary depending on the number of nodes and their type. A small number of devices providing real-time control will place greater demands on the network than a large number of devices sending data only occasionally.
- **Cost** – the communications module and connection to the network must be cheap enough that it will not increase to an uncompetitive level the cost of the device in which it is embedded.
- **Robustness** – some applications require the deployment of devices in remote locations. Their network connection must be reliable.
- **Energy usage** – where there is no permanent power supply available or opportunity to regularly recharge, the minimum amount of energy should be required for communications in order to extend battery life.
- **Coverage** – the network must provide sufficient coverage and penetration to reach devices regardless of the geographical area they cover or their mobility.
- **Security** – the network must be secure against unauthorised devices and users.
- **Latency** – the delay between data being transmitted and reaching its destination A longer delay is tolerable in the transmission of energy readings than in connecting an automatic emergency call (eCall) which will need to be sent in real time.
- **Bandwidth** – a measure of the amount of data (in bits) the network is capable of sending or receiving per second. Sending a large amount of data over a network with low bandwidth can increase latency.

M2M will make use of wired connections for some applications but in many cases this will be either impractical or prohibitively expensive, in which case a wireless connection must be used. Several wireless network technologies are available (Table 1) although none of them meet all of the above criteria. Bluetooth for example has a relatively high bandwidth but limited coverage and penetration. On the other hand 2G offers excellent coverage, but low bandwidth. This is a hindrance to the implementation of M2M applications in many sectors.

## Challenges to M2M Implementation

The increasing number of M2M devices presents many challenges to privacy and security, protocol standardisation and

**Box 3. Network Types**
Networks can be either wired or wireless and each of these can be either a wide area network (WAN) or a local area network (LAN).

**Wired**
Wired devices are connected directly to a network via a fixed cable. This can connection can be either to a WAN (e.g. DSL, Fibre, etc) connecting devices nationally or internationally or to a LAN (e.g. Ethernet), which typically is itself connected to a WAN. The speed and efficiency of a traditional wired network tends to depend on the type of cable used, copper/coaxial or optical fibre (POSTnote 305), in the immediate and supporting network.

**Wireless**
These networks can be WANs or LANs and make use of radio signals to connect the device to a gateway or router and to allow them to exchange information. This gateway is then in turn usually connected to a wired network. Common examples of wireless LANs (WLANs) are Wi-Fi, ZigBee and Bluetooth. Wireless WANs (WWANs) include the mobile networks (2G, 3G and 4G).While WWANs tend to operate in licensed parts of the radio spectrum, WLANs tend to use licence-exempt spectrum. The coverage, penetration and bandwidth at which WLANs and WWANs transmit data is dependent on the frequencies at which they operate and their power.

| | ***Data rate (max.)*** | ***Range*** | ***Operating frequency*** | ***Battery life*** |
|---|---|---|---|---|
| ***Bluetooth*** | *~1 Mbits/sec* | *5-10m* | *2.4 GHz* | *1-5 days** |
| ***Wi-Fi*** | *~1-600 Mbits/sec* | *50-100m* | *2.4, 5.0 GHz* | *1-2 days* |
| ***ZigBee*** | *~ 0.25 Mbits/sec* | *10-100m* | *868 MHz 2.4 GHz* | *Years* |
| ***2G*** | *0.38 Mbits/sec* | *Long range* | *900, 1800 MHz* | *1-5 days*** |
| ***3G*** | *0.38 - 2 Mbits/sec* | *Long range* | *900, 1800, 2100 MHz* | *1-5 days*** |
| ***4G*** | *50 – 130 Mbits/sec* | *Long range* | *1800 MHz (800 MHz, 2.6 GHz)* | *1-5 days*** |

**Table 1.** Key characteristics of some common wireless network technologies. *Low-power usage versions may have significantly longer battery lifetimes (months-years). ** Where data is sent very rarely battery life can be extended to years.

spectrum usage. Furthermore, in selecting any single network solution the manufacturer or end user may commit themselves to technologies that could become redundant. This is especially important for devices with a long lifecycle such as smart meters or technology for building maintenance.

## Network Lifetimes

The communications modules for 2G networks are relatively cheap compared to 3G and 4G modules and are often used for M2M applications. However, the higher initial cost of a 3G module can be offset by lower ongoing network costs. The longevity of 2G networks is a concern for device manufacturers, especially those manufacturing low value or long lifespan devices, but installing multiple communications technologies in order to 'future proof' devices increases manufacturing costs. How much of a deterrent this uncertainty is for manufacturers or companies in Europe wishing to implement M2M is unknown.

Many operators are now redeploying spectrum currently used for 2G to support their 3G and 4G networks. In America, the operator AT&T has announced it will shut down its 2G network by 2017, while operators in South Korea and Japan have already shut down their 2G networks. In the UK, the communications regulator Ofcom is not aware of any plans regarding the switch off of 2G services. While none of the UK mobile operators have announced plans to turn off their 2G services, parts of the spectrum are being redeployed for 4G.

## Standardisation

The power of M2M relies on connecting billions of devices and merging data within and across industry sectors to provide new services. In order to do this the multiple systems that will make use of these data need to use common protocols for their communications. However, even for well established technologies like 2G there are multiple standards in use. Those wishing to develop M2M technologies can make use of proprietary standards but they will have to pay royalties and may be locked into a single technology or supplier. The use of open standards (POSTnote 414) is an alternative. Although these are normally free, some may use patented technology and still require royalty payments. They may also require the user to invest time and money in customising them.

Several WWAN standards are already competing in the market place but industry influences are being felt, for example the support in Europe for LTE in preference to WiMax for 4G. For WLANs, however, there is no clear preference. The network technology choices made in connection with national projects such as smart meters may have a significant impact.[6] Most M2M experts agree that while standards will be set through industry collaborations and standards development organisations (SDOs) as the M2M industry develops, the current lack of standards is hindering growth.

Several groups including the International Telecommunications Union have highlighted the importance of developing common standards and device interoperability as a critical part of enabling M2M. In January 2012, seven SDOs, including the European Telecommunications Standards Institute (ETSI), agreed to work together to set global standards for M2M. Technologies and standards specifically for M2M are being developed. Examples include Weightless and Wavenis. Weightless, developed by the technology firm Neul, has been launched as an open standard and takes advantage of 'white space' (portions of the radio spectrum between 470-790 MHz that have been allocated for TV broadcasting but which are not always in use). Wavenis is another standard that operates in license-exempt frequency bands.

## Spectrum Usage

The radio spectrum (POSTnote 292) is a valuable and limited resource used for navigation, communications and broadcasting services. Frequencies below ~1000 MHz are particularly useful as they offer good range and can penetrate buildings. In the UK, use of the radio spectrum is managed by

Ofcom, which awards licences for use of specific parts of the spectrum through auctions. Projections for the growth in the number of connected machines and traffic generated have led to concerns over spectrum congestion and a more flexible approach to the use of spectrum will probably be required. This could include the redeployment of spectrum to support multiple or more spectrally efficient technologies (2G, 3G and 4G) and more extensive use of currently licence-exempt spectrum such as white space or the industry, science and medical (ISM) bands.

Ofcom recognises M2M as being likely to be one of the prime uses of radio spectrum and has supported the use of white space for wireless networks. This is beneficial to users who wish to deploy an M2M network but who do not want to make the large investment required to purchase a spectrum licence. However, the use of licence-exempt spectrum does raise issues relating to interference, as several devices operating in the same part of the spectrum but using different communication protocols may interfere with, delay or completely block each other's transmissions.

An alternative to simply licensed or licence-exempt spectrum is 'managed spectrum access' which provides a more efficient way of using the available spectrum while minimising interference between devices. The theory behind shared use of spectrum is to allow several independent users to access the same frequencies provided they agreed to certain conditions; perhaps the use of a common protocol. Shared spectrum access has been the subject of a recent report by SCF Associates for the European commission[7] and a communication from the European Commission to the European Parliament this year. Any future allocation of spectrum for M2M network technologies will be influenced by the protracted lifetimes of some devices and the need to support their communications network over many years.

## Privacy and Security Issues

The volume and detail of data collected using M2M will introduce new risks to security and privacy. For example, data privacy groups and the European Data Protection Supervisor have raised concerns about how detailed energy usage information could be used to gather information about the life-styles of individuals and households. The Department of Energy and Climate Change has said that consumers will be able to choose how their data are used and who has access, apart from where it is required for billing and other essential tasks. However, exact definitions of what constitutes an essential task, and who will require access to the data for these tasks to be completed have not been given.

Transmissions across the network must also be secure against interference and alteration. Data encryption (POSTnote 270) and the use of smarter nodes that are able to partially process the data themselves may improve security but will also impact cost, energy usage and latency. Device authentication, through the use of a username and password may also protect the network. SIM cards are one of the most secure and cost effective methods of authenticating a device on the network and could be used with M2M.[6]

Where M2M is already in use it tends to be in closed systems, within one company or supply chain.[8] In order to drive the creation of new services and applications there must be a back-end system (platform) on which data from a diverse range of sensors can be safely shared. However, many leading data privacy and security experts feel that the UK is not doing enough to promote this way of thinking and address the privacy and security issues in M2M.

Data security and privacy issues pervade many M2M applications. A European Commission report states that for M2M and the IoT to flourish, strong data protection practices must be put in place and cannot be treated as an afterthought. The Design and Technology Alliance Against Crime, which was set up by the Home Office in 2007, aims to reduce crime by making crime prevention a priority during the design process. Although the alliance has looked at 'hot products' such as mobile phones no work has been done on M2M devices as yet.

## SIM card usage

Current policy allows only public network operators to issue SIM cards. The OECD believes that this is suppressing competition and hindering the growth of M2M on the mobile networks. In order to secure the connectivity of their devices for the lifetime of their product, large-scale users such as car manufacturers may have to sign long-term contracts with a single network provider. Smaller national mobile network providers will be unable to compete in this market despite possibly having better regional coverage. The OECD suggests instead that large-scale users should be able to use their own SIM cards and become independent of mobile operators. Ericsson calls this the Private Virtual Network Operator. Large users could then buy access on one or more mobile networks making it possible to change operators without physically changing the SIM card. The OECD argues that this will prevent lock-in, stimulate competition between the mobile network providers, enhance network coverage for the user and reduce the impact of failure on a single network.

Switching between multiple networks would also be facilitated by reprogrammable SIM cards, which unlike current SIM cards could be remotely reprogrammed as the user switched network operators. Standards for reprogrammable SIMs are currently being decided by ETSI and earlier this year Ofcom released a report in which they outlined the drivers for reprogrammable SIM cards in the M2M and other industries.[9]

**Endnotes**

1 DECC (2012), "Smart Metering Implementation Programme"
2 http://europa.eu/rapid/press-release_IP-11-1010_en.htm?locale=en
3 http://www.wireless-mag.com/News/22517/M2M_connected_bins_cut_Dutch_councils%E2%80%99_carbon_footprint.aspx
4 Economist Intelligence Unit (2012), "Rise of the machines"
5 http://www.gsma.com/newsroom/gsma-announces-the-business-impact-of-connected-devices-could-be-worth-us4-5-trillion-in-2020/
6 OECD (2012), "Machine-to-Machine Communication: Connection Billions of Machines"
7 SCF Associates (2012), "Perspectives on the value of shared spectrum access"
8 ICT Knowledge Transfer Network (2011), ""Internet of Things (IoT) and Machine to Machine (M2M) Challenges and Opportunities"
9 CSMG/Ofcom (2012), "Reprogrammable SIMs: Technology, Evolution and Implications"

POST is an office of both Houses of Parliament, charged with providing independent and balanced analysis of policy issues that have a basis in science and technology. POST is grateful to Lisette Sibbons for researching this briefing, to STFC for funding her parliamentary fellowship, and to all contributors and reviewers. For further information on this subject, please contact the co-author, Dr Martin Griffiths. 