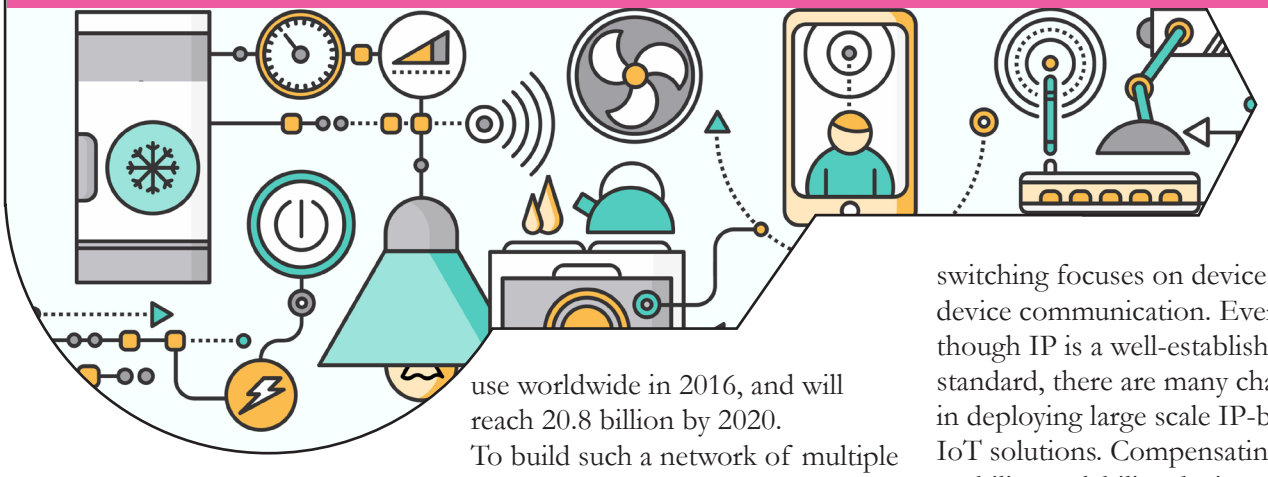
Information Centre Networking for the Internet of Things

Shashini De Silva



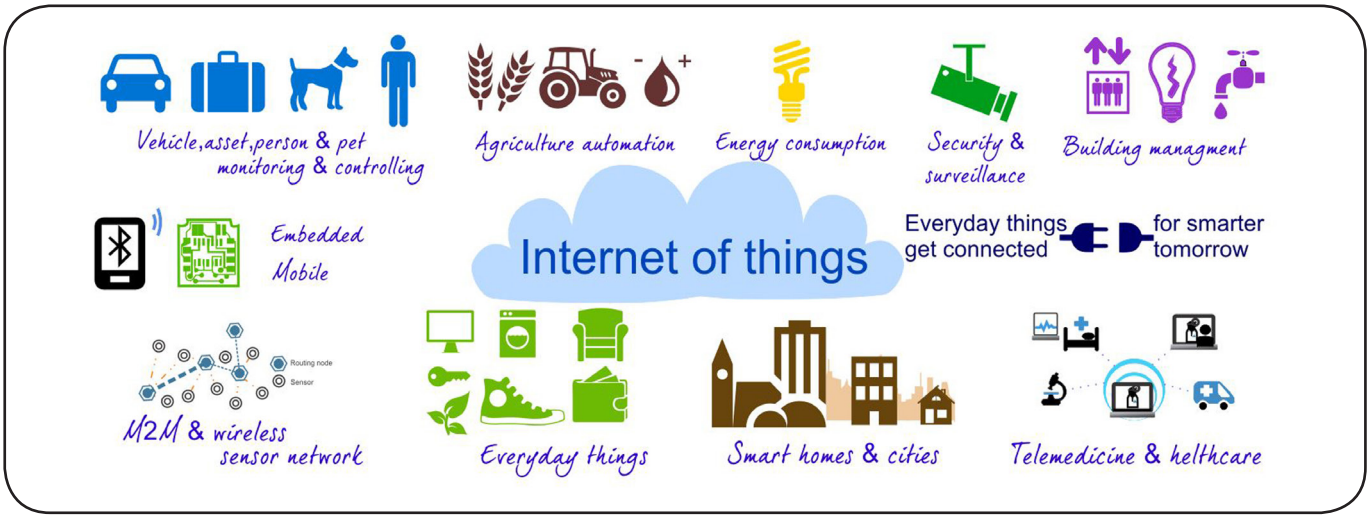
Introduction

Internet of things (IoT) is the network of physical objects embedded with electronics and software which enable them to exchange data. IoT turns these every-day physical objects into smart "things" which sense, understand and react to certain phenomena. Due to low cost sensors/actuators, and the advancement in wireless technologies, the number of "things" connected have rapidly increased over the past few years. According to forecasts of Gartner Inc. the world's leading technology research advisory company, 6.4 billion connected things will be in use worldwide in 2016, and will reach 20.8 billion by 2020.

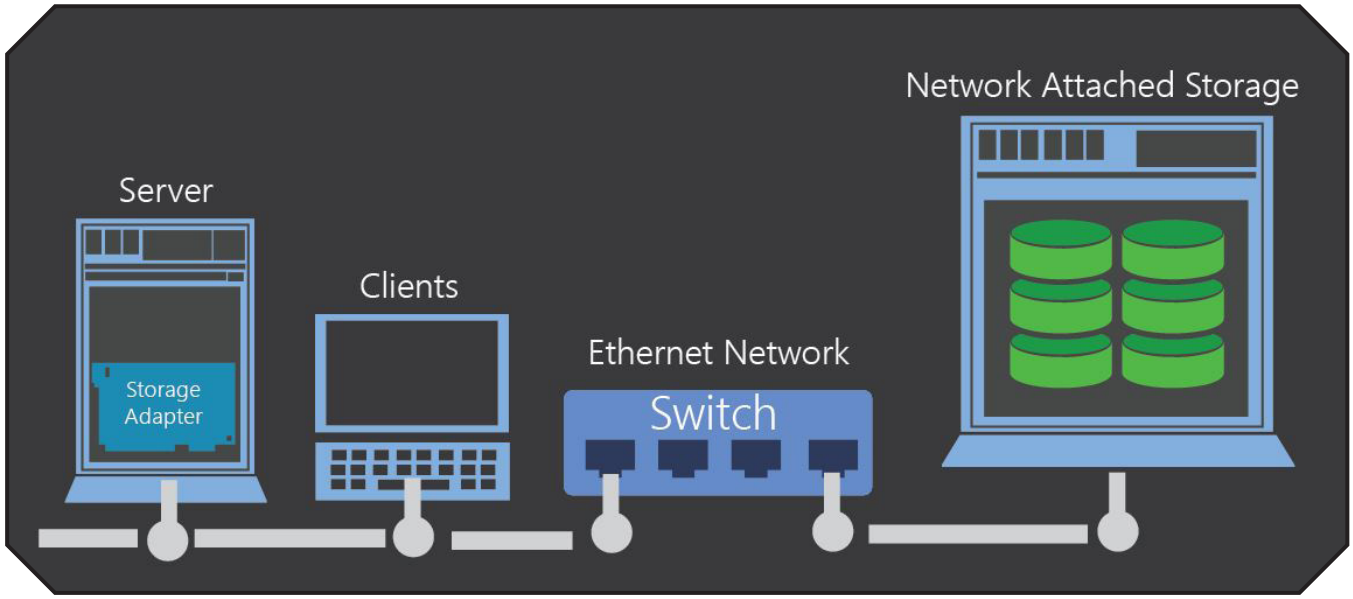
To build such a network of multiple things, many different networking solutions have been proposed. The most common approach is using packet switching networks based on the Internet Protocol (IP). Each device in such networks has a unique numerical label assigned to it called the IP address. Packet switching breaks data into suitably sized blocks, called packets. Each packet is composed of a header containing destination IP address and payload which is the data block required to be transmitted. At the receiver, all the packets are collected in the order they were sent from the transmitter and the payload is bundled together in order to retrieve the original transmitted data. Hence packet switching focuses on device to device communication. Even though IP is a well-established open standard, there are many challenges in deploying large scale IP-based IoT solutions. Compensating mobility, scalability, device to device communication security are a few of them.

The Information Centric Networking Concept

Information Centric Networking (ICN) is the most recently considered networking approach for IoT to overcome such challenges. With IoT, networks are more concerned with connecting people to information such as video, audio & web sites rather than connecting people with other devices. Their requirement is to access specific content, rather than identifying a server where that content resides. In contrast



to packet switching where packets are the basic unit of work, ICN consider content as the basic unit of work. Each piece of content has a unique name which makes content directly addressable and routable. Hence end points communicate using named content instead of IP addresses.
Each content object has a name and a custodian, a known location where content resides. When a content request is first generated by an end point, it is forwarded among content routers towards the custodian. Each router has a separate memory called cache to store pieces of content which pass through the router to their content requesters. Hence before forwarding content requests to their custodian, routers first check whether the requested content is available in its cache. If so, the router itself provides the required content to the content requester. If not, the request will be passed on towards the custodian. When content is transmitted from custodian to requester, it is cached at content routers along the path. Fig. 1 shows a simple 5 node network which uses the ICN approach. Node 'D' and node 'E' are custodians who permanently store content 1 and content 2. Here node 'A' requests for content 2 from custodian node 'E'. This content request is first sent to router 'C'. Since content 2 is not available in 'C' router's cache, it forwards the request to node 'E'. Node 'E' will send required content to node 'A' through router 'C'. On this return path content 2 will be stored in 'C' router's cache. Now if another content request was generated from node 'B' requesting content 2 from custodian node 'E', router 'C' will provide requested content directly without forwarding the request to custodian 'E' because content 2 is already stored in its cache.



Benefits of ICN in the IoT

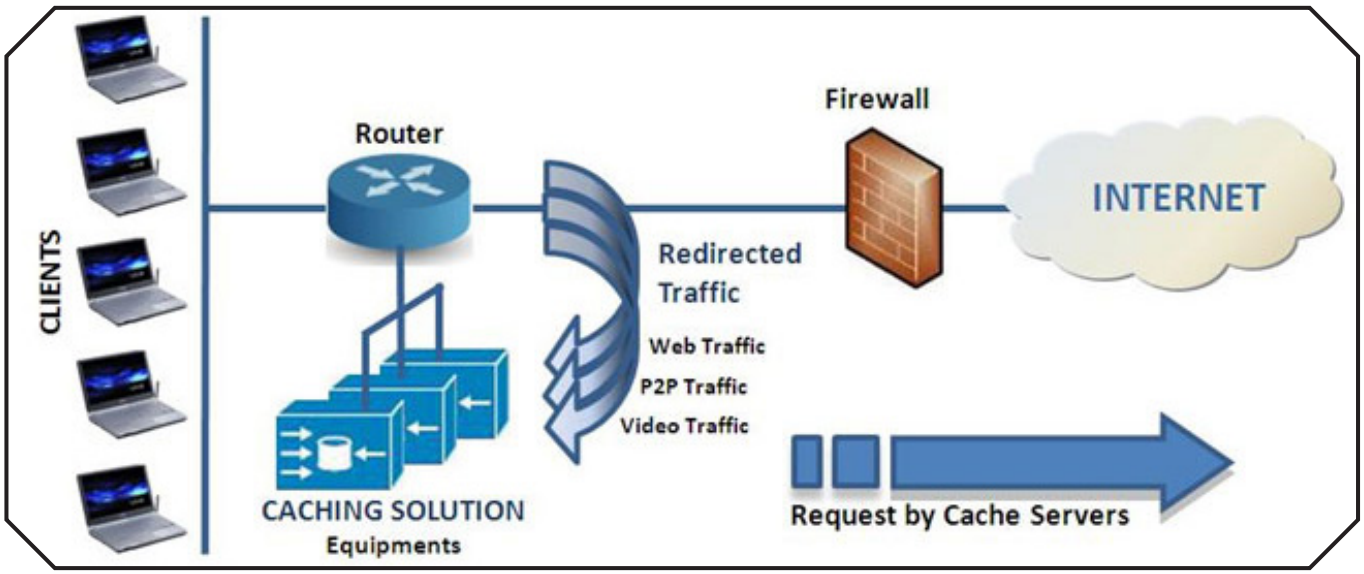
Since the IoT is a dynamic system of interconnected devices with ever increasing intelligence that generates massive amounts of data, it is naturally inclined towards the concept of centralized content. There are many benefits as well as challenges identified by research done on integration of ICN and IoT.
Location independent routing and in-network storing are the two major features in ICN which is advantageous when deployed in the IoT.

Location Independent routing:

Due to ICN's ability to name data independently from the location at which it is stored, routing in network happens based on named content requests rather than location addresses. This is beneficial in IoT since it focuses mainly on distributing content in a heterogeneous network instead of establishing communication links between two devices. This makes it easy to distribute constantly generated streams of data from a group of sensors among a variety of devices.

In-network storing:

ICN routers include cache memory to store traversing content while it is transmitted from its permanent



location to content requester. Such stored content can be used later if the same content is requested again by another device in the network. This prevents unnecessary data transmission in the network which in turn decreases the energy consumed by the devices in the network. On the other hand, in-network storage decrease end to end delay which occurs when retrieving data. Hence using the ICN approach in the IoT saves wireless bandwidth, battery power of devices and decreases transmission delay.
Both of these features together support mobility and scalability in a network. The IoT network may contain many dynamic devices and data objects. Consumers or sensors/actuators might relocate or can be constantly moving (e.g. vehicle traffic monitoring). When ICN is used in IoT, content requests of dynamic "things" can be satisfied without the need to perform registration or configuration. This also simplifies scaling up the network. Adding or removing a node becomes easy with ICN. The distributed nature of content in the network also establishes reliable communication when a few nodes in network are malfunctioning or when channel conditions are poor.

Challenges of Using ICN in the IoT

On the other hand, there are several challenges in using ICN in IoT applications.

Naming:

For proper operation of the ICN network, it is important to have a unique, pertinent name to identify devices in the network as well as content generated by those devices. Identifying each device uniquely is required in an IoT network in order to control and monitor them individually (e.g. switch on/off actuators, administrative operation).These names must relate to location, task/service or other relevant attribute.
For example in the naming scheme for a smart home has defined two different sub classes for namespaces: (i) Configuration and management namespace, identified by prefix/conf. This is used for home network initialization, configuration updates and management operations. (ii) Task namespace, identified by prefix/task, used to identify and enable control and monitoring operations. Here each home is given a 'homeID' which is related to either the location of the house or owner identification number. A configuration and authorization manager is in charge of registering devices to the network by assigning namespaces under which they can operate. A content object with the name bobHouse/task/action/light/on/kitchen is issued to require the kitchen light fixture to turn on in bob's house. When the task is completed, the end device can also send packets with the same name with the payload indicating whether the task is successfully completed or not.

This unique naming might cause unacceptable size of content names. Usually in IoT, sensors and actuators generate/use very short amounts of data (e.g. Boolean value to switch on/off an actuator, integer containing a temperature reading). For this reason, many existing naming schemes assign longer names to the content object than the actual data encapsulated

inside it. In this has been overcome by keeping a dictionary to store long names and map them in to shorter name versions to be used locally in the network.

Caching Management:

As mentioned earlier, distributed caching is a key opportunity with ICN based IoT network. But it must be carefully designed to fit with IoT network application, type of data exchanged and the capabilities of IoT nodes. When the same content is requested frequently by many consumers, the network can benefit from caching.

However distributed caching mechanism is not useful if content is requested only once.
Another issue with caching occurs when data is frequently updating. Caching such data with short time validity might cause distribution of outdated content. For example, temperature of an oven may change rapidly, generating temperature content objects every second. If routers cache temperature content objects, the temperature value contained in the payload might not be the current temperature value of the oven. In using a time-stamp field when naming content object or appending a version tag to the name has been suggested to overcome this challenge.

Depending on the type of service required, even the same sensor can send content objects to different consumers at different rates.
As mentioned in, a temperature sensor in a smart home can send temperature information every 20 seconds to the fire alarm system, every 5 minutes to the heating system and a few times in a day to the house owner. Here it is suggested that it is reasonable to keep a single node in charge of caching data originated by set of devices under its control. This node will supply necessary content on its devices to applications which requests them.

Security:

The information-centric approach is based on the idea of securing information objects rather than securing the communication channel between a pair of nodes. ICN naming strategies guarantee data integrity since given data corresponds to the name with which it was addressed. Apart from this signed data, some sort of authentication is required to make sure that devices in the network are handled only by authenticated users. Especially when content is used to operate devices in the network it is essential that only trusted people do so. This issue has been addressed in the lighting control system in. It sends commands to operate lighting fixtures as content objects protected with a private key. If it is successfully verified, the task can be performed. As in the case with assigning long names to short content messages, here also there is a cost of authentication in terms of computation and delay.

Summary

This article introduced the concept of Information Centric Networking, and its use in the Internet of Things. While the IoT is enabled by a large number of versatile devices, applications deal with information (i.e., content, rather than the devices in the network. As such, ICN is well suited for IoT. ICN has the ability to convey information over the IoT in a bandwidth-efficient manner and with low delay. However, naming of content/devices, in-network caching of dynamic information, and security of the content remain as challenges.

Ms. Shashini De Silva
Lecturer
Department of Electronics and Telecommunication Engineering,
University of Moratuwa
0715647126