Managing Internet of Thing Devices

Luke Blum
East Carolina University
ICTN 6885
Dr. John Pickard

Abstract

The proliferation of network capable devices, collectively known as the Internet of Things, has provided the unprecedented opportunity for owners to manage and control their devices at any time and from any place. These devices are significantly different from the traditional computing devices that most people are accustomed to. Often smaller in size with limited processing resources, unique protocols were needed to allow these devices to operate effectively.

This paper will look into the protocols most commonly used and how they are implemented within end user devices. It will determine if there are a set of common standards that have been developed along with the mechanisms that are utilized for control, reporting, and error detection. Using a methodical process of analyzing vendor white papers as well as industry standardization documents, this paper will outline the most common protocols used, the ease of their use, and how they are applied.

Index

Introduction and Characteristics of Internet of Things Devices

As networking has grown and developed, the number of Internet capable devices has grown exponentially. It began with major devices such as television and home audio systems. It has now spread into just about every realm of the household. Lights can be turned on and off remotely. Sensors can report on produce freshness. This device connectivity has been coined the Internet of Things (IOT). At the basic level they are similar to any other internet connected device being comprised of a network interface, hardware, and information input/output systems. However, when digging deeper there are substantial differences:

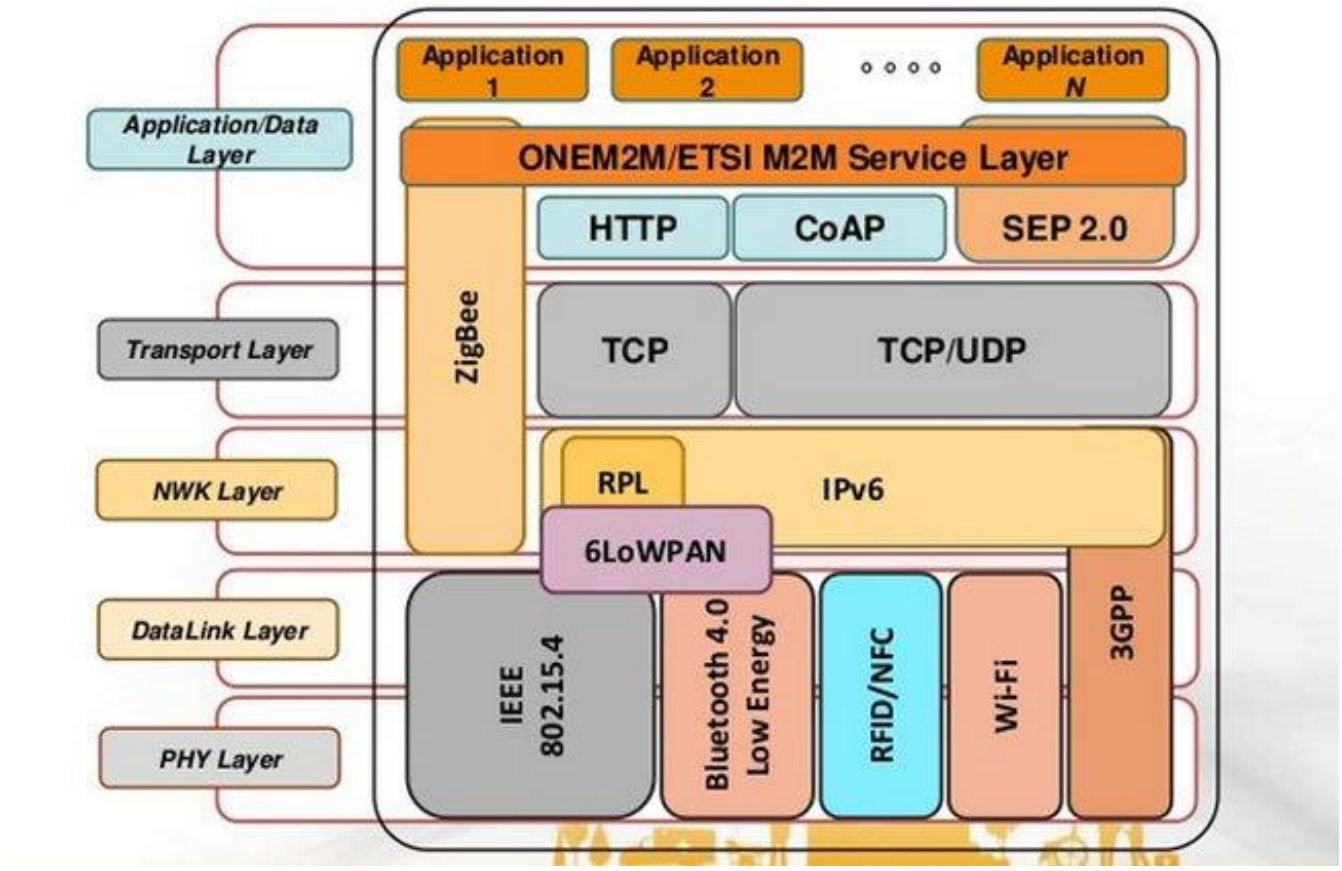
- Hardware - IOT devices often do not look like traditional network hardware devices. They are small in size, frequently no larger than a deck of cards, but often even smaller. They offer only a fraction of the services that larger Internet devices provide. Due to their small size, they are low on processing power an require low energy consumption. This is do to the fact that they do not have direct access to a power source other than internal battery. They have low computing resources and operate of extremely low data rates for this same reason.
- Number of Devices - The expansion of the IOT will dwarf the number of devices that are currently on the market today. In 2012, it was estimated that there were 8.7 billion devices connected to the Internet (Soderbery, 2013). This is roughly one device per person worldwide. Imagine if each person had twenty devices, or even fifty. Methods of device management would change drastically. It is common for mobile sensor networks to comprise hundreds to thousands of devices all reporting status updates to a central hub. These devices must be able to interoperate in a meshed network, reporting information

either to a central management hub or to another device that will process this information.

- Speed and Addressing - The number of IOT devices within a location makes connecting them to wired Internet impractical. This also means that they will not be able to connect to the "fast" connectivity that most people are accustomed to. End node devices often are limited by their low energy and computing resources, having data speeds of 100 Kbps or less. This is where reduced overhead is needed. Most IOT devices are required to use IPv6 addressing. Realizing that IPv4 addresses have been exhausted, developers decided to make these mobile devices IPv6 only. This requirement was beneficial for several reasons. The large IP space made sense considering the many IP capable devices that would be added to the Internet. The IPv6 header is also smaller than the IPv4 version. This helped with the lower data rates that are common with IOT networks. Finally, IPv6 has built-in security mechanisms that make is a clear choice for IOT networks.
- Users - Most of current Internet capable devices are designed for human users. The services supported are the World Wide Web, email, file sharing, and video services. IOT devices are designed for just the opposite. Their primary communication is through machine-to-machine channels, almost completely excluding humans from direct intervention. Sensors report data points to a central management hub that complies data and ensures that it falls within tolerance. If needed the management hub can issues further instructions to the device in question. When users need to be involved for decision making, they currently contribute via personal computers and mobile phones on a front-end application.

IOT Layers

The IOT structure is based on the ISO reference model to simplify its processes and related protocols. Here is a representation that shows these layers and services related to each.



Source: Sensinode

The physical layer is where each device collects all kinds of information through physical equipment and identifies the physical world. The information includes object and environmental properties being collected from equipment such as RFID readers, sensors, and GPS devices. The key component in this layer are sensors for capturing and representing the physical world onto the digital world. The shortage of processing power and storage prevents typical physical layer implementations of frequency hopping communications and public key encryption algorithm to

enable security protection. Still, there are three major requirements for the full integration of these to IPv6 internet: low power communication stack, highly reliable communication stack, and a secure communication stack (Sajjad, 2014). In 2003, the IEEE 802.15 working group defined the IEEE 802.15.4 standard which specifies the physical and media access control layers for personal area networks. This standard focuses on low-cost, low speed communications with little human interaction. The IEEE 802.15.4 MAC address format differs from the traditional IEEE802.3 Ethernet standard. It does not support the 802.1D or 802.1Q formats. It will only support frames up to 127 bytes. In this layer the information may be transmitted by several means. It may take the form of wireless transmission such as blue tooth, cellular (3 or 4G) services, or WiMax.

This data still needs the protection for integrity, authenticity and confidentiality. Node authentication is necessary to prevent unauthorized access and possible compromise of the integrity and confidentiality of information. One possible solution is lightweight encryption technology which includes the lightweight cryptographic algorithm and lightweight cryptographic protocol. To achieve end-to-end security, end nodes have an implementation of a symmetric key algorithm. Low resource-devices would benefit from a lightweight security protocol that limits energy consumption. Security in the physical layer is important due to the fact that they may not be actively managed or may not be located in an area that would be considered a secure location. Sensor devices must be secured physically against tampering and ensuring that a power source is readily available (Katagi, 2014).

Network Layer

The network layer is responsible for the reliable transmission of information from

physical and Data Link layers to the Transport layer. This layer takes information collected from the device and provides initial processing, classification and addressing.

The developers of IP based Smart Object Networks realized that there would be difficulties trying to adapt current routing protocols such as OSPF or EIGRP to networks that are limited by power consumption, small form factor, and communication issues such as low data speeds and high error rates. This led to the Internet Engineering Task Force (IETF) forming a new Working Group to standardize an IPv6-based routing solution for IP smart object networks. This new Working Group called ROLL (Routing Over Low power and Lossy) networks was established in 2008 (Bartolozzi, 2012). This working group developed the specifications for the IPv6 "Ripple" routing protocol for Low-Power and Lossy (RPL) specification. This specification included all details on routing metrics, objective functions and security.

RPL is a Distance Vector IPv6 routing protocol for LLNs that specifies how to build a Destination Oriented Directed Acyclic Graph (DODAG) using an objective function and a set of metrics/constraints. The DODAG is sometimes referred to as a graph (Sohraby, 2007). Like other routing protocols it tries to determine the best path using a defines series of metrics.

The first step in the graph building process begins when a system administrator configures a LowPan Boarder Router (LBR), also known as the root or parent. Three defined messages that are used during the graph building process are:

- DIS (DODAG Information Solicitation)
- DIO (DODAG Information Object)
- DAO (DODAG Destination Advertisement Object)

The root first advertises information about the graph using the DIO message. Any nodes within receiving vicinity of the root will process the DIO message and make decisions based on

applied rules of local policy, path cost, DAG characteristics, and objective function. Once the node has joined, it has a route to the graph root. The node will compute its position within the graph and determine the hierarchy of its position. If configured as a router it will start advertising its information to neighboring peers. If it is a leaf node, it will simply join the graph without sending any further DIO messages. Neighboring devices will repeat this process and do parent selection, route addition and graph information advertisement using DIO messages. This rippling effect builds the graph edges out from the root to the leaf nodes where the process terminates (Vasseur, 2011).

As with traditional routing protocols, routing using RPL within a LNN requires a different strategy that is driven by the type of data traffic. Using data from both links and nodes it gives a measurable data point to make path selections on. Node level metrics include node state attribute and node energy state, while link level metrics can be latency and reliability. LLNs must react different than traditional data networks. The goal of routing protocols are to converge as quickly as possible reducing the amount of downtime of a device or network. LLNs based on this principle may experience instability, oscillations, and additional energy use by sending control packets. LLNs operate on the premise of under-reporting. While loops are a concern, the low data rate lossy links make fast convergence more of a detriment and could lead to network instability or even failure. Loop prevention is not guaranteed but not as much of an issue do to mechanisms such as data path validation.

The logical functions must be secured also. This includes device access, routing protocols, and during transmission. Each of these areas have technologies that have been developed to provide a solution.

RPL supports message confidentiality and integrity. It is designed in such a way that link-layer mechanisms can be used when available and appropriate; yet, in their absence, RPL can use its own mechanisms:

- Unsecured - RPL control messages are sent without any internal security mechanisms
- Preinstalled - nodes joining a RPL instance have preinstalled keys that enable them to process and generate secured RPL messages.
- Authenticated - nodes have preinstalled keys as in preinstalled mode, but the preinstalled key may only be used to join a RPL instance as a leaf. Joining an authenticated RPL Instance as a router requires obtaining a key from an authentication authority (Winter, 2012).

One of the biggest constraints that WSN devices experience are the available power source. Often these devices are not able to tie into commercial power and must rely on batteries. There are several methods that these devices use to conserve energy and prevent loss of services. The first is through the use of trickle timers. RPL messages are based on a timer system. Message intervals increase as the network stabilizes, stretching out the time between messages as time passes. When a router transmits a DIO message, the neighboring router takes note of the information that is contained in the message. If the information contained within the message is consistent with its own state, the router will increment a redundancy counter, increasing the time between the current message and when the next message must be sent. If the information received is different the timer will reset, starting the incremental counter again and increasing the message frequency. The second method of battery conservation relates to the path selection process. Nodes will base their parent selection on the energy levels of their neighbors. When setup messages are sent, two pieces of information are used: the type of the node which indicates

how it is supplied with power and the energy estimation. The formula used for energy estimation is EE=Powernow/Powermax · 100. The RPL metric defines three possible states for the power information field: powered, on batteries and scavenger. If a network device is powered it means that it may be a root or data collector. These nodes will report a maximum power level to other devices. If on batteries, a node must compute its energy estimation. This information will be used by the other devices to determine if the reporting device is a good primary pathway to the parent (Tsvetkov, 2011).

Top three layers

The network, transport, and application layers have also been designed to run protocols that are specific to the IOT devices. One of the emerging protocols is called Zigbee. Zigbee is based on the IEEE 802.15.4 standard. Conceived in 1998 and standardized in 2003, its devices are used to create personal area networks using small, low-power digital radios. Due to its low-power output communication ranges are typically limited to 10-100 meters line-of-sight. This limitation can be overcome through the use of a mesh network. Mesh networks can be formed as point-to-point, point-to-multipoint, or multipoint-to-point networks. These meshed networks pass the Zigbee protocols defined data rate of 250 Kbit (http://www.digi.com/technology/rf-articles/wireless-zigbee) which is best suited for intermittent data transmissions from a sensor or input device. A key feature of the Zigbee protocol is the support of up to 65,000 devices.

Security within the top layers is especially important considering this is where user interaction occurs. The developers of the Zigbee protocol took this into consideration when development took place. The ZigBee network model must take particular care of security considerations, as ad hoc networks may be physically accessible to external devices and the particular working environmentt may not be determined ahead of time. Also, Zigbee may run

different applications concurrently using the same transceiver to communicate. Zigbee uses AES 128 bit encryption to accomplish this. It is assumed that they are mutually trustworthy and for cost reasons the model does not assume that a firewall exists between application-level entities. As an additional measure, group policies can also be put into place to ensure separation of different domains. For this reason, the network must be designed with security in mind.

Conclusion

Consumer products will continue to be produces with Internet connectivity integrated into its functionality. Devices will become intertwined, reporting their current status to a centrally management system for control purposes. As new technologies are developed, standards that will allow them to work correctly in their given environments must also be created. These developments will create a rich and positive experience for end users as they gain more control over the devices that they own.

Sources

Bartolozzi, L. Pecorella, T., & Fantacci, R. (2012). RPL Module: IPv6 Routing Protocol for Low-Power and Lossy Networks. Retrieved March 15, 2015 from https://www.nsnam.org/wpcontent/uploads/2011/10/rpl.slides.pdf

Katagi, M. & Moriai, Shiho. (2014). Lightweight Cryptography for the Internet of Things. Retrieved April 5, 2015 from https://www.iab.org/wp-content/IAB uploads/2011/03/Kaftan.pdf

Sajjad, S.M.; Yousaf, M., "Security analysis of IEEE 802.15.4 MAC in the context of Internet of Things (IoT)," *Information Assurance and Cyber Security (CIACS), 2014 Conference on* , vol., no., pp.9,14, 12-13 June 2014 doi: 10.1109/CIACS.2014.6861324

Soderbery, R. (2013). How Many Things Are Currently Connected To The "Internet of Things" (IoT)?. Retrieved April 5, 2015 from http://www.forbes.com/sites/quora /2013/01/07/how-many-things-are-currently connected-to-the-internet-of-things-iot/

Sohraby, K., & Minoli, D. (2007). *Wireless sensor networks: Technology, protocols, and applications*. Hoboken, N.J.: Wiley-Interscience.

Tsvetkov, T. (2011). RPL: IPv6 routing Protocol for Low Power and Lossy Networks. Retrieved April 5, 2015 from http://www.net.in.tum.de/fileadmin/TUM/NET/NET-2011-07 1/NET-2011-07-1_09.pdf

Vasseur, J., Agarwal, N., Hui, j., Shelby, Z., Bertrand, P., & Chauvenet, C. (2011). RPL: The IP routing protocol designed for low power and lossy networks. Retrieved April 5,2015 from http://www.ipso-alliance.org/wp-content/media/rpl.pdf

Winter, E. T., Thubert, E. P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., . . . (2012). RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550. Retrieved April 5, 2015 from https://tools.ietf.org/html/rfc6550#page

Yang, G., Xu, J., Chen, Z., Qi, H., & Wang, H. "Security characteristic and technology in the internet of things," Journal of Nanjing University of Posts and Telecommunications (Natural Science), vol. 30, no. 4, Aug 2010.