System Architecture Challenges in the Home M2M Network

Michael Starsinic, Member IEEE
InterDigital Communications, LLC
King of Prussia, PA

Abstract—**Wireless home networks are extending beyond phones and computers to include every imaginable type of electronic device from TVs and audio components, to appliances and thermostats. The benefits include distribution of multimedia throughout the home, energy savings through remote or automatic control, and reduced cost through packaged services. Though people are often enamored by the technology that provides very broadband wireless streaming for multimedia, an important new class of low data rate machine-to-machine (M2M) devices are key to this highly connected home. The M2M device class is typically characterized by very low power consumption and little or no human intervention. In many cases, they autonomously communicate with each other or with a central controller. The home of the future will be outfitted with many such devices. Applications, such as home security sensing, lighting control, HVAC systems, appliances that run smart grid applications, medical devices, and entertainment systems, will all need to connect and communicate from within the home.**

There are many challenges in the design of the home M2M network. Varying security, power, and data rate requirements for M2M devices necessitate that they use different network protocols to communicate. The 802.15.4 (ZigBee/6LoWPAN) protocol is well suited for low power / low data rate applications such as HVAC control and appliances. The 802.11 (Wi-Fi) protocol works well for higher data rate applications such as audio and video streaming. Cellular is the best fit for applications that need to roam into and out of the home network. The Bluetooth protocol is well suited for low data rate communications such as audio connections and file transfer.

The home network will require an M2M gateway to facilitate communication among the various devices and to provide a connection to a backhaul that reaches the Internet. The gateway can have many different embodiments; it needs to support one or more of the local network protocols as well as the back haul connection to the Internet. The backhaul connection may be Ethernet, cable, DSL, fiber, or cellular. As M2M gateways become more commonplace, they may be integrated into miniature cellular base stations, or femtocells. Femtocells will allow multiple devices (cellular and non-cellular) to access the Internet through an IP-based backhaul.

This paper explores some of the many systems architecture challenges that are associated with the evolving home M2M network. In particular, the focus is on the design of the home M2M gateway and the challenges that arise when building a home network that utilizes multiple network protocols. Several questions need to be addressed. First, what protocols should be supported by the M2M gateway and how can the gateway best handle communication between nodes that use different protocols? Second, what data aggregation and dissemination techniques can the gateway use to assist low power / low duty cycle service requirements? Finally, can technologies, such as software defined radio (SDR), be used to build gateways that allow the user or operator to select what network protocols and air interfaces are supported?

Keywords-M2M, Data Aggregation, Home Networks

I. Introduction

Wireless home networks are extending beyond phones and computers to include every imaginable type of electronic device from TVs and audio components to appliances and thermostats. The benefits include distribution of multimedia throughout the home, energy savings through remote or automatic control, and reduced cost through packaged services. Though people are often enamored by the technology that provides very broadband wireless capability for streaming of multimedia, an important new class of low data rate machine-to-machine (M2M) devices are key to this highly connected home. The M2M device class is typically characterized by very low power consumption and little or no human intervention. In many cases, they autonomously communicate with each other or with a central controller. The home of the future will be outfitted with many such devices. Applications such as home security sensing, lighting control, HVAC systems, appliances that run smart grid applications, medical devices, and entertainment systems will all need to connect and communicate from within the home.

It will be necessary for a home network that supports such varying applications to support multiple local network protocols. Fig. 1 illustrates a home M2M network that can be built with products that are commercially available today. In Fig. 1, three local networks (802.15.4 (ZigBee), 802.11 (Wi-Fi), Bluetooth) tie into a common backhaul. The ability to control home security, HVAC, lighting, appliances, and entertainment systems remotely or from within the home is certainly attractive to the homeowner. However, this architecture requires that a homeowner be capable and willing to manage several local networks, each with its own gateway and each gateway requiring different applications. This paper will explore some of the protocols that created this disjointed architecture and what protocol enhancements are being proposed that will make the home network more user friendly. Particular focus is paid to the power requirements of M2M devices, as well as the complications that arise when

communicating between local networks and across the Internet.

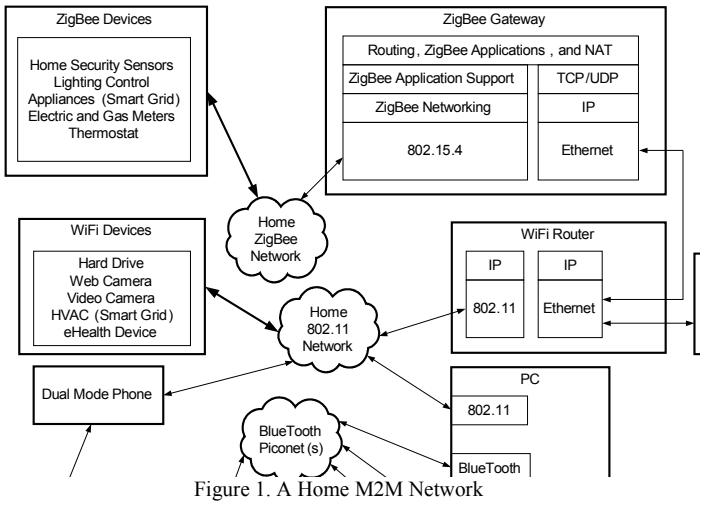

Figure 1. A Home M2M Network

The gateway and router in Fig. 1 are required to perform much more than just the basic routing of packets from a source to a destination. They must also support Network Address Translation (NAT) applications in order to facilitate communication between local networks. NAT applications can introduce a number of issues. NAT complicates peer-to-peer communications, applications that explicitly use IP addresses, and applications that require specialized QoS [1] [2]. These issues are certain to become more pronounced in a home network that may need to support on the order of 100 devices, many of which use different addressing protocols.

The low power requirements of M2M devices result in additional expectations for the gateway. In order to conserve power and increase device lifetimes, M2M devices are equipped with minimal resources. Gateways must understand what processing and energy resources are available in the M2M devices, and disseminate data in ways that minimize the use of these resources. Whenever possible, processing should be performed in the gateway instead of the network devices. The gateway must also be aware of when devices are sleeping and when they are available to communicate. Queries, commands, and responses need to be processed in ways that allow the low power devices to have efficient sleep cycles.

When we consider Fig. 1 and the features that must be supported by each gateway, we see that the home M2M network lacks scalability and is difficult to manage. The addition of new devices could require more power management and NAT applications on the gateways, and may even require additional gateways. To achieve the most network value, all devices in the home must be able to communicate with each other. For example, in Fig. 1, there are smart grid applications running on both the Wi-Fi network and the ZigBee network. It could certainly be advantageous to have these devices share information; however, this is not possible without specialized NAT applications.

This paper is partitioned as follows. Section 2 is an overview of some of the M2M network protocols that are commonly used today, and protocol enhancements that are gaining traction for future implementation. In particular, section 2 focuses on the impact of addressing protocols on communications that span local networks. Section 3 is a discussion of the unique power requirements that are found in many M2M devices, and how they influence the communication protocols. Section 4 describes the converged M2M gateway; a single product that uses advanced protocols to control all of the home network devices. Section 4 also includes a discussion of where the architecture of the home network is heading beyond convergence, and what role cellular communications and software defined radio (SDR) will play in the home network. Section 5 concludes the paper.

II. M2M Home Netwrok Protocols

The M2M devices that are found in home networks span a wide range of applications and, therefore, use a wide range of network protocols to communicate. IEEE 802.15.4-based protocols, such as ZigBee and 6LoWPAN, are well suited for low power / low data rate applications where numerous sensors are spread out over a large area. The IEEE 802.11 (Wi-Fi) protocol works well for higher data rate applications such as audio and video streaming. The Bluetooth protocol is well suited for short range / low data rate peer-to-peer communications such as file transfer and audio. Table 1 summarizes some of the M2M protocols and their important properties.

TABLE I. M2M Radio Access Technologies

	802.15.4 (ZigBee / 6LoWPAN)	**Bluetooth Low Energy**	**Bluetooth**	**802.11 (Wi-Fi)**
Max Data Rate	250 kb/s	1 Mb/s	3 Mb/s (Enhanced) 1 Mb/s (Basic)	22 Mb/s (802.11g) 144 Mb/s (802.11n)
Indoor Range	10 m – 20 m (Extended via multi-hop routing)	5 to 15m	1 m, 10 m and 100 m classes	45 m (802.11g) 70 m (802.11n)
Power	Low	Low	Medium	High
Battery Life	Years	Years	Days	Hours
Frequency Band	2. 4 GHz, 868 MHz, and 915MHz	2.4 GHz	2. 4 GHz	2. 4 GHz, 3.6 GHz, and 5 GHz
Applications	Smart Appliances Smart Meters Lighting Control Home Security	Health / Sports Monitors Watches Keyboard	Voice Data Transfers Keyboard Game Control	Networking Digital Audio Voice Digital Video

IEEE 802.15.4 is perhaps the most accepted protocol in the low power M2M space and serves as the primary building block for numerous other standardized and proprietary protocols. 802.15.4 defines a physical and MAC layer for low duty cycle, low throughput, and low power wireless devices. The protocol is simple enough to implement with an 8-bit microprocessor, a low cost transceiver, and less than 4 Kbytes of SRAM. 802.15.4 does not specify network topology, routing schemes, or network growth and repair mechanisms [3]. It simply defines peer-to-peer communication protocols and provides the tools necessary for creating efficient protocols based on the application. The 802.15.4 standard is flexible enough to be used in many different network topologies. It has become the defacto standard physical and MAC layer for M2M applications.

ZigBee is a protocol that is used in many home networking solutions. The protocol is developed and maintained by a consortium of over 300 companies called the ZigBee Alliance. ZigBee runs on top of 802.15.4; it defines the network layer, transport layer, and a set of application layer interfaces. Fig. 2 shows a diagram of where the ZigBee protocol sits in the OSI stack. ZigBee was developed specifically for low power, long lifetime, wireless devices. Battery life in the range of months to years is achieved through the use of long duty cycles and multihop routing. Multihop routing allows each packet to travel over relatively large distances, while each individual device only needs to transmit over short distances. The ZigBee network layer takes advantage of the flexibility that is provided by the 802.15.4 standard and allows for a star, cluster tree, or self-healing mesh network topologies.

ZigBee's current addressing approach introduces some complications when communicating over the Internet. ZigBee addressing uses the 802.15.4 addressing scheme, where all devices are assigned a 64 bit address that gets remapped to a 16 bit address when a device joins the network. If an application running on a PC needs to access a ZigBee node somewhere on the home network, then a NAT application will be required on the ZigBee gateway.

The ZigBee Alliance's "Core Stack" working group is working on a new generation of the ZigBee protocol that is intended for home networking applications such as smart metering, demand response, and energy control. This new 802.15.4 based protocol stack will use IPv6 addressing. The working group is also addressing topics such as transport, routing, security, and service location protocols. This effort is leveraging standards from the Internet Engineering Task Force (IETF), IEEE, and other standards organizations [4].

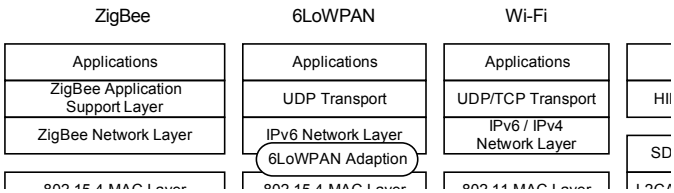

Figure 2. M2M Protocol Stacks

The IETF is an open community who develops documentation that provides guidance and recommendations for how devices should use the Internet [5]. Several IETF documents provide guidance for how low power resource nodes should use IPv6 addressing. Two fundamental problems with sending IPv6 packets over an 802.15.4 link are that IPv6 headers are large relative to 802.15.4 packet sizes, and that IPv6 packets can be much larger than the 127 byte maximum size that is allowed in 820.15.4 [6][7]. The IETF 6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks) working group has defined an adaption layer that sits between the 802.15.4 data link layer and an IP stack; this is shown in Fig. 2. The adaption layer defines how to compress IPv6 headers and how to segment IPv6 datagrams so that they can be sent over 802.15.4 links [7]. A protocol stack that uses the 6LoWPAN adaption layer can perform routing at the IP layer as is done in a standard IP network. The adaption layer will effectively hide the details of the 802.15.4 link.

Although application protocols, e.g., HTTP and SNMP and IP routing algorithms, e.g., OSPF and IS-IS that are common today could run on top of the 6LoWPAN adaption layer, they would be inefficient for the low resource / low power nodes that are used in M2M networks. The IETF ROLL (Routing Over Low Power and Lossy Networks) working group is developing routing protocols that are efficient in low resource nodes, and the IETF is initiating a 6LoWAPP (Low Power Embedded Application Profiles) group whose mission is to develop application level protocols that can run efficiently over low resource networks.

The Bluetooth is popular for short-range voice, data, and audio wireless connections. The Bluetooth Special Interest Group (SIG) is an alliance of companies that develops and maintains the Bluetooth protocol. As shown in Fig. 2 and in Table 1, the Bluetooth protocol stack already supports IP addressing. However, it is not as well suited as the 802.15.4-based protocols for low power sensing applications. Bluetooth is better suited for applications that require only a few communicating devices, slightly higher data rates, and have more liberal power requirements. Bluetooth networks, called piconets, only support up to 8 devices communicating at a time. The protocol provides methods for additional devices to share connections into the piconet and for piconets to communicate. However, Bluetooth's scalability does not compare to the self-healing network growth protocols that are used in many 802.15.4 networks. Additionally, Bluetooth devices need to periodically wake up and synchronize with the master device of the piconet. A Bluetooth device can take about 3 seconds to wake up before it synchronizes, while an

802.15.4 device may take only milliseconds to exit its sleep state. An 802.15.4 device that use the CSMA/CA protocol would not need to schedule special wake up events in order to communicate and maintain synchronization.

The Bluetooth (SIG) is working on protocol enhancements to support lower power applications. The SIG is developing a yet to be released Bluetooth Low Energy standard whose power requirements are more competitive with the 802.15.4 based standards. Bluetooth Low Energy is not backwards compatible with existing Bluetooth technology. The architecture dictates that low resource devices, such as health monitors, will support a new low energy protocol stack while higher end devices, such as mobile phones and PCs, will support both the existing Bluetooth protocol stack and the new low energy stack. The Bluetooth Low Energy protocol calls the low resource devices "single-mode" and the higher end devices "dual-mode." Dual-mode devices will facilitate communication between the low energy devices and the rest of the network. Bluetooth Low Energy devices will support higher data rates than 802.15.4 and will be able to take advantage of the infrastructure offered by the dual-mode devices. Transmission distances will be in the range of 5 to 15 meters [8].

Wi-Fi (IEEE 802.11) is included in nearly all home networks. By far, it is the most accepted protocol for wireless communications inside of the home. Although Wi-Fi typically requires more power than Bluetooth or any of the 802.15.4-based protocols, it enjoys an enormous infrastructure. There are products that are considered "Low-Power" Wi-Fi and serve some of the same applications as 802.15.4-based protocols. These offerings are mostly standards compliant proprietary solutions that achieve lower power consumption with lower data rates and by reducing the amount of time that they permit the radio to listen to the channel. When communication is not necessary, the chip sets are placed in standby mode, high-speed clocks are shut off, and a low frequency clock source is typically used to keep a schedule of times when the device must wake up. Although low-power Wi-Fi solutions are not as low-power as 802.15.4-based solutions, these products can work well in cases where it is desirable to use battery power, low data rates, and an already existing Wi-Fi infrastructure. Wi-Fi's stable infrastructure could make it a major player in the home network.

The value of a home network to the homeowner grows with the number of devices that can connect and communicate. The wide range of home networking applications and large number of devices that need to connect necessitate that the home network use several physical links. Ethernet, 802.15.4, 802.11, Bluetooth and cellular all have a place in the home network. It is not likely that one protocol can completely replace the others, nor are any protocols claiming to move in that direction. The home M2M network will need to support multiple physical links and protocol stacks.

The protocol stacks that run on top of the physical links need to communicate efficiently and share information. The first step in facilitating efficient communication between devices is to use a common addressing scheme. The natural choice for a common addressing scheme is IPv6 addressing. If all local networks support IPv6 addressing, then the gateway will become more like a router that only needs to be concerned with routing packets, instead of running specialized NAT applications. IPv6 addressing supports 128 bits of address space, which is more than enough addresses space to allow every device in the world to have its own IP address. The challenge for M2M communications is to develop low power network protocols that support IPv6 addressing, effectively removing the need for NAT. This is the type of effort that is being performed in the ZigBee core stack working group and IETF working groups which were discussed earlier. These efforts will allow the gateways that are shown in Fig. 1 to more readily share computational resources and information across local networks.

III. M2M Power Requirements

The feature that most distinguishes M2M devices from other home electronic devices is their very low power consumption. Many M2M devices are expected to last years without requiring replacement batteries. Some devices use energy harvesting techniques to allow them to operate indefinitely without any power source; for example, a switch may harvest energy from the toggling of the switch to transmit a signal to a relay that controls a light fixture. It is easy to envision scenarios where there are over 100 low power devices in a home, many of them in hard to reach places; for example, actuators can be used to move elevated security cameras, relays can be embedded in electrical outlets, and motion detectors can be mounted high on walls external to the home. Tedious maintenance requirements associated with these devices could be the deciding factor in a homeowner's purchasing decisions. In order to increase battery lifetimes, the computational resources in the gateway need to be leveraged in a way that decreases the amount of processing that is required by the low power devices.

One common theme that is found in almost all of the low power M2M network protocols is the rule that battery powered devices should be in a sleep, or low power, state for as long as possible without degrading the intended performance of the network. Devices can go minutes, hours, or even days without waking up; duty cycles can approach 0.1%. Long sleep cycles have a significant impact on M2M routing algorithms. In order to conserve energy, the IETF ROLL working group recommends that the home network avoid using any battery powered devices for routing [9]. However, it is necessary to use such devices for routing if there are not mains powered devices near every battery powered device.

When battery powered devices are used for routing, the network topology will continuously change due to nodes going into and out of sleep. Other events, such as changes to the RF

channel and the movement of devices through the home, will also change network topology. Many low power protocols, such as ZigBee, use an Ad hoc On-demand Distance Vector (AODV) routing protocol. In a network that uses AODV, nodes that are not a part of active communication paths neither maintain any routing information nor participate in any periodic routing table exchanges [10]. Routing paths are established on an as-needed basis, so the routes can be based on whatever nodes are awake and able to communicate. Nodes that are not part of active communications can sleep while the rest of the network communicates. Additionally, the device that initiates the information exchange performs most of the computational work in the routing protocol. The necessary computations include evaluating the responses to the route request and then choosing the route with the lowest network cost. This evaluation may simply select the path with the smallest number of hops or it could take more information into account such as the amount of energy that is remaining in the batteries of each node in the possible routes [11].

Numerous other techniques are available to make routing more power efficient. Reference [12] uses an approach similar to AODV to establish the delivery route, and then commands the nodes along the selected route to switch channels before downloading large amounts of data. This approach prevents nodes that are not included in the routing path from overhearing the data exchange and processing unwanted data. Reference [13] proposes placing powerful aggregation nodes throughout a dense sensor network to assist in collecting data. This same idea can be applied to home networks. Instead of using special aggregation nodes, mains powered devices, such as appliances, could be used to assist with routing data to and from battery powered devices. Reference [12] proposes a novel approach to wakeup where the sensor node does not immediately listen to the channel upon wake up. Instead, the low power node sends a probe message to its neighbors to check if anyone whishes to communicate with it. This concept can be extended to home networks. Instead of the gateway continuously attempting to send packets to low duty cycle nodes, the packets can be routed to the node's nearest mains powered neighbor who can store the query or command until the low power device wakes up and transmits a probe. Here we see a case where the gateway can intelligently delegate to a mains powered device the responsibility of caching and forwarding a message. The common theme in all of these data dissemination approaches is an attempt to minimize the computational demands on the low resource devices and extend sleep durations by allowing the gateway or other mains powered devices to do most of the work.

IV. M2M Gateways

As the home network matures, the gateway will become an integrated device, and the architecture shown in Fig. 1 will converge to something that is closer to that of Fig. 3. The integrated gateway will be able to intelligently manage the power concerns of the entire network and provide an efficient path for communication between networks. It will be knowledgeable of the resources available in each of the connected devices, and it will use this knowledge to make intelligent routing and caching decisions.

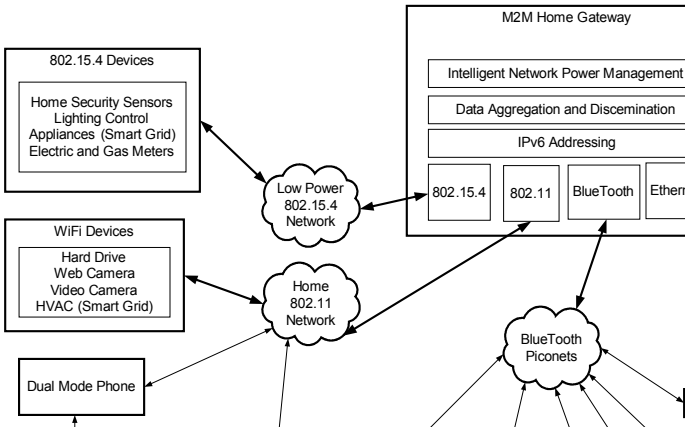

Figure 3. A Converged Home M2M Network

An integrated M2M gateway could provide convenient web-based management for the home network [14]; it could be a single point of contact that the homeowner can use to manage the entire network. The fact that there are many different physical communication links in the network would be transparent to the homeowner. The always connected, always powered gateway could query and collect data from the network at the most efficient times, and the homeowner could examine or control the network status by logging onto the gateway. The homeowner would not be burdened with managing several gateways. Beyond the basic convergence of the local gateways, the addition of SDR technologies and cellular communications are two enhancements that could make the gateway an even more efficient management point for the home network.

Software Defined Radio (SDR) has a number of characteristics that make it well suited for the home M2M gateway architecture. The SDR Forum defines SDR as "a collection of hardware and software technologies where some or all of the radio's operating functions (also referred to as physical layer processing) are implemented through modifiable software or firmware operating on programmable processing technologies. The use of these technologies allows new wireless features and capabilities to be added to existing radio systems without requiring new hardware" [15]. SDR-based home gateway designs would be multicarrier and multiband products that can communicate simultaneously with different protocols, on different frequencies, and in different frequency bands.

Reference [16] proposes a vehicular gateway that is SDR-based and supports cellular, Bluetooth, and ZigBee protocols. Rather than an IP-based backhaul, the design routes data to and from a generic bus that connects to the vehicle's internal components such as audio, diagnostic, and navigation systems. The design shares processing resources across communication

protocols and can use multiple protocols simultaneously. An SDR architecture simplifies network upgrades; protocol modifications and updates could be supported via software downloads [17]. This type of flexibility increases the lifetime of the gateway and allows for extended support of legacy devices. Many of the advantages that SDR offers in the vehicular network would also be useful in the home network.

As the home network continues to evolve, it will become even more important to better support devices that move into and out of the home, such as cellular devices, e.g. phones and mobile PCs. Cellular devices need to communicate in the same manner when inside the home or when miles away from the home. Highly mobile devices are often the most convenient interface to the home network. Examples are sharing multimedia content between a mobile PC and a television or simply adjusting the thermostat from a phone.

Some cellular devices also support Wi-Fi so that they can communicate from within the home network. These devices use a cellular connection when outside of the home and switch to Wi-Fi when inside of the home. This approach requires that the cellular device support multiple radio access technologies, with the additional features resulting in increased product cost. An alternative approach is to allow the home network to be managed by a femtocell, a miniature cellular base-station with an IP-based backhaul that also supports the local network protocols that are found within the home. Mobile devices would no longer need to support multiple physical links because they could connect to the femtocell with their cellular radio interface. Femtocells would give cellular operators an avenue into the home network, and it would allow more services to be offered to the homeowner.

The integrated home gateway, SDR technologies, and femtocells, all help to continue the trend towards making the gateway more powerful and network devices more cost-effective. The result is a network that is more valuable to the homeowner and service providers. The homeowner benefits because more devices will be able connect, control will become more convenient, and additional services will be available. Service providers will benefit from the new revenue opportunities that will be created by additional devices connecting to the network.

V. Conclusion

As M2M devices achieve more market penetration, we will see home networks with devices numbering in the hundreds. There will be no single physical layer solution that fulfills all of the power, distance, and data rate requirements in the home network. Instead, multiple physical layer protocols will be used throughout the home, and it will be necessary for the protocol stacks to communicate with each other. In order for a large home network with diverse physical links to gain wide acceptance, it must be highly integrated and user friendly. The M2M gateway will be the component that is most responsible for integrating the local home networks. It will facilitate communications between devices that were previously disjoint and provide the homeowner with a convenient interface for network management. This will result in new opportunities for device manufactures, content providers, and bandwidth providers. Device manufactures will be able to pursue new product offerings that take advantage of the highly connected home. Bandwidth and content providers will be able to reach more devices than what they can reach today, thus presenting opportunities to offer new service bundles.

In order to be successful, home M2M gateway designs must carefully consider the characteristics of the devices in the home and the types of traffic that they generate. Although most of the home network traffic is for high data rate multimedia, the majority of devices in the home are low power and low data rate. The gateway must efficiently manage both types of traffic. It is important to manage the network such that the many low resource devices use their energy resources wisely. This could make the difference between a device being an asset to the homeowner or an annoyance because of frequent maintenance requirements.

References

[1] C. Park, K. Jeong, S. Kim Y. Lee, “NAT issues in the remote management of home netwrok devices,” IEEE Network, vol. 22, issue 5, pp. 48-55, September-October 2008.

[2] S. Guha, P. Francis, “Characterization and management of TCP traversal through NATs and firewals,” Proc. Internet Meansurement Conference, Berkeley, CA, October 2005.

[3] J. Adams, “An introduction to IEEE STD 802.15.4,” IEEE Aerospace Conference, 2006.

[4] D. Sturek, “ZigBee IP stack overview,” ZigBee Alliance, 2009.

[5] The Internet Engineering Task Force (IETF), www.ietf.org

[6] X. Ma, W. Luo, “The analysis of 6LoWPAN technology,” IEEE Computational Intelligence and Industrial Application 2008, pp. 963–966, December 2008.

[7] D. Culler, “Secure, low-power, ip-based connectivity with IEEE 802.15.4 wireless networks,” Industrial Embedded Systems, Summer 2007.

[8] A. Omre, “Reducing healthcare costs with wireless technology,” 2009 Wearable and Implantable Body Sensor Networks, pp. 65-70, June 2009.

[9] A. Brandt, J. Buron, G. Porcu, “Home Automation Routing Requirements in Low Power and Lossy Netwroks”, IETF, November 2009.

[10] C.E. Perkins, E.M. Royer, “Ad-hoc on-demand distance vector routing,” Mobile Computing Systems and Applications, 1999, pp. 90–100, Febuary 1999.

[11] A. Mohajerzadeh, M. Yaghmaee, “An energy aware routing protcol for real time traffic in wireless sensor networks,” International Conference on Ultra Modern Telecommunications and Workshops, pp. 1-9, October 2009.

[12] R. Musaloiu-E, C.-J.M. Liang, A. Terzis, “Koala: ultra-low power data retrieval in wireless sensor networks,” Information Processing in Sensor Networks, 2008, pp. 421–432, April 2008.

[13] W. Liang, G. Ma, Y. Xu, and J. Shi, “Aggregate node placement in sensor networks,” Communication Systems, 2008, pp. 926–932, November 2008.

[14] K. Hwang, J. In, N. Park, D. Eom, “A design and Implementation of wireless sensor gateway for efficient querrying and managing through world wide web,” IEEE Transactions on Consumer Electronics, vol 49, issue 4, pp. 1090–1097, November 2003.

[15] Software Defined Radio Forum, www.sdrforum.org

[16] B. Gu, J. Heo, S. Oh, N. Park, G. Jeon, Y. Cho, “An SDR-based wireless communication gateway for vehicle networks,” Asia-Pacific Services Computing Conference, pp. 1617–1622, December 2008.

[17] A.C. Tribble, “The Software Defined Radio: Fact and Fiction,” Radio and Wireless Symposium, 2008, pp. 5–8, January 2008.