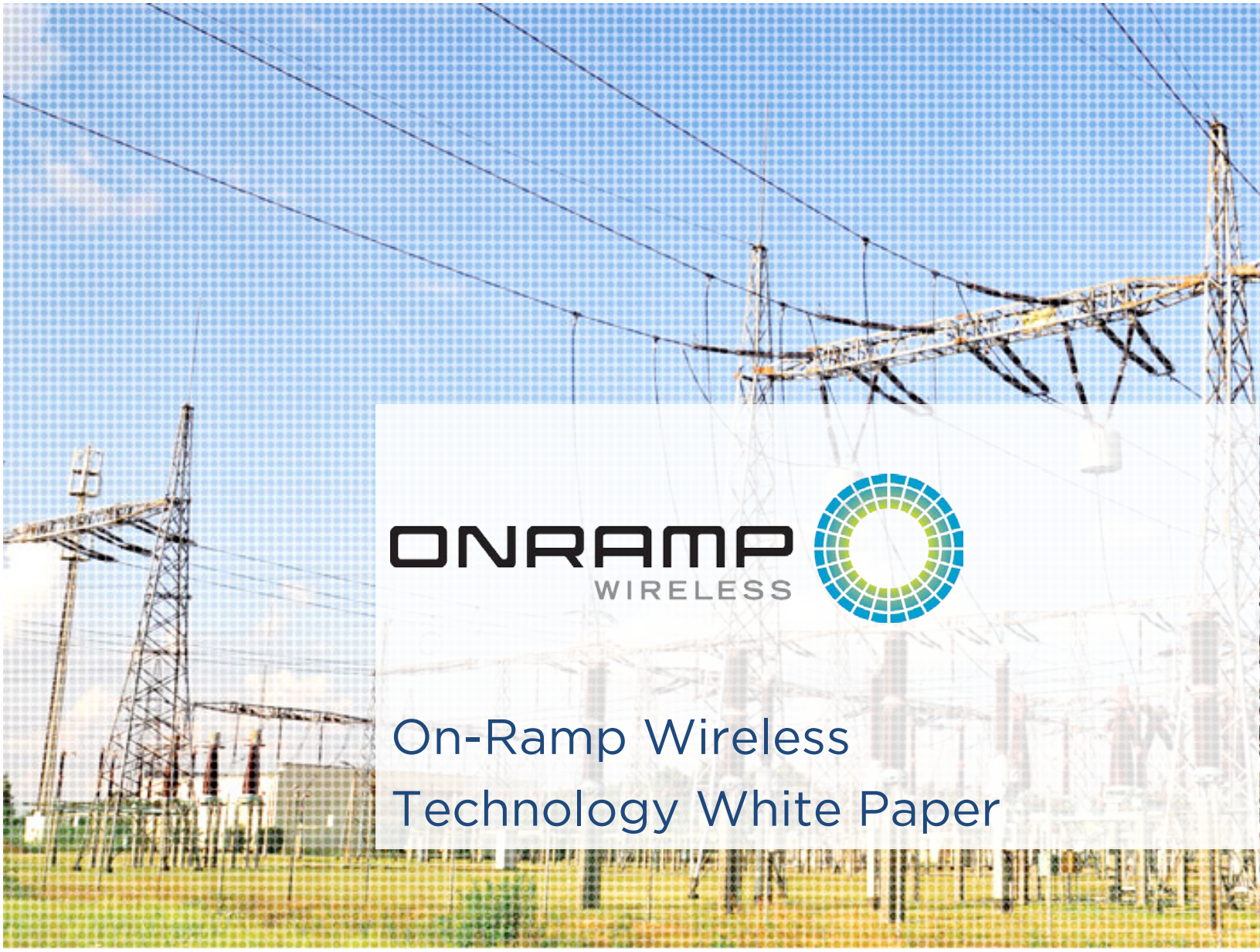

ONRAMP WIRELESS

On-Ramp Wireless Technology White Paper

On-Ramp Wireless Incorporated
10920 Via Frontera, Suite 200
San Diego, CA 92127
U.S.A.

On-Ramp Wireless Technology White Paper

008-0012-00 Rev. H

January 9, 2013

Contents

Figures

Tables

Revision History

Revision	Release Date	Change Description
A	April 5, 2011	Initial release.
B	May 19, 2011	Updated for technical engineering changes.
C	June 6, 2011	Updated for technical engineering changes.
D	July 1, 2011	Expanded content.
E	December 19, 2011	Added information to Section 6.2, Limited Source of Interference.
F	February 23, 2012	Updated Table 5: Endpoints Serviceable per AP for Different Target Applications.
G	December 21, 2012	Updated branding.
H	January 9, 2013	Removed confidentiality restrictions.

1 Introduction

1.1 The Vision

Over the last two decades, billions of people have connected themselves to the Internet using computers, and most recently, mobile phones. This communication revolution is now extending to objects. This revolution goes by many names, from "machine-to-machine" (M2M) communication to the "Internet of Things." Whatever the name, the vision is the same: to connect objects so that they have the information to function optimally (1). The vision includes:

- Smart electric grids that automatically adapt themselves to changing load conditions and drive lower energy use by spreading demand.
- Gas and water distribution systems with automated metering and leak detection.
- Buildings that adapt to changing temperatures to save energy.
- Shipping containers that can track temperature, humidity, location, and tampering as they travel across the world.

Table 1 lists examples of more applications across various industries. Though the data throughput requirements for these devices are often relatively low, there are significant challenges in connecting them:

- They are widely distributed across large geographic areas.
- They are often located in difficult radio environments, e.g., in basements, below ground, and in shielded environments.
- They require latency in near real-time, i.e. on the order of seconds, less than one minute.
- They require an extremely secure network due to their critical nature.

Due to these challenges, most devices remain unconnected. There has not been a secure, reliable, and cost-effective way to connect them…until now. On-Ramp Wireless has developed a ***purpose-built*** wireless communication solution to overcome these challenges.

Table 1. On-Ramp Wireless Target Applications

Utilities/Smart Grid	Process Industries	Personnel and Asset Tracking	Critical Infrastructure
Smart Electric Meters Smart Transformers Fault Circuit Indicators Distribution Automation Gas Meters Water Meters	Pressure Sensors Temperature Sensors Vibration Sensors Chemical Sensors Radiation Sensors Leak Detection	First Responders Military Personnel Vehicle Fleets Railroad Freight Shipping Containers Other Vehicles	Surveillance and Security Border Control Bridge Monitoring Fire Detection Landslide Monitoring

1.2 What is the On-Ramp Solution?

The On-Ramp Total Reach Network is a ***purpose-built***, Direct-Sequence Spread Spectrum (DSSS) technology powered by Random Phase Multiple Access (RPMA)—an innovative new multiple access method. It is a frequency-agnostic technology that can be operated on any 1 MHz slice of spectrum, licensed or unlicensed. The current RF-integrated solution operates in the globally available 2.4 GHz band.

As mentioned above, the On-Ramp Total Reach Network is ***purpose-built*** to the needs of device monitoring. It is designed with a focus on connecting data from a large number of devices to a network infrastructure that collects data for processing in various back-end applications. While the system favors uplink transmissions (device to network), it also features advanced downlink (network to device) unicast, multicast, and broadcast features. For example, the On-Ramp Total Reach Network allows for the broadcast of large firmware upgrades, either for the device or for the wireless module.

Though the fundamental communication breakthrough is capable of servicing many vertical markets, On-Ramp Wireless was initially focused on commercializing the technology for the utility space. To this end, the On-Ramp Total Reach Network is built to be utility-grade. The system meets or exceeds all smart grid communication requirements, including those recommended by the United States National Institute of Standards and Technology (NIST). These requirements include specific security guarantees, reliable data delivery, redundancy, availability, remote upgradeability, logging, event alarms, greater-than 20 year battery life for certain applications, and complete network management capabilities.

The On-Ramp Wireless Total Reach Network is an end-to-end wireless communication system, including back-office integration and network management. This system integrates seamlessly with a vast ecosystem of companies involved in other network and delivery components; including architecture design, network optimization, manufacturing, installation, network operations and maintenance, data warehousing, data analytics, business process integration, information technology, etc. Even though the On-Ramp Total Reach Network is still a relatively small piece of the puzzle, it is the foundation for effective communications—the base of the pyramid as illustrated in Figure 1.

As the foundation, it is an extremely important piece to get right. In any communication network, the physical (PHY) and medium access control (MAC) layers are closest to the laws of physics. Consequently, it is virtually impossible to correct inadequacies in the PHY/MAC at higher layers without sacrificing other fundamental aspects. Fortunately, the performance of these lower pieces of the pyramid can be analyzed objectively, and unlike higher layers, clear decisions based on objective criteria can be made.

Not only is it possible to select the correct technology as the “base of the pyramid”, it is ***essential***! The selection of a non-suitable technology will result in a greatly increased expense and degraded wireless performance for the envisioned applications. In addition, it will threaten the existence of a substantially larger ecosystem that uses the foundational technology.

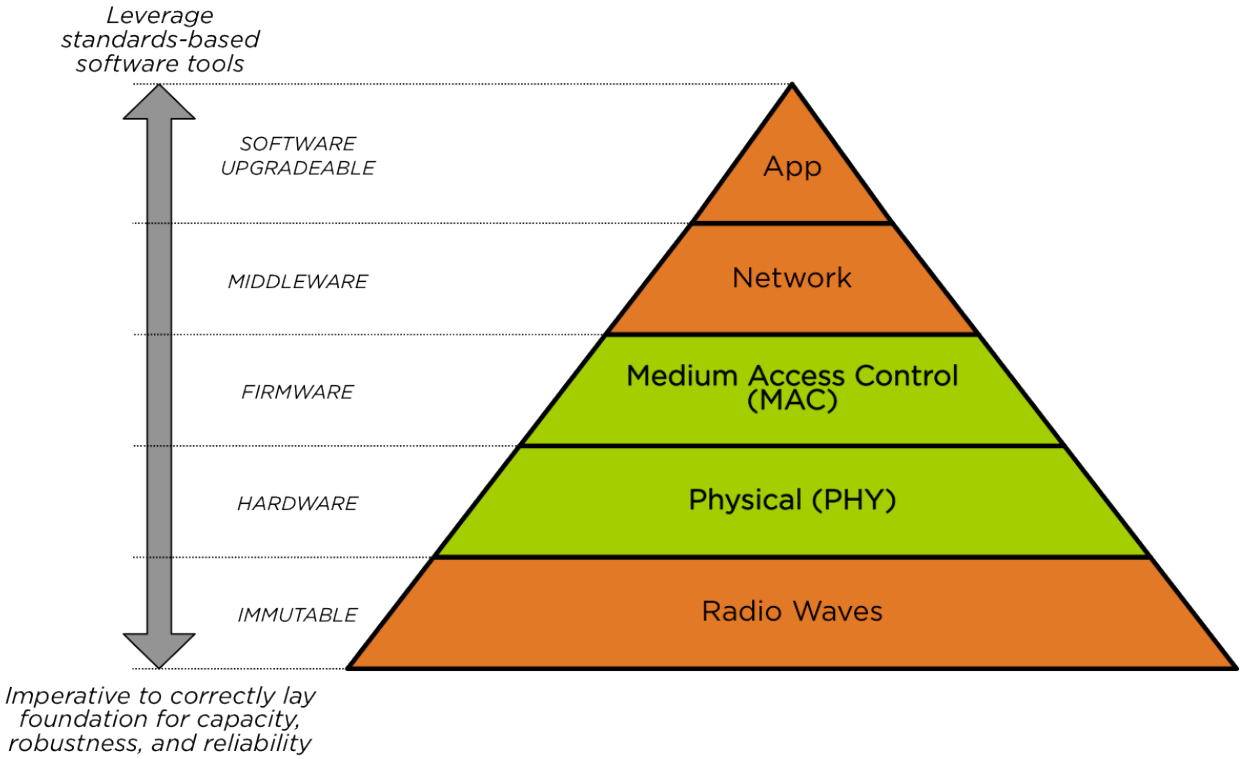

Figure 1. The PHY and MAC layers are the foundation of any wireless communication technology.

On-Ramp Wireless strongly believes that its network is the foundation upon which device networking will be built. With this belief, On-Ramp Wireless is firmly committed to standardization. In an effort to accelerate this process, On-Ramp Wireless was a founding member of the IEEE® 802.15.4k Low Energy Critical Infrastructure Monitoring (LECIM) task group. Through this group, and in cooperation with other industry leaders, On-Ramp Wireless continues to move toward an open standard under the IEEE umbrella.

1.3 End-to-End Solution

The On-Ramp Wireless solution is more than the wireless communication link. Building on the foundation of wireless communication, On-Ramp Wireless has built the On-Ramp Device Management System (DMS), including:

- The wireless modules (endpoints[1]) used for simple and standardized integration with the endpoint devices.
- The Access Points (APs), which are mounted on mountain tops, pole tops, towers, rooftops, and other elevated sites, and provide the ***only*** field installed network infrastructure.

[1]Endpoint refers to the wireless module connected to the monitored device.

- The Gateway (GW), managing AP connections in a network, handover between APs, and the data path to the back-end applications.
- The Security Key Management Server (KMS), responsible for providing end-to-end security features.
- The Critical Infrastructure Management Application (CIMA), providing endpoint data management and seamless integration into back-office systems through a suite of standard interfaces.
- The Element Management System (EMS) responsible for network management and alarms related to network components.
- IPv6 addressability.

Figure 2 illustrates the On-Ramp Wireless end-to-end system architecture along with examples of third-party applications that can be integrated.

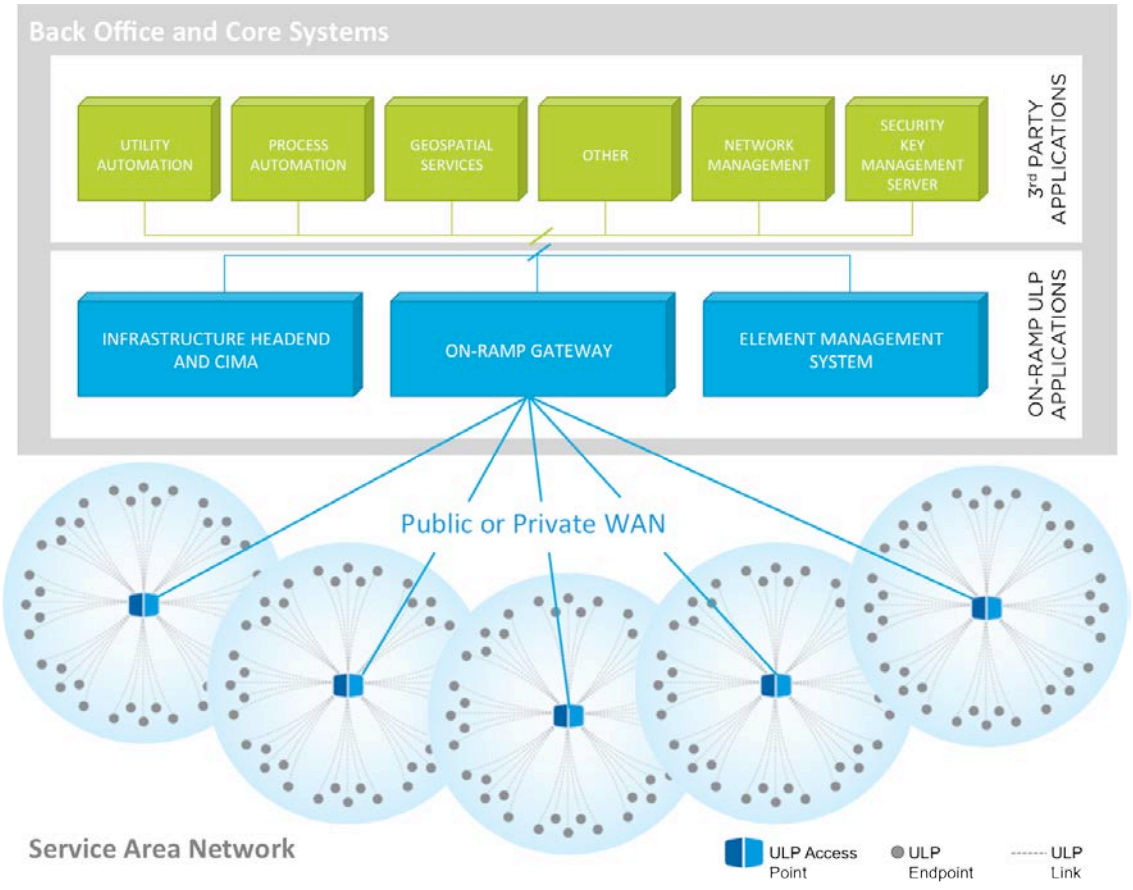

Figure 2. On-Ramp Wireless System Architecture

1.4 System Highlights

The On-Ramp Total Reach Network represents a significant breakthrough in wireless signal processing technology, and On-Ramp Wireless has now commercialized this core innovation. To summarize, here are some of the system highlights which set this technology apart:

- Greater than 40 miles (65 km) line-of-sight range
- Up to 400 square miles of non-line-of- sight coverage from a single advantaged AP site.
- Coverage to underground assets over 2 miles away from AP sites.
- Random Phase Multiple Access (RPMA), a unique multiple access method with order of magnitude capacity improvements, and demodulation of up to a thousand incoming signals, below the noise floor, for every frame.
- Capacity to support millions of devices on a single network.
- Ultra low power consumption, allowing up to a 20-year battery-life for water meter applications, gas pressure sensors, etc.
- Comprehensive, third-party validated security.
- Seamless failover in case of an AP outage, a backhaul failure, etc.
- Worldwide applicability in license free spectrum that is adaptive to local regulatory regimes.
- Simple and flexible integration with back-end automation systems, such as OMS, DMS and MDMS systems, process automation systems (e.g., OSIsoft PI™, Modbus™), and others.
- Intelligent Data Integrity throughout the entire data path.

When combining all these advantages, the result is a system that provides the lowest total cost of ownership in the industry. The On-Ramp Wireless System is, by far, the best wireless sensor networking solution on the market today.

2 Competitive Landscape

2.1 The Competitor's Approach

There are a number of wireless technologies competing in the device monitoring space. The three primary competitors are:

- Cellular radios
- Unlicensed wireless mesh radios
- Licensed narrowband radios

These are all reputable technologies with a strong track record in many application spaces. They are not, however, the right selection for the class of devices On-Ramp Wireless targets. These technologies were originally designed for applications that are significantly distinct from the needs of the target device endpoints. They have significant limitations in scaling to a low bandwidth, widely distributed wireless network with potentially tens of thousands of hard-to-reach devices.

For example, cellular is evolving in the opposite direction of what is needed for device networking. Consumers are clamoring (and paying) for costly endpoints, such as smart phones and tablet PCs. This is driving the cellular industry toward high bandwidth, high cost, and power hungry wireless communication technologies. This clearly goes against the grain of many performance aspects that are essential for device connectivity:

- Low-cost infrastructure
- Efficiency for small payload data transactions (as opposed to streaming video)
- Coverage of locations where consumers do not frequent, e.g., underground, rural.
- Minimal power consumption for un-connected devices.

Table 2 lists various competing technologies and their limitations. Compared with these technologies, On-Ramp Wireless is the ***only*** one that delivers the optimal mix of coverage, capacity, robustness, low power consumption, and security for wide area device monitoring applications.

Table 2. Competing Technologies and their Limitations

Cellular Radios	Limitations
GSM/GPRS WCDMA WiMax™/LTE	■ Telephone company or operator controls the licensed network ■ Coverage gaps and limited coverage for hard-to-reach locations ■ Capacity is limited with networks already overloaded ■ Short battery life ■ Network end-of-life issues, e.g. sunsetting of 2G networks ■ High monthly op-ex ■ Unfavorable prioritization in the event of an emergency (forest fire, flood, etc.)
Unlicensed Wireless Mesh Radios	**Limitations**
SSN 900 MHz FHSS Mesh Itron 900 MHz FHSS Mesh 802.15.4. ZigBee® Mesh 802.11 WiFi Mesh	■ Limited range ■ Requires dense deployment of network infrastructure ■ Difficulty handling urban or rural scenarios ■ Requires deployment of entire infrastructure for connectivity, i.e. cannot have slowly scaling deployments ■ Limited capacity ■ Not robust to congestion ■ Not suited for long battery life ■ High total cost of ownership
Licensed Narrowband Radios	**Limitations**
Sensus Flexnet™ Aclara® STAR® Network 169 MHz wM-BUS	■ Vendor controls the licensed band – costly ■ Limited regional availability ■ Limited capacity leads to a denser AP deployment for higher data rate applications ■ Not robust to congestion ■ Higher total cost of ownership

2.2 The On-Ramp Wireless Approach

The On-Ramp Total Reach Network is based on a fundamental signal processing approach called DSSS. This approach was introduced in the 1950s and was most famously applied in the form of Code Division Multiple Access (CDMA) developed by Qualcomm® beginning in the 1980s.[2] Qualcomm upended the world of cellular communications with CDMA; a purpose-built DSSS based technology for voice telephony that was orders of magnitude better than the competition at the time. CDMA is now the standard technology for all 3G cellular communications. On-Ramp Wireless' innovations are a close parallel to those founding the basis of success for Qualcomm, continuing to build on San Diego's wireless technology dominance.

Fundamentally, DSSS is a way to optimize robustness for lower data rate applications. Not surprisingly, a link with a lower data rate can be successfully received a greater distance away than a link of a higher data rate. The fundamental knob of DSSS is processing gain, which parameterizes the trade of robustness for data rate. A large class of devices benefit from turning the processing gain knob as far as possible in favor of robustness, even though that reduces the

[2] DSSS terminology is also referenced in the 802 family of standards. However, the DSSS aspect is not a component of the channelization mechanism and is very distinct from the On-Ramp Wireless System.

data rate. Indeed, the tolerance of an endpoint to relatively low link data rates is the most important qualification to being within the strike-zone of On-Ramp. It is important to note that even though a single link has a modest data rate, DSSS technology allows for many simultaneous links to occur. As described in more detail in the Capacity chapter, this allows for a large aggregate data rate at each AP in the network.

The question, then, is this: Why haven't others taken the On-Ramp Wireless approach to wireless device networking? The short answer, is because it is very difficult, and the timing has not been right until now. The On-Ramp Total Reach Network is not a clever trick. It is the culmination of many factors:

1. **Computational Power.** Moore's law[3] has driven down the cost and power consumption of silicon to achieve today what could not have been achieved 10 years ago in commoditized silicon. The cellular industry has harnessed this power to create devices with higher bandwidth, faster data rates, and lower latencies. On-Ramp Wireless has harnessed the same computational power to optimize for coverage and capacity instead.
2. **Significant capital.** The development of the On-Ramp Total Reach Network required a commitment of many millions of dollars to develop it from the ground up, including the cost of a special-purpose ASIC.
3. **Innovative Algorithms.** Demodulation in the On-Ramp Wireless System requires innovative algorithms that reduce the computational complexity by a factor of 10,000.
4. **A World-Class Team.** The On-Ramp Total Reach Network was developed by a team of wireless experts capable of designing complicated modems that are extremely power efficient.

To highlight one of the many challenges of implementing a high processing gain modem, consider the complexity of acquiring (i.e., finding) a signal that is at -35 dB of signal-to-noise ratio (SNR). Cellular technology uses 20 dB of "processing gain", and there is no technology driver for more, because, as mentioned earlier, data rates below voice are not interesting to the consumer. The On-Ramp Total Reach Network, by contrast, is exclusively interested in data rates below voice. All things being equal, the amount of computations required to acquire the signal compared to a cellular signal is proportional to the processing gain cubed. Specifically, if acquiring a cellular signal requires 10,000 arithmetic operations, acquiring the On-Ramp Wireless signal requires 10,000*1,000,000 operations—a factor of 1 million more! A radically different looking modem and waveform is required to make this number manageable. On-Ramp Wireless' successful convergence on all these factors is translating into the rapid adoption of the On-Ramp Wireless solution for targeted applications. The next chapter provides a few objective methods that evaluate the strengths of the On-Ramp Total Reach Network.

[3] Moore's law refers to the doubling of the number of transistors on silicon every 2 years.

3 Wireless System Performance Metrics

Due to the unique challenges of device monitoring, there are a number of important characteristics to consider when evaluating a wireless solution, including:

- **Coverage:** The range of a wireless link to reliably connect devices. The range is measured in meters from the AP and varies depending on the RF propagation environment. Factors, such as terrain, clutter type (urban, suburban, rural, etc.), interference, and local output power regulations determine the range capabilities of a specific radio.
- **Capacity:** The amount of data from device endpoints an AP can simultaneously serve. The capacity is measured as the aggregate application throughput (kbps) at the AP.

  Coverage and capacity must work hand-in-hand to achieve a highly performing network. They work in conjunction to drive the ratio of APs (or network infrastructure points[4]) to device endpoints. Providing coverage for many devices without proper capacity is pointless; conversely, excess capacity without coverage to reach devices is equally pointless. It is the optimal mix of the two that delivers cost effective performance for a wireless network.
- **Coexistence:** The ability of a wireless technology to coexist with other devices that can cause significant and dynamic interference. This is particularly important when operating in unlicensed bands.
- **Power Consumption:** The ability to support a long battery life. Many devices, such as gas and water meters, are not continuously powered. Connecting these devices with extremely long battery life wireless modules, on the order of years, is important in creating a cost-effective connectivity solution.
- **Security:** The ability of a wireless system to resist malicious attacks from cyber criminals. To prevent malicious attacks, the device networks, particularly those focused on critical infrastructure, require proven and robust cyber-security across the network.

  The following chapters describe how the On-Ramp Total Reach Network powered by RPMA excels in all five of these critical areas.

[4] Network infrastructure is required to support the network and route the data back and forth. The term, Access Point (AP), is used for the On-Ramp Wireless System. Base station or gateway may be used to refer to other systems.

4 Coverage

As mentioned above, coverage, along with capacity, drives the ratio of APs to endpoints. This ratio, in turn, drives the total cost of ownership for the network. The coverage goal is to reach as many devices as possible per AP.

4.1 Link Budget

The primary driver of coverage is link budget. Link budget measures the ability of a wireless system to overcome obstacles to close a link. It is a balance sheet of gains and losses, accounting for the effect of all the processes throughout the link, including transmit power, noise sources, and signal attenuators. Conceptually, it can be thought of as a financial budget. It determines how much "money" we have to spend in closing the link by overcoming interference, shadowing, fading, and propagation losses. Different people consume money differently, and different configurations of the same system can consume link budget differently. In the following section, we illustrate certain configurations of the On-Ramp Total Reach Network and how they consume link budget.

First, we focus on figuring out how much "money" we have. Link budget is driven by many factors, but at the highest level, there are three primary factors that contribute to link budget: transmit power, antenna gain, and receiver sensitivity.

In all radio frequency bands, especially unlicensed ones, regulation limits the Effective isotropic Radiated Power (EiRP), which is the transmit power, minus the cable loss, plus the antenna gain. For example, in North America, the Federal Communications Commission (FCC) limits the EiRP in the 2.4GHz band to 36 dBm (4W) per 1 MHz. In Europe, the European Telecommunications Standards Institute (ETSI) limits the EiRP to 10 dBm (10mW) per 1 MHz. All radios in the same band face these restrictions which ultimately limit transmit power and antenna gain.

This leaves receiver sensitivity as the differentiator. Receiver sensitivity reflects the radio's ability to detect signals—the lower the sensitivity, the better. It is a function of modulation technique, coding, and other advanced signal processing. On-Ramp Wireless has developed a ground breaking, DSSS physical layer with a 40 dB advantage in receiver sensitivity over typical unlicensed band radios. Competing radios operate at a positive SNR above the thermal noise floor with approximately -102 dBm receive sensitivity. By contrast, the On-Ramp Total Reach Network, with a receive sensitivity of -142 dBm on the uplink, operates significantly below the thermal noise floor.

Table 3 tabulates the link budget of the On-Ramp Total Reach Network in both the uplink and downlink direction with FCC and ETSI limits. The link budgets are asymmetric, because the receiver sensitivity is asymmetric. Adding up all the factors, the On-Ramp Wireless System has a link budget of 172 dB with FCC limits and 145 dB with ETSI limits. The On-Ramp Total Reach Network has 40dB more link budget as compared to competing radios. Continuing the "money" analogy, the On-Ramp Total Reach Network has 10,000 times as much "money" as the competition.

Table 3. The On-Ramp Total Reach Network Link Budget[5]

Uplink	Uplink (FCC)	Uplink (ETSI)	Downlink	Downlink (FCC)	Downlink (ETSI)
Endpoint Tx Power (dBm)	20	8	AP Tx Power (dBm)	30	8
Endpoint Antenna Gain (dBi)	4	2	AP Antenna Gain (dBi)	6	2
AP Antenna Gain (dBi)	6	2	Endpoint Antenna Gain (dBi)	4	2
AP Rx Sensitivity (dBm)	-142	-142	Endpoint Rx Sensitivity (dBm)	-133	-133
Link Budget (dB)	**172**	**154**	**Link Budget (dB)**	**173**	**145**

4.2 Consuming Link Budget

Now that we have accounted for how much "money" is available, we will figure out how to spend it. The following four factors consume link budget:

- Interference due to other local transmitters and system self-interference.
- Shadowing due to foliage, buildings, underground vaults, etc.
- Fading due to multipath reflections.
- Propagation losses due to distance.

For a given range, the propagation loss is fixed; range enhancement is dependent on reducing the effects of interference, shadowing, and fading. Endpoint locations are typically fixed, so the only degree of freedom is the placement of the AP. Placing the AP antenna in an elevated location can reduce the effect of shadowing and fading, as the RF signal has less clutter to travel through. This explains why cellular base stations are placed on tall towers, mountaintop antenna farms, or skyscrapers. On-Ramp Wireless encourages the same approach. The drawback of these sites, with many co-located transmitters is that they have significant interference. On-Ramp Wireless' innovative interference mitigation techniques make the tradeoff well worth it.

[5] The transmit power in this table is the power at the antenna after cable loss. It assumes that the output power of the endpoint or AP has been increased to compensate for the cable loss.

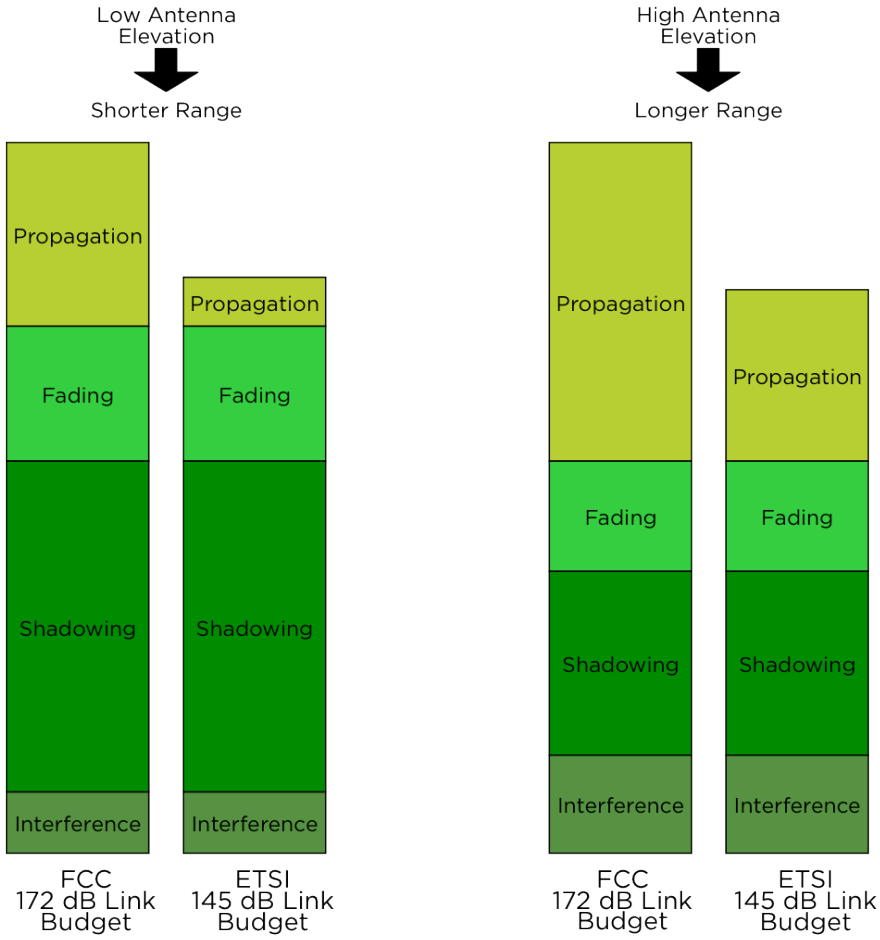

Figure 3. Link Budget Tradeoff in the Log dB Domain

Note that figures scale exponentially in the linear domain.

4.3 Coverage Maps

Figure 4 illustrates the coverage from an AP sited at Mt. Woodson, a mountain top antenna farm in San Diego, California. The antenna site has, on average, 8 dB of interference. The surrounding area is largely sub-urban. The right side of Figure 4 illustrates an approximate link budget breakdown for an FCC limited system (36 dBm EiRP) when the signal is not shadowed by terrain. The left side of Figure 4 illustrates the coverage area from the FCC-limited AP to endpoints at 2 meters height on the road. In this configuration, the On-Ramp Total Reach Network can reliably connect to sites 16 km (10 miles) away at 36 dBm EiRP.

The colors on the map correspond to the probability of coverage[6]:

- Green: Represents > 95% probability of coverage
- Yellow: Represents > 75% probability of coverage
- Red: Represents > 50% probability of coverage
- Areas without color: Represent < 50% probability of coverage

Figure 5 illustrates the coverage to endpoints at 2m on the sidewalk from an AP site located on top of Sempra Energy®[7] headquarters, a tall building in downtown San Diego, California. The antenna site has, on average, 13dB of interference. The surrounding area is mostly dense urban. In this configuration, the On-Ramp Total Reach Network can reliably connect to endpoints about 4 km (2.5 miles) in an FCC-limited system. Note that the coverage range is less than Mt. Woodson, because the urban environment shadows the RF signal.

Figure 4 and Figure 5 illustrate the coverage to endpoints at 2 meters height on the road or sidewalk. Many potential endpoints that need connectivity reside in much more disadvantaged locations, such as on the side of a building, in a basement, or in an underground vault. These configurations will have more of their link budget consumed by shadowing, further reducing the coverage footprint of the AP to these locations. Radios will be equally affected in these locations. Only On-Ramp Wireless has the link budget needed to reliably connect to these hard-to-reach locations and still maintain extensive coverage from the AP.

Wireless meshing has recently become a popular technique to extend the limited range of weak radios that have limited link budget. When deployments are dense and in favorable RF environments, such as a suburban neighborhood, meshing can be successful[8]. When deployments are sparse or not in favorable RF environments, such as exurban neighborhoods or urban environments where meters may be located in basements, the mesh architecture fractures into many clusters, requiring extensive APs to ensure reliable connectivity. Despite its success in certain environments, meshing has significant limitations and is fundamentally a

[6] Note that coverage is inherently probabilistic as the Received Signal Strength Indicator (RSSI) prediction error has a standard deviation of approximately 8 dB. The coverage maps were generated using EDX Signal™, an industry standard RF propagation-modeling tool. The model was verified with extensive drive testing.

[7] Sempra Energy is an electric and gas utility company covering all of San Diego and parts of Riverside and Orange County.

[8] This has yet to be proven in regions with lower EiRP limits than in the United States.

"patch" to the limited range of a radio. By contrast, the On-Ramp Total Reach Network is ***purpose-built*** with a massive link budget to reliably deliver extensive coverage.

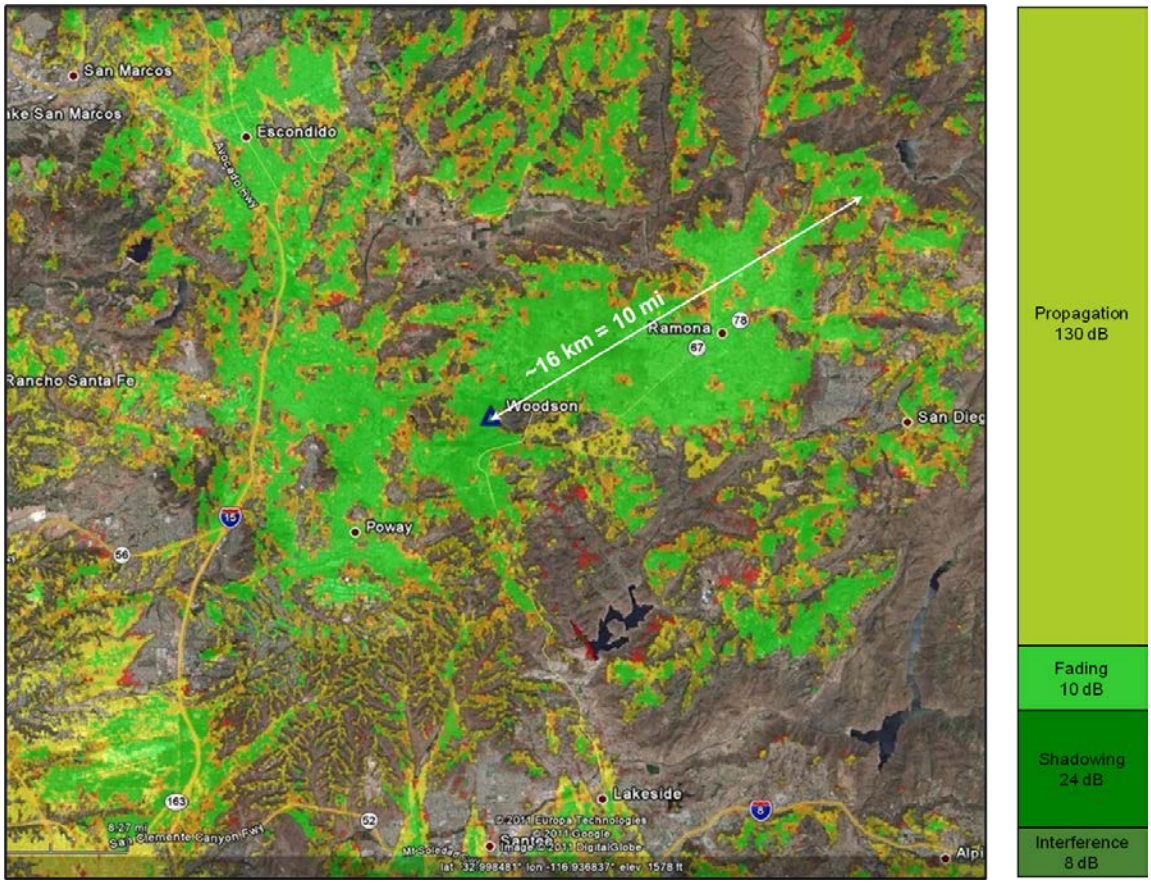

Figure 4. Mt. Woodson Coverage Map

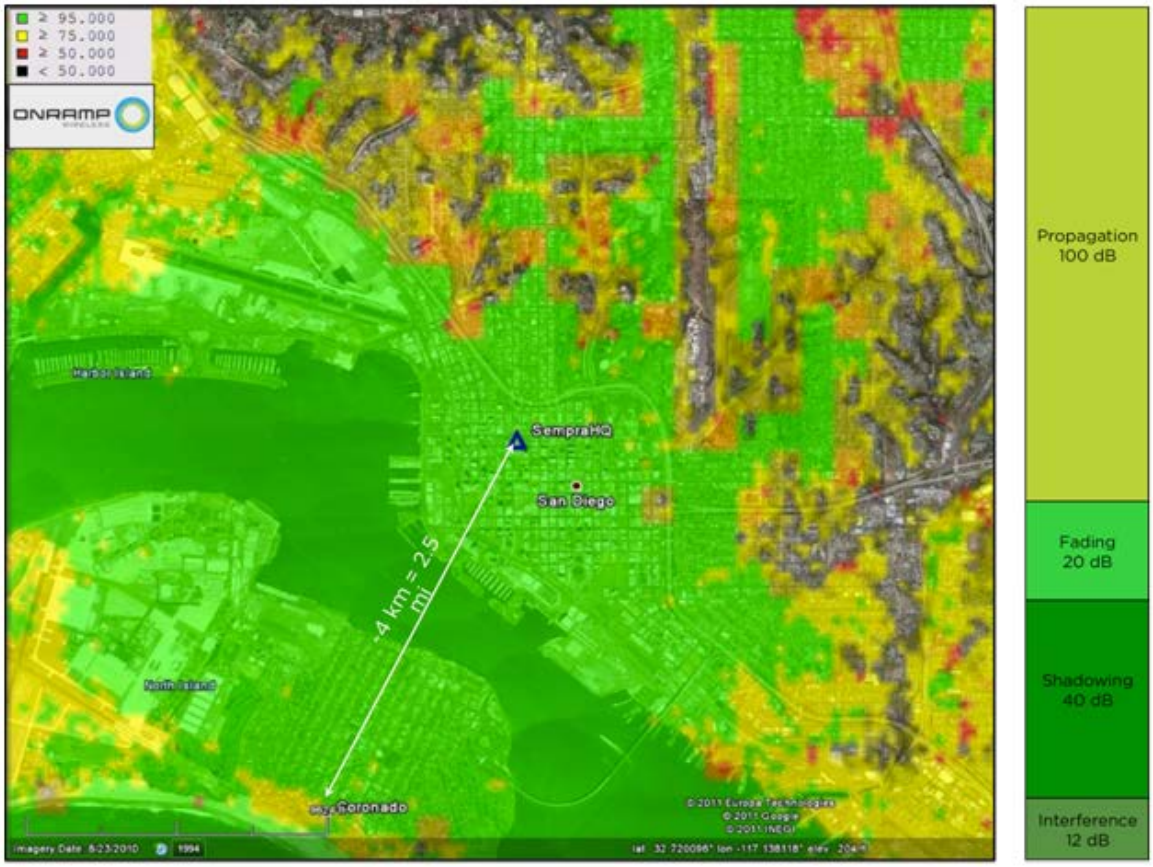

Figure 5. Sempra Headquarters Coverage Map

5 Capacity

Along with coverage, capacity drives the ratio of endpoints to APs. The capacity goal is to minimize the number of APs needed to service the large number of endpoints in a typical sensor network.

5.1 Random Phase Multiple Access

The On-Ramp Total Reach Network is ***purpose-built*** to have an immense uplink capacity. It supports thousands of simultaneous connections to a single AP using a unique flavor of DSSS called RPMA[9]. Whereas CDMA was extremely effective in channelizing 10s of users at voice data rates (~10 kbps), RPMA has been designed to channelize 1000s of endpoints each at data rates of 10s of bits-per-second. This channelization mechanism allows for an implementation in the AP that is feasible in low-cost silicon.

One of On-Ramp Wireless' fundamental innovations is an RPMA receiver which can efficiently demodulate all possible "arrival phase" hypotheses for all possible spreading factors. This requires significant amounts of computation, yet through clever algorithms, On-Ramp Wireless has been able to condense the search space to allow implementation in commodity hardware. Competing radios use more traditional statistical multiple access techniques, such as ALOHA. These techniques, though simple, are far less efficient than RPMA and squander much of the potential throughput of the physical layer.

In addition to RPMA, the On-Ramp Wireless System is designed with an extremely lightweight Over-the-Air (OTA) protocol optimized for the transmission of many small data packets from many dispersed devices. This minimizes overhead and maximizes application throughput. RPMA also allows endpoints operating in widely ranging link conditions to connect to the AP through tight power control. A device with a very weak signal does not impede any other endpoints in the network. It simply reverts to a higher level of processing gain, and in turn, consumes less of the overall available throughput.

The final capacity is a function of RPMA self-interference. As more endpoints transmit packets, each endpoint has to transmit stronger until none of them have the necessary SNR to close the link. The effect is analogous to a large party where more and more people start to talk, each raising their voices to be heard, until no one can be heard at all. The loading of RPMA can be expressed mathematically as a loss of link budget:

$$L_{dB} = 10log_{10}(E[S_{RX}]) - S_0$$

Where $E[S_{RX}]$ is the expected receiver sensitivity which, in turn, can be expressed as:

$$E[S_{RX}] = \frac{N_0 \cdot \mu_{SNR}}{G - (N_{TX} - 1) \cdot \mu_{SNR} \cdot e^{\frac{1}{2}\left(\frac{\sigma_{SNR}}{10log_{10}(e)}\right)^2}}$$

[9] RPMA channelizes (uniquely identifies) devices through random chip offsets (also known as "phase" offsets) in a single scrambling code rather than using separate scrambling codes for each users as done in CDMA/WCDMA.

The parameters in this equation are as follows:

- N_{TX} = The number of transmitted physical layer packets. This is related to the number of received packets, NRX through the packet error rate, i.e. $N_{rx} = N_{tx}*(1\text{-PER})$.
- G = The maximum processing gain = 8192.
- N_0 = The ambient noise floor at the AP which includes thermal noise and other out-of-system interference.
- μ_{SNR} = The target SNR for the power control loop. This is nominally set to 5.5 dB, however, the user can increase it to reduce the packet error rate.
- σ_{SNR} = The variance around target SNR after power control due to channel fading, estimation errors, and calibration errors.
- S_0 = The receiver sensitivity with no loading at the AP = -142 dBm.

Figure 6 illustrates the capacity as a function of the received bit-rate at the nominal 5.5 target SNR and various standard deviations.

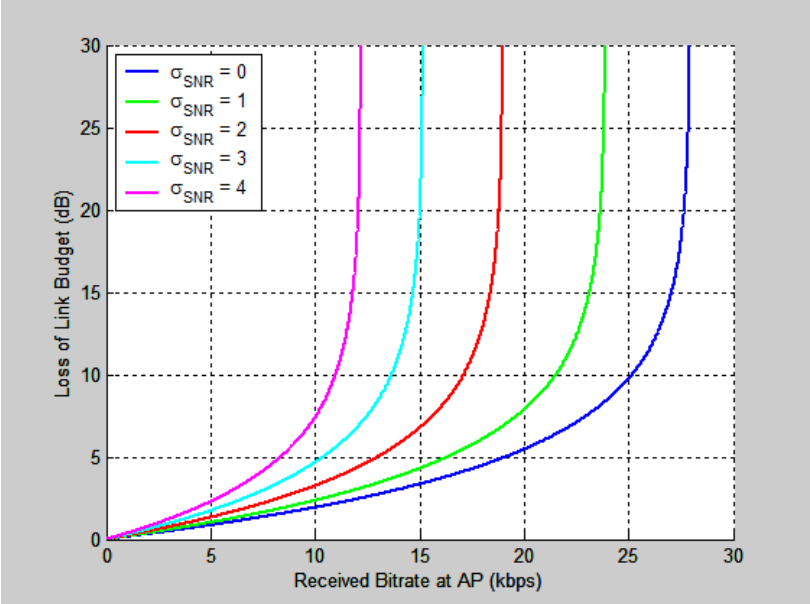

Figure 6. Uplink Capacity at AP

The plot in the figure above measures loss of link budget as a function of receive bitrate at the AP. The various curves illustrate the effect of power control variance around the target SNR.

The capacity of RPMA occurs where the loss of link budget curve asymptotes. At the nominal 5.5 dB target SNR, the capacity of RPMA is ~28 kbps with perfect power control ($\sigma = 0$). In deployed systems, with $\sigma = 2$, the capacity of RPMA is ~19 kbps.

Wireless systems should not be operated at full capacity in steady state. Traffic is unpredictable, and there must be slack capacity in the system to manage traffic fluctuations. For example, in electric metering, an outage event can set off a sudden flurry of alarm traffic that can temporarily congest the network. To manage this flurry, the wireless system should be deployed with adequate margin. Fortunately, the On-Ramp Total Reach Network's simple star topology

makes it easy to manage congestion due to unpredictable traffic. This allows the On-Ramp Total Reach Network to be operated with a smaller margin in steady-state, at about 60% capacity. In contrast, wireless mesh communication requires a large margin due to the inherent instability of the statistical random access methods used. It can only be safely operated in steady-state at approximately 20% capacity. Table 4 summarizes the capacity characteristics.

Table 4. Capacity Characteristics

Capacity Line Items	On-Ramp
Occupied Bandwidth (MHz)	1
Raw PHY (kbps)	120
Multi-Access Scheme	RPMA
Topology	Star
Maximum Capacity (kbps)	**19**
Margin for Robustness (%)	60%
Capacity at Operating point (kbps)	**11.4**

Table 5 describes various applications and the daily throughput and number of devices that can be served per AP at the recommended operating point.

Table 5. Endpoints Serviceable per AP for Different Target Applications

Application	Data Requirement	Endpoints Serviceable per AP
Smart Electric Meters	100 bytes/24x/day UL 24 bytes/day UL (Alarm) 24 bytes/day DL (Command)	20,000
Gas Meters	70 bytes/2x/day UL 24 bytes/day UL (Alarm 10%) 24 bytes/day DL (Command 10%)	300,000
Water Meters	96 bytes/day UL 24 bytes/day UL (Alarm 10%) 24 bytes/day DL (Command 10%)	450,000
Fault Circuit Indicators (FCI)	72 bytes/day UL 96 bytes/day UL (Alarm 10%)	550,000
FAA Light Monitoring	24 bytes/60x/day UL 24 bytes/day UL (Alarm 10%) 24 bytes/day DL (Command 10%)	21,500
Smart Transformers	50 bytes/120x/day UL 24 bytes/day DL (Command 10%)	7,000

5.2 Capacity vs. Link Budget

It is important to illustrate the relationship between link budget and capacity for On-Ramp Wireless and other competing technologies. Figure 7 and Figure 8 illustrate the capacity and link budget tradeoff space for On-Ramp Wireless and other systems. Link budget is also converted into coverage using the Okamura-Hata model for comparison. Figure 7 illustrates the FCC regulatory regime with 36 dBm EiRP. Figure 8 illustrates the ETSI regulatory regime with both 10

dBm and 27dBm EiRP shown. The On-Ramp Total Reach Network has the largest tradeoff space for both regulatory domains. Narrowband licensed radios have similar coverage with a fraction of the capacity. Meshed radios have limited coverage, which can be extended through meshing and limited capacity. The On-Ramp Total Reach Network is the only technology ***purpose-built*** with the coverage to reach thousands of endpoints and the capacity to serve them. It enables a network that has the lowest cost to serve each endpoint and enough capacity to support future applications.

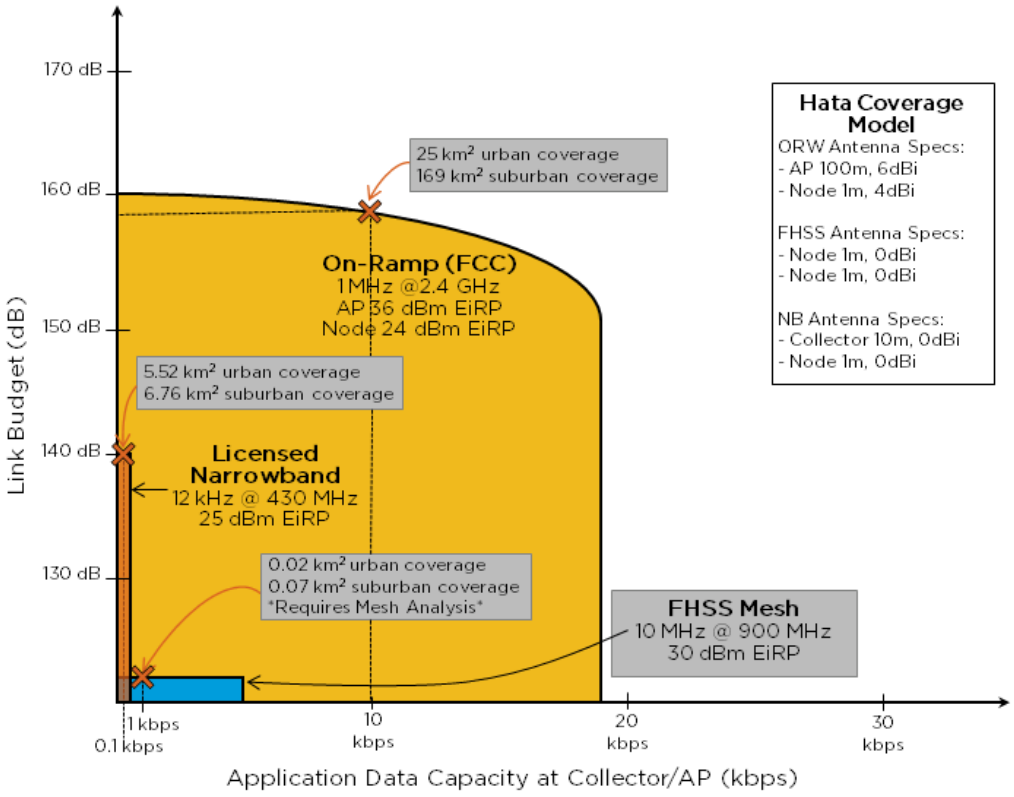

Figure 7. Capacity and Link Budget Tradeoff Space for On-Ramp Wireless and Competing Technologies for FCC Regime

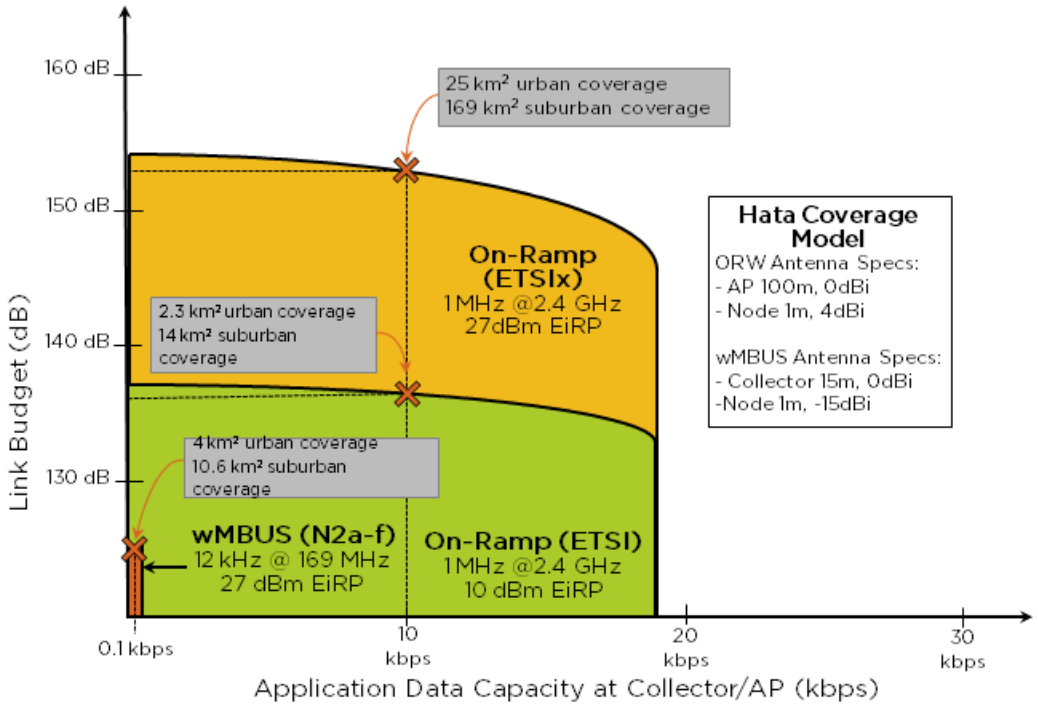

Figure 8. Capacity and Link Budget Tradeoff Space for On-Ramp Wireless and Competing Technologies for ETSI Regime

Note that ETSIx is an ETSI exemption where the max EiRP can be 27 dBm.

6 Coexistence

Radios, especially those operating in unlicensed spectrum, must address the issue of coexistence with other wireless technologies. Coexistence is a two-way street—a superior radio must:

- Be robust to interference from other radios, as transmitters are lightly regulated and the propagation environment is unpredictable and in constant flux.
- Be a good neighbor and not cause undue RF interference.

The On-Ramp Total Reach Network is ***purpose-built*** to provide superior performance for both of these coexistence requirements. In this chapter, both sides of the coexistence story are addressed in detail.

6.1 Robustness to Interference

On-Ramp Wireless' technology is designed to be extremely robust to interference. Unlike competing technologies, this robustness is built in at every protocol layer. As illustrated in Figure 9, interference mitigation techniques are built up like a layer cake starting with the PHY layer.

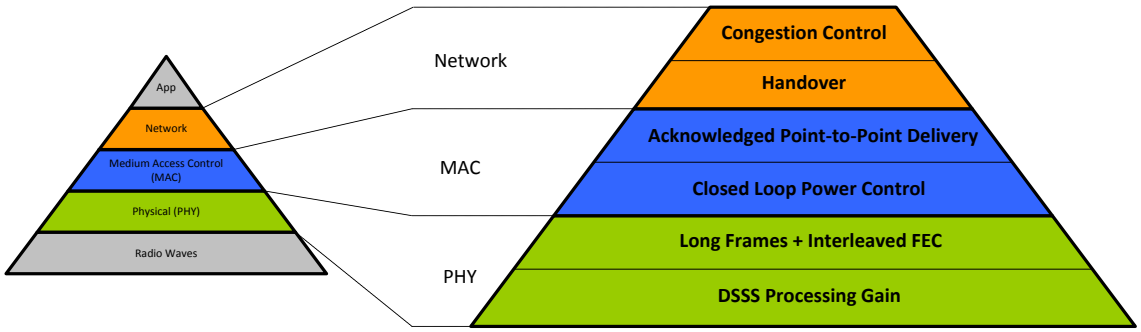

Figure 9. Interference Mitigation Techniques

The foundation of robustness is the high DSSS processing gain in the physical layer. This provides superior co-channel and adjacent channel rejection as summarized in Table 6. Rejection is quoted in dBc, which refers to the relative power of the interferer relative to the carrier or signal of interest. Note that the rejection is positive for the On-Ramp Wireless System because it can operate at a negative SNR. Competing technologies, like narrowband radios, must operate at a positive SNR with rejection characteristics less than -5 dBc.

Table 6. Interference Rejection Characteristics

Rejection Characteristic	On-Ramp Value
1MHz Interference Co-Channel Rejection	25 dBc
1 MHz Interference Adjacent Channel Rejection (@ 2 MHz)	73 dBc
1 MHz Interference Adjacent Channel Rejection (@10 MHz)	100 dBc

On top of the raw processing gain, the On-Ramp Wireless System has long frame durations coupled with an interleaved Forward Error Correction (FEC) code. This provides protection against burst interference that can be much stronger than the numbers quoted in Table 6. As an example, the On-Ramp Wireless System can demodulate in the presence of a limitlessly strong 250us, 50% duty cycle pulse jammer. In fact, such a jammer only causes 3dB of degradation in receiver sensitivity. Most other wireless technologies would be rendered useless in the presence of such a strong pulse jammer.

Above the PHY at the MAC layer, the On-Ramp Total Reach Network implements a closed-loop power control scheme that adapts to changing interference. This feedback loop controls the radio so that it only sends the minimum amount of power for the minimum time necessary to close the link. It ensures that data packets arrive with enough SNR to be demodulated under dynamic interference conditions, such as low interference at night shifting to high interference during business hours.

The MAC also implements an acknowledged point-to-point data transfer between the endpoint and the AP. This transfer protocol is purpose-built for use in extremely challenging interference conditions. It uses an advanced FEC scheme coupled with an Automatic Repeat Request (ARQ) mechanism to ensure reliable data delivery. It is designed to implement a reliable link even under packet error rates greater than 50%. The protocol makes the underlying wireless medium, with all its interference and channel variation, seem like a wire to the higher protocol layers.

At the higher layers, the On-Ramp Wireless endpoints can handover to another AP if their current connection goes down. This feature, coupled with overlapped AP deployment, makes the On-Ramp Total Reach Network extremely resilient in the case of excessive noise at a particular AP. In addition, the simple star topology of the On-Ramp Total Reach Network enables sophisticated congestion control in event floods and outage alarm floods, making the network the most reliable technology when it is needed the most. By contrast, in a mesh topology, congestion is more difficult to manage which significantly complicates event/alarm management and last gasp transmissions.

As an example of operation in an extremely noisy environment, Figure 10 illustrates the interference at the Mt. Woodson AP. The thermal noise floor in 1 MHz is 108.25 dBm. On average, the AP sees a 7 dB rise over thermal in 1 MHz. In addition, one of the interferers seems to be a co-located pulse jammer in the band of interest. Despite this challenging interference environment, the On-Ramp Total Reach Network provides robust operation as it reliably connects to endpoints over 10 miles away.

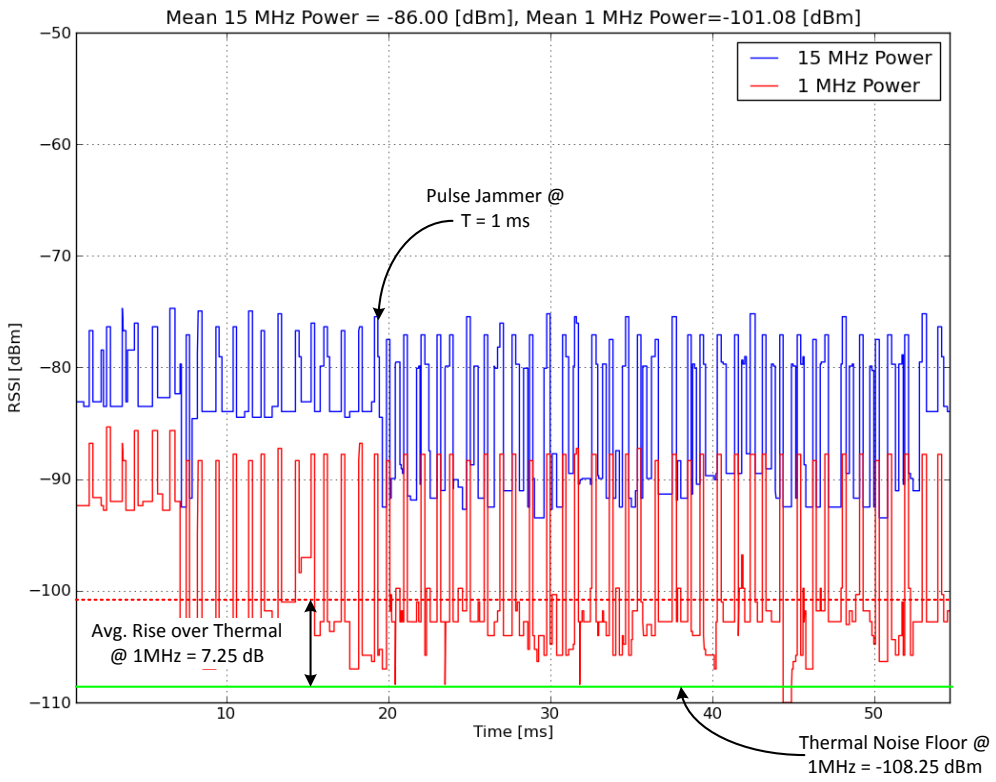

Figure 10. Interference at Mt. Woodson AP

The robustness of the On-Ramp Total Reach Network has numerous benefits:

- It enables On-Ramp Wireless to take advantage of elevated AP locations, such as those located on mountain top antenna farms, mobile operator RF towers, and tall buildings. This gives far better coverage. Less robust technologies cannot use these types of sites due to the interference they receive from co-located transmitters and the surrounding areas.
- It allows deployment in the unlicensed, but noisy, 2.4 GHz band. Licensed spectrum is expensive, and in many situations, it is much more cost effective to work in unlicensed spectrum. In addition, the 2.4 GHz band is globally available, so the same radio module can be used worldwide—lowering integration costs for vendors.
- It allows the network to operate as a single frequency network, which minimizes the spectral footprint of the On-Ramp Wireless System and enables multiple, non-coordinated networks to coexist in a given area.

6.2 Limited Source of Interference

In addition to being robust, the On-Ramp Total Reach Network is designed to have limited interference with other technologies. This is especially critical in the 2.4 GHz ISM band that the On-Ramp Total Reach Network shares with other technologies such as Wi-Fi, Bluetooth, garage door openers, and cordless phones.

In terms of coexistence, there are two potential sources of interference: the endpoint and the AP. The endpoint is a potential source of interference because it can be located near the home or office in close proximity to other ISM technologies, e.g., in a smart electric meter. By contrast, the AP is usually located in a protected area away from consumers. The AP signal is well below the thermal noise floor in homes, offices, and outdoor areas—so it is rarely a significant source of interference.

The endpoint is ***purpose-built*** to be a good neighbor by minimizing the ISM resources it consumes. It is designed to have a limited transmit duty cycle[10] of 5% when active. This limited active duty cycle spreads out data transfers in time, minimizing collisions with other ISM devices. Note that this duty cycle limitation refers to only the time when the endpoint is actively transmitting data. Given typical data models, the endpoint is asleep and not transmitting most of the day. In this discussion, we only focus on the period of time where the device is actively transmitting. We can quantify the ISM interference caused by a device using a metric called the ISM footprint defined as:

ISM Footprint = Active Duty Cycle x Bandwidth (BW)

This metric captures the potential for interference because, in order for a collision to occur, a device must share its transmission both in frequency and in time with another device. We can compare the On-Ramp Wireless devices with other ISM devices using this metric. For example, Bluetooth only has 1MHz bandwidth but has a high active duty cycle (around 50%)[11]. Thus, as illustrated in Figure 11, it has a rather large ISM footprint. Wi-Fi, on the other hand, has a smaller active duty cycle (between 10-20%) but consumes around 17MHz of BW. Illustrated in Figure 11 using an optimistic 10% duty cycle, Wi-Fi has an even larger ISM footprint than Bluetooth. On-Ramp Wireless has both a low active duty cycle (5%) and a low 1 MHz bandwidth. As illustrated in Figure 11, it has the smallest ISM footprint—10 times smaller than Bluetooth and 34 times smaller than Wi-Fi. With active duty cycle limiting, On-Ramp Wireless is more than compliant to the first FCC Part 15 rule, namely that "[An ISM] device may not cause harmful interference."

[10] Active duty cycle is defined as the ratio between the time of each average transmission divided by the average total time between the beginning of each transmission

[11] See section 2.2.3 of the Baseband Bluetooth Specification (v4) to see that the duty cycle of a Bluetooth device is roughly 50%.

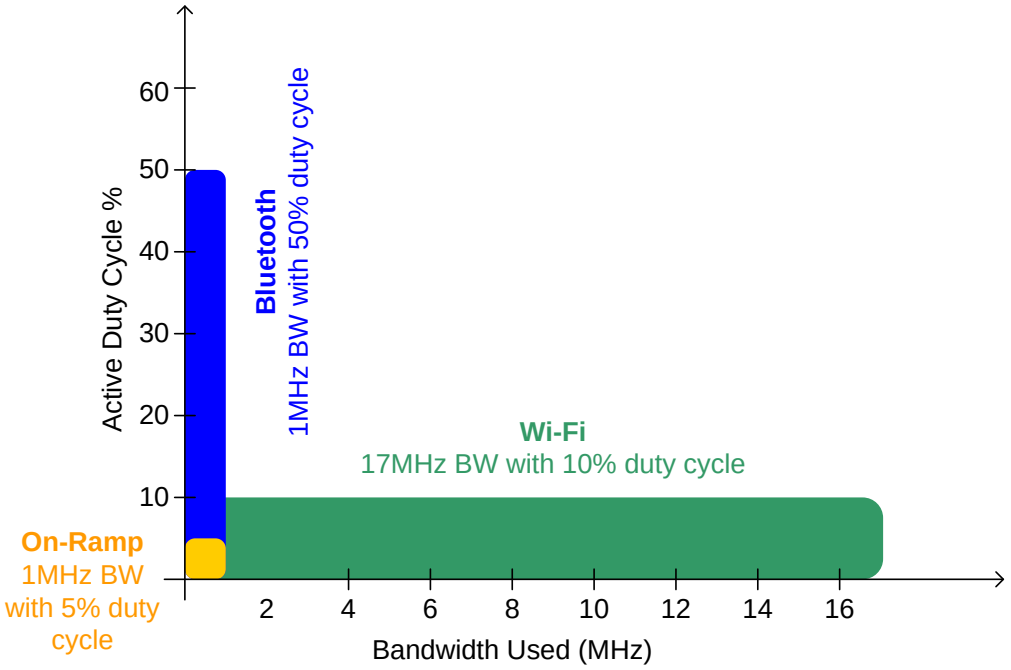

Figure 11. ISM Footprint of On-Ramp Wireless System Compared to Other ISM Technologies

Nevertheless, the On-Ramp Wireless System will add its footprint to the ISM band and occasionally cause collisions. FCC Part 15 has another rule which states that "[an ISM] device must accept any interference, including interference that may cause undesired operation." With such a small ISM footprint, interference is easily handled by other devices via their existing protocol (e.g., backoff and retry mechanisms, channel agility). To that end, On-Ramp Wireless has comprehensively tested the coexistence of its system and WiFi with a variety of applications, including file transfers, streaming video, and VOIP telephony. In the cases where the endpoint is close enough to cause disruption, the active duty cycle limiting makes the interference almost imperceptible to the application.

It should be noted that active duty cycle limiting does not impact the ability of an endpoint to get its daily data through. Even in an extreme case, with an application requiring 2kBytes per day, the endpoint is operates well below the 5% active duty cycle limit. In rare cases where minimum latency is imperative, like alarms, the endpoint is able to suspend its active duty cycle limit to get the data across quickly.

On-Ramp Wireless coexistence should be contrasted with competing technologies, such as wireless mesh. As Table 7 illustrates, wireless mesh technology has the potential to significantly pollute the band that it is in. There are already a number of anecdotes of consumer devices being disrupted by 2.4 GHz and 900 MHz mesh technologies.

Table 7. On-Ramp Wireless vs. Wireless Mesh Coexistence

Feature	Wireless Mesh	On-Ramp
Output Power	Up to 1W No power control	Up to 500mW Power control enabled
Duty Cycle	High duty cycle with each endpoint acting as a continuous relay for messages in the mesh topology.	Low with endpoints asleep most of the day in the star topology
Bandwidth	High bandwidth due to frequency hopping across the ISM band.	Low 1MHz bandwidth

7 Power Consumption

The On-Ramp Total Reach Network can be used to connect both continuously powered devices, such as electric meters and remote monitoring units, and battery powered devices, such as gas meters, water meters, and FCIs. The protocol is ***purpose-built*** to be extremely efficient for battery-powered devices, and On-Ramp Wireless has developed extremely efficient ASIC hardware for these applications. The key power-saving features include:

- The endpoint can be in a low power "deep sleep" mode most of the time. Depending on the data transmission requirements, it is awake for only a short period of time to receive and transmit data.
- The endpoint transmits at the minimum processing gain required to close the link, based on a locally calculated RSSI inferred from parameters received in the downlink portion of the frame cycle.
- The endpoint has a patented, low power network acquisition algorithm that saves power through maintaining synchronization to the On-Ramp Total Reach Network.
- The On-Ramp Total Reach Network has a simple star topology, as opposed to wireless mesh, so there is no requirement for endpoints to be awake to repeat traffic.

Low duty cycle applications, such as water meters, gas meters, and FCIs, can achieve a battery life of greater than 10 years. Table 8 lists the battery life estimate for three different applications based on battery capacity, daily payload, average receiver sensitivity, and battery life.

Table 8. Battery Life Estimates for Certain Target Applications

	Water Meter	Gas Meter	FCI
Battery Capacity	19 Ahr	19 Ahr	9 Ahr
Daily Payload	96 bytes	166 bytes	72 bytes
Average Receiver Sensitivity	-136 dBm	-136 dBm	-136 dBm
Battery Life[12]	22 years	19 years	10 years

By contrast, wireless mesh cannot serve battery-powered devices. Battery-powered devices in a mesh network must piggyback onto continuously powered mesh endpoints using a low power radio, such as ZigBee.

On-Ramp Wireless enables a single network that supports a host of devices, from grid-powered electric meters to battery-powered pressure transmitters or gas/water meters.

[12] Battery self-discharge rate is not accounted for in these estimates.

8 Security

Many of the target applications for device monitoring are critical infrastructure devices. Once the endpoint devices are connected, they will become the targets of hacking and cyber crime. These devices require a secure network, such as the On-Ramp Wireless System, that is built using proven security algorithms. The On-Ramp Total Reach Network uses NIST[13]-approved security algorithms that have greater than 20 years of life. This makes On-Ramp Total Reach Networks secure beyond 2030.

On-Ramp Wireless uses the following comprehensive approach to deliver this information security:

- **Prevention mechanisms:** Provide access control, mutual authentication, confidentiality, and high availability.
- **Detection mechanisms:** Identify attempts to break into the system and alert operators.
- **Recovery mechanisms:** Ensure the system degrades gracefully and continues to operate successfully even when under attack.

On-Ramp Wireless OTA security is ***purpose-built*** for use in a power-constrained, low-bandwidth wireless network with a simple star topology. Table 9 describes the key security guarantees.

Table 9. Security Guarantees

Security Attribute	Description
Mutual Entity Authentication	■ Registration ensures that only valid endpoints join a valid network
Message Authentication	■ AES128 based CMAC ■ Immune to replay attacks
Message Confidentiality	■ 168-bit 3DES encryption
Limited Anonymity	■ Communication link is anonymous after initial registration
Secure Endpoint Upgrade	■ OTA upgrade of deployed nodes and endpoints using only authenticated firmware

[13] National Institute of Standards and Technology. For more information, click http://www.nist.gov/index.html.

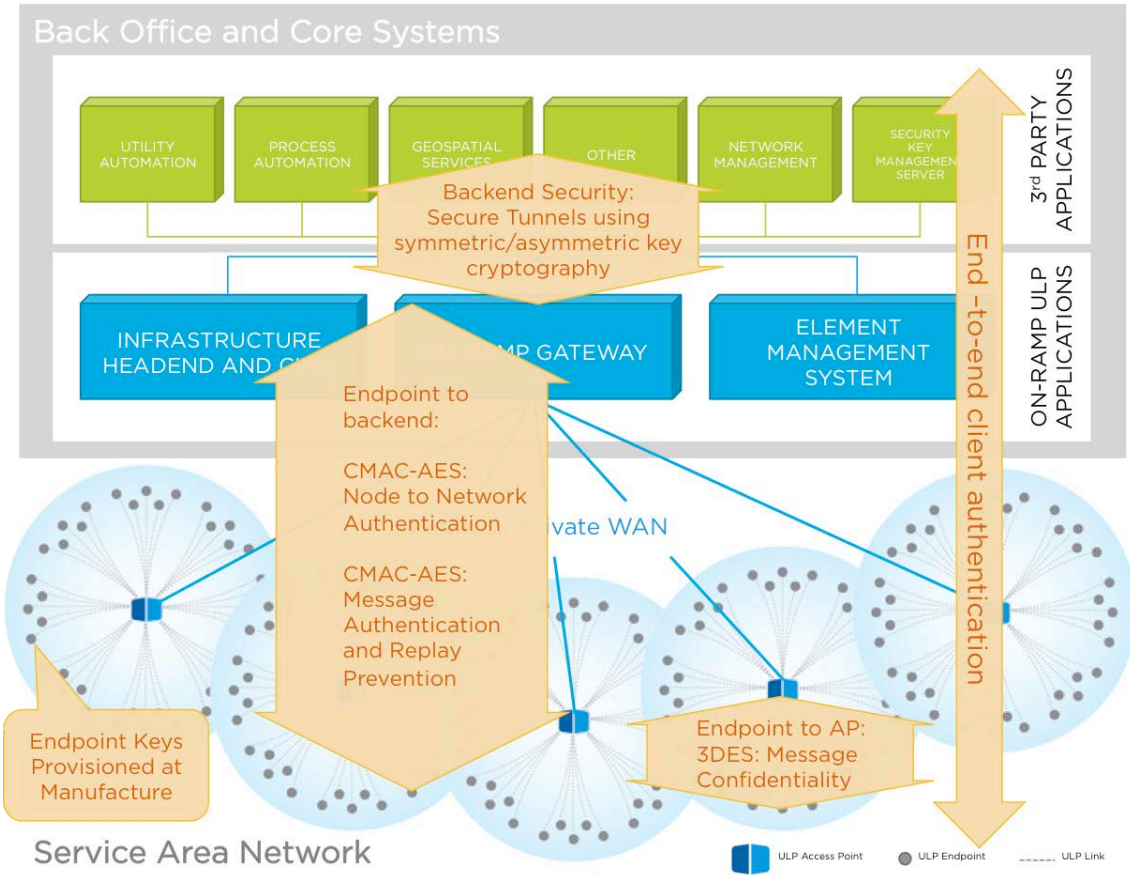

Figure 12. On-Ramp Total Reach Network Security Overview

Figure 12 illustrates the various security mechanisms in the network. Note that there is no OTA key exchange. Endpoints are securely provisioned with keys at the manufacturer. In addition, the network uses standards-based security throughout the network, AES and TDES OTA, and SSL and Diameter protocol in the core network. Furthermore, in case of a security breach, compromised keys are designed to have a limited effect. If node keys are breached, they can only corrupt the pair-wise communication between an AP to a single node. If network keys are breached, the worst-case scenario is a denial of service attack.

If a deployed endpoint requires a firmware update, over-the-air upgrade requires the endpoint to authenticate the firmware package and manage the update to either the Node or the endpoint device. This operation can be completed for the entire On-Ramp Total Reach Network in a matter of days, in contrast to weeks or months for competing technologies.

The robust security scheme passed rigorous third party security assessments and has been deployed on the SDG&E® electricity grid, a Tier 1 utility company with extremely stringent security standards.

9 Conclusion

In 2010, On-Ramp Wireless was selected as a World Economic Forum Technology Pioneer for 2011 for its development of the On-Ramp Total Reach Network and its promise to deliver a wireless system that will significantly reduce resource consumption around the world. Today, On-Ramp Wireless is delivering on this promise with an end-to-end system that breaks down barriers for wireless sensor networking.

The On-Ramp Total Reach Network is at the perfect intersection of the critical wireless performance metrics: coverage, capacity, power consumption, robustness, and security. The system can cover cities, states, and even countries at a fraction of the cost previously achievable. It provides coverage to locations previously unreachable by other technologies. On-Ramp Wireless makes existing wireless sensing applications much more cost effective and enables a new breed of applications. The ***purpose-built*** On-Ramp Total Reach Network is, by far, the most comprehensive, robust, secure, and cost-effective wireless sensor networking solution on the market today.

10 Bibliography

1. **Schumpeter.** The Internet of Hype. *The Economist.* December 10, 2010.

2. **Sage Associated Environmental Consultants.** Assessment of Radiofrequency Microwave Radiation Emissions from Smart Meters. [Online] 2011. http://sagereports.com/smart-meter-rf/.

Appendix A Abbreviations and Terms

Abbreviation/Term	Description
AP	Access Point. The On-Ramp Total Reach Network component geographically deployed over a territory.
ARQ	Automatic Repeat Request
CDMA	Code Division Multiple Access
DMS	Device Management System
DSSS	Direct-Sequence Spread Spectrum
EiRP	Effective isotropic Radiated Power
ETSI	European Telecommunications Standards Institute
FEC	Forward Error Correction
FCC	Federal Communications Commission
FCI	Fault Circuit Indicator
FHSS	Frequency-Hopping Spread Spectrum
GPIOs	General Purpose Input Outputs
GW	Gateway. The network appliance that provides a single entry point into the back office for the network. A gateway talks upstream to the NMS and CIMA. It talks downstream to multiple APs.
IEEE	Institute of Electrical and Electronics Engineers
LECIM	Low Energy Critical Infrastructure Monitoring
MAC	Medium Access Control
M2M	Machine-To-Machine
NIST	National Institute of Standards and Technology
OTA	Over-The-Air
PHY	Physical
RMU	Remote Monitoring Unit. The end device that monitors Federal Aviation Administration (FAA) obstruction lights.
RPMA	Random Phase Multiple Access
RSSI	Received Signal Strength Indicator
SNR	Signal-to-Noise Ratio
SSL	Secure Sockets Layer