Wi-Fi Enabled Sensors for Internet of Things: A Practical Approach

Serbulent Tozlu, Murat Senel, Wei Mao, and Abtin Keshavarzian, Robert Bosch LLC

ABSTRACT

The vision of Internet of Things calls for connectivity not only to consumer electronics and home appliances, but also to small battery powered devices which cannot be recharged. Such small devices, often various types of sensors and actuators, are required to sustain reliable operation for years on batteries even in the presence of heavy interference. The IEEE 802.11 standard has established itself as one of the most popular wireless technologies offering connectivity. Using commercially available chips, we demonstrate the feasibility of low-power Wi-Fi technology to enable IP connectivity of battery powered devices. Three typical sensor application scenarios are investigated. We evaluate the power consumption of Wi-Fi enabled devices for each of the scenarios, investigate the impact of interference, and measure the range performance.

INTRODUCTION

The term "Internet of Things" (IoT) refers to the possibility of connecting sensors, actuators or any device to the Internet. It can lead to a significant change in our daily lives in the way we live and interact with the devices such as home appliances, smart meters, security sensors, HVAC systems, etc. Various companies are exploring this domain as it can potentially open up new business opportunities.

Since proprietary solutions are difficult to interface and manage as the network scale grows, standardized technologies are preferred over proprietary protocols. IP (Internet Protocol) is a good candidate as the most appropriate layer to achieve this coherence. Its advantage was recognized by industrial organizations such as IPSO (Internet Protocol for Smart Objects) Alliance, which promotes IP-integration to sensors for Internet connectivity. This approach enables a wide range of applications in the areas of home and building automation, factory monitoring, smart cities, transportation, smart grid and energy management [1]. IEEE 802.15.4 with 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) adaptation layer and low-power Wi-Fi are two candidates to make IoT a reality:

- 6LoWPAN was developed to cater IP for the specific needs of wireless sensors
- Companies in Wi-Fi domain are working on decreasing power consumption of Wi-Fi transceivers to enable years of battery lifetime.

Traditionally ZigBee and other IEEE 802.15.4 based protocols have been considered for sensor network applications due to their energy-efficient design. However, recently developed power-efficient Wi-Fi components, with appropriate system design and usage model, have become a strong candidate in this domain [2]. Low-power Wi-Fi promises multiple years of battery lifetime while providing easy integration to existing infrastructure with built-in IP-network compatibility. Reuse of existing Wi-Fi infrastructure offers key cost savings and faster deployments. Widely deployed IEEE 802.11 networks reduce the infrastructure cost to a minimum while improving the total cost of ownership. Wi-Fi devices have the advantage of native IP-network compatibility, which is a big plus for IoT. Well-defined and universally accepted IP connectivity overcomes the expensive gateway requirements of proprietary protocols. Furthermore economy of scale is another important advantage of Wi-Fi with an expected 22 percent annual growth rate between 2010 and 2015 [3]. Finally, the availability of network management tools and knowledge base is strong benefit of IEEE 802.11, and IT personnel are already familiar with managing Wi-Fi networks.

Our study targets Internet connectivity of devices at home. Different types of Wi-Fi enabled devices can be found in residential buildings (Fig. 1):

- **AC-powered Devices (home appliances, PCs):** Power consumption for wireless communication is not critical.
- **Rechargeable Devices (laptops, smartphones):** They can run at most a few days with rechargeable batteries.
- **Battery-Powered Devices (sensors like smoke detectors, motion detectors, etc.):** Simple, low-power devices that need to run multiple years with standard batteries.

In this article, we investigate the feasibility of

0163-6804/12/$25.00 © 2012 IEEE

Wi-Fi for battery-powered, low-power sensors. In particular, we focus on the performance with respect to power consumption, reliability, and range. The rest of the article is organized as follows: we present the system model of a typical Wi-Fi enabled sensor network. Our findings on power consumption, interference/reliability, and communication range are presented. Finally, we conclude the article.

System Model

Figure 1 shows a typical Wi-Fi enabled sensor network setup. Network consists of multiple Wi-Fi enabled sensors/actuators that are associated with an Access Point (AP) through which the nodes may be connected to Internet. We consider a set of basic operations that cover most sensor applications.

Initialization/Association: After the sensor is powered up, it authenticates and associates itself with a predetermined AP and acquires an IP address.

Keep-alive Messages: Depending on the implementation, an AP may remove a device from its associated client list if it does not hear from the device for a certain interval. To maintain its association, the device needs to communicate with the AP periodically.

Periodic Data Transmission: A very common use-case where the device reads sensor data periodically and transmits the data to a control unit.

Event-triggered Data Transmission: The sensor device monitors the environment and if certain events are detected, a message is generated and transmitted.

Command Messages: Another common use-case is transmission of messages to the sensor or actuator device. Examples of this can be a query, configuration or command/action messages to an actuator device.

Sensor nodes are typically battery-powered and are expected to function for multiple years without changing the batteries. Hence, energy-efficiency and long battery lifetime are the main requirements. Furthermore, reliability, security, communication range, and latency are critical for different wireless sensor applications. In this article we address the viability of Wi-Fi technology for sensor network applications with respect to these requirements.

In order to compare the energy requirements and power consumption of various systems, we define three application scenarios (Table 1).

Figure 2 illustrates the operations of a sensor device to enable different scenarios. For all scenarios we assume that the initialization/association is performed once every day (Ti =1 day). Scenario I represents a simple sensor device (e.g., a temperature sensor or a thermostat in heating system) which periodically sends data at 5 minute intervals (Ts = 5 min). In order for the device to remain connected to the AP, it also sends keep-alive messages every minute (Ta = 1 min). Scenario II represents a monitoring sensor device (e.g., a smoke detector) which sends event-triggered data and periodic keep-alive messages every minute (Ta = 1 min) to stay connected. Event-triggered messages can occur anytime and they need to be delivered reliably and quickly. Event-triggered messages occur rarely. However, in order to understand their impact on battery lifetime, we consider a high rate of one event per hour. Scenario III combines all use-cases representing a device which sends both periodic data every minute (Ts = 1 min) and event-triggered messages, and checks for incoming messages from AP every 10s (Tc = 10s). This scenario represents an application where we can have configurable sensors and actuators (e.g., a fire alarm system with both smoke detectors and alarm sirens).

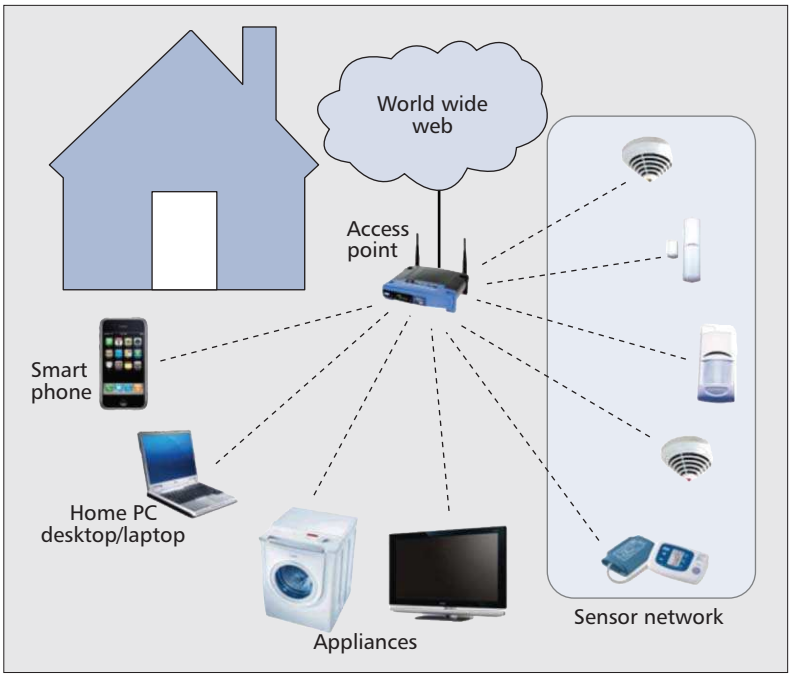


Figure 1. *Connected devices at home.*

Scenarios/Phases	Scenario I	Scenario II	Scenario III
Init./Association (1/Ti)	1/day	1/day	1/day
Keep-alive Msgs (1/Ta)	1/min	1/min	—
Periodic Data Tx (1/Ts)	1/(5 mins)	—	1/min
Event-triggered Msgs	—	1/hr	1/hr
Command Messages	—	—	delay ≤ 10s

Table 1. *Battery lifetime scenarios.*

ZigBee (IEEE802.15.4) based solution can typically achieve years of battery lifetime for scenarios defined above. In next section, we demonstrate how a low-power WiFi based solution can achieve similar performance.

Power Consumption

In this section, we study different aspects of power consumption for Wi-Fi enabled sensors along with experimental evaluation.

During the wake-up process, the low-power Wi-Fi sensor node initializes the hardware and operating system, stabilizes the regulators and loads the program from flash. The program loading step makes the application size an important factor for wake-up time and energy.

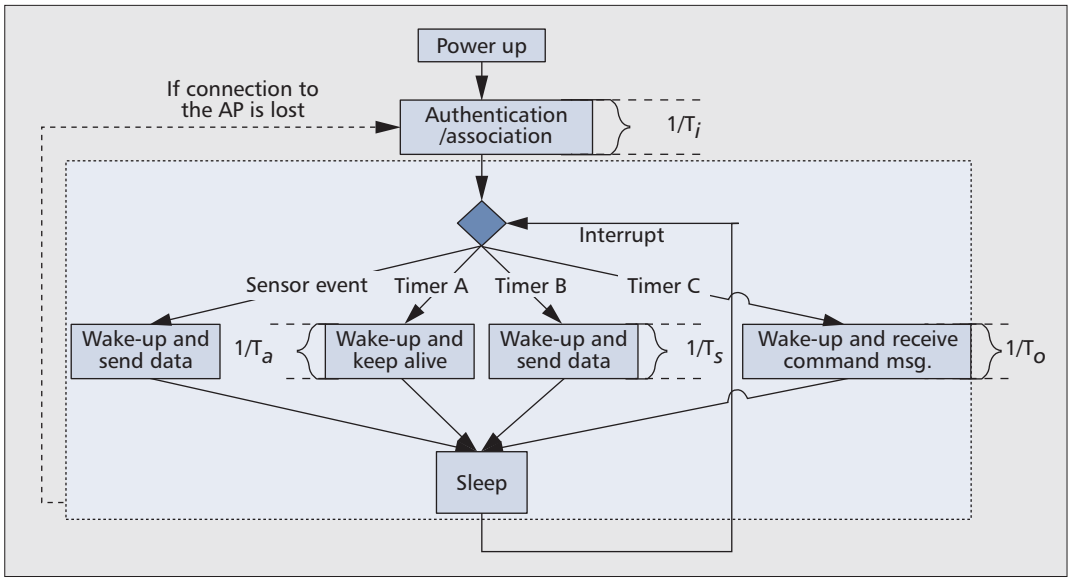


Figure 2. *Typical sensor operation.*

IEEE 802.11 Power Save (PS) Mode

IEEE 802.11 standard defines a power saving (PS) mechanism that allows mobile stations to enter a power saving state where they turn off both the transmitter and the receiver to save power.

In PS mode, APs buffer messages for the power saving mobile stations and indicate in the periodic beacon that there are messages buffered for the mobile station. The mobile station wakes up periodically according to the listen interval to receive the beacon message. The listen interval is an integer multiple of the beacon interval. If no message is waiting, the mobile station goes back to sleep until the next wakeup. If there is any buffered message and the message is a broadcast or multicast message, the AP will send the message immediately after the beacon and mobile station simply stays awake and receives it. If the buffered message is a unicast message, the mobile station needs to send a PS-Poll message and receive the buffered message accordingly.

Power Consumption Considerations

In this segment, we briefly cover the key aspects of power consumption for Wi-Fi sensors.

Low-power Wi-Fi Module — The capabilities of low-power Wi-Fi chip/module will be the main determining factor on the battery lifetime performance of Wi-Fi sensors. We selected G2M5477 [4], an off-the-shelf low-power Wi-Fi module from G2 Microsystems, for power consumption evaluation. This module is equipped with a 32-bit CPU, real-time clock, hardware encryption engine, sensor interface and a full 802.11b/g PHY and MAC. It includes eCos real-time operating system and lwIP TCP/IP stack. The chip's architecture enables low-power operation through its power management system, which turns off the components that are not needed and controls transitions across different power states.

New low-power Wi-Fi modules have been introduced in the market that support IEEE 802.11n [5]. However, the higher data rate advantage of 802.11n comes with moderately less power efficiency and higher cost due to its relatively complex circuitry. 802.11b/g was determined to be a better option for our sensing application scenarios depicted in Table 1 that do not require high data rates.

Sleep Current and Wake-up Energy — Sleep current and wake-up energy play a major role in the overall battery lifetime of any duty cycled system. Wi-Fi sensors are expected to stay in sleep state for most of the time and certain events will cause transition to active state. For regular Wi-Fi chips, the typical sleep current is around 150 to 250 μA while a single wake-up process lasts hundreds of milliseconds and costs several millijoules of energy. Low-power Wi-Fi systems reduce the sleep current along with wake-up time and energy. We measured the sleep state current for G2M5477 as 4μA [6].

During the wake-up process, the low-power Wi-Fi sensor node initializes the hardware and operating system, stabilizes the regulators and loads the program from flash. The program loading step makes the application size an important factor for wake-up time and energy. G2M5477 allows using multi-image applications, where boot code can select from a number of executables stored in flash based on specific wake-up reason. Multi-image implementation reduces the wake-up time and energy significantly. To exploit this feature, we implemented one executable for each of the operations defined earlier: Initialization, Keep-alive, Periodic-Data, Sensor-Event and Command-Messages. Our measurements show that increasing application size by 1KB costs 200μs of time and 12μJ of energy [7]. Using a program with 25KB application code size, we measured the wake-up time and energy around 9ms and 400μJ, respectively.

Transmit and Receive Energy — Compared to IEEE 802.15.4 with 250kb/s maximum data rate, IEEE 802.11b/g operates at much higher data rates ranging from 1Mb/s to 54Mb/s. This

allows Wi-Fi enabled sensors to spend very little time with actual transmission or reception. Operating at higher data rates also yields less power consumption since the higher the date rate is, the lower the receive/transmit energy per bit becomes. Hence, the impact of transmit and receive energy on battery lifetime becomes a secondary factor unless the Wi-Fi enabled sensor sends or receives large amounts of data.

MAC Retransmissions — Some sensing applications require high-level reliability for certain message types such as alarms. IEEE 802.11 uses simple acknowledgements to ensure reliable transmission between two stations. Unacknowledged frames are retransmitted up to a predetermined number of retries before getting discarded. The successful or failed transmissions are reported to upper layer protocols. Wi-Fi enabled sensors are expected to experience different MAC retransmission rates due to collisions or other interference sources in the environment. Our experimental evaluations show that the impact of MAC retransmissions on power consumption becomes especially significant for low data rate operation.

Security — Wireless sensors handle sensitive information in various application domains, which makes effective security mechanisms an important requirement. Due to inherent memory and computation limitations of sensor networks, security poses several challenges. IP-enabled sensors bring additional challenges on providing end-to-end security. 802.11 provides several standard security schemes that accommodate data confidentiality, authentication and availability.

Investigating the impact of commonly used Wi-Fi security schemes like WEP, WPA/TKIP-PSK and WPA2/AES-PSK on power consumption, we noticed that there exists a tradeoff between the strength of the security mechanism and energy usage. The vulnerable WEP introduces negligible authentication and encryption overhead. On the other hand, both WPA and WPA2 evoke considerable authentication time and energy usage overhead due to several message exchanges during handshake process. Thus, re-association/re-authentication should be avoided after each wake-up to have better latency and battery lifetime performance. Conversely, encryption has a minor impact on energy consumption, which can be attributed to the hardware encryption engine on the Wi-Fi module. Our measurements show that WPA2/AES-PSK gives the best tradeoff between security and performance for Wi-Fi enabled sensors [8]. The power consumption overhead of upper layer security protocols (IPSec, TLS) that will provide end-to-end security is not considered within the scope of this article.

Performance Evaluation

Based on the application scenarios defined in Table 1, we performed several experiments to understand the energy consumption characteristics of Wi-Fi enabled sensors. Figure 3 compares daily Wi-Fi sensor energy usage for these scenarios when different data rate and packet size combinations are applied. The contributions of each operation to daily energy consumption are shown in percentages.

Initialization/Association — The Initialization/Association phase is common to all scenarios. Normally, initialization/association should be a one-time only procedure during network setup but for daily energy consumption calculations we assume that this process occurs once a day to cover the possibility of losing connection to AP for any reason. Initialization phase duration and energy consumption vary based on the security scheme applied and whether DHCP or static IP address assignment is used. Using WPA2/AES-PSK with static IP assignment, we measured duration of initialization process around 3s and energy consumption as 280mJ. Initialization/Association operation is an energy consuming process but if frequent associations/authentications are avoided; its impact on overall battery lifetime will be limited.

Keep-alive Messages — Keep-alive messages are needed to maintain the communication with AP and avoid expensive initialization/association process if Wi-Fi sensors don't need to transmit or receive for an extended amount of time. There is no defined standard time for disassociation of inactive clients from an AP and it is implementation dependent. We used one minute keep-alive messages in our scenarios. Keep-alive messages are not needed if Wi-Fi sensor already communicates with AP frequently enough such that it is not disassociated as in Scenario III. For the first two scenarios, we used null function (no data) MAC frames as keep-alive messages to be energy efficient. At 1 Mb/s, we measured the duration and energy usage of keep-alive message event from wake-up to going back to sleep after sending the frame as 10.72ms and 809mJ respectively. With its associated wake-up energy cost every minute, we observe that keep-alive messages contribute to daily energy consumption of Scenarios I and II considerably. However, even for scenario II, keep-alive messages are still more energy efficient than going through the initialization/association phase once per hour.

Periodic Data Transmission — Most common sensing applications require sensor nodes to wake up periodically, read sensor data, transmit data packet and go back to sleep. For example, a room temperature sensor may send its measured value to a thermostat every five minutes. The defining factors of power consumption for this operation will be the frequency of wake-ups along with packet size and data rate. Periodic data transmission consumes proportionally less energy for Scenario I because of five minute periodicity but the energy consumption increases for Scenario III where transmission frequency is smaller (Fig. 3).

We performed several measurements to better understand the effect of data rate and packet size on energy consumption employing UDP as the transport layer protocol. By comparing Fig. 3a with Fig. 3e or Fig. 3b with Fig. 3f, we clearly observe the advantage of operating at higher

Most common sensing applications require sensor nodes to wake up periodically, read sensor data, transmit data packet and go back to sleep. For example, a room temperature sensor may send its measured value to a thermostat every five minutes.

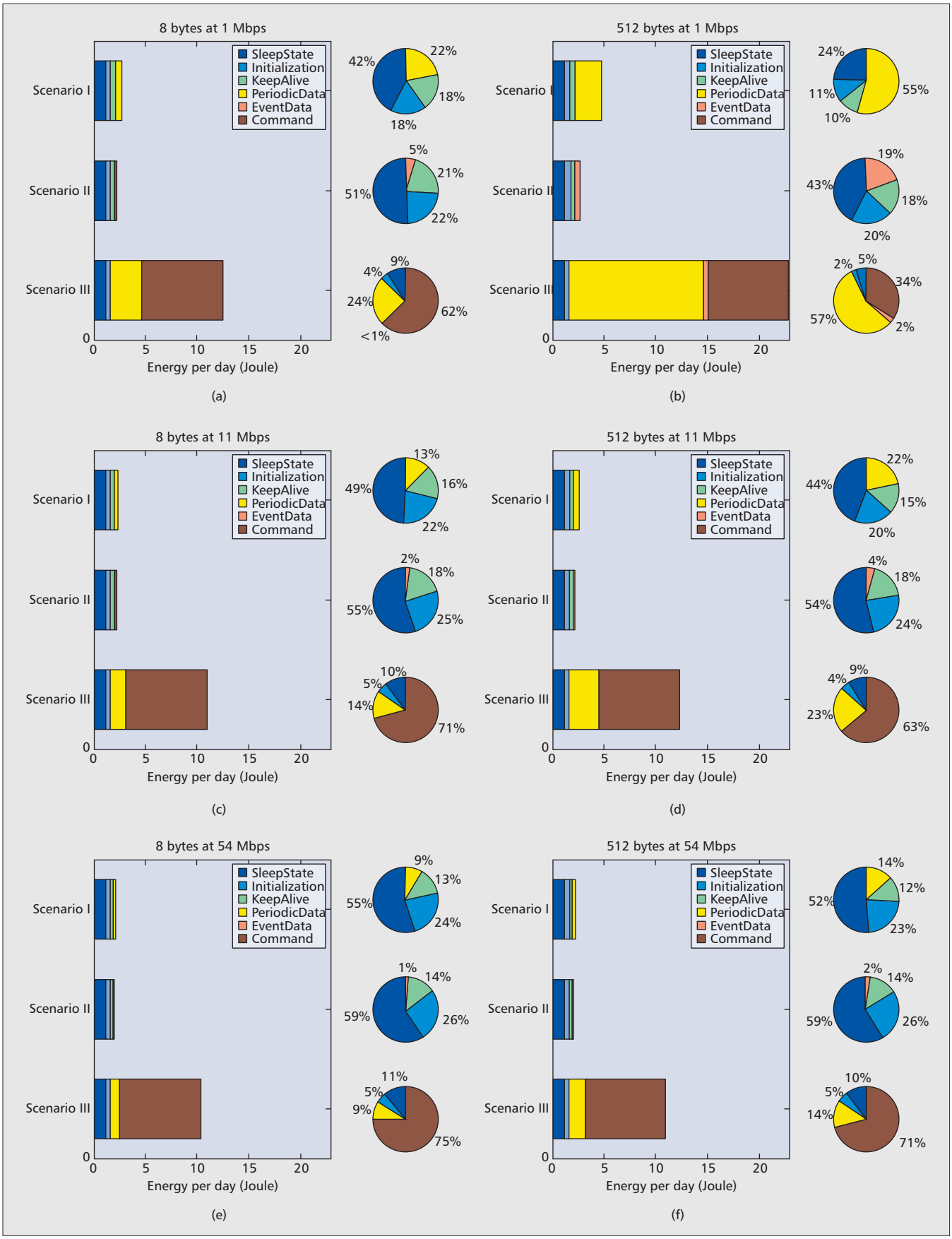


Figure 3. *Daily energy consumption of different operations for three application scenarios using four data-rate/packet-size combinations (calculations are based on: Pre-Known SSID, Static IP assignment, WPA2/AES-PSK security scheme, MAC retransmission rate of 100%): a) 8Bytes application data at 1Mbps; b) 512Bytes application data at 1 Mb/s; c) 8Bytes application data at 11 Mbps; d) 512Bytes application data at 11 Mb/s: e) 8Bytes application data at 54Mbps; f) 512Bytes application data at 54 Mb/s*

data rates. For Scenarios I and III, percentages of daily energy consumption for transmitting periodic data decrease substantially by just increasing the data rate from 1Mb/s to 54Mb/s. Packet size has a marginal impact on battery lifetime while operating at higher data rates but the impact becomes substantial for lower data rates. Daily energy consumption for periodic data transmission increases from 22 percent (Fig. 3a) to 55 percent (Fig. 3b) for Scenario I just by increasing the packet size from 8B to 512B. For the same scenario at 54Mb/s, percentage of periodic data energy consumption increases slightly from 9 percent (Fig. 3e) to 14 percent (Fig. 3f).

Therefore, transmitting or receiving smaller packet sizes at higher data rates results in optimum power consumption [7]. Most sensor devices require sending few bits of information. However, an IP/Web-capable Wi-Fi sensor will require handling larger packet sizes due to additional protocol overhead [9].

Event-triggered Messages — Event-triggered messages are expected to be sent infrequently but they are generally latency critical messages with high reliability requirements. For example, a smoke detector generates a fire alarm message, or a motion detector reports a movement upon detection. To enable fast delivery of these messages, it is important that the Wi-Fi enabled device remains associated with the AP so that it does not need to go through the time consuming initialization/association process again. In terms of energy consumption, it is quite similar to periodic data send but additional retransmissions are required to ensure reliability. We selected UDP over TCP as the transport layer protocol for event triggered messages due to latency requirements. Reliability requirement is addressed by the application via redundant retransmissions. Event-triggered messages don't have much of an impact on daily energy consumption because of their seldom occurrences (Scenarios II and III).

Command Messages — Command messages are relatively infrequent compared to keep-alive messages and periodic data. However, receiving the command messages in a timely fashion is one of the most energy demanding task for the sensor nodes. Depending on the required response time, the sensor nodes need to wake up periodically to check if there is any command message waiting for them. Using aforementioned PS mechanism with 10 seconds beacon listening interval, the sensor node would consume 7 to 8 Joules per day for command message reception under Scenario III (Fig. 3).

To give an idea of the typical battery lifetime under Scenario III, Fig. 3c translates to a reasonable battery lifetime of five and a half years with two AA batteries with 2000mAh available capacity, of which 71 percent, 14 percent, 10 percent and 5 percent of battery power is spent on command messages, periodic data, sleep state, and initialization, respectively. In comparison, sensor node under Scenario I and II without command message reception would have much longer battery lifetime.

Interference and Reliability

It is envisioned that most IoT-related applications will operate in the globally available 2.4GHz-band. Due to the fact that a variety of technologies, e.g., IEEE 802.11, IEEE 802.15.4, Bluetooth and microwave devices operate in this band, interference can potentially be a problem for sensor applications.

It should be noted that sensor applications are inherently different than high throughput applications in terms of underlying traffic patterns. Hence the impact of interference to sensor applications needs to be investigated in this context. Furthermore, the investigated performance metrics will also be different. Rather than throughput we considered packet success rate (PSR) and round-trip-time (RTT) as performance metrics to measure impact of interference on reliability and real-time capability of Wi-Fi enabled sensors.

In this context, we investigate the impact of different wireless technologies (IEEE 802.15.4, Bluetooth microwave devices, as well as legacy Wi-Fi devices) on Wi-Fi enabled sensors and can conclude that none of these technologies have significant impact on latency and reliability of Wi-Fi enabled sensors. Due to space considerations, in this article we present only the effect of heavy traffic from legacy Wi-Fi devices on sensor network traffic.

Considered Scenarios

In our set-up, we have three Wi-Fi enabled sensors, which send test packets of 128, 512, and 1024 Bytes every 50ms to a server via an AP and receive an echo back. We want to record packets from all sensors nodes, so we limit the number of sensor nodes in our system to three. However, in order to compensate for the limited number of sensors, our sensor nodes send packets a lot more frequent than standard sensor network applications. (In Table 1, the highest frequency of data-transmission is 1/min, which is significantly less frequent than 1/50ms.)

During the benchmark phase of the experiments, we do not include extra Wi-Fi interferers into the system, but background Wi-Fi traffic in our office environment was always present. In the benchmark cases, we have observed almost 100 percent PSR and the 95 percent-tile RTT is around 15ms. These values are within the desired sensor networking requirements. However, more interesting results can be observed if we push the system to the limits. Hence we consider two scenarios:

- **Out-of-Network Interference:** Wi-Fi enabled sensors and legacy Wi-Fi interferers are in the same channel but they are associated to different APs.
- **In-Network Interference:** Wi-Fi enabled sensors and legacy Wi-Fi interferers are associated to the same AP.

In both cases, there is always background traffic in an office environment. On top of the background traffic, we intend to find out the impact of heavy traffic conditions on Wi-Fi enabled sensors. Hence legacy Wi-Fi devices send packets of 64, 512, and 1024 Bytes every 1ms. In the next segment, we focus on the results

Event-triggered messages are expected to be sent infrequently but they are generally latency critical messages with high reliability requirements. For example, a smoke detector generates a fire alarm message, or a motion detector reports a movement upon detection.

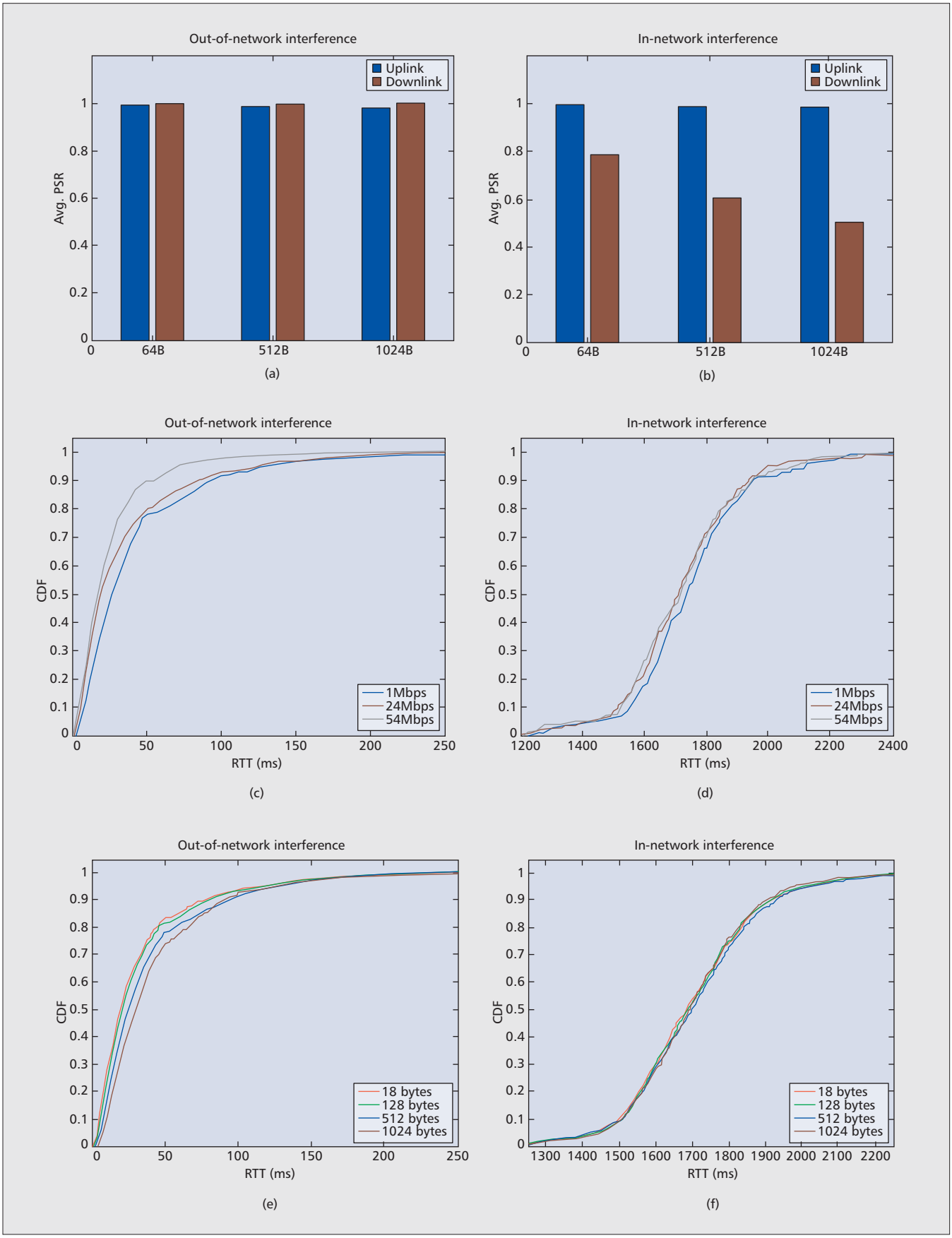


Figure 4. *Impact of heavy legacy Wi-Fi traffic on Wi-Fi enabled sensor applications: a) packet size of out-of-network interferers = 64, 512, 1024B; b) packet size of in-network interferers = 64, 512, 1024B; c) data-rate of the sensor node = 1, 24, 54 Mb/s; d) sensor's data packets of 18, 128, 512, and 1024B; e) data-rate of the sensor node = 1, 24, 54 Mb/s; f) sensor's data packets of 18, 128, 512, and 1024B.*

of these two cases with additional Wi-Fi traffic in the background.

Experimental Results

Figure 4 summarizes the measurement results for one of the sensor nodes. Our results on the average PSR of the sensor node in the presence of background Wi-Fi traffic and heavy interference from legacy Wi-Fi devices with different packet sizes (64, 512, and 1024B) are presented in Fig. 4a and Fig. 4b. The cumulative distribution function (CDF) of the RTT of sensor packets are plotted in Fig. 4c–f: In Fig. 4c and Fig. 4d, the results are plotted for all packet-sizes for different data-rates of the sensor node, i.e.; each plot includes data from all packet sizes at that data-rate. In Fig. 4e and Fig. 4f, the results are plotted for all data-rates for different packet sizes of the sensor node, i.e.; each plot includes data from all data-rates at that packet size.

Our first observation is that the sensor network performs significantly better for the out-of-network scenario. In this scenario, the PSR is around 100 percent for both uplink and downlink communication (Fig. 4a). However, we can also observe that RTT is significantly higher (in Fig. 4c and Fig. 4e) than our benchmark case, where 95 percent-tile RTT was around 15ms. Due to the fact that PSR is almost 100 percent, we can conclude that due to MAC-layer retransmissions packets are not lost but RTT has increased significantly. In this scenario, we did not observe any significant impact of the packet size of the interferer (Fig. 4a). As expected, the higher data-rates of the sensors decrease the RTT slightly (Fig. 4c), and the packet size of the sensors seem to have limited effect on the performance (Fig. 4e).

More interesting results can be observed for the in-network scenario (Fig. 4b, Fig. 4d, and Fig. 4f). Although the uplink channel to the AP is perfect in terms of PSR, the downlink channel experiences significant losses (Fig. 4b). Furthermore, RTT increases significantly. Due to the difference between uplink and downlink channel we conclude that the AP becomes the bottleneck in this case. To verify this claim, we have conducted OPNET simulations to replicate the scenarios and observed that the transfer buffer of the AP fills up quickly and starts dropping packets. These results are also in-line with the observation that according to Fig. 4a in the downlink channel, PSR decreases with bigger packets (64B vs. 1024B) of the interference: AP could simply send out smaller packets faster.

We can conclude that in the "Out-of-Network Interference" scenario, the results show the impact of pure interference from our interfering Wi-Fi devices and background traffic without the limiting impact of the buffer space of the AP. On the other hand, the "In-Network Interference" scenario also shows the effect of the limited buffer space of the AP on top of the Wi-Fi interference. Furthermore it should be noted that we pushed the interference traffic to the limit. In a typical residential or office setting we do not expect to observe such high RTT values. This expectation was verified in our benchmark scenario, when we test the system under typical network traffic without heavy interference.

Range

Communication range is determined by multiple factors, namely, the output power of transmitter, antenna gain, path loss between sender and receiver, and receiver sensitivity. Among these factors, output power is limited by regulatory requirements and transmitter's capability. Most Wi-Fi transceivers (including G2M5477) operate at an output power close to 100mW (20dBm) which is the regulatory limit in Europe. Path loss is heavily dependent on the physical environment. Receiver sensitivity is defined as the minimum threshold required for received signal power for a successful packet reception and it depends on transceiver's capability, signal bandwidth and data rate. This dependence creates a design tradeoff option between the data rate and communication range: The receiver is more sensitive when operating at lower data rates which results in longer communication range and more coverage area.

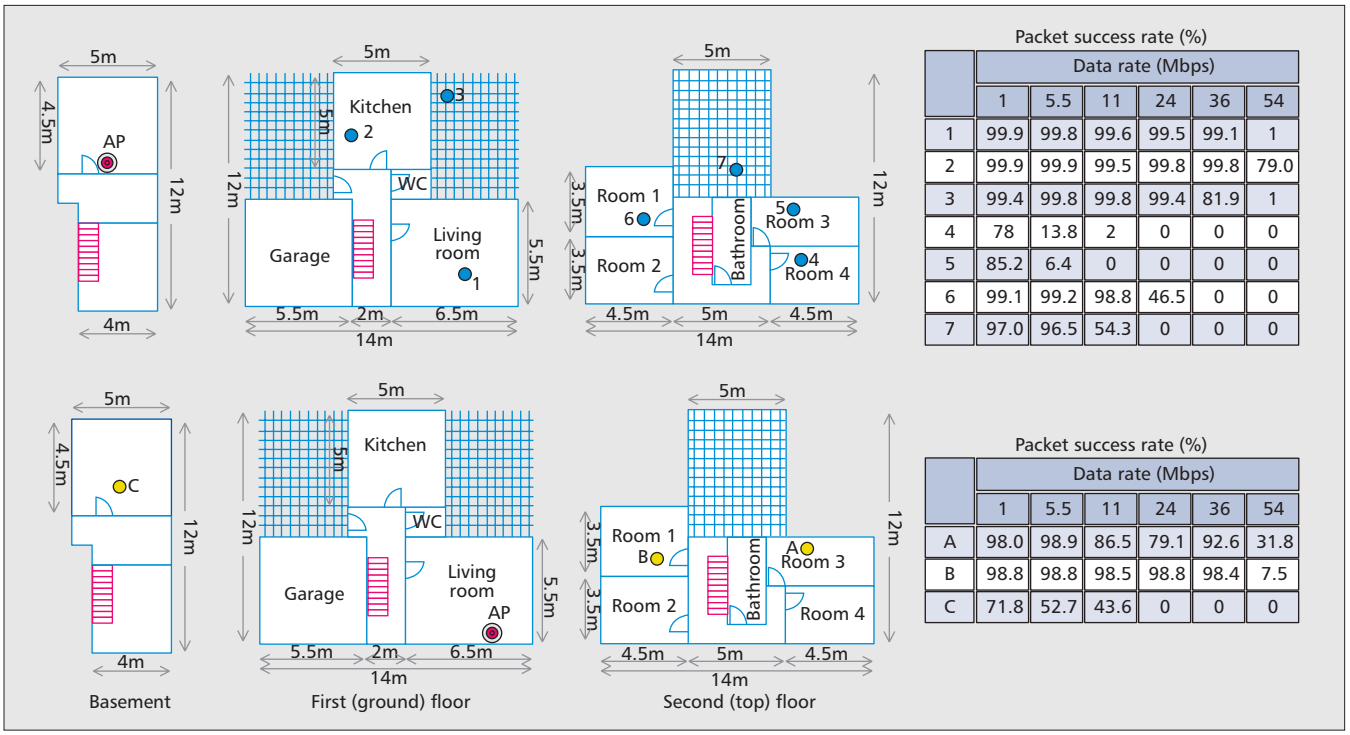
Range Requirements

Coverage requirements for wireless sensor network applications depend on where the network is deployed. For commercial/office environments, typically a backbone network consisting of multiple routers and APs provide wireless Internet access throughout the building. For residential environments, typically, a single AP covers the entire home. Furthermore, location of the AP may not be centrally positioned in the building because it is dictated by the location of the broadband modem. For Internet access, it is important that the AP is placed in an optimal location such that it can provide a good coverage at higher data rates enabling higher throughput in common living areas of the building. However, Wi-Fi enabled sensors may be deployed in all corners of the building from basement to roof. But due to low traffic load generated by sensor devices, operation at higher data rates is not required which in turn helps improve the coverage area. If an extended coverage area is needed, a repeater AP can be used.

Measurement Results

To check if a single AP can provide coverage for a typical house, we performed measurements at a newly built and fully furnished typical European house consisting of a basement, ground floor and a first floor. The house is a concrete building with mesh grid heating systems installed on each floor which significantly block RF signal. For the first set-up, we placed the AP in the basement and measured the Wi-Fi signal quality (PSR, signal power) at different locations in/around the house covering all the possible locations that a sensor device may be installed. For the second set-up, we placed the AP in center of the house in the living room area. Figure 5 shows the floor plan and measurement locations for these setups. On right side, the measured PSR values are shown for different locations at different data rates. With the AP in the living area, we observed that we had good coverage at 36–54Mb/s at most locations in the house including the entire ground floor and top floor but not so good coverage in the basement. Good cover-

For commercial/office environments, typically a backbone network consisting of multiple routers and APs provide wireless Internet access throughout the building. For residential environments, typically, a single AP covers the entire home.



Packet success rate (%)

	Data rate (Mbps)					
	1	5.5	11	24	36	54
1	99.9	99.8	99.6	99.5	99.1	1
2	99.9	99.9	99.5	99.8	99.8	79.0
3	99.4	99.8	99.8	99.4	81.9	1
4	78	13.8	2	0	0	0
5	85.2	6.4	0	0	0	0
6	99.1	99.2	98.8	46.5	0	0
7	97.0	96.5	54.3	0	0	0

Packet success rate (%)

	Data rate (Mbps)					
	1	5.5	11	24	36	54
A	98.0	98.9	86.5	79.1	92.6	31.8
B	98.8	98.8	98.5	98.8	98.4	7.5
C	71.8	52.7	43.6	0	0	0

Figure 5. *Range measurement scenarios with corresponding PSR results: AP in basement (top) and AP in living-room (bottom).*

age in basement could be achieved at 1–11Mb/s. With AP in basement, we get high data rate coverage for ground floor, but we could communicate with certain location in top floor only at 1Mb/s. Our measurements confirmed that even when AP is not installed in an optimum location, we can operate at lower data rates in almost all points that a sensor device may be installed within the house.

Conclusion

In this article, the feasibility of low-power Wi-Fi to enable IP connectivity of battery-powered devices is studied with three key practical areas of concern: Power consumption, impact of interference, and communication range.

At high data rates, transmitting/receiving data and packet size have small impact on power consumption. On the other hand, at low data rates the impact of transmit/receive energy and packet size becomes noticeable. Retransmissions can have an impact on energy consumption and the impact is more pronounced for low data rate operation. As far as security is concerned, WPA2 gives the best tradeoff in terms of security and battery lifetime overhead.

Our study shows that battery lifetime of a Wi-Fi enabled sensor depends heavily on the operating scenario. In particular, whether or not it is required to receive timely command messages plays an important role in overall energy consumption, since such operation requires frequent wakeups. Other operations like initialization/association, periodic data transmission, event triggered messages, and keep-alive messages for connection maintenance have smaller impact on overall power consumption, especially when high data rates are used. Generally, multiple years of battery lifetime is achievable for most real-world scenarios.

Under normal circumstances, in-network and out-of-network interference do not affect reliable communication of sensor devices. To identify potential bottleneck to reliable and low-latency communication, we have examined the network performance under extreme conditions. Only under heavy in-network traffic, the AP becomes a bottleneck and affects the latency and reliability considerably.

The communication range is directly related to the link data rate. As expected, lower data rate results in longer communication range and wider coverage area. Our experimental results show that in a typical residential building, a single AP operating at 1Mb/s, even if not installed in an optimal location, can provide full coverage for all potential sensor locations. However, it is favorable to operate at higher data rates to achieve lower power consumption. Hence, selection of data rate creates a tradeoff between communication range and battery lifetime. Thus, it is recommended to operate at highest data rate at which the device is within communication range of AP.

References

[1] A. Dunkels and J.-P. Vasseur, "IP for Smart Objects," IPSO White Paper, Sept. 2008.
[2] K. West, K. Hall, and G. West, "Wireless Sensor Network Technology Trends Report," West Technology Research Solutions, LLC, Tech. Rep., Dec. 2008.
[3] "Wireless Connectivity Market Data," ABI Research, Jan. 2011.
[4] "G2M5477 Preliminary Datasheet," G2 Microsystems, May 2009, available: www.g2microsystems.com.
[5] "GS1500M Product Brief — Preliminary," GainSpan Corporation, Apr. 2012, available: http://www.gainspan.com/products/GS1500M_modules.php.

[6] S. Tozlu, "Feasibility of Wi-Fi Enabled Sensors for Internet of Things," *Int'l. Wireless Commun. and Mobile Computing Conf. (IWCMC 2011)*, Istanbul, Turkey, July 2011.
[7] S. Tozlu and M. Senel, "Battery Lifetime Performance of Wi-Fi Enabled Sensors," *Consumer Communications & Networking Conf., 2nd IEEE Int'l. Wksp. Densely Connected Networks*, Jan. 2012.
[8] S. Tozlu, "Experimental Study of Security Impact on Battery Lifetime for Low-Power Wi-Fi Systems," *Wireless Congress*, Munich, Germany, Nov 2010.
[9] B. Ostermaier, M. Kovatsch, and S. Santini, "Connecting Things to the Web using Programmable Low-Power WiFi Modules," *Int'l. Wksp. Web of Things (WoT 2011)*, San Francisco, CA, USA, June 2011.

Biographies

Serbulent Tozlu (serbulent.tozlu@turktelekom.com.tr) received his B.Sc. degree in Electronics Engineering from Istanbul University in 1997 and his M.Sc. degree from Department of Electrical Engineering at University of Southern California in 2000. He then joined Bosch Research & Technology Center in Palo Alto, CA as a Research Engineer, where he worked on various topics including embedded systems, in-car networking, PIR/uW based intrusion detection systems, low-power wireless protocols and Internet of Things. As of February 2012, he is with Turk Telekom responsible for Wi-Fi services.

Murat Senel received his Ph.D. degree in Electrical and Computer Eng. at Purdue University, West Lafayette, IN in 2008 and his B.Sc. degrees in Electrical Eng. and Industrial Eng. (double-major) at Bogazici University, Turkey in 2002. In 2008, he joined Bosch Research & Technology Center and works as R&D Project Manager on wireless M2M applications. His research interests are in the area of low-power wireless communication, in particular he is interested in connecting wireless sensor networks to the Internet.

Wei Mao received the B.A. degree in physics, and the M.S. and Ph.D. degrees in electrical engineering from the University of California at Berkeley in 1998, 2001, and 2005, respectively. From 2005 to 2008, she was with ArrayComm LLC, San Jose, CA, where she designed various MIMO algorithms for PHS, HSDPA, and WiMAX systems. She is currently working as a Senior Research Engineer at Research and Technology Center, Robert Bosch LLC, Palo Alto, CA. Her current research interests include indoor localization, sensor fusion algorithms, low-power wireless technologies, and visible light communications.

Abtin Keshavarzian received the B.Sc. and M.Sc. degrees in Electrical Engineering from Sharif University of Technology in Tehran, Iran in 1999 and 2001 respectively, and the Ph.D. degree in Electrical Engineering from Stanford University, Stanford, CA in Jan 2005. Since 2005 he has been with Bosch Research and Technology Center, Robert Bosch LLC, Palo Alto, CA working on wireless technologies with focus on low-power wireless solutions for sensor networks. He is currently working as a Senior Research Project Manager, and his research interests are low-power wireless IP-enabled systems for smart objects.