Two-Way Communication Protocol using Bluetooth Low Energy Advertisement Frames

Giorgio Corbellini
Disney Research Zurich
Switzerland
giorgio
@disneyresearch.com

Stefan Schmid
Disney Research & ETH
Zurich, Switzerland
stefan.schmid
@disneyresearch.com

Stefan Mangold
Disney Research Zurich
Switzerland
stefan.mangold
@disneyresearch.com

ABSTRACT

Bluetooth Low Energy (BLE) is a wireless personal area network technology designed to provide low-power connectivity to smartphones and wearable devices. To transmit bidirectional data, devices must first discover each other and then start a pairing process. Usually, the pairing process requires manual intervention that might result in undesirable user experiences. If security and privacy requirements allow, communication sessions could be limited to the advertisement channels only, without pairing the devices. Further, the use of only advertisement channels without pairing devices enables scenarios in which different radio systems can also join the communication. For example, the nRF24L01+ radio system can be programmed to communicate using the advertisement channels defined by BLE. This is relevant because the nRF24L01+ radio system is a popular technology for the Internet- of-Things and for location-based services with wearable devices in smart cities. This paper evaluates a two-way communication protocol between the nRF24L01+ and BLE devices, using only advertisement frames. We show a practical protocol implementation and use an experimental testbed to evaluate its performance. The evaluation shows that it is possible to build a simple and reliable communication protocol that works in both directions.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Wireless Communication*

Keywords

Bluetooth Low Energy; Advertisement Channels; nRF24.

SmartObjects'15, September 07-11 2015, Paris, France

ACM 978-1-4503-3535-5/15/09 ...$15.00.
DOI: http://dx.doi.org/10.1145/2797044.2797049.

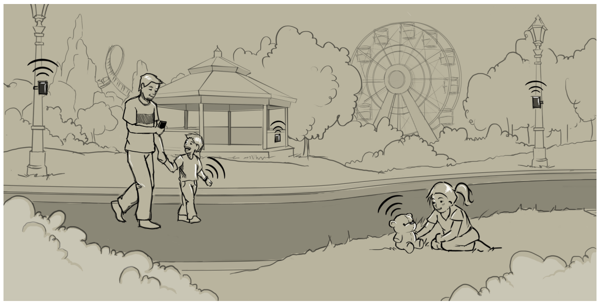

Figure 1: Concept art (© Disney): Wearable devices that are used in controlled environments such as entertainment theme parks enrich the story telling and experience design.

1. INTRODUCTION

The nRF24LE1 radio System on a Chip (SoC) enables low-complexity and low-power transmission for wireless networking of consumer devices such as computer peripherals or embedded systems for wearable electronics. The SoC (identified as nRF24 in this paper) belongs to the chip series nRF24 and operates in the 2.4GHz Industrial, Scientific and Medical (ISM) band. Its basic physical layer is known for its efficiency and often used in the context of the Internet-of- Things (IoT) [7], [9] in low-complex and resource- constraint applications. Its main application is low-latency and low- throughput communication in consumer electronics. For example, wearable devices, step counters, wireless keyboards and other computer accessories, or toys, can benefit from the connectivity provided by the nRF24 [13]. Another popular usage scenario is related to wearable devices (bracelets) that are used in entertainment theme parks to enable personalized location-based services [1]. Theme parks are controlled environments comparable in size and complexity to a city, and can serve as model environments [4].

Another popular short- range radio technology is Bluetooth Low Energy (BLE) [12], [5], also known as Bluetooth Smart. BLE is available in many smart- and feature phones. BLE devices must be paired to communicate among each other. Usually, the pairing process is needed only the first time that two devices communicate.

1.1 Motivation

Because of the popularity of BLE and the nRF24 for the IoT, it is interesting to enable interworking between them. To interoperate with each other, the two technologies need a communication protocol that manages the coordination of medium access and maintains reliable and spectrum efficient data exchange. BLE uses frequency hopping and the nRF24 does not, thus, to provide a reliable communication channel, the proposed protocol is based on opportunistic communication windows and relies on frame retransmissions, acknowledgments, and timeout patterns.

There are various other possible use cases for such a communication protocol: The interworking enabled by the proposed communication protocol can be used to manage spectrum coexistence between nomadic BLE devices and nRF24-based IoT systems.

1.2 Contribution

An nRF24LE1 chip can be programmed to transmit and receive data in a way that can be decoded and processed by BLE devices. The required frame format of the nRF24-to-BLE communication are known from [6] and adopted here. This paper describes the complete two-way communication protocol, which is designed by extending the existing frame formats. The communication in both directions is based on BLE advertisement frames.

The contributions of this paper are: (1) A protocol to establish reliable communication between nRF24 and BLE devices by using advertisement frames and (2) an experimental testbed validation to evaluate the efficiency of the proposed communication.

2. RELATED WORK & STATE OF ART

BLE and the basic communication protocol used by the nRF24 family chips are both largely adopted technologies [2,5,8,9,12,13]. BLE is supported by most operating systems for mobile and wearable devices, mainly because of its low power consumption [11] when small amounts of data are transmitted.

BLE is a low-power extension for Bluetooth. Similar to Bluetooth, BLE operates in the 2.4 GHz ISM radio band. It uses Gaussian Frequency Shift Keying (GFSK) as modulation and coding scheme and achieves a maximum data rate of 1 Mb/s. BLE operates on 40 channels spaced 2 MHz apart, with center frequencies ranging from 2402 MHz to 2480 MHz. Channels are organized as three advertisement channels and 37 data channels. BLE uses frequency hopping to avoid interference and to coexist with other devices operating in the ISM band. The three advertisement channels are indexed as 37, 38 and 39 and indicated in Figure 2.

The acronym nRF24LE1 refers to a commercially available low-power SoC [9]. The product is today often considered for IoT use cases with a variety of applications of low-power short-range communication and was recently used in a large roll-out of wearable devices in a theme park [1]. The nRF24LE1 board includes a 2.4 GHz transceiver (model nRF24L01+), an 8051 compatible Micro Controller Unit, and a 16 kB embedded flash memory. The nRF24L01+ offers data rates of 250 kb/s, 1 Mb/s, and 2 Mb/s; just like BLE, nRF24L01+ uses the GFSK modulation. The nRF24 operates at 2.4 GHz with 80 orthogonal frequency channels.

BLE and nRF24 are different technologies used in scenarios with similar requirements. Therefore, there might be hybrid scenarios that require full interoperation. An existing multi-protocol radio chip addresses the problem of bridging the two radio technologies [10]. Nevertheless, there are scenarios in which it is interesting to be able to achieve multi-protocol communication using only software updates. In fact, avoiding hardware modifications allows hardware reuse that is favorable in scenarios with large amount of devices already rolled-out.

3. PROTOCOL DESIGN

With the nRF24 and BLE, it is not possible to pair two devices following the standard BLE pairing process. It is however possible to transmit data using the advertisement channels that are normally used by BLE peripherals to advertise their services.

Without pairing, transceivers are not coordinated on what advertisement channel use to communicate or when to start a transmission. Furthermore, BLE devices such as smartphones dynamically tune the radio front- end so that BLE hops among the three advertisement channels in such a way that is unknown to the nRF24 device. As result, without a reliable protocol, a receiver might miss data frames.

The proposed protocol uses acknowledged unicast traffic, as opposed to unacknowledged broadcast (advertisement) traffic. Every frame carries a header with three fields, each one byte long, and the payload (16 bytes because of a nRF24 limitation [6]). The first and the second fields represent the destination and the source address. The third field holds the frame sequence number. The destination allows directed communications using the advertisement frames, which are broadcast messages. The source address indicates to the receiver where to send the subsequent acknowledgment frame. The sequence number is used to sort received frames, to recognize missing frames, and to enable multicast transmissions.

The communication system and the protocol described in this paper are designed to support an application layer that transmits sporadic and short sequences of data frames.

All devices duty cycle the use of the radio: When a device has no messages to deliver it spends most of the time in sleep mode and periodically wakes up to listen to all the three advertisement channels for incoming discovery frames. The radio duty cycle approach follows the preamble sampling principle used in wireless sensor networks protocols such as X-MAC where preamble messages (in this case, the discovery frames) are repeated for a duration of at least equal to the sleep period of every other device [3].

3.1 Topologies

Two communication topologies (or, scenarios) are considered: (1) Peer-to-peer (P2P), in which a pair of de-

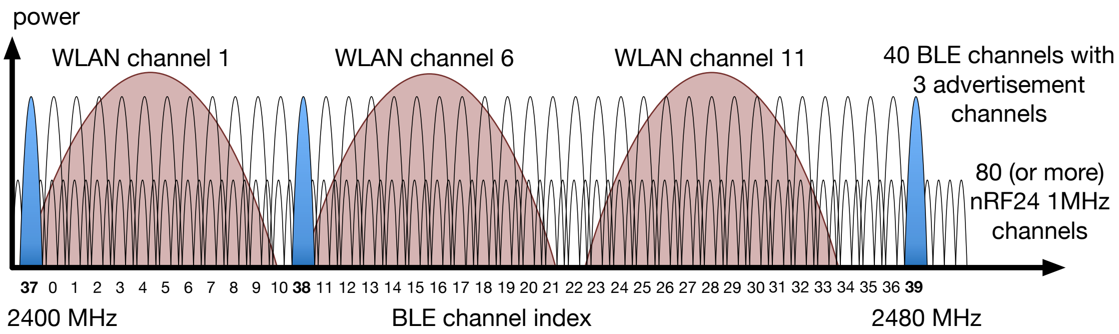

Figure 2: BLE channels with highlighted BLE advertisement channels together with Wi-Fi channels and the eighty channels of the nRF24 system.

vices exchanges data directly and (2) one-to-many, where one device delivers frames to a number of devices in its vicinity. In P2P scenarios with uncoordinated devices, the transmitter discovers the receiver by sending preambles on all advertisement channels. Upon reception of a valid preamble frame, the receiver sends an acknowledgment (ACK) and the communication can start.

In one-to-many scenarios, the transmitter always broadcasts the same number of preamble frames (the number is known by all devices). After the transmission of the last preamble, the data frame is transmitted. Every receiver that intercepts one of the preambles sends an ACK and remains awake until the reception of the data frame.

3.2 Discovery, Data, ACK Frames

There are three different kinds of frames: discovery, data, and ACK frames described as follows.

The discovery frame contains the protocol header and does not carry any payload. The destination address field is set to `0xFF`, which is the broadcast address. The source address field contains the sender address and the sequence number is set to zero. Upon reception of a discovery frame, a device sends an ACK. To mitigate ACK collisions, each device waits a random time before responding transmitting. The approach of random start of ACK transmissions is taken from short range RFID, like (slotted) ALOHA. Upon collection of multiple ACKs, the transmitter of the discovery frame knows the identity of its neighbors. Since ACKs can still collide, the initial sender of discovery frames might need several transmission rounds before collecting the IDs of all neighbors.

Data frames can be unicast or multicast frames, thus, both source and destination address must be set accordingly. The sequence number starts at zero and is increased by one with every new frame. Upon reception of a unicast data frame, if the destination address matches the internal address, an ACK that echoes the sequence number is sent back. Else, if the data frame is a multicast frame, no ACK is sent. If the original transmitter of the unicast data frame receives a valid ACK frame (same sequence number, matching source address), it can proceed to the next data frame. If no ACK is received within a timeout, the data frame will be retransmitted. The maximum number of retransmissions is a configuration parameter.

Like a discovery frame, an ACK frame contains only the protocol header. The source address of the ACK frame is set to the sender address and the destination field is set to the source address of the received frame (that can be a discovery or a data frame). The sequence number is echoed in case of data frames.

4. EVALUATION

The performance of the proposed two-way communication protocol is evaluated with the help of the testbed implementation shown in Figure 3.

4.1 Testbed Description

The nRF24LE1 SoC is plugged into an nRFGo evaluation board for chips of the nRF24L- Series. The BLE device is an iPhone 5s that is set to alternate between central coordinator and peripheral role. A central coordinator periodically listens to the advertisement channels whereas a peripheral device uses the advertisement channels to transmit connection requests. Tuning the BLE radio front-end to a specific advertisement channel is not supported.

All measurements are performed inside an electromagnetic shielded box to avoid external interference. Figure 3 shows the evaluation setup. All measurements focus on the data transmission part of the protocol and they always involve one transmitter and one receiver. We show measurements of the P2P scenario to show the effects of having one device, the iPhone, which automatically hops among the three advertisement channels and the other device, the nRF24, whose radio front-end can be manually tuned. If the transmitter requests an ACK, the ACK timeout immediately starts after the end of the frame's transmission. The ACK timeout is set to 30 ms, a value large enough to compensate both hardware and software constraints.

Since nRF24 and BLE devices can initiate a discovery process or a data transmission, there are two different communication directions (1) from nRF24 to BLE device (hopping) and (2) from BLE device to nRF24.

The key performance criteria used to evaluate the protocol approach are the frame delivery ratio, which expresses the fraction of correctly received frames, and

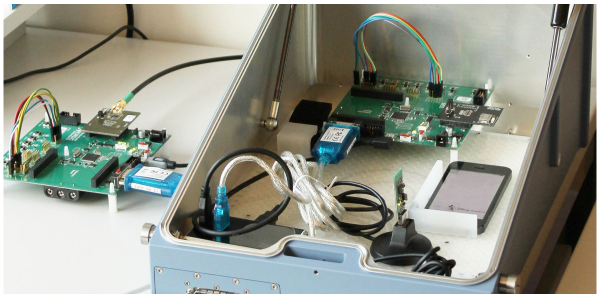

Figure 3: Setup used for the measurements.

the achievable throughput in bit per second (b/s), which shows the data rate that the communication link is able to provide.

Every measurement is repeated 5 times and all figures show the average results with the corresponding confidence intervals at 95 % confidence level.

4.2 ACK Timeout

When the nRF24 is the transmitter, the ACK timeout duration only depends on the radio front-end turnaround time of the iPhone that we measured to around 11 ms.

When the iPhone is the transmitter, every frame is sent to all the three advertisement channels because the BLE device does not know which channel the nRF24 chip is tuned to. The nRF24 chip needs some time to transmit the ACK on the same channel used for reception. For these reasons, the ACK timeout is set to 30 ms in both devices.

The ACK timeout should also take into account the fact that when the ACK is sent by the nRF24 the BLE device might be already tuned to another advertisement frequency and miss the ACK. This fact opens several design choices such as introducing some randomness between two consecutive frames (the approach followed in this paper) or repeating the ACK multiple times.

One protocol choice might be to have the nRF24 chip repeating the ACK multiple times. However, since the advertisement channel hopping sequence is not defined in the BLE standard and not published by Apple, we discarded this option. Instead, to limit the effect of missing ACKs because of channel hopping, the sender introduces some randomness between two consecutive frames.

4.3 nRF24 to BLE

The nRF24 chip transmits unicast data frames to the BLE device. Hardware constraints impose a constant delay of 10.8 ms to the transmission of every frame. Depending on the scenario, we use repetitions in case of missed ACK within the timeout. During a measurement, the transmitter is always tuned to one advertisement channel. Measurement results are provided for all three channels. Since the iPhone continuously hops over the three channels, the probability that the iPhone receives a frame is limited. In fact, assuming that a BLE device listens to every advertisement channel the same amount of time, one frame out of three is likely to be delivered successfully. When the iPhone receives the unicast frame, it immediately sends back an ACK over all the three advertisement channels echoing the received sequence number.

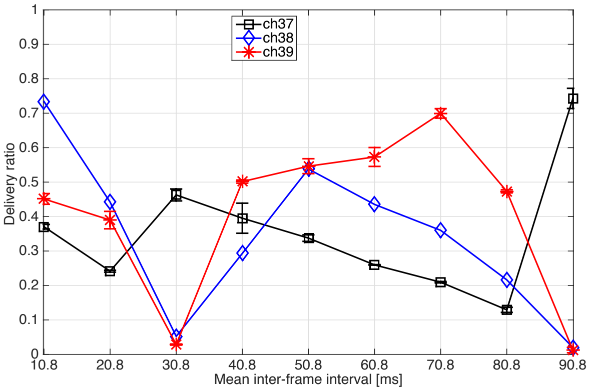

Figure 4: Periodic nRF24 to iPhone communication without retransmissions. The channel hopping procedure leads to lost frames.

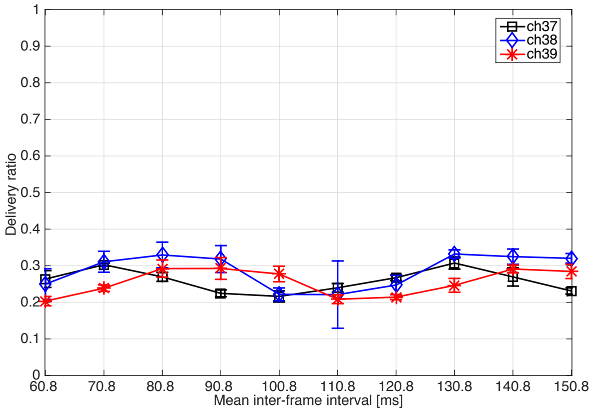

Figure 5: Delivery ratio of the nRF24 to iPhone communication with random interval between frames and no retransmissions.

Delivery Ratio for Periodic and Random Frames. Figure 4 shows the delivery ratio of 1000 unicast frames sent to an iPhone over the three channels. Every measurement is repeated 5 times. In this scenario without ACK frames or retransmissions, the delivery ratio is evaluated at the iPhone side. All frames are sent with constant period; the x-axis of the figure already takes into account the hardware delay of the nRF24 radio front-end. The figure gives a hint about the repetition period of the BLE device used for the measurements. The figure shows that the lack of channel coordination and the channel hopping procedure of the iPhone can set a severe limitation to the performance. In fact, if frames are sent every 30.8 ms, most of them are not received by the iPhone. When comparing Figure 5 (randomization of consecutive frames) with Figure 4, we understand that adding a random delay helps even without ACK

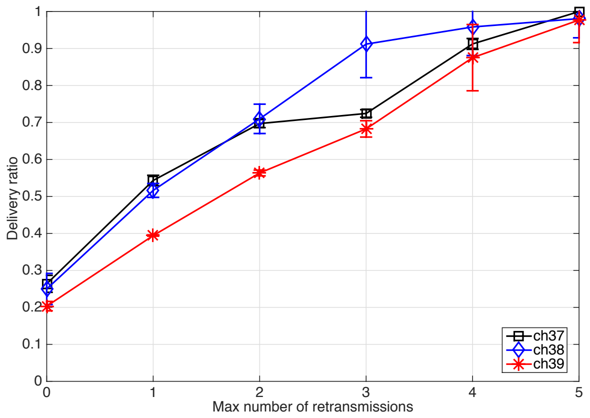

Figure 6: Effect of increasing the number of retransmissions for the nRF24 to iPhone communication direction. Frames are sent with random inter-frame intervals.

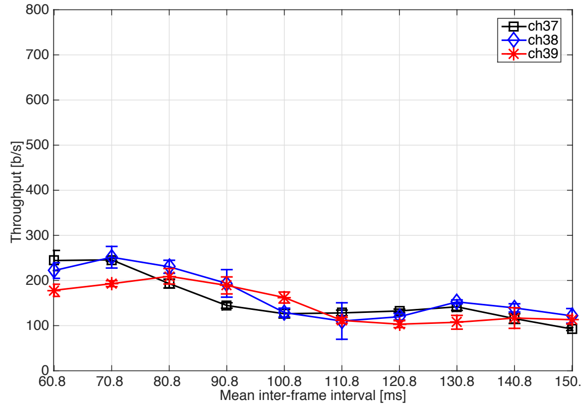

Figure 7: Throughput of nRF24 to iPhone communication for no retransmissions and random inter-frame intervals.

frames. Thus, all the following results use random intervals between frames.

Figure 5 shows the delivery ratio of 1000 unicast frames over the three advertisement channels without retransmissions. The offered traffic changes with the mean interval between two frames, but the interval between two frames is not constant. Instead, the nRF24 transmitter waits for a random time of up to 100 ms (uniformly distributed) before initiating the subsequent frame transmission. In the scenario without retransmissions (cf. Figure 5), this helps to smooth the delivery ratio. Figure 6 illustrates the performance improvement when missed frames are retransmitted. In Figure 6, every first attempt is separated by a period of 60.8±50 ms (that translates to a fixed minimum-inter-frame delay of around 10 ms, which is the shortest delay the nRF24 can handle, plus a random delay of up to 100 ms). Every retransmission is sent immediately after the ACK timeout fires. Since there is no coordination between transmitter and receiver on channel usage, the transmitter tries to reach the receiver with multiple consecutive retransmissions as early as possible. Figure 6 shows that increasing the number of retransmissions improves the reliability of the channel, guaranteeing higher delivery ratio at the expense of increased overhead and latency.

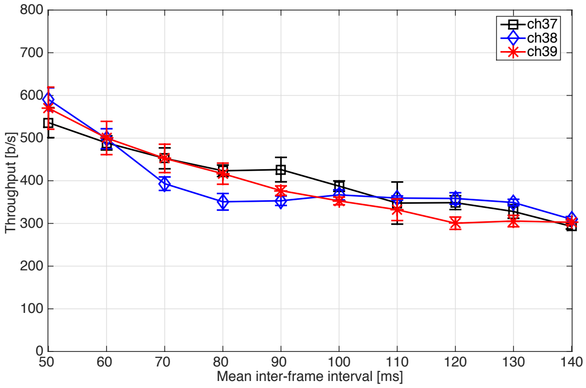

Figure 8: Throughput of iPhone to nRF24 communication without retransmissions.

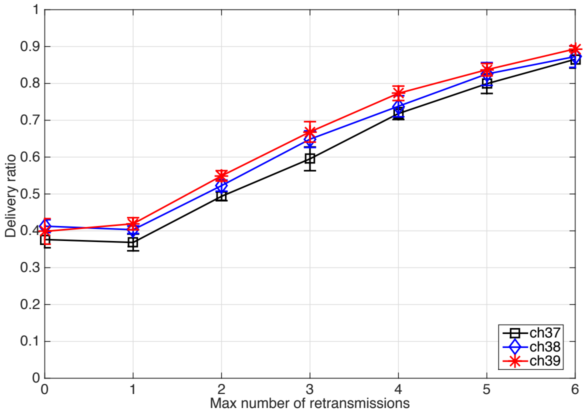

Figure 9: Delivery ratio versus increasing number of retransmissions for the iPhone to nRF24 communication.

Achievable Throughput.

Figures 7 shows the achieved throughput as function of the inter-frame interval without retransmissions. The figure shows a decreasing trend with increasing interval because incrementing the interval reduces the offered traffic.

4.4 BLE to nRF24

The evaluation shows the results for 1000 unicast frames sent by the iPhone to the nRF24 over all the three advertisement channels. The values are the result of 5 independent measurements. Each data frame is acknowledged. Since the receiver is tuned to one advertisement channel (there is no frequency hopping for the nRF24 chip), it always receives frames and responds with ACKs. IN fact, inside the shielded box there are no collisions because there are only one transmitter and one receiver; when a data frame is sent by the iPhone, the nRF24 chip always replies with an ACK. However, because of the BLE channel hopping process, ACKs might be missed jeopardizing the delivery ratio. Retransmissions are used to limit this effect.

Delivery Ratio and Achievable Throughput.

Figure 8 shows the throughput versus (random) inter-frame transmission interval. Increasing the mean inter-frame interval reduces the offer and therefore, the throughput decreases. The figure shows that all advertisement channels provide similar performance. Figure 9 illustrates the impact of retransmissions with randomized inter-frame interval of 50±50 ms for all the three advertisement channels. If no ACK is received, a new frame is sent after the timeout expires whereas if an ACK is received, then the new frame is sent immediately after its reception. As expected, increasing the number of retransmissions improves the reliability of the communication while decreasing the throughput (cf. Figure 8).

4.5 Collision Avoidance

The random time added before each initiation of a frame exchange can be used to minimize the undesirable effect of multiple devices operating on the same channel. The nRF24 supports a rudimentary carrier sensing on its operating frequencies, and hence a simple collision avoidance protocol is possible. The randomization is therefore not only needed to mitigate the correlation between BLE advertisement channel access and the nRF24, but also helps avoiding collisions, which is already a first step towards a complete MAC protocol.

5. CONCLUSION AND FUTURE WORK

A two-way communication protocol between BLE and nRF24 systems without using multi-protocol chips is demonstrated. The protocol can be used for applications with the low-complex nRF24 (IoT sensors, toys), as well as BLE (smartphones). The interworking protocol is tested using experimental lab experiments. The evaluation shows that it is possible to build a simple and sufficiently reliable data exchange that works in both directions. The results shown this in paper are a first step towards testing additional scenarios inside and outside a shield box and on the design of a MAC protocol based on random medium access and collision avoidance. Such MAC protocol must handle the communication of a combination of BLE and nRF24 devices using only the advertisement radio channels.

Acknowledgment

We thank Jani Saloranta, Lorenzo Bergamini, and Adriano Galati for their contributions.

6. REFERENCES

[1] B. Barnes. At Disney Parks, a Bracelet Meant to Build Loyalty. Available at http://www.nytimes.com, 7-January-2014.

[2] Bluetooth SIG. Bluetooth Core Specification 4.2. Available at https://www.bluetooth.org/en-us/specification/adopted-specifications, 2-Dec-2014.

[3] M. Buettner, G. V. Yee, E. Anderson, and R. Han. X-MAC: A Short Preamble MAC Protocol for Duty-cycled Wireless Sensor Networks. SenSys '06, pages 307–320, New York, NY, USA. ACM.

[4] K. Collins, S. Mangold, and G. Muntean. Supporting Mobile Devices with Wireless LAN/MAN in Large Controlled Environments. *Communications Magazine, IEEE*, 48(12):36–43, December 2010.

[5] J. DeCuir. Introducing Bluetooth Smart: Part 1: A look at Both Classic and New Technologies. *Consumer Electronics Magazine, IEEE*, 3(1):12–18, Jan 2014.

[6] Dimitry Grinberg. Bit-Banging Bluetooth Low Energy. Available at http://dmitry.gr, 31-July-2012.

[7] I. Glaropoulos, S. Mangold, and V. Vukadinovic. Enhanced IEEE 802.11 Power Saving for Multi-hop Toy-to-Toy Communication. In *GreenCom, IEEE Internet of Things (iThings/CPSCom)*, pages 603–610, Aug 2013.

[8] J.-S. Lee, Y.-W. Su, and C.-C. Shen. A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. In *IECON 2007*, pages 46–51, Nov 2007.

[9] Nordic Semiconductor. nRF24LE1: Ultra-low Power Wireless System On-Chip Solution - Product Specification v1.6, 2014.

[10] Nordic Semiconductors. nRF51822 Bluetooth Smart and 2.4GHz proprietary SoC.

[11] M. Siekkinen, M. Hiienkari, J. Nurminen, and J. Nieminen. How Low Energy is Bluetooth Low Energy? Comparative Measurements with ZigBee/802.15.4. In *WCNCW, IEEE*, pages 232–237, April 2012.

[12] R. Want, B. Schilit, and D. Laskowski. Bluetooth LE Finds Its Niche. *Pervasive Computing, IEEE*, 12(4):12–16, Oct 2013.

[13] N. Zhu and I. O'Connor. Performance Evaluations of Unslotted CSMA/CA Algorithm at High Data Rate WSNs Scenario. In *IWCMC*, pages 406–411, July 2013.