Fafoutis, X., Tsimbalo, E., & Piechocki, R. (2016). Timing Channels in Bluetooth Low Energy. IEEE Communications Letters, 20(8), 1587-1590. DOI: 10.1109/LCOMM.2016.2574311

Timing Channels in Bluetooth Low Energy

Xenofon Fafoutis, *Member, IEEE,* Evgeny Tsimbalo, *Student Member, IEEE,* and Robert Piechocki

***Abstract*—This letter introduces timing channels in connectionless Bluetooth Low Energy (BLE). The proposed standard-compliant enhancement, BLE-TC (BLE with Timing Channels), improves the energy efficiency of an energy-constrained connectionless BLE transmitter by encoding additional information in the interarrival time between BLE advertisements. BLE-TC is analytically compared to the connectionless BLE standard. Using realistic timing noise that is empirically determined through a proof-of-concept-implementation, the results indicate that more than 10% improvement in energy efficiency can be achieved for low-throughput applications, such as smart metering and environmental sensing for smart cities.**

***Index Terms*—Bluetooth Low Energy; Timing Channels; Energy-constrained communications; Smart cities; Low-throughput applications**

I. Introduction

A timing channel is a communication channel that uses different time values as alphabet [1]. Gallager [2] was the first to study the information packets can carry, beyond the information encoded in their payload. The work of Anantharam and Verdu [3], followed by the work of Bedekar and Azizoglu [4], identifies the timing capacity of a channel and indicates that the overall capacity can be increased by encoding information in the interarrival times between packets originating from bursty sources. Timing channels have been extensively studied in the literature, mainly from the perspective of system security [1][5][6][7]. Covert timing channels, that coexist along traditional data channels, constitute a means of secretly transmitting information, and can be exploited by compromised systems to convey sensitive information without being detected. More recently timing channels have been proposed as a means of improving the energy efficiency of energy-constrained networks [8][9], such as satellite networks [10], intra-body sensor networks [11], and nanonetworks [12].

This letter focuses on Bluetooth Low Energy (BLE), also known as Bluetooth Smart [13], a wireless standard targeted for energy-constrained applications. BLE is a widely-used Internet-of-Things (IoT) enabling technology for smart cities [14] and smart home applications [15]. BLE is also the basis of the iBeacon technology [16] which enables proximity-based services and applications. In this context, timing channels are introduced in BLE as a standard-compliant extension that is called BLE-TC (BLE with Timing Channels). The goal of the proposed scheme is to improve the energy efficiency of a BLE advertiser by encoding additional information in the duration of sleep between sequent BLE advertisements (ADV). To the best of the authors' knowledge, this is the first time in the literature timing channels are applied to BLE. Additional contributions of this work include the proof-of-concept implementation of a basic version of the proposed scheme; and the analytical identification of the potential gains in energy efficiency compared to standard connectionless BLE, after optimising the scheme's configuration parameters and under empirically-determined realistic noise in the time domain.

This work was performed under the SPHERE IRC funded by the UK EPSRC, Grant EP/K031910/1. The authors are with the University of Bristol, UK (email: xenofon.fafoutis@bristol.ac.uk).

II. BLE with Timing Channels (BLE-TC)

In connectionless BLE, a transmitter node (advertiser) communicates data to a receiver node (scanner) via broadcasting non-connectable undirected ADVs [13]. Such frames are typically transmitted periodically, whilst the standard dictates that the advertising period must not be less than 0.1 s. An ADV can be up to 39 bytes in total, with up to 24 bytes of payload data. The advertiser never needs to switch into the listening mode, as the protocol is unidirectional. On the other side, the scanner node, which is out of the scope of the paper, keeps its radio continuously in listening mode.

Let us now enhance the advertiser node with timing channels (BLE-TC). In BLE-TC, the advertising period is dynamic, so that additional information is encoded in the interarrival time between ADVs. The scheme reschedules the ADVs as shown in Fig 1. Two types of ADVs are defined, the guard ADVs and the floating ADVs. The former have a fixed interarrival time between them. Each guard ADV signals the transmission of a timing message. The transmission of the floating ADV is scheduled in a variable manner, so that information is encoded in the interarrival time between each floating ADVs and its preceding ADV. Between ADVs the transmitter node sleeps, similarly to the standard. The number of floating ADVs between two guard ADVs is defined as $N \in \mathbb{N}$. $N = 0$ corresponds to standard connectionless BLE. Applicable encoding algorithms have been investigated in [17].

It should be noted that BLE-TC is based on time intervals that are calculated using timestamps that are obtained from the same clock source. As a result, it is not vulnerable to clock drift, and no additional complexity for regular synchronisation is introduced. Constant errors that do not accumulate over time can be corrected without being a regular overhead in the energy consumption. Nevertheless, temperature compensation on the clocks is required for outdoors deployments.

The section continues with the analytical approximation of the energy efficiency of BLE-TC in comparison to the connectionless BLE standard. Let us assume that a BLE transmitter consumes $E_{L,P_{tx}}$ units of energy to turn on the radio, generate an ADV frame of L payload bits, and transmit it with a transmission power of P_{tx}. Assuming no channel errors, the energy efficiency of the BLE advertiser is defined as $\eta = E_{L,P_{tx}}/L$, expressed in energy units per bit.

Let us now consider the BLE-TC enhancement that encodes information in the ADV interarrival time. BLE-TC is prone to

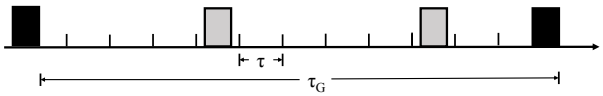

Fig. 1. An instance of the mechanics of BLE-TC for $N = 2$. Dark frames are guard ADVs that define the beginning of a timing message. The floating ADVs (light frames) are scheduled dynamically so that additional information is encoded in the interarrival time between the ADVs. The advertiser sleeps between ADVs, similarly to the connectionless BLE standard.

errors due to noise in the time domain. A scheduled ADV arrives at the receiver with some delay, which is experienced as noise in the interarrival time. Let us assume that this noise is following a normal distribution, $\epsilon \sim \mathcal{N}(0, \sigma^2)$. To tolerate this noise, a timeslot, $\tau \in \mathbb{R}^+$, is defined. Encoded messages are expressed as multiples of τ. As a result, there is a decoding error probability that depends on the length of the timeslot τ.

$$p = 1 - \Pr\left[-\frac{\tau}{2} \leqslant \epsilon \leqslant \frac{\tau}{2}\right] = erfc\left(\frac{\tau}{2\sigma\sqrt{2}}\right) . \quad (1)$$

Given a particular τ that satisfies the error rate requirements of the system, all time intervals can be expressed in timeslots, as a multiple of the basic time quantum τ. For example, the BLE specifications dictate that for an implementation to be BLE-compliant the minimum interarrival time between ADVs cannot be less than $\tau_A = 0.1$ s. Therefore, BLE ADVs should be separated by at least $G \in \mathbb{N}$ timeslots, where $G = \lceil \tau_A/\tau \rceil$. Two guard ADVs are characterised by a fixed interarrival time, τ_G. As a result, there are $K \in \mathbb{N}$ available timeslots between them. For $N \geq 1$, K can be expressed as:

$$K = \left\lceil \frac{\tau_G}{\tau} \right\rceil - 2G . \quad (2)$$

The guard interarrival time τ_G needs to be sufficiently large, so that $K > 0$. The available number of codewords in the timing channel, $D \in \mathbb{N}$, can be calculated as the number of combinations of N floating ADVs over K timeslots without repetitions, subject to the constraint that all ADVs need to be separated by G timeslots, as specified by the BLE standard.

$$D = \frac{\big(K - (N-1)G\big)!}{\big(K - (N-1)G - N\big)!N!} \quad (3)$$

This corresponds to $L_T = \lfloor \log_2 D \rfloor$ encoded bits.

A timing message is encoded using N floating ADVs and a single guard ADV. Therefore, the energy efficiency of BLE-TC can be expressed as:

$$\eta_T = \frac{(N+1)E_{L,P_{tx}}}{(N+1)L + (1-p)^N L_T} , \quad (4)$$

where the term $(1-p)^N L_T$ is the average number of useful bits delivered by the timing channel. This models timing errors as statistically independent, which is a worst case scenario assumption that provides an upper bound for the probability of error in a timing message.

The gain in energy efficiency (F) compared to the connectionless BLE standard can be expressed as:

$$F = \frac{\eta}{\eta_T} = \frac{(N+1)L + (1-p)^N L_T}{(N+1)L} = 1 + \frac{(1-p)^N L_T}{(N+1)L} . \quad (5)$$

It can be noted that the gain does not depend on the absolute energy required for a transmission, $E_{L,P_{tx}}$. Therefore, it depends neither on the transmission power nor on the implementation of the BLE radio.

For the remainder of the paper, some additional definitions are made. In theory, the timeslot size, τ, is a positive real number. In practice, transmission timings are controlled by oscillators and, therefore, are quantised. Typically, BLE embedded systems use $f_0 = 32,768$ Hz oscillators for scheduling wake-up events. This results in a time quantum of $T_0 = 1/f_0$. Thus, $\tau = \alpha T_0 = \alpha/f_0$ where $\alpha \in \mathbb{N}$.

In the proposed BLE-TC, the ADV period varies as information is encoded in it. In the standard, the ADV period is fixed. We define T as the average ADV period in both cases. To compare various scenarios under the same power budget, τ_G is set according to it: $\tau_G = T(N+1)$. This guarantees that BLE-TC transmits same number of ADVs as the standard.

For a given power budget that allows a certain long-term average transmission period (T), payload size (L), and noise level (σ), the gain in energy efficiency depends on two protocol parameters, namely N and α. It can be observed in (5) that the effect of those two parameters is two-fold. Decreasing α (or τ) increases the amount of encoded bits (L_T), but at the same time it increases the error rate p. Same applies for the number of floating ADVs N. We, next, identify the optimal values for N and α, so that the gain is maximised.

$$\underset{N\in\mathbb{N},\ \alpha\in\mathbb{N}}{\operatorname{argmax}} F(N,\alpha) = \underset{N\in\mathbb{N},\ \alpha\in\mathbb{N}}{\operatorname{argmax}} \frac{(1-p)^N L_T}{(N+1)} \quad (6)$$

We solve the maximisation problem using a variation of gradient ascent with discrete-space derivatives:

$$\begin{bmatrix} N_{n+1} \\ \alpha_{n+1} \end{bmatrix} = \left\lfloor \begin{bmatrix} N_n \\ \alpha_n \end{bmatrix} + \gamma \begin{bmatrix} F(N_n+1,\alpha) - F(N_n,\alpha) \\ F(N_n,\alpha+1) - F(N_n,\alpha) \end{bmatrix} \right\rfloor , \quad (7)$$

where $n \in \mathbb{N}$ and $\gamma \in \mathbb{N}^2$.

III. Proof-of-Concept Implementation

A basic version of BLE-TC is implemented next. Beyond proving the concept, the implementation is used to empirically identify a realistic approximation of the timing error ϵ, and verify that it can be accurately modelled with a Gaussian distribution. The BLE-TC encoder is implemented at a software level, *i.e.* on top of the BLE stack, using an nRF51822 BLE advertiser [18], whereas the BLE-TC decoder is implemented on top of a CC2650 BLE scanner. We stress that such a high-level software implementation introduces additional timing error due to processing and operating system delays, which could be mitigated with a low-level implementation closer to the radio. Therefore, it can be seen as a worst-case scenario.

More specifically, BLE-TC is implemented with the following configuration: $N = 1$, $\alpha = 3276$ ($\tau \approx 0.1$ s), $\tau_G = 1.8$ s. This encodes $L_T = 4$ bits on the timing channel. Fig. 2 shows the empirical approximation of the probability density function (PDF) of the timing error, ϵ, demonstrating Gaussian characteristics. The timing error is calculated as the difference of the scheduled and the measured interarrival time.

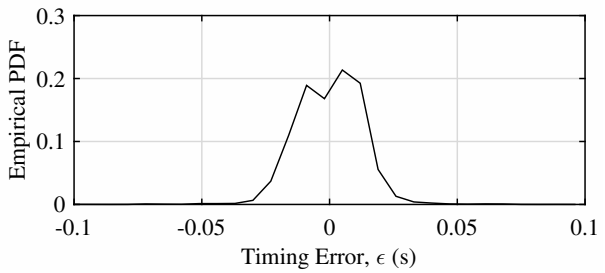

Fig. 2. Empirical approximation of the PDF of the timing error for various scheduled intervals. The sample standard deviation is $\sigma = 12.7$ ms.

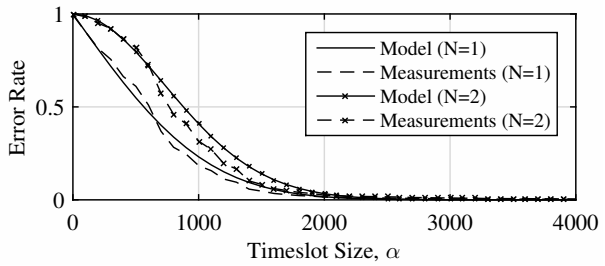

Fig. 3. Empirical approximation of the error probability against the model with the same standard deviation, $\sigma = 12.7$ ms.

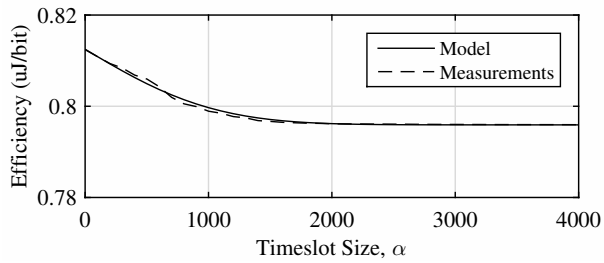

Fig. 4. Empirical approximation of the energy-efficiency of BLE-TC ($N = 1$, $L = 96$ bits, $L_T = 4$ bits, $\sigma = 12.7$ ms) against the model.

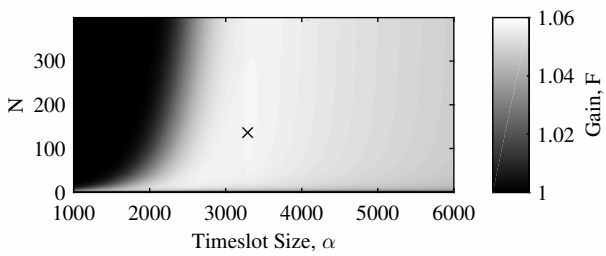

Fig. 5. Improvements in energy efficiency of BLE-TC ($T = 2$ s, $L = 96$ bits, $\sigma = 12.7$ ms) compared to standard BLE for various configurations of the timeslot size (α) and the number of floating ADVs (N). The cross marks the the optimum configuration: $N = 135$, $\alpha = 3300$ ($\tau = 100.7$ ms).

The sample standard deviation is $\sigma = 12.7$ ms. There was no observable interference during the measurements.

Given these empirical statistics of the timing error, Fig. 3 plots the error probability, $p = 1 - \Pr\left[-\frac{\tau}{2} \leqslant \epsilon \leqslant \frac{\tau}{2}\right]$, against various timeslot sizes, τ. The dashed lines are based on the empirical measurements, whereas the solid lines are based on model, for the same standard deviation $\sigma = 12.7$ ms. It can be observed that, for the purposes of this work, the model approximates the timing error probability sufficiently well. In addition to the implemented scenario ($N = 1$), the figure emulates the scenario of $N = 2$ by considering that each two consecutive interarrival times are part of the same timing message, thus both are required to be decoded correctly for the timing message to be correct. The results demonstrate that the model provides an upper bound on the timing message error rate. Similarly, Fig. 4 compares the modelled energy efficiency of BLE-TC, based on (4), against the energy efficiency obtained from measurements, using the methodology presented in [15]. The comparison further validates the model and justifies the analytical results that follow.

IV. Optimal Gain in Energy Efficiency

The scheme parameters, α and N, which control the timeslot size (τ) and the number of floating ADVs respectively, can be optimally configured to maximise the gain in energy efficiency of BLE-TC compared to the BLE standard. This is visualised in Fig. 5. The figure plots a heat map, where the axes correspond to the α and N parameters. The colour code corresponds to the gain in energy efficiency as derived by (5), while $\times$ marks the global maximum, and thus the optimal configuration: $N = 135$, $\alpha = 3300$ ($\tau = 100.7$ ms). The figure assumes: the timing error measured in Section III ($\sigma = 12.7$ ms); a BLE ADV payload size of 12 bytes ($L = 96$ bits); and an application-defined power budget that allows a long-term average transmission period of $T = 2$ s. In this configuration, BLE-TC yields a maximum improvement of 5.75% in energy efficiency compared to standard BLE. It can be observed that initially the gain rises steeply with the timeslot size, which is caused by the falling timing error rate, as shown in Fig. 3. At the same time, a larger timeslot size leads to a smaller number of bits that can be encoded, which has a negative effect on the gain. After a certain point, the latter effect prevails, and the gain starts decreasing with α. The effect of the number of floating ADVs, N, is more subtle.

Fig. 6 plots the maximised gain in energy efficiency that BLE-TC yields in comparison with the connectionless BLE standard. The maximised gain is calculated using (5) with the optimal configuration for the scheme parameters α and N, obtained by (7). The step parameter γ is empirically set to $\gamma = [2 \cdot 10^2 \;\; 2 \cdot 10^6]$. Focusing on the dark solid line, which corresponds to the same scenario as Fig. 5 (*i.e.* $L = 96$ bits, $\sigma = 12.7$ ms), it can be observed that increasing the long-term average ADV period (T) monotonously increases the gain. This is because of the increasing number of available codewords, D, due to more timeslots between frames. The improvement is more than 10% for applications (or power budgets) that require transmissions every $T \geq 40$ seconds on average. This indicates that exploiting the timing channels in BLE is particularly beneficial for low-throughput applications, such as environmental sensing and smart meters.

Focusing on the three dark lines, one can observe the effect of the ADV payload size, L, on the gain in energy efficiency. As shown in the figure, increasing L makes the number of the additional bits encoded in the timing channel, L_T, less significant. Yet, the improvement is more than 5% when $T \geq$

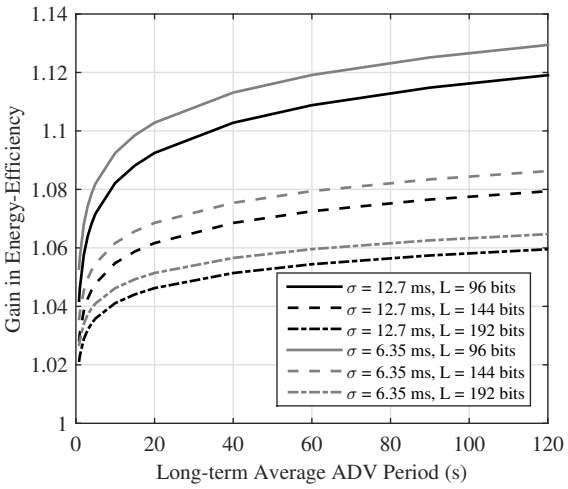

Fig. 6. Maximised gain in energy efficiency of BLE-TC compared to standard BLE for various application parameters: long-term average ADV period (T), level of timing noise (σ), and payload size (L).

40 seconds for $L = 192$ bits (*i.e.* 24 bytes), which is the maximum payload size allowed by the BLE standard. The results indicate that timing channels in other protocols that, unlike BLE, use large packet sizes, would be less beneficial.

In an attempt to demonstrate what would be the additional benefit of an implementation of the BLE-TC encoder / decoder closer to the radio, the light-coloured lines in Fig. 6 plot the gain in energy efficiency, assuming half the timing error measured in Section III. It can be observed that a 50% reduction of the error level ($\sigma = 6.35$ ms) leads to a 10% increase in the gain in energy efficiency ($T = 40$ s). This is because reducing the timing error would allow a larger number of timeslots, K, for the same error probability, p. Yet, increasing the available number of codewords, D, has a logarithmic effect on the number of encoded bits, L_T.

V. Conclusion

In timing channels, information is encoded in time intervals. In this letter, timing channels are introduced to connectionless BLE, a wireless IoT-enabling standard for energy-constrained applications. In addition to the payload of the BLE ADV, the proposed standard-compliant enhancement, named BLE-TC, encodes information in the sleeping time between ADVs. These additional bits are encoded without increasing the radio duty cycle, effectively improving the energy efficiency of the energy-constrained connectionless BLE transmitter.

The proposed scheme is first analytically modelled. As a performance metric, the gain in energy efficiency compared with the connectionless BLE standard is proposed. It is shown that an optimal set of parameters can be chosen to maximise this gain. To provide a realistic input for the analysis, a basic version of the proposed scheme, which encodes 4 bits in the timing channel, is implemented on top of off-the-shelf BLE radios. Using this proof-of-concept implementation, the statistics of the timing noise is measured and used as a realistic input in the subsequent analysis. The proposed scheme is then optimised and its performance is studied. It is shown that significant improvements in the energy efficiency of BLE can be achieved by exploiting the timing channel. Particularly for low-throughput applications that operate on tight power budgets, such as smart metering and environmental sensing applications for smart cities, this gain is analytically approximated to be more than 10%.

Complexity issues may rise from the implementation of the timing channel encoder. Whilst the design of an encoding algorithm is beyond the scope of this letter, encoding complexity can be mitigated with a cache memory. However, practical limitations on the size of the cache memory may introduce a constraint on the value of N. For that reason, in future work, we aim at identifying the optimal gain under the presence of such system-level constraints. Additional directions for future work include the introduction of application-specific delay constraints with regard to the timing message, and the introduction of channel errors to the model.

References

[1] I. S. Moskowitz and A. R. Miller, "Simple timing channels," in *Proc. IEEE Comp. Society Symp. on Research in Security and Privacy*. IEEE, 1994, pp. 56–64.

[2] R. Gallager, "Basic limits on protocol information in data communication networks," *IEEE Trans. on Inform. Theory*, vol. 22, no. 4, pp. 385–398, 1976.

[3] V. Anantharam and S. Verdu, "Bits through queues," *IEEE Trans. on Inform. Theory*, vol. 42, no. 1, pp. 4–18, 1996.

[4] A. Bedekar and M. Azizoglu, "The information-theoretic capacity of discrete-time queues," *IEEE Trans. on Inform. Theory*, vol. 44, no. 2, pp. 446–461, 1998.

[5] W.-M. Hu, "Reducing timing channels with fuzzy time," *J. of Comput. Security*, vol. 1, no. 3, pp. 233–254, 1992.

[6] J. Giles and B. Hajek, "An information-theoretic and game-theoretic study of timing channels," *IEEE Trans. on Inform. Theory*, vol. 48, no. 9, pp. 2455–2477, 2002.

[7] R. Sundaresan and S. Verdu, "Robust decoding for timing channels," *IEEE Trans. on Inform. Theory*, vol. 46, no. 2, pp. 405–419, 2000.

[8] G. Morabito, "Exploiting the timing channel to increase energy efficiency in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 8, pp. 1711–1720, Sept. 2011.

[9] Y. Zhu and R. Sivakumar, "Challenges: Communication through silence in wireless sensor networks," in *Proc. 11th ACM Ann. Int. Conf. on Mobile Comput. and Networking (MobiCom)*, 2005, pp. 140–147.

[10] G. Morabito, "Increasing capacity through the use of the timing channel in power-constrained satellite networks," in *Proc. 26th IEEE Int. Conf. on Comput. Commun. (INFOCOM)*, May 2007, pp. 580–588.

[11] L. Galluccio, G. Morabito, and S. Palazzo, "Exploiting timing channel in intra-body sensor networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec 2012, pp. 5368–5373.

[12] S. D'Oro, L. Galluccio, G. Morabito, and S. Palazzo, "A timing channel-based MAC protocol for energy-efficient nanonetworks," *Nano Commun. Networks*, vol. 6, no. 2, pp. 39 – 50, 2015.

[13] *Specification of the Bluetooth system. Core Version 4.1*, Bluetooth SIG, 2013. [Online]. Available: http://www.bluetooth.com

[14] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, 2014.

[15] X. Fafoutis, E. Tsimbalo, E. Mellios, G. Hilton, R. Piechocki, and I. Craddock, "A residential maintenance-free long-term activity monitoring system for healthcare applications," *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, no. 31, Jan. 2016.

[16] N. Newman, "Apple iBeacon technology briefing," *J. Direct, Data Digit. Mark. Pract.*, vol. 15, no. 3, pp. 222–225, Jan. 2014.

[17] R. Piechocki and D. Sejdinovic, "Combinatorial channel signature modulation for wireless ad-hoc networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, June 2012, pp. 4684–4689.

[18] X. Fafoutis, B. Janko, E. Mellios, G. Hilton, R. S. Sherratt, R. Piechocki, and I. Craddock, "SPW-1: A Low-Maintenance Wearable Activity Tracker for Residential Monitoring and Healthcare Applications," in *Proc. of the Int. Conf. on Wearables in Healthcare (HealthWear)*, 2016.