HAL open science

Privacy Leakage of Physical Activity Levels in Wireless Embedded Wearable Systems

Xenofon Fafoutis, Letizia Marchegiani, Georgios Papadopoulos, Robert Piechocki, Theo Tryfonas, George Oikonomou

To cite this version:

Xenofon Fafoutis, Letizia Marchegiani, Georgios Papadopoulos, Robert Piechocki, Theo Tryfonas, et al.. Privacy Leakage of Physical Activity Levels in Wireless Embedded Wearable Systems. IEEE Signal Processing Letters, 2017, 24, pp.136 - 140. 10.1109/LSP.2016.2642300 . hal-01616477

HAL Id: hal-01616477

https://hal.science/hal-01616477v1

Submitted on 13 Oct 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Privacy Leakage of Physical Activity Levels in Wireless Embedded Wearable Systems

Xenofon Fafoutis, *Member, IEEE,* Letizia Marchegiani, *Member, IEEE,*
Georgios Z. Papadopoulos, *Member, IEEE,* Robert Piechocki, Theo Tryfonas, and George Oikonomou

***Abstract*—With the ubiquity of sensing technologies in our personal spaces, the protection of our privacy and the confidentiality of sensitive data becomes a major concern. In this paper, we focus on wearable embedded systems that communicate data periodically over the wireless medium. In this context, we demonstrate that private information about the physical activity levels of the wearer can leak to an eavesdropper through the physical layer. Indeed, we show that the physical activity levels strongly correlate with changes in the wireless channel that can be captured by measuring the signal strength of the eavesdropped frames. We practically validate this correlation in several scenarios in a real residential environment, using data collected by our prototype wearable accelerometer-based sensor. Lastly, we propose a privacy enhancement algorithm that mitigates the leakage of this private information.**

***Index Terms*—Security and Privacy; Embedded System Security; Wearable Systems; Internet of Things**

I. Introduction

Ageing populations [1] and the rise of chronic illness push the limits of national health systems [2]. Wearable technologies [3] and Ambient Assisted Living (AAL) infrastructures are widely considered as promising solutions that could encourage people to monitor their own well-being and facilitate timely interventions. Activity monitors, such as Fitbit, Jawbone UP and Nike+ Fuelband SE, have recently appeared in the consumer electronics market [4]. These wearable gadgets demonstrate the rise of a trend towards self-monitoring, as well as the user acceptability of wearable technologies. Yet, such gadgets are of limited use for novel applications due to their lack of interoperability with other healthcare systems, their limited expandability to new sensing technologies, and the restricted accessibility of the raw data. More recently, wearable sensors have been used along other sensing technologies to form multi-modal residential infrastructures that are capable of understanding how daily activities affect our well-being. The goal of these multi-modal platforms is to relieve the healthcare sector and improve the quality of life [5] [6].

Privacy concerns rise with the ubiquity of sensing technologies in our daily life and our private spaces [7] [8]. The legal right to information privacy is defined as the right for the protection of personal or private information from misuse or unauthorised disclosure. As a result, any unintentional disclosure of personal data can be considered as a violation of privacy. In [9], the authors evaluate various commercial personal health monitoring devices with respect to policies they adopt to protect the privacy of their users. Other works in this space have identified privacy attacks on wearable embedded systems and proposed mechanisms against them. In [10], the authors identified that different medical wearable sensors tend to have different traffic patterns, and information about the nature and the urgency of the medical condition of the patient may leak through those patterns. In [11], the authors identified security vulnerabilities in a commercial fitness tracker that allowed them to extract private fitness information. In [12] and [13], the effect of human bodies on WiFi signals is leveraged to passively extract information about their pose and gesture.

In this letter, we identify and experimentally validate that, in wireless embedded wearable systems, information about the physical activity levels of the user may leak through the wireless channel, when such devices transmit periodically. More specifically, we demonstrate that a passive eavesdropper can measure the dynamic changes of the wireless channel caused by the activity of the user, through the variability of the Received Signal Strength (RSS) of the eavesdropped packets. This metric strongly correlates with the physical activity levels of the user. Using our prototype wearable sensor [14], mounted on the wrist of a user in a real residential environment, we experimentally validate this potential violation of privacy in data sets that include a wide range of Activities of Daily Living (ADL). Moreover, this letter proposes a privacy enhancement algorithm that mitigates this leakage, by introducing artificial randomness in the wireless channel when the user is inactive.

The remainder of this letter is structured as follows. Section II sets the scope of this work, presenting the legitimate use of the wearable system and the assumptions about the attacker. Section III presents and experimentally validates the privacy attack on data collected in a residential environment. Section IV proposes and experimentally validates the effectiveness of a privacy enhancement countermeasure against this privacy attack. Lastly, Section V concludes the paper.

X. Fafoutis is with the Department of Electrical and Electronic Engineering, University of Bristol, U.K. (e-mail: xenofon.fafoutis@bristol.ac.uk).

L. Marchegiani is with the Department of Engineering Science, University of Oxford, U.K. (email: letizia.marchegiani@eng.ox.ac.uk).

G. Z. Papadopoulos is with IRISA, Télécom Bretagne, Institut Mines-Télécom, France (email: georgios.papadopoulos@telecom-bretagne.eu).

R. Piechocki is with the Department of Electrical and Electronic Engineering, University of Bristol, U.K. (e-mail: r.j.piechocki@bristol.ac.uk).

T. Tryfonas is with the Department of Civil Engineering, University of Bristol, U.K. (e-mail: theo.tryfonas@bristol.ac.uk).

G. Oikonomou is with the Department of Electrical and Electronic Engineering, University of Bristol, U.K. (e-mail: g.oikonomou@bristol.ac.uk).

This work was partially performed under the SPHERE IRC funded by the UK EPSRC, Grant EP/K031910/1.

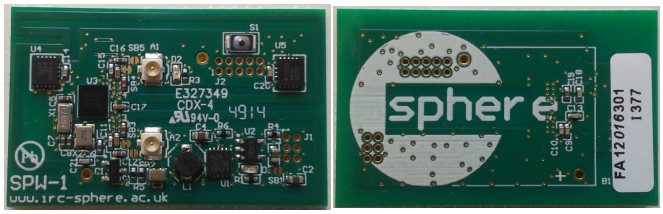

Fig. 1. The wearable embedded system used for the experimental results [14].

II. Scope and Threat Model

Let us consider *Alice*. Alice is using a wearable sensor to monitor her physical activity levels. The wearable sensor is equipped with a triaxial accelerometer for sensing, and a wireless radio for transmitting the raw data in her smart home for post-processing and for fusing them with other sensing modalities. In addition, the raw acceleration data are transformed into activity levels using the Integral of the Modulus of Acceleration (IMA). This metric is commonly used in the literature for estimating physical activity levels [15], as it correlates with the energy expenditure of a person [16]. The magnitude of a single acceleration sample, $\vec{a} \in \mathbb{R}^3$, is calculated as:

$$||\vec{a}|| = \left|\sqrt{a_x^2 + a_y^2 + a_z^2} - 1\right| \tag{1}$$

where a_x, a_y and a_z denote the acceleration on each of the three axes respectively, measured in g-units ($g = 9.8\ m/s^2$). The gravity component ($1\ g$) is subtracted from the magnitude of the raw signal to isolate the acceleration of Alice. Considering a discrete time series of samples, $\vec{a}_0, \vec{a}_1 \ldots \vec{a}_n$, the rolling IMA of the N-th sample over a window of w samples is then approximated as:

$$IMA_N = \sum_{i=0}^{w-1} ||\vec{a}_{N-i}|| \ , \ N \geq w \ . \tag{2}$$

Alice considers her physical activity levels private. Thus, she uses an off-the-shelf encryption algorithm to encrypt the raw acceleration data that are transmitted over the air.

In this paper, we demonstrate that despite any encryption, private information about Alice's physical activity levels can be leaked through the RSS of eavesdropped packets. Let us consider *Eve*, the eavesdropper. We assume that Eve has no physical access to Alice's home environment home. Instead, we assume that Eve has physical access to the common areas *outside* of Alice's home environment; areas that are within the wireless range of the wearable device of Alice. Indeed, it has been shown that the signal of a wearable system can traverse through multiple walls in residential environments [17]. Hence, Eve is able to eavesdrop and store the encrypted packets of the raw acceleration data, using a passive sniffer. Lastly, we assume that Eve has no access to the encryption key of Alice, and has no other means of decrypting the transmitted packets.

III. The Privacy Attack

Eve, the eavesdropper, listens to the wireless channel and collects all the encrypted frames that contain the raw acceleration data. For each received frame, Eve, measures the power of the received signal, RSS. The fundamental hypothesis for the success of the privacy attack is that the physical activity levels of Alice, IMA, correlate with the standard deviation of the first derivative of the RSS, denoted as RSS', as measured by Eve. Indeed, human activity inevitably makes the wireless channel more dynamic. Practically, Eve calculates this rolling standard deviation of the N-th sample (σ_N) over a window of w samples as follows:

$$\sigma_N = \sqrt{\frac{1}{w-1} \sum_{i=0}^{w-1} (RSS'_{N-i} - \overline{RSS'_N})^2} \ , \ N \geq w \ , \tag{3}$$

where $\overline{RSS'_N}$ is the mean over the same window w.

A privacy attack on the physical activity levels is considered successful when there is statistically significant correlation between the secret signal (2) and the one derived by Eve (3) for at least one window configuration, w. More specifically, we use the Pierson's linear correlation coefficient (denoted as c), and we test its significance against a null hypothesis of no significant correlation with a randomisation test ($N_{samples} = 10000$). The correlation is considered statistically significant when the null hypothesis is rejected with a p-value < 0.05. The Pierson's correlation coefficient is chosen because the data suggest a linear relationship.

We validate the hypothesis of the presented privacy attack with real data collected in a prototype 2-storey terraced house in the city of Bristol, UK [17]. The acceleration data are generated by SPW-1 [14], an accelerometer-based wearable sensor that communicates data to the smart home using the Bluetooth Low Energy (BLE) standard [18]. SPW-1 (shown in Fig. 1) employs the ADXL362 accelerometer [19], which is configured to: 20 Hz sampling frequency, 12-bit resolution, and $\pm 4\ g$ sampling range ($g = 9.8\ m/s^2$). The transmission frequency is 5 Hz, because of the fact that 4 data samples are packed in one advertisement frame. As a result, Eve collects RSS values at a maximum rate of 5 Hz (packets can be lost due to channel errors). In this context, we validate the privacy attack on data retrieved from a person living freely in the prototype smart house, whilst wearing the wearable sensor on their dominant wrist (the data is available in [20]). Therefore, we validate our hypothesis on several sessions of actual data

TABLE I
Activities of Daily Living Included in Each Session

Session	Duration	Activity List
1	16 m	Walking, vacuuming, dusting, cleaning
2	30 m	Walking, sitting, cooking, eating, preparing drink, drinking, watching TV
3	30 m	Walking, washing hands, drying hands, brushing teeth, grooming
4	16 m	Walking, sitting, watching TV
5	14 m	Sitting, working, using computer
6	13 m	Sitting, working, using computer
7	13 m	Sitting, walking, working, using computer, watching TV
8	13 m	Sitting, walking, watching TV
9	14 m	Sitting, watching TV
10	14 m	Sitting, watching TV
11	18 m	Sitting, walking, watching TV, cooking, eating

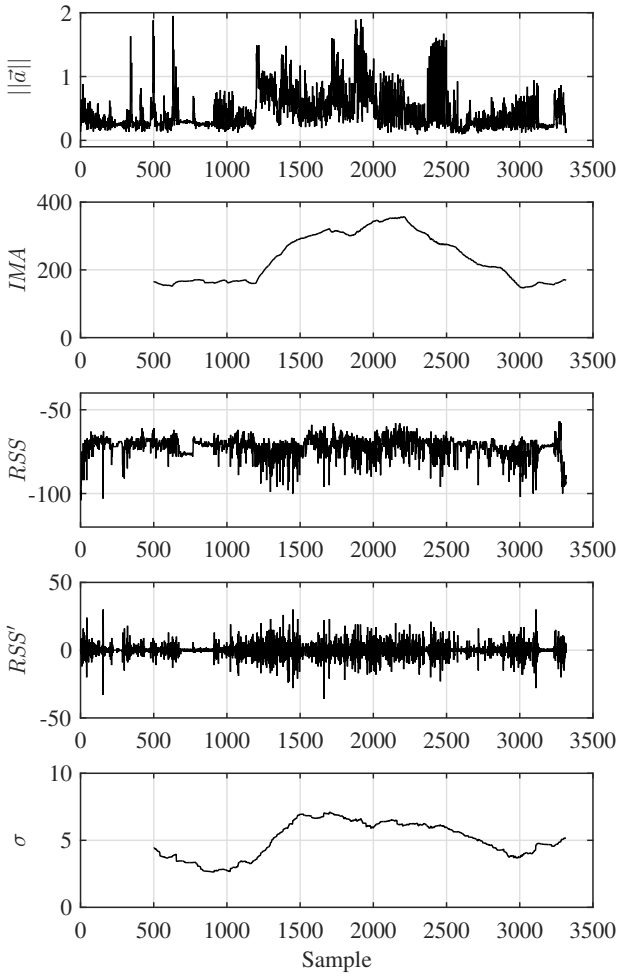

Fig. 2. Experimental results on the first session yield very strong correlation ($c = 0.87$) between the physical activity levels (IMA) and the standard deviation of the derivative of the RSS ($w = 500$). The magnitude of the acceleration, $||\vec{a}||$, is in g-units. The received signal strength, RSS, is in dBm. Its derivative, RSS', is in dBm per sampling period.

of a person being engaged in various activities of daily living (such as cooking, eating, working, and watching TV) in a real residential environment. A summary of the sessions and the activities of daily living is shown in Table I.

As an example, Fig. 2 demonstrates the privacy attack on the first session. The first two subplots (top of the figure) plot the secret signal of Alice, *i.e.,* the magnitude of acceleration $||\vec{a}||$ obtained by (1) and the IMA obtained by (2) for a window of $w = 500$ samples. It can be observed that there is an offset of approximately $0.2\ g$ in the acceleration profile. This is because of sensing noise, and because the accelerometer is not calibrated to the supply voltage (see Fig. 48 in [19]). The remaining three subplots (bottom of the figure) plot the signal observed by Eve, *i.e.,* the raw received signal strength (RSS), its derivative and the rolling standard deviation of the derivative as obtained by (3). It is calculated that there is a significant ($p < 0.0001$) and very strong ($c = 0.87$) correlation between the IMA and the signal derived by Eve.

Fig. 3 illustrates the correlation coefficient for the same session for various window sizes (w). It can be observed that there is moderate short-term correlation for $w \leq 60$, and strong

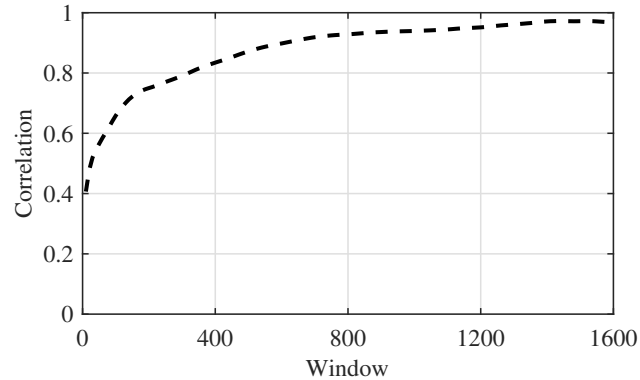

Fig. 3. Correlation between the private signal, *i.e.* the physical activity levels, and the signal derived by the eavesdropper for various window sizes, w. The correlation is significant ($p < 0.0001$) at all considered window sizes.

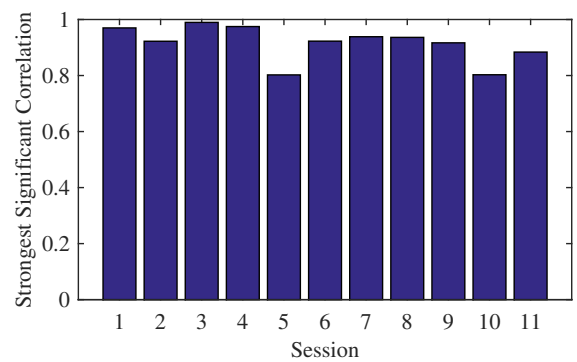

Fig. 4. Strongest significant correlation ($p < 0.05$) in each of the sessions. The results demonstrate that psychical activity information leaks consistently in different sessions that capture various activities of daily living. Each session number corresponds to the session number shown in Table I.

and very strong long-term correlation for $w \geq 60$, indicating that information leaks both when physical activity levels are fine-grained and coarse-grained. The strongest correlation ($c = 0.97$) is observed at $w = 1500$. The measured correlation is significant ($p < 0.0001$) at all considered window sizes.

Extending the analysis on the remaining of our sessions validates the vulnerability in various activities of daily living. Fig. 4 plots the strongest significant ($p < 0.05$) correlation observed in each session. The average strongest correlation is 91.6%. This demonstrates that private information about the physical activity levels of the user can be unintentionally disclosed in a wide range of scenarios. In addition, this vulnerability can be potentially exploited by a malicious eavesdropper as an initial step towards recognising the actual activities of the user. To this end, the attacker would require additional information to disambiguate between activities that correspond to similar physical activity levels.

IV. Privacy Enhancement

Fundamentally, information about the physical activity levels of Alice leak to Eve because the physical movements of Alice cause variations in the channel observed by Eve. This can be illustrated by the link budget formula: $RSS_i = P_{TX} + PL_i(\vec{a})$, where P_{TX} is the transmission power and PL is the channel gain, including the antenna gains. The channel gain partially

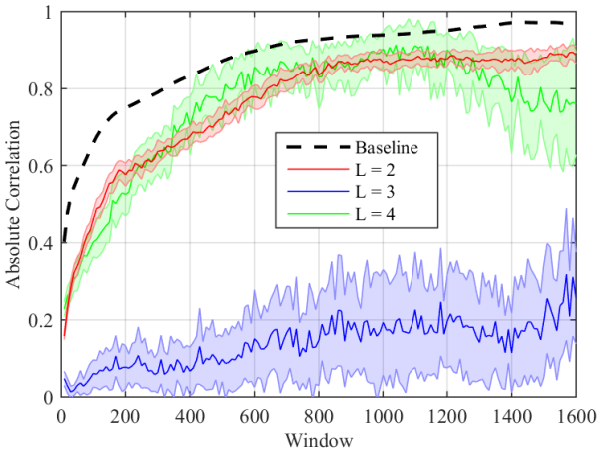

Fig. 5. The effectiveness of the proposed privacy enhancement scheme for various randomisation levels (L). The solid line corresponds to the mean and the shade corresponds to one standard deviation over 20 runs ($A = 0.08$ g).

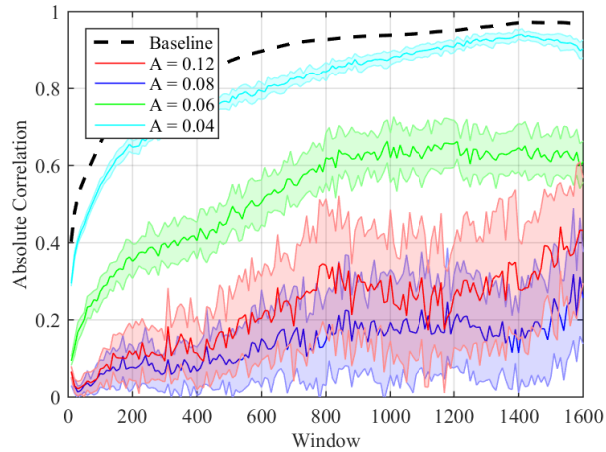

Fig. 6. The effectiveness of the proposed privacy enhancement scheme for various thresholds (A). The solid lines correspond to the mean and the shade corresponds to one standard deviation over 20 runs ($L = 3$).

depends on the movements of Alice. The transmission power, on the other hand, is fully controlled by Alice within the limits of the radio. Therefore, the leakage can be mitigated if Alice introduces artificial variations in the channel by randomly changing the transmission power when low physical activity is detected by the accelerometer. By doing so, Eve would not be able to infer the source of the observed variations in the channel. In addition, if Alice needs to reconstruct the channel state, she can include P_{TX} in the encrypted payload.

Let us consider the following privacy enhancement mechanism running on the wearable system. The algorithm has two input parameters: A, an acceleration threshold below which the randomisation is introduced, and L, the randomisation level. It is noted that if Alice introduces more artificial variation than her physical activity, she would create negative correlation, and information about her physical activity levels would leak to Eve. Thus, the goal of Alice is to run the algorithm with the input parameters that minimise the absolute correlation.

Algorithm 1 Privacy Enhancement Algorithm

input : A, L
output: P_{TX}
for *every ADV transmission* **do**
  calculate $||\vec{a}||$ using (1);
  if $||\vec{a}|| < A$ **then**
    $k \leftarrow \texttt{rand}()$;
    $P_{TX} \leftarrow P_{max} - P_{step} \cdot (k \bmod L)$;
  else
    $P_{TX} \leftarrow P_{max}$;
  end
end

Next, we apply the proposed privacy enhancement algorithm on our platform, SPW-1. The radio of SPW-1 offers 7 transmission power levels from -20 dBm to $+4$ dBm with a 4 dB step (*i.e.* $P_{max} = 5$ dBm, $P_{step} = 4$ dB) [14]. Focusing on the first data session, Fig. 5 demonstrates the impact of the randomisation level (L) to the absolute correlation of the signal extracted by Eve and secret signal for a constant threshold $A = 0.08$ g. Similarly, Fig. 6 demonstrates the impact of the threshold (A) to the absolute correlation for a constant randomisation level $L = 3$. In both figures, the solid lines correspond to the mean and the shades correspond to one standard deviation over 20 runs. The dashed line corresponds to the baseline scenario, as presented in Section III. It can be observed that proposed algorithm can be a very effective privacy enhancement scheme against the presented attack. It can also be observed that both configuration parameters have an optimum value; beyond which Alice overcompensates the effects of her movement on the channel gain.

Following the same methodology on the remaining sessions leads to similar results, yielding an average strongest correlation of 41.8%.

V. Conclusion and Future Work

As wearable embedded systems collect sensitive personal information, data confidentiality becomes a fundamental system requirement. Any unintentional disclosure of private information can be considered as a violation of privacy.

In this paper, we focus on wearable systems that communicate data periodically. We demonstrate that private information about the physical activity levels of their wearer can leak through the physical wireless channel to an eavesdropper, even when the data is encrypted. Using data collected with our prototype wearable sensor in a real residential environment, we demonstrate that the physical activity levels of the user strongly correlate with the standard deviation of the derivative of the received signal strength, as observed by a passive eavesdropper, in a wide variety of daily life activities. Furthermore, we propose a privacy enhancement algorithm that introduces artificial variations in the wireless channel, by randomising the transmission power when there is lack of activity.

As future work, it would be interesting to investigate if Eve can successfully execute the attack under packet loss by applying missing data techniques [21] on the eavesdropped signal. In addition, we plan to combine this privacy attack, with RSS-based indoors localisation algorithms. For instance, Eve could use the wall prediction model, presented in [22], to correspond the physical activity levels of Alice to the room in which these activities occurred.

References

[1] Department of Economic and Social Affairs, "World Population Ageing: 1950-2050," United Nations, Tech. Rep., 2011.

[2] A. J. Cruz-Jentoft *et al.*, "Silver paper: the future of health promotion and preventive actions, basic research, and clinical aspects of age-related disease–a report of the European Summit on Age-Related Disease," *Aging Clin. Exp. Res.*, vol. 21, no. 6, pp. 376–385, 2009.

[3] M. Chan, D. Estève, J.-Y. Fourniols, C. Escriba, and E. Campo, "Smart wearable systems: Current status and future challenges," *Artificial Intell. in Medicine*, vol. 56, no. 3, pp. 137 – 156, 2012.

[4] T. J. M. Kooiman, M. L. Dontje, S. R. Sprenger, W. P. Krijnen, C. P. van der Schans, and M. de Groot, "Reliability and validity of ten consumer activity trackers." *BMC Sports Sci. Med. Rehabil.*, vol. 7, no. 1, p. 24, 2015.

[5] K. Ozcan and S. Velipasalar, "Wearable camera- and accelerometer-based fall detection on portable devices," *IEEE Embedded Syst. Lett.*, vol. 8, no. 1, pp. 6–9, March 2016.

[6] P. Woznowski *et al.*, "SPHERE: A Sensor Platform for Healthcare in a Residential Environment," in *Designing, Developing, and Facilitating Smart Cities: Urban Design to IoT Solutions*. Springer International Publishing, 2017, pp. 315–333.

[7] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *Journal of Medical Systems*, vol. 36, no. 1, pp. 93–101, 2012.

[8] S. Avancha, A. Baxi, and D. Kotz, "Privacy in mobile technology for personal healthcare," *ACM Comput. Surv.*, vol. 45, no. 1, pp. 3:1–3:54, 2012.

[9] G. Paul and J. Irvine, "Privacy implications of wearable health devices," in *Proceedings of the 7th International Conference on Security of Information and Networks*, ser. SIN '14. ACM, 2014, pp. 117–121.

[10] L. Yao, X. Li, and G. Yu, "Pattern Regulator: Protecting Temporal Usage Privacy for Wireless Body Area Sensor Networks," in *Proc. IEEE 33rd Int. Conf. on Distributed Computing Systems Workshops (DCSW)*. IEEE, 2013, pp. 327–332.

[11] M. Rahman, B. Carbunar, and M. Banik, "Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device," in *Proc. 16th Privacy Enhancing Technologies Symposium (PETS)*, 2013.

[12] M.-C. Tang, F. K. Wang, and T. S. Horng, "Human gesture sensor using ambient wireless signals based on passive radar technology," in *Proc. IEEE MTT-S Int. Microwave Symposium*, May 2015, pp. 1–4.

[13] Q. Chen, B. Tan, K. Chetty, and K. Woodbridge, "Activity recognition based on micro-doppler signature with in-home wi-fi," in *Proc. IEEE 18th Int. Conf. on e-Health Networking, Applications and Services (Healthcom)*, Sept 2016, pp. 1–6.

[14] 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. Int. Summit on eHealth (eHealth 360)*, 2016, pp. 294–305.

[15] S. Bosch, R. Marin-Perianu, P. Havinga, and M. Marin-Perianu, "Energy-Efficient Assessment of Physical Activity Level Using Duty-Cycled Accelerometer Data," *Procedia Computer Science*, vol. 5, pp. 328–335, 2011.

[16] C. V. Bouten, K. R. Westerterp, M. Verduin, and J. D. Janssen, "Assessment of energy expenditure for physical activity using a triaxial accelerometer." *Medicine and science in sports and exercise*, vol. 26, no. 12, pp. 1516–23, 1994.

[17] 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, 2016.

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

[19] Analog Devices, "ADXL362 - Micropower, 3-Axis, ± 2 g / ± 4 g / ± 8 g, Digital Output MEMS Accelerometer, Rev. B," 2013.

[20] N. Twomey *et al.*, "The SPHERE challenge: Activity recognition with multimodal sensor data," *arXiv preprint arXiv:1603.00797*, 2016.

[21] S. Karadogan, L. Marchegiani, L. Hansen, and J. Larsen, "How efficient is estimation with missing data?" in *Proc. 2011 IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2011, pp. 2260–2263.

[22] X. Fafoutis, E. Mellios, N. Twomey, T. Diethe, G. Hilton, and R. Piechocki, "An RSSI-based Wall Prediction Model for Residential Floor Map Construction," in *Proc. 2nd IEEE World Forum on Internet of Things (WF-IoT)*, 2015, pp. 357–362.