Enabling Support of Legacy Devices for a more Sustainable Internet of Things

A position paper on the need to proactively avoid an "Internet of Trash"

Carlo Alberto Boano
cboano@tugraz.at
Institute of Technical Informatics
Graz University of Technology, Austria

ABSTRACT

Despite the increasing concerns on sustainability issues worldwide, IoT devices are still being designed unsustainably, and often end up as e-waste in landfill after a very short lifespan. This state of affairs is alarming, as we expect hundreds of billion connected devices in a few years, and calls for solutions to help maximizing the usable lifetime of IoT systems. In this paper, we review this problem in detail, and argue that legacy devices using outdated wireless technologies could make use of cross-technology communication to directly interact with newer IoT products, thereby increasing their durability. We also summarize our recent efforts in this domain and highlight how they could help in designing sustainable IoT systems.

CCS CONCEPTS

• **Social and professional topics** → Sustainability; • **Computer systems organization** → Embedded and cyber-physical systems; • **Networks** → Network services.

KEYWORDS

Cross-technology communication, E-waste, IoT, Legacy devices, Obsolescence, SERVOUS, Sustainability, Sustainable IoT, X-Burst.

ACM Reference Format:
Carlo Alberto Boano. 2021. Enabling Support of Legacy Devices for a more Sustainable Internet of Things: A position paper on the need to proactively avoid an "Internet of Trash". In *GoodIT '21: ACM International Conference on Information Technology for Social Good, September 09-11, 2021, Rome, Italy*. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

The Internet of Things (IoT) has unarguably revolutionized our society and many aspects of our daily lives for the better. Billions of "smart" objects have increased the comfort of people in their homes, improved healthcare as well as transportation, enabled large-scale environmental monitoring, and optimized production processes.

GoodIT '21, September 09–11, 2021, Rome, Italy

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/10.1145/1122445.1122456

The ubiquity of smart objects is projected to further increase in the next decade, as we will witness *several hundred billions* connected devices according to both IHS Markit [26] and Cisco [16]. These IoT devices will help us tackling key global challenges such as the increasing urbanization, the ageing population, the depletion of the energy resources in our planet, as well as the scarcity of food and water[1]. Smart cities filled with connected IoT devices will help us improving the quality of life in dense urban environments [66]; smart grids will optimize the production and distribution of energy [6]; smart health systems will allow a more efficient elderly care [49]; smart farming solutions will minimize the amount of water and fertilizers wasted, thereby improving agricultural practices and reducing environmental footprint [5]; whereas smart water networks will detect leaks and avoid precious drinkable water to be lost [11]. IoT systems are also expected to help us mitigating the effects of climate change on humans and civil infrastructure; *e.g.,* by performing an early warning for destructive events such as flash floods, forest wildfires, or thawing permafrost leading to rockfalls [42].

The IoT as a driver for sustainability. All these smart IoT systems are hence expected to drive *sustainability* in the years to come [10, 29, 37], and are often portrayed as essential to achieve many of the seventeen United Nation's sustainable development goals by 2030 [54]. An analysis conducted by IoT Analytics and the World Economic Forum supports this view, highlighting how many of the IoT products available on the market today already help (i) building smart cities, (ii) improving health and well-being, (iii) promoting a responsible production and consumption, (iv) increasing awareness and visibility into energy and resource usage, (v) facilitating access to clean energy, or (vi) accelerating industrial innovation [3]. While this is encouraging, there is still a lot of room for improvement, since the executives of large technology companies have confirmed that "sustainability is not a consideration at all in the design phase of most IoT projects" [59]. To cope with this issue and to further increase the impact that IoT technologies have on sustainability, the World Economic Forum has published a set of guidelines encouraging the prioritization of sustainability goals as part of the design of IoT projects [59]. Such guidelines touch, among others, aspects such as measurement of impact, collaboration models, incentives alignment, and infrastructure investments.

[1] By 2030, the world's population is expected to grow to 8.6 billion, out of which 60% will be living in cities, 10% will be food insecure, and almost 50% will be living in areas of high water stress. Furthermore, according to recent statistics, people aged 60 years or above will outnumber the amount of children aged nine or below by 2030, which will put an enormous pressure on the healthcare industry [4, 38, 53].

The other face of sustainability. Despite the increasing interest in the link between IoT technologies and sustainability, there is still relatively little focus on how to design sustainable IoT systems, *i.e.,* on how to minimize the effects that IoT devices have on the natural environment throughout their lifespan – from their design to their disposal. As observed by Stead et al., indeed, IoT devices are still being designed, manufactured, and disposed of unsustainably [50].

2 AN "INTERNET OF TRASH"

Especially the disposal of IoT devices is worrisome: with hundreds of billion connected devices in a few years from now [16, 26], it is essential to come up with solutions that help maximizing their usable lifetime. Without these, the concrete risk is to have a plethora of obsolete IoT devices and no way to dispose of them [23], which would drastically increase the amount of e-waste.

Planned obsolescence. A key problem in this regard is the fact that IoT devices are often explicitly designed to have a brief lifetime, an issue also known as planned obsolescence. The latter does not only refer to the functionality of a device, but also to its desirability: new generations of IoT devices typically offer additional features, better performance, nicer aesthetics, and are more likely to be compatible with the latest products available on the market. As a result, IoT devices that are just a few months or years old quickly become obsolete, and are likely to end up as electronic waste in landfill [50]. Even worse, "smarter" products are typically replaced more often than traditional appliances, which, instead, last for decades [23].

Lack of means to maintain IoT devices. Unfortunately, it is also not rare that IoT products are shipped without software update functionality, which prevents an efficient maintenance. This issue is often linked to (i) the reduction of the development time in favour of a faster time-to-market, and to (ii) the severe memory constraints of some IoT devices, which often embed just a few kilobytes of RAM and ROM [32]. This is not only a major security risk (unmanageable devices with vulnerable software may get recruited into botnets[2] attacking essential services of the Internet [31, 44]), but also a significant catalyst leading to a short device usability and lifetime.

A plethora of unnecessary IoT gadgets. While several IoT systems have tangibly helped us improving many facets of our daily life for the better, it is undeniable that many of the connected objects being commercialized today do not solve relevant problems or do not represent a need for most end-users. Smart bottle openers sharing the number of cheers over social media; smart toasters notifying us when the desired level of crispness has been reached; smart kettles that can be turned on/off remotely (but that cannot fill themselves with water); connected egg trays informing us about how many eggs are left; smart umbrellas reminding us to carry them along; and smart hair brushes measuring the strokes' speed and orientation are just a few examples of seemingly unnecessary IoT devices [58, 60]. Despite being advertised as technologies improving our lives, it is more likely that such devices – when sold in large quantities – generate more environmental damage once disposed of than benefits throughout their usable lifetime [52].

Unsteadiness of IoT businesses. Another catalyst for a short usability of IoT devices is the large number of IoT businesses driven by wild excesses of hype and inflated expectations. Indeed, the number of IoT-related start-ups and companies going bankrupt or ceasing to exists soon after releasing their first products is rather high [17, 48]. As a result, cloud services may suddenly be unavailable (which practically bricks all IoT devices that were relying on them [56]); small successful businesses may be acquired by larger companies in order to avoid competition (which often leads to IoT products being no longer supported or functional [19]); or IoT giants can launch products similar to those of smaller start-ups (but with a better integration into their ecosystem), practically destroying their business [48]. These and other factors can contribute to an even quicker obsolescence of commercial IoT products.

Volatility of wireless technologies. The IoT ecosystem evolves very rapidly: every year, new radio technologies are commercialized and several standards are created (or revised), which continuously increases the fragmentation of the IoT landscape. As a result, there are no de-facto solutions that system designers can adopt with the hope of a high durability [55]. For example, in the low-power wireless wide area networks (LP-WANs) domain, there are several competing connectivity options, *e.g.,* Sigfox, LoRa, Weightless, Dash7, Symphony Link, Ingenu RPMA, Narrowband-IoT, LTE-M, and many other cellular-IoT standards. The same holds true for the low-power wireless personal area networks (LP-WPANs) domain, where Bluetooth Low Energy (BLE), IEEE 802.15.4, ANT+, Thread, WirelessHART, Enhanced ShockBurst, Gazell, DigiMesh, and MiWi are just a few of the available options. While each technology has its unique features and advantages, it is to be expected that only a subset of these will stand the test of time and receive long-term support. Within this context, one can hardly predict how long a technology will survive: in the last two decades, we have seen technologies that were massively widespread or that were pushed by large consortia becoming obsolete rather quickly. For example, security concerns have triggered the revision of standards and deprecated earlier hardware, as we have witnessed with BLE 4.0/4.1 devices[3] and with ultra-wideband modules employing IEEE 802.15.4a/f[4]; whereas technologies heralded with great fanfare (*e.g.,* Wireless USB) were quickly discontinued. Devices embedding outdated technologies, even though fully-functional and with up-to-date software, cannot communicate with newer systems: this prevents their use/integration and leads to an early disposal.

3 HOW TO DEAL WITH LEGACY DEVICES?

Given the pace at which IoT systems may become obsolete or no longer compatible with the latest communication standards, it is important to design solutions allowing to prolong the usable lifetime of devices that are still fully-functional and complete in all their parts.

[2] A botnet is a cluster of Internet-connected devices infected by a malware allowing hackers to control their operations. A notable example of botnet is Mirai, which caused a few hours of massive disruption in the USA during October 2016. With Mirai, many IoT devices using primitive authentication schemes (*e.g.,* with default username and passwords) were exploited to attack the Internet's central infrastructure, more specifically several DNS servers. This resulted in the inaccessibility of high-profile websites, such as Amazon, Netflix, GitHub, Twitter, and Reddit for several hours [31].

[3] BLE v4.0 and v4.1 devices cannot make use of secure connections, and hence provide less security than more recent BLE modules. Especially protection to eavesdropping and man-in-the-middle attacks during the pairing process is a major concern [39].

[4] Several works have shown how ultra-wideband devices adhering to the IEEE 802.15.4a/f standards are vulnerable to physical-layer attacks affecting the reliability of their ranging measurements. As a result, the IEEE 802.15.4z standard has recently been approved to improve the security of UWB ranging systems [47, 51].

This is not only crucial to avoid an "early-tossing" of IoT devices (which would drastically increase the amount of e-waste), but also to prevent manufacturing of new devices performing the exact same task(s) that a legacy device could still fulfil. Both of these aspects are essential towards a sustainable IoT development.

Example Ⓐ: smart home device using an outdated radio. Consider a fully-functional smart smoke detector embedding a radio compliant to technology A. Imagine that the next-generation smart speakers (which often act as hubs in smart homes to orchestrate the activities of the various IoT devices) only support technologies B/C/D and do no longer include hardware to communicate with IoT products based on technology A. Since devices using different communication technologies cannot directly exchange messages, the smart smoke detector (or any other legacy IoT device using technology A) cannot be integrated into the new smart home ecosystem. Although multi-radio gateways bridging the communications between technology A and B/C/D may exist, it is much more likely that the end-user purchases a newer smoke detector that can directly connect with the latest smart speakers. On the one hand, the price of a new smart sensor is likely cheaper than that of a gateway; on the other hand, the need to install additional devices is typically not appealing and leaves end-users frustrated [7, 20, 65]. To avoid this scenario (*i.e.,* to let the smoke detector retain its original purpose and remain operational), we need a way to let two devices with incompatible technologies directly exchange data without the need of extra hardware. As we discuss in Sect. 4, cross-technology communication could provide a solution in this regard.

Example Ⓑ: dismissed smart sensors. Consider a set of smart temperature and humidity sensors that were originally installed in a building to keep track of the climate in various rooms. Imagine that these devices are no longer desirable or appealing for their original purpose (*e.g.,* they have been replaced by newer devices incorporating the same and many other features). Instead of being tossed, these smart sensors could be reprogrammed and reused for different tasks. For example, they could be used together with other refurbished products (e.g., air quality sensors) to set up mesh networks performing large-scale low-rate sensing tasks, such as identifying urban heat islands or monitoring the air pollution in a specific city district[5]. After all, IoT devices, although obsolete, still embed several sensors that may allow one to gather sufficient insights about specific physical quantities; and may be as good as newer devices embedding the same type of sensors[6]. Connecting together several legacy devices towards a common goal, however, may be challenging due to the large fragmentation of wireless technologies discussed in Sect. 2. Assuming that one can easily reprogram each device with a new firmware, one would still need the ability to let heterogeneous devices interact with each other (*i.e.,* let several devices with potentially incompatible technologies directly exchange data without the need to change their hardware configuration). To this end, we argue next that one could use cross-technology communication, an emerging paradigm allowing the exchange of data across devices making use of heterogeneous wireless technologies.

[5]Our hope is that city counsellors would incentivize the reuse of legacy devices for such purposes, rather than spending money to produce new IoT sensors. Although utopistic, we should aim to create the conditions for this to become a concrete possibility.

[6]Think, for example, at the almost 20-years old TelosB wireless sensor nodes [41], which were proven to be incredibly durable, and are often still in use today.

4 CROSS-TECHNOLOGY COMMUNICATION

Cross-technology communication (CTC) has recently emerged as a promising technology to allow a *direct* interaction between wireless devices with incompatible physical layer (PHY) without the need of extra-hardware, *e.g.,* multi-radio gateways. Although sometimes considered a mere academic exercise with limited applicability to real-world scenarios, CTC was shown to allow the creation of attractive services among heterogeneous devices and platforms, including clock synchronization [63], sensor reconfiguration [45], as well as coexistence mechanisms mitigating cross-technology interference and improving spectral efficiency [40, 57, 61, 64].

As of today, the largest body of work on CTC has focused on devices sharing the 2.4 GHz ISM band, given the massive amount of devices sharing these frequencies [14]. Several CTC schemes allow indeed communication between BLE, Wi-Fi, and IEEE 802.15.4 devices in various directions, *e.g.,* BLE → IEEE 802.15.4 [28, 30], IEEE 802.15.4 → BLE [24, 27], Wi-Fi → IEEE 802.15.4 [13, 30, 35], IEEE 802.15.4 → Wi-Fi [9, 21, 22, 30], BLE → Wi-Fi [15, 30, 34], or Wi-Fi → BLE [36]. Other works have also explored communication between BLE and LoRa [33], as well as across devices operating in other ISM bands, *e.g.,* the sub-GHz [46], and the 5 GHz band [18].

CTC schemes can be broadly divided into two main categories: those exploiting *packet-level modulation*, and those making use of *PHY emulation* techniques to convey information across devices using different standards. Recent CTC approaches employ PHY emulation techniques, which transmit information such that (a portion of) the transmitted frames can be recognized by a device using another technology as legitimate and received seamlessly [27, 28, 35]. Packet-level modulation techniques, pioneered by the work by Chebrolu et al. [12], instead, encode information into different packet-level properties, *e.g.,* frame lengths [13, 24], gap durations [68], beacon intervals [30], and power levels [15]. This information is then decoded using energy detection, *i.e.,* by letting the radio perform a high-frequency sampling of the received signal strength (RSS).

Whilst PHY emulation techniques allow to achieve a very high throughput and do not require devices to switch into RSS sampling mode to receive information, they typically only work in one direction, and may require hardware modifications [22, 27]. Conversely, packet-level modulation techniques achieve a lower throughput, but are more generic and may allow a bidirectional data exchange as well as the transmission of cross-technology broadcast frames [8].

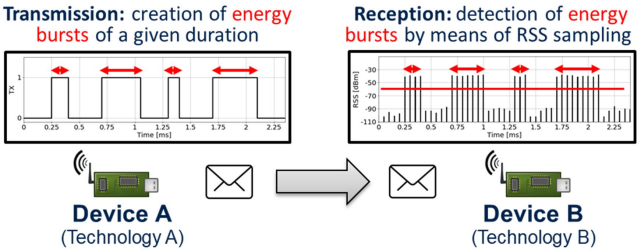

Figure 1: Basic principle of packet-level modulation CTC schemes such as `X-Burst`. Almost any wireless device has the ability to transmit payloads of arbitrary length and to perform energy detection: this enables the creation of a side channel where information is transmitted by adjusting the length of normal packets, and received by observing the energy level on the RF channel.

A universal side channel between wireless devices. Essentially, CTC schemes based on packet-level modulation create and exploit a mutually-available side channel between wireless devices using heterogeneous standards, but operating on the same ISM bands. The basic observation is that almost any wireless device has the ability to transmit payloads of arbitrary length and to perform energy detection (*e.g.,* in order to perform a clear channel assessment). This can be exploited to transmit information by adjusting the length of legitimate packets, and to receive data by observing the energy level on the RF channel through high-frequency RSS sampling, as illustrated in Fig. 1. `X-Burst`, for example, is a portable CTC framework designed in our group that exploits this principle to convey information between heterogeneous IoT devices by sending and receiving precisely-timed energy bursts [24]. One just needs to agree on a common RF channel where to exchange cross-technology frames and on a shared alphabet to encode and decode information[7]. We have successfully implemented `X-Burst` on several off-the-shelf IoT platforms operating in the 2.4 GHz ISM band, *e.g.,* the Raspberry Pi 3B+, the Zolertia Firefly, the TI CC2650 Launchpad and SensorTag, the Nexus 6P smartphone, the Nordic Semiconductor nRF52840DK, the TelosB node, as well as the Silicon Labs EFR32 Thunderboard Sense [8, 9]. All these devices can exchange broadcast packets among each other at data rates of approximately 1 kbps; all of this despite being a mixture of IoT platforms supporting either BLE, IEEE 802.15.4, or Wi-Fi, which are incompatible wireless standards by default. This shows the generality of this CTC approach, and the potential that `X-Burst` has in enabling a universal side channel between legacy IoT devices operating on the same frequency bands.

5 LEVERAGING CTC TO ENABLE SUPPORT FOR LEGACY IOT DEVICES

In light of the proliferation of IoT systems becoming obsolete or no longer compatible with the latest communication standards, CTC may play a crucial role to prolong the usable lifetime of legacy devices. Indeed, as described in Sect. 3, the ability to establish a communication channel that is common to older and newer wireless technologies would be key in prolonging the lifespan of many IoT devices that would normally be tossed due to an early obsolescence.

Consider, for example, the case in which CTC functionality (*i.e.,* the transmission and reception of cross-technology frames) coexists in parallel with the normal communications of an IoT device, as illustrated in Fig. 2. Essentially, each IoT device is enriched with an add-on feature giving it the ability to interact with any nearby device operating on the same frequencies using CTC alongside its normal operations. With such functionality, the smart smoke detector illustrated in Example **A** could now directly exchange data to a modern smart speaker using CTC. The smart speaker would communicate with modern IoT devices using its latest technology `B`; but would also reuse a portion of its radio's idle time to exchange cross-technology frames with surrounding legacy appliances. Similarly, the set of heterogeneous dismissed smart sensors illustrated in Example **B** could now use CTC to establish a "common language" with other legacy devices to build a large-scale mesh network.

[7]The alphabet specifies how symbols are mapped to a predefined set of burst lengths, and is derived based on the characteristics of the communicating devices, *e.g.,* the time granularity, the RSS sampling rate, and the response time of the radio to a command.

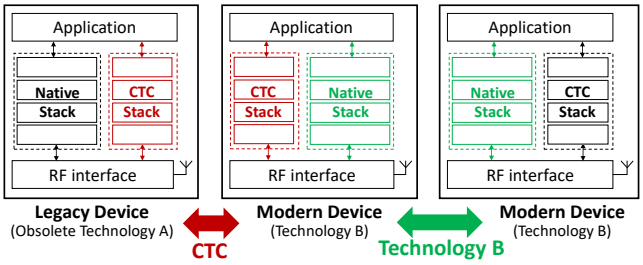

Figure 2: Leveraging CTC to support legacy IoT devices. By enriching each IoT device with an additional stack supporting CTC, a newer IoT device can establish a universal communication channel with any legacy device operating on the same frequencies.

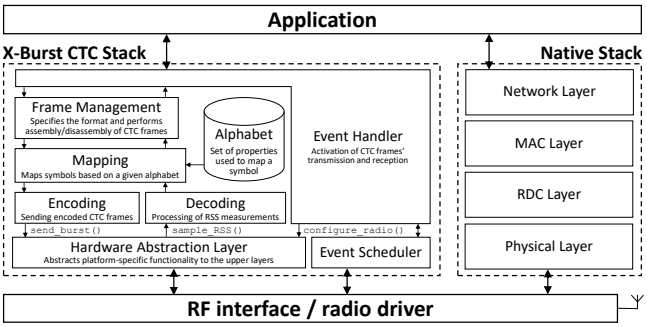

Figure 3: Overview of the `X-Burst` CTC framework. Its modularity reduces the complexity of CTC implementations, maximizes the code reuse, and simplifies the development of new functionality.

Supporting a dual network stack. In order to realize this vision, IoT devices need to embed a CTC stack alongside their native network stack. Our work on `X-Burst` allows exactly this [24], as it offers a modular framework enabling a seamless transmission and reception of cross-technology frames alongside the traditional stack of a device, as illustrated in Fig. 3. A hardware abstraction layer separates low-level hardware-specific details from the development of the main CTC functionality (*i.e.,* the encoding/decoding of cross-technology frames according to a specific alphabet and frame format), ensuring a high portability; whereas an event scheduler coordinates CTC activities ensuring a seamless coexistence with the native communication stack of the device. We have recently showcased how to augment off-the-shelf IoT devices with `X-Burst` alongside their original operations. Specifically, we have used `X-Burst` to let a smartphone use its Wi-Fi interface to directly and simultaneously control commercial smart home devices based on BLE and IEEE 802.15.4 such as smart light bulbs and door locks without the need of any gateways and hardware modifications [9][8].

Cross-technology neighbour discovery & rendezvous. In order to exchange information with surrounding devices using CTC, the ability to autonomously discover their presence and to initiate an interaction despite the incompatible PHY is essential. To this end, we have developed `SERVOUS`, a cross-technology neighbor discovery protocol allowing low-power wireless devices using incompatible PHYs to autonomously find and directly communicate with each other, while still operating at low duty cycle [25].

[8]A demonstration video is available on YouTube at https://youtu.be/whD_H-UynJY.

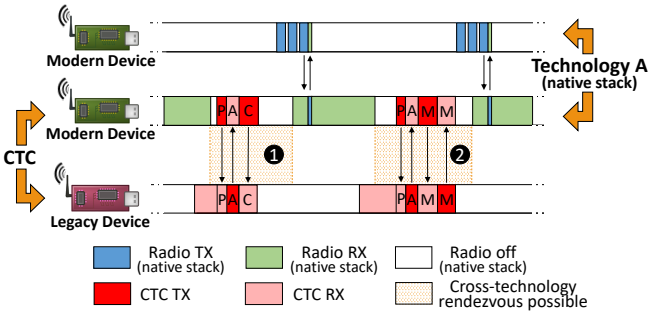

Figure 4: SERVOUS uses a receiver-initiated scheme to enable a seamless cross-technology neighbour discovery and rendezvous. CTC operations in SERVOUS are only carried out when a device radio would otherwise be idle, which avoids interference with the operations of the native communication stack.

SERVOUS reuses a portion of the time during which a device radio is idle to exchange cross-technology frames with surrounding appliances, *i.e.,* without affecting the operations of the native stack. As illustrated in Fig. 4, SERVOUS makes use of a receiver-initiated scheme in which a device periodically sends cross-technology probes (P) to announce its readiness to receive cross-technology frames. In this exemplary case, a modern device broadcasts a probe to announce its presence to nearby devices ❶. A legacy device keeps its radio on at regular intervals to discover any surrounding devices willing to communicate with CTC. After the reception of P, the legacy device adds the modern device in its neighbour table and acknowledges the reception of its probe (A). In answer to the acknowledgement (which contains information about the legacy device and its configuration), the modern device transmits back an additional cross-technology frame with details about its configuration (C). With this information, which contains among others, the device address, the protocol being employed, and the duty cycle configuration, the two devices know how often and for how long to listen for cross-technology probes to successfully establish a rendezvous to exchange data (M). The latter also takes place only during the time in which the device radio is normally idle ❷. Furthermore, SERVOUS exploits the Chinese remainder theorem to determine the minimum amount of idle time that needs to be reused to *guarantee* a cross-technology rendezvous, and can adjust itself to maximize energy efficiency while satisfying specific application requirements on responsiveness, as described in [25].

Next steps. X-Burst and SERVOUS can hence play a crucial role in leveraging CTC to support legacy IoT devices based on the concept proposed in Fig. 2. To this end, an important aspect that still needs to be addressed is the *security* of the CTC connection, as real-world use of this technology requires mechanisms providing both authentication and encrypted communication. While, in principle, traditional solutions can be adopted also for CTC (e.g., solutions used to secure IoT systems based on BLE mesh or ZigBee), it is important to investigate more efficient schemes tailored to the CTC context and its limitations (*e.g.,* accounting for the lengthiness of burst transmissions and for the easy manipulation of burst durations). This aspect started to attract the attention of the community only recently [62, 67] and is an interesting direction for future work.

Another fundamental assumption behind the concept proposed in Fig. 2 is the existence of a common application layer that is well-understood across all devices. A few efforts in this regard have emerged recently, *e.g.,* new connectivity standards increasing compatibility among smart home products such as CHIP[9]. This is promising in order to rely on predefined, mutually available commands and device addresses: we will investigate how to incorporate these efforts with our solutions in future work.

6 CONCLUDING REMARKS

With the growing number of IoT devices being manufactured and commercialized, it becomes increasingly important to provide solutions enabling the design of sustainable IoT systems. Whilst the re-characterization of IoT objects as spimes [50] and the ongoing research on reconfigurable and adaptable IoT hardware and software components [2, 43] will play a crucial role in this regard, it is also important to study how to increase the lifetime of IoT devices that have become obsolete or no longer compatible with the latest communication standards, so to prevent an early disposal.

In this paper, we discuss the potential of cross-technology communication in this regard, arguing that it could enable a seamless support for legacy IoT devices without the need of hardware modifications. Although the practicability of the concept illustrated in this paper is arguably a long shot, we hope that this paper serves as a springboard for the community to investigate the problem and to come up with effective solutions, towards a more sustainable IoT.

REFERENCES

[1] 2018. CHIP – Project Connected Home over IP. [Online] https://github.com/project-chip/connectedhomeip – Last access: 2021-04-30.
[2] E. Aras, S. Delbruel, F. Yang, W. Joosen, and D. Hughes. 2021. Chimera: A Low-Power Reconfigurable Platform for Internet of Thing. *ACM Transactions on Internet of Things* 2, 2 (2021).
[3] R. Arias, K.L. Lueth, and A. Rastogi. 2018. The Effects of the Internet of Things on Sustainability. [Online] https://iot-analytics.com/effect-iot-sustainability/ – Last accessed: 2021-04-30.
[4] F. Baquedano, C. Christensen, K. Ajewole, and J. Beckman. 2020. International Food Security Assessment. [Online] https://www.ers.usda.gov/publications/pub-details/?pubid=99087 – Last accessed: 2021-04-30.
[5] J. Bauer and N. Aschenbruck. 2018. Design and Implementation of an Agricultural Monitoring System for Smart Farming. In *Proce. of the IoT Vertical and Topical Summit on Agriculture*. IEEE, 1–6.
[6] C.A. Boano, K. Römer, R. Bloem, K. Witrisal, M. Baunach, and M. Horn. 2016. Dependability for the Internet of Things – From Dependable Networking in Harsh Environments to a Holistic View on Dependability. *Elektrotechnik & Informationstechnik* 133, 7 (2016), 304–309.
[7] M. Brown. 2019. Apple, Google and Amazon's Plan could finally end the Smart Home Nightmare. [Online] https://bit.ly/3hYX0S2 – Last access: 2021-04-30.
[8] H. Brunner, R. Hofmann, M. Schuß, J. Link, M. Hollick, C.A. Boano, and K. Römer. 2020. Cross-Technology Broadcast Communication between Off-The-Shelf Wi-Fi, BLE, and IEEE 802.15.4 Devices. In *Proc. of the 17th EWSN Conference, demo session*. 176–177.
[9] H. Brunner, R. Hofmann, M. Schuß, J. Link, M. Hollick, C.A. Boano, and K. Römer. 2021. Leveraging Cross-Technology Broadcast Communication to build Gateway-Free Smart Homes. In *Proc. of the 17th SECON Conference*. IEEE.
[10] B. Buntz. 2019. How IoT Technology Can Help the Environment. [Online] https://www.iotworldtoday.com/2019/12/19/how-iot-technology-can-help-the-environment/ – Last accessed: 2021-04-30.
[11] M. Cattani, C.A. Boano, D. Steffelbauer, S. Kaltenbacher, M. Günther, K. Römer, D. Fuchs-Hanusch, and M. Horn. 2017. Adige: An Efficient Smart Water Network based on Long-Range Wireless Technology. In *Proc. of the 3rd CySWATER Workshop*. ACM, 3–6.

[9] Connected Home over IP (CHIP) is an ongoing standardization effort launched, among others, by Amazon, Apple, Google, Comcast, and the Zigbee Alliance that aims to design a specialized application layer protocol for constrained devices to achieve interoperability in the context of smart home automation systems [1].

[12] K. Chebrolu and A. Dhekne. 2009. Esense: Communication through Energy Sensing. In *Proc. of the 15th MobiCom Conference*. ACM, 85–96.

[13] K. Chebrolu and A. Dhekne. 2013. Esense: Energy Sensing-Based Cross-Technology Communication. *IEEE Transactions on Mobile Computing* 12, 11 (2013), 2303–2316.

[14] Y. Chen, M. Li, P. Chen, and S. Xia. 2019. Survey of Cross-Technology Communication for IoT Heterogeneous Devices. *IET Communications* 13, 12 (2019).

[15] Z. Chi, Y. Li, H. Sun, Y. Yao, Z. Lu, and T. Zhu. 2015. B2W2: N-way Concurrent Communication for IoT Devices. In *Proc. of the 14th SenSys Conference*. ACM, 245–258.

[16] Cisco Systems Inc. 2016. Internet of Things: Connected means Informed. [Online] https://bit.ly/2vpGRxp – Last accessed: 2021-04-30.

[17] A. D'mello. 2019. IoT: Where are we going wrong? [Online] https://www.iot-now.com/2019/06/11/96471-iot-going-wrong/ – Last accessed: 2021-04-30.

[18] P. Gawłowicz, A. Zubow, and A. Wolisz. 2018. Enabling Cross-technology Communication between LTE Unlicensed and WiFi. In *Proc. of the 37th INFOCOM Conference*. IEEE, 144–152.

[19] A. Gilbert. 2016. The Time that Tony Fadell Sold me a Container of Hummus. [Online] https://arlogilbert.com/the-time-that-tony-fadell-sold-me-a-container-of-hummus-cb0941c762c1 – Last accessed: 2021-04-30.

[20] T. Green. 2019. The Greatest Barrier to 'Smart Home' Adoption is Complexity. [Online] https://www.strata-gee.com/the-greatest-barrier-to-smart-home-adoption-is-complexity-new-study-shows/ – Last access: 2021-04-30.

[21] X. Guo, Y. He, X. Zheng, L. Yu, and O. Gnawali. 2020. ZigFi: Harnessing Channel State Information for Cross-Technology Communication. *IEEE/ACM Transactions on Networking* 28, 1 (2020), 301–311.

[22] X. Guo, Y. He, X. Zheng, Z. Yu, and Y. Liu. 2019. LEGO-Fi: Transmitter-Transparent CTC with Cross-Demapping. In *Proc. of the 38th INFOCOM Conference*. IEEE, 2125–2133.

[23] S. Higginbotham. 2018. The Internet of Trash: IoT Has a Looming E-Waste Problem. [Online] https://spectrum.ieee.org/telecom/internet/the-internet-of-trash-iot-has-a-looming-ewaste-problem – Last accessed: 2021-04-30.

[24] R. Hofmann, C.A. Boano, and K. Römer. 2019. X-Burst: Enabling Multi-Platform Cross-Technology Communication between Constrained IoT Devices. In *Proc. of the 16th SECON Conference*. IEEE, 1–9.

[25] R. Hofmann, C.A. Boano, and K. Römer. 2021. SERVOUS: Cross-Technology Neighbour Discovery and Rendezvous for Low-Power Wireless Devices. In *Proc. of the 18th EWSN Conference*. 151–162.

[26] IHS Markit. 2017. The Internet of Things: A Movement, not a Market. [Online] https://cdn.ihs.com/www/pdf/IoT_ebook.pdf – Last accessed: 2021-04-30.

[27] W. Jiang, S.M. Kim, Z. Li, and T. He. 2018. Achieving Receiver-Side Cross-Technology Communication with Cross-Decoding. In *Proc. of the 24th MobiCom Conference*. ACM, 639–652.

[28] W. Jiang, Z. Yin, R. Liu, Z. Li, S.M. Kim, and T. He. 2017. BlueBee: a 10,000x Faster Cross-Technology Communication via PHY Emulation. In *Proc. of the 15th SenSys Conference*. ACM, 1–13.

[29] N. Joshi. 2019. How IoT And AI Can Enable Environmental Sustainability. [Online] https://www.forbes.com/sites/cognitiveworld/2019/09/04/how-iot-and-ai-can-enable-environmental-sustainability/ – Last accessed: 2021-04-30.

[30] S.M. Kim and T. He. 2015. FreeBee: Cross-Technology Communication via Free Side-Channel. In *Proc. of the 21st MobiCom Conference*. ACM, 317–330.

[31] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas. 2017. DDoS in the IoT: Mirai and other Botnets. *IEEE Computer Journal* 50, 7 (2017), 80–84.

[32] A. Langiu, C.A. Boano, M. Schuß, and K. Römer. 2019. UpKit: An Open-Source, Portable, and Lightweight Update Framework for Constrained IoT Devices. In *Proc. of the 39th ICDCS Conference*. IEEE, 2101–2112.

[33] Z. Li and Y. Chen. 2020. BLE2LoRa: Cross-Technology Communication from Bluetooth to LoRa via Chirp Emulation. In *Proc. of the 17th SECON Conference*. IEEE, 1–9.

[34] Z. Li and Y. Chen. 2020. BlueFi: Physical-layer Cross-Technology Communication from Bluetooth to WiFi. In *Proc. of the 40th ICDCS Conference*. IEEE, 399–409.

[35] Z. Li and T. He. 2017. WEBee: Physical-Layer Cross-Technology Communication via Emulation. In *Proc. of the 23rd MobiCom Conference*. ACM, 2–14.

[36] R. Liu, Z. Yin, W. Jiang, and T. He. 2021. WiBeacon: Expanding BLE Location-Based Services via WiFi. In *Proc. of the 27th MobiCom Conference*. ACM, 83—-96.

[37] M. Maheswaran. 2020. Why The IoT Will Save Our Natural Resources. [Online] https://www.forbes.com/sites/forbestechcouncil/2020/02/21/why-the-iot-will-save-our-natural-resources/ – Last accessed: 2021-04-30.

[38] N. Mancosu, R.L. Snyder, G. Kyriakakis, and D. Spano. 2015. Water Scarcity and Future Challenges for Food Production. *Water* 7, 3 (2015), 975–992.

[39] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella. 2019. IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. *IEEE Internet of Things Journal* 6, 5 (2019), 8182–8201.

[40] Y. Pan, S. Li, B. Li, Y. Zhang, Z. Yang, B. Guo, and T. Zhu. 2020. CDD: Coordinating Data Dissemination in Heterogeneous IoT Networks. *IEEE Communications Magazine* 58, 6 (2020), 84–89.

[41] J. Polastre, R. Szewczyk, and D.E. Culler. 2005. Telos: Enabling Ultra-Low Power Wireless Research. In *Proc. of the 4th IPSN Symposium*. IEEE, 364–369.

[42] P.P. Ray, M. Mukherjee, and L. Shu. 2017. Internet of Things for Disaster Management: State-of-the-Art and Prospects. *IEEE Access* 5 (2017), 18818–18835.

[43] L. Ribeiro, F. Schlager, and M. Baunach. 2020. Towards Automatic SW Integration in Dependable Embedded Systems. In *Proc. of the 17th EWSN Conference*. 85–96.

[44] E. Ronen, C. O'Flynn, A. Shamir, and A. Weingarten. 2017. IoT Goes Nuclear: Creating a ZigBee Chain Reaction. In *Proc. of the IEEE SP Symposium*. IEEE, 195–212.

[45] I. Rüb, S. Acedański, and K. Iwanicki. 2018. Ad Hoc 802.11-802.15.4 Crosstalk-Based Communication in Practice. In *Proc. of the 3rd MadCom Workshop*. 239–244.

[46] J. Shi, D. Mu, and M. Sha. 2019. LoRaBee: Cross-Technology Communication from LoRa to ZigBee via Payload Encoding. In *Proc. of the 27th ICNP Conference*. IEEE, 1–11.

[47] M. Singh, P. Leu, and S. Capkun. 2019. UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks. In *Proc. of the 26th NDSS Symposium*. USENIX Association.

[48] P. Staples. 2019. There's A Massive Barrier To Entry For IoT Companies. Here's Why Most Fail. [Online] https://about.crunchbase.com/blog/why-most-iot-internet-of-things-companies-fail/ – Last accessed: 2021-04-30.

[49] T.G. Stavropoulos, A. Papastergiou, L. Mpaltadoros, S. Nikolopoulos, and I. Kompatsiaris. 2020. IoT Wearable Sensors and Devices in Elderly Care: A Literature Review. *Sensors* 20, 10 (2020).

[50] M. Stead, P. Coulton, J. Lindley, and C. Coulton (Eds.). 2019. *The Little Book of Sustainability for the Internet of Things*. PETRAS National Centre of Excellence for IoT Systems Cybersecurity.

[51] M. Stocker, B. Großwindhager, C.A. Boano, and K. Römer. 2020. Towards Secure and Scalable UWB-based Positioning Systems. In *Proc. of the 17th MASS Conference*. IEEE, 247–255.

[52] Y. Strengers. 2013. *Smart Energy Technologies in Everyday Life: Smart Utopia?* Palgrave Macmillan.

[53] United Nations. 2017. World Population Ageing, Document ST/ESA/SER.A/397. [Online] https://www.un.org/en/development/desa/population/publications/pdf/ageing/WPA2017_Highlights.pdf – Last accessed: 2021-04-30.

[54] United Nations – Department of Economic and Social Affairs Sustainable Development. 2015. Transforming our World: the 2030 Agenda for Sustainable Development. [Online] https://sdgs.un.org/2030agenda – Last accessed: 2021-04-30.

[55] X. Vilajosana, C. Cano, B. Martínez, P. Tuset, J. Melià, and F. Adelanta. 2018. The Wireless Technology Landscape in the Manufacturing Industry: A Reality Check. *CORR – arXiv preprint 1801.03648* (2018).

[56] Virgil's Utopia. 2019. The Silent Extinction of IoT Startups. [Online] https://medium.com/@virgil.utopia/the-silent-extinction-of-iot-startups-767c08773c9a – Last accessed: 2021-04-30.

[57] W. Wang, T. Xie, X. Liu, Y. Yao, and T. Zhu. 2019. ECT: Exploiting Cross-Technology Transmission for Reducing Packet Delivery Delay in IoT Networks. *ACM Transactions on Sensor Networks* 15, 2 (2019).

[58] L. Watson. 2017. 15 Idiotic Internet of Things Devices Nobody Asked For. [Online] https://gizmodo.com/15-idiotic-internet-of-things-devices-nobody-asked-for-1794330999 – Last accessed: 2021-04-30.

[59] World Economic Forum. 2018. Internet of Things: Guidelines for Sustainability. [Online] http://www3.weforum.org/docs/IoTGuidelinesforSustainability.pdf – Last accessed: 2021-04-30.

[60] K. Wouk. 2019. 6 Smart Home Devices that Are Totally Useless. [Online] https://www.iottechtrends.com/useless-smart-home-devices/ – Last accessed: 2021-04-30.

[61] Z. Yin, Z. Li, S.M. Kim, and T. He. 2018. Explicit Channel Coordination via Cross-technology Communication. In *Proc. of the 16th MobiSys Conference*. ACM, 178–190.

[62] S. Yu, X. Zhang, P. Huang, and L. Guo. 2019. Secure Authentication in Cross-Technology Communication for Heterogeneous IoT. In *Proc. of the DySPAN Symposium*. IEEE, 1–2.

[63] Z. Yu, C. Jiang, Y. He, X. Zheng, and X. Guo. 2018. Crocs: Cross-Technology Clock Synchronization for WiFi and ZigBee. In *Proc. of the 15th EWSN Conference*. 135–144.

[64] Z. Yu, P. Li, C.A. Boano, Y. He, M. Jin, X. Guo, and X. Zheng. 2021. BiCord: Bidirectional Coordination among Coexisting Wireless Devices. In *Proc. of the 41st ICDCS Conference*. IEEE.

[65] T. Zachariah, N. Klugman, B. Campbell, J. Adkins, N. Jackson, and P. Dutta. 2015. The Internet of Things Has a Gateway Problem. In *Proc. of the 16th HotMobile Workshop*. ACM, 27–32.

[66] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi. 2014. Internet of Things for Smart Cities. *IEEE Internet of Things Journal* 1, 1 (2014), 22–32.

[67] X. Zhang, P. Huang, L. Guo, and Y. Fang. 2019. Hide and Seek: Waveform Emulation Attack and Defense in Cross-Technology Communication. In *Proc. of the 39th ICDCS Conference*. IEEE, 1117–1126.

[68] X. Zhang and K.G. Shin. 2013. Gap Sense: Lightweight Coordination of Heterogeneous Wireless Devices. In *Proc. of the 32nd INFOCOM Conference*. IEEE, 3094–3101.