RetroIoT: Retrofitting Internet of Things Deployments by Hiding Data in Battery Readings

Victor Ariel Leal Sobral*
University of Virginia
sobral@virginia.edu

Nurani Saoda*
University of Virginia
saoda@virginia.edu

Ruchir Shah
University of Virginia
rvs4xt@virginia.edu

Wenpeng Wang
University of Virginia
wangwp@virginia.edu

Bradford Campbell
University of Virginia
bradjc@virginia.edu

ABSTRACT

Commercial Internet of Things (IoT) deployments are mostly closed-source systems that offer little to no flexibility to modify the hardware and software of the end devices. Once deployed, retrofitting such systems to an upgraded functionality requires replacing all the devices, which can be extremely time and cost prohibitive. End users cannot generally leverage deployed infrastructure to add their own sensors or custom data. However, we observe that IoT systems sometimes report battery voltage information to the cloud, and batteries are often user-serviceable. This indicates that perturbing the battery voltage to encode customized information could be a minimally invasive method to retrofit existing IoT devices.

In this paper, we propose a new approach, RetroIoT, to encode custom commands and data into the battery voltage channel of IoT systems and retrofit devices with enhanced capabilities. RetroIoT enables this functionality by replacing the device's original battery with a controlled power supply that manipulates the input voltages of the battery terminal. RetroIoT can encode both analog values and digital symbols which are later decoded once the battery voltage readings are stored in the cloud. This retrofit data channel enables transmitting additional data, sending new metadata, and even swapping batteries for energy-harvesting. This technique requires no modification to the IoT device beyond replacing the battery. We prototype this technique using two commercial LoRa devices and one BLE device. Results show a 95th percentile channel error of only 3.96 mV and 99% successful packet decoding with digital symbols.

CCS CONCEPTS

• **Computer systems organization** → **Sensor networks**; **Embedded systems**.

KEYWORDS

IoT, Deployment, Retrofitting, Energy-harvesting

*Both authors contributed equally to this research.

ACM MobiCom '22, October 17–21, 2022, Sydney, NSW, Australia

ACM ISBN 978-1-4503-9181-8/22/10.
https://doi.org/10.1145/3495243.3560536

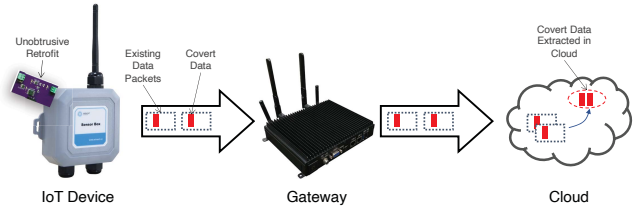

Figure 1: Many IoT devices sample and report their battery voltage, and by simply swapping the battery these devices can be repurposed to encode additional useful information. This retrofitting gives users new control to capture new data, upgrade to energy-harvesting, or strategically deactivate sensitive sensors.

ACM Reference Format:
Victor Ariel Leal Sobral, Nurani Saoda, Ruchir Shah, Wenpeng Wang, and Bradford Campbell. 2022. RetroIoT: Retrofitting Internet of Things Deployments by Hiding Data in Battery Readings. In *The 28th Annual International Conference On Mobile Computing And Networking (ACM MobiCom '22), October 17–21, 2022, Sydney, NSW, Australia.* ACM, New York, NY, USA, 13 pages.
https://doi.org/10.1145/3495243.3560536

1 INTRODUCTION

Commercial Internet of Things (IoT) systems today are commonly "walled gardens", as vendor lock-in advantages, first-to-market benefits, and interoperability overhead conspire to incentivize companies to develop their own end-to-end IoT solutions. This leads to closed-source implementations with few configurability or modification capabilities accessible to end users. As a counterpoint, open-source and maker-lead IoT platforms and systems offer significant flexibility to users and developers, with the potential for significant interoperability, but often at the cost of robustness, aesthetics, and ongoing support. Establishing design points between these extremes would enable IoT users and developers to leverage well-supported IoT infrastructure, while being able to customize their IoT systems for their own requirements and applications. Further, innovation often flourishes when open channels are introduced to previously closed systems and the broader community is able to experiment with and develop for the platform.

Enabling users to leverage the infrastructure of their existing IoT systems, including the sensors, wireless networks, gateways, cloud backends, and cloud APIs, without having to build their own devices or replicate the infrastructure could enable a series of upgrades to

Hardware Heterogeneity. Different hardware platforms may have different acceptable voltage ranges and resolutions for their battery voltage monitors. This essentially alters the data channel for the retrofit device. To accommodate this, a programmable range selector can be added to change the voltage output range. Also, using fewer voltage values could help with resilience at the expense of datarate.

Cloud API Access. We rely on the cloud API to retrieve the encoded battery voltage. For some signals, like the on-off of a button, this is likely readily available. But the battery voltage readings, may not be exposed through an API, either only used locally by the application provider or exposed only through a "battery low" alert. This limits the channels that can be used for this approach, or requires further consideration of the cloud-provided API when considering how the data to communicate is encoded. For example, a battery low alert could still be used as a low data rate channel.

Lossy Channels. The retrofit data channel may be constructed on top of a lossy underlying channel, and therefore data symbols can be lost. If the receiver is expecting to use multiple symbols to decode a packet, the protocol must handle the potential lossiness. Many standard data communication techniques could be used, including checksums and packet headers with length values.

Retrofit Synchronization. To synchronize the voltage encoder with the unmodified sensor we detect its sampling interval and only output new voltage readings before we expect the sensor to take its next reading. However, if the sensor is event-based, it may not follow a regular pattern when sending battery voltage state. This would hinder the ability to send packets of data without missing or duplicating symbols. One workaround is updating the voltage output only after a detected current spike, however, this would lead to an unpredictable datarate and perhaps stale data if events are infrequent. Some sensors both detect events and have a periodic transmission (such as a heartbeat packet), and a future version of this work could attempt to identify the regularly spaced packets and only transmit using those.

Another challenge related to our synchronization approach is that sensor devices also increase their power draw during receive mode, what could be falsely identified as a triggering event. However current peaks tend to be significantly lower for receiving modes, so the retrofit module controller can learn the IoT operation pattern and only use the highest current peaks as trigger events.

Another potential opportunity is the coupling between the energy harvesting rate of the devices in Section 6 and the datarate of the channel. More favorable harvesting conditions could lead to a better performing channel as the sensor is able to transmit more often. This increased performance may enable a secondary use of the channel and change how the energy-harvesting optimization algorithm works.

Temperature Variation Effects. Since outdoor sensor deployments can be exposed to a wide range of temperatures, more investigation is needed to understand what impact it can have on the encoder regulator retrofit. For instance, the manufacturer of the TPS784 voltage regulator indicates that the regulator output voltage accuracy varies by around 0.25 % in its recommended operation range from -55 °C to 125 °C for a 3.3 V output and 1 mA current. While the error mitigation approach presented in Section 5 is helpful to deal with voltage offset issues, fast temperature variations might result in reduced maximum achievable bandwidth.

Attack Potential. The ability to send data through the battery voltage channel, and that many devices are designed with user serviceable batteries, suggests that a possible attack vector is surreptitiously replacing the battery in the target IoT device with a "smart battery" that is controlling its own voltage output to exfiltrate data without any visual signs of tampering. The attacker would still need to be able to access the data once it is sent to the cloud, but the end-to-end attack may be feasible in conjunction with another vulnerability. Further analysis is required to understand the extent of this possible issue and future safeguards.

12 CONCLUSION

As IoT deployments grow larger in scale, designs and techniques that build on the existing device and network infrastructures can unlock many new applications and capabilities. Such design technique can not only enhance the functionality of existing systems, but also can significantly reduce the design time and developer overhead. We introduce one such technique that encodes information in the battery voltage enabling end-to-end communication, which otherwise just provides insight-less battery voltage information. We envision that this can lead to future explorations of other interesting underused channels in IoT deployments. Further, providing open and configurable channels can increase the solution flexibility and usefulness of new IoT devices and infrastructure. Open analog and digital ports and cloud API support to retrieve acquired data enable future users to customize IoT platforms for their own need at reduced cost and design effort.

13 ACKNOWLEDGEMENTS

We thank the anonymous reviewers and our shepherd for their valuable insights and feedback on improving this paper. This work was supported by the University of Virginia Strategic Investment Fund under grant SIF128, and the National Science Foundation under awards CBET-1735587 and CNS-2144940.

REFERENCES

[1] Mikhail Afanasov, Naveed Anwar Bhatti, Dennis Campagna, Giacomo Caslini, Fabio Massimo Centonze, Koustabh Dolui, Andrea Maioli, Erica Barone, Muhammad Hamad Alizai, Junaid Haroon Siddiqui, et al. 2020. Battery-less zero-maintenance embedded sensing at the mithræum of circus maximus. In *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*. 368–381.
[2] Analog Devices. 2015. TMP37. https://www.analog.com/en/products/tmp37.html.
[3] Awair. 2021. Awair Glow C . https://www.getawair.com/.
[4] Bosch-Connectivity. 2020. 3 Examples of How to Retrofit IoT Sensor Devices. https://www.bosch-connectivity.com/newsroom/blog/3-examples-of-how-to-retrofit-iot-sensor-devices/.
[5] Decentlab. 2018. Soil moisture and temperature profile sensor. https://cdn.decentlab.com/download/datasheets/Decentlab-DL-SMTP-datasheet.pdf.
[6] Dragino. 2021. LoraWan Door Sensor . https://www.dragino.com/downloads/downloads/LoRa_End_Node/LDS01/Datasheet_LDS01_Door_Sensor.pdf.
[7] Bruno V Guerreiro, Romulo G Lins, Jianing Sun, and Robert Schmitt. 2018. Definition of Smart Retrofitting: First steps for a company to deploy aspects of Industry 4.0. In *Advances in Manufacturing*. Springer, 161–170.
[8] Josiah Hester, Lanny Sitanayah, and Jacob Sorber. 2015. Tragedy of the coulombs: Federating energy storage for tiny, intermittently-powered sensors. In *Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems*. 5–16.
[9] Josiah Hester and Jacob Sorber. 2017. The Future of Sensing is Batteryless, Intermittent, and Awesome.