Passive Packet Sniffing Tools for Enabling Wireless Situational Awareness

Kwon Nung Choi, Harini Kolamunna, Kanchana Thilakarathna, Suranga Seneviratne, Ralph Holz, Mahbub Hassan*, Albert Y. Zomaya
The University of Sydney, * The University of New South Wales

Abstract

IoT is becoming a multi billion dollar market and has shown exponential growth in the last few years. IoT deployments targeting different application domains are being unfolded at various administrative levels such as countries, states, local councils, corporations, or even individual households. As a result, it is pivotal for government defense bodies to attain wireless situational awareness in any scenario, to profile the type of traffic and number of devices connected and their diverse activities. For corporations, these IoTs are usually connected via Low Power WAN technologies (LP-WANs) that have a low power consumption whilst supporting longer transmission ranges. LoRa (Long Range) is one of such LP-WAN technologies that has recently gained significant popularity due to its ease of deployment. For individual households, WiFi is a common WAN technology used. In this paper, we present our work on tools for passive sniffing for both WiFi and LoRa, built using off-the-shelf hardware. By solely carrying out passive measurements in a given location, our tool is able to deduce the devices connected and their activities in action for WiFi. For LoRa, our tool can provide important insights related to LoRa deployments such as available LoRa networks, deployed sensors, their make, and transmission patterns.

CCS Concepts

• **Networks** → **Network measurement**; **Sensor networks**; Network reliability; • **Computer systems organization** → **Embedded systems**.

Keywords

IoT, LoRa, LPWAN, Network Traffic Monitoring, WiFi

ACM Reference Format:
Kwon Nung Choi, Harini Kolamunna, Kanchana Thilakarathna, Suranga Seneviratne, Ralph Holz, Mahbub Hassan*, Albert Y. Zomaya, The University of Sydney, * The University of New South Wales. 2020. Passive Packet Sniffing Tools for Enabling Wireless Situational Awareness. In *Proceedings of Cyber Defence Next Generation Technology and Science Conference (DST'20).* ACM, New York, NY, USA, Article 4, 3 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

DST'20, March 2020, Brisbane, Australia

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 Introduction

Internet of Things (IoT) deployments are becoming increasingly common in multiple application domains such as smart buildings and cities, agriculture, manufacturing, transport, health care, and environmental monitoring. According to recent reports, over 25 billion IoT devices are currently connected to the Internet and expected to grow exponentially [14]. The total size of the IoT market is expected to reach 450 billion US dollars by the end of 2020 [15].

Short-range radio access for IoT devices is dominated by well-known protocols such as Bluetooth LE, WiFi, ZigBee, and Z-Wave. However, long range IoT communications with a range of tens or hundreds of kilometers need a special set of WAN protocols with minimum power usage (commonly known as LPWAN protocols) with more focus on low bit-rate periodic transfers. Such protocols include LoRa [7], NB-IoT [5], and SigFox [13]. Among these protocols, LoRa is becoming increasingly popular due to its use of an unlicensed frequency band, ease of deployment, low cost, and flexibility in choosing an operator [11]. LoRa sensors are currently used in applications in the likes of smart cities [2], agriculture and livestock management [1], transport and logistics [4], and manufacturing [3]. As of now, over 100 LoRa operators exist globally [6] and many more customer-managed gateways connect to open networks such as The Things Network (TTN).[1]

Consequently, the growth of IoT deployment calls for government bodies to have wireless situational awareness to understand the kind of wireless traffic active, as well as the number of connected sensors and their status at all times. As it is a common practice in natural disasters or tactical operations in an unfamiliar territory to conduct wireless scans and assess what kind of operational wireless infrastructure and check whether any type of communication is on-going, data gathered by such means can be crucial and provide vital information about survivors or telemetry from a region where the support or tactical teams have limited access [8].

To this end, we have built a hardware and software framework for taking passive measurements from WiFi and LoRa networks. They are built using only commodity hardware and are able to passively capture LoRa and WiFi frames in the neighbourhood. Our work on WiFi passive sniffing leverages a hierarchical approach to deduce devices in operation and their activities in action. For LoRa, we are able to enumerate and identify operational LoRa sensors in the neighbourhood, the networks they are connected to, their data transmission patterns, and activation methods. In this extended abstract, we summarise the details of the passive LoRa network situational awareness tool, the dataset, and the preliminary results.

2 Passive Sniffing Tool

Separate tools were developed for each wireless network type. WiFi network traces were captured using a Raspberry Pi 3 [12] running Kali Linux [9] using tcpdump [16] with the wireless interface in monitor mode.

[1] https://www.thethingsnetwork.org/

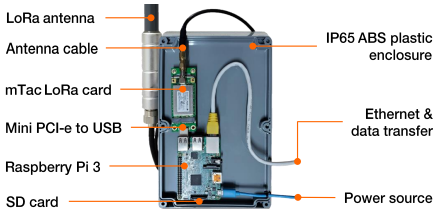


Figure 1: Breakdown of components used in *LoRadar* version 1.

For LoRa, we built a variant of an offline LoRaWAN gateway that logs all the messages sent by any LoRa sensors in range as our tool *LoRadar*, because LoRa sensors broadcast messages and any gateway in the range listening on the same frequency band is able to pick them up. Indeed as the data is encrypted with the network key, we will not be able to read the packet payload. However, for each packet, we are able to read all the information in the packet header and extract a significant amount of wireless link quality related parameters and deployment statistics. Due to the diversity in LoRa sensor and gateway hardware setups, we provide support for three types of LoRa hardware as explained in our Github repository at *https://github.com/loradar/loradar_tool*, similar to version 1 as shown in Fig. 1. Additionally, our tools support a visual representation of the collected information on a web dashboard, further detailed in our Github repository mentioned above.

3 Data Collection Methodology & Dataset

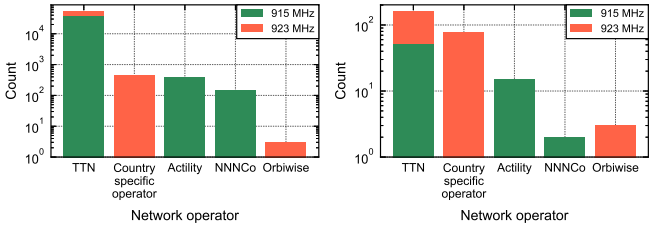
For LoRa, we validated our data extraction using 11 different LoRa sensors. We then conducted a state-wide LoRa network performance and situational awareness study deploying our tool across eight geographically distributed key locations by collecting data for one-week per location.

Based on the observed physical payload of a LoRa packet, we are able to extract message types, unique sensor identifiers, transmission frequency and time of transmission. Using this information, we are able to deduce sensor manufacturers through an online API [10], the network operator hosting the sensor, and the transmission interval.

4 Results

LoRa data analysis revealed five network operators in use, with TTN being the most popular. For the selected locations, Fig. 2 shows that more sensors are deployed on the 923 MHz frequency band compared to 915 MHz band (209 vs 69) whilst more packets are transmitted on 915 MHz (39,792 vs 14,303). Only TTN operates on both bands.

Fig. 3 presents an anonymous geographical map of the measurement locations. Highest LoRa activities and number of sensors were observed for Universities and CBD locations. *Location 3* has generated the most number of packets (approximately a few hundreds per hour) whereas most number of sensors were observed in *Location 5* (108 in total). Out of the locations where we were able to confirm the number of deployed devices through the authorities responsible, our results identified at least 84.4% of the deployed devices. In some of these locations such as location 6, inquiring the difference in the number of devices was able to help the authorities in identifying the issue of deployed devices going offline due to their batteries running out.



(a) Count of packets **(b) Count of unique sensors**

Figure 2: Observed network operators.

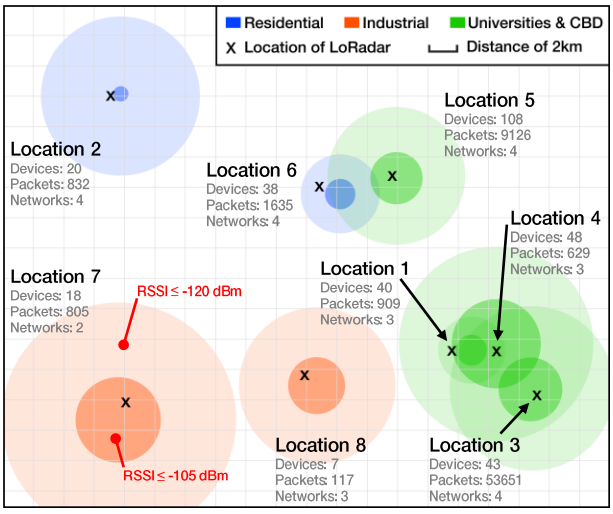


Figure 3: Geographical map of *LoRadar* measurement locations.

5 Conclusion & Future Work

To summarize, we demonstrated the feasibility of wireless situational awareness in WiFi and LoRa through passive packet sniffing using off-the-shelf hardware modules. We systematically validated the accuracy of information extraction and the robustness of the developed tool by conducting a set of experiments with real devices in controlled settings as well as with a real sensor network deployment. Our measurement results also shed light on possible security vulnerabilities and commercially sensitive information leakage through WiFi and LoRa networks. In future work, we aim to increase the portability of our tool to enable a much wider range of measurement scenarios and develop mitigation strategies to limit the sensitive information leakage and predictive nature of transmissions, using our tools to validate the proposed strategies.

References

[1] [n. d.]. Semtech and Lar.Tech Enable Smart Ranching with LoRa Technology. https://www.semtech.com/company/press/semtech-and-lar.tech-enable-smart-ranching-with-lora-technology.

[2] [n. d.]. Smart Pedestrian. https://www.liverpool.nsw.gov.au/business/innovation/smart-pedestrian.

[3] [n. d.]. Swiss Post Tests IoT LoRa Network in bid to Improve Logistics. https://internetofbusiness.com/swiss-post-to-test-iot-lora-network-to-improve-logistics/.

[4] [n. d.]. Tekelek LoRa Tank Monitoring Technology Deployed by Picoty in France. https://iotbusinessnews.com/2019/03/12/80550-tekelek-lora-tank-monitoring-technology-deployed-by-picoty-in-france/.

[5] 3GPP. [n. d.]. Standardization of NB-IOT completed. https://www.3gpp.org/news-events/1785-nb_iot_complete

[6] LoRa Alliance. [n. d.]. LoRa Alliance Passes 100 LoRaWAN Network Operator Milestone with Coverage in 100 Countries. https://lora-alliance.org/in-the-news/lora-alliance-passes-100-lorawantm-network-operator -milestone-coverage-100-countries. Accessed: 2019-05-13.

[7] LoRa Alliance Technical Committee. 2017. LoRaWAN 1.1 Specification. (2017).

[8] B. Jalaian, T. Gregory, N. Suri, S. Russell, L. Sadler, and M. Lee. 2018. Evaluating LoRaWAN-based IoT devices for the tactical military environment. In *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*. 124–128. https://doi.org/10.1109/WF-IoT.2018.8355225

[9] Kali.org. [n. d.]. Kali Linux. https://www.kali.org/. Accessed: 2019-12-23.

[10] MACVendors.com. [n. d.]. Find MAC Address Vendors. Now. https://macvendors.com/

[11] Kais Mekki, Eddy Bajic, Frederic Chaxel, and Fernand Meyer. 2019. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express* 5, 1 (2019), 1–7.

[12] Raspberrypi.org. [n. d.]. Raspberry Pi 3 Model B. https://www.raspberrypi.org/products/raspberry-pi-3-model-b/. Accessed: 2019-10-22.

[13] SigFox. 2019. Sigfox connected objects: Radio speci cations. (2019).

[14] Statista. [n. d.]. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[15] Statista. [n. d.]. Size of the IoT market worldwide from 2016 to 2020 (in billion U.S. dollars). https://www.statista.com/statistics/764051/iot-market-size-worldwide/

[16] Tcpdump.org. [n. d.]. Manpage of Tcpdump. https://www.tcpdump.org/manpages/tcpdump.1.html. Accessed: 2019-12-23.