Abstract

The growth of Internet of Things (IoT) applications underscores the need for efficient and reliable localization of end devices in Low Power Wide Area Networks (LPWANs) like LoRa. Accurate localization is vital for applications such as asset tracking, environmental monitoring, and smart agriculture. However, LoRa networks face challenges in balancing power consumption, range, accuracy, and security. Traditional GPS solutions are impractical for IoT devices due to high energy consumption and privacy concerns.

This study aims to investigate the feasibility of localizing end devices based on network traffic within LoRa networks. To achieve this, we conducted three experiments. The first experiment focused on counting the number of end devices in the network. The second experiment analyzed the communication between two WiFi devices. The final experiment involved sniffing the traffic of gateways to perform multilateration calculations using Time Difference of Arrival (TDoA) methods. Our results demonstrate that analyzing network traffic can effectively estimate the number of end devices in the network. The second experiment indicates a clear relationship between RSSI, SNR, and distance, providing valuable information on how signals degrade over distance and under various conditions. However, the final experiment revealed that even with traffic from four synchronized gateways, the TDoA-based multilateration approach did not provide the exact location of end devices.

The findings of this research are part of a self-experiment conducted to explore the interdisciplinary field between IoT and cybersecurity. A significant positive aspect of this study was the use of real data provided by The Things Industry company, enhancing the practical relevance and applicability of the results.

Keywords: Internet of Things, Cybersecurity.

1.Introduction

1.1. Goal of the thesis

In this thesis we aim at investigating techniques to localize resource constrained devices connected over LORA and forming an IoT network. LORA is a low power communication technology and in recent times has been widely adopted in many deployments due to its long-range capabilities, low energy consumption, and suitability for Internet of Things (IoT) applications. This makes it ideal for a variety of use cases, such as smart cities, agriculture, industrial automation, and environmental monitoring. LORA's ability to transmit data over several kilometers while maintaining minimal power usage allows for the creation of battery-powered devices that can operate for years without needing a recharge or replacement. Additionally, LORA operates in unlicensed frequency bands, which reduces costs and simplifies deployment. Its robust modulation technique also provides excellent resilience against interference, making it reliable even in noisy environments. Localization is an important feature of IoT deployments and it is a key building block of many applications, such as asset tracking, environmental monitoring, smart agriculture, indoor navigation, and healthcare monitoring. In asset tracking, precise location data ensures the efficient management and security of valuable resources. Environmental monitoring relies on accurate positioning to map and analyze environmental data across large areas. Smart agriculture uses localization to monitor livestock and optimize farming operations. Indoor navigation systems provide real-time location services in complex buildings, improving accessibility and user experience. In healthcare, localization enables the tracking of patients and equipment within medical facilities, enhancing patient care and operational efficiency. Furthermore, localization supports applications in smart cities, such as traffic management and public safety, and enhances the functionality of wearable devices, offering users personalized and context-aware services.

We started our investigation from a very simple, but relevant question. How to list all the devices currently connected to a specific gateway. Note that in this first question we are not interested in the exact location of the devices, but we simply aim at understanding whether they are in the proximity of the gateway. We answered this question analyzing the dataset provided by the company. For this purpose, we filtered the data based on the network to narrow the search scope. Next, we examined the traffic at each gateway within the networks. Since we couldn't use the device names as indicators, we estimated the number of devices in each network by analyzing the received frames and applying rules derived from the supervisor of the company monitoring experience. We used Google Labs and Apache Beam for this process, and the programming language was Python.

You can find more details about this experiment in the section discussing the first experiment.

Then we considered a more complex question, namely how to estimate the exact location of the device. This can be done by exploiting the information on the physical link (e.g SNR and RSSI) delivered in the LORA packet, together with some timing information to synchronize the packets. We deployed a simple testbed in which two nodes are positioned at well known distances and we estimate this distance employing the physical parameters. Given that the testing environment was indoors, we used the long-distance formula with a path loss exponent of three. The results indicate that as the physical distance increases, the potential for error in calculating the distance using the formula also increases. This is naturally due to factors that reduce the strength of the received signal.

You can find more details about this experiment in the section discussing the second experiment.

We finally tried to run a more realistic experiment - based on real logs provided us by The Things industry to multiliterate the position of a device in view of the data collected on the gateways. We attempted to check the traffic of gateways synchronized. However, the calculations made to determine the measured distance proved unreasonable, leading to the cessation of multilateration at this stage. Nonetheless, the calculations in the attached file related to the test have yielded valuable information. For instance, the filtered traffic of packets sent by a device at very close times to different gateways has enabled the calculation of TDOA.

You can find more details about this experiment in the section discussing the third experiment.