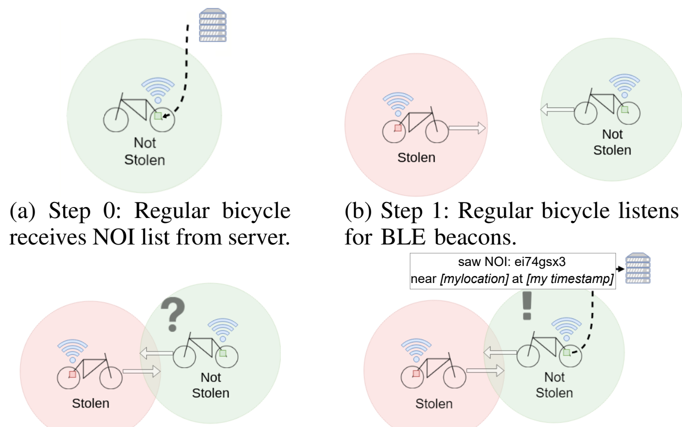
Cooperative Bicycle Localization System via Ad Hoc Bluetooth Networks

Pedro M. Santos*†, Miguel Rosa*, Luís Ramos Pinto‡ and Ana Aguiar*§
*Universidade do Porto, Faculdade de Engenharia
†CISTER Research Center, Instituto Politécnico do Porto
‡IFPN, Instituto Superior Técnico, Lisboa, Portugal; §Instituto de Telecomunicações
pss@isep.ipp.pt, up201406660@fe.up.pt, lpinto@ipfn.tecnico.ulisboa.pt, anaa@fe.up.pt

***Abstract*—Bicycles are becoming increasingly more equipped with embedded connected devices, by design or through after-market products, to support applications such as fitness monitoring and tracking. Bluetooth (BT) and BT Low Energy (BLE) technology is often embedded in such devices to support connectivity to a personal mobile device or a dock, when parked. BT/BLE transmit periodic beacons for node discovery that can be explored for V2X applications, such as safety and fleet management. We present a distributed system that explores periodic BT beacons sent by a module embedded in a bicycle to opportunistically locate nodes of interest (NOI). We address the particular application of stolen bicycle detection. In a scenario in which a bicycle is stolen and has its communication system tampered with but BLE remains functional, a service provider (e.g., fleet operator, authorities) is informed of this new NOI and shares an updated NOI list with the NOI detection-enabled bicycles. In turn, the bicycles flag contacts with stolen bicycles to the provider backoffice, at the earliest convenience (depending on available communications interfaces: immediately if cellular is available, or opportunistically when passing by a dock). We describe the operation and software architecture of the system, and an actual implementation in COTS equipment. Experimental measurements of the communication range and a demonstration of the system for proof-of-concept are also reported.**

***Index Terms*—Ad hoc Communication, Cooperative Localization, Bluetooth Low-Energy**



(a) Step 0: Regular bicycle receives NOI list from server.

(b) Step 1: Regular bicycle listens for BLE beacons.

(c) Step 2: Received beacon is from stolen bike.

(d) Step 3: Regular bicycle informs backend server.

Fig. 1: Operation of the NOI detection system.

I. Introduction

Bicycles have for long been an affordable and widely-used mobility solution, and in recent years have received renewed interest with the advent of practical battery-based solutions for assisted cycling. In parallel, a number of connected devices and gadgets can now be found in bicycles. Bicycles have been equipped with production or after-market devices that use Bluetooth/Low Energy (BT/LE) technology for integration with user devices, e.g. BT-controlled locks, digital odometers, or lights. Although not initially designed to that end, built-in communication interfaces can be explored for V2X applications. Beacons sent by BLE transceivers can be leveraged in a fashion similar to ITS-G5 CAM messages. When a bicycle receives a beacon, even if no position information is exchanged, the typically small range of Bluetooth informs that other road-user is in the vicinity of the current bicycle. This enables safety (e.g., extend the spatial awareness of cyclists) and fleet management (e.g., tracking) applications.

In this paper, we present a system that explores ad hoc BLE beacons for opportunistic identification of **Nodes of Interest** (NOI), framed in a relevant social and fleet management application: detection of stolen bicycles. Under the assumption that our distributed system has a high penetration ratio in BLE-enabled bicycles, our system will allow that a bicycle reported as stolen, and whose cellular and/or GPS systems are unavailable or have been tampered with, is identified by other legitimate BLE-enabled bicycles that receive beacons from the stolen bicycle. The receiving bicycles can check a *list of nodes of interest* (NOI list), that is stored locally or remotely and was compiled earlier by the service provider (e.g., authorities, fleet manager), and report the sighting to the service provider. The sighting report contains a timestamp of the NOI observation and the location of the legitimate bicycle, thus offering a sighting timeframe and area. The actual prediction of the stolen bicycle location can later be obtained through post processing various sightings in the server. Fig. 1 depicts how such distributed NOI detection based on ad-hoc BLE communications would operate. We report the design and architecture of the system, its implementation in a representative BLE-enabled device, an experimental characterization of its communication range and throughput, and a functional proof-of-concept.

Most works addressing the use of Bluetooth in bicycles propose its use to support a link between bicycle sensors and a personal mobile device [3], [6], [5]. An intuitive external

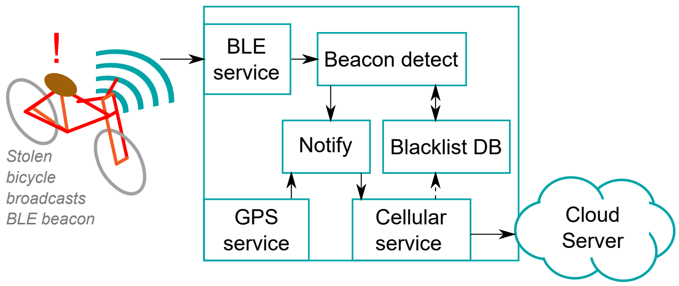


Fig. 2: Software architecture of NOI detection system.

element with which to establish a link is the dock where private of fleet bicycles rest. The authors of [4] report an air quality monitoring system installed in a fleet of bicycles, which transmit collected data is to the dock via Bluetooth. The authors of [1] propose a different use to Bluetooth beacons: as a way of differentiating mobility modes. The work closest to ours is [2]: the authors propose a theft mitigation mechanism based on Bluetooth beacons that relies on static base stations for bicycle detection. Our solution improves over this proposal as it obviates the need for any dedicated infrastructure.

The assumption that, upon theft, GPS and cellular can be made inoperative while BLE remains functional can be taken as credible considering that GPS and cellular, being long-range technologies, need to have their modules (or antennas) positioned in bicycle points with good exposure, whereas the BLE module, a close-range technology, can be installed in a different location (e.g., near wheel for rotation counting, under-seat lock).

II. Stolen Bicycle Detection System

A. Information System Context and Architecture

We consider the existence of numerous bicycles, private or belonging to a fleet, equipped with a BLE transceiver, and possibly with GPS and/or cellular interfaces. A service provider (e.g., fleet operator, authorities, or another provider) operates an information system to keep track of the bicycles (e.g., location, status, usage analytics) and issues remote commands to the monitored bicycles. The NOI detection system can be integrated in such a broader information system. The resulting system architecture is composed of two main logical components: one that runs in the embedded communication/electronics module at the bicycles (i.e., bicycle-side), and a second that runs at the service provider's cloud server.

Prior to operation of the NOI detection system, all bicycles equipped with it receive the NOI list (in this case, a list of IDs of bicycles reported as stolen) from the service provider backend server, and keep a local version of the list. The update frequency of the NOI list from the cloud server to bicycles will depend on the communication technologies the bicycle is equipped with: in real-time (e.g., via cellular), in an opportunistic fashion during transit (e.g., WiFi, Bluetooth) or when at a dock (e.g., wired). By having a local copy of NOI list (and not remote, on the backend server), the bicycle obviates the need to communicate with the backend server at every opportunistic contact. The downside is that the local copy may become outdated, but we consider that issue negligible as long as opportunities for list update remain much larger than the frequency of theft event updates.

B. Operation of the NOI Detection System

In line with the previous scenario, consider a set of bicycles equipped with BLE transceivers (that broadcast beacons periodically) and the NOI detection system. Of these bicycles, one has been reported as **stolen** to the service provider. If existing, the GPS and/or cellular communication modules may have been tampered with and are now inactive, and thus the service provider cannot communicate with it. The BLE transceiver, however, was not deactivated and continues to transmit beacons. All other BLE-enabled bicycles keep their functionalities operating normally, and are refered to as **regular**. While a regular bicycle travels around the city, it:

1) Listens to beacons of nearby bicycles;
2) Every time a new beacon is received, it inquires the local copy of the NOI list to see if the new node is stolen.
3) If so, the regular bicycle reports the finding to the backend server, geo-referrencing the encounter with its own position and current timestamp.

C. Software Architecture at the Bicycle

The bicycle-side component of the NOI detection system has the following software architecture. The embedded `BLE service` notifies a `Beacon detect` module on each beacon reception. In turn, `Beacon detect` queries the `Blacklist DB` to learn if the transmitter ID corresponds to a bicycle reported as stolen. If so, the `Notify service` informs the cloud server through the appropriate communication interface. A timestamp and GPS position are attached to the notification to identify the current whereabouts of the stolen bicycle. The `Blacklist DB` gets updated from the cloud server at the earliest convenience. Fig. 2 presents the software architecture of NOI detection system.

III. Implementation and Performance Evaluation

We implemented the NOI detection system in a representative single-board computer (SBC) equipped with a BLE transceiver. We used the SBC module Nordic Semiconductor **nRF52832**, that is built around a 32-bit ARM Cortex-M4F CPU with 512kB + 64kB of RAM, and has hardware and libraries to support operation of a BLE transceiver. We used the respective development kit, that is equipped with a filament antenna for 2.4GHz communication. The NOI software components were implemented according to the architecture described in Section II-C, in C/C++ using the respective SDK (based on the Keil uVision5 tool). The MAC ID of the BLE interface was used as unique NOI identifier of each bicycle.

We now describe the experimental characterization of the performance in terms of range and throughput of the nRF52832 module when installed on a bicycle. Although the packet reception rate would be a more insightful metric, these results provide practical insight of the range at which the NOI detection system could operate.

Fig. 3: Module encasing.

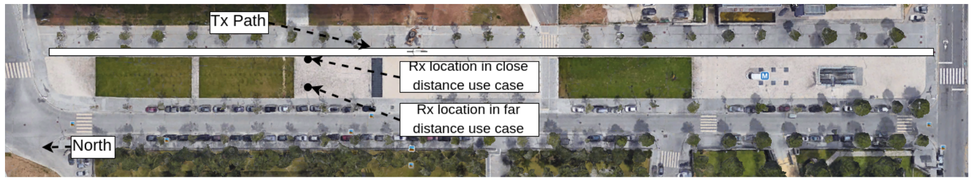
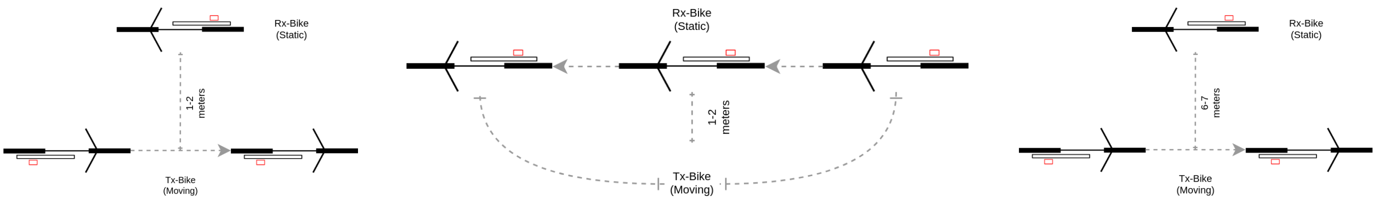


Fig. 4: Experimental setting and path.



(a) Short PD; opposite directions. (b) Short PD, same direction. (c) Large PD; opposite directions.

Fig. 5: The three parallel motion scenarios studied.

A. Methodology and BLE Parameters

We focus on scenarios of parallel interaction between two bicycles. This is inspired by typical road settings, namely two-way cycleways whose lanes are either contiguous or at the edges of roadway. One of the bicycles is kept static, while the other rides past the first. We explore three scenarios that differ in two aspects – direction of bicycle movement and perpendicular distance (PD). These are:

1) Short perpend. distance; opposite-direction motion (Fig. 5a);
2) Short perpend. distance; same-direction motion (Fig. 5b);
3) Large perpend. distance; opposite-direction motion (Fig. 5c).

These measurements were performed on a wide pedestrian area crossed by a cycle-way lengthwise and sided by two-lane road, as seen in Fig. 4. The receiving (Rx-)bicycle was kept static and the transmitter (Tx-)bicycle moved back and forth; we performed four test runs in each scenario, for statistical significance. In the third scenario, the Tx-bicycle rode aligned with the Rx-bicycle when approaching and when moving away from it, overtaking it in due time. The lateral distances between the two bicycles were one meter for the two first scenarios (to resemble a cycleway of contiguous lanes), and six meters in the third scenario (to mimic cycleway lanes at the margins of a roadway).

In these measurements, we opted to collect and present throughput samples (versus distance) instead of RSSI, as it provides a more meaningful metric for applications. If the NOI detection system is extended in the future to have more extensive data transfers, these results provide already a characterization of the attainable transfer rates with the BLE setup at hand (that RSSI alone would not provide). Currently, given that the system is based on beacons (i.e., very small management packets), very low throughput values are sufficient and the range of the NOI detection system should be close to the measured range. We defined the BLE communication parameters as follows: physical nominal connection rate of 1Mbit/s and the extended ATT payload using the feature *Data Length Extensions (DLE)* which allows a payload value up to 244 bytes. The communication flow was set to be unidirectional. The modules were set to know each other prior to the measurements, so that there is minimum connection setup delay (we find this a valid assumption given that nodes are equipped with the NOI list). Instantaneous positions were obtained with a USB GPS BU-353-S4 (one position estimate per second).

We installed the BLE module in a dedicated enclosing strapped to the bar between the seat and the cogset (shown in Fig. 3, in its encasing). This location mimics that of commercial products (e.g., dynamos and fitness monitors) that are often installed in the same bar. It was installed on the right side of the bicycle; in right-hand driving conditions, it faces outward the cycleway.

B. Experimental Results and Discussion

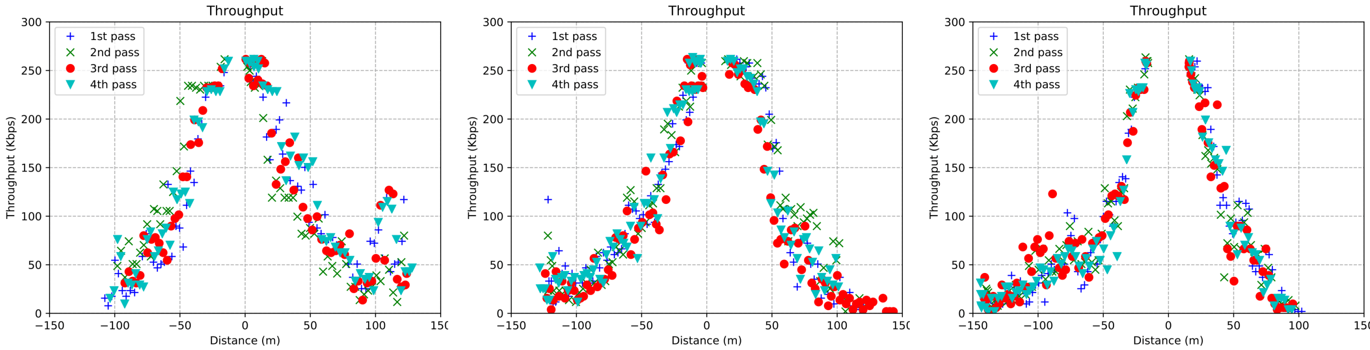
All three cases presented similar performance of the BLE link, as shown in Fig. 6. In this Figure, the X-axis increases with the motion direction: negative values refer to the area in front of the moving bicycle, and positive values to the area at the back of the moving bicycle.

Close lateral distance, opposite orientation bicycles (Fig. 6a): the maximum throughput value was around 270 kbit/s between the two bicycles and the maximum distance with connection was around 130m. The spurious values at the right end are due to insufficient cycleway range, which caused the rider to turn around.

Close lateral distance, same orientation bicycles (Fig. 6b): as in the previous case, the maximum value of throughput between the two bicycle was around 270 kbit/s and the maximum distance recorded at 140m.

Far lateral distance, opposite orientation bicycles (Fig. 6c): despite the larger perpendicular distance, the results are in line with the previous scenarios. The maximum value of throughput was 270 kbit/s and the maximum distance obtained was 150m.

These results show that the NOI detection system is able to operate in a variety of scenarios with reasonable range (around 150m in line of sight). In a parallel scenario, bicycles riding in opposite directions at 20km/h have a time frame of around 27s for a BLE beacon to be received from the stolen bicycle.



(a) Short PD; opposite directions. (b) Short PD, same direction. (c) Large PD; opposite directions.

Fig. 6: Throughput vs. distance for the parallel motion scenarios.

(a) Location of stolen bicycle. (b) Location of regular bicycle. (c) Detection of stolen bicycle.

Fig. 7: Graphical interface (L: real-time video from stolen bicycle; RT: position of bicycles; RB: console at regular bicycle).

IV. Proof-of-Concept

We prepared and showcased a proof-of-concept demonstrator of the NOI detection system (https://youtu.be/zc8JpLaUkHA). To this end, we prepared two bicycles with a nRF52832 module: one as **stolen**, equipped also with a smart phone for real-time video streaming and positioning via cellular, and a second as **regular**, with its modules connected to a laptop to report (if any) received beacons and NOI detection. In this demonstration, there was no real-time communication integration with a cloud server; it is assumed the regular bicycle has a local, up-to-date copy of the NOI list. Fig. 7 highlights moments of the demonstrator.

Step 1: The two bicycles start out of range; the location of the **stolen** and **regular** bicycles are shown in Fig. 7a and Fig. 7b, respectively.

Step 2: The **stolen** bicycle starts moving toward the **regular** bicycle casually; the live feed shows the movement.

Step 3: When in range, the regular bicycle indicates that a beacon belonging to a stolen bicycle was received – Fig. 7c.

V. Conclusion

We present a distributed system that harnesses the periodic BLE beacons transmitted by devices embedded in bicycles, for opportunistic detection of Nodes of Interest. This system is leveraged to support a relevant application: stolen bicycle localization. The legitimate bicycle's systems inspect the IDs of received beacons and report to the service provider server if a NOI is found. The bicycle-side software components and operation are described in the context of the broader cloud-enabled information architecture. We implemented the system in a representative single-board computer with BLE transceiver and stack. In a dedicated experimental campaign, we observed an operational range of 150m and maximum throughput to 270kbit/s in parallel-motion scenarios. Finally, we showcase an operational implementation of the NOI detection system on a bicycle, showing the feasibility and usefulness of the system. As future work, NOI detection could be carried out by legitimate users' smartphones.

Acknowledgment

This work is a result of projects Mobiwise (POCI-01-0145-FEDER-016426) and Generation.Mobi (POCI-01-0247-FEDER-017369), co-funded by ERDF and by Portuguese national funds (COMPETE 2020, PORTUGAL 2020), and the IT (UIDB/50008/2020) and CISTER (UIDB/04234/2020) Research Units funded by FCT/MCTES through national funds and when applicable co-funded EU funds.

References

[1] N. Bathaee, A. Mohseni, Se J. Park, J. D. Porter, and D. S. Kim. A cluster analysis approach for differentiating transportation modes using Bluetooth sensor data. *Journal of Intelligent Transportation Systems: Technology, Planning, and Operations*, 22(4):353–364, 2018.

[2] A. Bochem, K. Freeman, M. Schwarzmaier, O. Alfandi, and D. Hogrefe. A privacy-preserving and power-efficient bicycle tracking scheme for theft mitigation. *2nd IEEE Int'l Smart Cities Conference*, pages 1–4, 2016.

[3] A. Lesani and L. Miranda-Moreno. Development and Testing of a Real-Time WiFi-Bluetooth System for Pedestrian Network Monitoring, Classification, and Data Extrapolation. *IEEE Transactions on Intelligent Transportation Systems*, 20(4):1484–1496, 2018.

[4] Xiaofeng Liu, Chaosheng Xiang, Bin Li, and Aimin Jiang. Collaborative bicycle sensing for air pollution on roadway. *Proceedings - 2015 IEEE 12th Int'l Conf. on Ubiquitous Intel. and Comput.*, pages 316–319, 2016.

[5] S. Nath, S. Sinha, L. M. Gladence, Y. Bevishjinila, and V. Rajalakshmi. Health analysis of bicycle rider and security of bicycle using IoT. *Proceedings of the 2017 IEEE Int'l Conf. on Communication and Signal Processing, ICCSP 2017*, 2018-Janua:802–806, 2018.

[6] Yu X. Zhao, Yu S. Su, and Yao C. Chang. A Real-Time Bicycle Record System of Ground Conditions Based on Internet of Things. *IEEE Access*, 5:17525–17533, 2017.