Volume XXI 2018
ISSUE no.2
MBNA Publishing House Constanta 2018

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

Automatically deploy a local positioning system based on open-source software and commodity hardware

To cite this article: A. N. Atodiresei, E. Bautu, A. Bautu, Scientific Bulletin of Naval Academy, Vol. XXI 2018, pg. 194-201.

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-18-I2-025

Automatically deploy a local positioning system based on open-source software and commodity hardware

A N Atodiresei[1], E Băutu[2], A Băutu[3]

[1] Information Technology Center, "Mircea cel Bătrân" Naval Academy, Romania
[2] Dep. of Mathematics and Informatics, "Ovidius" University of Constanta, Romania
[3] Dep. of Navigation and Naval Transport, "Mircea cel Bătrân" Naval Academy, Romania

anca.atodiresei@anmb.ro, ebautu@univ-ovidius.ro, andrei.bautu@anmb.ro

Abstract. Due to the modern construction materials used (mainly steel and concrete), the GPS signal is blocked (partially or completely) in most military facilities, civilian buildings, industrial halls, etc., as well as in certain special working environments (e.g. navy, merchant and cruise ships), making GPS assistance impossible to locate and navigate within these locations. This paper presents a low-cost technical solution using free open-source software and commodity hardware that can be used to enable local positioning and navigation when needed. The system is independent of the existence of GPS signals and can be deployed automatically via a priori scripting. Therefore, it can be used indoors and as a limited-range alternative/backup for GPS systems (e.g. in case of a GPS jamming attacks).

1. Introduction

In the absence of a strong GPS signal, locating a person or object, as well as navigating between different points can be a difficult task and, depending on the environment, even dangerous.
Due to the modern construction materials used (mainly steel and concrete), the GPS signal is blocked (partially or completely) in most military facilities, civilian buildings, industrial halls, etc., as well as in certain special working environments (e.g. navy, merchant and cruise ships), making GPS assistance impossible to locate and navigate within these locations.

Moreover, even if GPS signals are normally available (i.e. not blocked due to environment factors), an industrial or military complex may become the victim of an electronic attack by jamming or spoofing the GPS signal. Both actions are simple and inexpensive, given the lack of security of the GPS eco-system and the low power of the satellite signals used for it. GPS jamming can be done using special GPS devices [1], but the attack is easy to detect, as most GPS equipment will report signal loss and stop [2]. Although the attack is easy to detect, identifying the source of jamming can be difficult, given the small size and disguised appearance of commercial jamming equipment [3]. Various technical solutions have been proposed to reduce the risks and effects of such an attack, ranging from functional optimization of the receivers [4] [5] [6] [7] to major changes to the whole GPS ecosystem [8].

On the other hand, spoofing of the satellite signal used by GPS devices is a much more difficult cybernetic attack due to the high technical level required to generate false, but still valid GPS signals [9] [10] [11] [12] [13]. However, the increased costs and technical skills required for GPS spoofing yield an attack with far more serious consequences, due to the fact that all GPS receivers will continue to operate, under attacker's control, causing false data for a good period of time in the entire IT system of the military or industrial complex under attack [10] [14].

In both situations, GPS signal jamming or spoofing, the loss caused to civilian entities by inactivity or misbehavior of electronic equipment is significant (e.g. a closed airport due to problems with navigation systems of aircrafts). In the case of military entities, such attacks are even more dangerous (e.g. misguided military weapons), up to the level of a threat to national security.

This paper presents a low-cost technical solution using free open-source software and commodity hardware that can be deployed ad-hoc to build a positioning and navigation system. The system is independent of the existence of GPS signals. Therefore, it can be used indoors, where GPS signals are usually weak. Through this system, anyone with a compatible receiving equipment (e.g. smartphone, tablet or laptop) can quickly identify their position within a building and use this navigation system (offline or online) to get navigation directions to another location within that facility. Thus, an indoor positioning and navigation system has many benefits: lower training time for beginner staff or visitors, reduce the risks of accidents by using safe routes, automate localization tasks and logistics activities, etc. With proper protection against the elements, the system can also be used outdoors, as an alternative or as backup for GPS systems (e.g. in case of a GPS jamming attack).

2. Local positioning technologies

In order to design the GPS-less local navigation system, we studied a suite of available open and commercial software and technologies, which can be combined to offer locally GPS-specific services. We also considered issues related to implementation costs, hardware availability, time required for installation and commissioning, etc. Similar to the GPS system, in order to correctly identify its location, the receiver requires input from multiple transmitters, which can use one or more communication technologies, in a homogenic or heterogenic setup. Some of the widely-available technologies that can be employed for a local positioning system include: Wi-Fi signals, Bluetooth beacons, image recognition (from simple QR codes to visual clues), or inertia measurement units (IMUs).

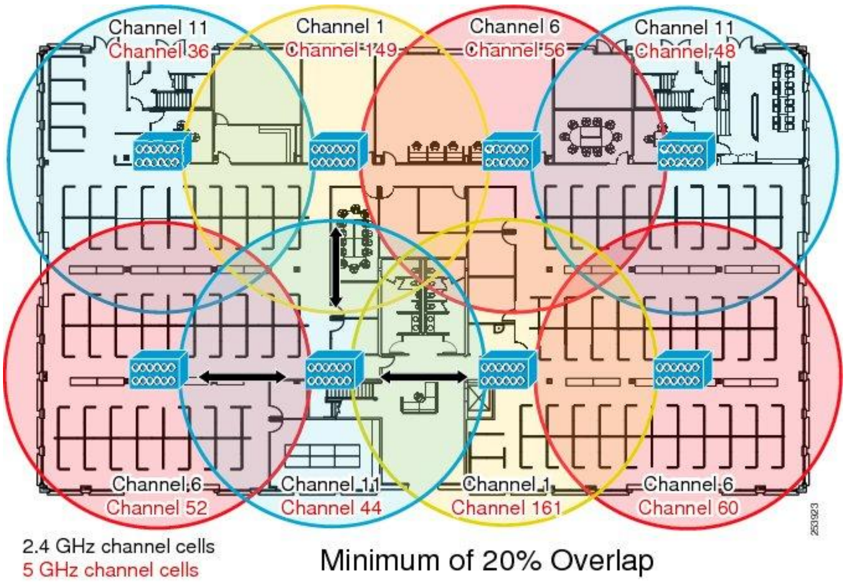

Figure 1 Example of distribution of Wi-Fi devices to cover a closed space (and minimize overlapping of the radio spectrum) [15]

Wi-Fi is a wireless radio technology for devices based on IEEE 802.11 standards [16] widely available in electronic equipment, including desktops, laptops, game consoles, smartphones, tablets, smart household devices (printers, TVs, fridges, washing machines, digital audio players), etc. Different Wi-Fi versions offer various coverage area and speeds. Currently, the most commonly used radio bands are 2.4 and 5.8 GHz, which are divided into several channels and time slots to be used "simultaneously" by multiple networks. A Wi-Fi transmitter (i.e. access point) has a range of about 20 meters indoors (or less if the walls block radio waves, like in the case of steel walls used in ships and industrial halls) and a larger range outdoors. Because Wi-Fi devices send specific, locally unique information (e.g. the MAC address, station ID), they can be used as approximate positioning markers for a positioning system (see Figure 1). Therefore, Wi-Fi access points can be used to identify checkpoints or points of interest in a wide space, but with limited accuracy due to their large coverage area.

Bluetooth beacons are hardware transmitters that transmit identification signals to nearby receivers. They use Bluetooth low-energy (LE) technology to transmit in their proximity a unique universal identifier. The identifier and any additional information can be used for indoor positioning, for tracking the movement of a device, or to trigger a location-based action on the device. Therefore, Bluetooth beacons can be used in indoor positioning systems to determine its approximate location, using a variety of setups (multiple beacons per camera, one beacon per camera, or one beacon per multiple rooms), depending on the required accuracy [17] [18] [19]. Using the Received Signal Strength Indicator (RSSI) sent by multiple beacons per room, trilateration can be used to estimate the position within 2 meters (see Figure 1). With only one beacon per room, a system can find out just an approximate current location within the building. Beacons can also be used to add checkpoints and points of interest in open spaces.

Unlike Wi-Fi and other local positioning technologies, Bluetooth beacons use unidirectional communication (from beacon to receiver), similar to the GPS system, which offers higher density of receivers and higher privacy levels for persons.

Figure 2 Example of distributing Bluetooth beacons to cover a closed space [20]

Image recognition technology allows camera-enabled devices to use visual clues (from QR codes to visual landmarks) to identity the approximate location of the receiver. The positioning accuracy of this technology varies largely to the underlying physical clues and the algorithms used for image recognition.

In general, QR codes offer the most robust image recognition positioning, with accuracies of within 1 meter, because of proximity scanning and embedded error correction codes. They can be used to add checkpoints and points of interest in an internal space of any size (small or large), similar to Bluetooth beacons, but with higher accuracy. However, unlike Bluetooth beacons and Wi-Fi hotspots, QR codes require manual interaction to scan them. They are also sensible to destruction or alteration because they need to be in an easily accessible area. Some examples of using QR codes for locating and navigating inside are found in [21] [22] [23] [24] [25].

Inertial Measurement Units (IMUs) are electronic devices that use accelerometers, gyroscopes, and/or magnetometers to measure forces, angular velocities, and/or magnetic fields. IMUs have long been used in commercial and military vehicles (such as airplanes, missiles, ships, submarines and satellites, unmanned systems, etc). Recent technological advances allowed inexpensive IMUs to be embedded in consumer electronics, such as smartphones and tablets. Therefore, IMU technology is an ideal candidate for use in indoor localization systems. A major drawback IMU-based navigation is the errors accumulated during position calculation (the system computes speed and position based on acceleration). However, other position estimation technologies such as Wi-Fi, Bluetooth beacons, or image recognition can be used to periodically adjust the position.

In conclusion, a combination of digital maps, virtual checkpoints (Wi-Fi hotspots, Bluetooth beacons, QR codes, etc), inertia measurement units, and predicted dead reckoning (PDR) algorithms, can be used for indoor and outdoor GPS-less positioning and navigation.

3. Local navigation software

Apart from the equipment used for local positioning, a local navigation system requires several software applications that collaborate to deliver the desired functionality. Although proprietary solutions are commercially available, we focused on building the entire system using open-source software that can be freely used, reviewed, modified and extended. Therefore, for our research we selected the Docker containers system, the Couchbase database engine, and the Anywhere positioning and navigation system [26]. We combined these software in order to create a local positioning system, which can be automatically deployed when needed.

Docker uses LXC (an operating-system-level virtualization technology available under Linux kernels) to run multiple isolated Linux systems (called containers) using a single Linux kernel, but also manage inter-container communication through well-defined channels. Unlike the use of physical computers, Docker containers allow configuring the entire system in a development environment and then delivering it when needed to a live environment (which has a software layer identical to the development one).

Containers also require fewer computing resources than virtual machines (VMs). It should be noted that although we used a laptop with Ubuntu/Linux for testing our system, Docker also runs on Windows, so the local positioning system we describe in this paper can be deployed in a wide variety of setups, from IoT and embedded devices, to personal computers, to cloud infrastructures.

Using Docker, we defined two containers (see Figure 3), which run the Couchbase database engine (version 5.1.1, community edition) and the Anyplace positioning and navigation software (version 3.4).

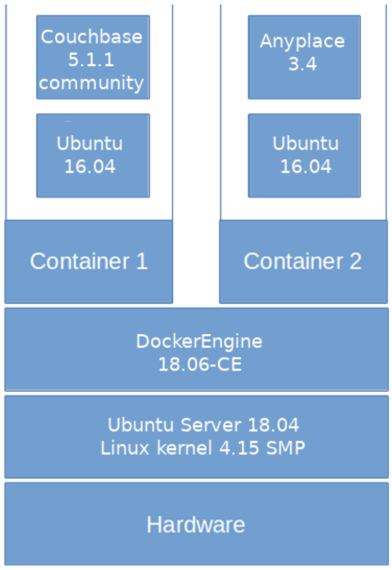

Figure 3 The software layers of the local positioning system

The Couchbase container was built using a Docker image for the Couchbase 5.1.1-community version available in the official Cockbase Docker Image Store. The Anyplace container was built using a Docker image for the Ubuntu 16.04 version available in the official Ubuntu Docker Image Store.

Manual installation and configuration of any software system requires the intervention of a qualified person and may lead to errors, which is something to be avoided in case of an emergency or for frequent uses. Therefore we have automated the configuration of Couchbase and Anywhere containers using the Dockerfiles (a special scripting language for Docker) from Figure 4 and Figure 5:

```
FROM couchbase:community-5.1.1
MAINTAINER Andrei Bautu <andrei.bautu@anmb.ro>
ARG CB_USERNAME Administrator
ARG CB_PASSWORD password
RUN /entrypoint.sh couchbase-server & && \
   couchbase-cli cluster-init --cluster localhost:8091  "--cluster-user=$CB_USERNAME" "--
cluster-password=$CB_PASSWORD" --services=data,index,query,fts --cluster-ramsize=256 --
cluster-index-ramsize=256 --cluster-fts-ramsize=256 && \
   couchbase-cli bucket-create --cluster localhost:8091 "--user=$CB_USERNAME" "--
password=$CB_PASSWORD" --bucket=anyplace --bucket-ramsize=256 --bucket-
type=couchbase && \
   couchbase-cli user-manage --cluster localhost:8091 "--user=$CB_USERNAME" "--
password=$CB_PASSWORD" --set --rbac-username anyplace --rbac-password password --
roles 'bucket_full_access[anyplace]' --auth-domain local
COPY anyplace_views /anyplace_views
RUN  cd /anyplace_views && \
   sed --in-place "--expression=s/USERNAME=\"\"/USERNAME=$CB_USERNAME/"
"--expression=s/PASSWORD=\"\"/PASSWORD=$CB_PASSWORD/"
"--expression=s/BUCKET=\"\"/BUCKET=anyplace/" create-views.sh && \
   create-views.sh && \
   kill %1
```

Figure 4 Dockerfile commands for building the Couchbase container

```
FROM couchbase:community-5.1.1
MAINTAINER Andrei Bautu <andrei.bautu@anmb.ro>
ARG CB_USERNAME Administrator
ARG CB_PASSWORD password
RUN apt-get update && \
   apt-get install -y -qq unzip openjdk-8-jre-headless && \
   apt-get autoremove && apt-get clean && \
   rm -rf /var/lib/apt/lists/* /tmp/* /var/tmp/*
RUN cd /tmp && \
   wget https://anyplace.cs.ucy.ac.cy/downloads/anyplace_v3.zip && \
   unzip anyplace_v3.zip -d /opt && \
   cd /opt/anyplace_v3-4.0/ && \
   sed                                  -i                                  -e
s/couchbase.username=\"anyplace\"/couchbase.username=\"$CB_REST_USERNAME\"/     -e
s/couchbase.password=\"\"/couchbase.password=\"$CB_REST_PASSWORD\"/
conf/application.conf
ENTRYPOINT /opt/anyplace_v3-4.0/bin/anyplace_v3
EXPOSE 9000
```

Figure 5 Dockerfile commands for building the Anywhere container

Couchbase or Anywhere containers can be easily started as required by using such Dockerfiles (to scale the entire system according to the number of users). However, we used Docker Compose, a programmable container manager, to simplify the management of the whole group of containers, virtual networks and their dependencies, via the YAML file from version: "3"

```yaml
services:
  db:
    build:
      context: ./couchbase/docker
      args:
        CB_USERNAME: Administrator
        CB_PASSWORD: password
    volumes:
      - ./couchbase/data/:/opt/couchbase/var
    ports:
      - "8091:8091"
  web:
    build:
      context: ./ anyplace/docker
      args:
        CB_USERNAME: Administrator
        CB_PASSWORD: password
    ports:
      - "9000:9000"
    volumes:
     - ./web/www/:/var/www/
    depends_on:
      - db
```

Figure 6.

```yaml
version: "3"
services:
  db:
    build:
      context: ./couchbase/docker
      args:
        CB_USERNAME: Administrator
        CB_PASSWORD: password
    volumes:
      - ./couchbase/data/:/opt/couchbase/var
    ports:
      - "8091:8091"
  web:
    build:
      context: ./ anyplace/docker
      args:
        CB_USERNAME: Administrator
        CB_PASSWORD: password
    ports:
      - "9000:9000"
    volumes:
     - ./web/www/:/var/www/
    depends_on:
      - db
```

Figure 6 YAML structure of the containerized software for the local positioning system

The Couchbase container can be preloaded with Anywhere digital maps and navigation data by mounting an existing folder with the required files inside the container under the /opt/couchbase/var directory. This step can also be automated, yielding a fully functional local positioning system up and running within minutes.

4. Conclusions

Open-source software and commodity hardware can be used to build a reliable and cost-efficient local positioning system that can be used for indoor navigation or as an alternative for GPS systems (e.g. in case of a attacks by GPS jamming or spoofing). Manual installation and configuration poses incompatibility or misconfiguration risks that should be minimized, especially when preparing for emergency or large scale deployments. Therefore, we use Docker to provide automated deployment and configuration scripts.

Acknowledgment

The work presented in this paper was partially supported by Projects no. 156 of the 2018 Research and Development Plan of the Romanian Ministry of National Defense.

References

[1] A. Pinker and C. Smith, "Vulnerability of the GPS Signal to Jamming," *GPS Solutions*, vol. 3, no. 2, pp. 19-27, 1999.

[2] J. Coffed, "The threat of gps jamming: The risk to an information utility," Report of EXELIS, 2014.

[3] R. H. Mitch, R. C. Dougherty, M. L. Psiaki, S. P. Powell and B. W. O'Hanlon, "Signal characteristics of civil GPS jammers," in *Radionavigation Laboratory Conference Proceedings*, 2011.

[4] M. J. Rezaei, M. Abedi and M. Reza Mosavi, "New GPS anti-jamming system based on multiple short-time Fourier transform," *IET Radar, Sonar & Navigation*, vol. 10, no. 4, pp. 807-815, 2016.

[5] B. R. Secrest, D. Richie and B. Rapp, "Mathematical underpinnings of crowdsource GPS jammer geolocation using signal strength readings from various locations," in *IEEE International Conference on Localization and GNSS (ICL-GNSS)*, 2017.

[6] R. L. Fante and J. J. Vacarro, "Cancellation of jammers and jammer multipath in a GPS receiver," *IEEE Aerospace and Electronic Systems Magazine*, vol. 13, no. 11, pp. 25-28, 1998.

[7] Y. D. Zhang and M. G. Amin, "Anti-jamming GPS receiver with reduced phase distortions," *IEEE Signal Processing Letters*, vol. 19, no. 10, pp. 635-638, 2012.

[8] A. J. Schneider and J. G. Small, "Airborne GPS guidance system for defeating multiple jammers". Patent U.S. Patent No. 6,300,898, 9 10 2001.

[9] C. Bonebrake and L. R. O'Neil, "Attacks on GPS time reliability," *IEEE Security & Privacy*, vol. 12, no. 3, pp. 82-84, 2014.

[10] A. J. Kerns, D. P. Shepard, J. A. Bhatti and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617-636, 2014.

[11] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon and P. M. Kintner, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Radionavigation Laboratory Conference Proceedings*, 2008.

[12] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *Proceedings of the 18th ACM conference on Computer and communications security*, 2011.

[13] D. P. Shepard, T. E. Humphreys and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attack," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 3-4, pp. 146-153, 2012.

[14] M. L. Psiaki, T. E. Humphreys and B. Stauffer, "Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies," *IEEE Spectrum*, vol. 53, no. 8, pp. 26-53,

2016.
[15] Cisco, Cisco Unified Communications System, Cisco, 2012.
[16] W. Lemstra, V. Hayes and J. Groenewegen, The innovation journey of Wi-Fi: The road to global success, Cambridge University Press, 2010.
[17] R. Faragher and R. Harle, "Location fingerprinting with bluetooth low energy beacons," *IEEE journal on Selected Areas in Communications,* vol. 33, no. 11, pp. 2418-2428, 2015.
[18] S. S. Chawathe, "Beacon placement for indoor localization using bluetooth," in *11th International IEEE Conference on Intelligent Transportation Systems*, 2008.
[19] Y. Zhuang, J. Yang, Y. Li, L. Qi and N. El-Sheimy, "Smartphone-based indoor localization with bluetooth low energy beacons," *Sensors,* vol. 16, no. 5, p. 596, 2016.
[20] Infsoft, "Indoor Positioning, Tracking and Indoor Navigation with Beacons," [Online]. Available: https://www.infsoft.com/technology/sensors/bluetooth-low-energy-beacons. [Accessed 2018].
[21] H. Zhang, C. Zhang, W. Yang and C. Y. Chen, "Localization and navigation using QR code for mobile robot in indoor environment," in *IEEE International Conference on Robotics and Biomimetics (ROBIO)*, 2015.
[22] O. Al Hammadi, A. Al Hebsi, M. J. Zemerly and J. W. Ng, "Indoor localization and guidance using portable smartphones," in *IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology (WI-IAT)*, 2012, 2012.
[23] M. Rostkowska and M. Topolski, "On the application of QR codes for robust self-localization of mobile robots in various application scenarios," *Progress in automation, robotics and measuring techniques*, pp. 243-252, 2015.
[24] P. Mirowski, T. K. Ho, S. Yi and M. MacDonald, "SignalSLAM: Simultaneous localization and mapping with mixed WiFi, Bluetooth, LTE and magnetic signals," in *International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, 2013.
[25] C. Gionata, F. Francesco, F. Alessandro, I. Sabrina and M. Andrea, "An inertial and QR code landmarks-based navigation system for impaired wheelchair users," *Ambient Assisted Living,* pp. 205-214, 2014.
[26] D. Zeinalipour-Yazti and C. Laoudias, "The Anatomy of the Anyplace Indoor Navigation Service," in *ACM SIGSPATIAL Special" (SIGSPATIAL '17)*, ACM Press, 2017, pp. 3-10.