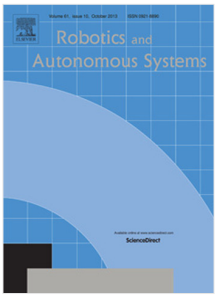

Detection of Cyber-attacks to indoor real time localization systems for autonomous robots

Ángel Manuel Guerrero-Higueras, Noemí DeCastro-García, Vicente Matellán

PII: S0921-8890(17)30283-X
DOI: https://doi.org/10.1016/j.robot.2017.10.006
Reference: ROBOT 2929

To appear in: *Robotics and Autonomous Systems*

Please cite this article as: Á.M. Guerrero-Higueras, N. DeCastro-García, V. Matellán, Detection of Cyber-attacks to indoor real time localization systems for autonomous robots, *Robotics and Autonomous Systems* (2017), https://doi.org/10.1016/j.robot.2017.10.006

Detection of Cyber-attacks to indoor real time localization systems for autonomous robots

Ángel Manuel Guerrero-Higueras[a,*], Noemí DeCastro-García[b], Vicente Matellán[a]

[a]*Research Institute on Applied Sciences in Cybersecurity, Universidad de León, Av. de los Jesuitas s/n. ES-24008 León, (Spain)*
[b]*Department of Mathematics, Universidad de León, León, (Spain)*

Abstract

Cyber-security for robotic systems is a growing concern. Many mobile robots rely heavily on Real Time Location Systems to operate safely in different environments. As a result, Real Time Location Systems have become a vector of attack for robots and autonomous systems, a situation which has not been studied well. This article shows that cyber-attacks on Real Time Location Systems can be detected by a system built using supervised learning. Furthermore it shows that some type of cyber-attacks on Real Time Location Systems, specifically Denial of Service and Spoofing, can be detected by a system built using Machine Learning techniques. In order to construct models capable of detecting those attacks, different supervised learning algorithms have been tested and validated using a dataset of real data recorded by a wheeled robot and a commercial Real Time Location System, based on Ultra Wideband beacons. Experimental results with a cross-validation analysis have shown that Multi-Layer Perceptron classifiers get the highest test score and the lowest validation error. Moreover, it is the model with less overfitting and more sensitivity for detecting Denial of Service and Spoofing cyber-attacks on Real Time Location Systems.

Keywords: Cyber-security, Indoor Positioning, Robotics, Cyber-attack, Beacon, Machine Learning

1. Introduction

Cyber-security of Cyber-physical Systems (CPSs) [1] has become an essential requirement. Specifically, cyber-security of autonomous systems is being increasingly scrutinezed [2]. It is particularly disturbing in critical areas such as medical or defense systems where security and safety problems are a growing concern [3]. Conventional Intrusion Detection Systems (IDSs) are not usually suitable for autonomous systems. They often do not take into account physical aspects, such us mobility or energy consumption. There is also an increasing interest in the cyber-security of robotic systems. For instance, [4] proposes a method based on the Cumulative Sum (CUSUM) algorithm for detecting stealthy attacks on a robotic system. In [5] a method to detect cyber-attacks on robot is proposed by using the data gathered by the on-board systems and processes to improve IDSs performance.

Real Time Location Systems (RTLSs) are critical components of many robotic systems. For example, to solve autonomous navigation in mobile vehicles, which has been one of the classical problems in robotics, RTLSs are used by robotic systems to obtain their relative position on a given map, which lets them calculate trajectories, plan next actions, etc. Several technologies have been proposed for self-locating robots. Simultaneous Localization and Mapping (SLAM) [6] has been one of the hot topics in robotics for many years (visual SLAM, laser SLAM, etc.). Although efficient algorithms have been developed to solve the SLAM problem, they demand considerable computing power, which is not usually available in commercial robots.

Many industrial applications of mobile robots relay rely on external RTLSs instead of using self-localization techniques. This makes RTLSs a vector of cyber-attacks for robotic systems. Mechanisms for detecting cyber-attacks and methods for deploying more resilient RTLSs have to be provided. Besides, these methods have to adapt to the different technologies used to implement RTLSs: Global Positioning System (GPS), UWB-based systems, ultrasound-based systems, etc.

Cyber-attacks on outdoor RTLSs have been widely reported. For instance, attacks on GPS have been recently analyzed in [7]. However, little research on cyber-security of RTLSs for indoor environments, also known as Indoor Positioning Systems (IPSs), can be found in the literature.

IPSs can be implemented using different technologies [8] and properties: time of flight, signal strength, angle of arrival, region inclusion, hop count, neighbor location, etc. Different types of attacks on these technologies have been already described [9]: forced multi-path, speedup attacks, delay transmissions, locally elevated ambient channels, jamming, replay, modify, etc. and proposes statistical methods to make localization attack-tolerant.

*Corresponding author
Email addresses: am.guerrero@unileon.es (Ángel Manuel Guerrero-Higueras), ncasg@unileon.es (Noemí DeCastro-García), vicente.matellan@unileon.es (Vicente Matellán)