LSTM-based GNSS Spoofing Detection Using Low-cost Spectrum Sensors

Roberto Calvo-Palomino
IMDEA Networks Institute
Madrid, Spain

Arani Bhattacharya*
KTH Royal Institute
Stockholm, Sweden

Gérôme Bovet
armasuisse
Thun, Switzerland

Domenico Giustiniano
IMDEA Networks Institute
Madrid, Spain

***Abstract*—GNSS/GPS is a positioning system widely used nowadays in our lives for real-time localization in Earth. This technology is highly vulnerable to spoofing/jamming attacks caused by malicious intruders. In the recent years, commodity and low-cost radio-frequency hardware have been used to interfere with the legitimate GPS signal. Existing spoofing detection solutions use costly receivers and computationally expensive algorithms which limit the large-scale deployment. In this work we propose a GNSS spoofing detection system that can run on spectrum sensors with Software-Defined Radio (SDR) capabilities and cost in the order of 20 euros. Our approach exploits the predictability of the Doppler characteristics of the received GPS signals to determine the presence of anomalies or malicious attackers. We propose an artificial recurrent neural network (RNN) based on Long short-term memory (LSTM) for anomaly detection. We use data received by low-cost SDR receivers that are processed locally by low-cost embedded machines such as Nvidia Jetson Nano to provide inference capabilities. We show that our solution predicts very accurately the Doppler shift of GNSS signals and can determine the presence of a spoofing transmitter.**

I. Introduction

Global Navigation Satellite System (GNSS) is a system that provides geo-spacial positioning based on the satellite constellation orbiting the Earth. The best known deployment is Global Positioning System (GPS) that provides time and geolocation information to GPS receivers as long as at least 4 GPS satellites are visible. GPS is widely used nowadays for both civil and military purposes. GPS is integrated on-board of aircraft, ships, probes, cars, smartphones, rescue systems, autonomous vehicles, drones, etc. Any disruption or malfunction could lead to serious problems for civil and military applications. In recent years, there has been high concern about the security of GPS signals, since it has been demonstrated that GPS is vulnerable to *spoofing/jamming* attacks where attackers can introduce fake *gps* signals [1] in the channel. Sophisticated and planned attacks to the GPS receivers can destabilize the economy of a country, besides endangering human lives. 5-days of GPS disruption could have an economical impact of 4.5 billion euros [2].

Intentional or non-intentional GPS attacks are not anymore a theoretical threat since during previous years real situations occurred in different contexts. An airport close to New Jersey (USA) could not operate for some hours due to GPS disruptions caused by an illegal GPS jamming device located in a vehicle, with main purpose of hiding the real position of the vehicle to the fleet tracking system installed in the vehicle itself. In June 2017, in the Black Sea area, more than 20 different vessels reported GPS malfunction since all of them were getting the GPS position with 25 nautical miles off. All ships were getting exactly the same location, an indicator that most probably they all were affected by a massive GPS spoofing attack. More recently, in July 2019, a probable GPS attack took place in the maritime port of Shanghai[1] where more than 100 vessels were affected by reporting wrong location. In the military context, some countries have reported that they were suffering jamming/spoofing GPS attacks during their military exercises[2].

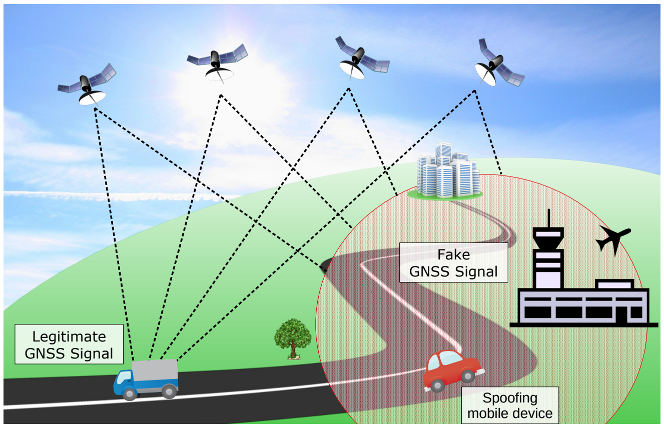

Fig. 1. A GNSS spoofing attacker can compromise wireless communications by impersonating the legitimate signal and affecting nearby infrastructures.

Fig. 1 illustrates at high level how a GPS attack can be performed. The malicious attacker only has to generate and transmit a fake GPS signal in the channel so that the power received in the target area is sufficiently higher than one received from the GPS satellite(s). In this way, the GPS receiver will take the fake signal as the legitimate one (GPS spoofing). This is easily plausible nowadays thanks to the quick rise of commodity and low-cost Software-defined radio (SDR) transceivers. For less than 300 euros is possible to acquire a full equipment of antenna and SDR

*Part of the work was done when A. Bhattacharya was a research intern in IMDEA Networks Institute, Madrid, Spain

[1] https://www.technologyreview.com/s/614689/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/

[2] https://edition.cnn.com/2018/11/14/politics/russia-nato-jamming/index.html

with transmission capabilities being able to transmit a signal in a range of 200 meters. For all these reasons, GPS attacks are real, and must be taken as a real threat in wireless communications.

In this work, we propose a GNSS spoofing detection system based on low-cost SDR receivers that are constantly monitoring the GNSS frequencies to detect anomalies and signal disruption caused by spoofing devices. We exploit the Doppler effect and its predictable pattern originated by the moving GNSS satellites to determine if the received signal belongs to the legitimate transmitter. We can generalize the Doppler shift pattern of the satellites by training a neural network (NN). Our deep learning-based solution can run efficiently in embedded systems which allows large-scale deployments, and therefore increase the system detection coverage.

II. Our Vision

We aim to create a spoofing detection system that can be used with any of the GNSS solutions available today. GNSS spoofing attacks can be performed anywhere at anytime without prior notice and during a very short time period. In addition to that, GNSS attacks usually cover a small range area. At the threats occur at the receiver side, we envision to build a collaborative large-scale GNSS monitoring system on the earth surface that leverages a large number of low-cost spectrum sensors. In particular, we envision that Radio Frequency (RF) sensors are widely spread around important infrastructures such as airports, large-dense cities, maritime ports, country borders, etc. In our envisioned system, spectrum sensors monitor GNSS channels 24/7 in real time with the aim of detecting anomalies that may derive from malicious attacks.

The solution proposed in this paper makes a first step in this direction and it aims to detect the GNSS anomaly as soon as possible keeping the computation cost low. This large-scale sensor network approach is definitely feasible for our interests as other existing initiatives already shown, such as Electrosense [3], for collaborative spectrum monitoring, and OpenSky [4] for aircraft messages collection. At a high level, this can in principle allow the system to detect any anomaly in the communications and track the spoofing device since GNSS attacks can be performed using a mobile vehicle such as cars or Unmanned Aerial Vehicle (UAV).

GNSS attacks work locally in the near area of the attacker and only GNSS receivers that are in range will be affected by the fake signal (see Fig. 1). Therefore, only sensors that are near the attacker will detect the anomaly, meanwhile other sensors out of the attacker range will receive the legitimate GNSS signal from the satellites. The fact that a multi-dense network of sensors is deployed, sensors can work collaboratively to detect and confirm anomalies reducing false positives in the spoofing device detection.

The detection stage is the first part of the system that will trigger the alarm about any suspicious symptom of the presence of a spoofing/jamming GNSS device. Only the sensors that have been able to detect the GNSS anomaly, will be the ones responsible for localizing the malicious transmitter. In this paper we focus our efforts on anomaly detection over GNSS signals, and building a solid architecture to address the localization of the spoofing device is left as future work.

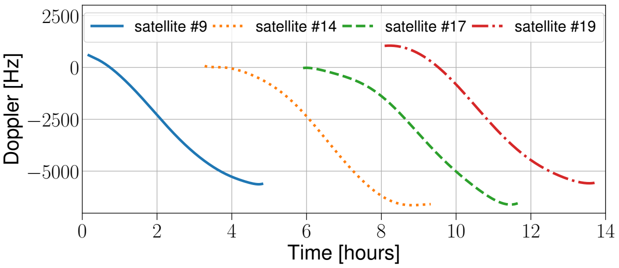

Fig. 2. Doppler shift detected by a GPS receiver observing different satellites of the constellation. [Madrid - (40.336994,-3.770459)]

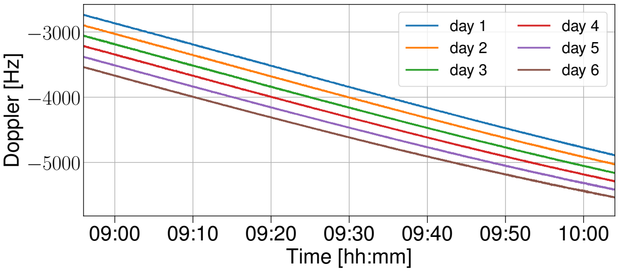

Fig. 3. Doppler shifts detected by a GPS receiver from the same satellite at same time interval along 6 adjacent days [Madrid - (40.336994,-3.770459)]

III. GNSS spoofing detection

The GNSS/GPS is a network of 31 satellites orbiting the Earth at an approximate altitude of 20.000 km distributed in such a way that at least 4 satellites are visible any point in the Earth. Each GPS satellite is transmitting a radio signal broadcasting the current time and data about its position. The satellites have a very stable atomic clock to keep a high time synchronization among them. A GPS receiver, which is monitoring multiple satellites, can estimate the distance from the satellite by analyzing the time delay between when the satellite transmits the signal and when the signal is received. Knowing the distance of at least 4 satellites, the GPS receiver can estimate its own position by applying trilateration.

One typical GPS attack is jamming by transmission of any arbitrary signal at a relatively high power. This is relatively easy to detect, and is usually done with the involvement of a hostile national authority. Other category of attacks is intentional spoofing of GPS signals. This can be done by giving a false location deliberately [1], [5]. In both cases attacker can be static or moving around the targets. We exploit the effect of imperfections in the spoofing signal to determine the presence of an anomaly.

A subset of the attacks aforementioned are not accurately detected by only looking at the Signal-to-noise ratio (SNR) of the specific signal if the spoofing is sophisticated. The common factor among all GNSS technologies that we exploit to design a spoofing detection system is that *satellites are*

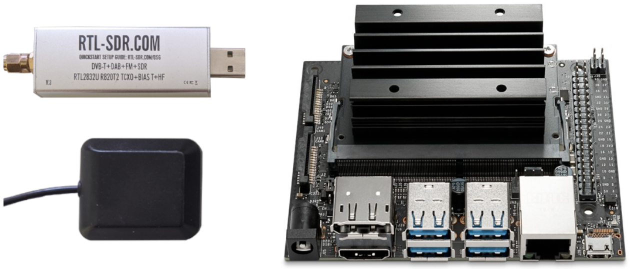

Fig. 4. GPS Spoofing detection sensor. Nvidia Jetson Nano (bottom-right) to provide inferencing capabilities locally, RTL-SDR receiver (top-left) and its active antenna (bottom-left).

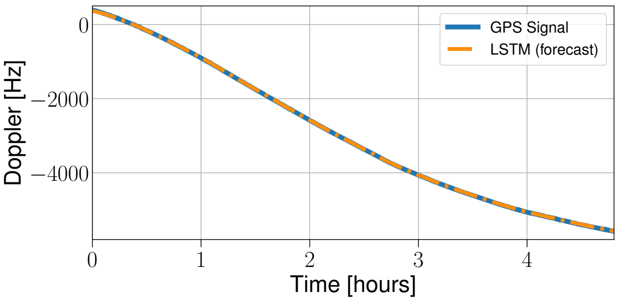

Fig. 5. LSTM forecast of Doppler shift of the satellite #3 of GPS constellation. [Madrid - (40.336994,-3770459)]

constantly orbiting the Earth along known trajectories. This generates Doppler shift *fingerprint* of the signal. The Doppler shift is the change in frequency of a signal caused because the transmitter (satellite in the legitimate case or spoofer in case of an attack) is moving. GNSS satellites are constantly moving along an orbital speed of about 14.000 km/hour. The latter creates a characteristic Doppler shift that can be observed in the GNSS receiver (as Fig. 2 shows). Therefore, for every location in Earth at every time we do know how many satellites are visible and how their Doppler shift should look like. All this information can be used to fingerprint somehow the signal received for every satellite. A potential mobile GNSS attacker will try to inject a non-legitimate signal in the channel with the proper characteristics of a GNSS signal, but it will also add the Doppler shift created by its own movement towards or around the sensors. We exploit the Doppler difference between the legitimate GNSS signal and the spoofing signal to determine the presence of a non-authorized transmitter.

We propose to use a deep learning approach to detect anomalies in the GNSS channel rather than traditional signal processing techniques. The latter requires the knowledge of the exact trajectories for the GNSS deployment under consideration, while a deep learning approach can directly exploit past Doppler measurements and the periodicity of the trajectories to train the system. We rely on Long short-term memory (LSTM) recurrent neural network (RNN) architecture to build a GNSS anomaly detector [6]. LSTM fits properly in our scenario since the Doppler shift of different satellites have similar patterns (Fig. 2) and the same satellite does not always have the same Doppler shift at the same time in consecutive days (Fig. 3) due to the inclination of GPS orbits of about 55 degrees with the Earth's equator. Our model's input is the Doppler shift of the visible satellites. This input can be obtained by measuring with a GNSS receiver or using historical data provided by the GNSS satellite networks, e.g. NASA[3] releases daily data of GPS broadcast. This data can be used by specific software[4] to generate the simulated signal and Doppler for the GPS satellites in view.

IV. Evaluation

We build a model based on 2 LSTM layers with 32 neurons, 1 dropout and 1 dense layer. The prediction of the model is built on the knowledge of the previous 50 measurements (look-back) to predict the next state. We train the network in batches of 128. We rely on Keras [7] framework to train and evaluate our model. For the training dataset we use GPS Doppler shift measurements with 5 seconds of granularity recorded in L1 channel (1575.42 MHz) during 100 days using GNSS-SDR software [8] and RTL-SDR. The training dataset could be also obtained by looking at the historical daily data provided by NASA.

A. Hardware

Since our architecture is designed to use low-cost IoT receivers to enable large-scale deployments, we rely on Electrosense [9] infrastructure to build our sensor (see Fig. 4). The low-cost sensors use the well-known RTL-SDR v3 software-defined radio as a front-end receiver. One of the peculiarities of the RTL-SDR is that includes a bias tee which can be enabled by software to power up an active antenna. The latter is very convenient for our interests since GNSS reception performs better with an active antenna. We add artificial intelligence (AI) capabilities to the Electrosense sensor by using Nvidia Jetson Nano which allows us to perform inference over deep learning models locally on the sensors. Our LSTM-based GNSS spoofing detection model can run in this sensor architecture in real time. The fact that the spoofing detection can be done locally on the sensors alleviates the communication bandwidth between sensors and the backend.

B. Results

Fig. 5 shows the Doppler shift of one satellite for one-single day in a specific position in Madrid (Spain). The same figure also shows the Doppler shift forecast computed by our model. The error of our forecasting model over the testing dataset is in the order of 0.0006%, which implies a Mean Absolute Error (MAE) of 4 Hz in the Doppler shift prediction. Therefore this model is able to forecast the Doppler shift of a GPS satellite with a very small error which allows us to determine very accurately the presence of an anomaly in the GPS channel.

[3] ftp://cddis.gsfc.nasa.gov/gnss/data/daily/

[4] https://github.com/osqzss/gps-sdr-sim

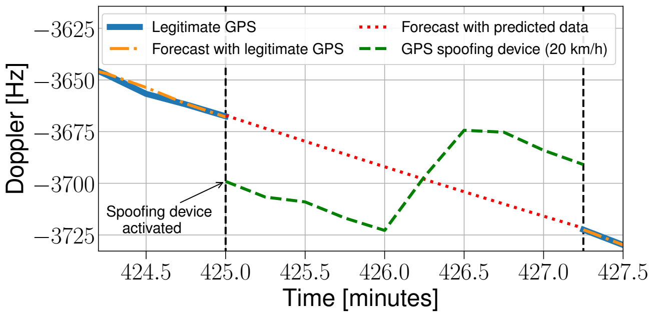

Fig. 6. Our model tracks the Doppler shift of the legitimate GPS signal. In the presence of a spoofing signal the model uses predicted data for forecasting since Doppler acquired by the receiver is not trustable anymore.

We simulate the presence of a spoofing device that is moving at 20 km/h towards the sensor transmitting a non-legitimate GPS signal to slightly change the location decoded by the receiver. Fig. 6 shows that the model is able to forecast the Doppler using the previous knowledge of the acquired data with a very small error. Then, we activate the simulated spoofing device (at minute 425 in Fig. 6) which intends to fake the GPS signal. We can observe how this spoofing signal generates a slightly different Doppler shift due to its own movement and speed. This Doppler variation can be detected by our model, which immediately starts making Doppler forecasting using only predicted data (generate by the own model) since real Doppler shift acquired by the receiver is not trustable anymore. The lower the speed of the transmitter, lower is the difference between the Doppler generated by the legitimate transmitter and the spoofing device. Our model is able to detect GPS anomalies by looking on the signal imperfections, detecting static spoofers with Doppler shift deviations higher than 4 Hz, and catching mobile spoofing devices at higher speeds of 2.5 km/h.

V. Related Work

GNSS spoofing detection has been extensively explored in the literature. Some studies utilize an array of antennas to compute the phase difference between the signals supposedly coming from different satellites. This allows them to identify if the signal is coming from a single source, which would indicate the presence of a spoofing device [10]. While this is effective in practice, such arrays of antennas can cost hundreds or even thousands of euros. This makes them infeasible to monitor the GPS signal at large scale. A second category of studies try to identify GPS jamming/spoofing only by monitoring the SNR or time difference of arrival [11]. While this can work with relatively low-cost sensors, such detection can be avoided by lowering the SNR of the spoofing signal. Additionally, SNR-based approaches largely depend on the environment and signal reflection, causing possible false positives in the detection stage. Since GPS spoofing does not necessarily require high SNR signals, this still leaves it possible to spoof GPS signals with impunity [12]. The closest related work is [13], which studies the Doppler shift to localize cellular phones from moving vehicles. However, unlike our work, it does not look for anomalies in the data, neither look at the problem of spoofing detection.

VI. Way Forward

We have proposed a LSTM-based GNSS spoofing detection model that is able to run in low-cost SDR sensors with AI capabilities, and to detect GNSS spoofing devices. Our method can complement other existing GNSS spoofing detection methods to improve the anomaly detection rate.

Anomaly detection in wireless communications is always the first step of a more complex process which aims to localize the malicious transmitter accurately and then, shut it down as soon as possible to minimize the damage caused. We will work in a collaborative sensor network where our GNSS spoofing detection sensors will be widely deployed near strategic infrastructures, and in case these anomalies are created by a malicious spoofing transmitter, localize it.

Acknowledgment

The research work at IMDEA Networks Institute was sponsored in part by armasuisse under the Cyber and Information Research Program, in part by the European Union's Horizon 2020 research and innovation programme under Grant No. 871249, and in part by the Madrid Regional Government through TAPIR-CM project S2018/TCS-4496.

References

[1] 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.

[2] *The economic impact on the UK of a disruption to GNSS. Full Report. June 2017. LE London Economics.*, 2017.

[3] S. Rajendran, R. Calvo-Palomino, M. Fuchs, B. V. den Bergh, H. Cordobés, D. Giustiniano, S. Pollin, and V. Lenders *IEEE Comm. Magazine*.

[4] M. Schäfer, M. Strohmeier, V. Lenders, I. Martinovic, and M. Wilhelm, "Bringing up opensky: A large-scale ads-b sensor network for research," in *13th international symposium on Information processing in sensor networks*, pp. 83–94, IEEE Press, 2014.

[5] 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 on Computer and communications security*, 2011.

[6] P. Malhotra, L. Vig, G. Shroff, and P. Agarwal, "Long short term memory networks for anomaly detection in time series," in *Proceedings*, vol. 89, Presses universitaires de Louvain, 2015.

[7] A. Géron, *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow.* O'Reilly Media, 2019.

[8] C. Fernandez-Prades, J. Arribas, P. Closas, C. Aviles, and L. Esteve, "Gnss-sdr: An open source tool for researchers and developers," in *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*.

[9] R. Calvo-Palomino, H. Cordobés, M. Engel, M. Fuchs, P. Jain, M. Liechti, S. Rajendran, M. Schäfer, B. Van den Bergh, S. Pollin, *et al.*, "Electrosense+: Crowdsourcing radio spectrum decoding using iot receivers," *Computer Networks*, p. 107231, 2020.

[10] P. Y. Montgomery, "Experimental results of a multi-antenna receiver defense against a portable civil gps spoofer," in *Radionavigation Laboratory Conference Proceedings*, 2011.

[11] A. Ranganathan, H. Ólafsdóttir, and S. Capkun, "Spree: A spoofing resistant gps receiver," in *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*, pp. 348–360, 2016.

[12] J. Choi, M. O. Mughal, Y. Choi, D. Kim, J. A. Lopez-Salcedo, and S. Kim, "Cusum-based joint jammer detection and localization," in *2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*.

[13] C. D. Demars, M. C. Roggemann, A. J. Webb, and T. C. Havens, "Target localization and tracking by fusing doppler differentials from cellular emanations with a multi-spectral video tracker," *Sensors*.