

# Characterizing Radar Network Traffic: a first step towards spoofing attack detection

Theobald de Riberolles, Jiefu Song, Yunkai Zou, Guthemberg Silvestre, Nicolas Larrieu

▶ **To cite this version:**

Theobald de Riberolles, Jiefu Song, Yunkai Zou, Guthemberg Silvestre, Nicolas Larrieu. Characterizing Radar Network Traffic: a first step towards spoofing attack detection. AeroConf 2020, IEEE Aerospace Conference, Mar 2020, Big Sky, United States. pp.ISBN:978-1-7281-2734-7, 10.1109/AERO47225.2020.9172292 . hal-02890995

**HAL Id: hal-02890995**
**https://enac.hal.science/hal-02890995**

Submitted on 6 Jul 2020

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Characterizing Radar Network Traffic: a first step towards spoofing attack detection

**Théobald de Riberolles, Jiefu Song**
**Activus Group, Toulouse, France**
**{theobald.deriberolles,jiefu.song}@activus-group.fr**

**Yunkai Zou, Guthemberg Silvestre, Nicolas Larrieu**
**ENAC, Université de Toulouse, France**
**{yunkai.zou,silvestre,nicolas.larrieu}@enac.fr**

***Abstract*—An Air Traffic Management (ATM) Surveillance System is used to provide services to perform Air Traffic Control (ATC) (e.g., horizontal separation between aircraft). This sytem carries messages containing aircraft's position from a collection of radars of an Air Navigation Service Provider (ANSP) through its network. Then Radar traffic is one of the most important sources of information for this system. The format of the radar messages is defined by a specific application-layer protocol entitled ASTERIX. The evolution of the security policy and technologies used makes existing radar systems, once considered safe, now potentially open to attack. Both safety and security of ATM system could be impacted by any kind of attack into the network traffic, who could maliciously modified information about aicrafts, in particular thanks to Spoofing Attack. To counter this risk, there is need to detect intrusion and then to have anomaly detection modules for this safety-critical network traffic, that can be deployed in a security appliance.**

**In order to design this module, we did a statistical analysis to have an overview of the traffic to better know what we need to protect. Specifically, we studied radar network traffic in order to extract high level statistic characteristics of normal radar traffic. This allowed us to identify a trend in the evolution of this traffic. We were then able to inject a spoofing attack (when a malicious party impersonates another device or network user for the purpose of altering the data) into this traffic to modify the nominal traffic. Thereafter, we were able to detect this attack using our method, which consists of the use of a machine learning detection method, using a Long-Short Term Memory (LSTM) mechanism.**

**This is the subject of our paper, an overview of radar traffic and a method to detect spoofing attack in this traffic. This would help to develop an ATM IDS especially as this type of attack could remain invisible for air traffic controller.**

## TABLE OF CONTENTS

1. INTRODUCTION ..... 1
2. STATE OF THE ART ..... 2
3. ATC NETWORK OPERATION ..... 3
4. OVERVIEW OF RADAR NETWORK TRAFFIC ..... 3
5. SPOOFING ATTACK DETECTION ..... 5
6. CONCLUSION AND FUTURE WORK ..... 6
7. ACKNOWLEDGMENT ..... 7
REFERENCES ..... 7
BIOGRAPHY ..... 7

## 1. INTRODUCTION

Surveillance information is the key data of the air navigation service providers, which has the goal to assure the safety of the air passengers and the functioning of Air Traffic Control (ATC). Consequently, in the ATM Surveillance System, the Radar System is one of the most important components. For doing that, an air traffic controller relies on an Air Traffic Control system which relies on radar. Airborne Control Radars are remote-sensing sensors used to locate, track and guide aircraft in the flight space around an aerodrome or in larger areas. They collect information about aircraft including its position, its speed, its identifier, the type of aircraft and everything that can be useful to a controller. When an aircraft enters a given area, it is detected by a sensor, the radar. The radar sends this information over a private network. On this network several SIRs (Server of Radar Information) send these packets to different navigation centers. In this center the track of the aircraft is rebuilt, and is displayed on a screen facing the controller to guide the planes. All these elements form the ATC system which is described in Figure 1.

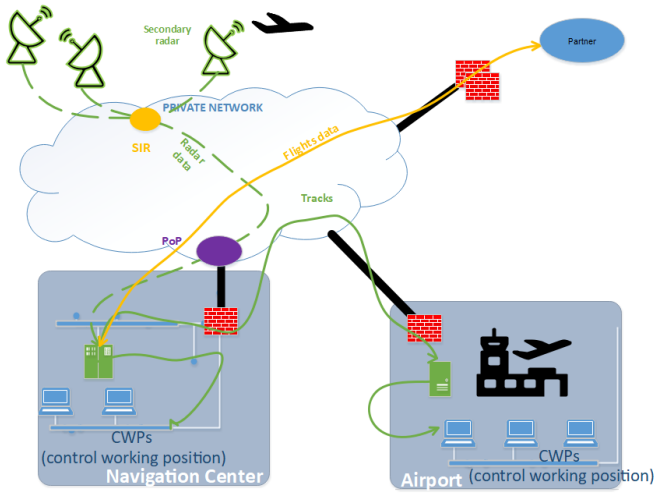



**Figure 1**. Schema of the ATC system.

By processing and correlating the information from multiple radars and flight plans in calculators in navigation centers the system provides more precise real-time positions of each aircraft and allows an air traffic controller to ensure the safety of passengers by avoiding possible collisions, and guaranteeing horizontal separation.

To transmit radar data, ATC systems use an open-source protocol to transport the radar informations, ASTERIX [1]. The informations about aircraft measurement are encapsulated in an Asterix message which is sent from the radar to the operations center. It was designed as an Application protocol of the TCP/IP model for communication media with limited bandwidth. This is why it is able to transmit all the information needed, with the smallest overhead possible. ASTERIX messages are commonly transported into either IP packets or Ethernet frames. Figure 2 depicts an overview of an Asterix message format.

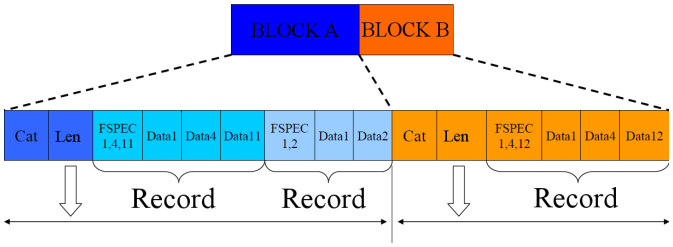



**Figure 2**. An overview of ASTERIX message format.

ASTERIX is an extensible format with different data categories. Each of them carries one type of information, such as target reports from radars, aircraft tracks, and various system status messages.

Despite the widespread use of ASTERIX messages to transport safety-critical ATM information [2], this protocol does not specify any security mechanism, which exposes the entire system to vulnerabilities. In fact, this lack of security has already been exploited by Casanovas et al. [3] who developed a tool that makes a Man In The Middle attack to manipulate ASTERIX messages. Moreover, the dependence of the global civil aviation on computer systems on a daily basis is growing as more and more modern airport and aircraft are commissioned and stakeholders are seeking to meet the growing demand for digital and computer service [4]. On the one hand, digitalization technology tools and systems enhance interoperability, but on the other hand their uses can pose serious risks to aviation cyber security. Therefore, it is necessary to maintain a high level of attention to the possible future developments of cyber-threat in this area [5]. This situation shows us that cyber-attacks are eventually possible to maliciously change the information about aircraft, especially with spoofing attacks [3]. The modification of information from a spoofing attack can be fine enough to be invisible by a human. Therefore, there is an increasing need to provide additional security mechanisms for radar data, by detecting anomalies in the system.

Despite being a open-source ASTERIX protocol,ASTERIX messages transporting ATM information are unknown by the off-the-shelf Intrusion Detection System (IDS), they are handled as conventional traffic. It is therefore necessary to learn more about these kind of messages to detect anomalies. However, to our knowledge, the literature has not yet addressed the issue. It is therefore essential to study the radar network traffic itself to have characterization of radar traffic useful for an IDS.

The paper aims to highlight characteristics from radar traffic data and to show that detecting a spoofing attack in this traffic is possible. We work with real radar traces collected inside the operational network of the French ANSP (DSNA - Direction des Services de la Navigation Aérienne).

The paper is organized as follows: a State of the art related to ATM/radar system is presented in Section 2, specificities of the radar operation are described in Section 3. In Section 4, an overview of radar traffic with the description of the dataset and a coarse-grained analysis of radar information is presented. In Section 5 an example of a spoofing attack and a method of detection is shown. Final remarks, and a word about future work conclude this paper.

## 2. State of the Art

In the literature, we find little work on radar data and the ASTERIX protocol itself. Standards developed by Eurocontrol can be found on its website[2]. The control authority presents there the protocol itself and its specification.

In the ATM field, the major research has been focused on air traffic delay or trajectory by using radar data, but less on radar network itself, as it is investigated by Bosson et al. in their paper "Supervised Learning Applied to Air Traffic Trajectory Classification" [6]. Moreover, according to Bosson et al. [6], other works focused on the anomaly detection are focused on aircraft behavior more than on the network traffic, thanks to methods based on machine learning. Bosson et al. [6] show that Gariel et al. [7] applied trajectory clustering techniques to GPS radar tracks in order to identify operational aircraft behaviors and their variability. Conde et al. [8] developed a data mining framework for air traffic flow characterization to identify aircraft trajectories and ensemble-based methods to detect flight non-conforming behaviors. Evans et al. [9] applied various data mining techniques to flight plan amendment data to train a predictor of operational acceptability for airborne reroute advisories.

Regarding air traffic data itself, there is little work about anomaly detection. In his thesis, Nanduri [10] deals with this type of anomaly detection, as detecting atypical flights and anomalies based on statistical signatures or detecting anomalies in the data in the vector space. In their document Üsing ÄSTERIX in accident investigation [11] Farrel and Schuurman explain that radar data are often used for investigation of air accidents, and discuss ASTERIX data for safety use. Nevertheless, Casanovas et al. [12] present a proof of concept about the vulnerability of the ASTERIX protocol. They were able to do Man In the Middle attack dedicated to this traffic in order to delete, modify or add aircraft in traffic. This study highlights the fact that there is a need to have additional level of security against of an attack from inside the network.

To the best of our knowledge, ours is the first study of a characterization of radar network traffic focusing on protocol itself in order to identify characteristics of traffic radar data in order to develop a security module dedicated to ASTERIX.

In this paper, we focus on a spoofing attack. A spoofing attack, is a type of Man In The Middle attack which is a type of attack in which the attacker manages to get between the transmitter and the receiver. Thereby he has the ability to read, insert and modify the messages that are being sent between the two hosts without them knowing that the link has been violated. Once the attacker is in the middle of the link, he has the capacity of sniffing and intercepting the messages that are exchanged between the victims. When he uses this position to impersonate another device or user on a network, by sending a packet in their place, by modifying or not the information, it is called a spoofing attack. There are several different types of spoofing attacks that malicious parties can use to accomplish this. Some of the most common methods include IP address spoofing attacks, ARP spoofing attacks and DNS server spoofing attacks.

[2]https://www.eurocontrol.int/services/asterix

## 3. ATC NETWORK OPERATION

Figure 1 shows schematically the operation of an ATC network. The information about aircraft is retrieved by two types of radar :

- Primary Radar: The signals are the echoes due to the reflection on the aircraft. There is no more information than the presence of the aircraft, or other physical target, on the controller's Plan View Display (PVD)
- Secondary Radar : The signals are obtained from the transponder carried on the aircraft. The radar emits several impulsions and the transponder answers to this interrogation. Depending on the mode, the transponder will give information as the position, the time, the id or other about the aircraft. Then, the radar will emit two types of messages in the network : **detection messages**, the information (horizontal/vertical location, time, id ...) given by the aircraft and **service messages** specific to its operation.

The radar encapsulates this information in an ASTERIX Packet and sends it in the operational network. From this network, the ACC retrieves radar packets about their sectors. Thanks to a calculator, they concatenate the information of the different radars visualizing the aircraft, and they obtain an accurate measurement of the aircraft. This accurate measure is sent to control working positions where they are displayed on the radar screen of the controller. Using data from flight plans, it allows the controller to do control en-route. To do control in approach, the tracks are sent from ACC to the airport, where the control is done after a passage in a new computer that compiles different data, which allows for more accurate information.

As we explain in the Introduction, an Asterix message is composed of one or more blocks of data, it is the base of ASTERIX messages. Each message contains the type of information transmitted, and the detail of the information sent by the radar.

The type of data transmitted by the protocol is standardized and classified into ASTERIX categories. The CAT identifier defines what category is used and allows us to know what kind of information is transmitted. For our case of ATC use, only two types of categories are used: the **detection categories** and the **service categories**.

- The detection categories, are for tracked plots that represent the traces of an airplane. The information transmitted in the block with these types of categories are recordings about aircraft to define a map of the sky.
- The message of service categories transmit information about the radar itself. They send information for each end of a sector (it is the coding of the antenna rotation).

With the use of Primary Surveillance Radar (PSR) and Secondary Surveillance Radar (SSR), only four categories are used:

- Two for detection: category **01** for PSR and **48** for SSR ).
- Two for messages of service: category **02** for PSR and **34** for SSR).

The specifications for the ASTERIX data categories (CAT) form part of the ASTERIX Standard Document (available through the EUROCONTROL website[3]).

[3]https://www.eurocontrol.int/services/asterix

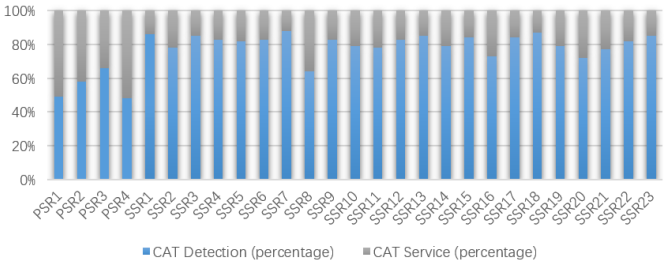



**Figure 3. Distribution of Service (red) and Detection (green) data in our dataset.**

## 4. OVERVIEW OF RADAR NETWORK TRAFFIC

*Dataset*

For this work, our dataset is a set of real radar data collected in the French ATM/ATC System. These data are data from twenty-three Secondary Surveillance Radar (SSR) and nine Primary Surveillance Radar (PSR) collected before they are processed by the calculators of the control center. We capture this data, in pcap format, from April 19, 2019 until today which represents around 200GB compressed data. The traces that can be observed, thanks to this data, are Asterix on IP or encapsulated on Ethernet.

With the ASTERIX protocol, the identifiers of the radars are represented by destination addresses, and source addresses are the last SIR (Server of Radar Information identifier), so we used Ethernet destination address to distinguish the different radars of our collection.

*Measurement methodology*

The traffic was captured with a TCPDump tool and saved in PCAP format. We used these raw files for our analysis.

We used the libpcap library to read the raw files and the ASTERIX python module developed by Damir Salantic for Croatia Control Ltd. to parse EUROCONTROL ASTERIX protocol data.

*Coarse-grained analysis of radar information*

This analysis is a coarse-grained level of analysis of our network traces. The goal of this study is to highlight the idea that there exists a recognizable trend away from our network traces which will help us to define rules/signatures about normal radar traffic.

In the radar data that we are studying, we know that there are categories of services that will regularly send messages on the operation of the radar (02 for PSR and 34 for SSR) and detection categories that will allow providing information about aircraft (01 for PSR and 48 for SSR). In our dataset, we have both PSR and SSR. When we look at the distribution of service categories and detection categories, as shown in Figure 3, we can see that the detection category is in majority. The ratios are of the order of 55% detection for 45% of services for PSR radar and of 75% detection against 25% of services for SSR radar.

Since the detection messages represent aircraft information and service messages, operating messages on the radar, we expect the proportion of the detection categories to be higher than that of the service categories, and that the data radar will contain more messages on the aircraft than on their operation.

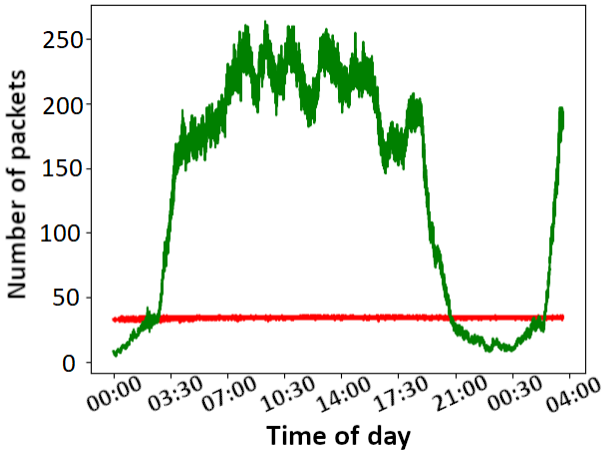



**Figure 4. Evolution of services and detection data in a day.**

The results of Figure 3 thus confirms this hypothesis that the detection data represent a majority of the radar traffic.

For the rest of the paper, we will focus mainly on the study of SSR radars because they represent a majority share in the French ATM. We will therefore be dealing with category 48 as detection data and category 34 for services data.

We have seen that the detection data were majority in our data. Nevertheless, we are interested in the impact that these data can have on evolution of the traffic. We have differentiated the evolution over time of detection data and services data for one day. The results are shown in Figure 4.

In red is represented the evolution in time of services data and in green the detection. We can see that for the services data, we have a continuous evolution whereas for detection data we have variation in time. This is because service messages are sent regularly. Indeed, a radar zone is divided into thirty-two sectors and each time the radar finished a zone, it sends a service message to say in which zone it observes. For our case, the radars have a rotation time of 4 sec. So, every 4 sec., we observe 32 messages of services data. If it is not the case, there is an anomaly somewhere.

With this observation for the rest of the section, we will focus on the evolution of the detection data in times which have variations.

Since network radar data represent the airspace network image at a specific point in time, we had the idea that the radar data traffic flow will follow the trend of air traffic. It has been seen in numerous papers [13], [14], [15] that in a normal day, the air traffic sees a peak of activities at the beginning of the day, at the end of the morning, at the beginning of the afternoon and in the evening, then it has a lull during the night to then resume the same trend. Thus, for radar data network flows, we expect to observe a trend that will be repeated over the days and the different radars that we can observe. To try to observe this trend, we were interested the evolution of the number of packet radars during a day.

We observed the evolution of detection packet for the first 15 days of May for a given radar. The result is given in Figure 5. We can visually observe that the radar traffic seems to follow

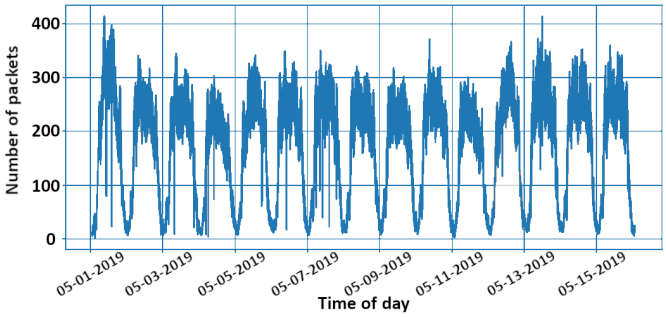



**Figure 5. Evolution of detection data during the first 15 days of May.**

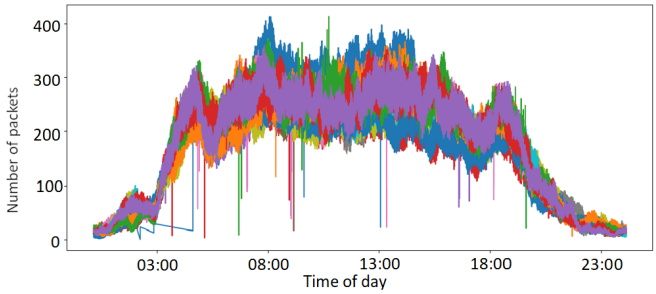



**Figure 6. Evolution of detection data during one day the first 15 days of May simultaneously.**

the same trend as the air traffic flow, with a drop in activity during the night, a peak high at 2 am, a rather stable variation during the day with peaks of activity and a drop in activities in the evening. This result is due to the fact that the radar data correlates with the aerial activity. Thus, if the air traffic follows a trend, we must find the same trend in the flow of radar packets.

The visualization of this trend is clearer in Figure 6, where we traced simultaneously over a period of 24 hours the evolution of detection packets in time for the first fifteen days of May.

Figure 6 reinforces the idea that indeed, we have a trend that seems to follow the same trend as air traffic with a drop in activity during the night and peaks during the day, and that, moreover, this trend will be similar in time since we find similarities through time.

Visually, we observe a trend that seems to be similar depending on the day. Figure 7 compares the evolution of the number of packets for a duration of one day for two days to one week apart, after normalization of the data. It confirms that the two curves overlap and have similar peaks. The cosine similarity for these two data is 0.97, which confirms to us that the two evolutions are very close. This reinforces our hypothesis of a trend that would be repeated every day.

Thus, the evolution in time for a radar will be similar through the days, because the state of the sky will be similar every day for this radar. However, we wondered if this was the case for all the radars for which we have data and if this model will be similar between the different radars.

To answer this question, we used Min and Max measurements as well as Mean. We measured the min and max of the number of detection data for each day over a period of two months, and we also averaged for each radar. This gives us,

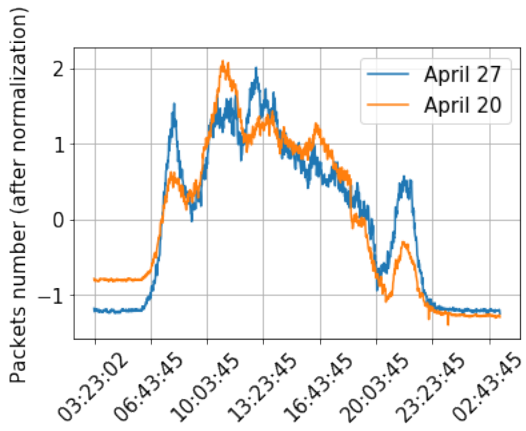



**Figure 7. Comparaison of two days.**

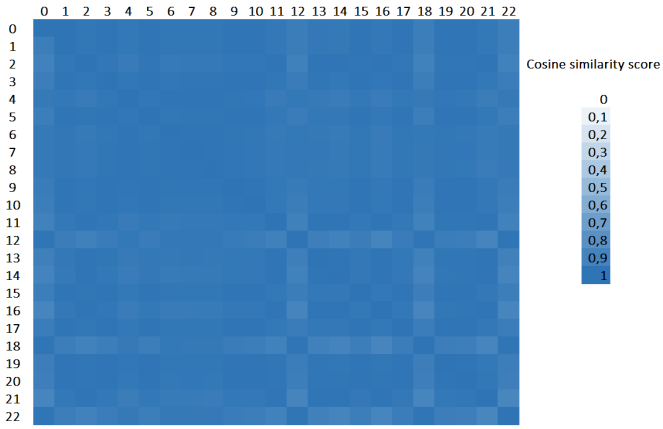



**Figure 8. Heatmap of cosine similarity score between the mean of the trend for the 23 radars.**

for a given radar, three different curves: a curve of the Min, a curve of the Max and a curve of the Mean. We have compared these twenty-three data among them, for the twenty-three SSR radars for which we have data, and we have measured the cosine similarity of the averages. The results are given in Figure 8 and we can see that the value of the cosine similarity is close to 1 each time, which means that the averages are similar to each other for the different radars.

Therefore, the trend that we observe from the beginning is a trend that will be repeated over time and that we will be able to find for the different radars. It is characterized by the average of this evolution through time that we were able to draw with a tolerance threshold which is defined by the Min and Max that we could observe.

With the help of these average values, we are able to define a trend that we will be able to find every day on all radars and that will allow us detect anomalies. In building this trend over a large time value and from a dataset that has been characterized without any anomaly, we can say that from the moment we move away from this trend, more or less the values of threshold of MIN and MAX, we can consider that there is potentially an anomaly.

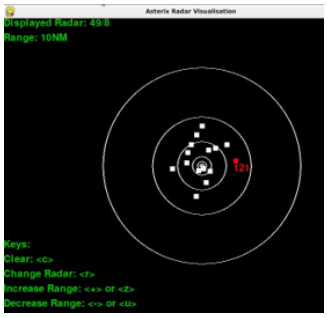



**Figure 9. Visualization of a normal traffic.**

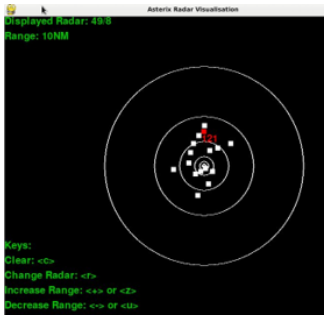



**Figure 10. Visualization of a spoofed traffic.**

## 5. Spoofing Attack Detection

In this section, we will consider the spoofing attacks, that is, artificially modify data in the dataset.

*Methodology of attack*

We used a python module: pygame which, coupled with an ASTERIX parser, allowed us to visualize the radar traffic. To manipulate radar data, we used an internal Scapy (a packet manipulation tool for computer networks) module. To operate the attack, we replayed a radar dataset from our dataset, with the TCP replay tool. Then, we visualized this dataset with our tool. We placed ourselves between the transmission and the visualization as an attacker (as an attack Man In the Middle). We received all the data from the transmitter and we re-transmitted it as is to the receiver. So we had at first a normal visualization of the dataset, with the representation of the planes in the sky, as shown in Figure 9. At some point, we decided to change the trajectory of an aircraft, for this example it is the one with the TPN (Track Plot Number) 121 to divert it to the West (offset by about 45 degrees). So we launched a scapy script that will modify in real time the position (Rho and Theta coordinates) of the aircraft, and sent this new data to the receiver. The result is a visual deviation, on the screen, of the aircraft identified with the TPN 121 to West, as shown in Figure 10.

Our goal is to detect such spoofing attacks. The idea of our system of detection is to predict the time series and compare the predicted value with the received value.

*Method of detection*

Because the Recurrent Neural Network (RNN) has a certain short-term memory advantage, it is often used as the preferred neural network for training time series. However, when the length of the sequence data exceeds a certain range, the data trained by the RNN will have a serious problem of gradient disappearance, which will lead to the training stop. That is

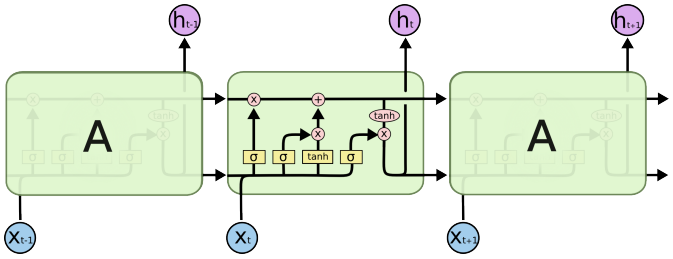



**Figure 11. The repeating module in an LSTM contains four interacting layers**

to say, the RNN can only learn the time series information of a certain interval. On the other hand, the Radar series sent by the aircraft can be regarded as a time series with context. It is difficult for RNN to effectively use this long history information because of its long length. This, RNN cannot learn the characteristics of long-term dependence. To solve this problem, Hochreiter and Schmidhuber first introduced the Long-Short Term Memory (LSTM) mechanism in [16]. Since then, researchers have also proposed a number of variants of LSTM, the most popular of which is described by Graves and Schmidhuber [17] in 2005.

The LSTM architecture consists of memory cells used to learn long-term modes, each cell containing its current state and three non-linear gates: the forget gate, the input gate, and the output gate. The forget gate is responsible for determining how much memory information to forget. It is determined by a nonlinear function that outputs a number between 0 and 1, where 0 means forgetting all information in memory, and 1 means retaining all information in memory. The input gate is responsible for deciding how to update the old cell state, ie, the new information is selectively recorded in the cell state. The output gate is responsible for deciding how much memorable information to pass to the next cell. The structure of the LSTM unit is shown in Figure 11.

*Detection*

In this paper, we use the LSTM neural network to predict the radar time series. After the model is trained, the correct data set is used to obtain the residual of the predicted value and the true value, and then calculate the statistical characteristics of the residual (the mean is denoted as $\mu$ and the variance is denoted as $\sigma$). The abnormal score is defined as the difference between the test dataset residual and $\mu$, and the abnormal threshold is defined as $3\sigma$. During the test phase, if the input time series contains an abnormal sequence, the abnormal score may exceed the threshold, thereby achieving the effect of anomaly detection.

We use the form of sliding window to predict the radar sequence. Specifically, we choose a window with a length of 10, and the training input and output forms are shown in Table 1. Use the first 10 data to predict the 11th data, 2 to 11 to predict the 12th data, and so on. The input time series is a window composed of 4-dimensional vectors, each of which contains the TPN, TIME, RHO, and THETA (RHO and THETA are measured positions of an aircraft in local polar coordinates) information of the aircraft.

We have taken the case of 10 different aircraft and injected them with abnormal data. In particular, we modified the position information of these aircraft at [100, 105], 45 degrees for THETA and 25 nautical miles for RHO respectively.

**Table 1**. Example of sliding window

| Input data number | Forecast data number |
|---|---|
| [1,10] | [11] |
| [2,11] | [12] |
| ... | ... |
| [n,n+9] | [n+10] |

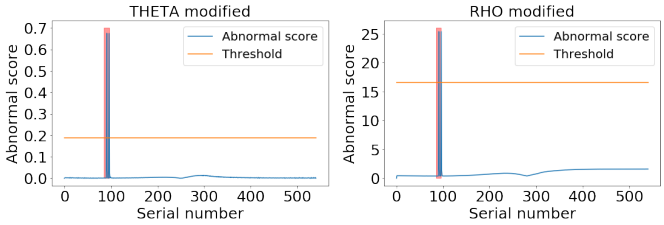



**Figure 12. Example of an aircraft after injecting a spoofing attack.**

Figure 12 represents the abnormal score of an aircraft (the situation of the remaining aircraft is similar) after injecting the attack. Modified sequences are marked in red.

As can be seen from the Figure, the method can effectively detect abnormal sequences, and the visualization effect is remarkable.

## 6. Conclusion and Future Work

The work that we conducted allowed us to highlight characteristics of radar network traffic that we will be able to find over time after the radar, which is a normal data signature basis. From these characteristic signatures, we will be able to set thresholds, based on statistical measures. As a result, we are taking a first step towards the development of a detection system dedicated to radar data. In addition, these characteristics allow us to better know the radar traffic, which will allow us, thereafter, to have an anomaly injection tool that will take into account these characteristics. Nevertheless, with our tool, we are already able to inject anomalies by making a spoofing attack, which will modify the measurements of an aircraft. Thus, we have developed a machine learning method that is able to detect this attack in a radar traffic. This is a first step to move towards the development of a dedicated detection module for ATM networks.

Several difficulties have arisen to develop our tools. Especially for the injection tool, because there are no data manipulation tools in ASTERIX, we had to develop our own, the same for the visualization tools, as we do not have on-site screen radar control, we had to develop our own visualization tool. Moreover, since the ASTERIX traffic was not studied in itself, it was necessary to find what elements could be characteristic of this traffic and which elements it would be relevant to modify. Finally, as we rely on real traces, we had to take into account all the errors that we can encounter in the traces.

For future work, we intend to develop other dedicated attacks to test our methods. The idea is to make the finest possible attacks and develop them with the controller partnership, in order to be closer to an operational context and expectations on the ground. To do this, we will work closely with ATM

professionals and we will test our tools of injection and detection on networks and machines close to an operational context in a real-time context. This will enable us to better characterize the actual traffic and to be able to test the reaction of the tools already in place on the operational network, as well as to test the controllers' response to an unknown attack. This will allow us to refine our rules for the development of the dedicated detection system.

## 7. Acknowledgment

We would like to thank DGAC DTI - the French innovation department of the navigation operator - for providing operational traces of their network to create our data set. The work for this paper is carried out as a part of a thesis funded by Activus-Group, a French company and ANRT, a French national association whose goal is to develop research in the private sectors.

## References

[1] Eurocontrol, "EUROCONTROL Specification for Surveillance Data Exchange - Part 1," *EUROCONTROL Specification for Surveillance Data Exchange*, Oct. 2016.

[2] M. Dzunda and A. Hrban, "Accuracy of the passive tracking systems," in *12th International Conference on Microwaves and Radar. MIKON-98. Conference Proceedings (IEEE Cat. No. 98EX195)*. IEEE, 1998, pp. 216–220.

[3] E. E. Casanovas, T. E. Buchaillot, and F. Baigorria, "Vulnerability of radar protocol and proposed mitigation," in *2015 ITU Kaleidoscope: Trust in the Information Society (K-2015)*. IEEE, 2015, pp. 1–6.

[4] B. Lim, "Emerging threats from cyber security in aviation–challenges and mitigations," *Journal of Aviation Management*, pp. 83–91, 2014.

[5] T. De Zan, F. d'Amore, and F. Di Camillo, "The defence of civilian air traffic systems from cyber threats," *Istituto Affari Internazionali*, 2016.

[6] C. S. Bosson and T. Nikoleris, "Supervised Learning Applied to Air Traffic Trajectory Classification," in *2018 AIAA Information Systems-AIAA Infotech@ Aerospace*, 2018, p. 1637.

[7] M. Gariel, A. N. Srivastava, and E. Feron, "Trajectory clustering and an application to airspace monitoring," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 4, pp. 1511–1524, 2011.

[8] M. Conde Rocha Murca, R. DeLaura, R. J. Hansman, R. Jordan, T. Reynolds, and H. Balakrishnan, "Trajectory clustering and classification for characterization of air traffic flows," in *16th AIAA Aviation Technology, Integration, and Operations Conference*, 2016, p. 3760.

[9] A. D. Evans and P. U. Lee, "Predicting the Operational Acceptability of Route Advisories," in *17th AIAA Aviation Technology, Integration, and Operations Conference*, 2017, p. 3078.

[10] S. K. A. Nanduri, "Anomaly Detection in Aircraft Performance Data," 2016.

[11] P. Farrell and M. Schuurman, *Using ASTERIX in accident investigation*, Sep. 2012.

[12] E. E. Casanovas, T. E. Buchaillot, and F. Baigorria, "Vulnerability of radar protocol and proposed mitigation," in *ITU Kaleidoscope: Trust in the Information Society (K-2015), 2015*. IEEE, 2015, pp. 1–6.

[13] M. Schultz, S. Lorenz, R. Schmitz, and L. Delgado, "Weather Impact on Airport Performance," *Aerospace*, vol. 5, no. 4, p. 109, 2018.

[14] C. Barnhart, D. Fearing, A. Odoni, and V. Vaze, "Demand and capacity management in air transportation," *EURO Journal on Transportation and Logistics*, vol. 1, no. 1-2, p. 141, 2012.

[15] H. Mannstein, A. Brömser, and L. Bugliaro, "Ground-based observations for the validation of contrails and cirrus detection in satellite imagery," *Atmospheric Measurement Techniques*, vol. 3, no. 3, p. 662, 2010.

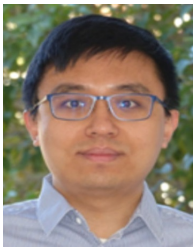
[16] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[17] A. Graves and J. Schmidhuber, "Framewise phoneme classification with bidirectional LSTM and other neural network architectures," *Neural networks*, vol. 18, no. 5-6, pp. 602–610, 2005.

## Biography



***Théobald de Riberolles*** *is a PHD student in the the company Activus-Group and in TELECOM research team of ENAC (French Civil Aviation University). He has a Master's degree in Telecommunications and Networks form University of Toulouse. Théobald is working on a thesis related to network security, machine learning and Air Traffic Management.*



***Jiefu Song*** *is currently chief R& D officer in Activus Group (France) and associated researcher at the IRIT research center (CNRS UMR 5505). He received a PhD degree in computer science from the University of Toulouse (2017). His research interests cover many aspects of the next generation of data management systems, with a focus on conceptual modeling and exploitation of knowledge graph. His publications appear in major national and international journals and conference proceedings.*



***Guthemberg Silvestre*** *is assistant professor in the TELECOM research team of ENAC (French Civil Aviation University). He has a PhD in computer science from UPMC Sorbonne Universités. He is broadly interested in the areas of distributed systems and computer networks. In the recent years, he has conducted research on distributed algorithms, replication and consistency models in dynamic networks.*



***Nicolas Larrieu*** *is full professor in the TELECOM research team of ENAC (French Civil Aviation University). He has a PhD in computer science from University of Toulouse. Dr. Larrieu works on secure communication architectures. He is also interested in Intrusion Detection System for environment with strong constraints. His field of expertise is related to civil aviation networks and embedded systems such as aircraft or UAV.*



***Yunkai ZOU*** *is a graduate student in the Sino-European Institute of Aviation Engineering at Civil Aviation University of China. He is currently conducting a PFE internship in TELECOM research team of ENAC (French Civil Aviation University). His research interests include security of avionic systems and machine learning.*