DEFENSE / CYBER / SECURITY

IDENTIFICATION OF UNMANNED AERIAL VEHICLE INTRUSION BASED ON WI-FI ANALYSIS

Benchmark vs. Logistic Regression, Random Forests, Boosted Trees & Neural Networks

Use Case 2023/01 (v1.0) • xtractis.ai

PROBLEM DEFINITION

PROBLEM

How to automatically, efficiently and transparently identify a type of invading Unmanned Aerial Vehicle (UAV) in a civilian environment, based on Wi-Fi traffic data records?

GOALS & BENEFITS

- ☑ Identify the Wi-Fi traffic data characterizing an UAV intrusion. Enhance expert knowledge by helping security specialists understand the causal relationships between specific Radio frequency characteristics, their combination, and the type of UAV.
- ☑ Help security agents qualify the type of UAV to diagnose the intrusion as early as possible.
- ☑ Avoid a large number of false alarms thanks to transparent diagnosis, in a context of increasing number of consumer UAVs.

REFERENCE DATA

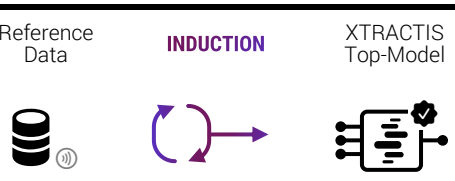
- ▶ **Observations**: 3,770 cases for Training / Validation/ Test and 35,019 for External Test.
  All duplicates were removed from the data to avoid biasing performance assessment.
  Source: Liang Zhao, George Mason University, Fairfax, Virginia. http://mason.gmu.edu/~lzhao9/materials/data/UAV
- ▶ **Predictive Variables**: 54 potential predictors obtained from a preprocessing of two-way radio frequency time series recordings
- ▶ **Variable to Predict**: the model must predict 4 possible classes
  [Not an UAV / DJI spark / DBpower UDI / Parrot Bebop].

MODEL TYPE

Regression | **Multinomial Classification** | Binomial Classification | Scoring

XTRACTIS SOLUTION

PROCESS



SOFTWARE ROBOTS

XTRACTIS® **GENERATE** — XTRACTIS® **PREDICT** — + **PREDICT**ion Report (for decision explainability)

RESULTS

- ☑ **Intelligible Predictive Top-Model**: Decision system composed of 4 unchained gradual rules, each rule using some of the 5 variables that XTRACTIS identified as predictors.
- ☑ **Robust Predictive Top-Model**: Perfect real performance in External Test.
- ☑ **Operational Efficient System**: Real-time predictions up to 70,000 decisions/s., offline or online (API).

TOP-MODEL INDUCTION

INDUCTION PARAMETERS

We launch 2,000 inductive reasoning strategies on the same single Training (60%) / Validation (20%) / Test (20%) partition of the learning dataset. Each strategy thus generates one unitary model called **Individual Virtual Expert (IVE)**.

Among the 2,000 induced models, the top-IVE is the one that has the best predictive performance, close to its descriptive performance, with the fewest predictors and rules (5 predictors shared by 4 rules).

Total number of induced unitary models	Criterion for the induction optimization	Validation criterion for the top-models selection	Duration of the process (Induction Power FP64)
2,000 IVE	Average F_1-Score	Average F_1-Score	2 hours (1 Tflops)

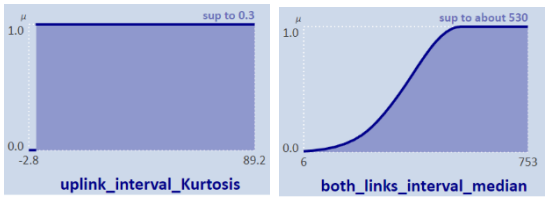
STRUCTURE

Intelligibility

The top-IVE model combines the 5 predictors, automatically selected by XTRACTIS into 4 rules. Its Structure Report reveals all the internal decision logic and ensures that the human expert understands the model. This decision system is a *white-box* model that can be audited by the domain expert and certified by the regulator before its deployment to end-users.

PREDICTORS

- 5 Radio frequency characteristics (out of 54)
- Ranked by impact significance (3 strong & 2 weak signals): #1 downlink_size_MIN / … / #5
- Labeled by fuzzy and binary classes
  Examples: **binary interval** "sup to 0.3";
  fuzzy interval "sup to about 530"



RULES

- 4 connective fuzzy rules without chaining
- 1 to 4 predictors per rule (on average, 2 predictors per rule)
- Example: **fuzzy rule R1** uses 4 predictors, and concludes "DBpower UDI". 3 other fuzzy rules complete this model, including 2 binary rules.

IF	uplink_interval_Kurtosis	IS	sup to 0.3
AND	uplink_interval_MIN	IS	inf to 79
AND	both_links_interval_median	IS	sup to about 530
AND	both_links_interval_MIN	IS	sup to 75
THEN	UAV type	IS	DBpower UDI

PERFORMANCE

Robustness

The top-IVE performances, measured in Training/Validation/Test, then in External Test, guarantee the model's predictive and real performances.

Performance	DESCRIPTIVE	PREDICTIVE	REAL
Dataset	60% Training	20% Validation	20% Test
Average F_1-Score	100.00%	100.00%	100.00%
Classification Error	0.00%	0.00%	0.00%

REAL
External Test
100.00%
0.00%

Xtractis Top-Model: Intelligible AND Perfect Predictive Capacity

EXPLAINED PREDICTIONS FOR 3 CASES FROM THE EXTERNAL TEST SET

CASE
(not used in Training/Validation)

DEDUCTIVE INFERENCE OF RULES

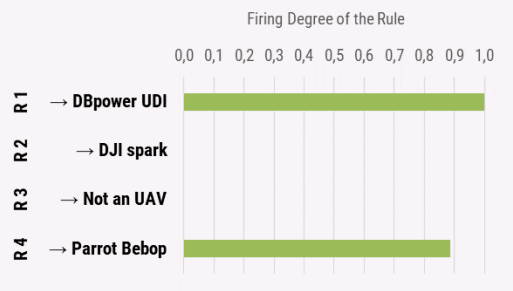
AUTOMATED DECISION

Record 6424
(actual value = DBpower UDI)

downlink_size_MIN	76
uplink_interval_Kurtosis	1.2
uplink_interval_MIN	76
both_links_interval_median	646
both_links_interval_MIN	76

→ Real Time

For this record, 2 rules are triggered:
R1 at 1.000 to conclude "DBpower UDI",
and **R4** at 0.887 to conclude "Parrot Bebop".
The 2 other rules are not activated.



NUMBER OF TRIGGERED RULES
2 / 4

FUZZY PREDICTION
{ DBpower UDI | 1.000,
Parrot Bebop | 0.887 }

FINAL PREDICTION
{ DBpower UDI }

The system delivers the correct diagnosis compared to that given by the security expert although it considered that it could also be a Parrot Bebop with a closer possibility:

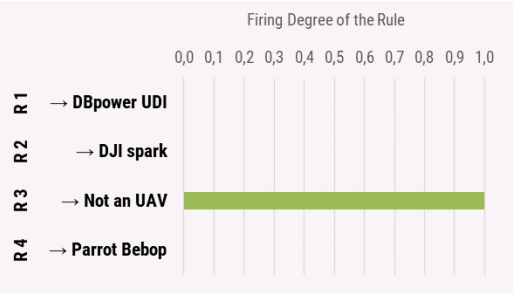
DBpower UDI Intrusion

Record 11614
(actual value = Not an UAV)

downlink_size_MIN	228
uplink_interval_Kurtosis	1.0
uplink_interval_MIN	204
both_links_interval_median	57
both_links_interval_MIN	204

→ Real Time

For this record, 1 rule is triggered:
R3 at 1.000 to conclude "Not an UAV".
The 3 other rules are not activated.



NUMBER OF TRIGGERED RULES
1 / 4

FUZZY PREDICTION
{ Not an UAV | 1.000 }

FINAL PREDICTION
{ Not an UAV }

The system delivers the correct diagnosis compared to that given by the security expert:

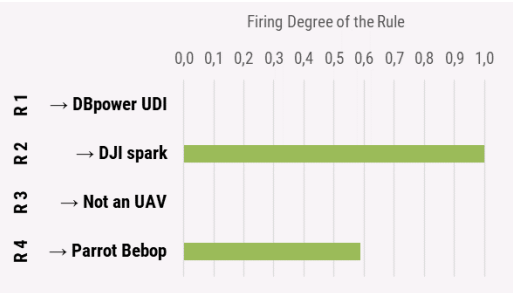
Not an UAV

Record 2064
(actual value = DJI spark)

downlink_size_MIN	86
uplink_interval_Kurtosis	12.4
uplink_interval_MIN	146
both_links_interval_median	209
both_links_interval_MIN	86

→ Real Time

For this record, 2 rules are triggered:
R2 at 1.000 to conclude "DJI spark",
and **R4** at 0.587 to conclude "Parrot Bebop".
The 2 other rules are not activated.



NUMBER OF TRIGGERED RULES
2 / 4

FUZZY PREDICTION
{ DJI spark | 1.000,
Parrot Bebop | 0.587 }

FINAL PREDICTION
{ DJI spark }

The system delivers the correct diagnosis compared to that given by the security expert:

DJI spark Intrusion

TOP-IVE BENCHMARK

	XTRACTIS	LOGISTIC REGRESSION	RANDOM FOREST	BOOSTED TREES	NEURAL NETWORK
MODELS RELEASE	2023/01	2023/01	2023/01	2023/01	2023/01
ALGO VERSION	XTRACTIS **GENERATE** 12.2.44533	Python 3.9; Scikit-learn 1.1.2	Python 3.9; LightGBM 3.3.2	Python 3.9; LightGBM 3.3.2	Python 3.9; TensorFlow 2.10.0 Keras 2.10.0
CROSS-VALIDATION TECHNIQUE	1-Split Validation for each IVE model: 60% Training / 20% Validation / 20% Test	1-Split Validation for each IVE model: 60% Training / 20% Validation / 20% Test	1-Split Validation for each IVE model: 60% Training / 20% Validation / 20% Test	1-Split Validation for each IVE model: 60% Training / 20% Validation / 20% Test	1-Split Validation for each IVE model: 60% Training / 20% Validation / 20% Test
NUMBER OF EXPLORED STRATEGIES[1]	2,000 induction strategies on Training / Validation / Test data	2,000 data analysis strategies on Training / Validation / Test data	2,000 ML strategies on Training / Validation / Test data	2,000 ML strategies on Training / Validation / Test data	2,000 ML strategies on Training / Validation / Test data
NUMBER OF MODELS	2,000 IVE + selection of the top-IVE	2,000 IVE + selection of the top-IVE	2,000 IVE + selection of the top-IVE	2,000 IVE + selection of the top-IVE	2,000 IVE + selection of the top-IVE
TOP-IVE STRUCTURE					
NUMBER OF PREDICTORS (out of 54 Potential Predictors)	**5**	**34**	**13**	**32**	**54**
DECISION STRUCTURE	System with **4** unchained fuzzy rules	**4** Linear equations	**4** trees; **20** binary rules	**52** chained trees; **237** binary rules	**2** hidden layer; **12** hidden nodes
MODEL INTELLIGIBILITY (& DECISION EXPLAINABILITY)	⊕⊕⊕ 2 predictors per rule on average; only a few rules are triggered at a time.	⊖⊖○ Equations with 81 coefficients in all	⊖⊖○ Lots of predictors and rules	⊖⊖⊖ Tree #N corrects the error of the N-1 previous trees	⊖⊖⊖ Unintelligible synthetic variables
TOP-IVE REAL PERFORMANCE (External Test)	*Random*[2]				
Classification Error	*64.03%*	**0.00%**	**1.16%**	**0.91%**	**0.51%**	**0.37%**
Min. Sensitivity	*11.91%*	99.99%	95.20%	94.40%	97.12%	97.68%
Average Sensitivity	*27.26%*	100.00%	98.10%	98.11%	98.97%	99.24%
Min. PPV	*11.91%*	99.99%	92.79%	98.25%	99.02%	98.27%
Average PPV	*27.26%*	100.00%	97.65%	98.94%	99.63%	99.34%
Min. F_1-Score	*11.91%*	99.99%	93.98%	96.29%	98.46%	97.97%
Average F_1-Score	*27.26%*	**100.00%**	**97.87%**	**98.52%**	**99.29%**	**99.29%**
Weighted Average F_1-Score	*35.97%*	100.00%	98.85%	99.08%	99.49%	99.63%
Refusals	N/A	0 (0.00%)	N/A	N/A	N/A	N/A
MODEL ROBUSTNESS		#1	#5	#4	#2	#2

[1] All IVE models are optimized according to their validation Average F_1-Score. All top-IVE models are selected according to their validation Average F_1-Score.

[2] Baseline performances that models must exceed to perform better than chance (P-value = 0.001; 100,000 models generated by random permutation of the output values).

More Use Cases: xtractis.ai/use-cases/