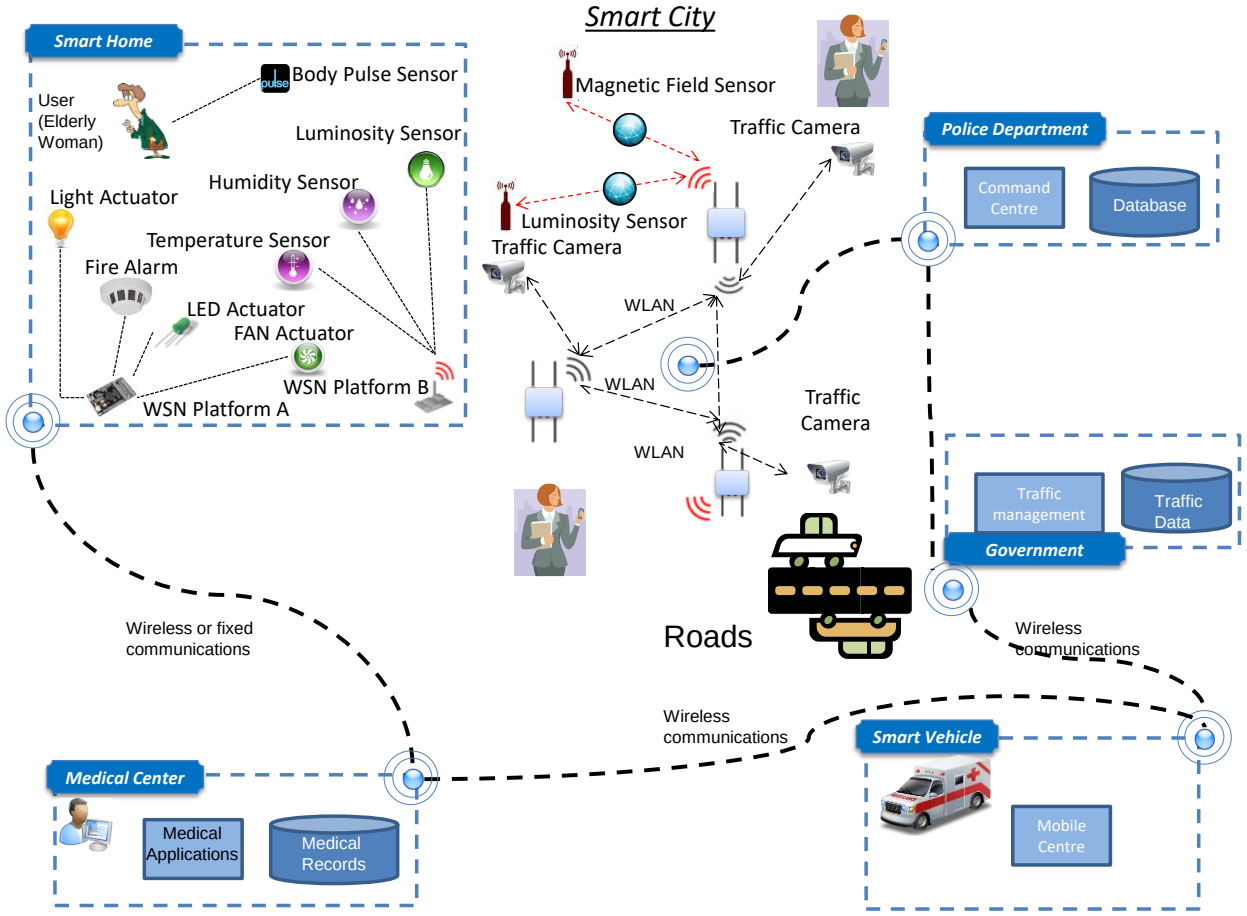
Physical layer authentication of Internet of Things wireless devices through permutation and dispersion entropy

Gianmarco Baldini
European Commission
DG.JRC.E3
Gianmarco.Baldini@ec.europa.eu

Joint Research Centre

Internet of Things: a complex world



Security in IoT is still a considerable challenge:

- Many different security solutions
- Lack of secure interoperability
- Limited computing capability of IoT devices to implement cryptographic algorithms
- Deployment issues for certificates
- Scalability for billions of devices in IoT

IoT device authentication

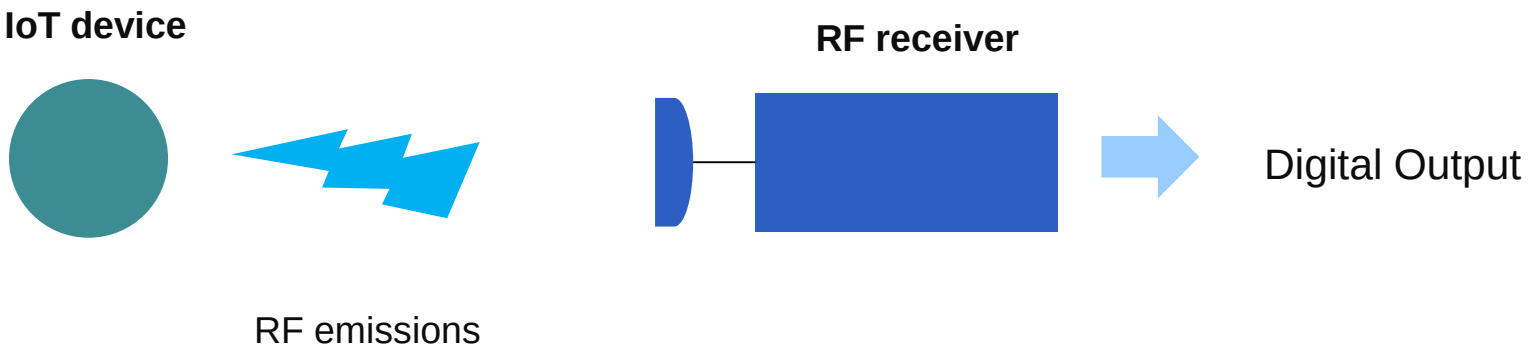
Most systems which bind IoT sensors and actuators rely on some proxy concept, i.e. sensors communicate to some more powerful entity which then authenticates the sensors on their behalf. However, the *last mile* may still be unprotected which also prevents to guarantee for important security properties such as non-repudiation. Lightweight solutions are still an open research issue for many devices. The long history of research in sensor networks domain has not produced secure and low-cost solutions feasible for most devices.

Thus, new types of security primitives or mechanisms which do not only focus on the higher layers in communication protocols may need to be investigated.

RF fingerprinting

The concept of RF fingerprinting is that electronic devices can be identified and authenticated through their radio frequency emissions.

Small differences in the material and the composition of the electronic circuits (e.g., due to different manufacturing plants or production chains) used for wireless transmission, generate small differences in the RF signal over the air.



IoT device authentication with RF fingerprinting

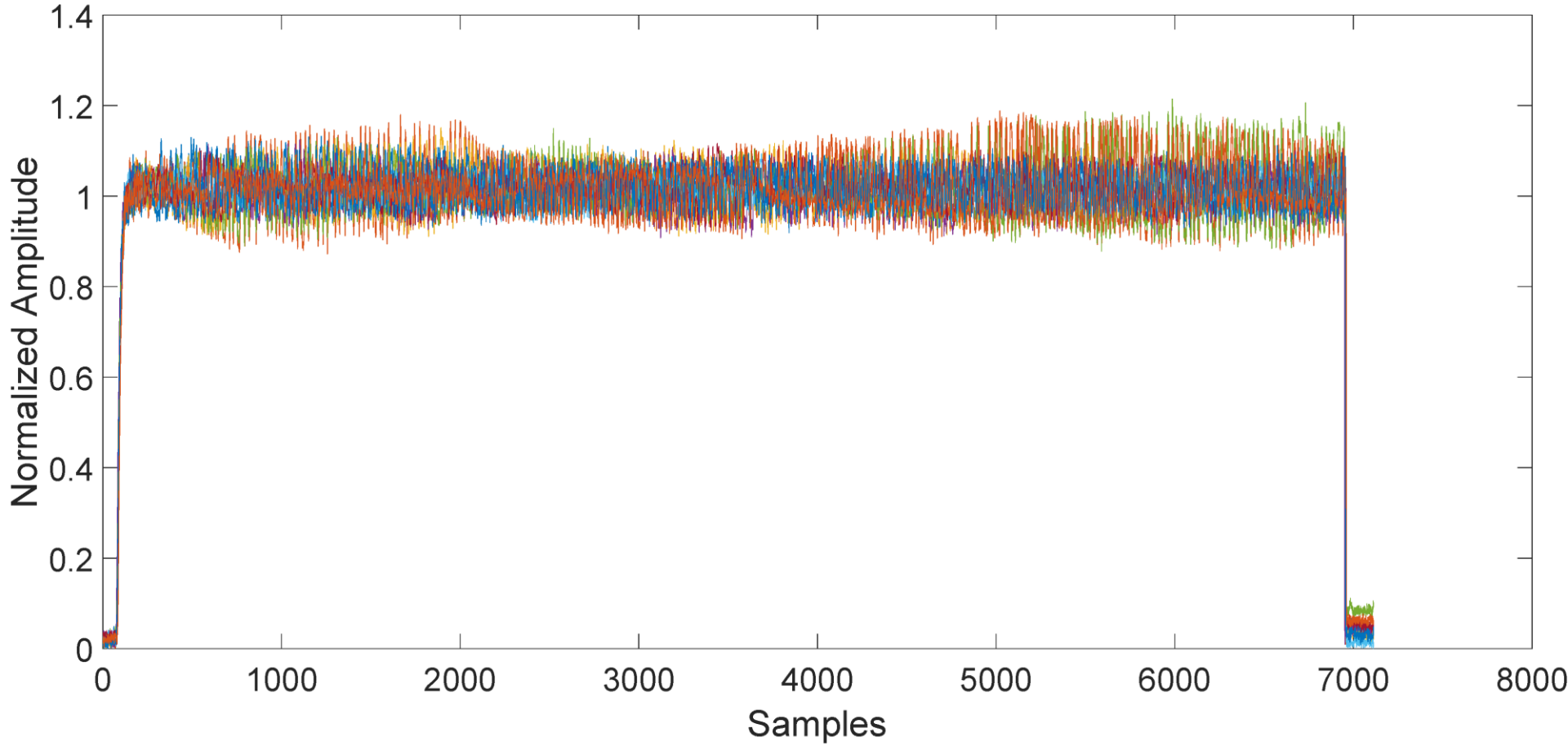
- RF fingerpriting can be used to support multi-factor authentication, where this physical layer authentication can be used on its own or to complement conventional cryptographic authentication.

- The advantage of physical layer authentication is that it is not easy to fake or duplicate because it is based on the physical properties of the RF circuits of the electronic device.

- To support multi-factor authentication, it is important to implement a classification algorithm, which is able to distinguish between wireless devices of the same model and different serial numbers.

European Commission

RF bursts from IoT device: nRF24LU1+



Joint Research Centre

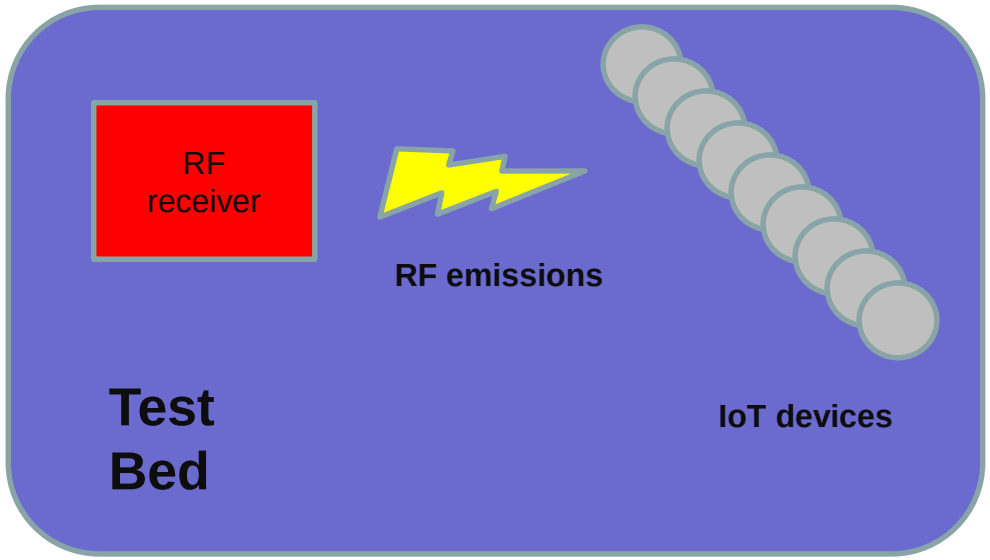
Test bed and equipment

- 9 nRF24LU1+ devices, which are used to implement wireless sensor networks for IoT applications. This wireless device is an Ultra Low Power (ULP) device transmitting for the 2.4GHz ISM band. It includes a 2.4GHz RF transceiver core, 8-bit CPU, full-speed USB 2.0 device controller, and embedded Flash memory. These wireless devices have been programmed to build a MySensors network. MySensors is a free and open source DIY (do-it yourself) software framework for wireless Internet of Things (IoT) devices allowing devices to communicate using radio transmitters.

- The RF signals transmitted by the wireless devices are collected using a low cost Universal Software Radio Peripheral (USRP) SDR receiver of type N210, equipped with XCVR2450 front end locked to the Global Positioning Systems (GPS) disciplined to 10 MHZ reference to ensure repeatability in the collection of RF observables. The SDR receiver was equipped with a ublox NEO6Q GPS receiver. The RF signals were sampled by the SDR with a sampling rate of 5 msamples/sec.

Methodology

Collection of the RF signal in space for 9 devices



Synchronization

Normalization

Extraction of statistical features

Application of 10-fold

Machine Learning

Estimate of Average Accuracy

Joint Research Centre

Statistical features used in this study

Feature Identifier	Name of statistical feature
1 (Amplitude)	Variance
2 (Amplitude)	Skewness
3 (Amplitude)	Kurtosis
4 (Amplitude)	Shannon Entropy
5 (Amplitude)	Log Entropy
6 (Amplitude)	Permutation Entropy with Order 4 and Delay Time 1
7 (Amplitude)	Permutation Entropy with Order 5 and Delay Time 1
8 (Amplitude)	Dispersion Entropy with Embedding Dimensions 3, Number of Classes 5 and Delay Time 1
9 (Amplitude)	Dispersion Entropy with Embedding Dimensions 4, Number of Classes 5 and Delay Time 1
10 (Amplitude)	Dispersion Entropy with Embedding Dimensions 5, Number of Classes 5 and Delay Time 1

Permutation Entropy

$$PE = -\sum_{i=1}^{D!} p_i * \log p_i$$

Dispersion Entropy

$$DE = -\sum_{i=1}^{n_{emb}} p_i * \log p_i$$

European Commission

Overall accuracy results

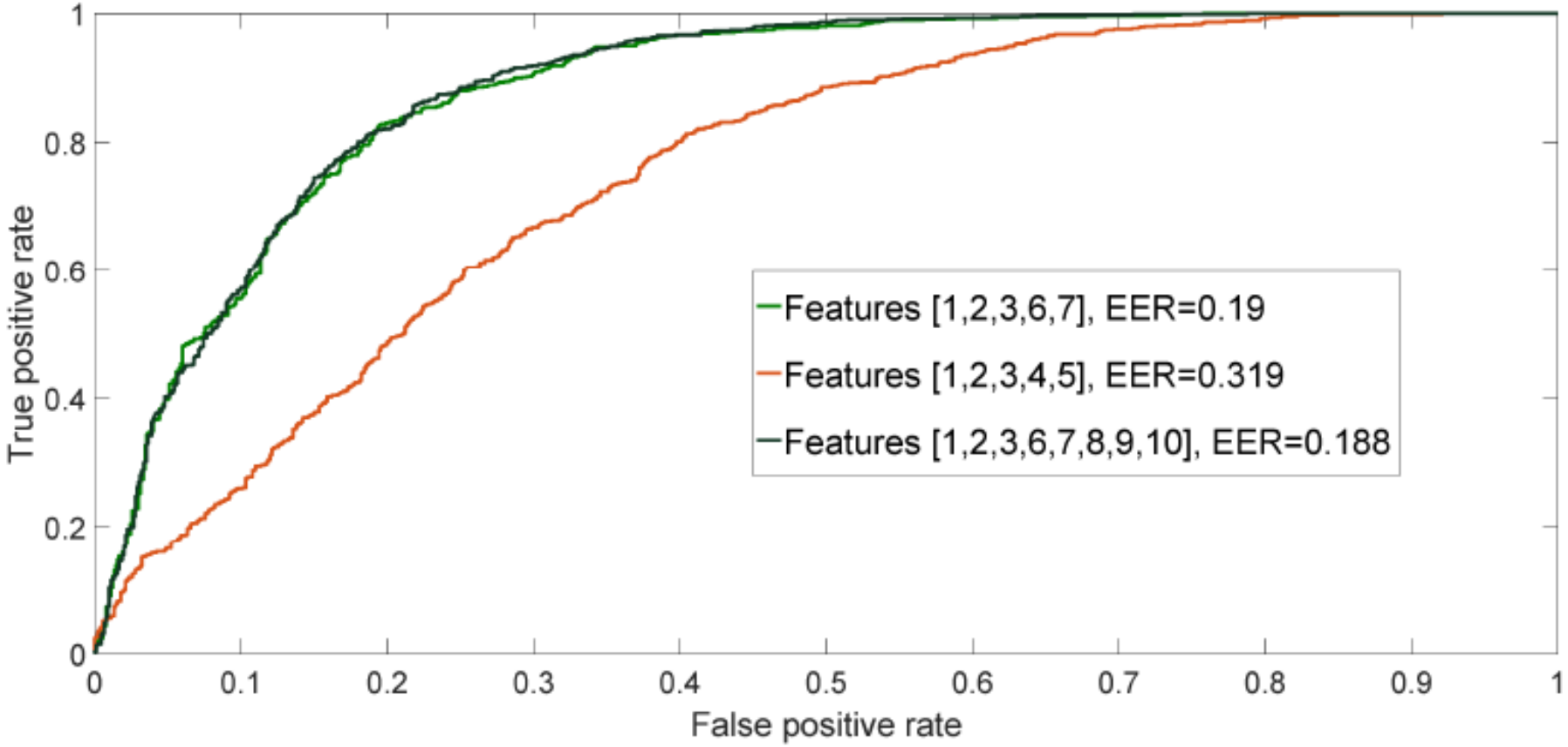
Machine Learning Algorithm	Set of features	Overall Accuracy
KNN	[1,2,3,4,5]	0.5918
KNN	[1,2,3,6]	0.7896
KNN	[1,2,3,7]	0.7834
KNN	[1,2,3,6,7]	0.808
KNN	[1,2,3,8,9,10]	0.541
KNN	[1,2,3,6,7,8]	0.8177
KNN	[1,2,3,6,7,9]	0.823
KNN	[1,2,3,6,7,10]	0.822
KNN	1,2,3,6,7,8,9,10]	0.819
SVM	[1,2,3,4,5]	0.49
SVM	[1,2,3,6]	0.8052
SVM	[1,2,3,7]	0.8031
SVM	[1,2,3,6,7]	0.8076
SVM	[1,2,3,8,9,10]	0.5382
SVM	[1,2,3,6,7,8]	0.8168
SVM	[1,2,3,6,7,9]	0.8191
SVM	[1,2,3,6,7,10]	0.8194
SVM	[1,2,3,6,7,8,9,10]	0.821
Decision Tree	[1,2,3,4,5]	0.5715
Decision Tree	[1,2,3,6]	0.7919
Decision Tree	[1,2,3,7]	0.7891
Decision Tree	[1,2,3,6,7]	0.8041
Decision Tree	[1,2,3,8,9,10]	0.6172
Decision Tree	[1,2,3,6,7,8]	0.7974
Decision Tree	[1,2,3,6,7,9]	0.8069
Decision Tree	[1,2,3,6,7,10]	0.8085
Decision Tree	[1,2,3,6,7,8,9,10]	0.8138

Confusion Matrix with Support Vector Machine and [1,2,3,6,7,8,9,10]

	D1	D2	D3	D4	D5	D6	D7	D8	D9
D1	811	0	10	79	0	0	0	0	0
D2	0	802	1	0	19	0	7	23	48
D3	24	1	746	119	8	0	2	0	0
D4	62	0	96	720	22	0	0	0	0
D5	9	2	12	177	700	0	0	0	0
D6	2	0	1	0	0	817	57	0	23
D7	0	3	2	0	0	80	704	0	111
D8	2	26	29	0	0	0	45	783	16
D9	0	85	0	0	0	104	146	0	565

European Commission

ROCs between devices 7 and 9 with different set of features:



Joint Research Centre

European Commission

Conclusions:

- Conventional statistical features used in literature (1 to 5) do not provide good accuracy results for these specific IoT devices.
- Permutation Entropy provides a significant improvement
- Dispersion Entropy add another 2% improvement accuracy
- Significant noisy IoT devices and real time test bed (interference, attenuation, fading)
- Intra-model identification accuracy
- Improving the accuracy using other techniques

Thank you for your attention.

Joint Research Centre (JRC)
Web: www.jrc.ec.europa.eu