Cyber Threat Analysis in IoT

Fernando Nakayama

Research Advisor: Dr. Michele Nogueira Lima

Center for Computational Security sCience (CCSC)

Belo Horizonte – Brazil

September 04, 2023

www.ccsc-research.org

Projeto DUST
Objectives

- Identify security threats in IoT environments
- Obfuscate information leakage and behavior of devices and users

Selected Paper

Profiling Attack on WiFi-based IoT Devices Using an Eavesdropping of an Encrypted Data Frames

Ibrahim Alwhbi Alharbi[*,1], Ali Jaber Almalki[2], Mnassar Alyami[3], Cliff Zou[4], Yan Solihin[5]

Advances in Science, Technology and Engineering Systems Journal (ASTESJ)

WiFi-based IoT Devices Profiling Attack based on Eavesdropping of Encrypted WiFi Traffic

Mnassar Alyami,[1] Ibrahim Alharbi,[1] Cliff Zou,[1] Yan Solihin,[1] and Karl Ackerman[2]

2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)

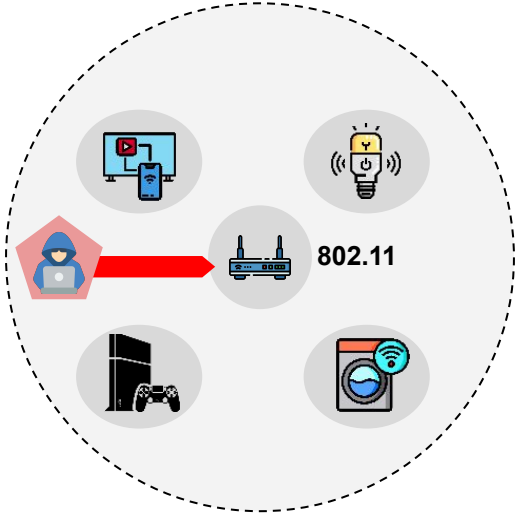
MAC-Layer Traffic Shaping Defense Against WiFi Device Fingerprinting Attacks

Publisher: IEEE Cite This PDF

WiFi-based IoT Devices Profiling Attack based on Eavesdropping of Encrypted WiFi Traffic

Problem

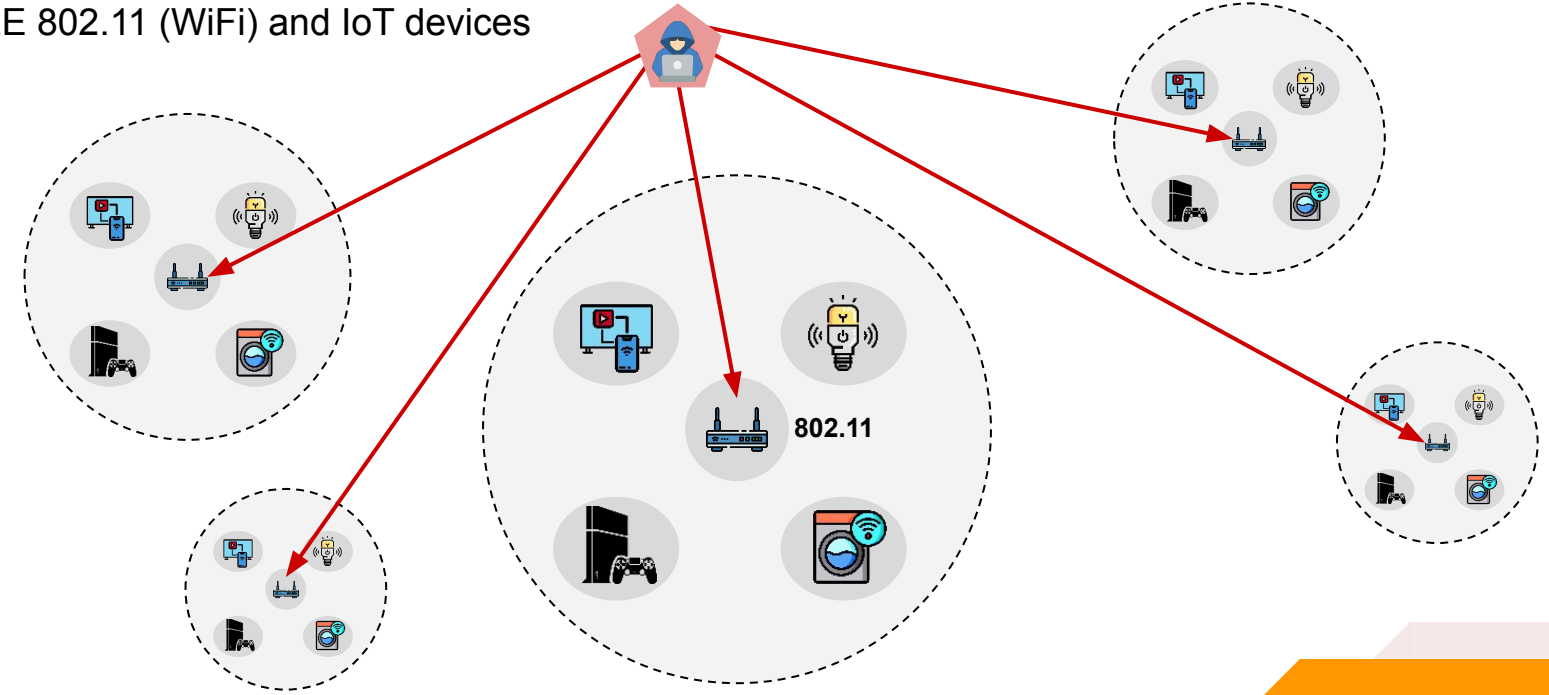
- Privacy leakage through wireless traffic analysis
- Devices and vulnerabilities identification



WiFi-based IoT Devices Profiling Attack based on Eavesdropping of Encrypted WiFi Traffic

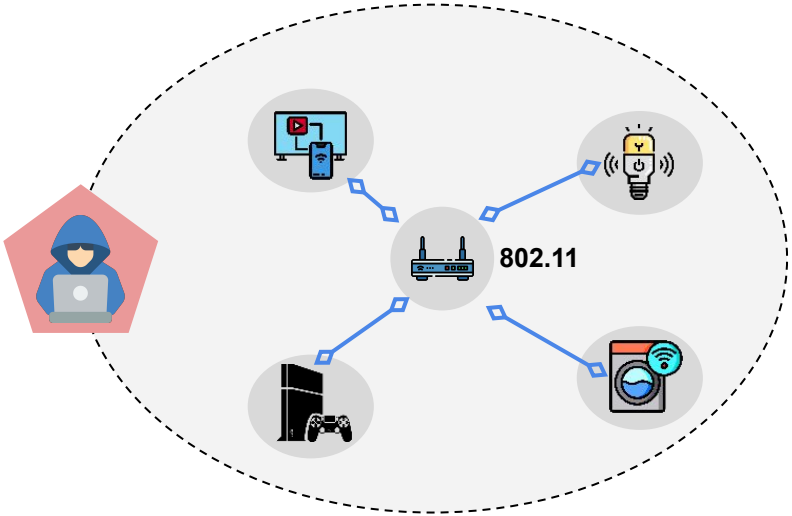
Motivation

- IEEE 802.11 (WiFi) and IoT devices



WiFi-based IoT Devices Profiling Attack based on Eavesdropping of Encrypted WiFi Traffic
Contribution

- Hypothesis: fingerprinting without joining a WiFi network



1. Fingerprinting attack
2. Employ time series and summary
3. Discussion on defense approaches

WiFi-based IoT Devices Profiling Attack based on Eavesdropping of Encrypted WiFi Traffic

Related Work

- Conventional approaches
  - IP address, port number, volumetric information, time series data
- Rogue Access points
- Clock-skew, physical unclonable function (PUF)
- Defense mechanisms

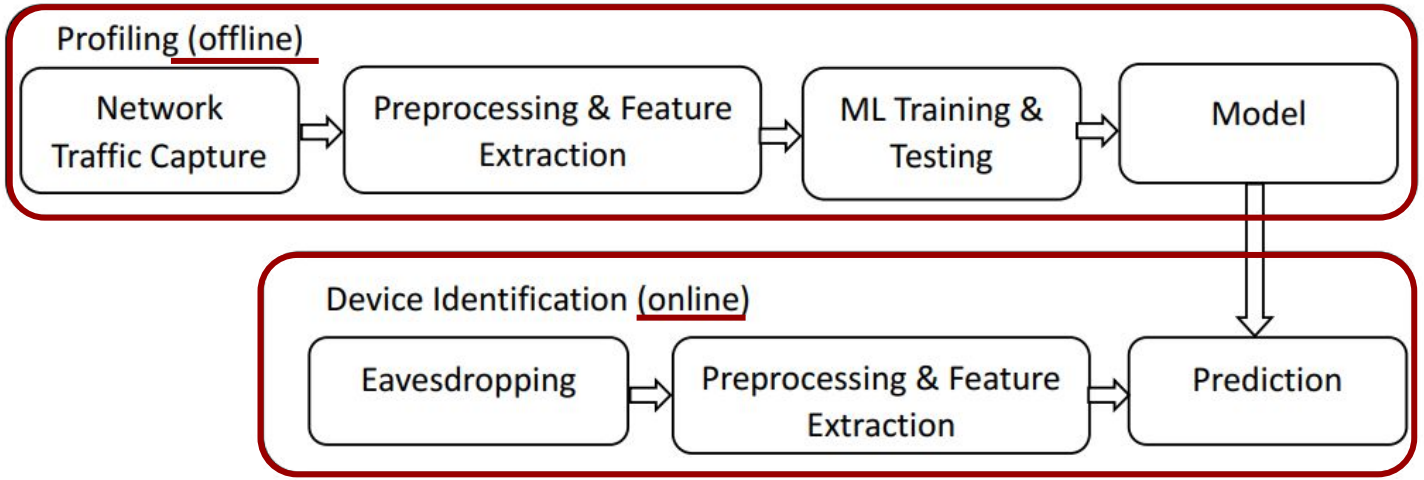
WiFi-based IoT Devices Profiling Attack based on Eavesdropping of Encrypted WiFi Traffic

Threat Model and Assumptions

- Passive observer
- Attacker can not break into the network

WiFi-based IoT Devices Profiling Attack based on Eavesdropping of Encrypted WiFi Traffic

Profiling Attack System



WiFi-based IoT Devices Profiling Attack based on Eavesdropping of Encrypted WiFi Traffic

Out-of-network Passive Traffic Capturing

- Limited capture
  - Airodump-ng
  - Kismet
- Unlimited capture
  - Airtool (Macbook)

Packets/Frames Size Range	Wireshark	Airtool	
	#Packets	#Frames	#Data frames
0-19	0	2428	0
20-39	0	5593	199
40-79	2441	0	0
80-159	260	2890	2883
160-319	108	239	239
320-639	173	194	190
640-1279	241	255	255
1280-2559	13574	13846	13846
Total	16797	25445	17612

BRCM 1062

https://www.intuitibits.com/products/airtool

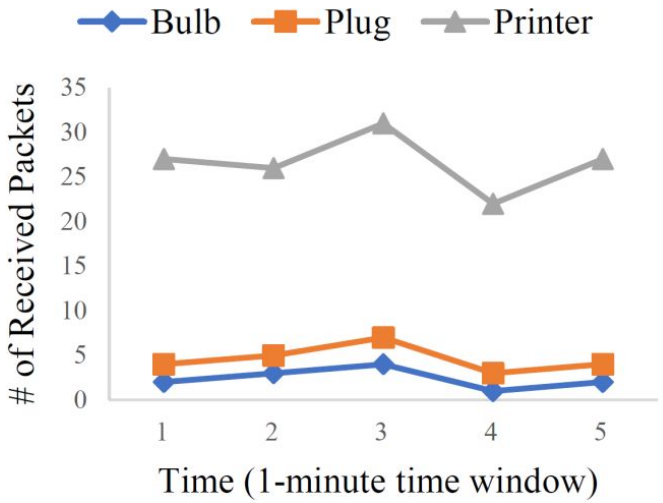
WiFi-based IoT Devices Profiling Attack based on Eavesdropping of Encrypted WiFi Traffic

Pre-Processing of Captured WiFi Traffic

- Filter AP MAC address (capture happens over multiple APs)
- Remove noise (leaving only bidirectional flow)
- Labeling dataset (only for offline mode)
- Calculate statistical features and export dataset

WiFi-based IoT Devices Profiling Attack based on Eavesdropping of Encrypted WiFi Traffic
Preliminary Data Analysis

- Header-based features
  - Flow-related
  - Volume-related



WiFi-based IoT Devices Profiling Attack based on Eavesdropping of Encrypted WiFi Traffic

Observable Data Fields in Out-of-Network Monitoring

- MAC-layer frame header
  - Source address
  - Destination address
  - Frame type
  - Frame size
- Frame timestamp
- Signal strength

WiFi-based IoT Devices Profiling Attack based on Eavesdropping of Encrypted WiFi Traffic

Machine Learning Algorithms

- Random Forest
- Support Vector Machine (SVM)
- Naive Bayes

WiFi-based IoT Devices Profiling Attack based on Eavesdropping of Encrypted WiFi Traffic

Device Profiling

- Time-series data
  - Inter-arrival time
  - Direction
  - Packet size
- Summary data
  - Various traffic features

1) The number of packets sent from the device to AP.
2) The number of packets received by the device from AP.
3) The variance of inter-arrival time.
4) The average number of consecutively sent packets before seeing a received packet.
5) The average number of consecutively received packets before seeing a sent packet.
6) Total number of bytes in sent packets.
7) Total number of bytes in received packets.
8) Number of different sizes in sent packets.
9) Number of different sizes in received packets.
10) Maximum packet size.
11) Mode of sent packet lengths (i.e., the packet size that appeared most in the monitoring window).
12) Mode of received packet lengths.
13) The variance of sent packet size distribution.
14) The variance of received packet size distribution.

WiFi-based IoT Devices Profiling Attack based on Eavesdropping of Encrypted WiFi Traffic
Evaluation

- Testbed
  - 10 devices (2 non-IoT)
  - 1 hour capture
  - Dataset split: 75% training and 25% testing

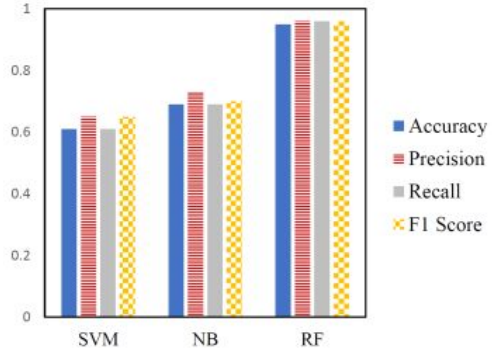
Device	15 min	15 min	30 min
Laptop	Browsing	Streaming	Idle
iPhone	Social Media		
TV	Internet Television App		
TV fire stick	Streaming		
Amazon Echo	Receive a query/control command regularly	Play media (e.g., Music)	
Google Home			
Printer	Occasionally Printing		
Bulb	ON		OFF
Plug			
Baby Monitor			
Doorbell			
Camera			

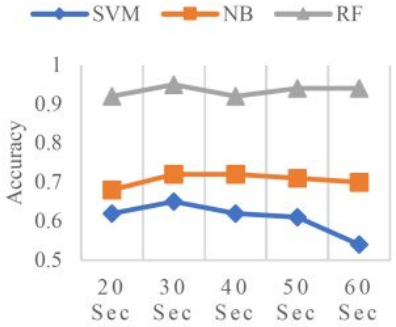
WiFi-based IoT Devices Profiling Attack based on Eavesdropping of Encrypted WiFi Traffic

Model Accuracy Results

- Accuracy, Precision, Recall and F1 Score

		SVM	NB	RF
Time Series	Non-IoT	0.34	0.25	**0.41**
	IoT	0.57	**0.74**	0.68
Summary Data	Non-IoT	0.51	0.41	**0.94**
	IoT	0.65	0.77	**0.96**





WiFi-based IoT Devices Profiling Attack based on Eavesdropping of Encrypted WiFi Traffic

Discussion

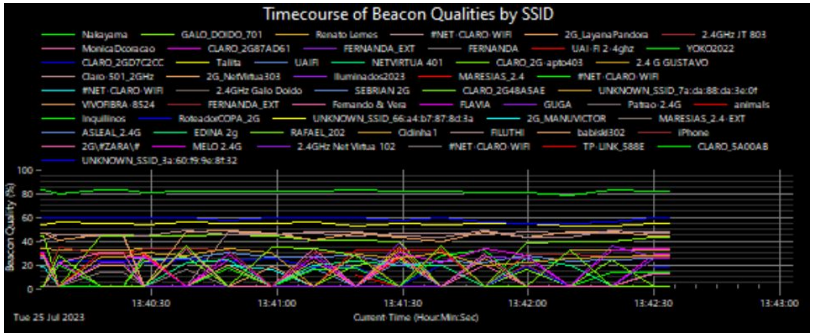
- Implications
  - Privacy concerns
  - Environmental awareness
- Defenses
  - Encrypt MAC information
  - Obfuscation through virtual devices

WiFi-based IoT Devices Profiling Attack based on Eavesdropping of Encrypted WiFi Traffic

Discussion

- Doubts
  - Dataset construction
  - Evaluation regarding more robust models
  - Obfuscation in MAC-layer

SSID	BSSID	Channel	RSSI (dBm)	Security
CLARO_5GD7C2CC	[redacted]:d7:c2:d1	100	-73	YES
Nakayama	[redacted]:9f:2c:f6	5	-35	YES
RENATO LEMES 5G	[redacted]:a3:21:f9	165	-100	YES
GUGA 5G	[redacted]:da:3e:0e	157	-90	YES
UNKNOWN_SSID_7a:da:88:da:3e:0e	[redacted]:da:3e:0e	157	-90	YES
Talita_5G	[redacted]:ed:4b:7c	157	-75	YES
MonicaDcoracao_5G	[redacted]:79:a6:dc	149	-80	YES
5.8 G GUSTAVO	[redacted]:b4:b3:be	149	-84	YES
GALO_DOIDO_701	[redacted]:17:22:c8	11	-76	YES
Renato Lemes	[redacted]:a3:21:f1	11	-79	YES
#NET-CLARO-WIFI	[redacted]:a2:0f:da	10	-63	None
2G_LayanaPandora	[redacted]:e2:0f:da	10	-63	YES
2.4GHz JT 803	[redacted]:c8:85:e0	9	-100	YES
MonicaDcoracao	[redacted]:79:a6:d8	4	-76	YES
CLARO_2G87AD61	[redacted]:87:ad:6e	5	-84	YES
FERNANDA_EXT	[redacted]:35:0a:7f	4	-100	YES
FERNANDA	[redacted]:a2:ae:14	4	-100	YES
UAI-FI 2-4ghz	[redacted]:e8:1b:94	3	-78	YES
YOKO2022	[redacted]:87:8d:3a	2	-76	YES
CLARO_2GD7C2CC	[redacted]:d7:c2:d9	11	-53	YES
Talita	[redacted]:ed:4b:78	1	-57	YES
5G_LayanaPandora	[redacted]:e2:0f:db	44	-73	YES
UAI-FI	[redacted]:e8:1b:95	36	-83	YES
UAIFI	[redacted]:d9:11:e0	7	-82	YES
NETVIRTUA 401	[redacted]:7e:c9:1f	7	-82	YES
CLARO_2G-apto403	[redacted]:31:69:c3	11	-66	YES
2.4 G GUSTAVO	[redacted]:b4:b3:b6	1	-75	YES
Claro-501_2GHz	[redacted]:4c:55:be	1	-64	YES
2G_NetVirtua303	[redacted]:83:08:c5	1	-100	YES
Claro-501_5GHz	[redacted]:4c:55:bf	52	-91	YES
FILUTHI_5G	[redacted]:79:ec:c8	149	-90	YES
UNKNOWN_SSID_66:a4:b7:87:8d:3b	[redacted]:87:8d:3b	44	-100	YES
Iluminados2023	[redacted]:d3:22:90	1	-82	YES
UAIFI_5G	[redacted]:d9:11:e4	149	-100	YES
MARESIAS_2.4	[redacted]:94:94:cc	11	-100	YES
#NET-CLARO-WIFI	[redacted]:28:89:1c	9	-100	None
animals	[redacted]:bd:10:cf	40	-86	YES
CLARO_5G87AD61	[redacted]:87:ad:66	40	-84	YES
#NET-CLARO-WIFI	[redacted]:09:94:d1	1	-100	None
2.4GHz Galo Doido	[redacted]:09:92:d0	1	-100	YES



fernandonakayama@ufpr.br