Machine learning software to detect ARP poisoning and sniffers: WLAN Unal

By : Nicolas Ricardo Enciso

UNSECURELAB

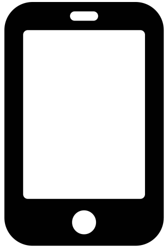
Topics:

- ARP poisoning/spoofing
- Packages sniffers
- Related paper
- Case of study
- Methodology: ML
- Conclusions
- References

UNSECURELAB

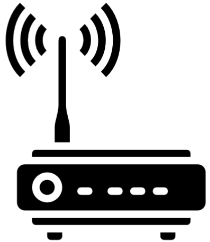
ARP Protocol: brief explanation

IP: 192.168.0.3
MAC: 01-00-5f-02-00-09



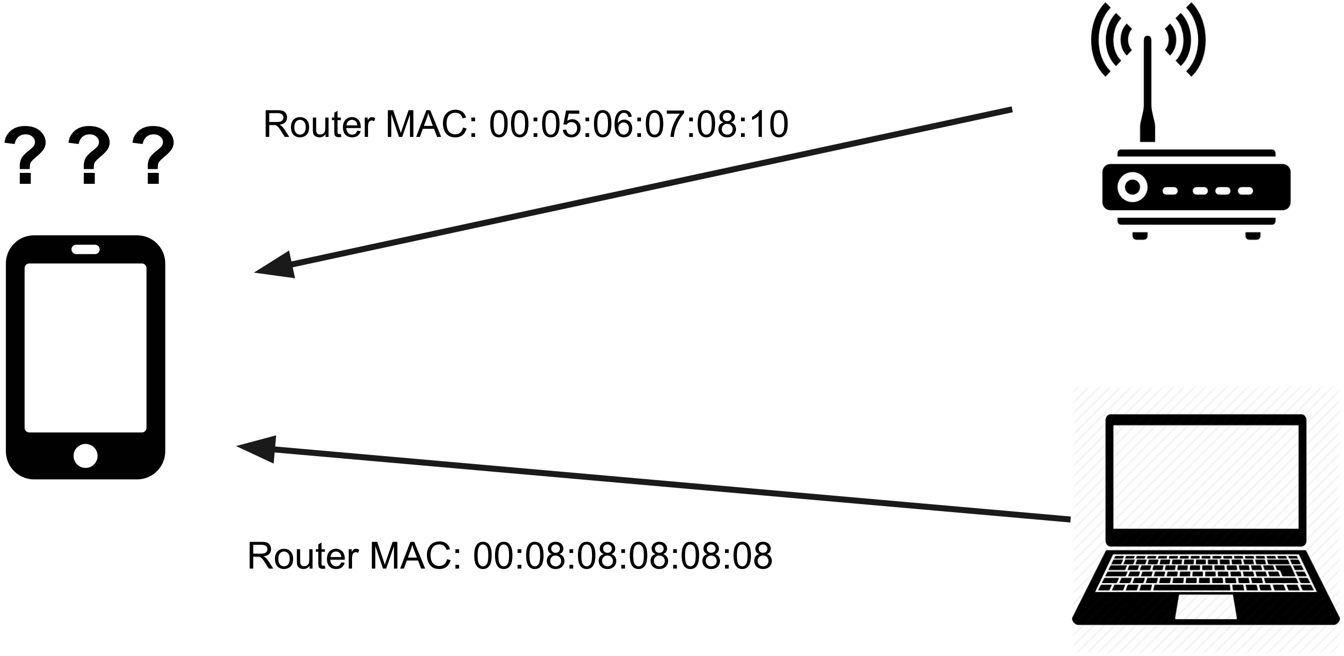
IP address	MAC address	Type
192.168.0.2	01-00-5e-00-00-16	Dynamic
192.168.0.255	FF-FF-FF-FF-FF-FF	Static

IP: 192.168.0.2
MAC: 01-00-5e-00-00-16

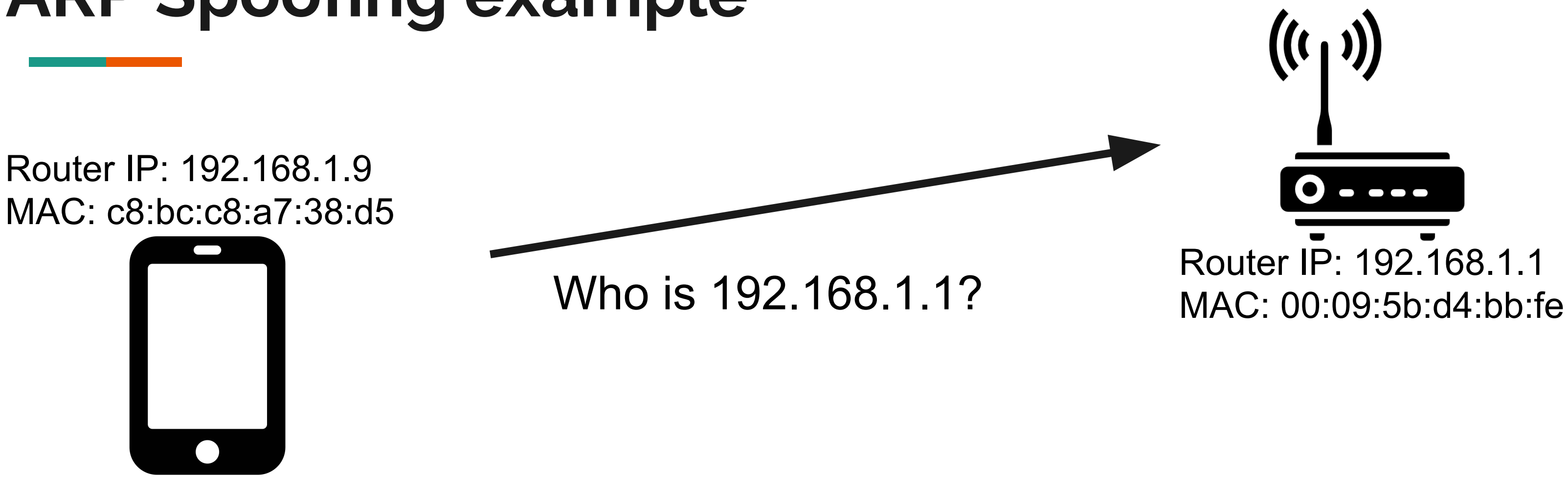


IP address	MAC address	Type
192.168.0.3	01-00-5f-02-00-09	Dynamic
192.168.0.255	FF-FF-FF-FF-FF-FF	Static

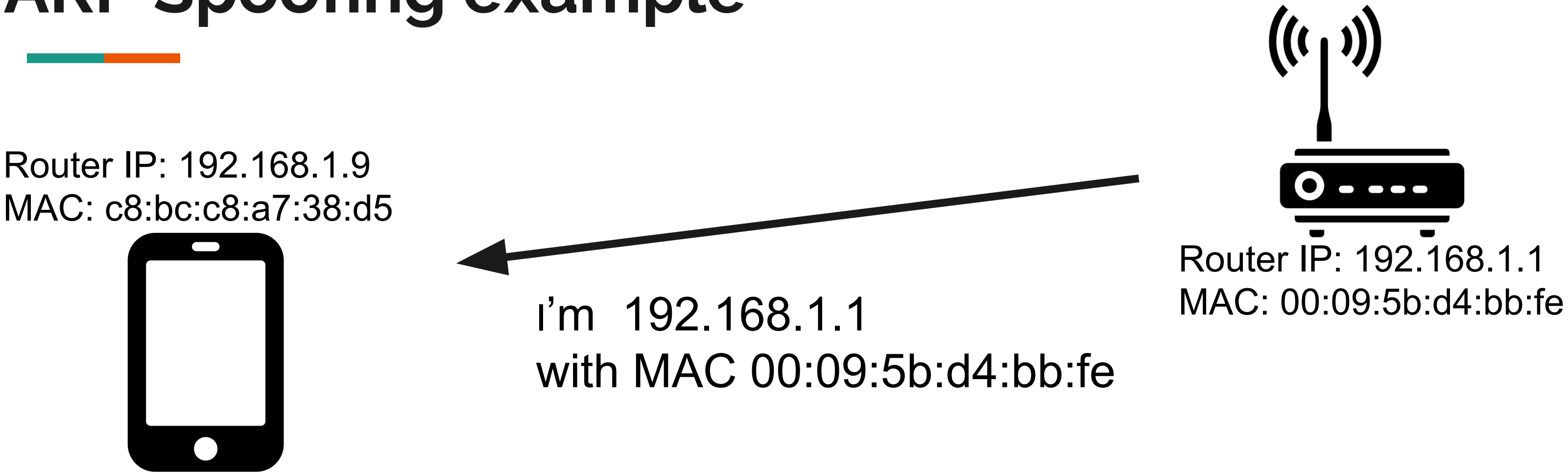
ARP poisoning/spoofing



ARP Spoofing example

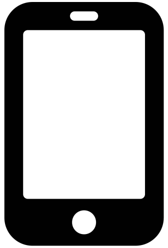


ARP Spoofing example

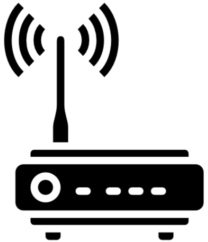


ARP Spoofing example

Router IP: 192.168.1.9
MAC: c8:bc:c8:a7:38:d5



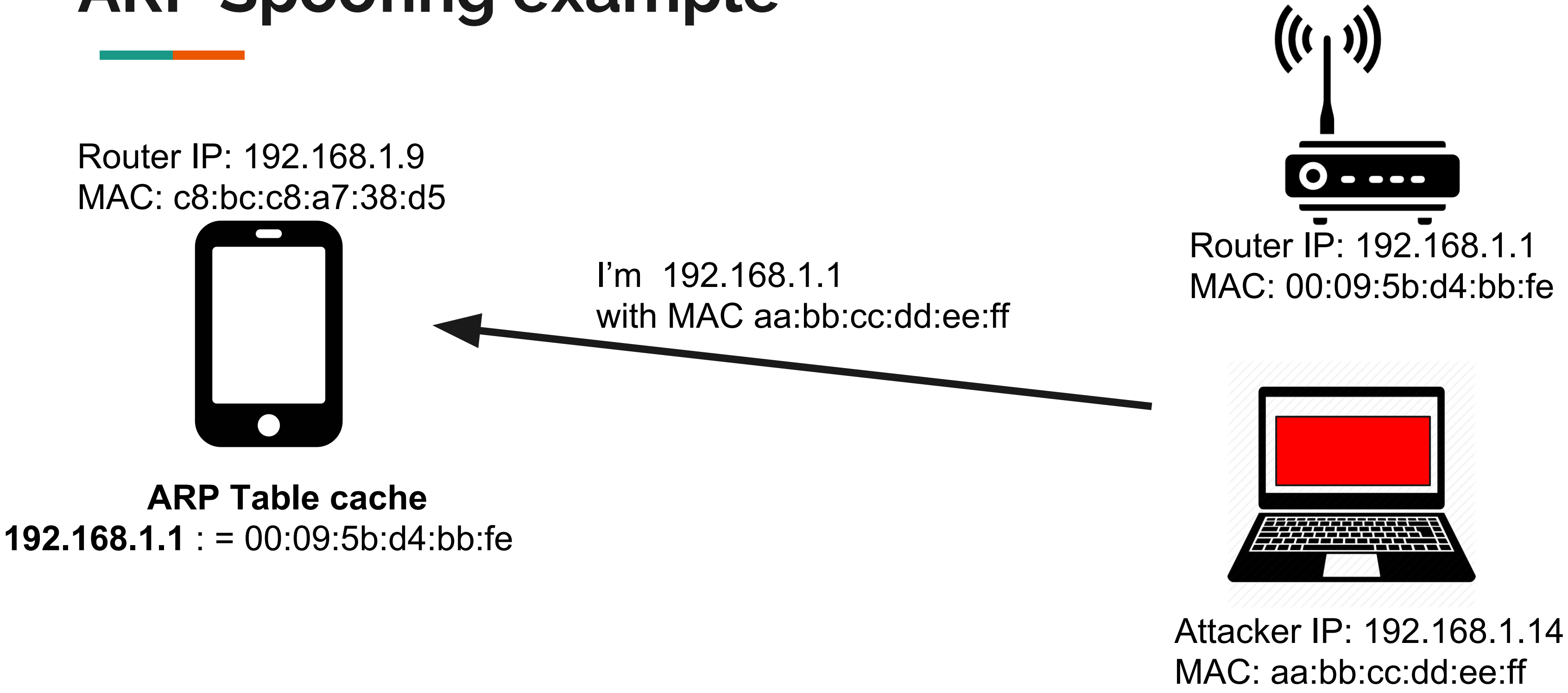
I’m 192.168.1.1
with MAC 00:09:5b:d4:bb:fe



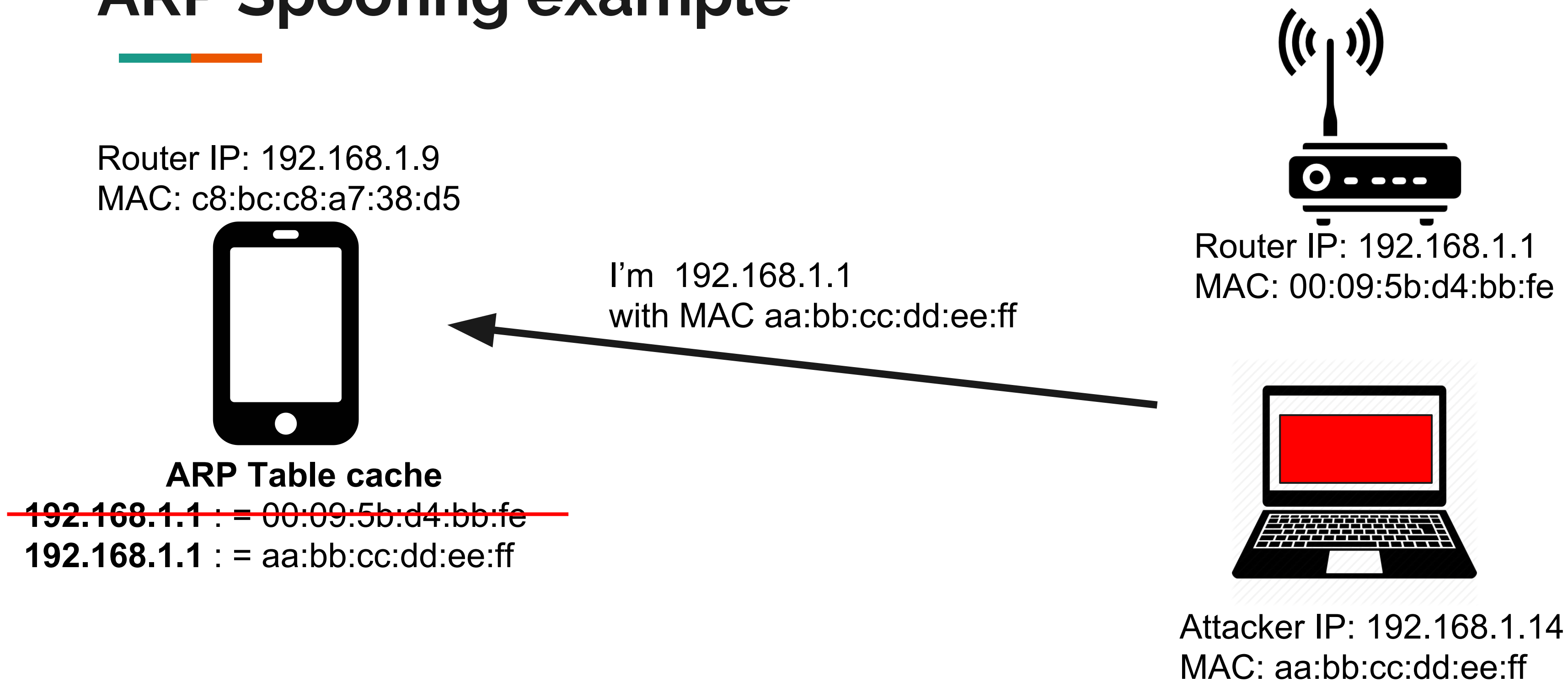
Router IP: 192.168.1.1
MAC: 00:09:5b:d4:bb:fe

ARP Table cache
192.168.1.1 : = 00:09:5b:d4:bb:fe

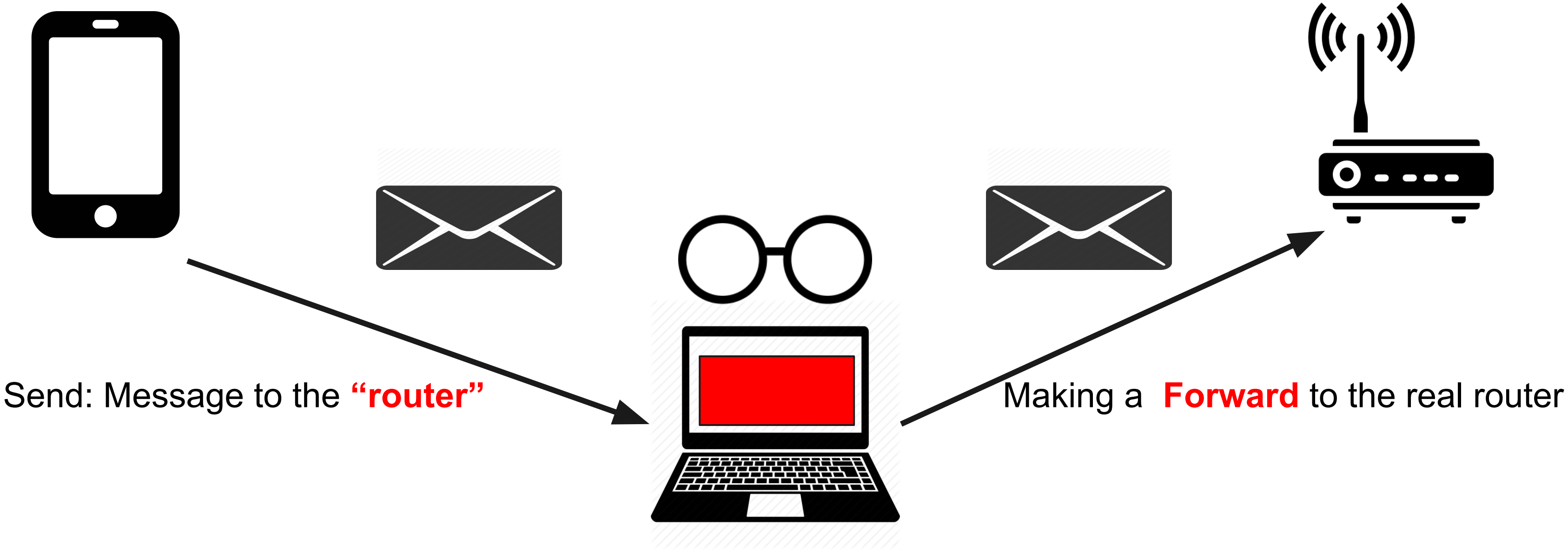
ARP Spoofing example



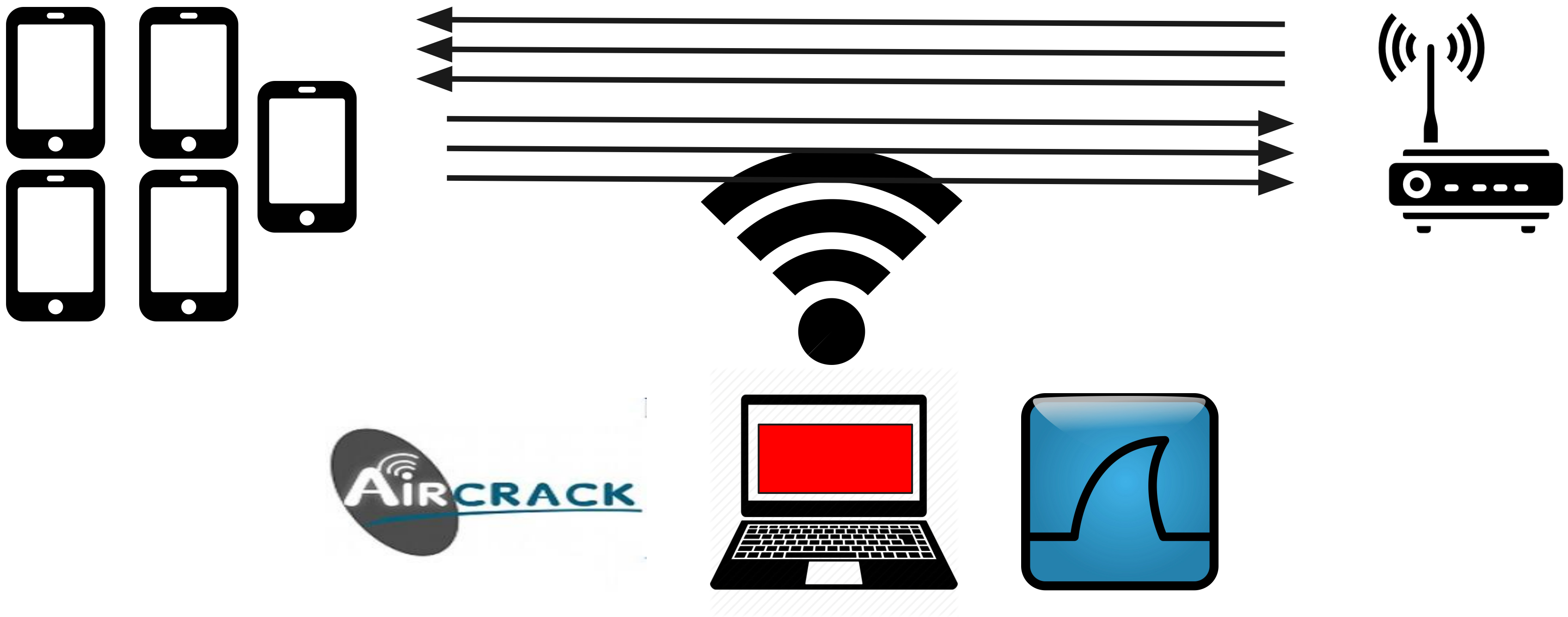
ARP Spoofing example



ARP Spoofing example



Sniffers in wifi



Related paper: brief review

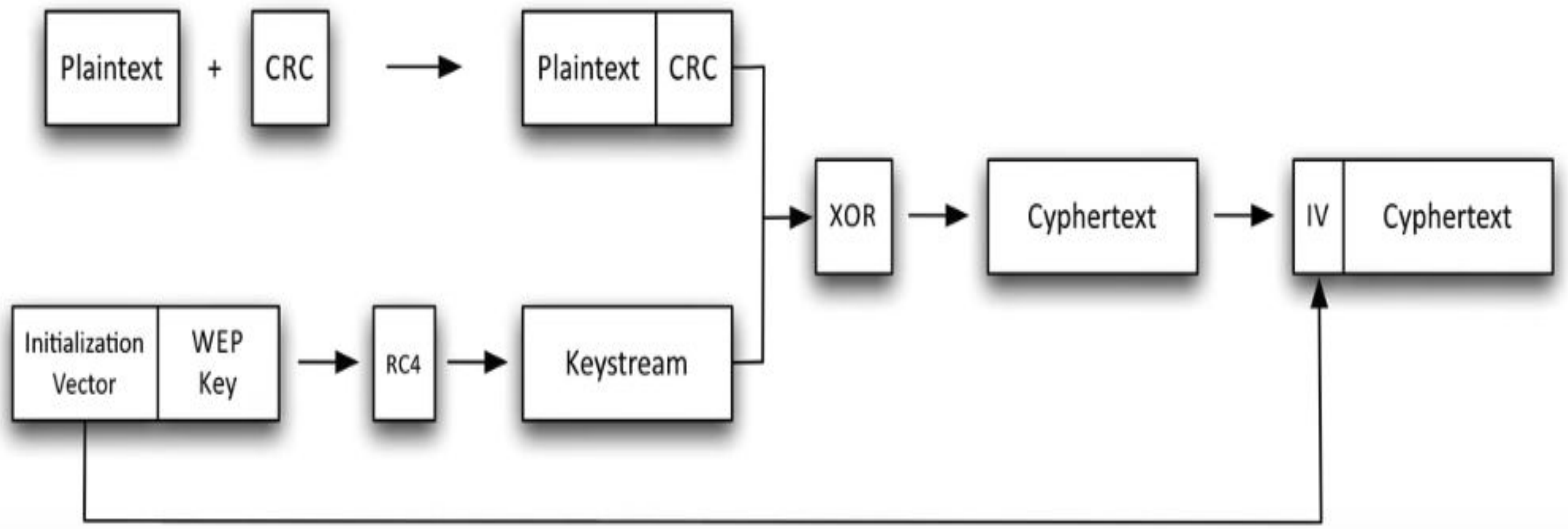
Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset

Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Stefanos Gritzalis

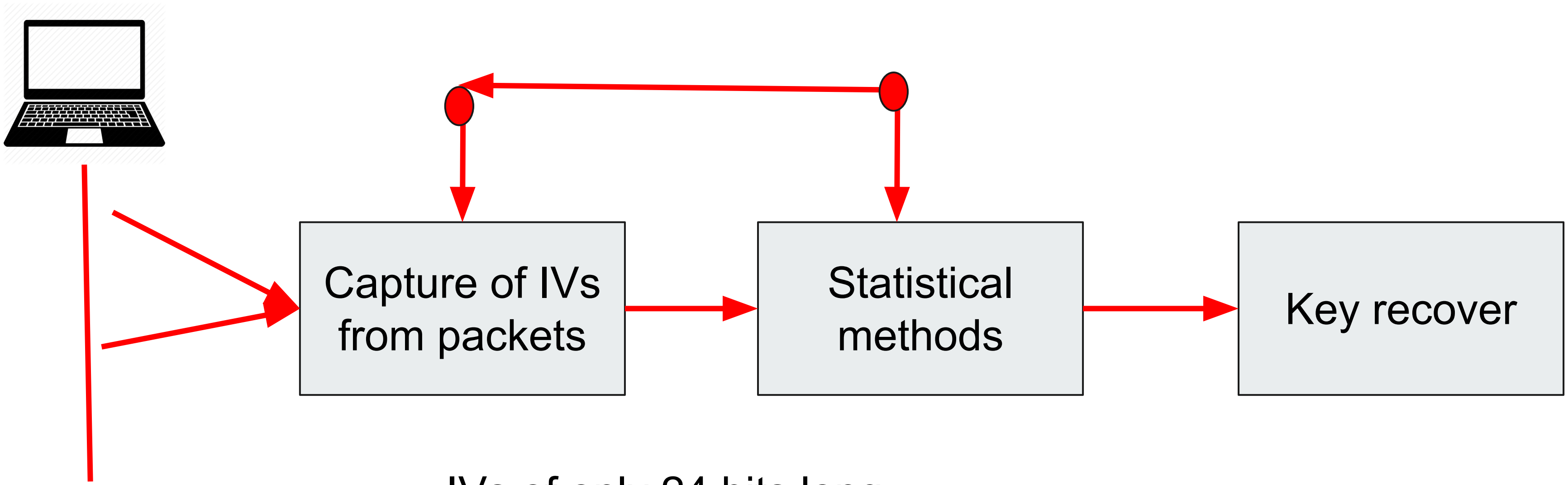
Topics at the paper

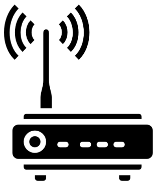
- Provides an open dataset for NIDS
- Explains architecture and components in 802.11
- Focus on wifi attacks
- Apply some machine learning techniques

WEP encryption



Attacks in WEP : IVs attack





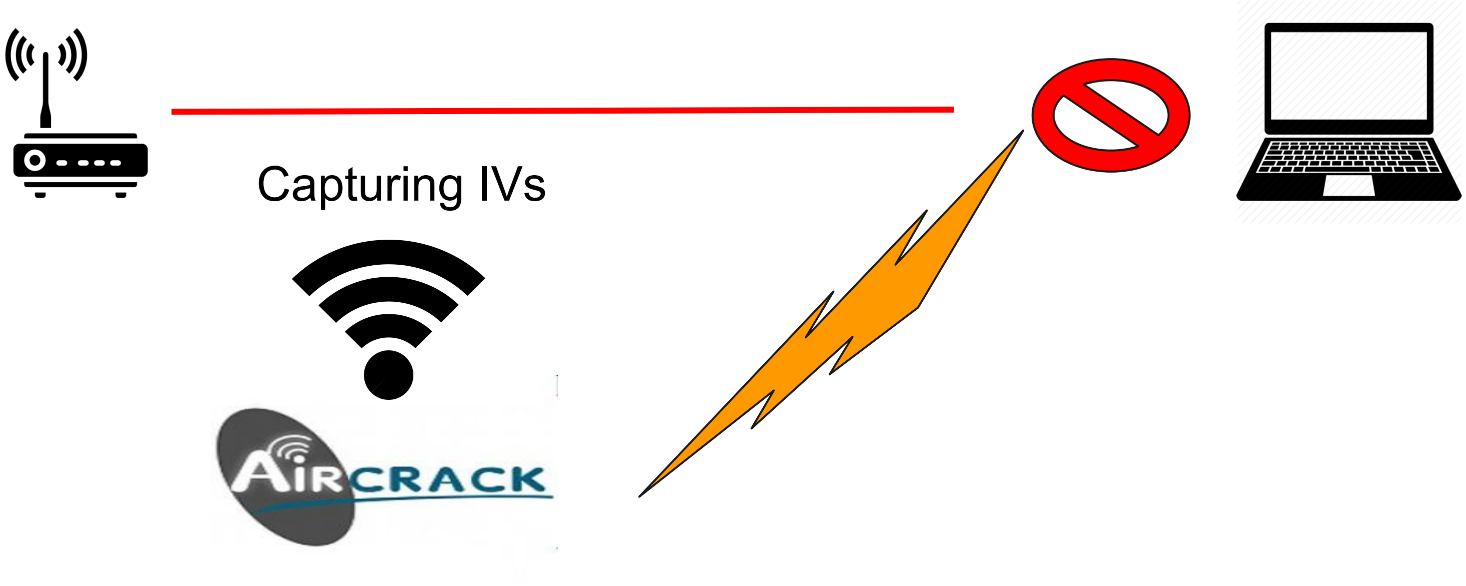
- IVs of only 24 bits long
- 16.777.216 possible RC4 cipher options. Easy brute force.
- IVs reused and static

Overall attack against WEP

1. Scan the network

Overall attack against WEP

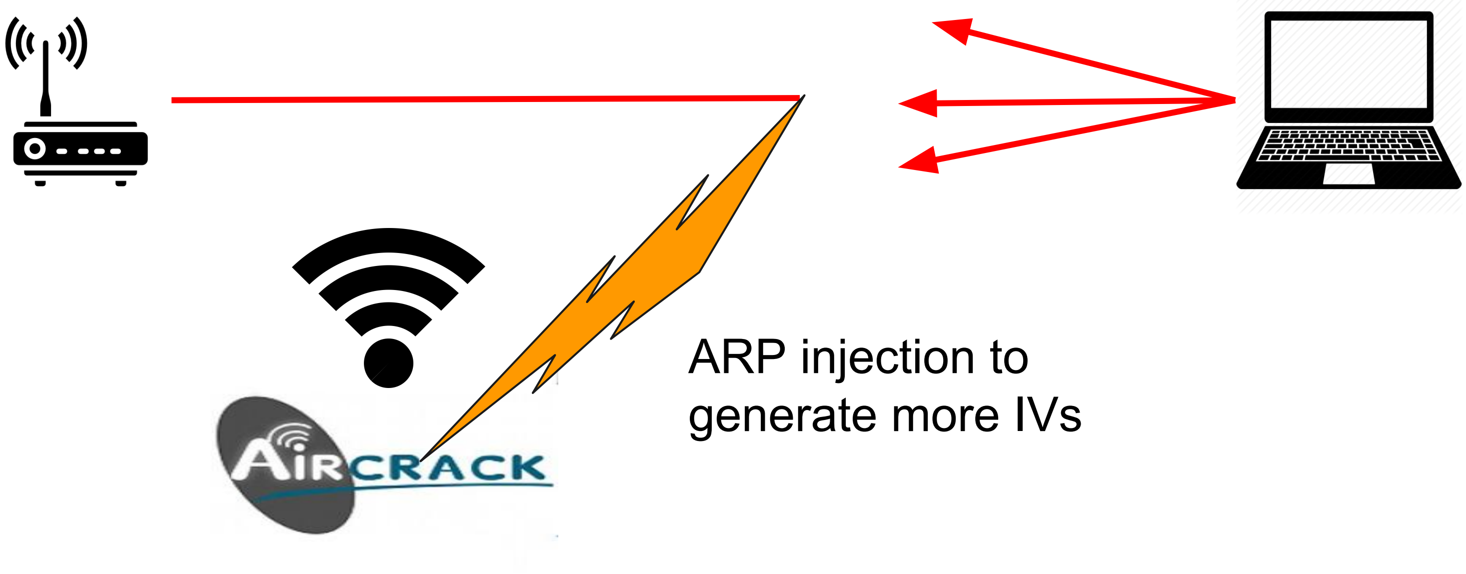
2. Capture IVs and force deauthentication



Overall attack against WEP

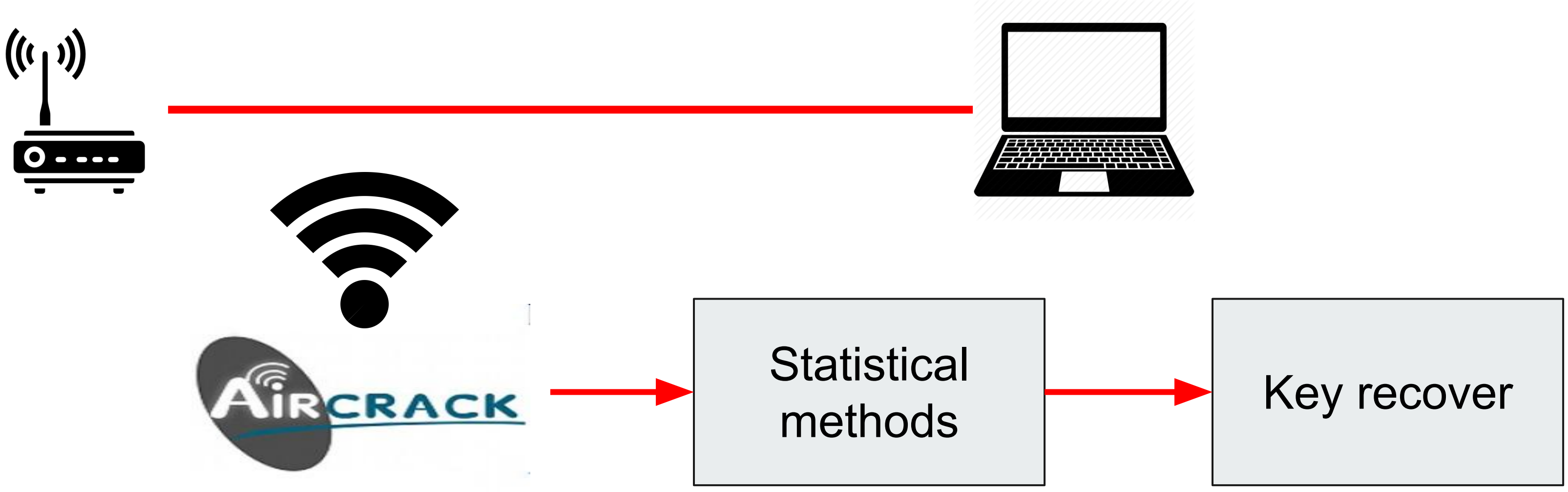
3. ARP injection

Tries to reconnect
sending ARP requests

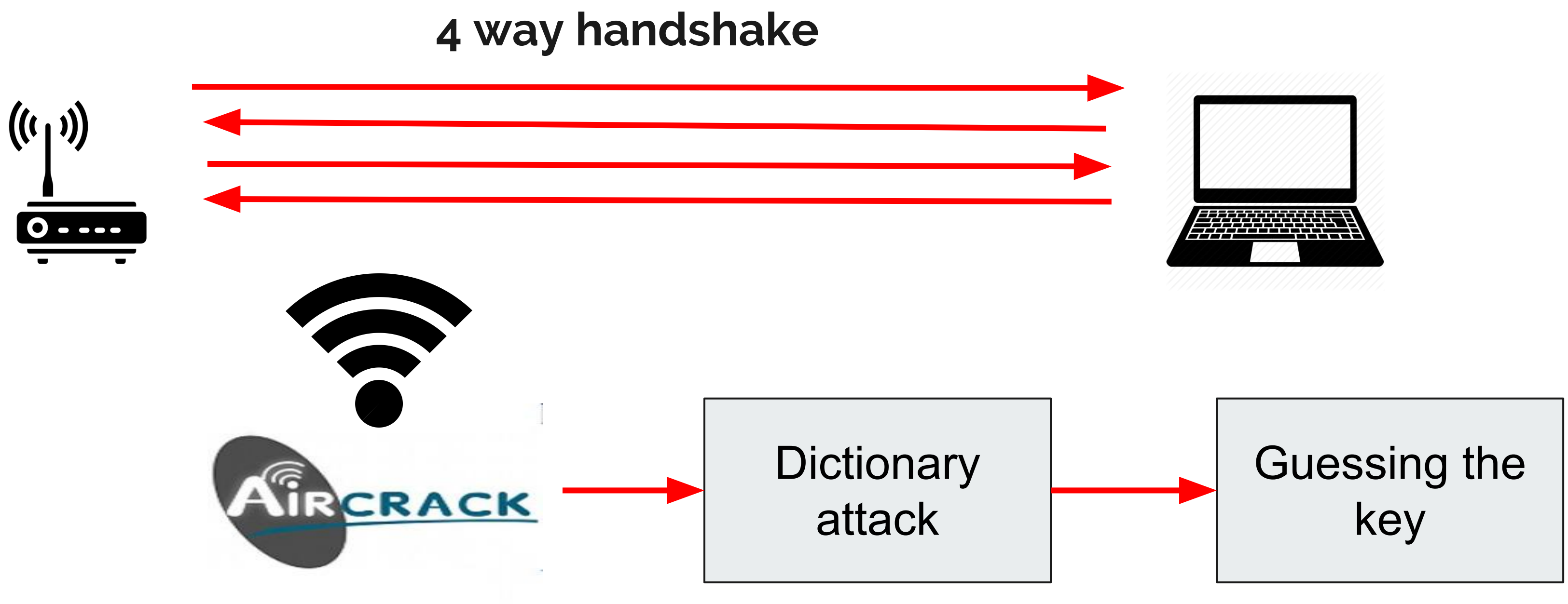


Overall attack against WEP

4. Perform a PTW, FMS or KoreK



Attack against WPA/PSK



Capturing IVs for each attack

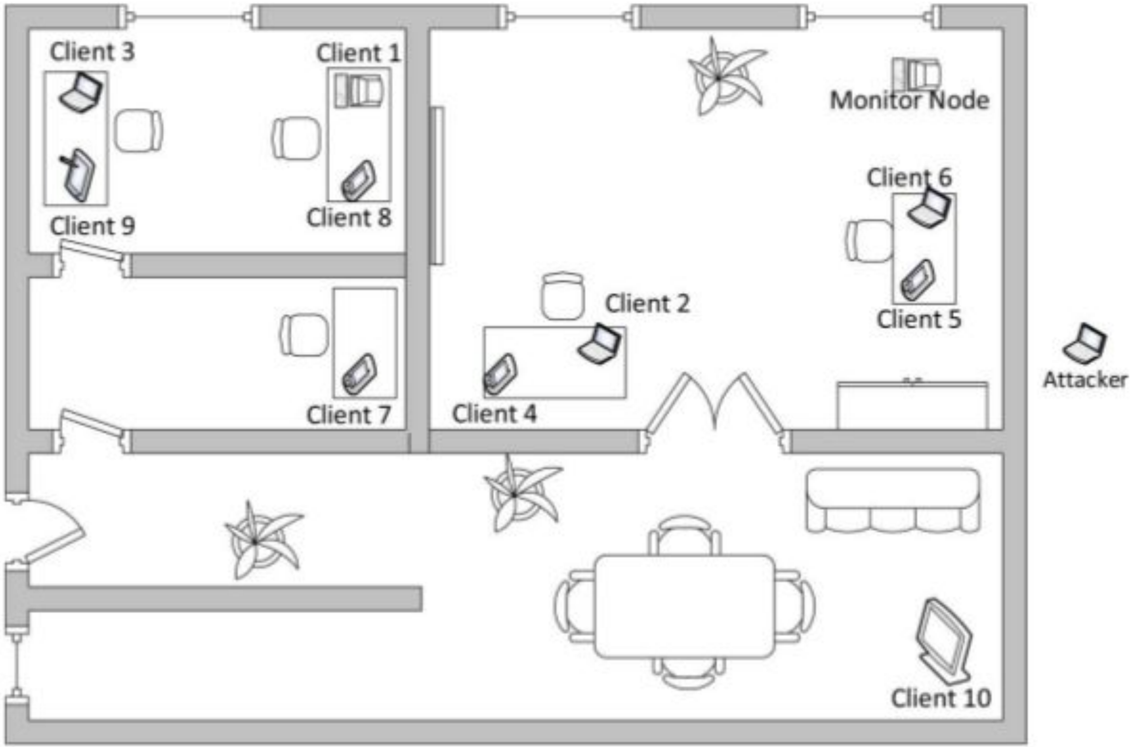
Number of IVs needed to perform the attacks:

TABLE II
AVERAGE IVS REQUIRED FOR WEP CRACKING BY VARIOUS ATTACKS

Attack	IVs (average)	Success	Year
FMS	5,000,000	50%	2001
KoreK	700,000-2,000,000	50%	2004
PTW	40,000-500,000	50%-95%	2007
VX	32,700	50%-95%	2007
Modified PTW	24,200	50%-95%	2008

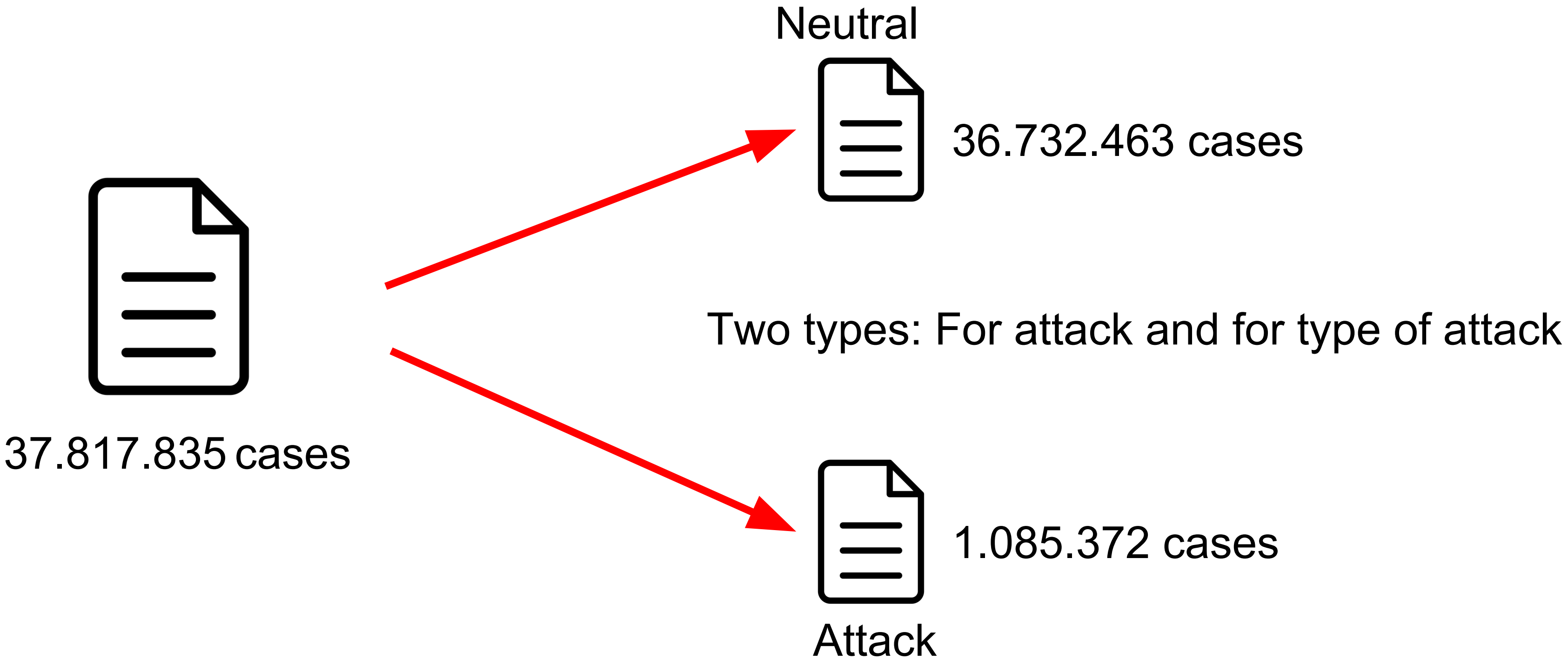
For more related info, references 9 and 10

Data set: Hardware and software



- 1 desktop
- 2 laptops
- 2 smartphones
- 1 tablet
- 1 smartTV
- 1 laptop attacker
- 1 router
- 1 Monitor Node

Data set: AWID



Machine learning algorithms

All machine learning algorithms:

- AdaBoost
- Hyper Pipes
- J48 / C4.5
- Naive bayes
- OneR
- Random Forest
- Random Tree
- ZeroR

First run: misclassified

- Very accurate but with high misclassified
- The 9 to 1 ratio between neutral and attack cases
- From 152 variables to 20 variables

Algorithm	Correctly Classified%	Incorrectly Classified%
AdaBoost	92.2073	7.7927
Hyperpipes	92.2073	7.7927
J48	96.1982	3.801
Naive Bayes	89.4323	10.5677
OneR	94.5758	5.4242
Random Forest	95.5891	4.4109
Random Tree	91.4379	8.5621
ZeroR	92.2073	7.7927

Second run: Better results

-Random forest and J48 algorithms were better

- To classify : 95% and 96% precision with low error in the confusion matrix

Algorithm	Correctly Classified%	Incorrectly Classified%
AdaBoost	92.2073	7.7927
Hyperpipes	92.2363	7.7637
J48	96.2574	3.7426
Naive Bayes	90.5504	9.4496
OneR	94.5741	5.4259
Random Forest	95.8247	4.1753
Random Tree	96.2258	3.7742
ZeroR	92.2073	7.7927

Conclusions

1. With a good dataset, ML is reliable in NIDS
2. Careful with the false positive
3. Unsupervised machine learning with good results avoiding labeling
4. Can be used for WPA/PSK research
5. Select the most important variables: more doesn't mean better
6. Keep in mind: Ratio between number of cases for each group in datset

My Project: Used software

NumPy

AIRCRACK

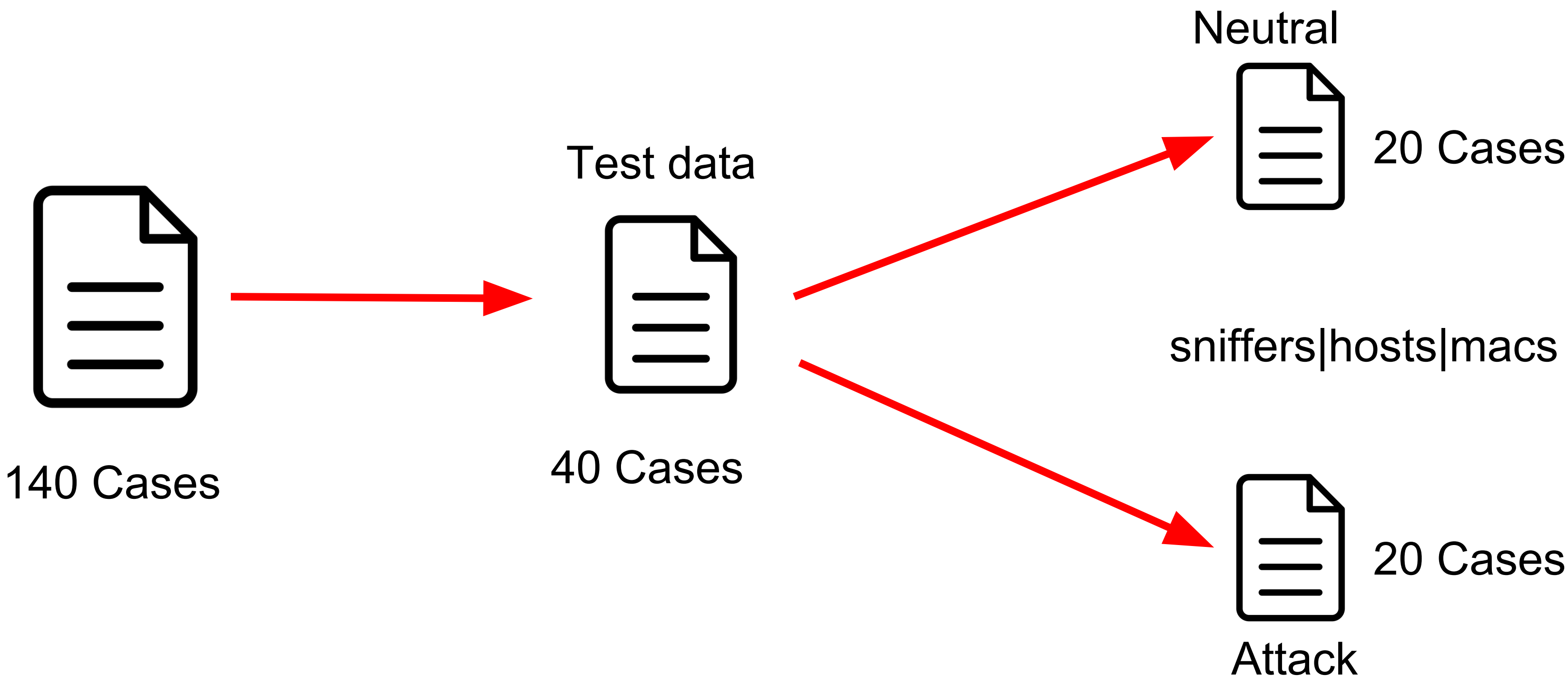
NMAP

Ettercap

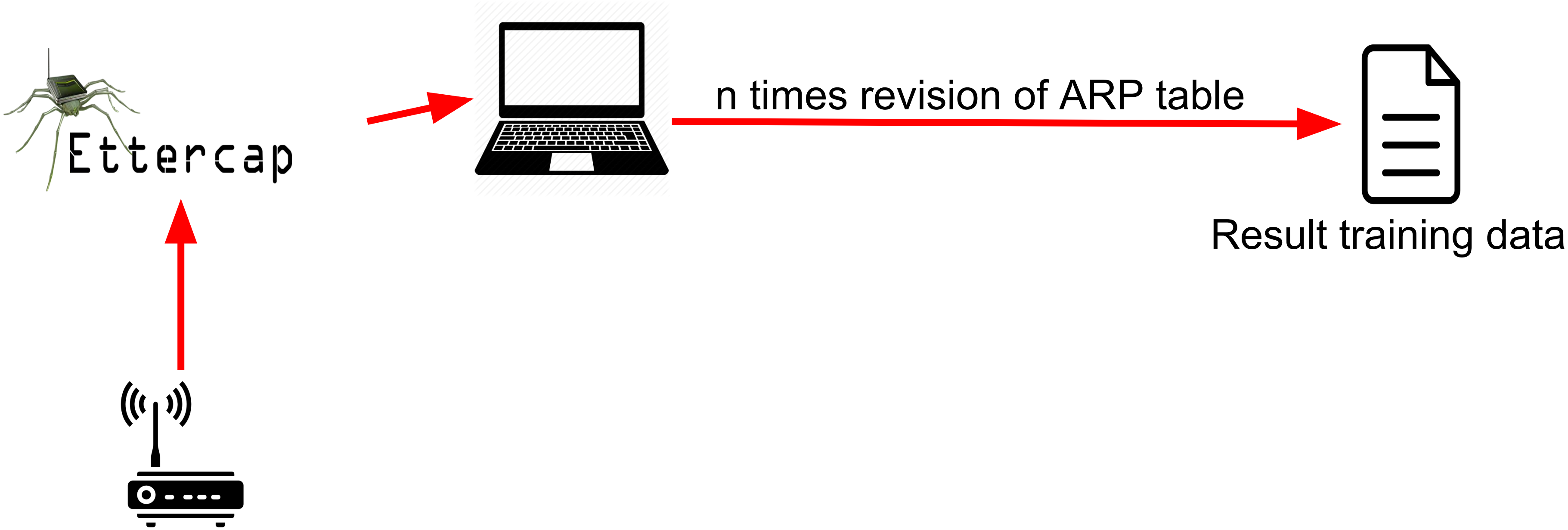
Project : Environment

- Wifi Unal_invitados
- Domestic wifi network
- Laptop running Kali linux
- Virtual machine with linux
- Extra wifi antenna TP- link

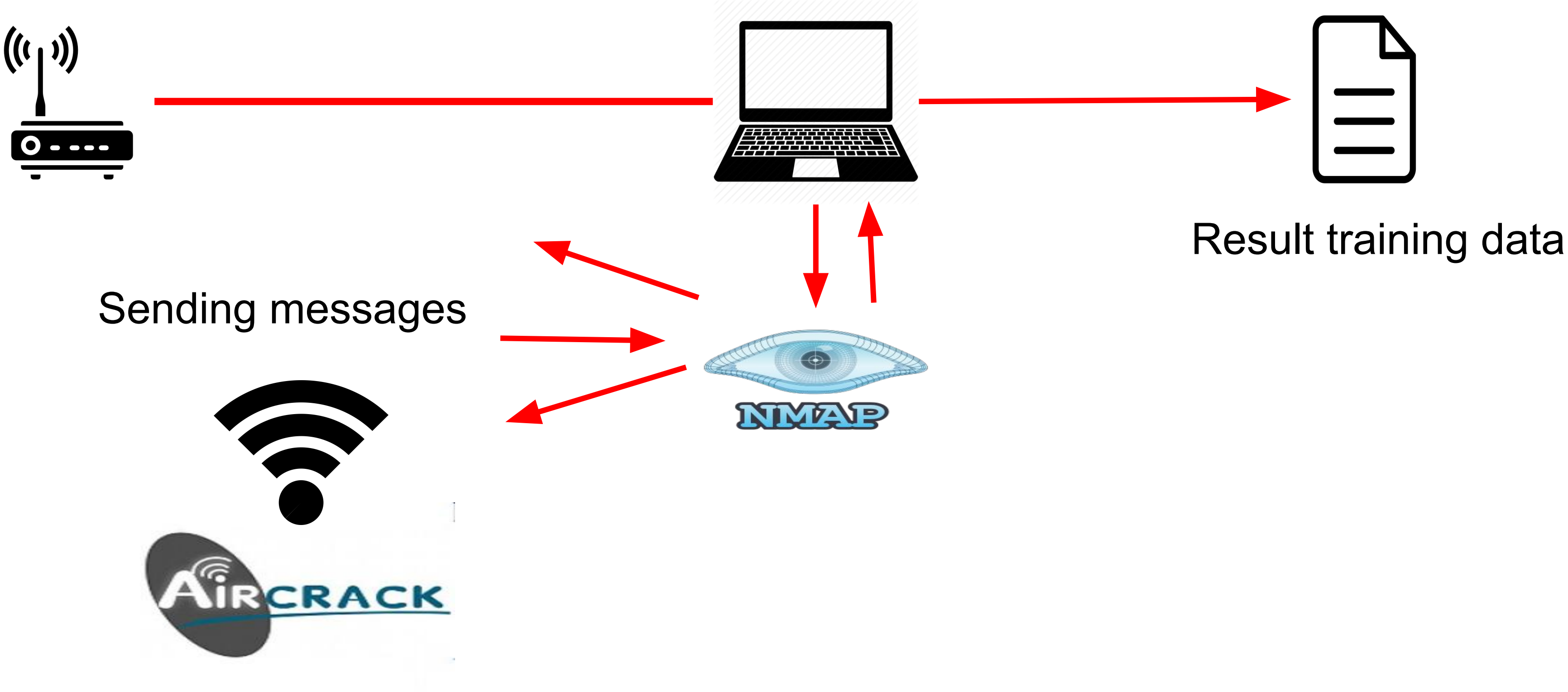
Project: Training data



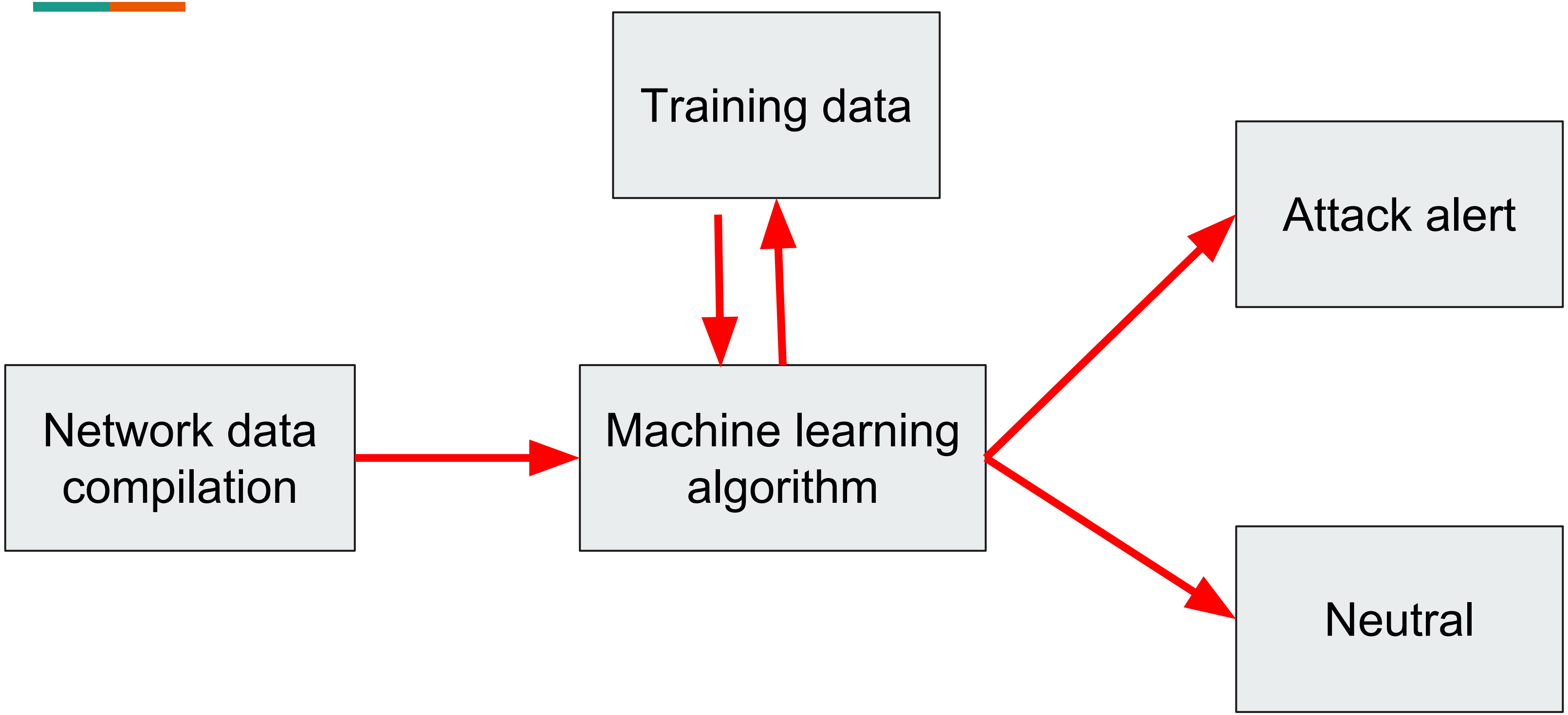
Project: ARP spoofing training



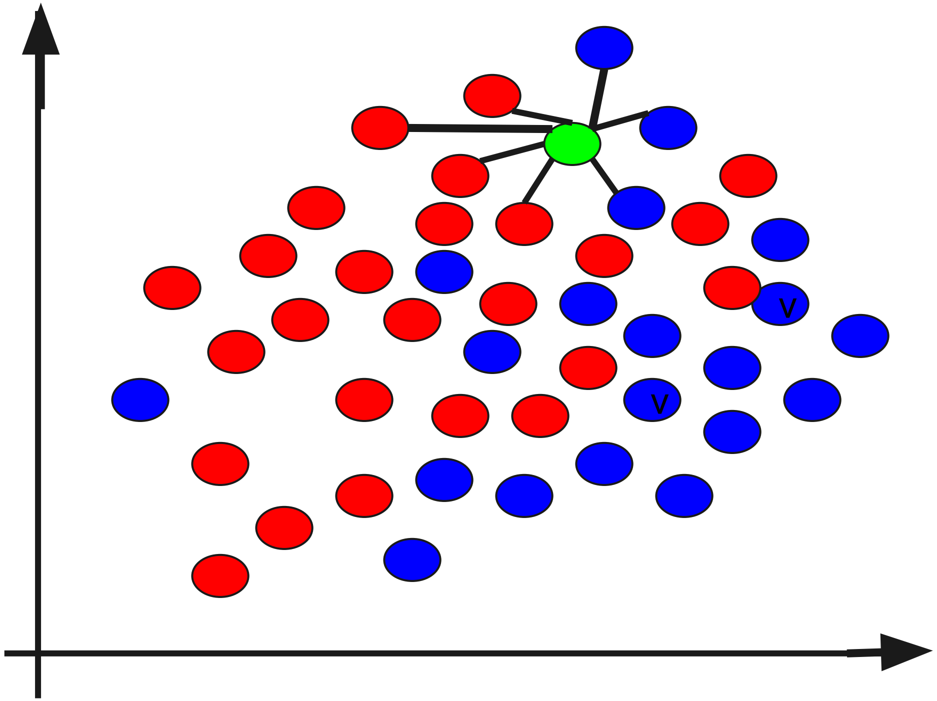
Project: Sniffing training



Machine learning algorithm



K - means algorithm



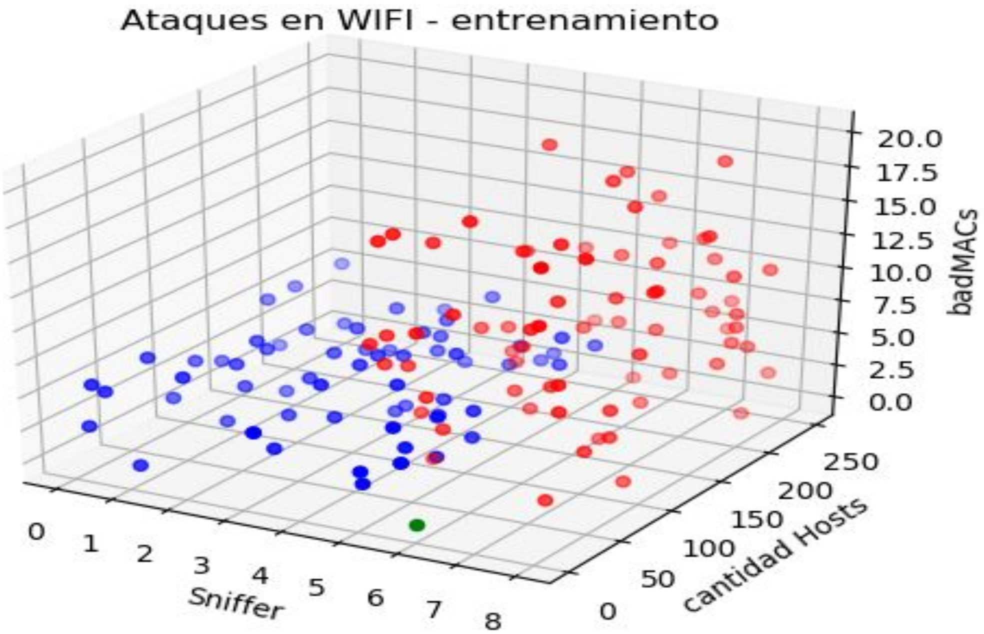
Actual case

Neutral case

Attack case

$$\sqrt{(X_1 - X_2)^2 + (Y_1 - Y_2)^2}$$

Project: K -means algorithm



Conclusions

- Nearly 60% accuracy.
- Tool with potential but relative high error
- Depends on the training data
- Needs larger data sets
- Better with combined ML techniques
- Very big field to research and create

References

1- Verizon 2017 Data Breach Investigations Report (DBIR,2017),Revisado en October 23, 2017 de http://www.verizonenterprise.com/verizon-insights-lab/dbir/20
17/

2- Sanjay Kumar, Ari Viinikainen, Timo Hamalainen, « Machine learning classification model for network based intrusion
detection system » , in 11th International conference for
internet technology and secured transactions (ICITST), 2016

3- Kriangkrai Limthing, Thidarat Tawsook, « Network traffic anomaly detection using machine learning approaches »,
Computer engineering department Bngkok University, 2015.

4 - Marek Majkowski, « Detection of promiscuous nodes using
ARP packets », NMAP documentation.

5- Book: Bob Fleck, Bruce Potter. (2015). 802.11 Security
Securing Wireless Networks. Estados Unidos: O'Reily.

References

6- Book: Stuart McClure, Joel Scambray, George Kurtz. (2016). Hacking exposed 7: network security secrets & solutions. Estados Unidos, New York: Mc Graw Hill. Nguyen Thanh Van, Tran Ngoc Thinh, Le Thanh Sach, « An amomaly-based network intrusion detection system using deep learning » , International conference on system science an engineering (ICSSE) , 2017.

7 - Jinsheng Xu1, Xiaohong Yuan, Anna Yu, Jung Hee Kim, Taehee Kim, Jinghua Zhang, " Developing and Evaluating a Hands-On Lab for Teaching Local Area Network Vulnerabilities» , Departamento de ciencias de la computación, Universidad del Estado de Carolina del Norte Greensboro A&T, Departamento de ciencias de la computación

8- Kazuki Fukuyama, Yoshiaki Taniguchi, Nobukazu Iguchi, « A Study on Attacker Agent in Virtual Machine-based Network Security Learning System", Universidad de Kink, Osaka Japón, IEEE 4ta Conferencia de electronica de consume, 2015.

9- Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, « Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset » , IEEE Encuestas de comunicaciones y tutoriales volúmen 18, Universidad del Egeo, Samos, Grecia, 2015.

References

10- Serge Vaudenay and Martin Vuagnoux, « Passive–Only Key Recovery Attacks on RC4 » , EPFL Laussane Switzertland CH- 1015 URL: https://link.springer.com/content/pdf/10.1007/978-3-540-77360-3_22.pdf