Intrusion Detection for WiFi and Bluetooth Protocols

DR. PRATIK SATAM

Introducing me

Position:

- Assistant Professor of Systems and Industrial Engineering
- Assistant Professor of Electrical and Computer Engineering

https://sie.engineering.arizona.edu/faculty-staff/faculty/pratik-satam

Name: Dr. Pratik Satam

Education:

- **Ph.D.** Electrical and Computer Engineering from University of Arizona, 2019
- **M.S.** Electrical and Computer Engineering from University of Arizona, 2015
- **B.E.** Electronics and Telecommunications Engineering from Mumbai University, 2013

Systems and Security Lab

THE UNIVERSITY OF ARIZONA

Teaching

- Courses taught previously in ECE:
  - **ECE 509:** Cyber Security- Concept, Theory, Practice
  - **ECE 524:** Cloud Security
  - **ECE 677:** Distributed Computing
  - Continuing and Profession Education (CAPE) at UArizona's Network and Computer Security certifications
- **Currently teaching:**
  - SFWE 411/511: Software for Industrial Control Systems (Fall)
  - SFWE 401/501: Software Assurance and Security (Spring)

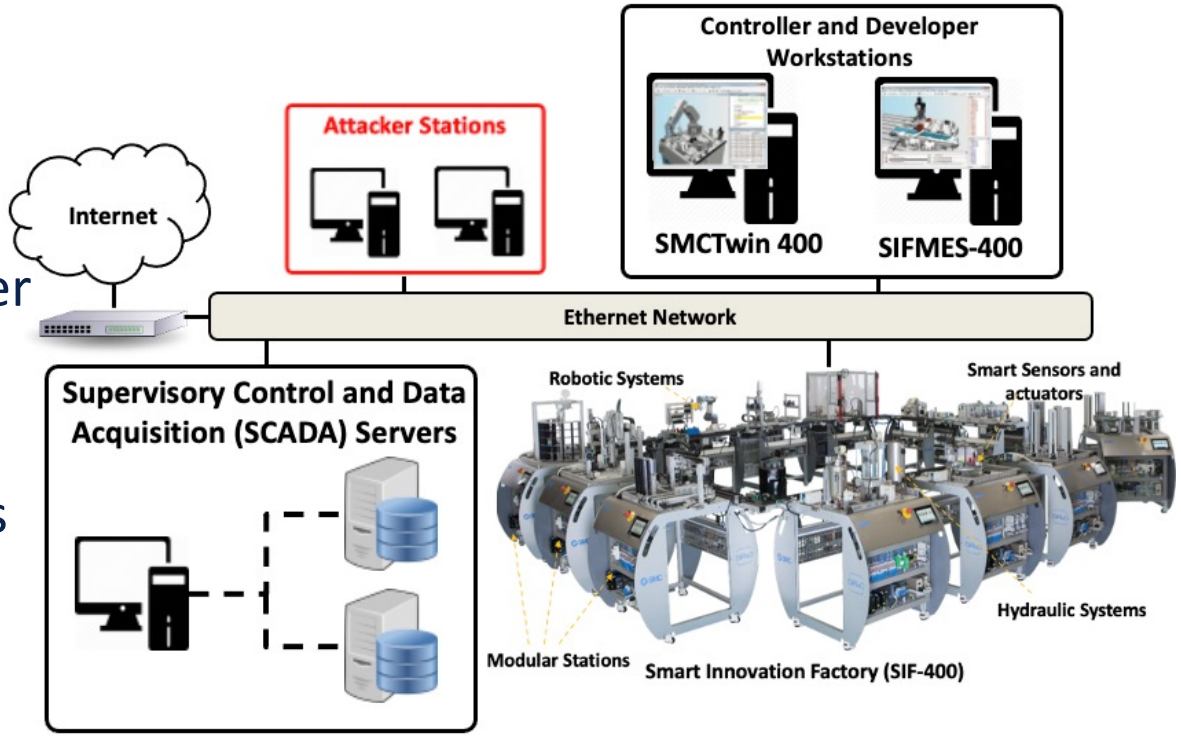
Research

- Research is on Cybersecurity with a focus:
  - Cyber physical system security
  - Network security
  - Computer security
  - Internet of Things Security
  - Software Security

UArizona Future Factory Testbed

The testbed consists of:

- SMC's Smart Innovation Factory (SIF-400)
- Controller and Developer Workstations
- Supervisory Control and Data Acquisition Servers
- Attacker Stations



Intrusion Detection

Goal of Intrusion Detection

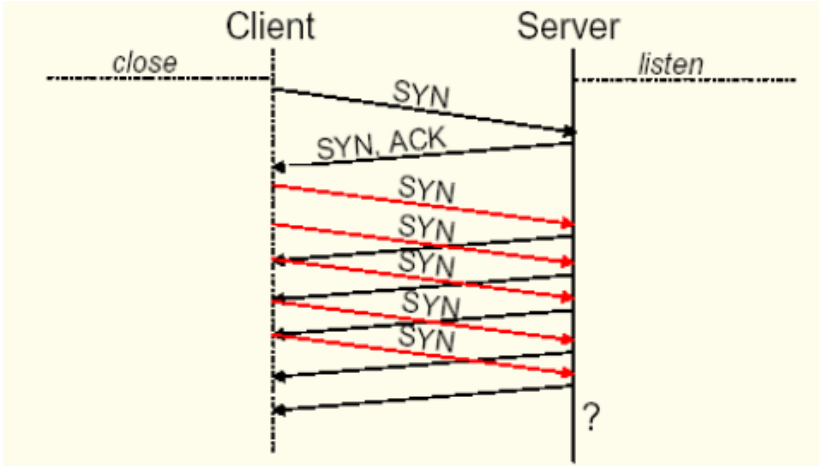
- What do you this is the goal of an Intrusion Detection System?
- What are its characteristics?

Goal of Intrusion Detection?

- Primary goal is to detect and stop attackers
- Generally a software to identify, assess, and report unauthorized access
- Tasks involved:
  - Detect Attacks
  - Raise alerts about the attacks

How to detect attacks?

- How would you go about detecting attacks?
- Lets take an example of ethernet network with syn flood



Signature based detection

- Create attack signatures to identify and detect attacks

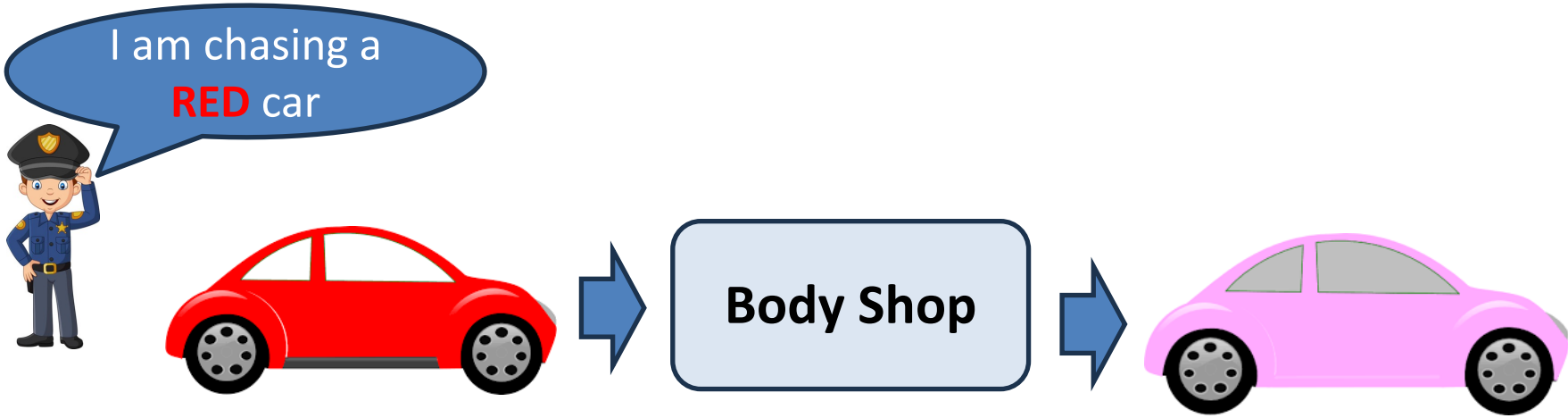
Example of a signature

- Here is an example SNORT rule to detect SYN Food

```
alert tcp any any -> $HOME_NET 80 (flags: S;
msg:"Possible TCP DoS"; flow: stateless;
detection_filter: track by_dst, count 70, seconds 10;)
```

Signature based detection problems

- What if the attack changes?



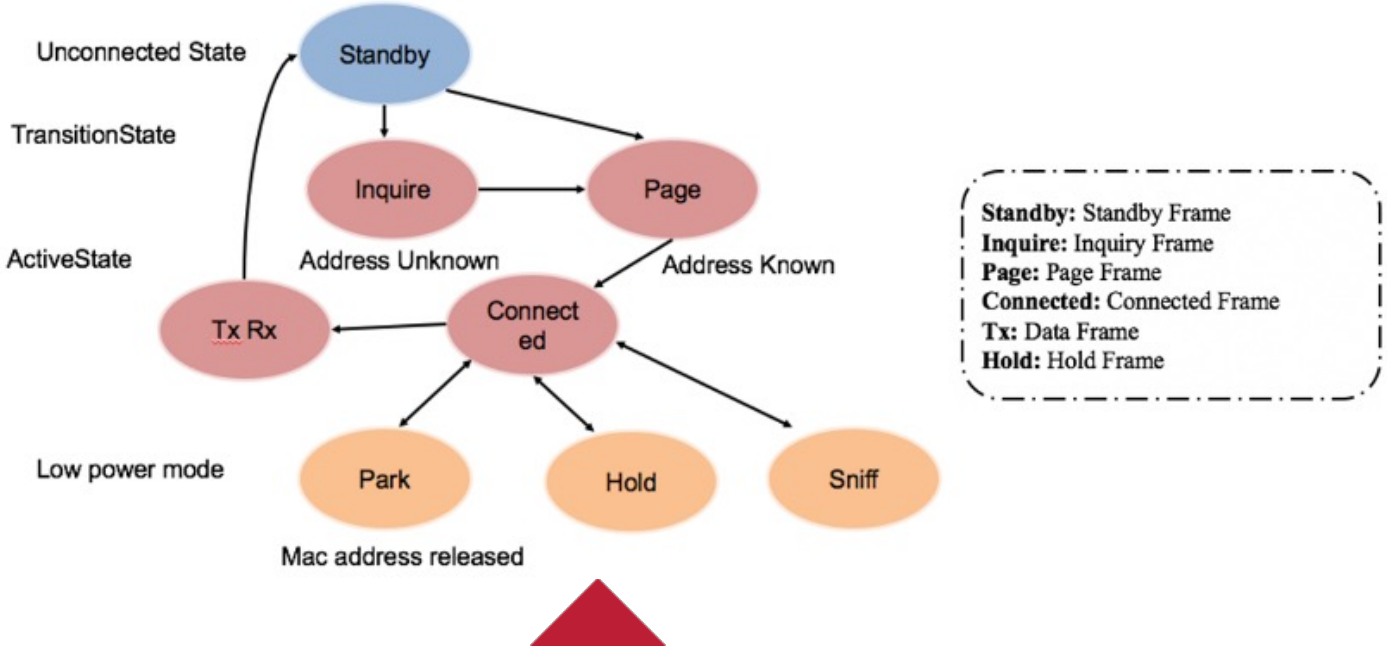
Anomaly based detection

- Learn the normal
- Use a model to detect normal

Anomaly Behavior Analysis based Intrusion Detection

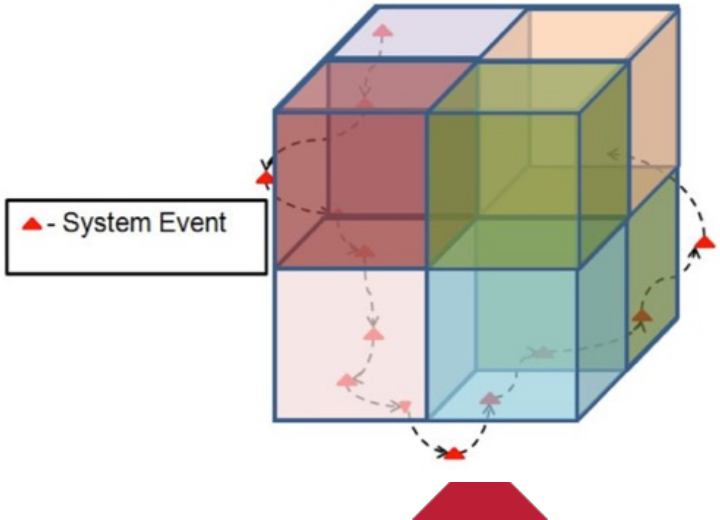
Anomaly Behavior Analysis

- Systems like communication protocols follow a specific state machine



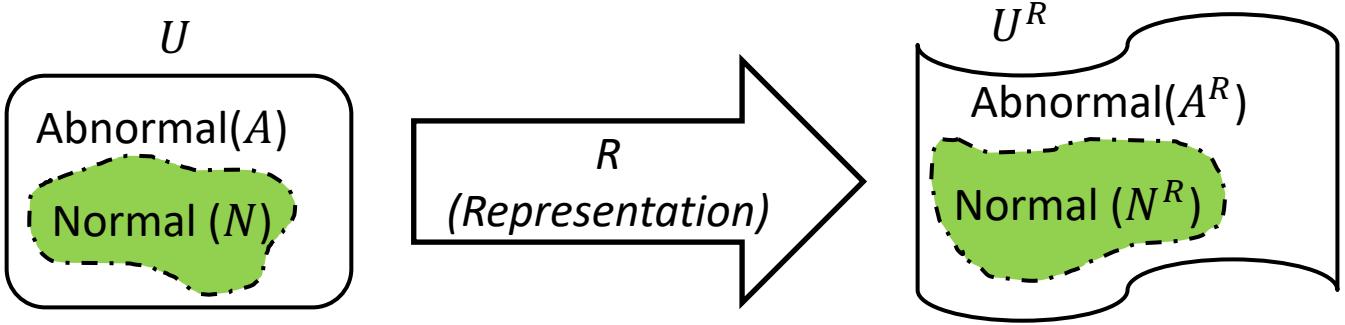
Anomaly Behavior Analysis

- State transitions through the protocol state machine can be tracked to analyze if the behavior is normal or not
- Abnormal Transitions can be detected through this monitoring



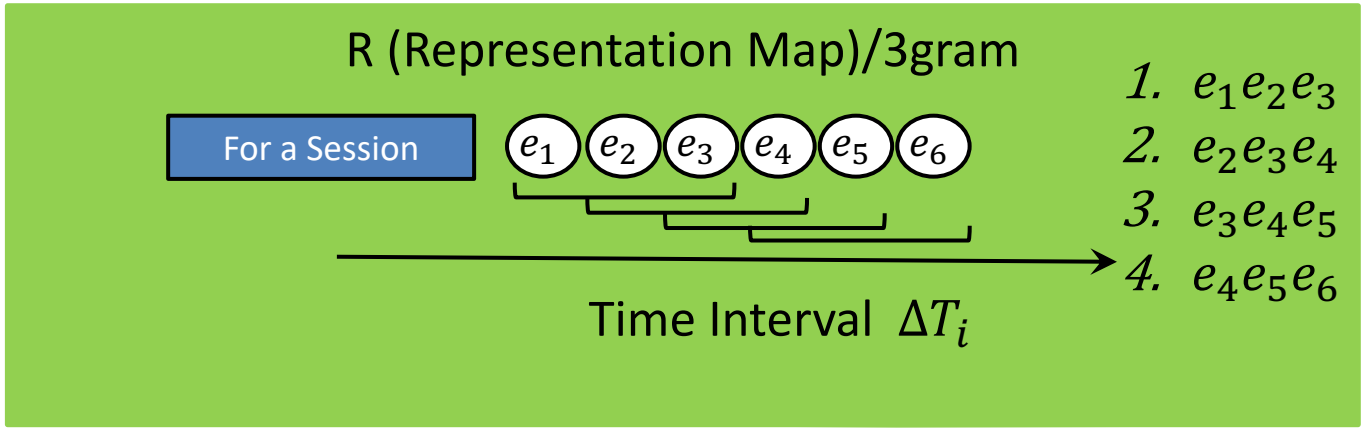
Event Space Definitions

- All events are in the space U and are of two types Normal and Abnormal
- A representation is used to observe them

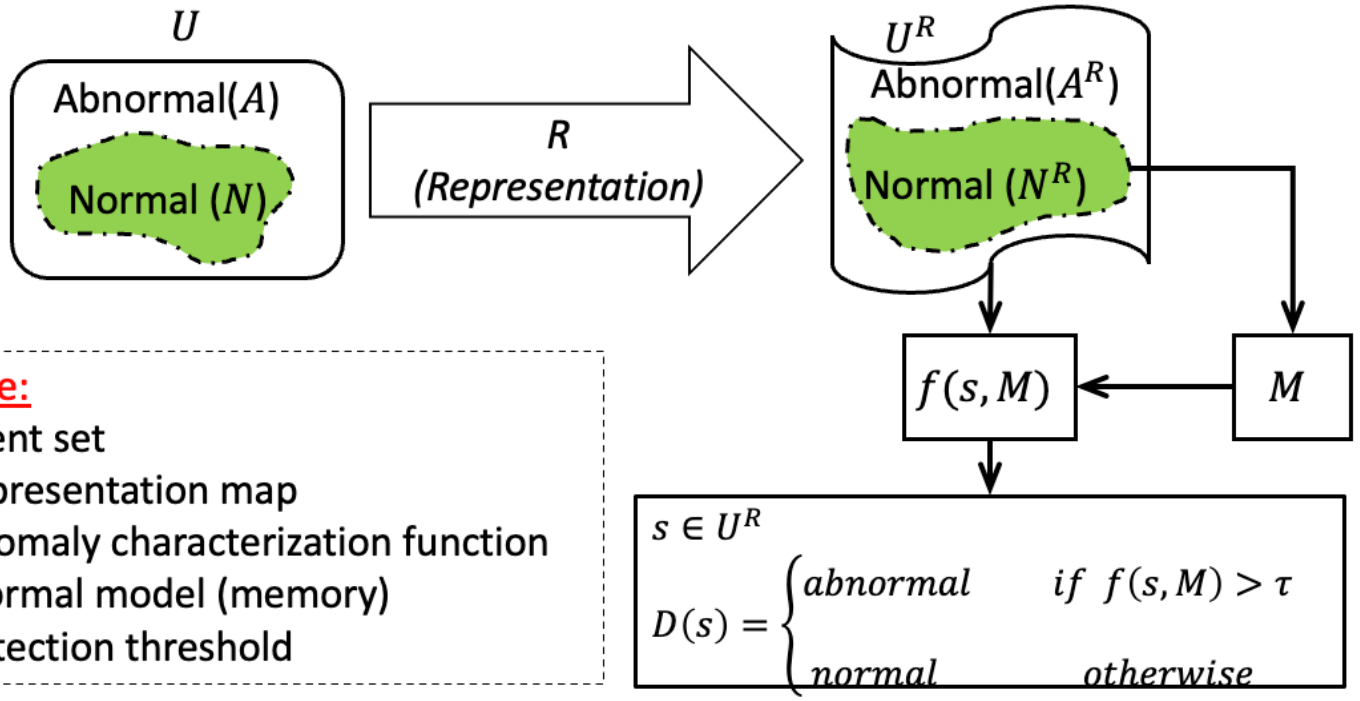


Tracking the state machine

- State transition through the state machine is tracked for events e_n through monitoring n-grams
- Generated n-gram patterns are: $\mathbb{P}_{l,\Delta T_i} = \{\{[e_{j_1}, \dots, e_{j_n}], \dots, [e_{j_{k-n+1}}, \dots, e_{j_k}]\}\}$
- Using these n-grams normal behavior models can be built



Problem Statement for ABA IDS



Need to define:

- U: The event set
- R: The representation map
- f: The anomaly characterization function
- M: The Normal model (memory)
- τ : The detection threshold

Use case1: WiFi Protocol

Wi-Fi Protocol

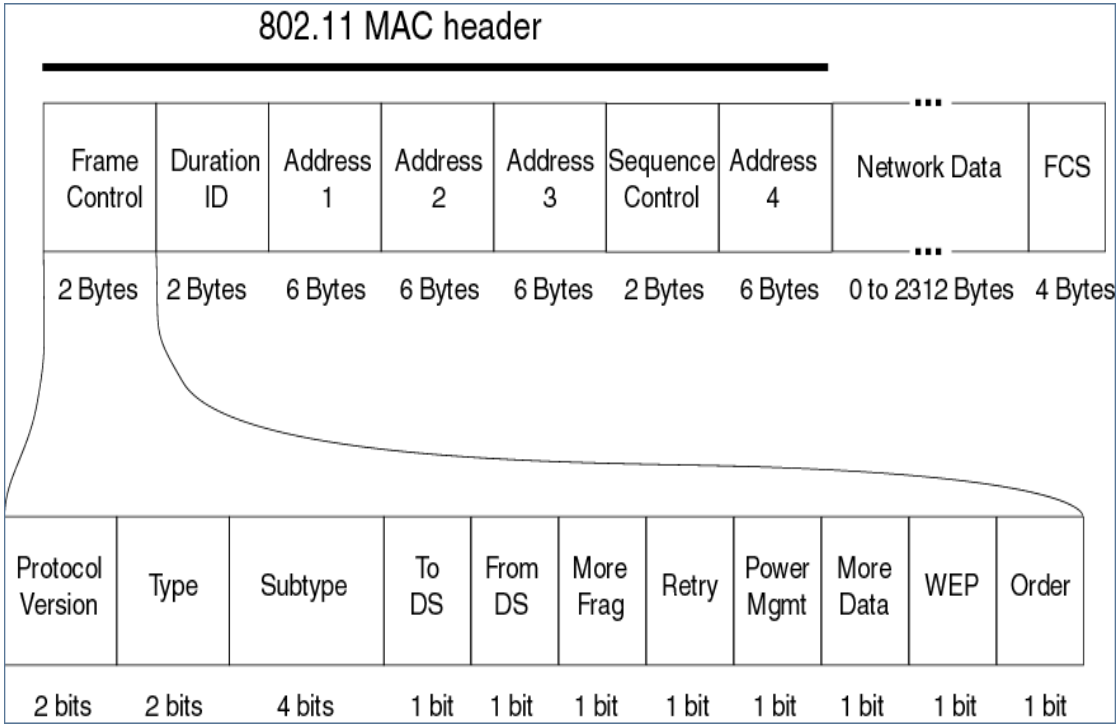
- Also known as IEEE 802.11, is a MAC and Physical layer protocol.
- Generally operates in the frequency range of 2.4Ghz and 5Ghz.
- Different releases of the standard use different frequency bands, bandwidth, modulation type and data rates.

Release Data	Standard	Frequency Band	Bandwidth	Modulation	Data Rate
1997	802.11	2.4GHz	20 MHz	DSSS, FHSS	2 Mbps
1999	802.11b	2.4GHz	20 MHz	DSSS	11 Mbps
1999	802.11a	5GHz	20 MHz	OFDM	54 Mbps
2003	802.11g	2.4GHz	20MHz	DSSS, OFDM	542 Mbps
2009	802.11n	2.4GHz, 5Ghz	20MHz, 40MHz	OFDM	600Mbps
2013	802.11ac	5Ghz	40MHz, 80MHz,160MHz	OFDM	6.93Gbps

- WiFi 6 & 7..

Wi-Fi Frame Header

- Preamble, header and data constitutes the 802.11 frame header.
- Major frame types are Management frames, Control frames and Data frames.
- Only the data in the frame can be encrypted(optional).



Wi-Fi Frame Types

- Management Frames:
- Control Frames
- Data Frames

Frame Name	Frame Type/Subtype
Association Request Frame	0
Association Response Frame	1
Reassociation Request Frame	2
Reassociation Response Frame	3
Probe Request Frame	4
Probe Response Frame	5
Beacon Frame	8
Announcement traffic indication map(ATIM) Frame	9
Disassociate Frame	10
Authentication Frame	11
Deauthentication Frame	12
Action Frame	13
Block ACK Request Frame	24
Block ACK Frame	25
Power Save Poll Frame	26
Request to Send Frame	27
Clear to Send Frame	28
ACK Frame	29
Contention Free Period End Frame	30
Contention Free Period End ACK Frame	31
Data + Contention Free ACK Frame	33
Data + Contention Free Poll Frame	34
Data + Contention Free ACK + Contention Free Poll Frame	35
NULL Data Frame	36
NULL Data + Contention Free ACK Frame	37
NULL Data + Contention Free Poll Frame	38
NULL Data + Contention Free ACK + Contention Free Poll Frame	39
QOS Data Frame	40
QOS Data + Contention Free ACK Frame	41
QOS Data + Contention Free Poll Frame	42
QOS Data + Contention Free ACK + Contention Free Poll Frame	43
NULL QOS Data Frame	44
NULL QOS Data + Contention Free Poll Frame	46
NULL QOS Data + Contention Free ACK + Contention Free Poll Frame	47

Management Frames

- **Authentication Frame**

An exchange of authentication frames takes place with an access point when the link setup between the access point and the user device takes place. It helps in establishment of the identity of the device connecting to the network.

- **Association Request Frame**

This Frame informs the access point that the device is ready to send data on the network and hence the access point allocates resources for the device.

Association Response Frame

This frame is sent by the access point in response to the Association Request Frame. The response frame may be a positive response or a negative response to the device.

Management Frames

- **Beacon Frame**

This is the frame that is broadcast by the access point after a fixed interval of time. This frame informs the devices that are trying to connect to the access point of the various characteristics of the access point, like the name, the operating frequency, the transfer rates, Type of encryption scheme used and more.

- **De-Authentication Frame**

De-Authentication Frame is a complement of the Authentication frame. It is the frame that is sent over the network by the user device to the access point when the user device wants to disconnect from the network.

- **Disassociation Frame**

Disassociation Frame is a complement of the Association Frame. It informs the access point that it can de-allocate the resources that it had allocated for the device as the device no longer plans to use the network.

Management Frames

- **Probe Request Frame**

This frame is sent from a station to another station to get information about that station.

- **Probe Response Frame:**

Probe response frame is the response sent by a station for the probe request.

- **Reassociation Request Frame:**

Reassociation Request Frame is a frame that is sent when a device moves out of the range of one access point and moves into the range of another. The device sends a Reassociation request to another access point with signal strength more than the current access point.

- **Reassociation Response Frame:**

This is the response frame that is sent in response to the Reassociation Request. The response may be a positive response or a negative response.

Control Frames

- **Control Frame:**

The control frames are sent over the network and control the contention issues of the network.

- **Acknowledgement (ACK) Frame:**

On the reception of a data frames the device sends an acknowledgement frame to the source.

- **Request to Send (RTS) Frame:**

It is the request to send that acts as an optional contention control over the network.

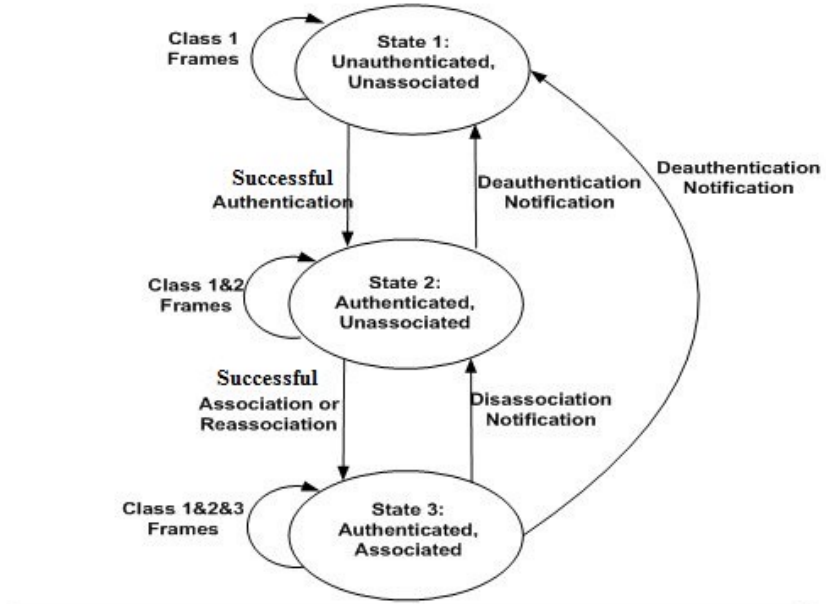
- **Clear to Send (CTS) Frame:**

It is the optional Clear to Send Frame that is sent in response to the Request to Send Frame.

Data Frames

- The Data frames are the frames that are used to move the data from the source to the destination. They generally carry higher level protocols in their data sections.

Wi-Fi Protocol State Machine



Class 1:
Control: RTS, CTS, ACK, CF-END, CF-END+CF-ACK,
Management: Probe Request/Response, Beacon, Authentication, Deauthentication, ATIM
Data: Any frame with false ToDS and FromDS (0)

Class 2:
Management: Association Request/Response, Reassociation Request/Response, Disassociation

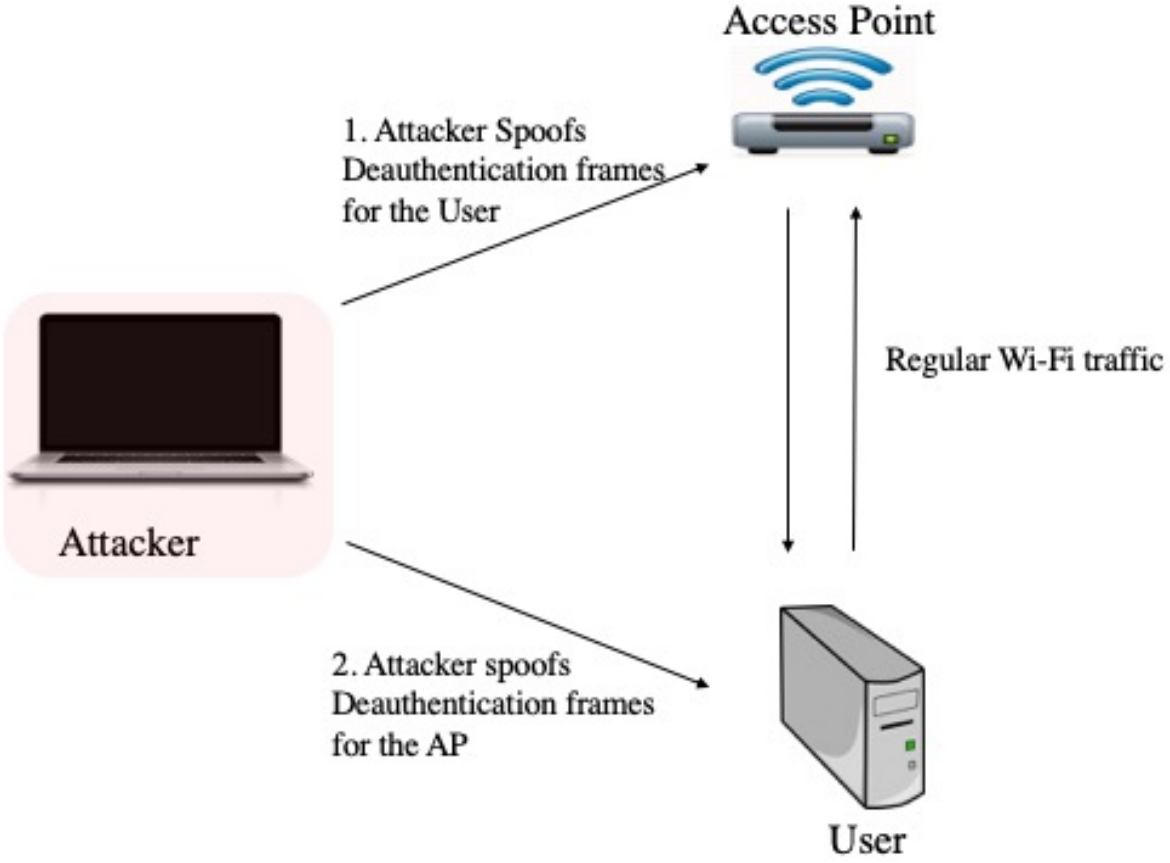
Class3:
Control: PS-Poll
Management: Deauthentication
Data: Any Data Frame

WiFi Attacks

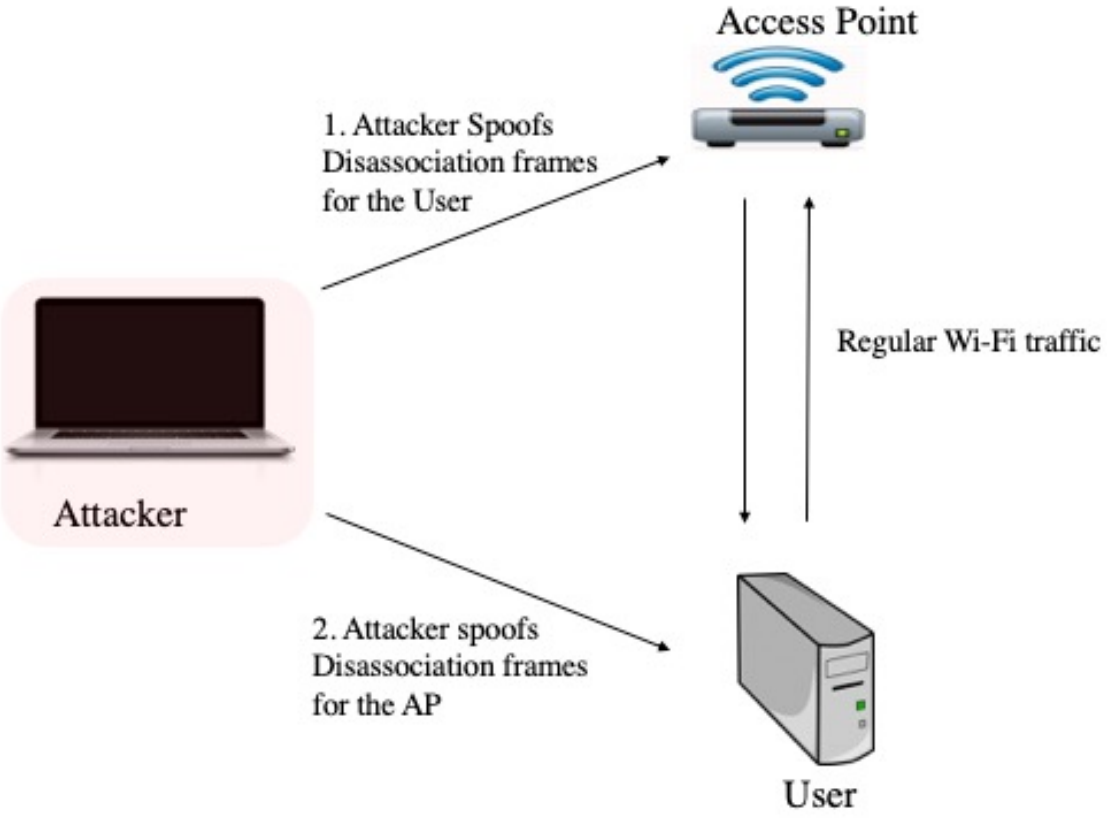
Sr. No	Availability Attacks
1.	Deauthentication Attack
2.	Disassociation Attack
3.	Fake Authentication Attack
4.	Deauthentication Broadcast Attack
5.	Disassociation Broadcast Attack
6.	Fake power saving Attack
7.	CTS Flooding Attack
8.	RTS Flooding Attack
9.	Probe request flooding Attack
10.	Probe response flooding Attack
11.	Man in the middle Attack
12.	Beacon flooding Attack
13.	Modified deauthentication attack

Sr. No	Encryption Attacks
1.	Chopchop Attack
2.	Fragmentation Attack
3.	Café Latte Attack
4.	Hirte Attack
5.	FMS Attack
6.	KoreK family of Attacks
7.	PTW Attack
8.	ARP injection attack
9.	Dictionary attack

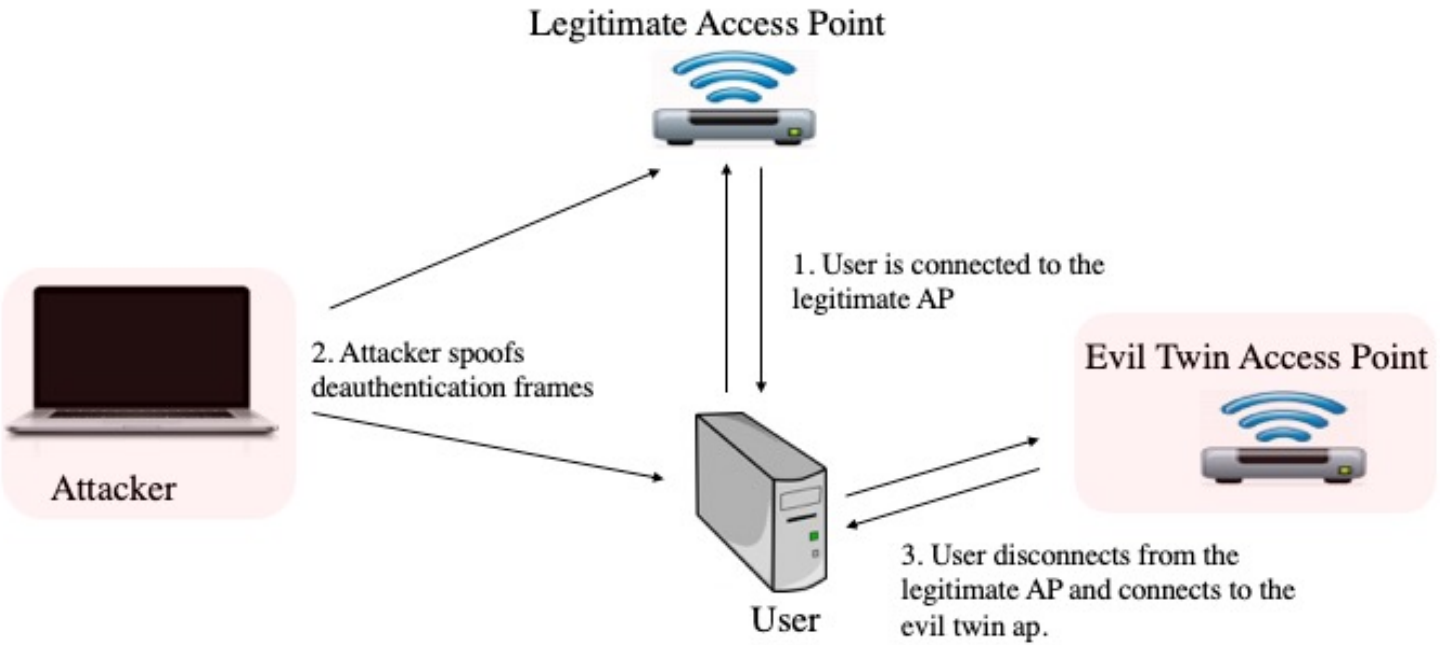
Deauthentication Attack



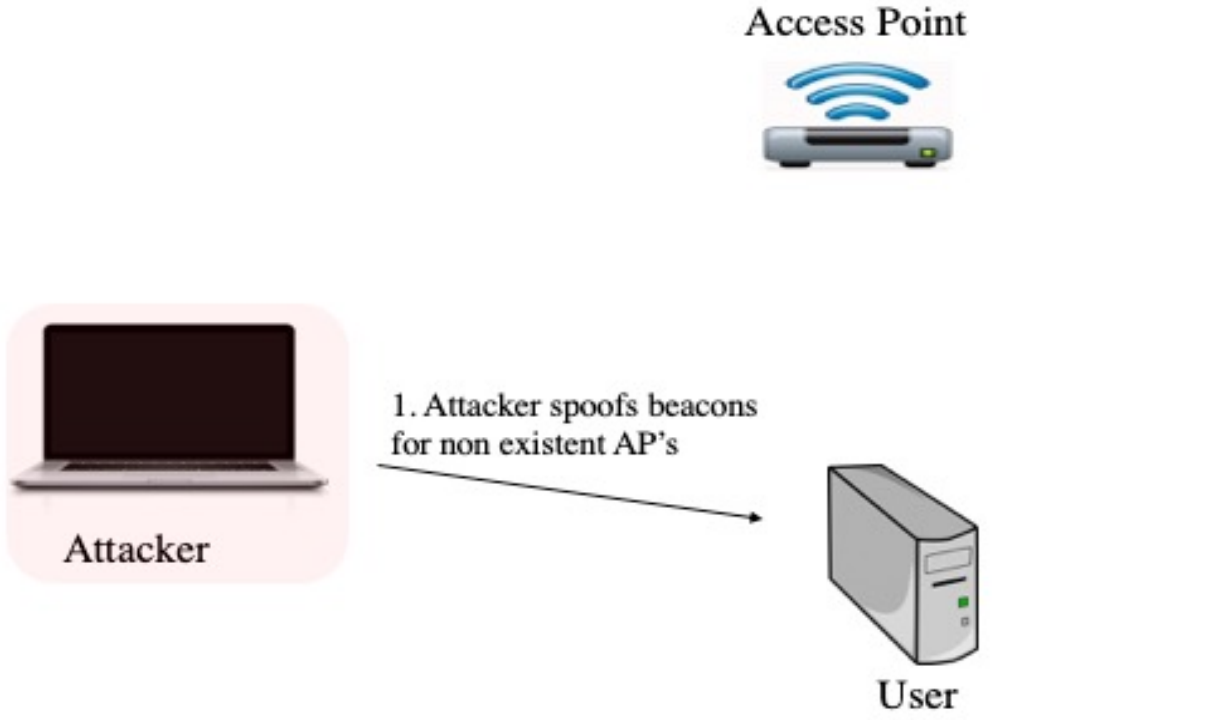
Disassociation Attack



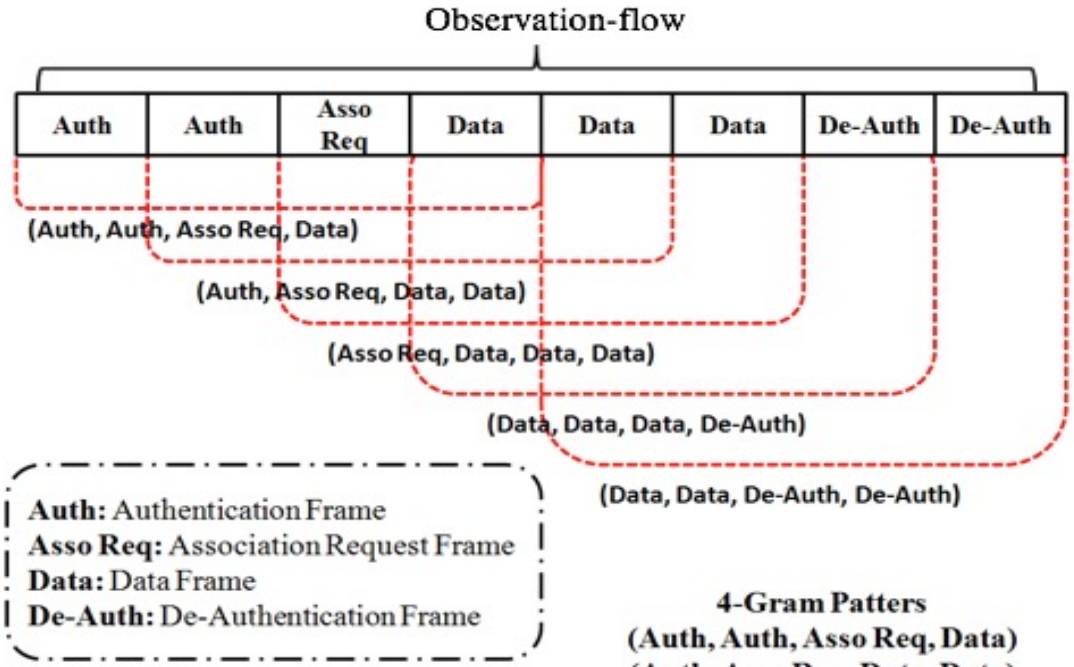
Man in the middle/Evil twin



Beacon flooding



WiFi state machine tracking



4-Gram Patters

(Auth, Auth, Asso Req, Data)
(Auth, Asso Req, Data, Data)
(Asso Req, Data, Data, Data)
(Data, Data, Data, De-Auth)
(Data, Data, De-Auth, De-Auth)

ABA Normal Behavior Modeling

- Representation:

Sr. No.	Features	Description
1.	frame_epoch_time	Epoch time
2.	Address 1	Mac address 1
3.	Address 2	Mac address 2
4.	Address 3	Mac address 3
5.	Address 4	Mac address 4
6.	frame_type	Frame type
7.	frame_subtype	Frame subtype

ABA Normal Behavior Modeling

- NGrams

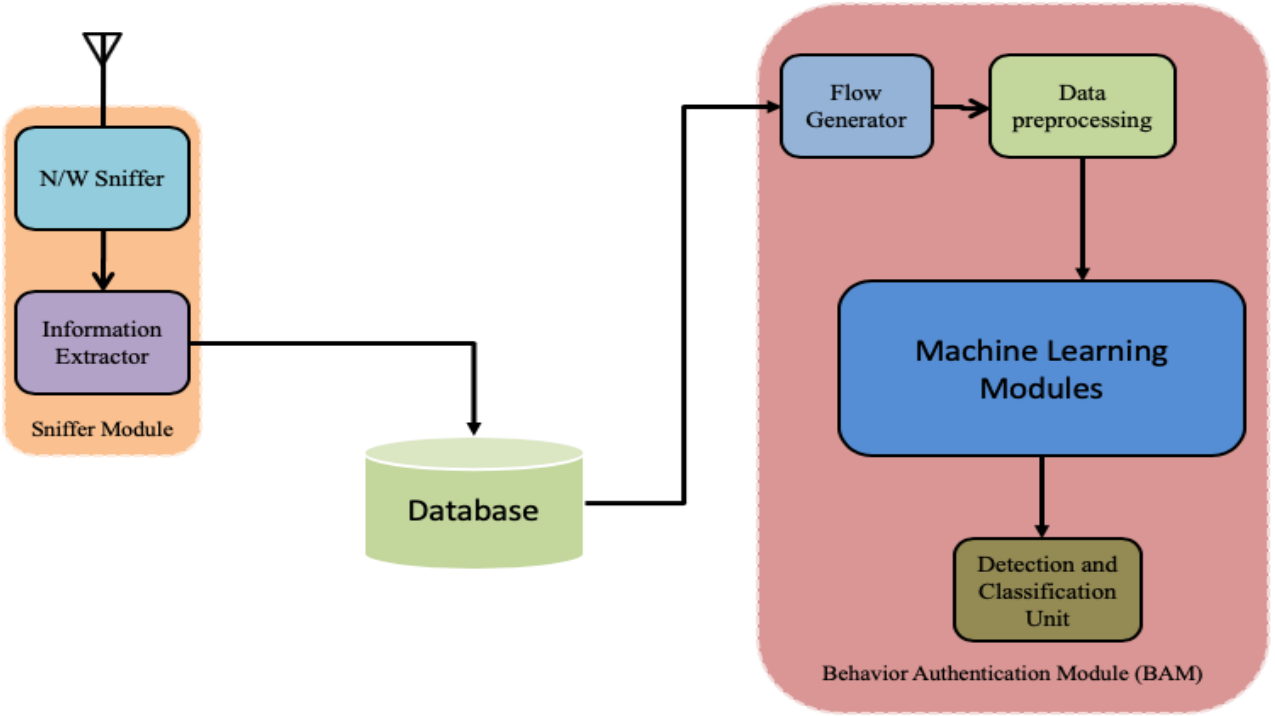
Normal behavior Model

- Flow probability smoothing:

$$P(W_1^{n-1}|W_n) = \lambda P(W_1^{n-1}|W_n) + (1-\lambda)P(W_1^{n-2}|W_n)$$

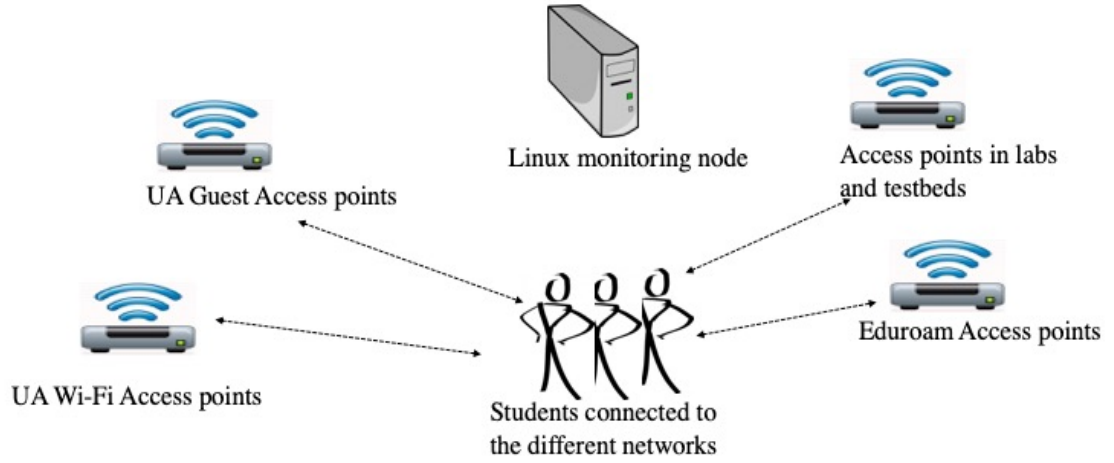
Sr. No.	Features	Description
1.	flowprobability	Probability of the flow
2.	totalframesinflow	Total frames in the flow
3.	managementratio	Ratio of number of management frames to total frames in the flow
4.	controlratio	Ratio of number of control frames to total frames in the flow
5.	dataratio	Ratio of number of data frames to total frames in the flow

IDS Architecture



Experiment Datasets

- Collected 3 Normal datasets in ECE
- The dataset timelines:
  - Dataset 1: June 2016 for 9 days
  - Dataset 2: August 2017 for 14 days
  - Dataset 3: November 2018 for 38 days

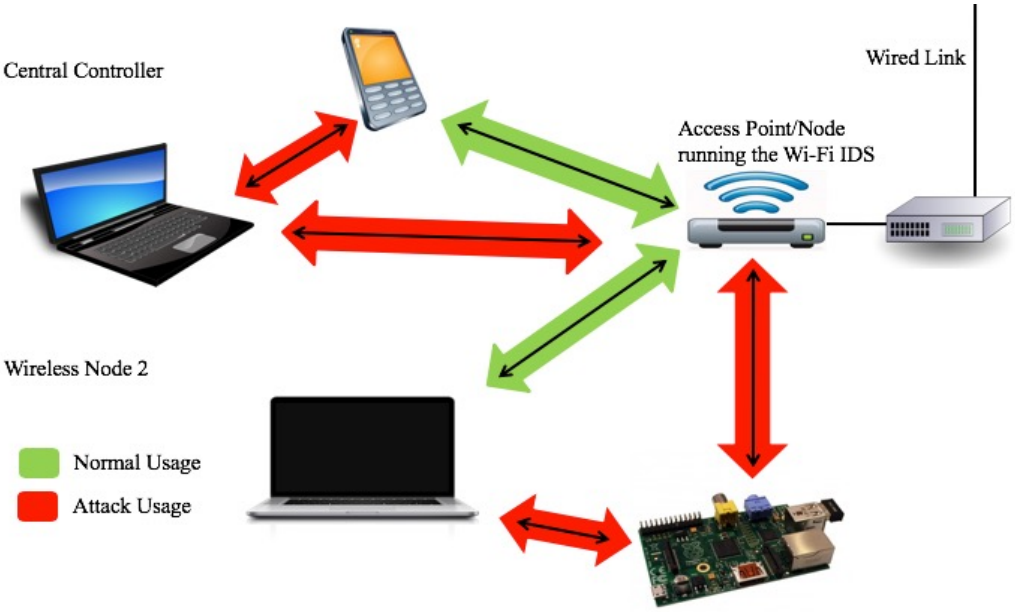


Dataset Name	Time of Collection	Total number of frames collected	% of Beacon frames	% of Authentication frames	Percentage of Deauthentication frames
Dataset 1	June 2016	16271211	85.55%	0.006%	0.001%
Dataset 2	August 2017	25810597	89.54%	0.004%	0.002%
Dataset 3	November 2018	64170469	87.52%	0.004%	0.001%

Experiment Datasets

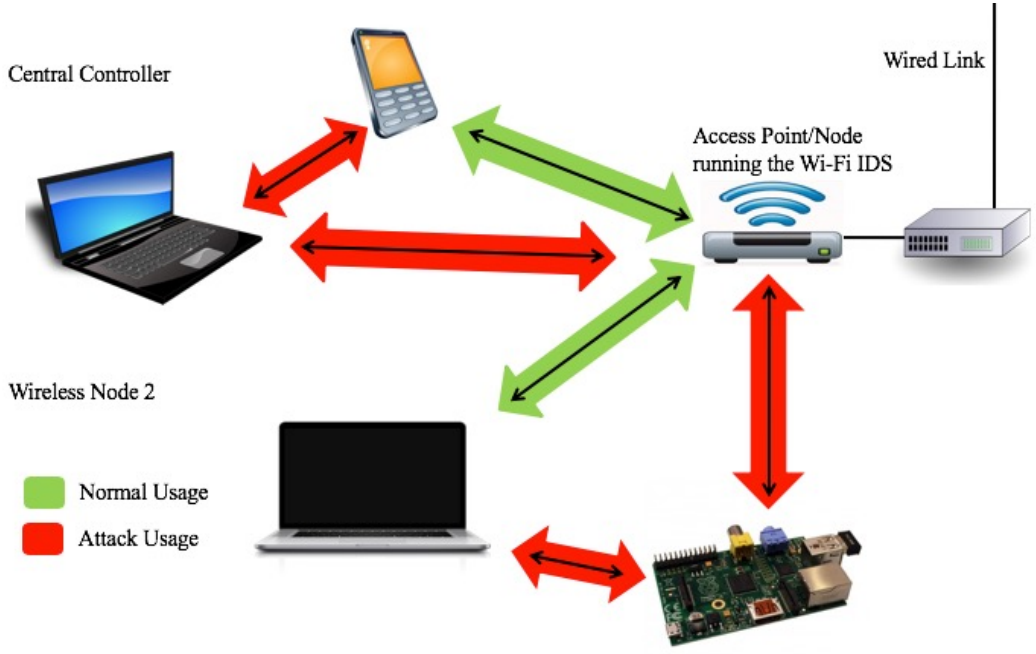
- Attack Dataset collected in CAC @ECE

Sr. No.	Attack Name
1.	Deauthentication attack
2.	Fake Authentication
3.	Syn flood
4.	Udp flood



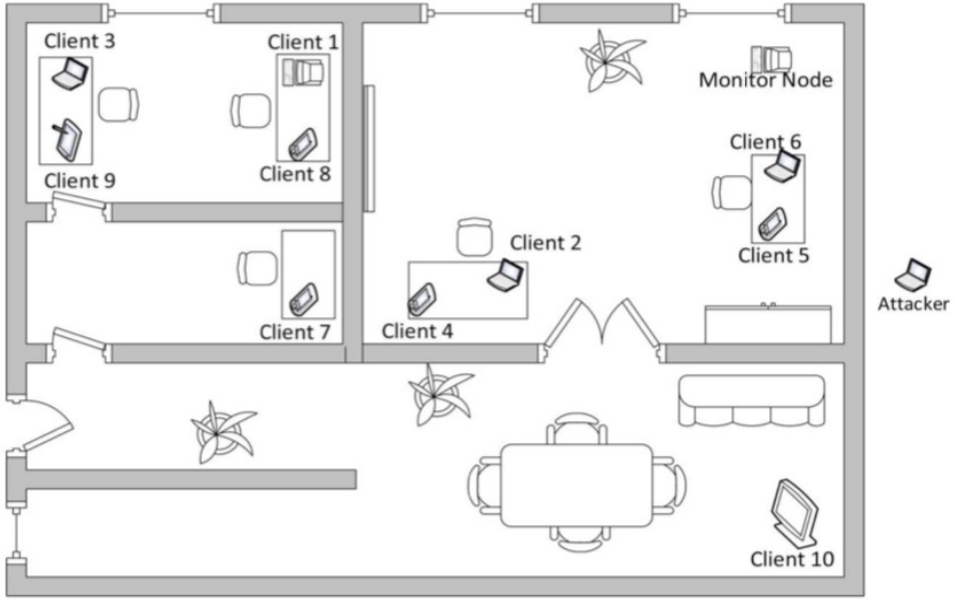
Experiment Datasets

- Runtime IDS evaluation setup



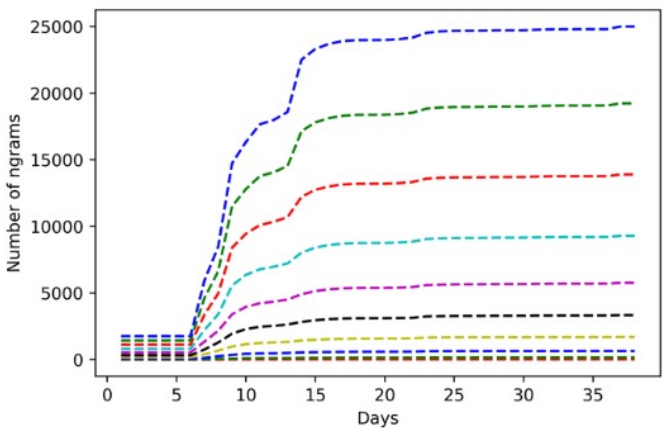
Experiment Datasets

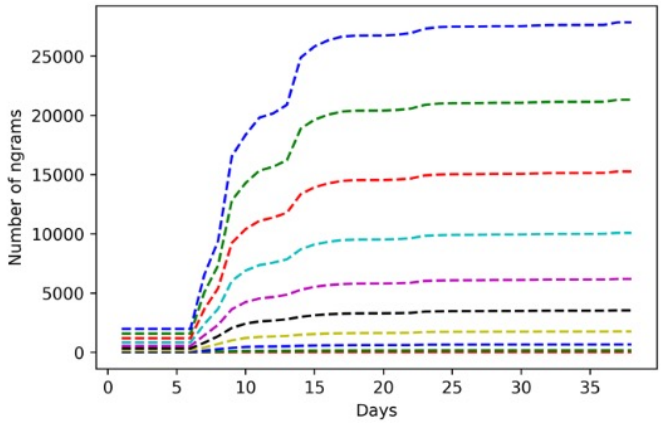
- AWID Dataset also used for evaluation
- Has 15 attacks

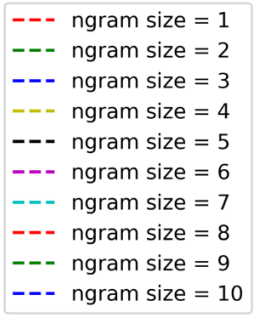


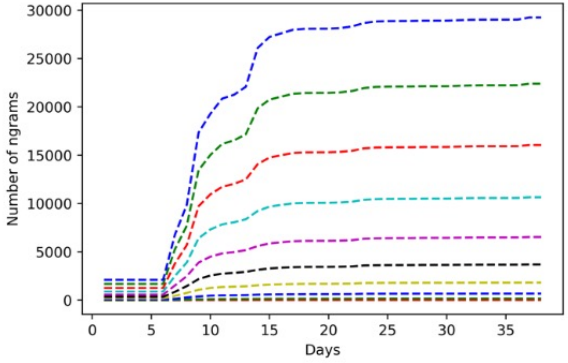
Dataset Name	Time of Collection	Total number of frames collected	% of Beacon frames	% of Authentication frames	Percentage of Deauthentication frames
Awid_atk _r_tst	March 2014	575643	41.83%	0.001%	1.4%

Experiment 1: Ngram Size





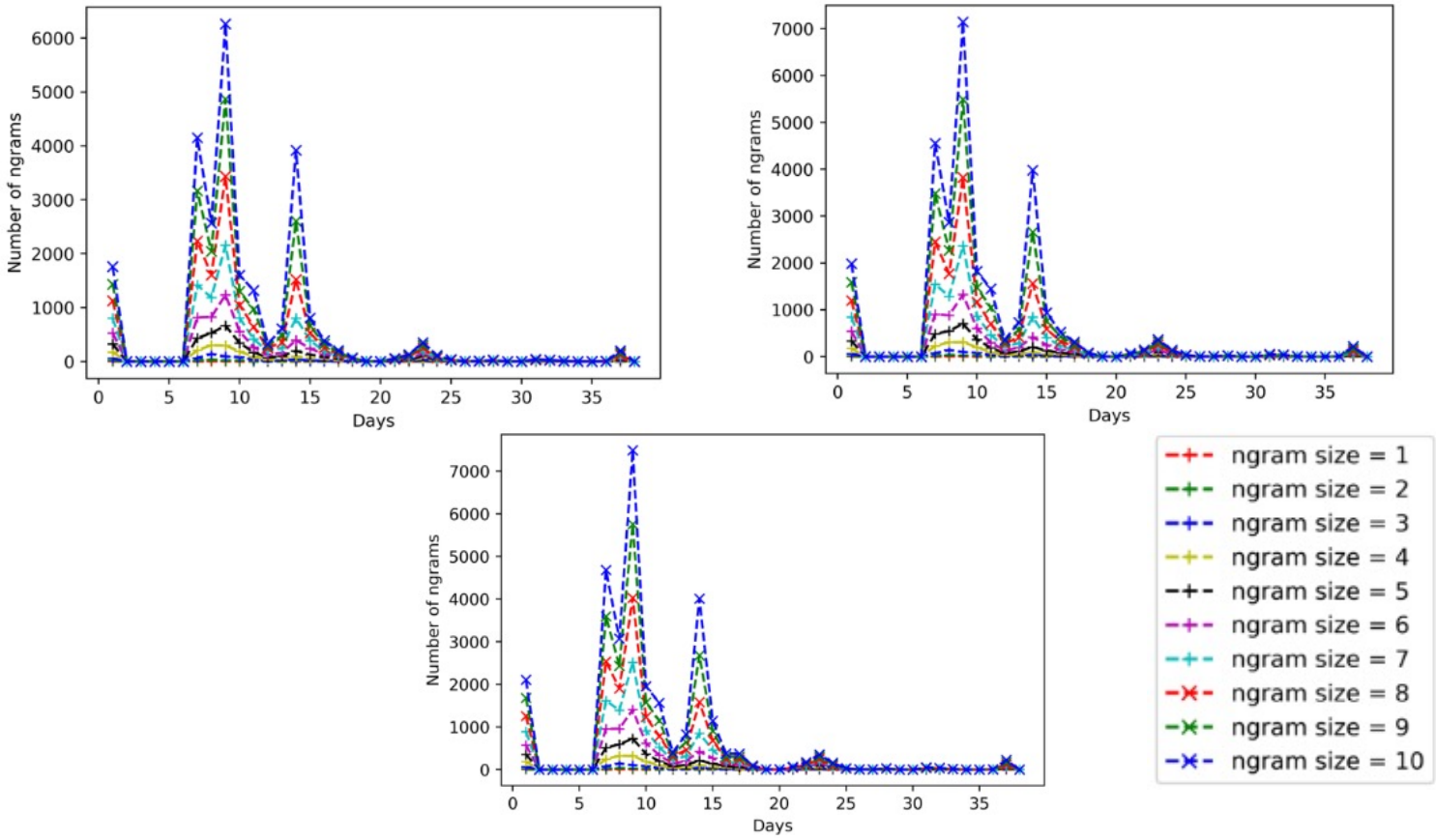




Systems and Security Lab

THE UNIVERSITY OF ARIZONA

Experiment 1: Ngram Size



Experiment 2: Model Performance

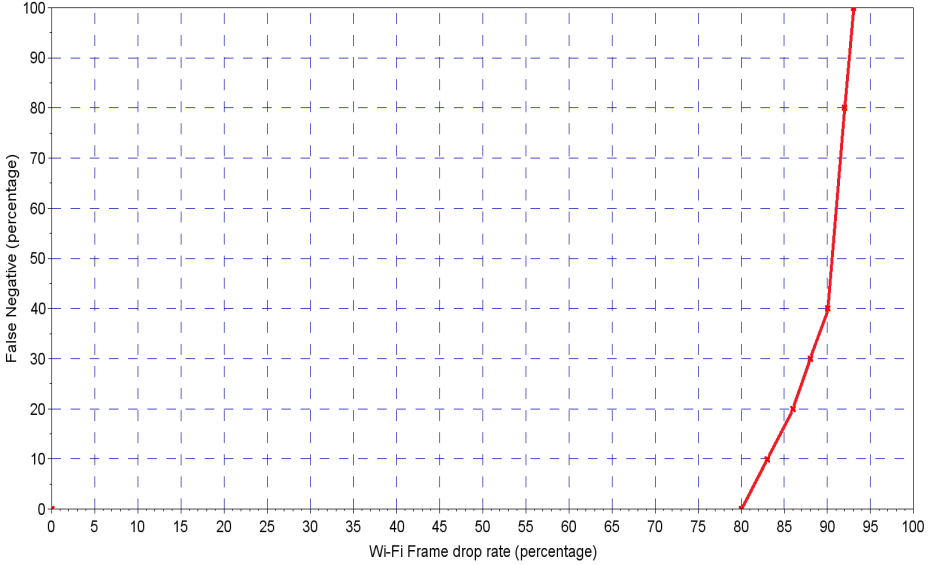
Datasets	Isolation Forest		C4.5		Random Forest		AdaBoost		Decision table	
	TP	FP	TP	FP	TP	FP	TP	FP	TP	FP
Dataset 1	0.962	0.038	1	0	1	0	1	0	0.999	0.001
Dataset 2	0.932	0.062	0.973	0.027	0.986	0.014	0.97	0.027	1	0
Dataset 3	0.932	0.068	1	0	1	0	1	0	1	0
Deauthentication attacks(attack dataset)	1	0	1	0	1	0	1	0	0.956	0.044
Fake authentication Attacks(attack dataset)	1	0	0.998	0.02	0.996	0.004	0.998	0.002	0.94	0.06
Syn Flood attack(attack dataset)	1	0	1	0	1	0	1	0	1	0
UDP flood attack(attack dataset)	1	0	1	0	1	0	1	0	1	0
AWID_atk_r_tst_amok	1	0	0.944	0.056	0.9	0.1	0.944	0.056	0	1
AWID_atk_r_tst_arp	1	0	1	0	1	0	1	0	1	0
AWID_atk_r_tst_caffelatte	0.071	0.929	0.0	1	0	1	0	1	0	1
AWID_atk_r_tst_chopchop	1	0	1	0	1	0	1	0	1	0
AWID_atk_r_tst_cts	1	0	1	0	1	0	1	0	1	0
AWID_atk_r_tst_deauthentication	1	0	0.98	0.02	0.95	0.05	0.93	0.07	1	0
AWID_atk_r_tst_disassociation	1	0	1	0	0.98	0.02	1	0	0.98	0.02
AWID_atk_r_tst_eviltwins	1	00.684	0	1	0	0	0	1	0	1
AWID_atk_r_tst_fragmentation	1	0	1	0	1	0	1	0	1	0
AWID_atk_r_tst_proberequest	1	0	1	0	1	0	1	0	1	0
AWID_atk_r_tst_hirte	0.652	0.348	0.552	0.478	0.5	0.5	0.48	0.52	0.522	0.478

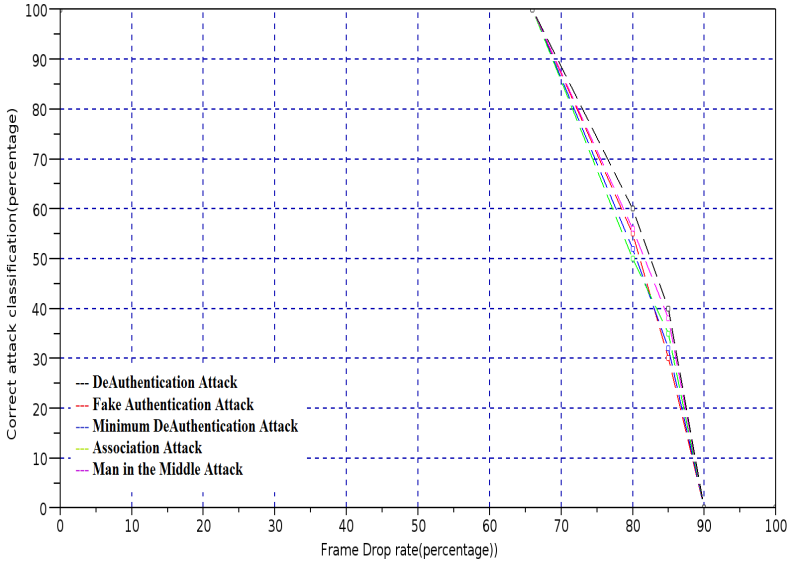
Experiment 3: Runtime Analysis

- The IDS was tested in the runtime environment for 2 days
- Different attacks were performed on the devices in the network
- The IDS was able to detect all the attacks with a 100% accuracy

Sr. No.	Attack Name
1.	Deauthentication attack
2.	Fake Authentication
3.	Minimal Deauthentication attack
4.	Disassociation attack
5.	Man in the middle attack

Experiment 4: Runtime performance at high interference





Systems and Security Lab

THE UNIVERSITY OF ARIZONA

Publications

- Alipour, Hamid, Youssif B. Al-Nashif, **Pratik Satam**, and Salim Hariri. "Wireless anomaly detection based on IEEE 802.11 behavior analysis." *IEEE transactions on information forensics and security* 10, no. 10 (2015): 2158-2170.

- **Satam, Pratik**, and Salim Hariri. "WIDS: An anomaly based intrusion detection system for Wi-Fi (IEEE 802.11) protocol." *IEEE Transactions on Network and Service Management* 18, no. 1 (2020): 1077-1091.

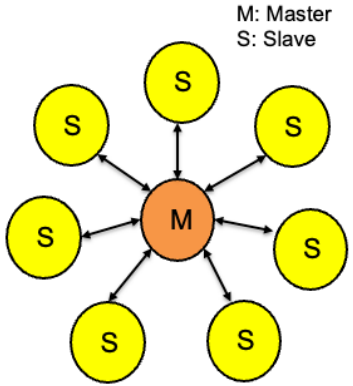
Use case 2: Bluetooth Protocol

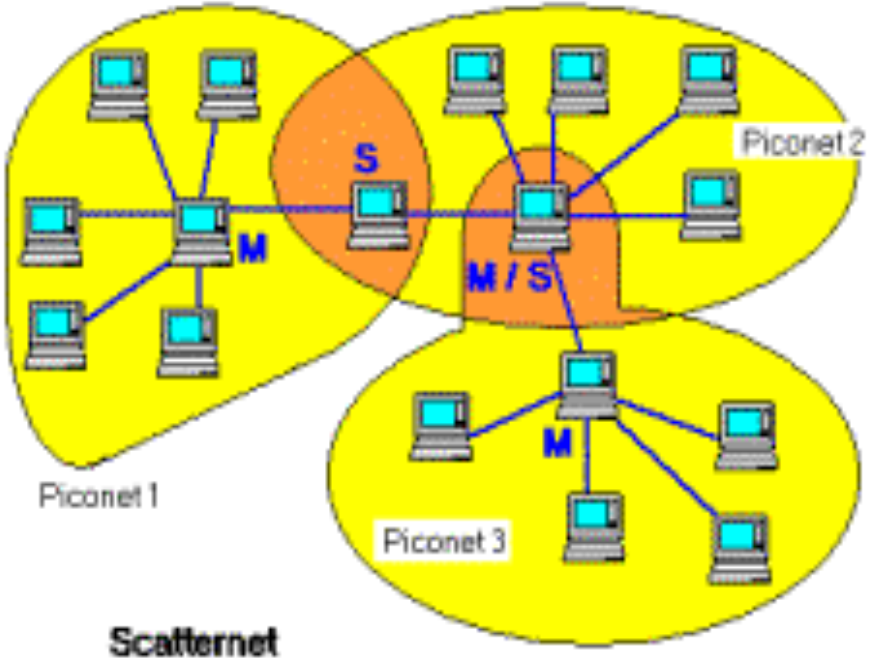
Bluetooth Protocol

- Bluetooth is a standard for short range, low power and low cost wireless communication that uses radio technology.
- Generally operates in the frequency range of 2.4Ghz.
- A master in a piconet may communicate with up to 7 active slave devices.

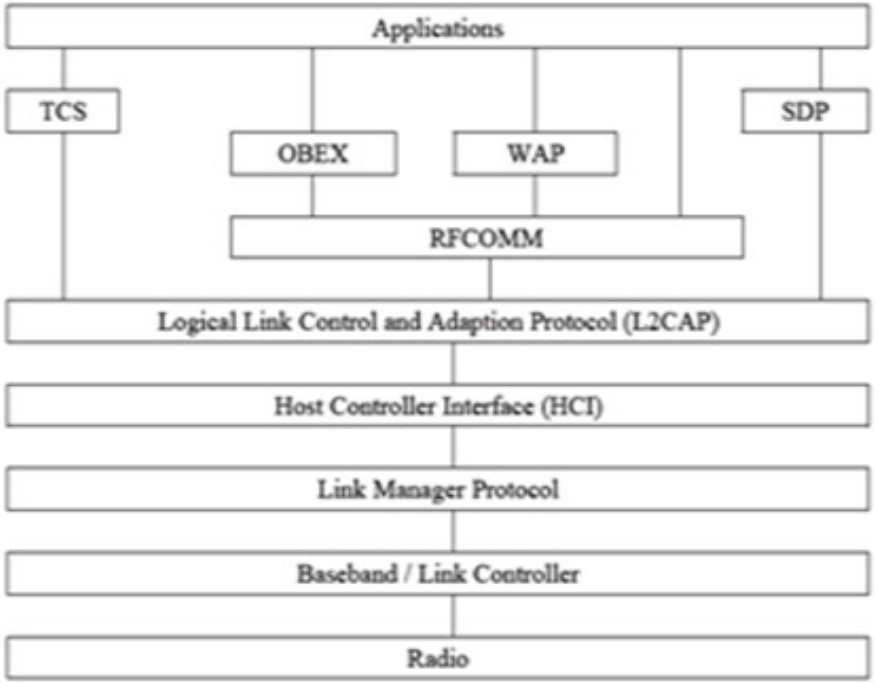
Bluetooth Piconet and Scatternet

- Piconet:
  - Master slave model
  - Upto 7 active devices

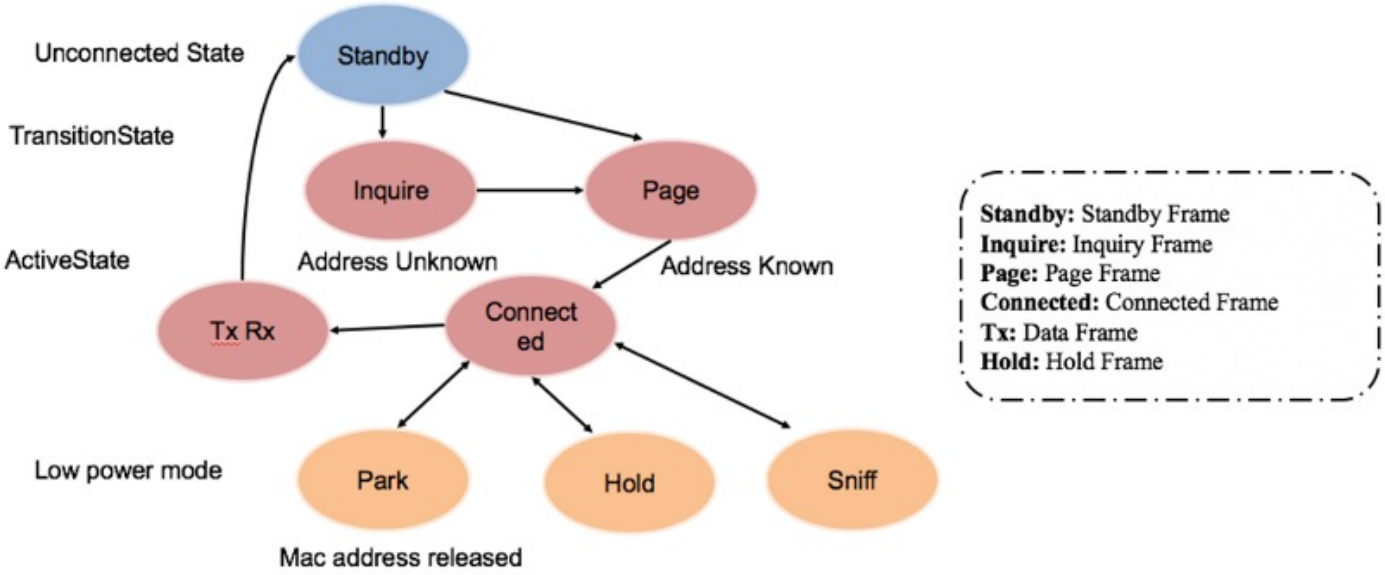




Bluetooth Protocol Stack



Bluetooth Protocol State Machine



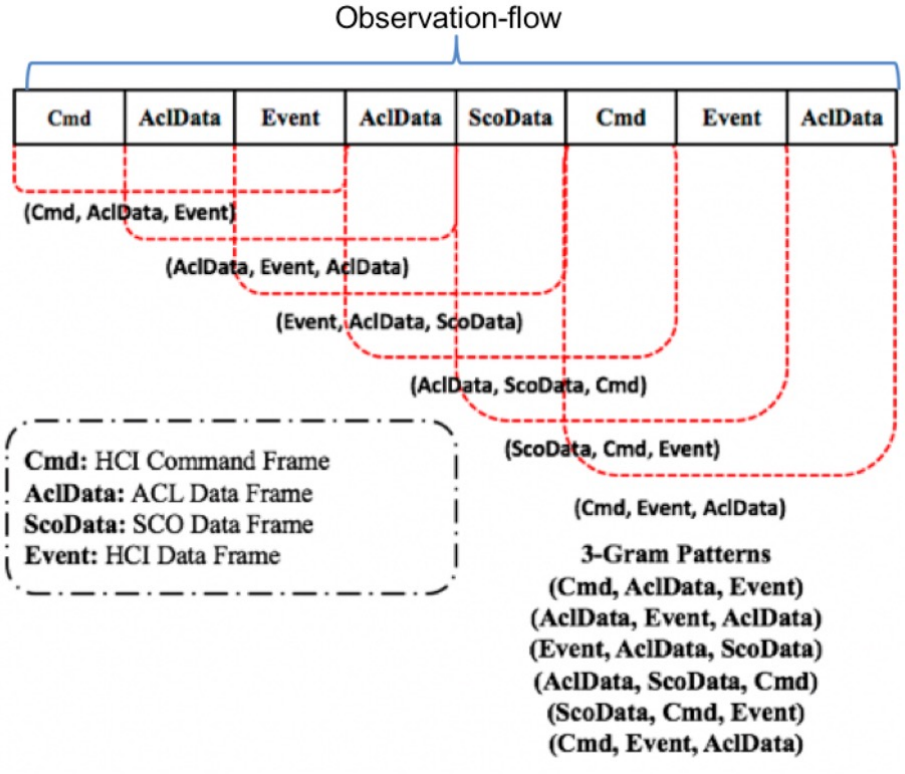
Bluetooth Attacks

- Battery Draining Attack:
  - Send repeated connection requests to drain the target devices battery
- Bluesnarfing Attack:
  - Target the Object Exchange (OBEX) application oriented transfer to send malicious files
- Replay Attack
- Bluejacking Attack
- Man in the middle attack

Bluetooth Attacks

- Replay Attack:
  - ➢ Replay frames in the network
- Bluejacking Attack:
  - ➢ Spam victim with unwanted connections
- Man in the middle attack

Bluetooth State Machine Tracking



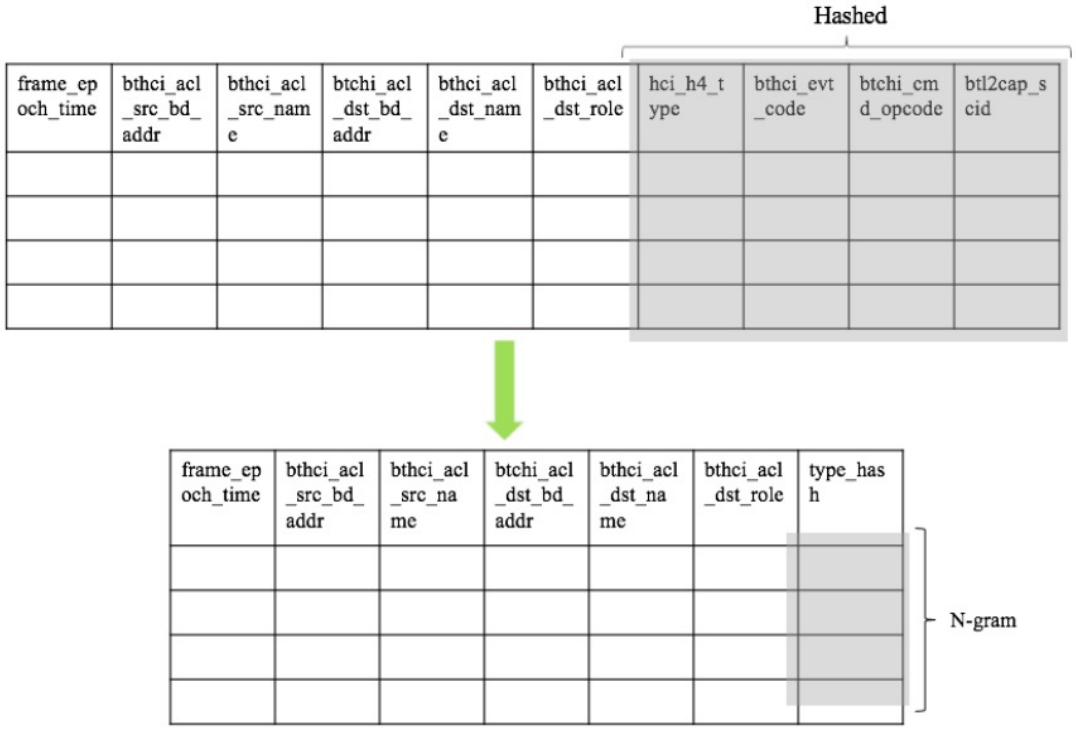
ABA Normal Behavior Modeling

- Representation:

Sr.no	Feature	Description
1.	frame_epoch_time	Epoch time
2.	hci_h4_type	HCI packet type
3.	bthci_evt_code	Bluetooth HCI event code
4.	btchi_cmd_opcode	Bluetooth HCI command opcode
5.	btl2cap_scid	Bluetooth L2CAP protocol source CID
6.	btchi_acl_dst_bd_addr	Destination BD_ADDR
7.	bthci_acl_dst_name	Destination device name
8.	bthci_acl_dst_role	Destination device role
9.	bthci_acl_src_bd_addr	Source BD_ADDR
10.	bthci_acl_src_name	Source device name

ABA Normal Behavior Modeling

- NGrams



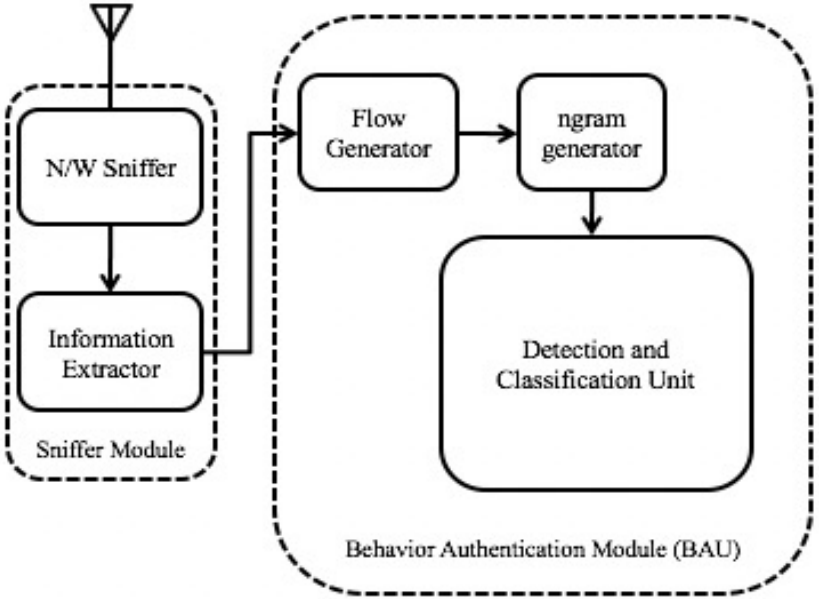
Normal behavior Model

- Flow probability smoothing:

$$P(W_1^{n-1}|W_n) = \lambda P(W_1^{n-1}|W_n) + (1-\lambda)P(W_1^{n-2}|W_n)$$

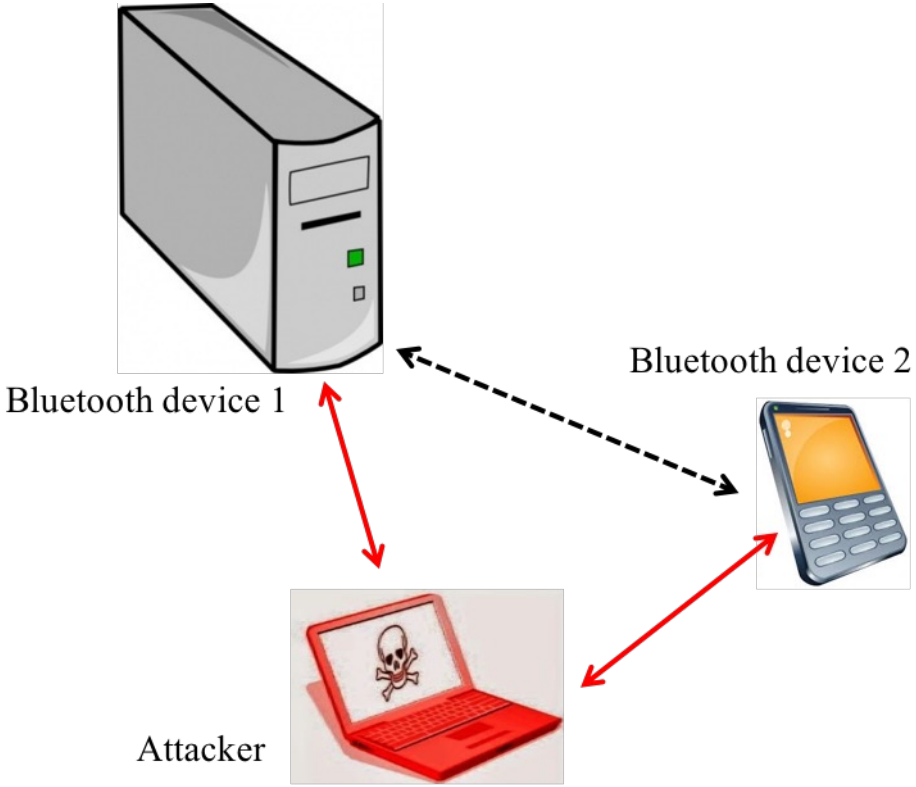
Features	Description
Probability of Flow	Probability of flow extracted after Jelinek-Mercer smoothing
Ratio of HCI command frames	HCI packet type
Ratio of ACL data frame	Bluetooth HCI event code
Ratio of SCO data frame	Bluetooth HCI OPCode
Ratio of HCI data frame	Bluetooth L2CAP protocol Source CID

IDS Architecture



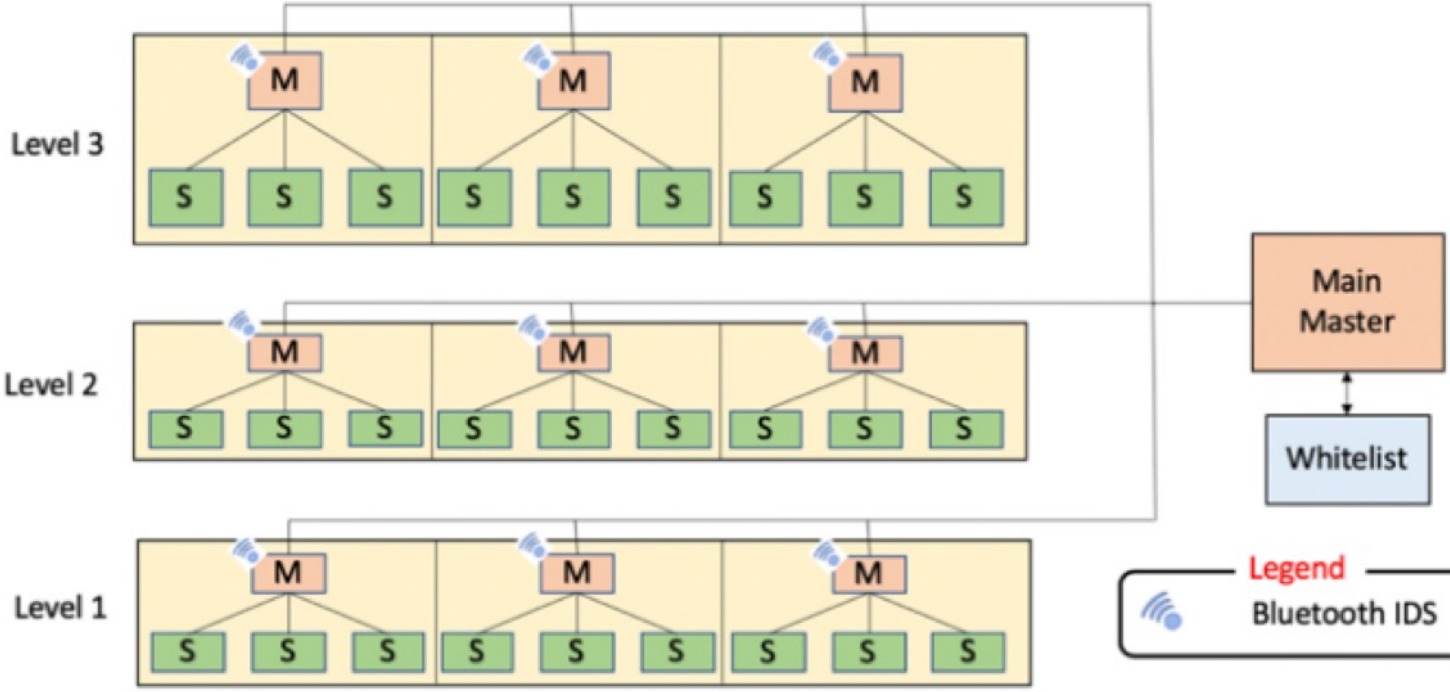
Experiment Testbeds

- Bluetooth Piconet with a Master and a Slave
- A compromised attacker device connected to the network

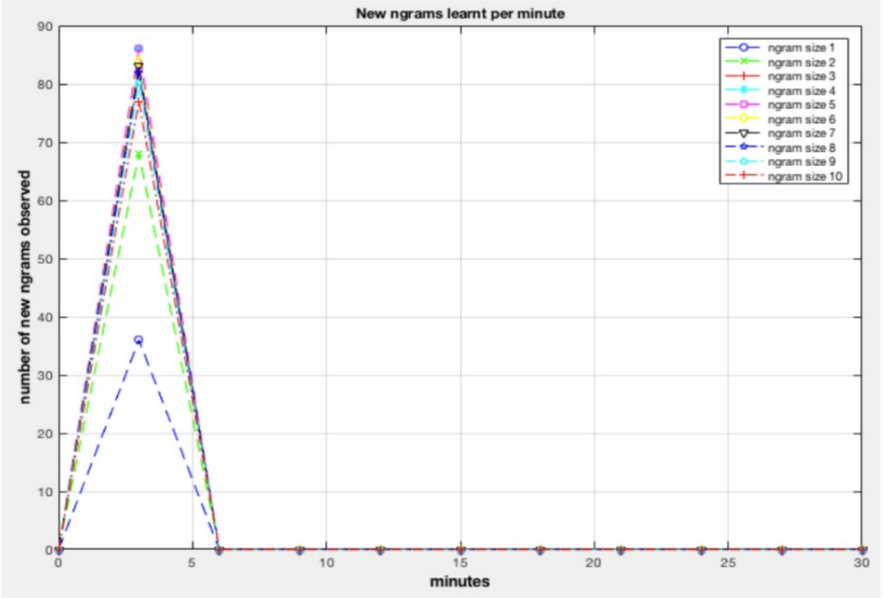


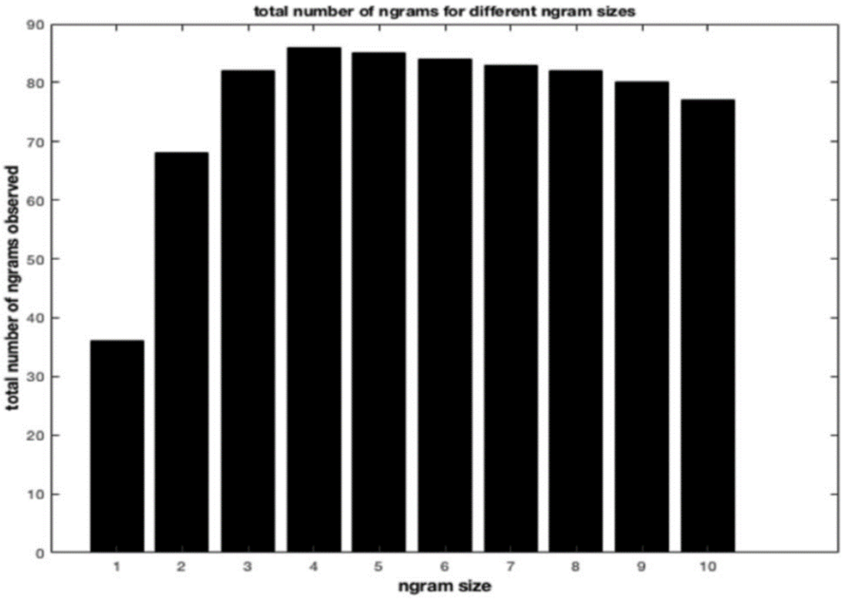
Experiment Testbeds

- Multi-Level Bluetooth Infrastructure (Scatternet) with multiple PicoNets



Experiment 1: Ngram Size



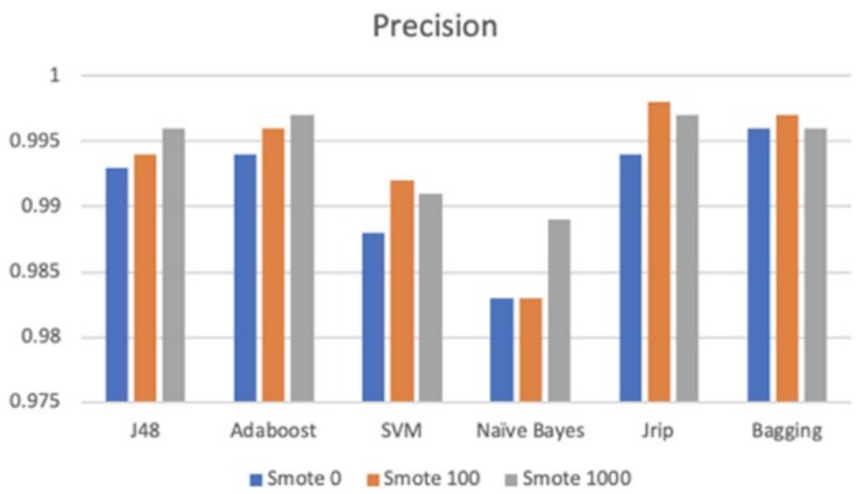


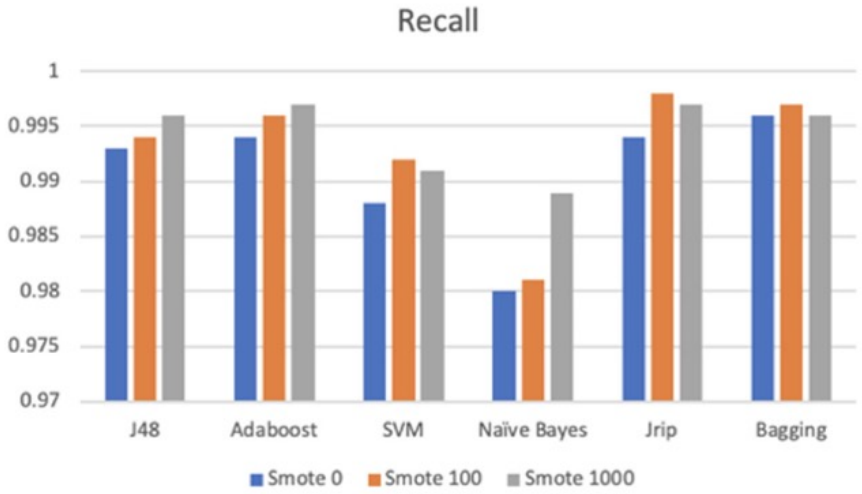
Systems and Security Lab

THE UNIVERSITY OF ARIZONA

Experiment 2: Model Performance

- Evaluated Attacks:
  - Denial of Service attacks
  - Blue Snarfing attacks
  - Power Draining attacks





Publications

- Satam, Shalaka, **Pratik Satam**, Jesus Pacheco, and Salim Hariri. "Security framework for smart cyber infrastructure." *Cluster Computing* 25, no. 4 (2022): 2767-2778.
- Satam, Shalaka, **Pratik Satam**, and Salim Hariri. "Multi-level bluetooth intrusion detection system." In *2020 IEEE/ACS 17th International Conference on Computer Systems and Applications (AICCSA)*, pp. 1-8. IEEE, 2020.
- **Satam, Pratik**, Shalaka Satam, Salim Hariri, and Amany Alshawi. "Anomaly behavior analysis of IoT protocols." *Modeling and design of secure internet of things* (2020): 295-330.
- **Satam, Pratik**, Shalaka Satam, and Salim Hariri. "Bluetooth intrusion detection system (BIDS)." In *2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)*, pp. 1-7. IEEE, 2018.

Interested in Research

- Contact me at:
  - Email: pratiksatam@arizona.edu
  - Webpage: https://sie.engineering.arizona.edu/faculty-staff/faculty/pratik-satam