



How Bad Are The Rogues' Impact on Enterprise 802.11 Network Performance ?

Kaixin Sui, Dan Pei, Youjian Zhao, Zimu Li
Tsinghua University

EWLAN, AC, EAP, and RAP

- EWLAN (*Enterprise WLAN*)
- EAP (*Enterprise AP*)



- AC (*wireless controller*)



- RAP (*Rogue AP*)
 - Security threat
 - **Great impact on EWLAN performance**



Chaotic RAP deployment in EWLAN

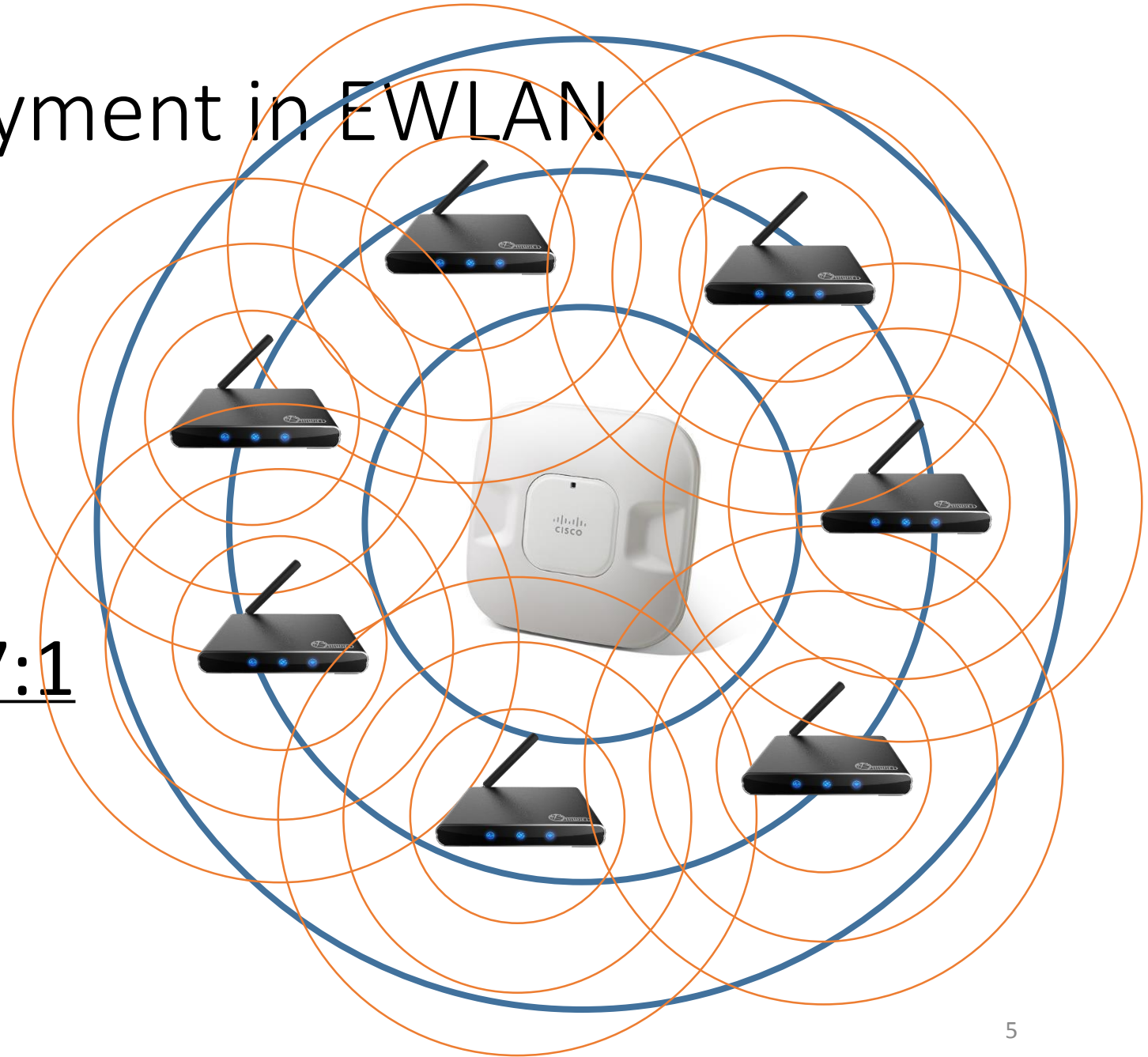
- 5GHz v.s. 2.4GHz of #RAP : **292 v.s. 15110**
 - Focus on 2.4 GHz

Chaotic RAP deployment in EWLAN

- 5GHz v.s. 2.4GHz of #RAP : **292 v.s. 15110**
 - Focus on 2.4 GHz
- #RAP v.s. #EAP in 2.4GHz : **15110 v.s. 2002**
 - The RAP to EAP ratio > 7:1

Chaotic RAP deployment in EWLAN

- The RAP to EAP ratio > 7:1



Chaotic RAP deployment in EWLAN

- 5GHz v.s. 2.4GHz of #RAP : **292 v.s. 15110**
 - Focus on 2.4 GHz
- #RAP v.s. #EAP in 2.4GHz : **15110 v.s. 2002**
 - The RAP to EAP ratio > **7:1**
- Chaotic RAPs may cause great performance degradation of EWLAN.
- **Our GOAL: Measure RAPs' impact on EWLAN performance**

Data collection

- EWALN of Tsinghua campus
- **4** km², **42000** students, **11000** faculties and staff
- **5** Weekdays (2014/07/14-18)
- **11** ACs (Cisco), **2002** EAPs (Cisco), **51269** EAP Clients
- **79** Buildings (**5** types: administrative, classroom, cafeteria, department, dorm)
- **15110** RAPs , **44996** RAP Clients

Data collection

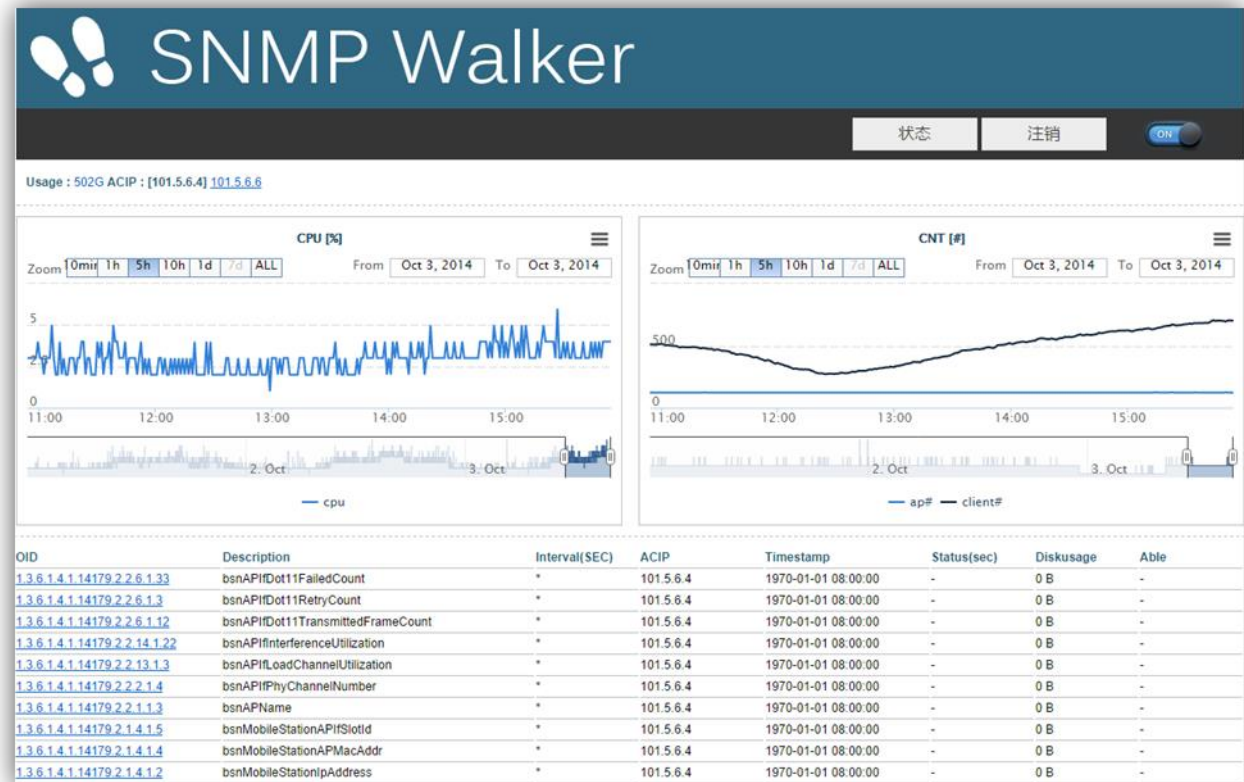
- EWALN of Tsinghua campus
- 4 km², 42000 students, 11000 faculties and staff
- 5 Weekdays (2014/07/14-18)
- 11 ACs (Cisco), 2002 EAPs (Cisco), **51269 EAP Clients**
- 79 Buildings (5 types: administrative, classroom, cafeteria, department, dorm)
- 15110 RAPs , **44996 RAP Clients**

Data collection

- EWALN of Tsinghua campus
- 4 km², 42000 students, 11000 faculties and staff
- 5 Weekdays (2014/07/14-18)
- 11 ACs (Cisco), 2002 EAPs (Cisco), 51269 EAP Clients
- 79 Buildings (5 types: administrative, classroom, cafeteria, department, dorm)
- 15110 RAPs , 44996 RAP Clients
- One of the **largest scale WiFi measurement**

Data collection

- **SNMP Data** without any additional measurement hardware
- 10 min interval



Data collection

- **SNMP Data** without any additional measurement hardware
- 10 min interval
- 17 Objects

TABLE I. SNMP DATA SUMMARY: 11 ACS; 2002 EAPS; EAP REPORTS OBJECT EVERY 90 SECONDS. POLLING INTERVAL IS 10 MINUTES.

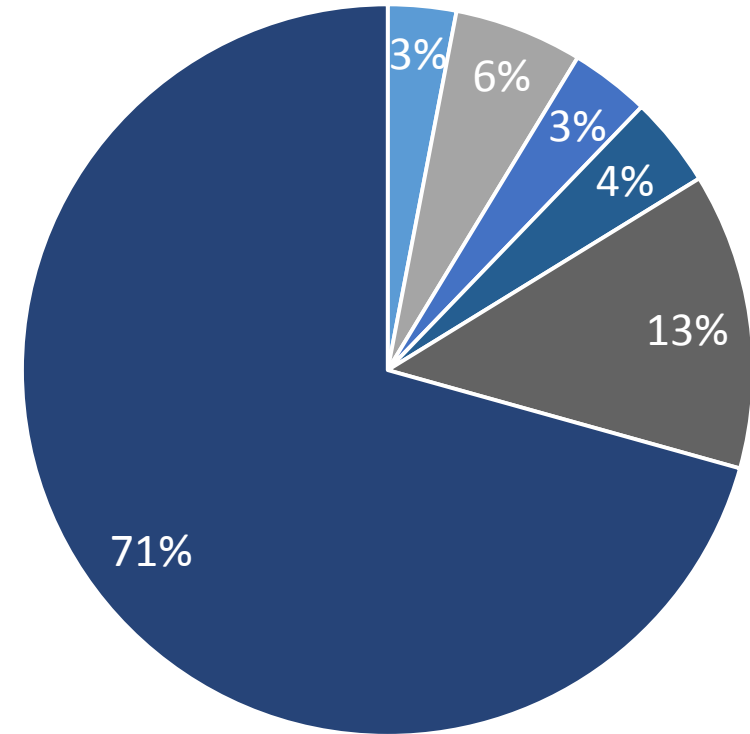
ID	Object name	Type/Reporting interval	Description	Location Key
1	bsnAPIfPhyChannelNumber	sampled/~180s	Current channel number of the AP radio.	EAP
2	bsnAPIfNoOfUsers	sampled/~90s	Number of clients associated with this radio.	EAP
3	bsnAPIfLoadChannelUtilization	sampled/~180s	Time percentage used by all non WiFi and WiFi traffic of current channel.	EAP
4	bsnAPIfInterferenceUtilization	sampled/~180s	Time percentage used by interference from other 802.11 networks on this channel.	EAP
5	bsnAPIfDot11TransmittedFrameCount	counter/~180s	This counter shall increment for each successfully transmitted MSDU.	EAP
6	bsnAPIfDot11RetryCount	counter/~180s	The number of attempts made by the EAP before transmitting the MSDU successfully.	EAP
7	bsnAPIfDot11FailedCount	counter/~180s	This counter shall increment when an MSDU is not transmitted successfully due to the number of transmit attempts exceeding either the bsnAPIf-Dot11ShortRetryLimit or dot11LongRetryLimit, (7 and 4 respectively in T)	EAP
8	bsnMobileStationAPMacAddr	sampled/~90s	802.11 MAC address of the AP to which the client is associated.	EAP, EAP client
9	bsnMobileStationAPIfSlotId	sampled/~90s	Radio of the AP to which the client is associated.	EAP, EAP client
10	bsnMobileStationSnr	sampled/~90s	The difference between signal strength and noise.	EAP, EAP client
11	bsnMobileStationBytesSent(Received)	sampled/~180s	Bytes sent to (received from) the client.	EAP, EAP client
12	bsnMobileStationPacketsSent(Received)	sampled/~180s	Packets sent to (received from) the client.	EAP, EAP client
13	cldcClientDataRetries	sampled/~180s	The number of attempts made by the client before transmitting the MSDU successfully.	EAP, EAP client
14	bsnRogueAPChannelNumber	sampled/~90s	The advertised channel number of the rogue picked up from the AP. It is different from bsnAPIfPhyChannelNumber.	EAP, RAP
15	bsnRogueAPAirespaceAPRSSI	sampled/~90s	RSSI of the rogue AP as seen by EAP.	EAP, RAP
16	bsnRogueAPTtotalClients	sampled/~90s	Total number of clients detected on this rogue.	EAP, RAP
17	bsnRogueClientAirespaceAPRSSI	sampled/~90s	RSSI seen by AP from the rogue client.	EAP, RAP client

CONFIRMED

RAP Classification

TABLE III
RAP CLASSIFICATION BASED ON SSID FIRST AND THEN OUI.

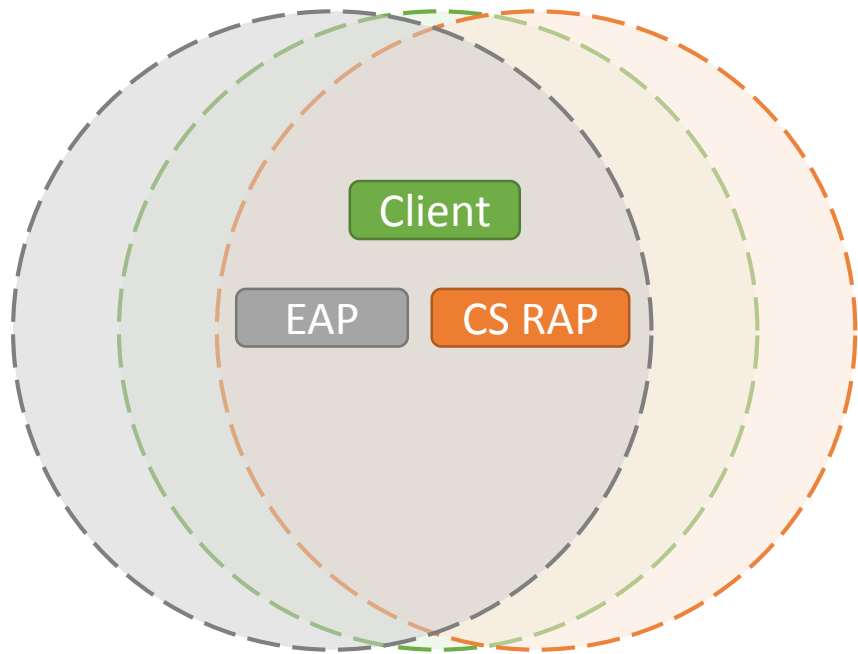
Type	Count. [Percentage]	Mobile?	SSID or OUI Keyword
3G Gateway	456 [3.02%]	Yes	[ssid] 3g, hame, incar, mobile, pocket, portable, u+net
Smart Phone	857 [5.67%]	Yes	[oui] meizu, mobile, nokia, oppo, samsung, xiaomi [ssid] android, coolpad, htc, ipad, iphone, mylgnet, ruitel
USB WiFi Dongle	532 [3.52%]	Yes	[ssid] 360wifi(504), baidu(28)
Software AP on Laptops	606 [4.01%]	Yes	[oui] apple, lenovo, toshiba [ssid] asus, dell, hp, lenovo, thinkpad, vaio [software] connectify, dubawifi, liebaofree
Neighbor Enterprise WiFi	1981 [13.11%]	No	[oui] aruba, cisco(383), h3c(829), juniper [ssid] cernet, chinacomm, chinanet(623), chinaunicom(308), cloudwifi, cmcc(208), ctt-T (259), cu_campus(69), cwic, gehua(51), ivi, nuctech(183), videophone
Residential AP	10678 [70.67%]	No	[oui] d-link(482), hiwifi(103), huawei(1144), netgear(360), tenda(603), tp-link(5387), zte(312) [ssid] b-link, buffalo, dd-wrt, d-link, dorm, fast, feixun, hiwifi, huawei, iptime, jcg, lab, mercury, netcore, netgear, openwrt, phicomm, print, room, tenda, toto-link, tp-link, volans, zte ...



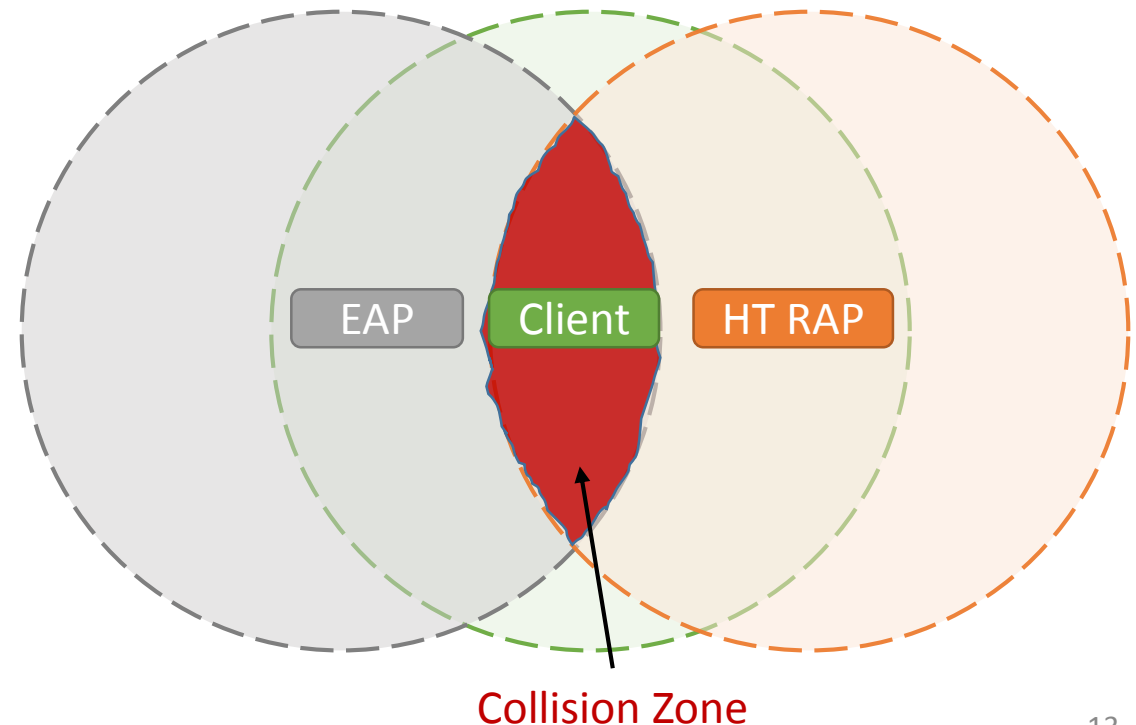
- 3G Gateway
- Smart Phone
- USB Wifi Dongle
- Software AP on Laptops

RAP Impact: CS RAP and HT RAP

- [CS RAP] Carrier Sense RAP
 - Impact: **EAP Access Delay**



- [HT RAP] Hidden Terminal RAP
 - Impact: **EAP Packet Loss**



RAP Impact: CS RAP and HT RAP

- [CS RAP] Carrier Sense RAP
 - Impact: EAP Access Delay
- [HT RAP] Hidden Terminal RAP
 - Impact: EAP Packet Loss

Due to the totally different impacts on EAP

RAP Impact: CS RAP and HT RAP

- [CS RAP] Carrier Sense RAP
 - Impact: EAP Access Delay
- [HT RAP] Hidden Terminal RAP
 - Impact: EAP Packet Loss

Due to the totally different impacts on EAP

- The CS RAP and HT RAP needs to be distinguished.
- The impact of CS RAP and HT RAP needs to be measured respectively.

Distinguish CS RAPs and HT RAPs

- CS RAPs or HT RAPs?



RSSI = -75dBm



RSSI = -80dBm



RSSI = -90dBm



RSSI = -95dBm

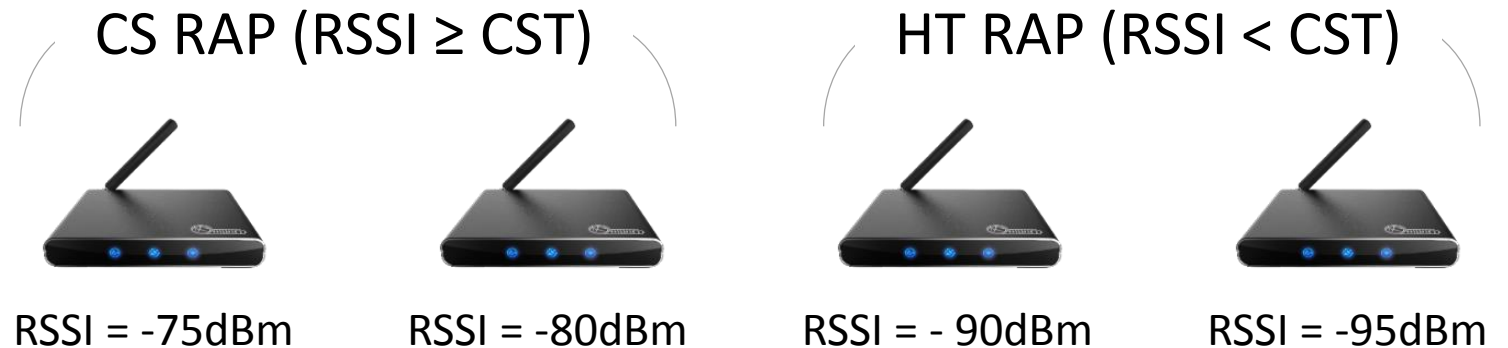
Use the RAP **RSSI** and **CST** to distinguish.
(Carrier Sense Threshold)

- RSSI is from SNMP
- CST = -85dBm

Distinguish CS RAPs and HT RAPs

- CS RAPs or HT RAPs?

RAP ∈ CS RAP IF RSSI ≥ CST



Use the RAP **RSSI** and **CST** to distinguish.
(Carrier Sense Threshold)

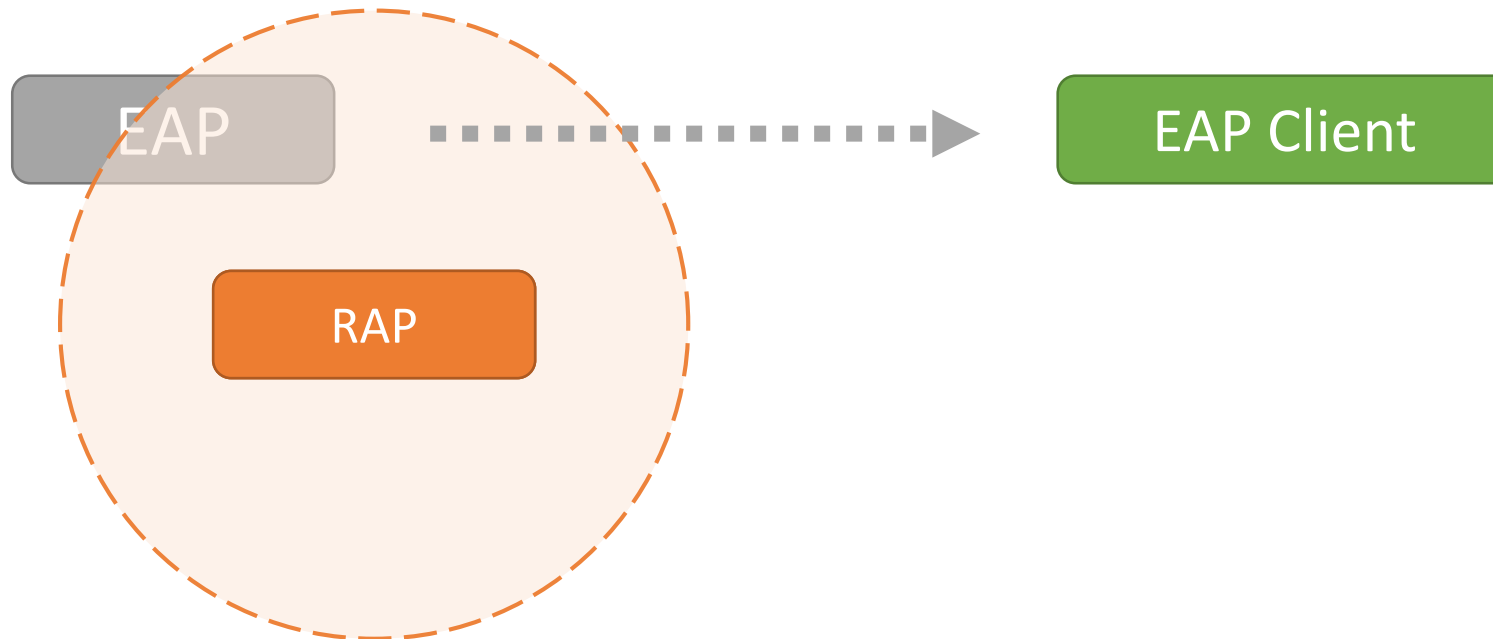
- RSSI is from SNMP
- CST = -85dBm

Distinguish CS RAPs and HT RAPs

- Why **CST** (*Carrier Sense Threshold*) = -85dBm ?
 - Empirical value : Nabeel Ahmed. *Interference Management in Dense 802.11 Networks*. PhD thesis.

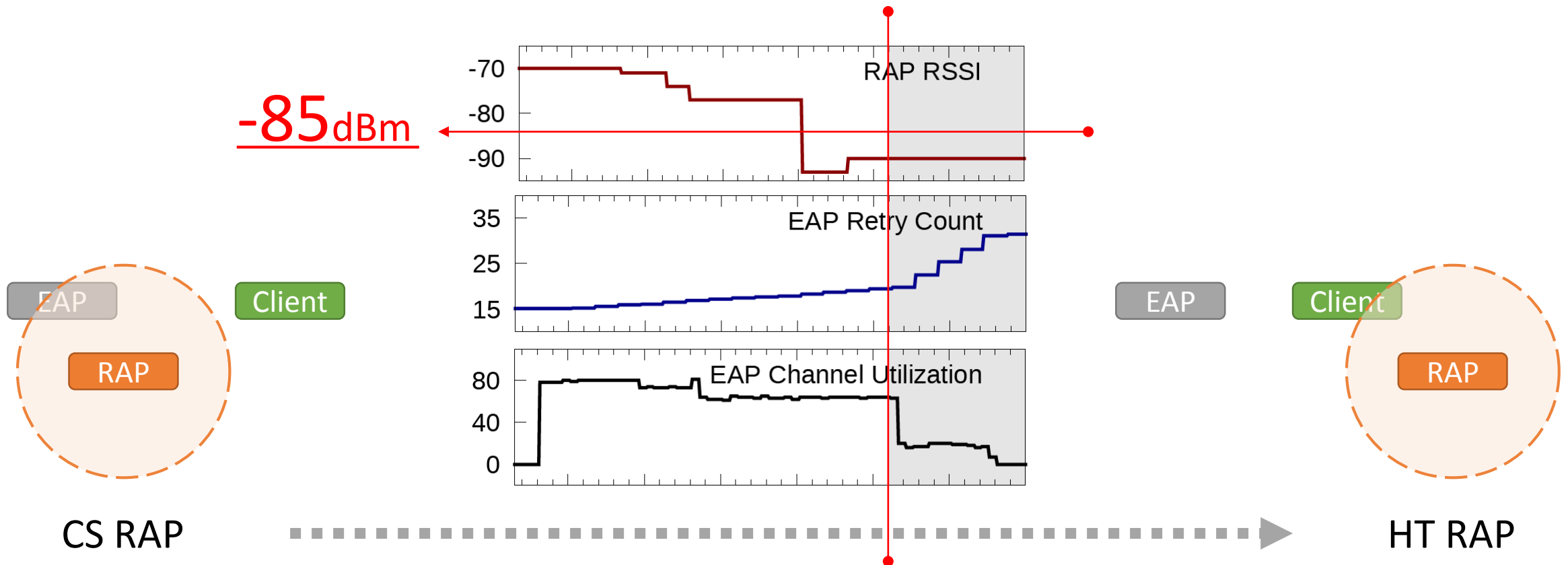
Distinguish CS RAPs and HT RAPs

- Why **CST** (*Carrier Sense Threshold*) = -85dBm ?
 - Empirical value
 - Control experiment

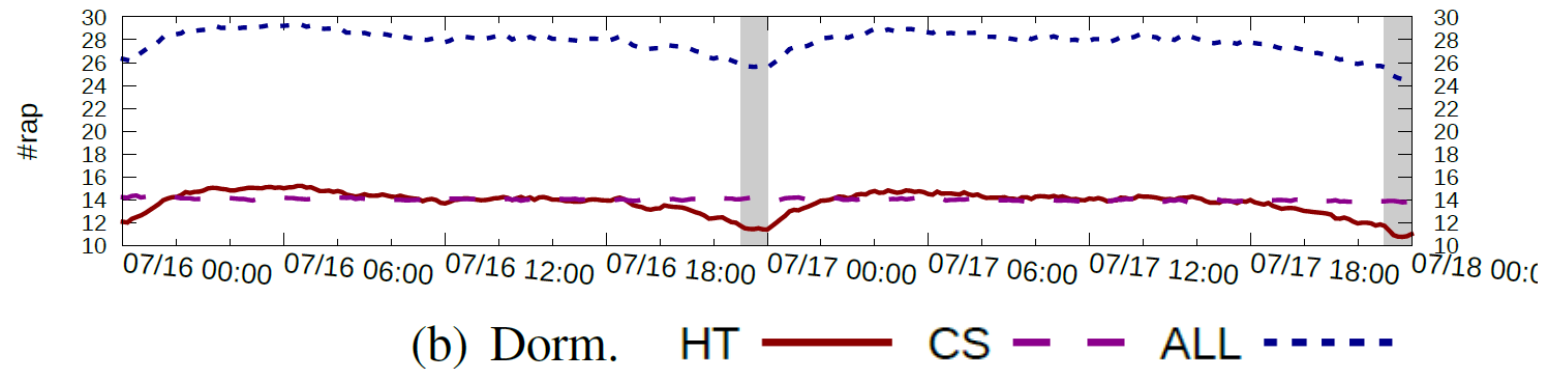


Distinguish CS RAPs and HT RAPs

- Why **CST** (*Carrier Sense Threshold*) = -85dBm ?



#CS RAP and #HT RAP - vary over time



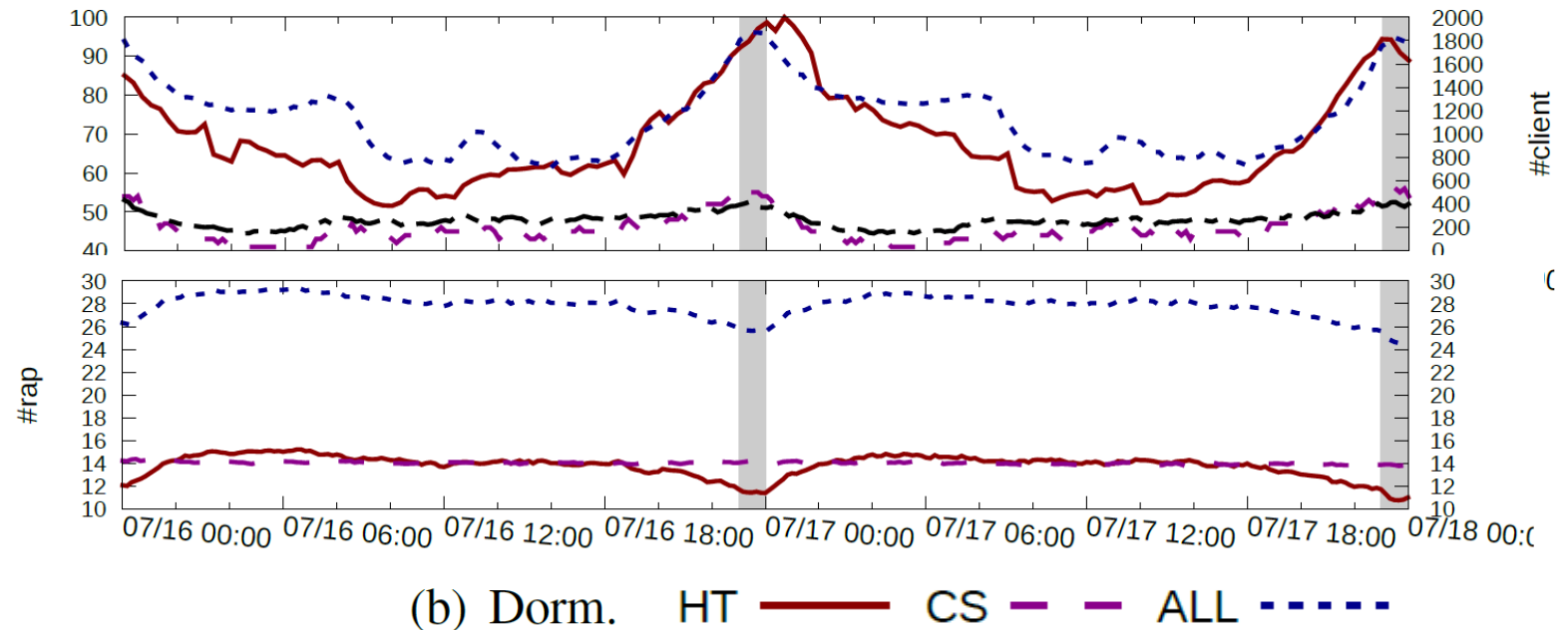
#CS RAP and #HT RAP - vary over time

- Human traffic has a significant impact on the RSSI of WiFi devices

★ *Some HT RAPs disappear at the Rush Hour : Multipath Fading*

Human Traffic ->

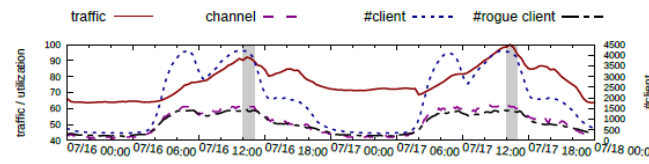
#RAP ->



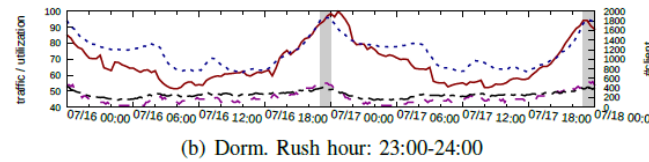
#CS RAP and #HT RAP - vary over time

- Human traffic has a significant impact on the RSSI of WiFi devices

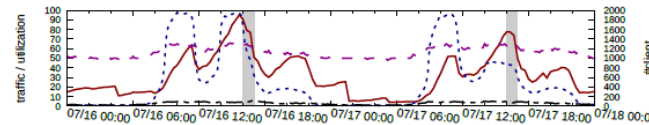
★ *Some HT RAPs disappear at the Rush Hour : Multipath Fading*



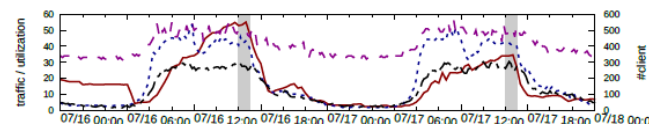
(a) Department. Rush hour: 16:00-17:00



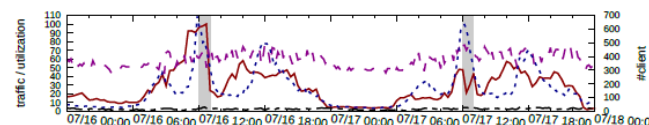
(b) Dorm. Rush hour: 23:00-24:00



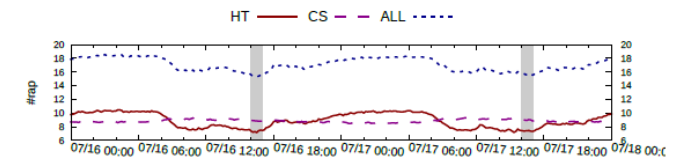
(c) Classroom. Rush hour: 16:00-17:00



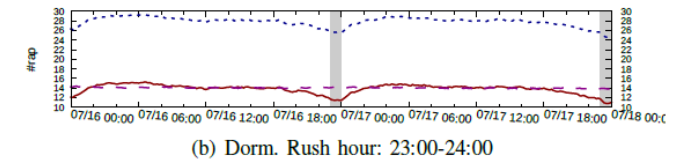
(d) Administrative. Rush hour: 16:00-17:00



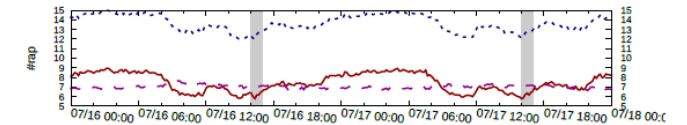
(e) Cafeteria. Rush hour: 12:00-13:00



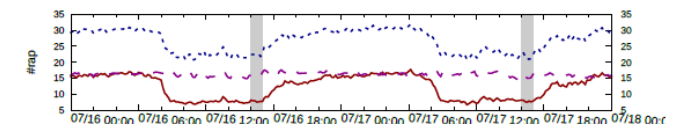
(a) Department. Rush hour: 16:00-17:00



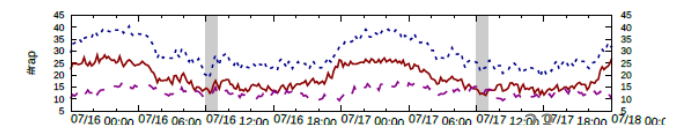
(b) Dorm. Rush hour: 23:00-24:00



(c) Classroom. Rush hour: 16:00-17:00



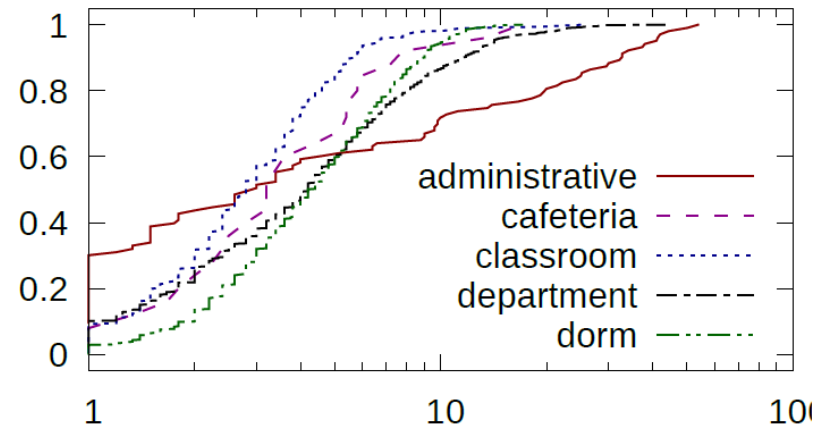
(d) Administrative. Rush hour: 16:00-17:00



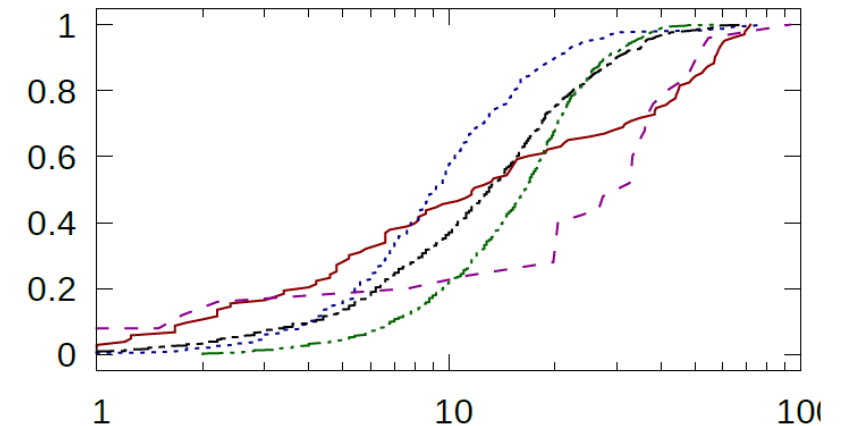
(e) Cafeteria. Rush hour: 12:00-13:00

#CS RAP and #HT RAP - at an EAP

- #CS RAP v.s. #EAP : 5 v.s. 1
- #HT RAP v.s. #EAP : 15 v.s. 1
- Large number of RAPs and more HT RAPs than CS RAPs.



(a) CS RAP at an EAP



(b) HT RAPs at an EAP

Measure RAPs' impact on EWLAN performance

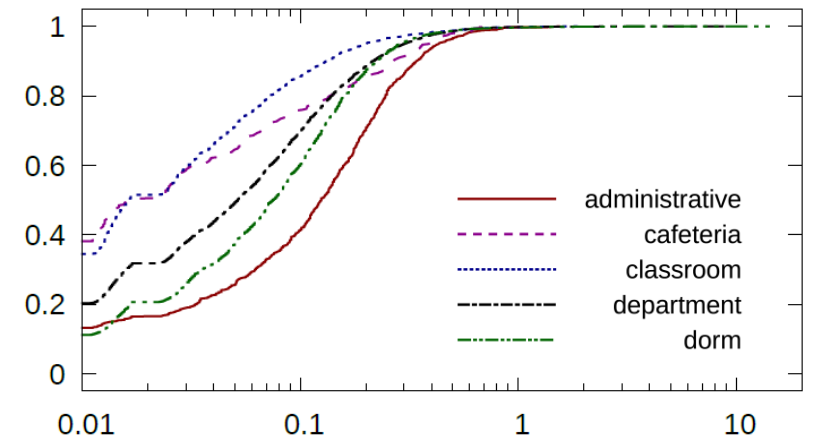
- CS RAP impact: EAP access delay
 - **CSI** (*Carrier Sense Interference*) when channel utilization is high

$$\text{CSI} = \text{Interference Utilization} / (\text{Channel Utilization} - \text{Interference Utilization})$$

- **Not Severe** ($\sim 5\%$, $< 10\%$ in most cases)



The EAP placement, channel, and power are carefully designed and optimized by the vendor software for the EWLAN.



(a) CSI ($LU > 60$ #EAP Client > 0)


Measure RAPs' impact on EWLAN performance

- HT RAP Impact: EAP packet loss
 - **LOSSRATE** of packets from EAP to high SNR clients

Measure RAPs' impact on EWLAN performance

- HT RAP Impact: EAP packet loss

- **LOSSRATE** of packets from EAP to high SNR clients

 *Filter the Packet Loss caused by Low SNR including Non-WiFi Interference, Fading Channel, etc.*

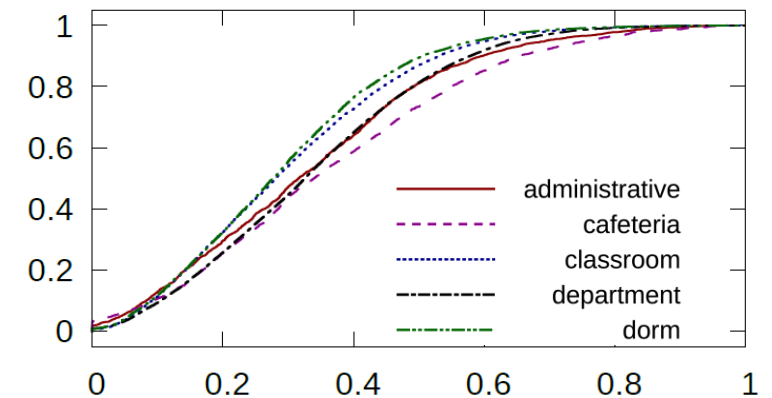
Measure RAPs' impact on EWLAN performance

- HT RAP Impact: EAP packet loss
 - **LOSSRATE** of packets from EAP to high SNR clients

$$\text{MAC LOSSRATE} = \frac{(\text{Retry Limit} * \text{Fail Count} + \text{Retry Count})}{(\text{Retry Limit} * \text{Fail Count} + \text{Retry Count} + \text{Success Count})}$$

- **Severe** (~ 30%, > 50% in 20% cases)

★ *Current EAP software do nothing about HT RAPs. Operators should take more attention to HT RAPs to alleviate the LOSSRATE.*



(d) MAC LOSSRATE of EAP to high SNR clients (SNR > 30)

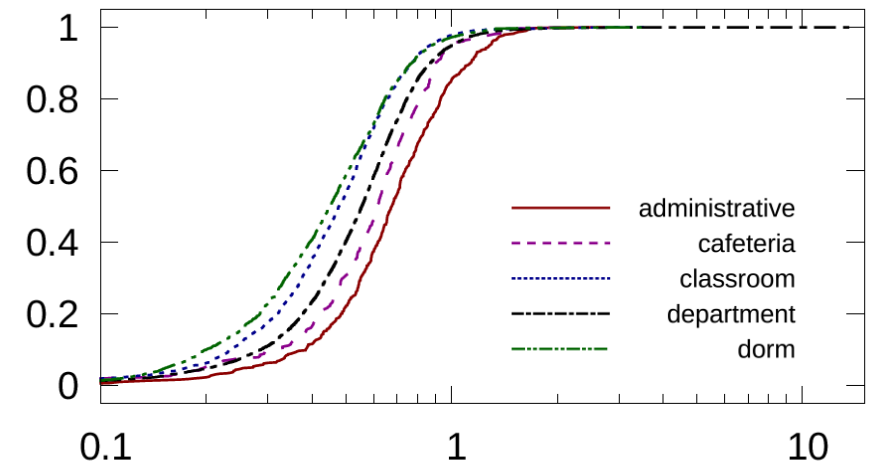
Measure RAPs' impact on EWLAN performance

- The overall impact of RAPs: IP layer delay at the WiFi hop

- **IMPACT**

$$\text{IMPACT} = (1 + \text{CSI}) * (1 + \text{MAC LOSSRATE}) - 1$$

- **Severe** (~ 50%, > 80% in 20% cases)



Conclusion

- The first large-scale measurement study on rogue APs' impact on the EWLAN performance.
- Propose a generic methodology to distinguish CS RAPs and HT RAPs, and roughly quantify their impact using only SNMP data.
- Key findings of our studied EWLAN
 - RAPs are chaotic in EWLAN.
 - Carrier sense interference due to RAPs are not severe.
 - Hidden terminal interference due to RAPs are much more severe.
(increasing up to 50% MAC loss rate)



Thank you !