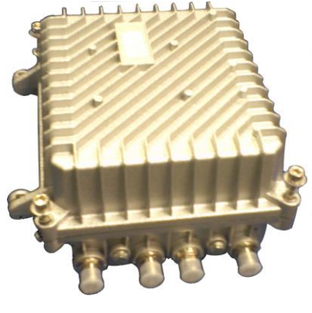


ROGUE AP DETECTION

Group Members: Lau Yiu Ching, Au Ho Wa

Supervisor: Prof. Chan Shueng Han

INTRODUCTION

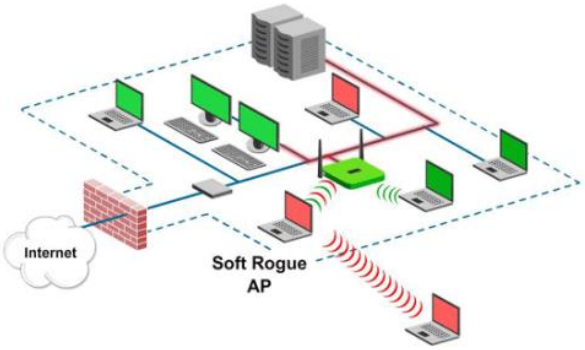
Recently year, engineers working on wireless security to prevent security threat happen. It seem that the above wireless security measures can be prevent our wireless networking, but unfortunately, these wireless security measures can easily be break.

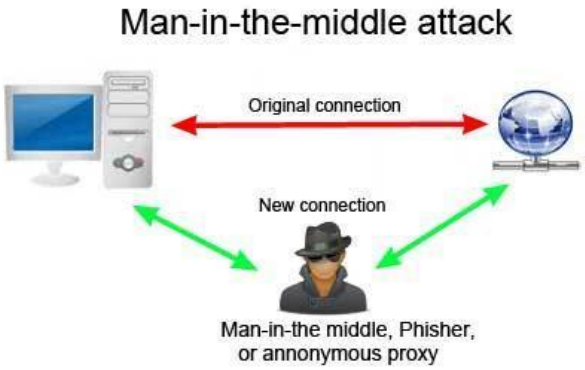
In addition, recent year, hacker using rogue access point technology in wireless network.

The rogue APs can be built with very similar or same settings with the secure APs by some tools just mention above. When the network users searching Wi-Fi networks, they will not know the different between the real secure AP and the rogue AP.

The problem of rogue AP is that it will raise some security issues. For example hacker can use it to conduct a man-in-the-middle attack, that the attack may be used simply to gain access to the message, or enable the attacker to modify the message before retransmitting it.

Because current solution cannot actually solve the rogue AP security thief, in this project, we are proposed a new solution to solve this security thief, which is by using each router beacon frame feature to detect rogue AP in a wireless network.





OBJECTIVE

Our project contains two main parts: Beacon frame discover and using the data we discovered to find out are there any rogue APs, if yes, how many rogue APs are there. The discover tool that included in the detection system has been implemented by first sniffing beacon frame packets by router, then decode the packet, there are important information, i.e. SSID, MAC address, timestamp. The most important data we need is timestamp. Since timestamp of the packets sent by router are unique that can help us to find out the rogue APs. After decoded the data what we need then the system will record down to database and pass it to another function to do another calculations, which is clock-skew. Using the result of clock-skew we can find out are there any rogue APs.

The system requires a network administrator to input all the information of his routers that in his local network into a table in the system database, it use for identify the real APs in the local network.

The system of our project can mainly detect three type of rogue APs:

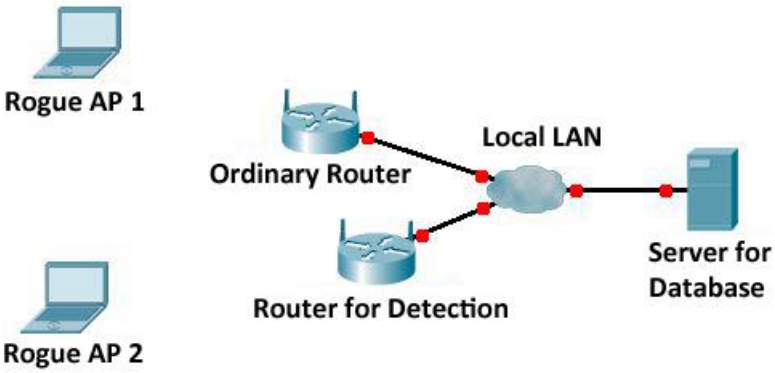
(1) Same SSID and not same MAC address with one of our router
(2) Not same SSID and same MAC address with one of our router
(3) Same SSID and same MAC address with one of our router

From a technical point of view, the detection system need as least two routers, as the router cannot detect the rogue APs for its own, so it need another router help it to detect, and it can help that router to detect rogue APs correspondingly.

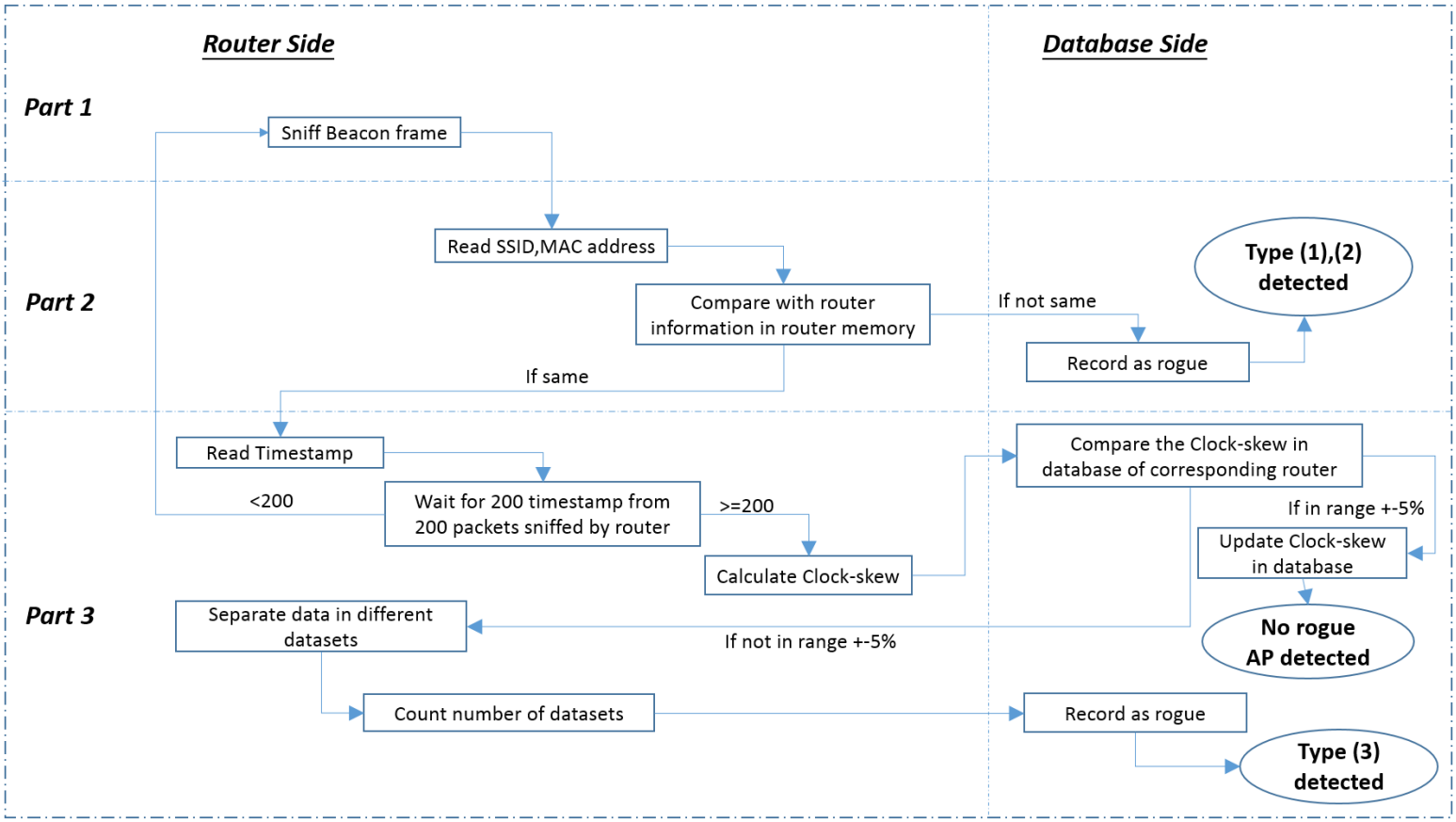
DESIGN

SCENARIO

We have 2 routers, 2 PC and 1 server. One router help another router to detect rogue APs, another router keep working as usual, the 2 PC will act as the soft rogue AP by using hostapd, and the server for providing database function.



SYSTEM FLOW



There are mainly three parts in our system cycle:

(1) Discover packet	(2) Find type (1), (2) rogue APs	(3) Find number of type (3) rogue APs, if any.

Part1 Discover packet

- ✓ Sniff packet with Libpcap
- ✓ Only get beacon frame

Part2 Find type (1), (2) rogue APs

- ✓ Compare SSID and MAC address with the information of local routers
- ✓ If match move to Part 3
- ✓ If not, ***Type 1,2 Rogue APs Detected***

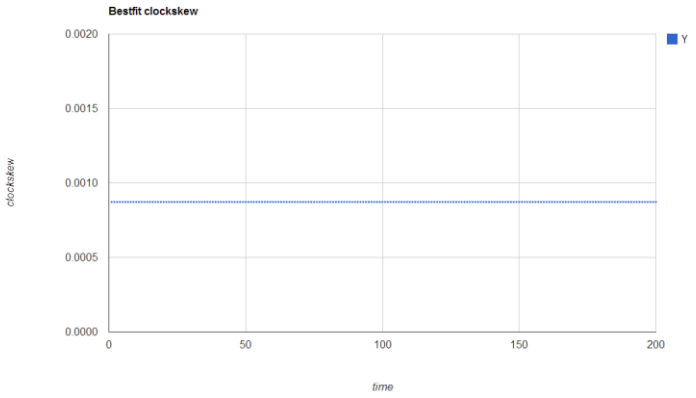
Part3 Find number of type (3) rogue APs, if any.

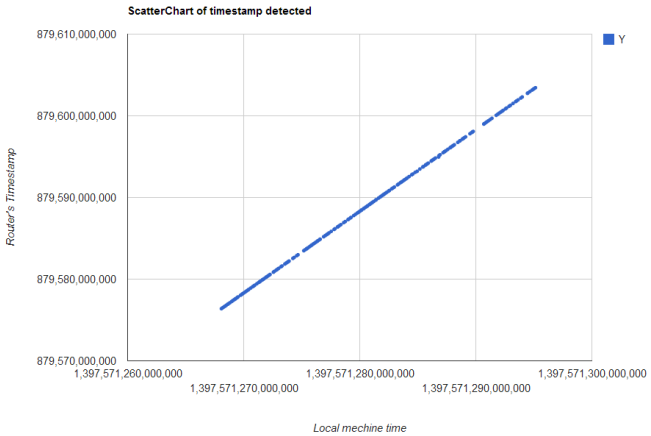
- ✓ Calculate Clock-skew using 200 sniffed packets
- ✓ Compare the Clock-skew with the reference
- ✓ If match **NO Rogue Detected**
- ✓ If not match separate the data into different data set and count number of them
  Number of datasets – 1(The ordinary AP) = Number of type 3 rogue APs
  And ***Type 3 Rogue APs Detected***

RESULT

Normal Operation

- ✓ Linear line for source timestamp vs local timestamp
- ✓ Only one line shown on clock-skew chart
- ✓ Stable range of clock-skew





	clock-skew
1st trial	0.001179408
2nd trial	0.000885813
3rd trial	0.000707698

date_time	mac_address_target	mac_address_source	type	router
2014-04-15 21:17:55	d8:5d:4c:af:13:9b	c0:c1:c0:41:e4:1	1	0

date_time	mac_address_target	mac_address_source	type	router
2014-04-15 ...	d8:5d:4c:af:13:9b	c0:c1:c0:41:e4:a5	2	0

Type (1), (2) rogue APs

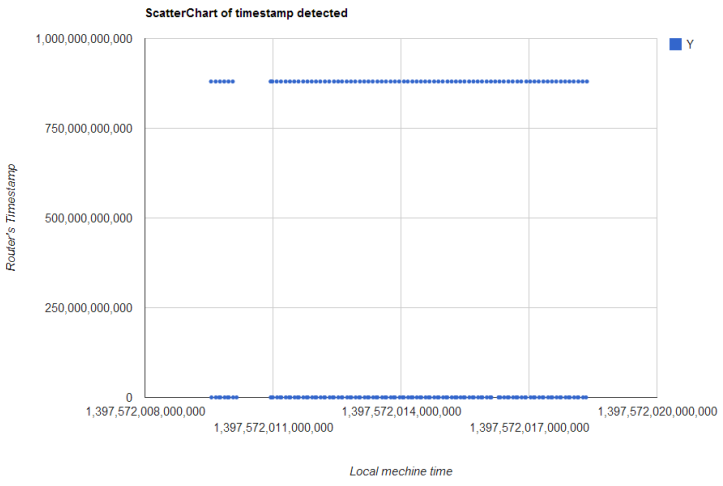
- ✓ Database will show rogue record with type(1) or (2)
- ✓ Packet will drop

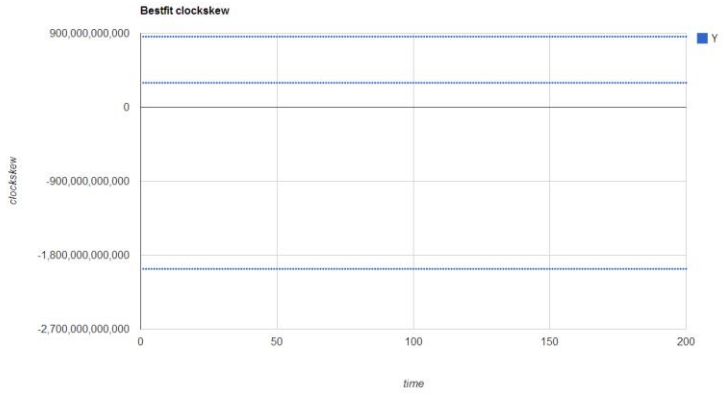
Type (3) rogue AP

- ✓ Database will show rogue record with type(3) and the number of routers exists is 3.
- ✓ Two likely straight line showing on source timestamp vs local timestamp
- ✓ There three line showing on clock-skew chart
- ✓ Various range of clock-skew shown on each routers

date_time	mac_address_target	mac_address_source	type	router
2014-04-15 21:26:15	d8:5d:4c:af:13:9b	c0:c1:c0:41:e4:a5	3	3

	routers	clock-skew
1st trial	1	7.48559E+12
	2	3.03687E+11
	3	-2.2773E+11
2nd trial	1	9.78352E+11
	2	2.77459E+11
	3	2.27477E+11
3rd trial	1	6.20207E+11
	2	4.07812E+11
	3	2.68039E+12





CONCLUSION

To conclude, wireless security is not enough to protect rogue ap security threat. Nowadays, many network company are working on that area to protect their client using their wireless network solution. In this project, we proposed a new way to detect rogue ap using beacon frame from each router. Due to limited time and resource, there is still much room for future development that would enhance the system and increase its business value such as auto deauthentication and localization detection. We hope that this project can helps Lavinet to enhance their security function and become one of the benefited compare with other mesh wireless network solution in Hong Kong.