Technology Platforms
Best Practices How to Use WLAN

September 12th, 2007

Mikko Jaakkola
Head of WiWLAN SF

NOKIA

Outline

- Introduction
- Best Practices for WLAN Mobile Device
- Best Practices for WLAN Network Configuration for Mobile Devices

Introduction

- Presenter: Mikko Jaakkola – worked ~11 at Nokia
- Strong SW background and mostly worked the SW developer career with HW/SW interfaces implementing device drivers for Windows, Linux and Symbian OSes
- Working with WLAN since 1999 from WLAN APs to PC-devices and ramping up Nokia WLAN SW device development
- Heading WiMAX & WLAN Software Factory at Technology Platforms

Best Practices for WLAN Mobile Devices

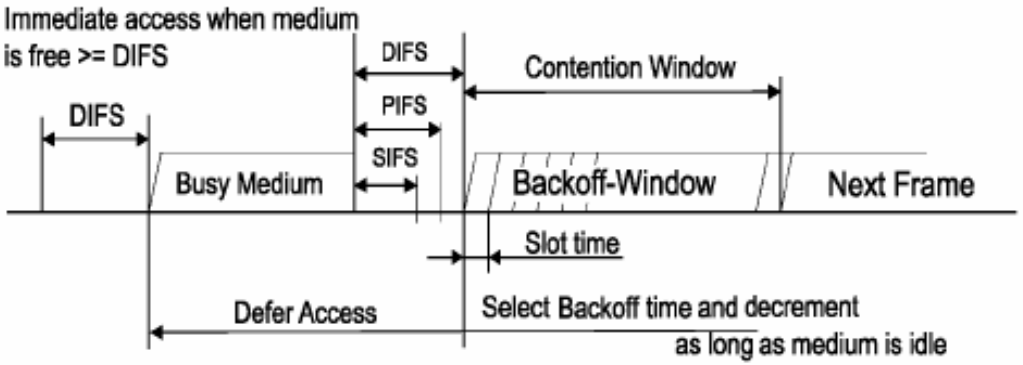
- Few words in general about power-consumption
- Power-saving considerations
- Aim at the best throughput

WLAN power save – key issues

- There are a lot of factors affecting to overall WLAN power efficiency
  - WLAN HW power consumption
  - Host processor power consumption
  - WLAN power save protocols
  - WLAN AP configuration
  - WLAN network discovery/selection
  - Upper layer/non-WLAN protocols
  - Applications
  - Load in the network

WLAN HW and host power consumption

- Natural sources of power consumption
  - WLAN HW consumes power when in RX and TX operations
  - Important to understand WLAN MAC protocol operation – RX is typically 'ON' even if no active reception is in process and if not in power save state => power save states shall be used aggressively



  - Typically TX power consumption bigger than RX although the gap is getting smaller
  - Scanning uses RX functionality in fully active-mode so it is very power-consuming operation compared to normal operations
  - Host power consumption is either due to WLAN specific operations or any other operations run in the host processor

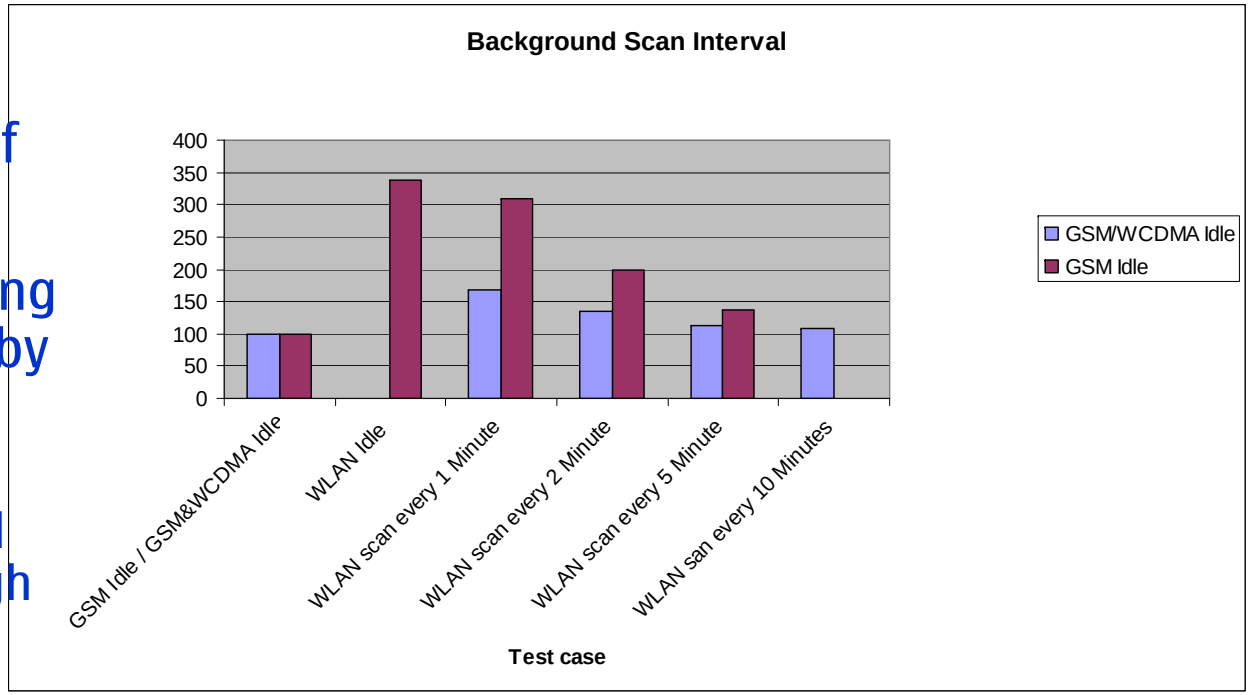
Figure source: IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

Power-saving Considerations

- Network Discovery (aka scanning)
- Power-saving schemes
- Application Implications

WLAN network discovery/selection

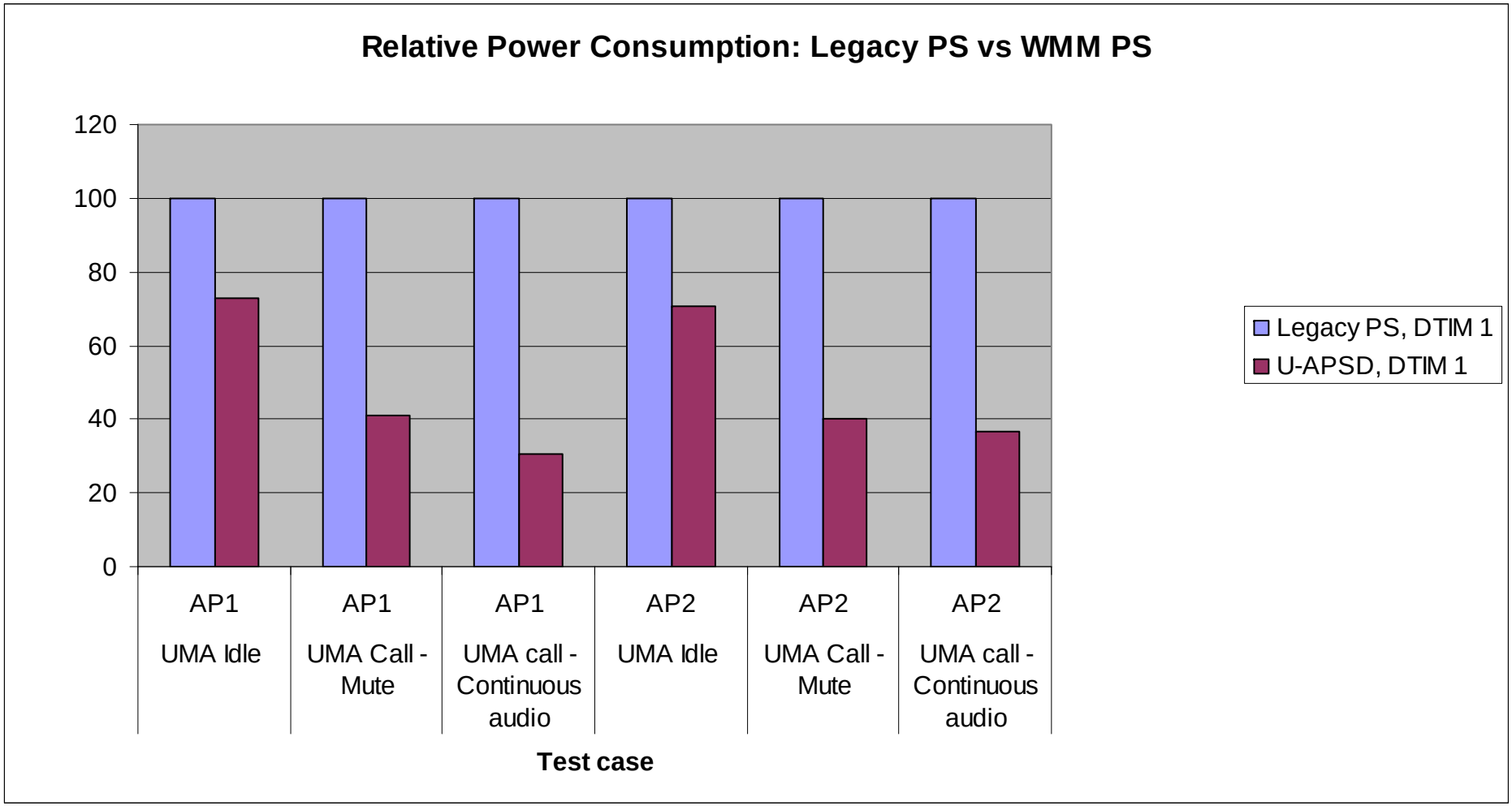
- WLAN network discovery is done using scanning
- WLAN device decides what type of scan is being used
- The frequency of scanning is having major impact to terminals stand-by times => avoid performing unnecessary scans
  - WLAN engine will scan if the signal level drops or if packet loss too high
- Try to leverage platform functionality as much as possible without trying to run algorithm locally unless you really need to



WLAN power save protocols (1/2)

- IEEE 802.11 power save protocol operation can be divided to unicast and broadcast/multicast parts
- New U-APSD (Unscheduled-Automatic Power-Save Delivery) provides significant improvements to active/talk times.
  - Especially VoIP power efficiency is increased dramatically if U-APSD can be used. Talk times easily doubled compared to the legacy power save (see next slide).
  - Requires that the voice packets are marked (DSCP, IETF RFC 4594) correctly
- Broadcast/multicast power save operation determines the devices stand-by times when being connected
  - Simple protocol
    - New standard proposals to enhance the protocol
  - Efficiency depends largely on WLAN AP configurations (covered later on)
  - Unnecessary broadcast/multicast packets (NETBIOS, bridge/switch control protocols,...) can cause significant power consumption in device side
- Generally WLAN SW/HW is taking care of power save protocol operations and applications does not have to care about it – however, applications developers are still in position to mess the system up ☺
- Main tools to improve WLAN power efficiency is to a) utilise latest WLAN power save features in the networks (U-APSD) and b) reduce unnecessary broadcast/multicast traffic in the networks or implement filtering functions (e.g. proxy ARP)

WLAN power save protocols (2/2)



Things to Impact About Power-save

- Applications have naturally big impact to power consumption
- Always-on applications
  - Push email
  - SIP/VoIP
  - And probably many others
- Overlapping application and protocol level keep-alive can be a real pain when not taken under consideration
- Other principles:
  - Avoid frequent scanning
  - Use correct DSCP settings
- Some of the new standardized WLAN features can increase the power consumption if used without consideration
  - WLAN measurements (802.11k)
    - Do not measure unnecessarily
  - WLAN location/presence (802.11k/802.11v)
    - Trade-off between location accuracy ⇔ power consumption
  - Typically these are taken care by the WLAN SW stack
- Activity of other co-located radios (e.g. Bluetooth) and distance from WLAN AP also impacts power-consumption

Aim at the Best Throughput

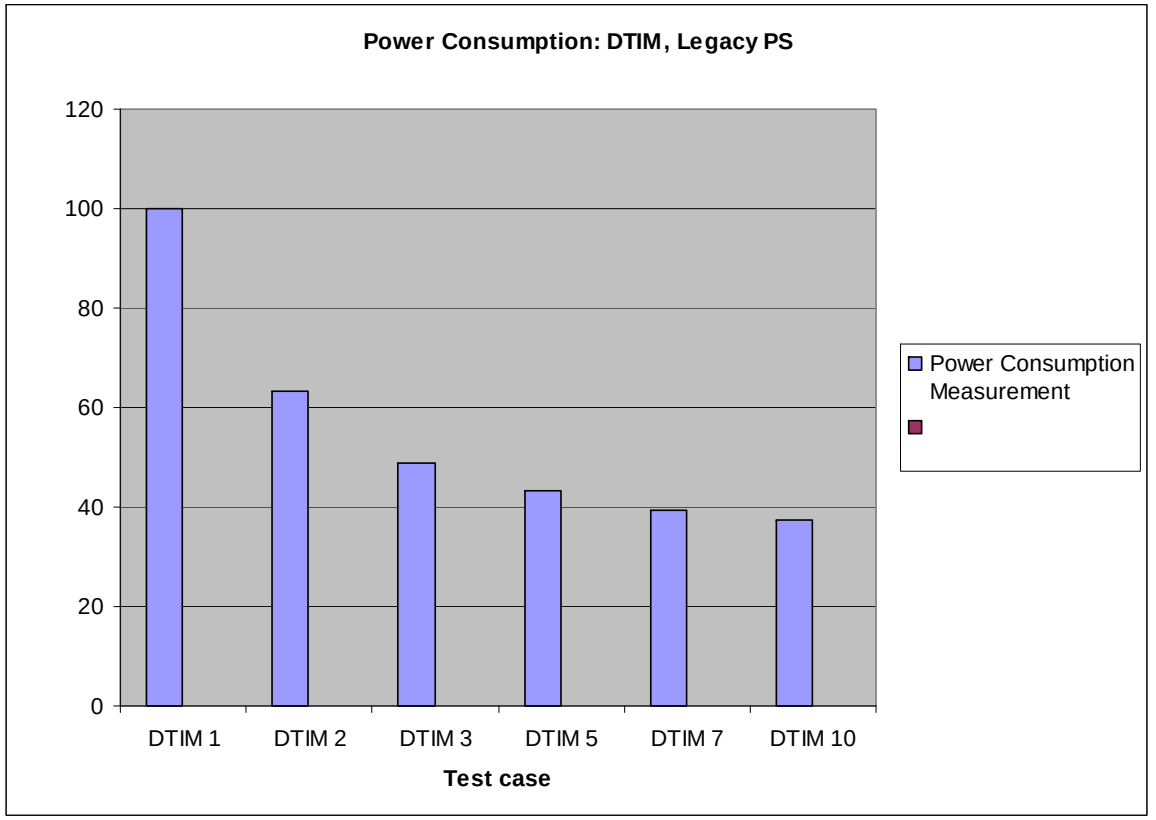
- Limited capacity in the mobile phones makes it challenging to use full WLAN capacity
- However, some schemes can be used to improve the performance
- The easiest scheme is to keep data path busy
  - Before writing data to disk or otherwise processing it, the application should initiate the next request to network so that receiving and processing data can overlap
- Use appropriate DSCP to tag bulk data from voice-traffic as power-save algorithms run per AC bases
- WLAN is very fast link so applications should try to send/receive large amounts data to reduce per byte overhead

Best Practices for WLAN Network Configuration for Mobile Devices

- WLAN AP Configuration
- Upper-layer protocols
- Handover times for security protocols

WLAN AP configurations

- Typically WLAN AP OOB settings are not very mobile friendly
- From power save perspective the most relevant setting is DTIM
  - DTIM setting is determining terminals stand-by power consumption
  - In many cases DTIM is set to 1 while DTIM=3 seem to be good value from PS point of view and without having impact to delays etc.
- Hidden SSID usage is another source of headaches (see next slide)



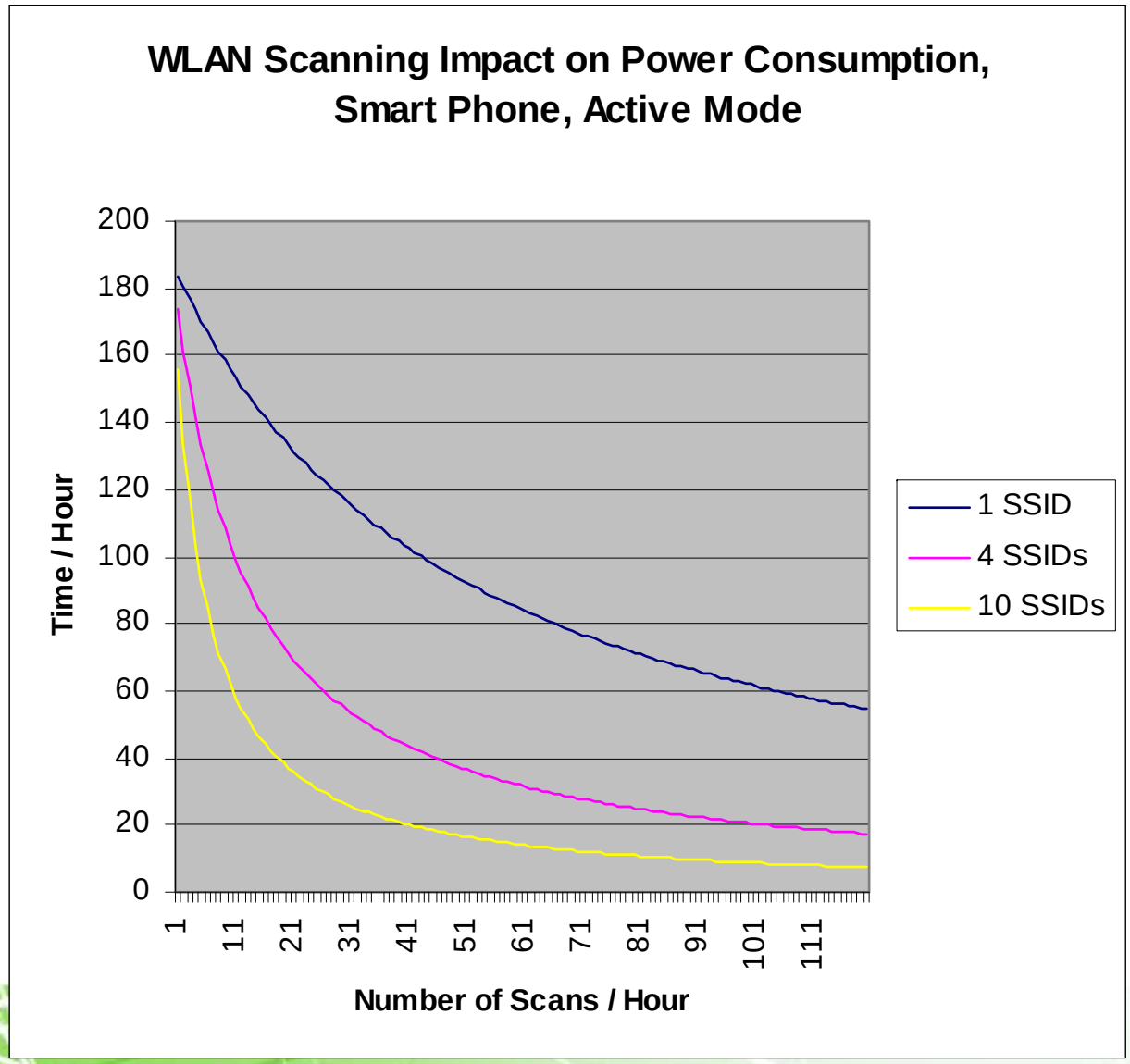
Hidden/Multiple SSIDs

- There is proprietary scheme for hiding SSID of the WLAN APs that was meant to improvement security by increasing obscurity
  - It does not really increase security (its like hiding a door)
  - It makes networking planning more difficult from common people

- Hidden SSIDs are an evil scheme to stop people from using WLAN in mobile environment
  - Every hidden SSID must be explicitly scanned
  - Increased scan time and increased power consumption
  - No standard way to implement hidden SSID, AP vendors are having different ways to indicated hidden SSID => detection of hidden SSID not as robust as normal broadcasted SSIDs

- **Do not use hidden SSIDs!**
  - All the BSSIDs should be, in general, made visible to help mobile device to be more efficient

Scanning Impact on Power-consumption



Upper layer/non-WLAN protocols

- ARP
  - Use of proxy ARP recommended
  - ARP cache expiry timers should be long enough (>30 min) if proxy ARP is not used
- Local broadcasts/multicasts
  - All the unnecessary BC/MC protocols should be filtered out/disabled
- NAT/firewall configurations
  - For TCP, keep alive intervals should be relatively long (20 min)
  - For UDP, keep alive intervals should be application specific if possible. For example for IPsec the interval could be long while for DNS is should be much shorter
  - General rule from the WLAN PS perspective is to send keep alive as seldom as possible

Load In The Network

- WLAN is random access protocol meaning that there is no centralised scheduler which allocates the capacity for the terminals
- Each terminal must contend for the medium access
- In lightly loaded networks the medium is practically free all the time and terminal can get access to the medium easily
- In medium-highly loaded networks the amount of contention increases and channel access will take more time and consumes power as well (as the terminal has to keep its RX on)
  - It is important to use DSCP mapping to guarantee that the high priority packets are correctly prioritized during channel access procedure
- Also neighbor APs/networks load can affect to the terminals performance
- With right network planning, the load related factors can be optimized
  - Don't use mixed-mode (b+g) network modes unless you really have old 802.11b clients

Handover Times For Security Protocols

- Measured average AP2AP handover times on E90

Roaming time	Average	Time
Open (no security)	30.66	msec
CCKM-LEAP-TKIP	41.89	msec
WPA-PSK-TKIP	158.40	msec
WPA-LEAP-TKIP	295.11	msec
WPA-TLS-TKIP	945.03	msec

Notes:

1) All tests included CCX "AP assisted roaming" feature, which improves the AP2AP roaming 50-70ms.

2) The CCKM-LEAP-TKIP measurement included CCX CCKM fast roaming feature.

3) EAP-TLS did not include PEAP. We would expect "PEAP with EAP-MSCHAPv2" to take as long time as EAP-TLS (800 - 900ms).

4) Proactive key caching will be improve the situation so the feature should be enabler when ever possible