Stuffing Wi-Fi Beacons for Fun and Profit

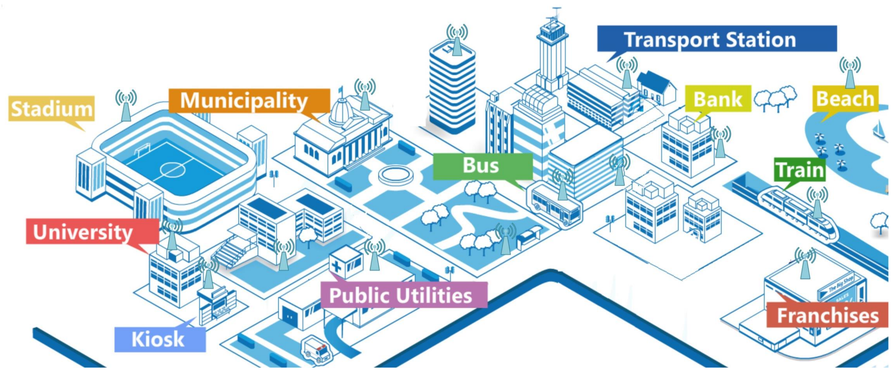
The Telecommunication Networks Group (TKN)
Technische Universität Berlin

Sven Zehl, Anatolij Zubow and Adam Wolisz
{zehl, zubow, wolisz}@tkn.tu-berlin.de
Department of Telecommunication Systems, Technische Universität Berlin

GET IT ON Google play

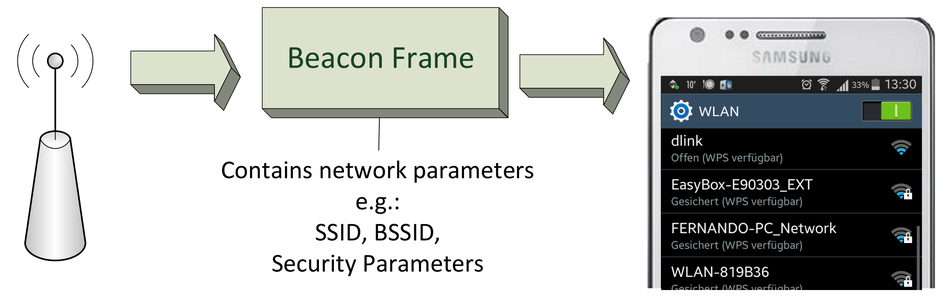
Download the LoWS app and participate live!

Motivation: Wi-Fi Access Points are everywhere!



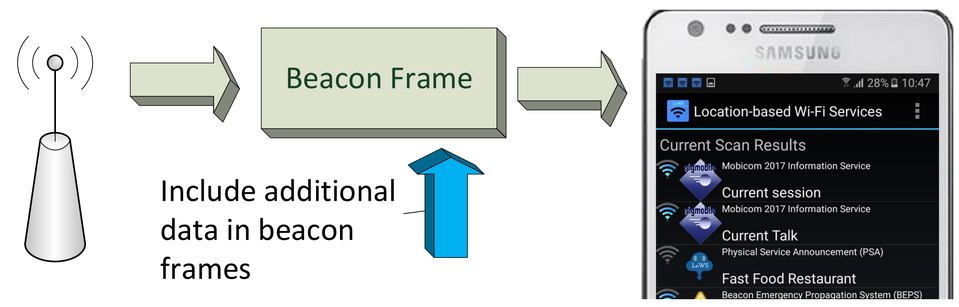
- IEEE 802.11 (Wi-Fi) is the standard technology for wireless networks especially in providing wireless Internet access
- IEEE 802.11 Access Points (APs) are widely deployed, nearly everywhere:
  - Shopping Malls,
  - Trains and Train Stations,
  - Airports and Planes,
  - Hospitals, Office Spaces...

Observation:



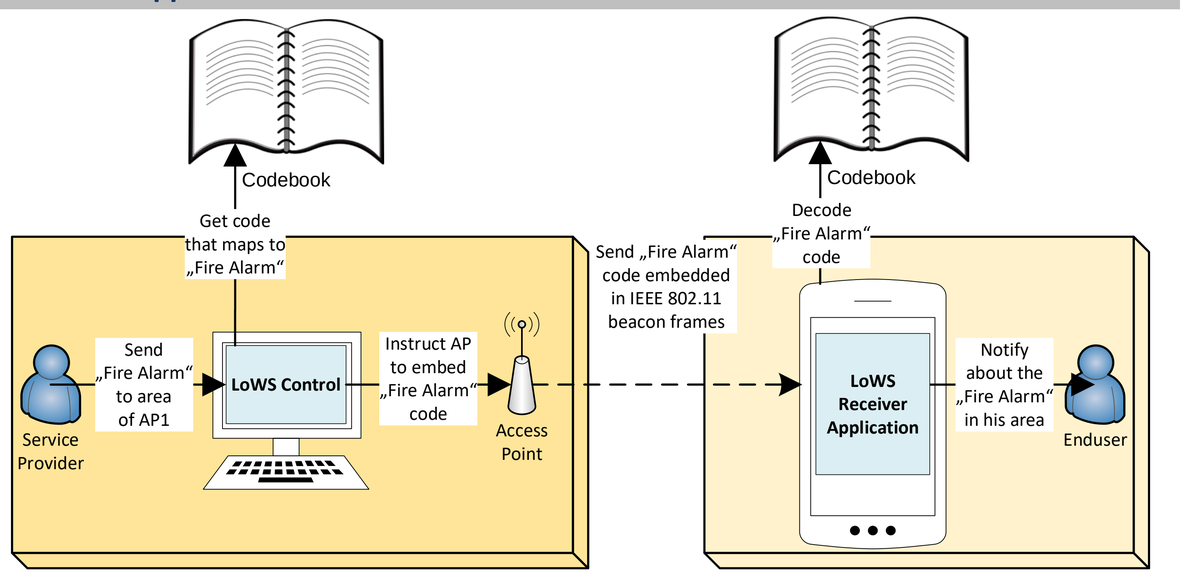
- To enable Wi-Fi clients to discover APs in their vicinity, Wi-Fi APs are announcing their presence by broadcasting beacon frames.
- Client devices receive these beacon frames through automatically triggered background scans.

Idea: Exploit Beacon Frames to transport Location-based Service Data!

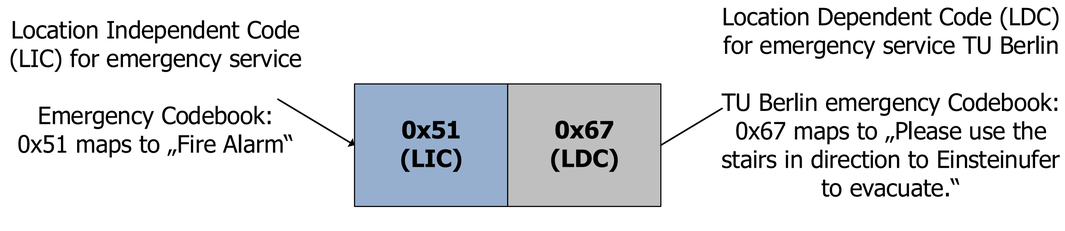


- Using Wi-Fi beacon stuffing enables to transmit location-based information from Wi-Fi AP to Wi-Fi client without the requirement of:
  - Clients to associate
  - Clients to have Internet access
  - Clients sharing their location
  - Any additional hardware or software for clients and APs!

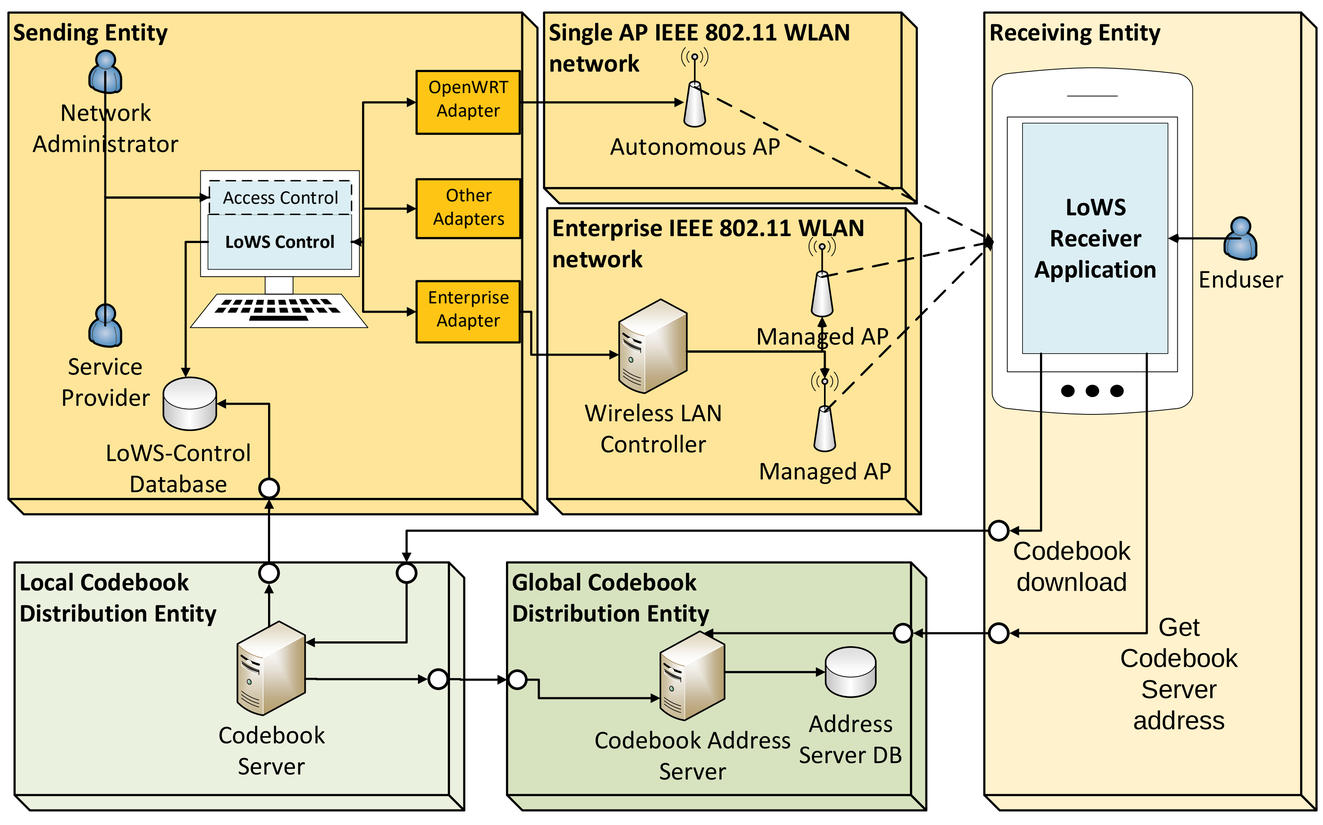
Codebook Approach:



- To keep amount of additional embedded data as small as possible, we utilize a codebook approach.
- Codebooks have to be automatically downloaded for each location or pre-installed, which is solved by the LoWS System DNS-like architecture.
- A two part coding scheme enables to decode always the most important part of the location-based service information.



Overall System Design of the Location-based Wi-Fi Service System



- LoWS System Architecture enables with its DNS-like architecture to download the location dependent codebooks on demand when entering a location the first time.
- Prevents superfluous huge global codebook.
- Small location independent codebook is pre-installed in every receiver application.

Course of the Demo:

Demo Szenario 1:
Fire emergency in a hotel

Using location-based Wi-Fi Services to:
1.) Inform people in hazardous area about emergency
2.) Give people instructions based on their location.
   -> Display evacuation plan to people in evacuation area
   -> Display „Do NOT move“ message to people when there is no possibility to evacuate.

Demo Szenario 2:
Everyday situation: subway station

Using location-based Wi-Fi Services to:
1.) Sending real-time data about departure of train. This information could be used to set alarms, e.g. 2min before departue or information can be translated in other languages.
2.) Sending information about the presence of an elevator for e.g. handicaped people, beacon signal strength can be used as navigation and orientation aid.

Demo Szenario 3:
Sending of advertisements and coupons

Using location-based Wi-Fi Services to:
1.) Inform people about the presence of a shop or restaurant
2.) Send coupon code, e.g. 10% discount by showing a screenshot of received LoWS, or include link to picture in codebook to show e.g. picture of coupon i.e. cheeseburger for free.
3.) Beacon signal strength can be used for navigation