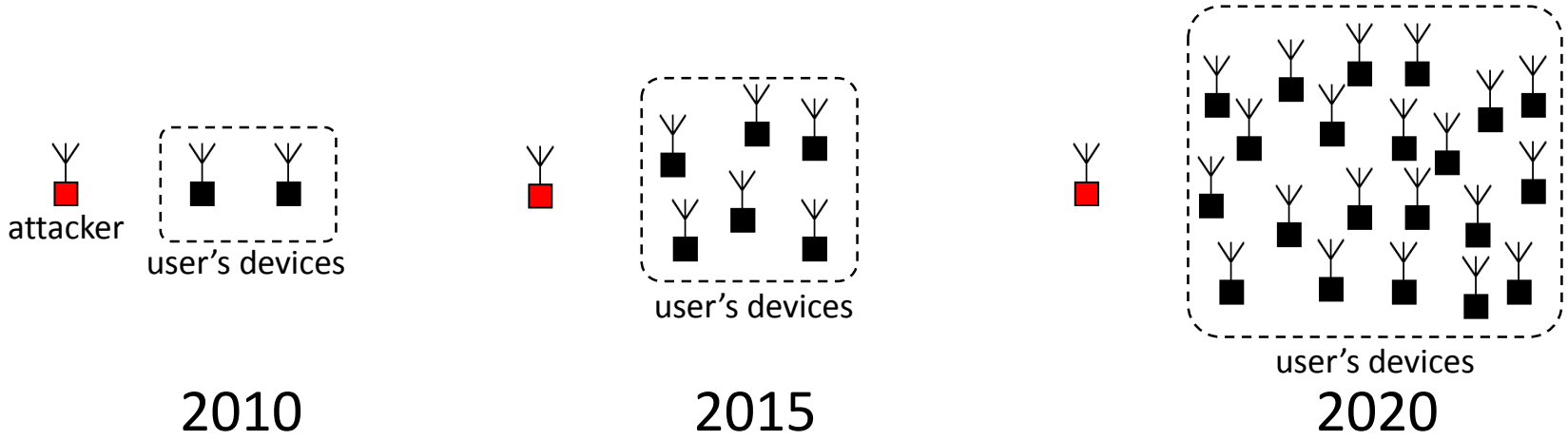
Flashing Displays

Toni Perković

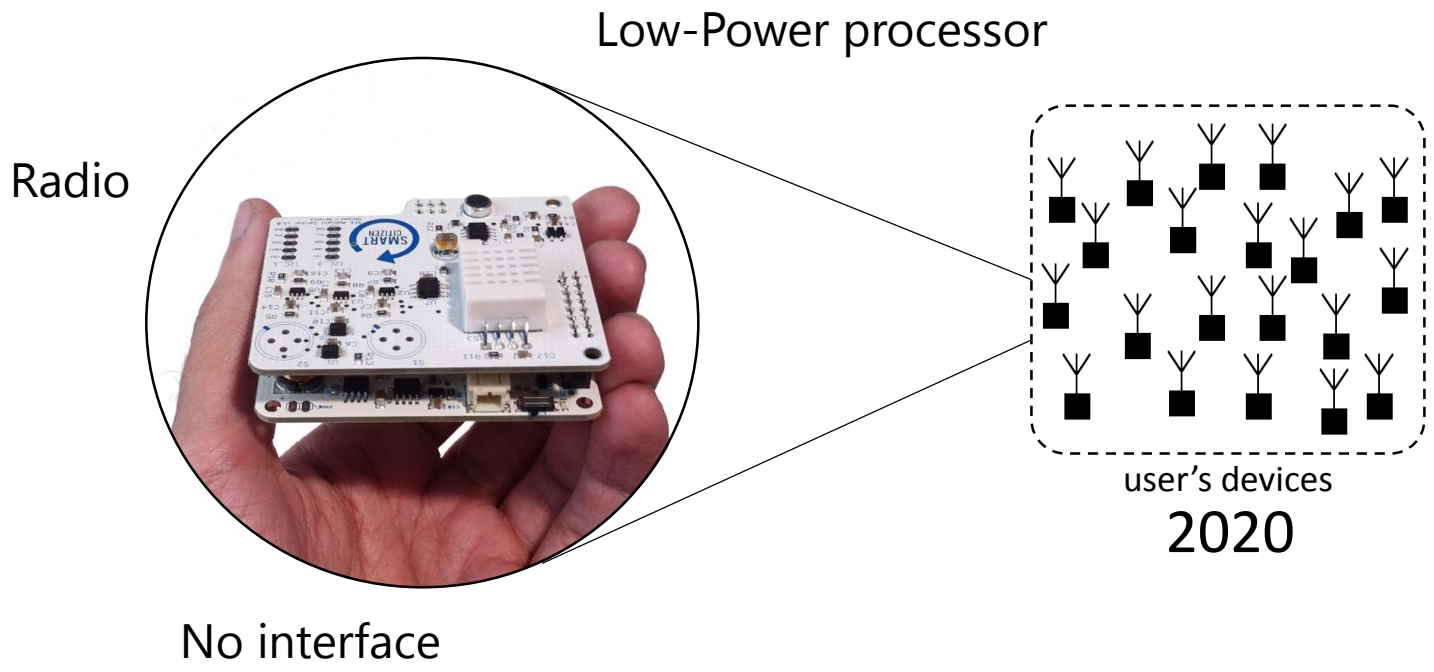
Motivacija

- Internet of Things (IoT)
  - Povezivanje objekata u inteligentne mrežne sustave
  - Predviđanja do 2020. - 50 milijardi M2M uređaja
  - Pametne kuće, pametni gradovi, zdravstvo, poljoprivreda...



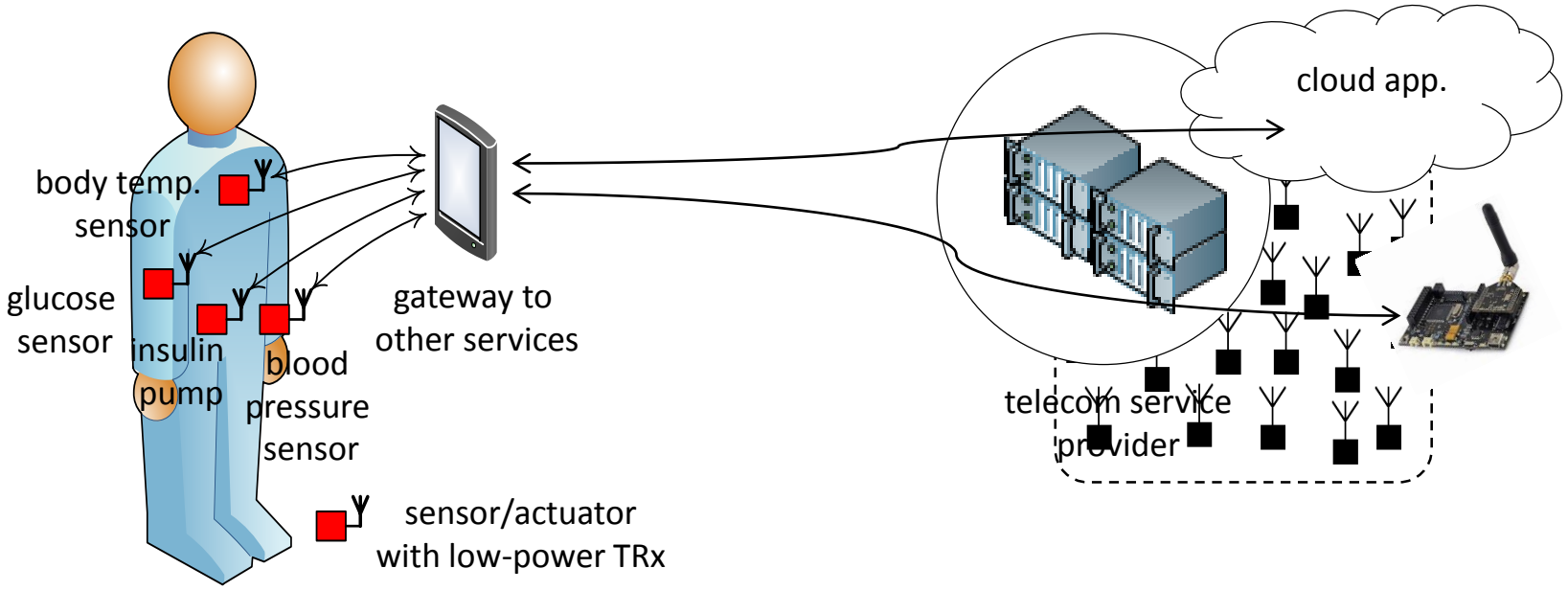
Motivacija

- Različite tehnologije/sustavi
  - Višestruko resursno ograničeni bežični uređaji
  - Primjena radio kanala - vrlo ranjiv
  - Neovisnost o autoritetu (user-centric)



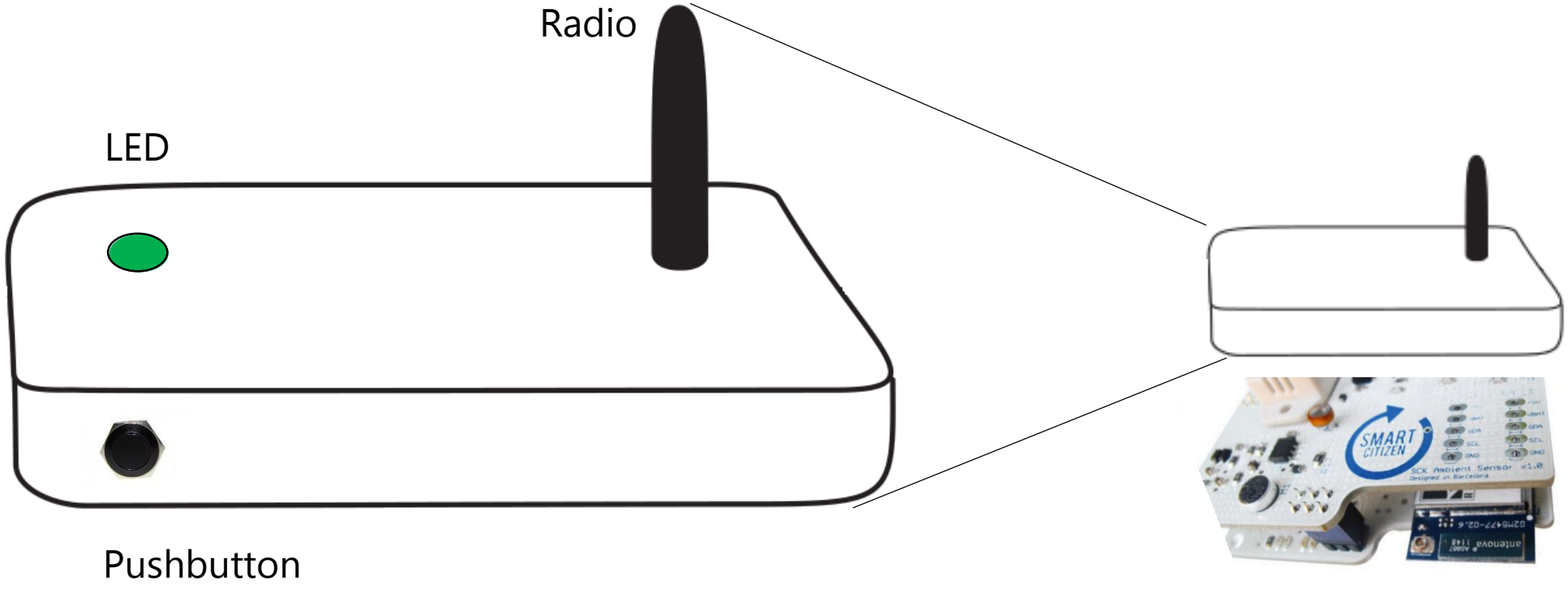
Motivacija

- IoT - preduvjeti za primjenu
  - Pouzdanost podataka, autentičnost i privatnost
- Ključni element prema sigurnoj komunikaciji
  - Kriptografski materijal (zaporke, ključevi, certifikati)
- Primjer:

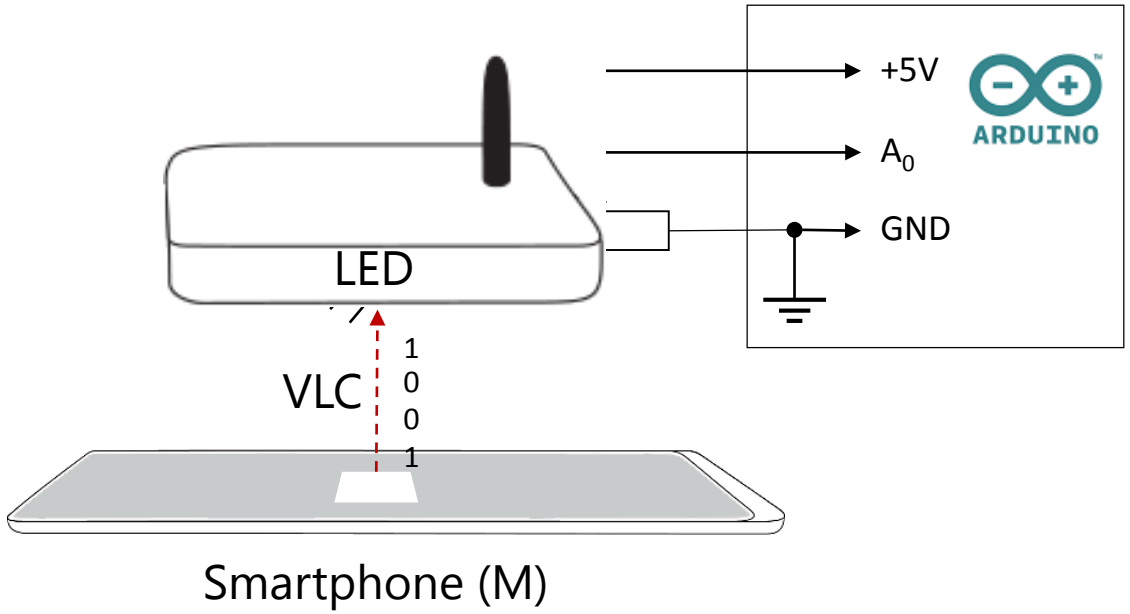


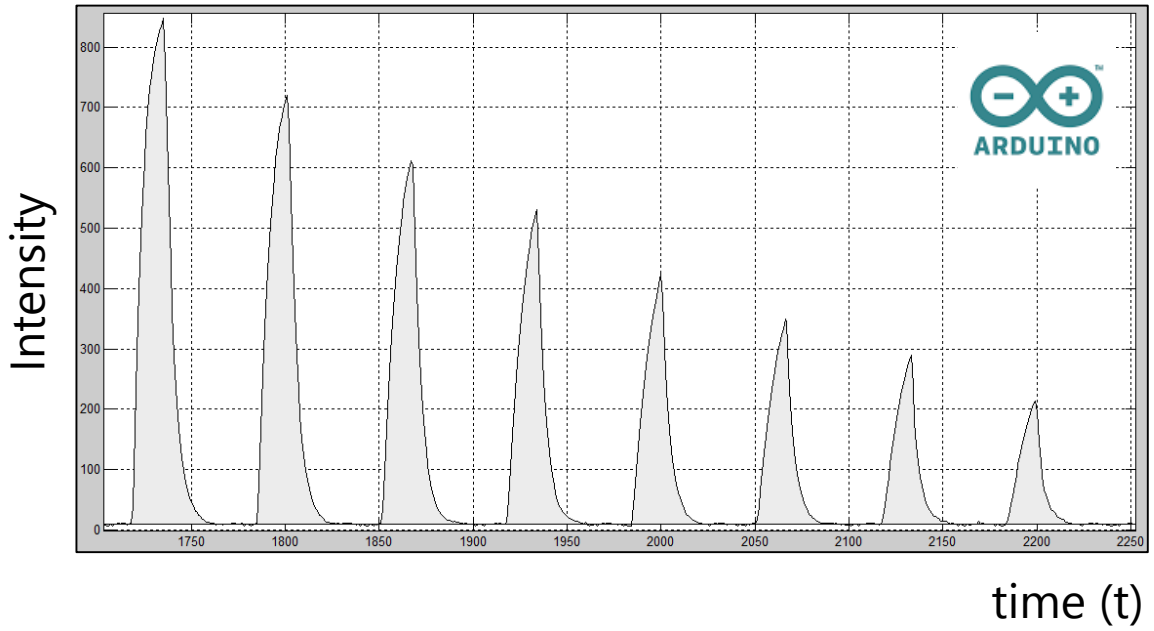
Naš cilj

- Razviti sigurne metode za inicijalizaciju bežičnih mreža osjetila/uređaja
  - Korisnički orijentirane (user-friendly)
  - Skalabilne - podržavaju razumno velik broj uređaja
  - Primjenjive na resursno ograničene uređaje – bez sučelja, zaslona, tipkovnice …

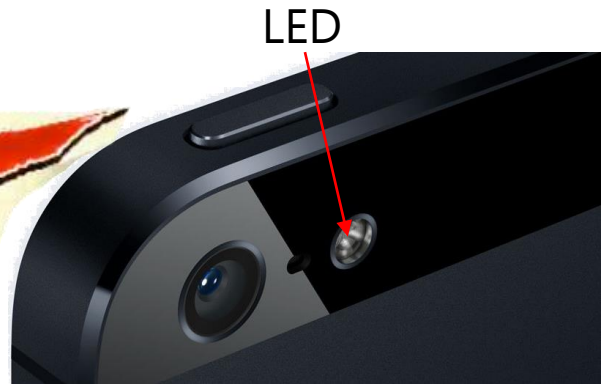


Kanal vidljive svjetlosti (VLC)





Kanal vidljive svjetlosti (VLC)



- Skalabilnost
- Ekrani su svugdje prisutni
- Nije potreban dodatan hardware

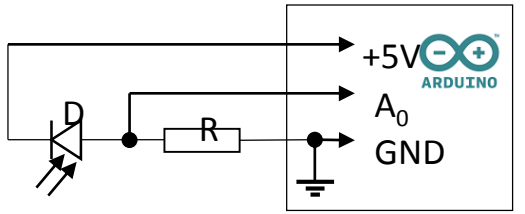
#1: Višerazinsko kodiranje - osnove

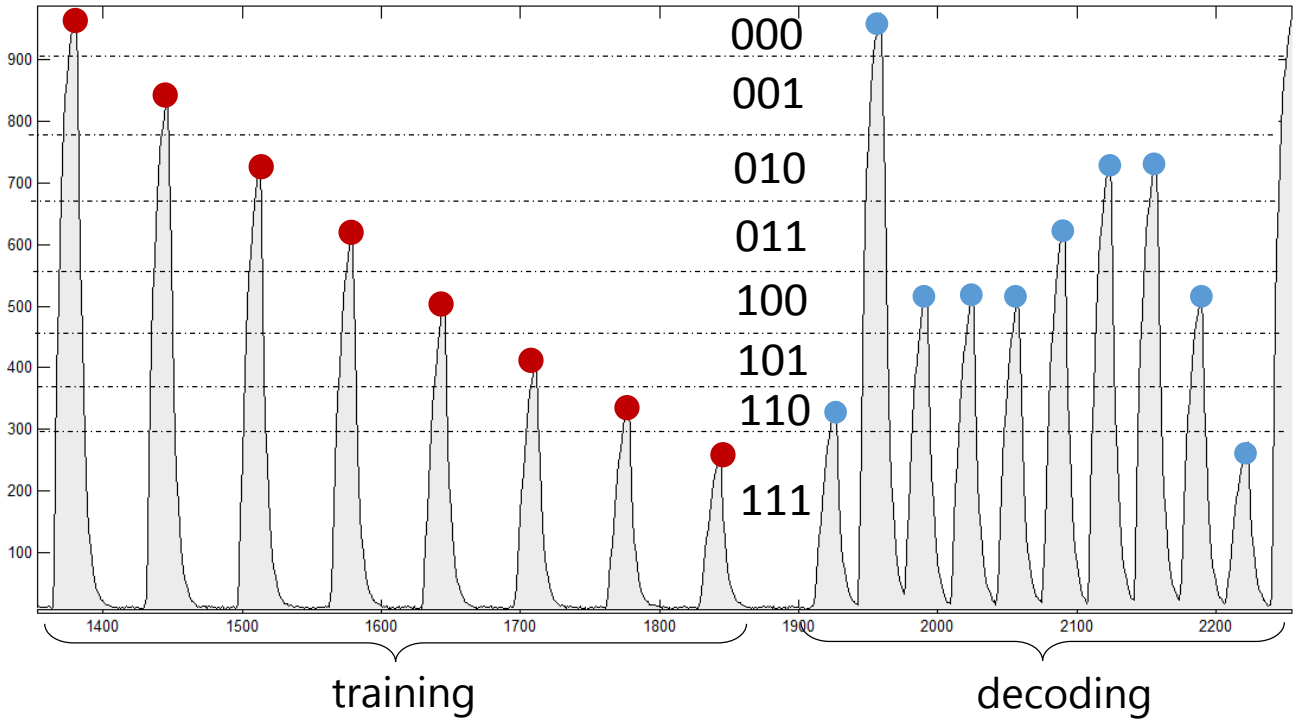
Transmitter

000	001	010
011	100	101
110	111	delimiter

Nijanse sive

Receiver

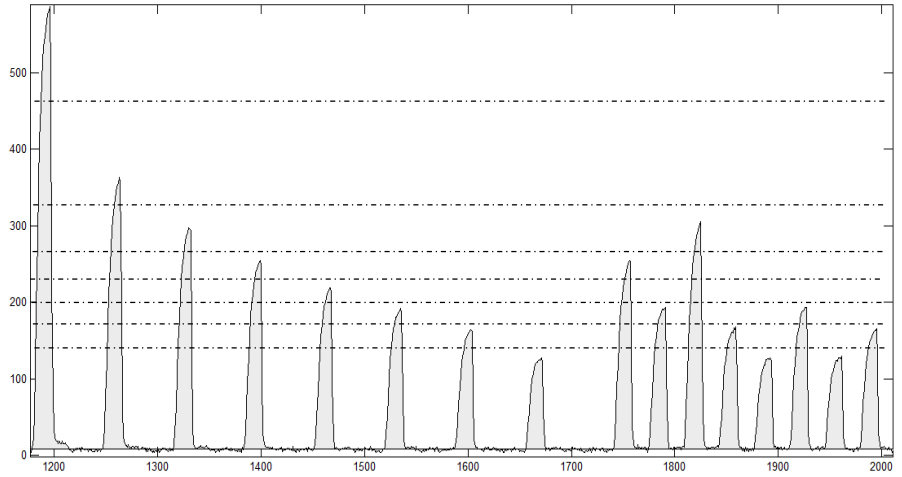




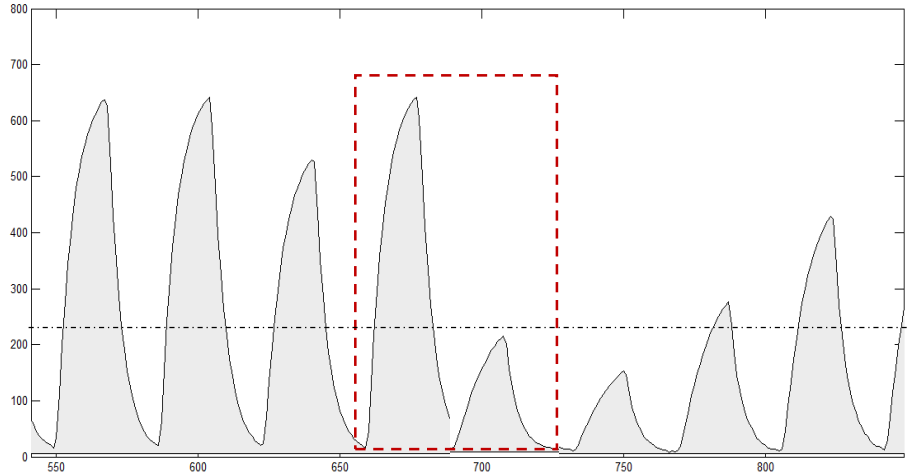
Brzina 90 bps!

#1: Višerazinsko kodiranje - izazovi

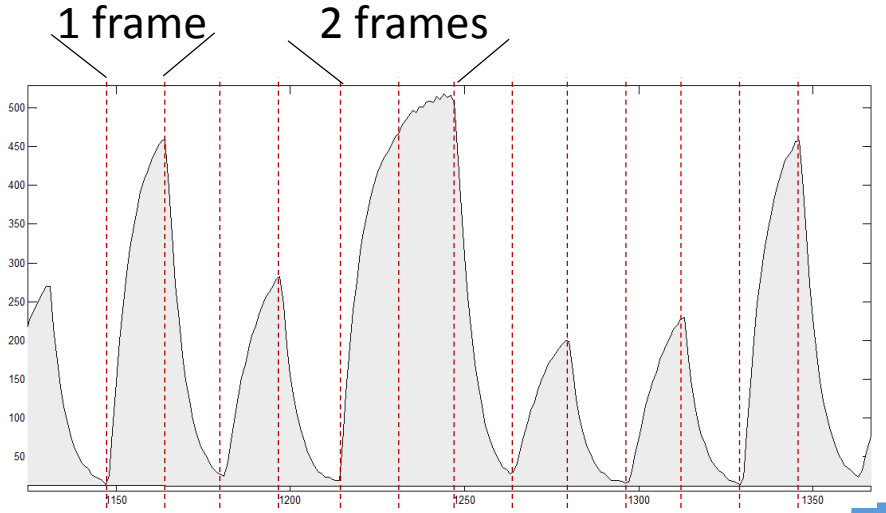
Nejednaki transmiteri



veća vj. greške

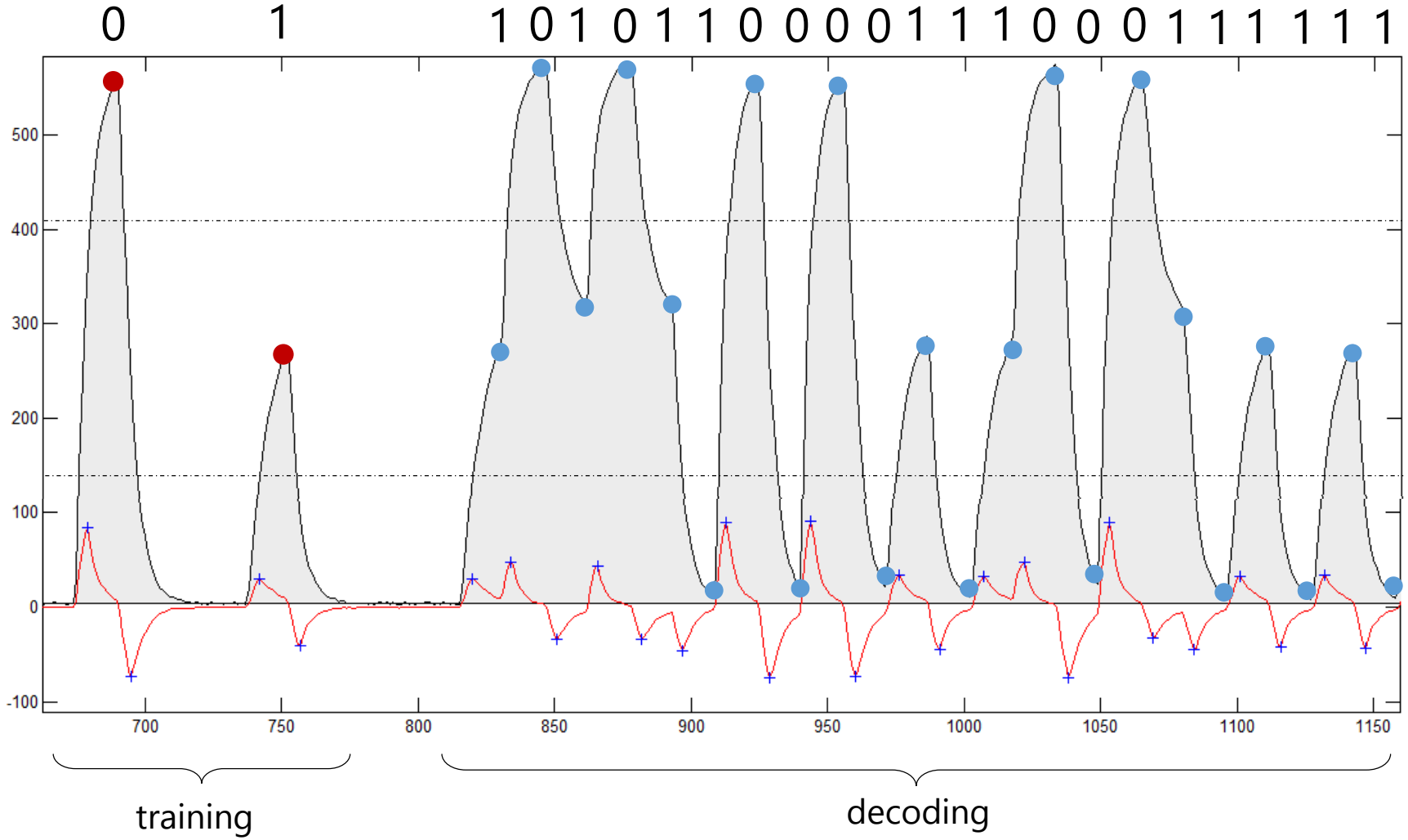


Inter-symbol interference (ISI)



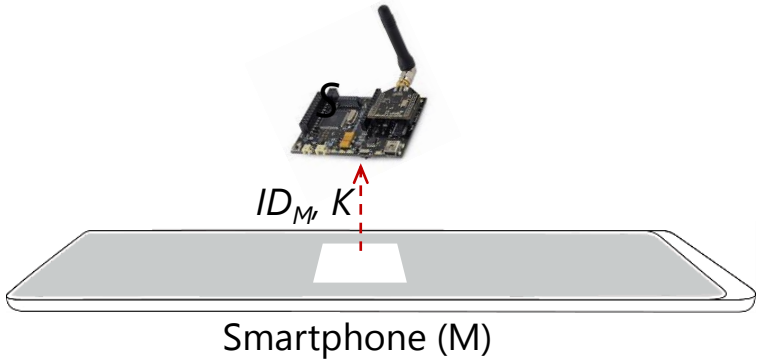
Pretek simbola

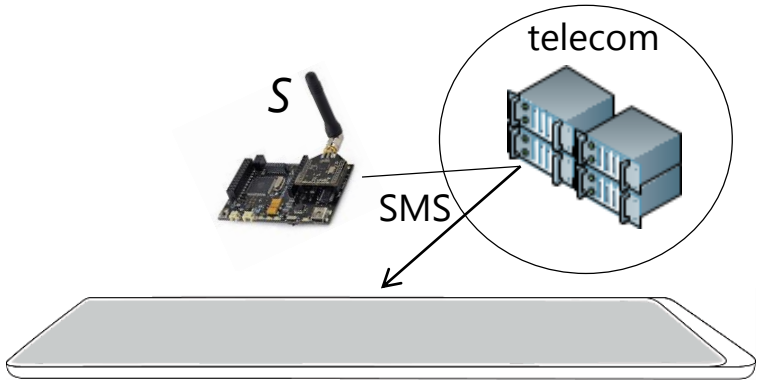
#2: Binarno-derivacijsko kodiranje

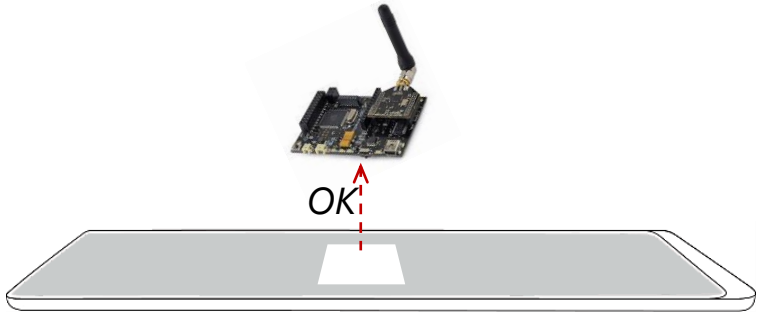


Brzina 60 bps!

Protokol: VLC + SMS (1)







Smartphone *M* Device *S*

Phase 1:

ID_M, K ⇢

Phase 2:

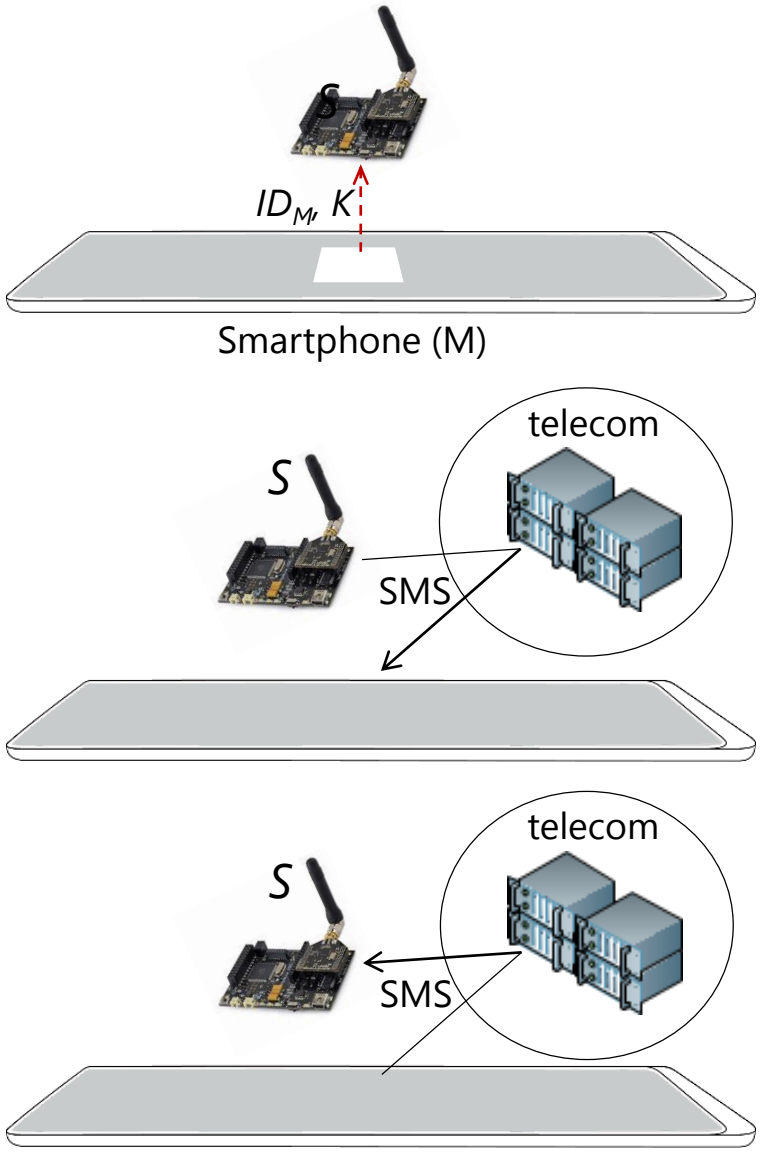
$ID_S, \{ID_M, ID_S\}_K$ ←

Verify ID_M, ID_S ← Send *SMS*

Phase 3:

OK message ⇢

Protokol: VLC + SMS (2)



Smartphone *M* Device *S*

Phase 1:

ID_M, K →

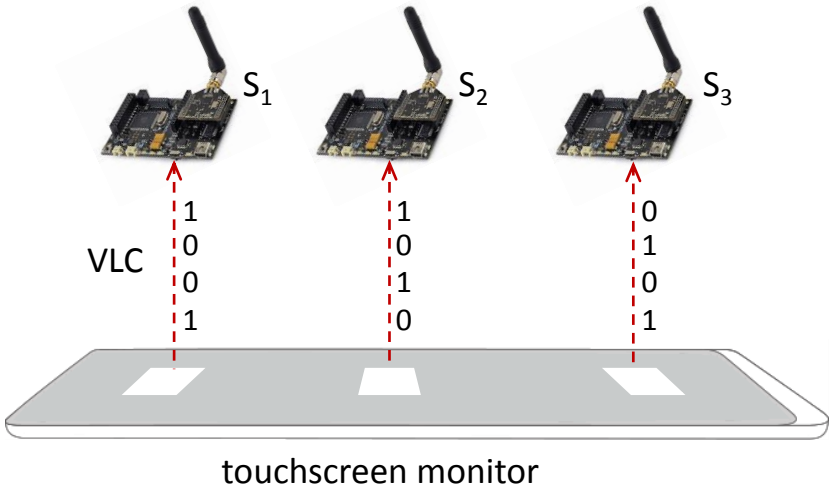
Phase 2:

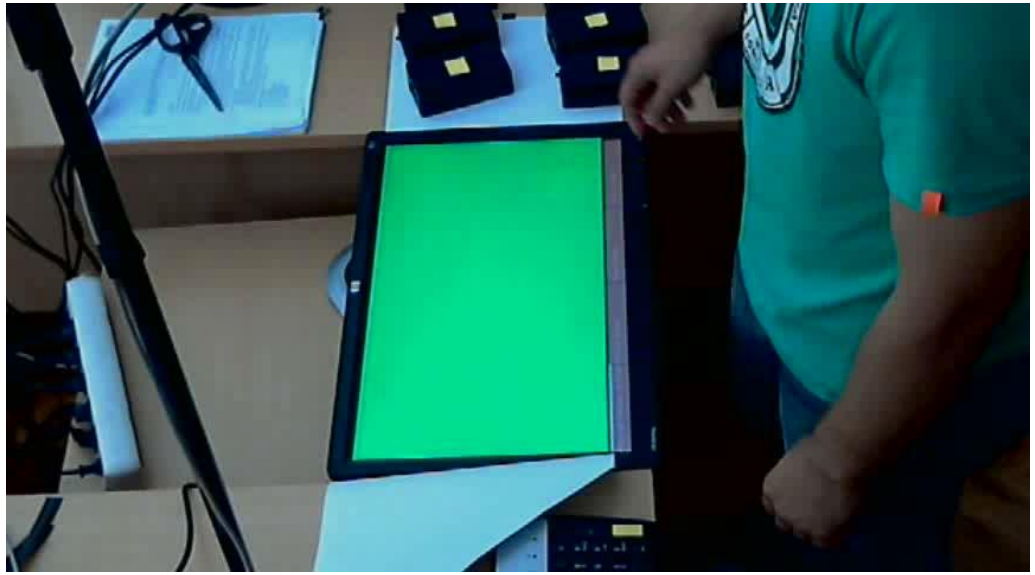
Verify ID_M, ID_S ← $ID_S, \{ID_M, ID_S\}_K$ Send *SMS*

Phase 3:

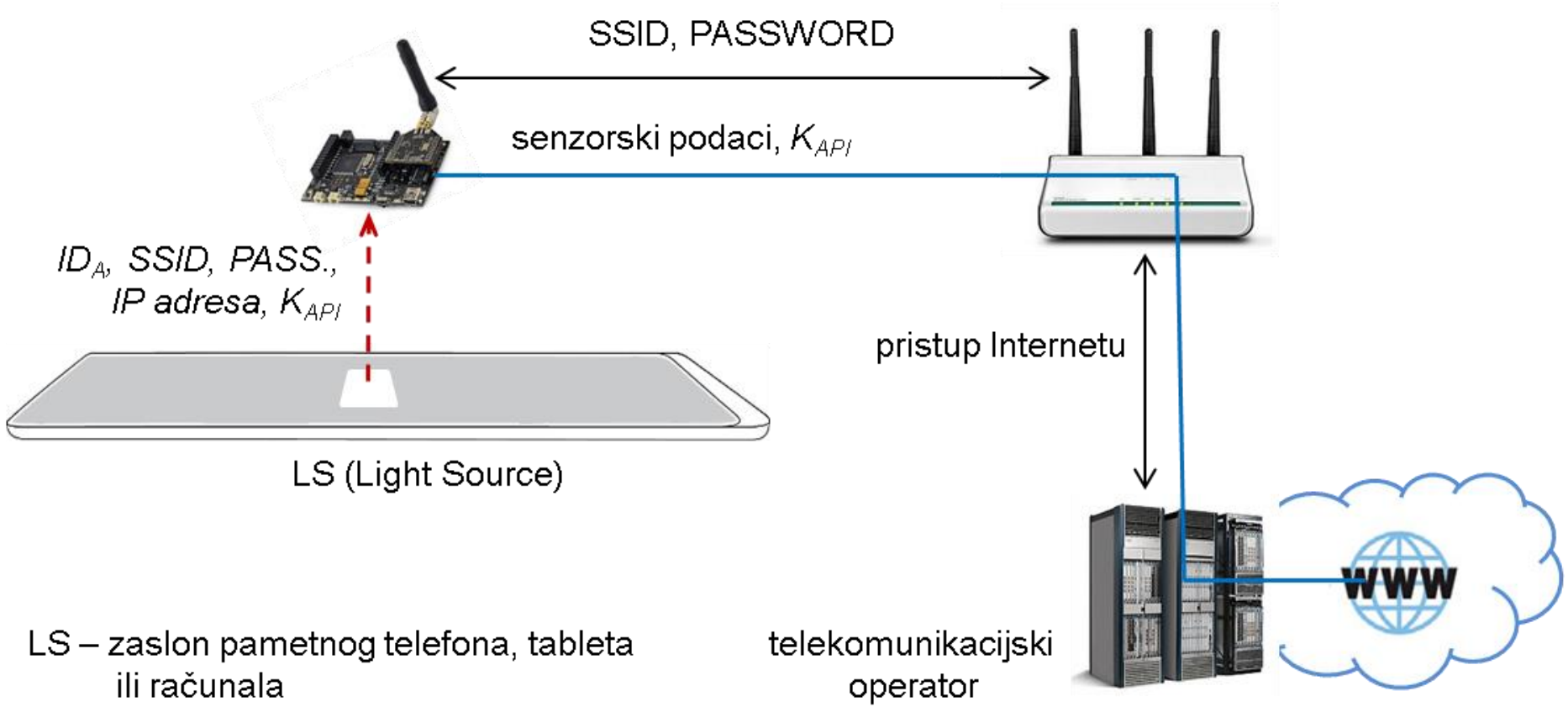
Send *SMS* → $\{ID_S, ID_M\}_K$ Verify ID_S, ID_M

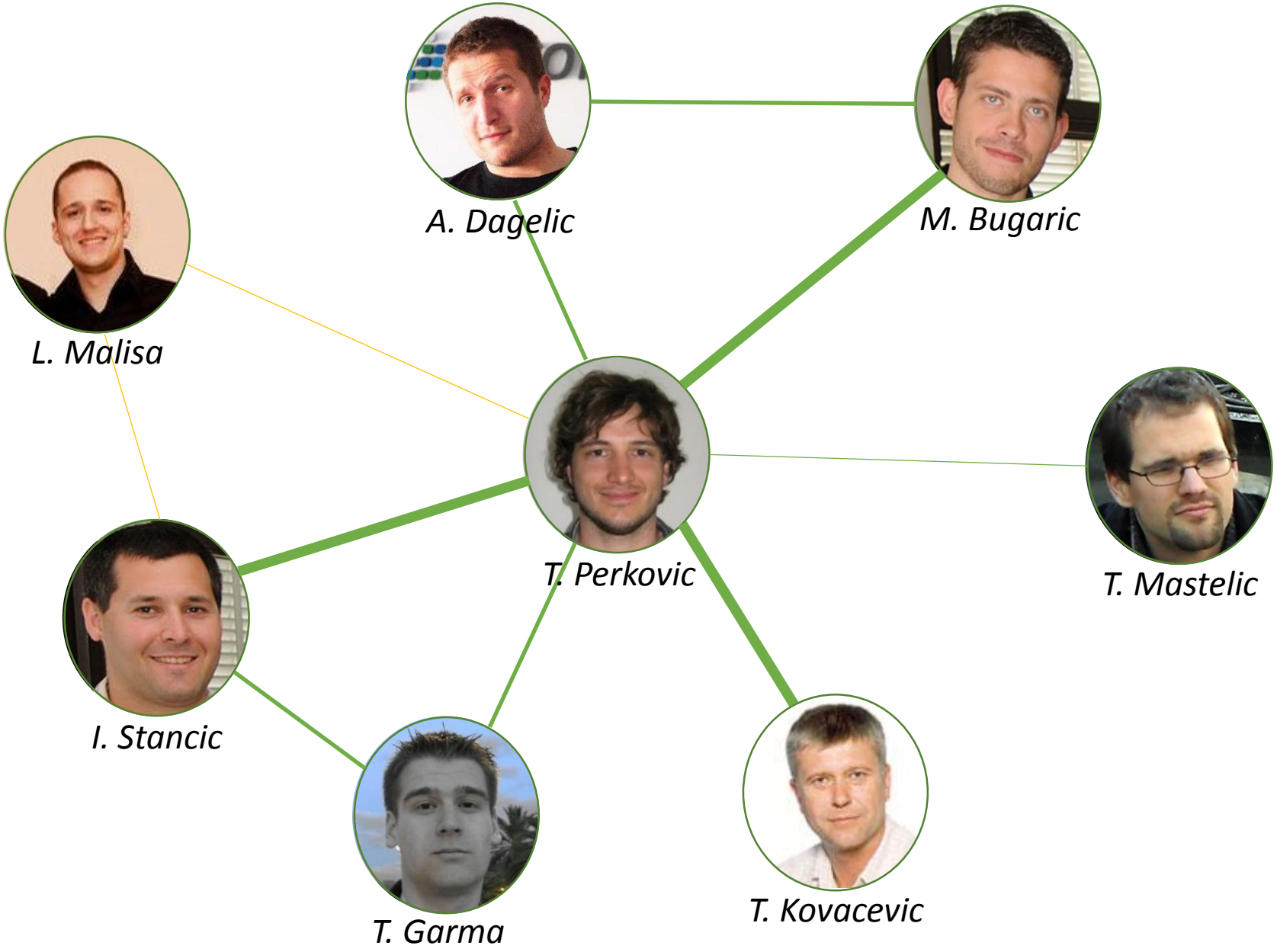
Skalabilnost predloženog rješenja





Demo


SSID, PASSWORD
senzorski podaci, K_{API}
ID_A, SSID, PASS.,
IP adresa, K_{API}
pristup Internetu
LS (Light Source)
WWW
LS – zaslon pametnog telefona, tableta ili računala
telekomunikacijski operator


A. Dagelic
M. Bugaric
L. Malisa
T. Perkovic
T. Mastelic
I. Stancic
T. Garma
T. Kovacevic

Proud of ☺ in 2014/15


M. Cagalj


T. Perkovic


M. Bugaric

Timing Attacks on Cognitive Authentication Schemes, IEEE Transactions on Information Forensics and Security, IF=2.065


M. Cagalj


T. Perkovic


M. Bugaric


S. Li

Fortune cookies and smartphones: Weakly unrelayable channels to counter relay attacks Pervasive and Mobile Computing Journal, IF=1.667


T. Perkovic


I. Stancic


T. Garma

Wake-on-a-Schedule: Energy-aware Communication in Wi-Fi Networks, Advances in Electrical and Computer Engineering, IF=0.642