RFID komunikacija

Jure Rebernik, Angela Nikodinovska, Anamarija Papež

Univerza v Ljubljani, Fakulteta za elektrotehniko

E-pošta: jr0464@student.uni-lj.si, an7632@student.uni-lj.si, ap6128@student.uni-lj.si

RFID communication

Abstract. *In this paper we have researched data exchange between RFID (Radio Frequency Identification) reader and a passive card. We were also interested in security aspect of such communication. As a transciever we have used Arduino with RC522 RFID module. With the help of ISO/IEC 14443 [2] international standard we have identified modulation and coding schemes used by the reader and the card. We successfully decoded the exchanged messages and retrieved the card's UID (Unique IDentification) number. Since the reader recognizes the card just by identifying its unique UID, we could potentially reproduce the card and in that way steal the card owner's identity.*

1 Uvod

Namen te seminarske naloge je pokazati, kako enostavno je prisluškovati izmenjavi podatkov v nekem RFID (Radio Frequency IDentification) sistemu ter kako enostavno jih lahko dekodiramo.

2 Meritve

Meritve smo opravili z osciloskopom in ne s spektralnim analizatorjem, saj želimo videti časovni potek signala. Spekter nam je tako ali tako znan; gre za ASK modulacijo pravokotnih pulzov s simbolno frekvenco $f_s = 847{,}5\ kHz$, ki se prenaša z nosilcem s frekvenco $f_c = 13{,}56\ MHz$.

Za simulacijo čitalca kartice smo zaradi enostavnosti uporabili Arduino in "shield" z imenom RC522 (slika 1).

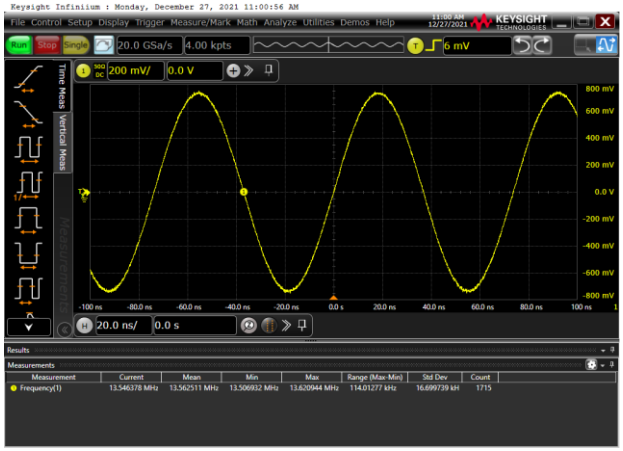
Slika 1. RC522 RFID čitalec kartic.

Za merjenje RFID komunikacije smo uporabili H sondo. RFID namreč deluje v bližnjem H polju in tu ne gre za prenos informacij preko elektromagnetnega valovanja, ampak samo preko magnetnega polja. Ko kartico približamo čitalcu, se med njima ustvari zračni transformator in preko le-tega se podatki prenesejo. Če bi uporabili anteno, bi se morali oddaljiti za 3,52m (enačba 1), da bi prešli v daljno polje in zaznavali elektromagnetno valovanje.

$$\frac{\lambda}{2\cdot\pi} = \frac{c_0}{2\cdot\pi\cdot f} = \frac{3\cdot 10^8 \frac{m}{s}}{2\cdot\pi\cdot 13{,}56 MHz} = 3{,}52m \qquad (1)$$

Na razdalji 3,52m pa ne bi več zaznali polja, saj je oddajna moč čitalca zelo majhna in njegova »antena« ni narejena za oddajanje elektromagnetnega valovanja, ampak za generiranje magnetnega polja.

H sondo približamo polju in na osciloskopu vidimo sinusoidni nosilec (slika 2).



Slika 2. Sinusoidni nosilec s frekvenco 13,56 MHz.

Čitalec periodično pošilja paketke in »posluša«, če se bo kakšna kartica odzvala (slika 3).

Slika 3. Začetni ukaz, ki ga pošilja čitalec.

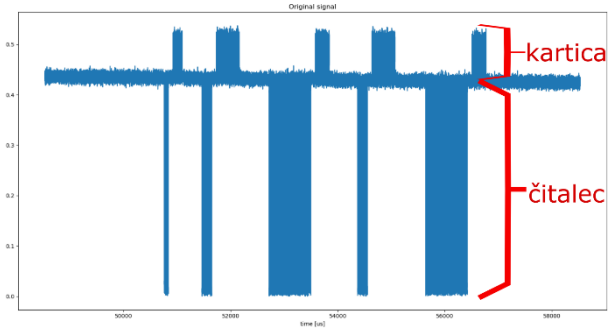
Kartica se odzove (slika 4).

Slika 4. Časovni potek komunikacije med čitalcem in kartico. Rumena krivulja je moduliran nosilec, torej surov napetostni signal iz H sonde, spodnja (oranžna) krivulja pa je amplitudna ovojnica, ki jo osciloskop sam izračuna.

Podatke, zajete z osciloskopom, smo izvozili v .csv datoteko in jih obdelali s programom, napisanem v jeziku Python.

3 Dekodiranje signala

V programu smo ločili signal (amplitudno ovojnico) na 2 dela: ukaze, ki jih kartici pošilja čitalec, in odgovore kartice (slika 5). Oba, čitalec in kartica, pošljeta 5 paketov podatkov.



Slika 5. Časovni potek komunikacije.

Da bi vsebino lahko dekodirali, smo si ogledali standard ISO/IEC 14443[2], ki opisuje dvosmerno komunikacijo med čitalcem/PCD (Proximity Coupling Device) in kartico/PICC (Proximity Integrated Circuit Card).

PICC je lahko tipa A ali B. Poglavitna razlika med njima je v uporabljenih metodah modulacije, kodiranju in protokolu komunikacije. Mi smo uporabljali kartico tipa A, zato bomo v nadaljevanju opisali le ta tip komunikacije.

3.1 Komunikacija PCD do PICC

Bitna hitrost f_b mora biti $f_c/128 \approx 106\ kbit/s$, kjer je f_c frekvenca nosilca (13,56 MHz). Kot modulacijski postopek se uporablja ASK. Za kodiranje bitov se uporablja modificirano Millerjevo kodiranje (slika 7), ki uporablja naslednje sekvence:

- zaporedje X: po pol trajanja bita se pojavlja “pavza”;
- zaporedje Y: ni modulacije skozi celotno trajanje bita;
- zaporedje Z: na začetku bita se pojavlja “pavza”.

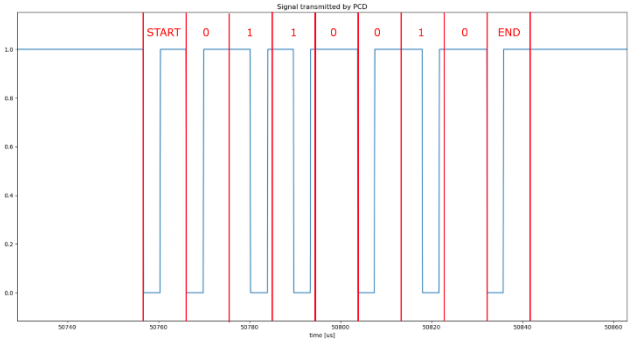
S pomočjo teh sekvenc se kodirajo naslednje informacije:

- začetek komunikacije: zaporedje Z
- logična '1' : zaporedje X
- logična '0': zaporedje Y z dvema izjemama:

i) če nastopita dve ali več zaporednih '0', se za drugo in vse nadaljnje zaporedne ničle uporablja zaporedje Z;

ii) če je prvi bit po začetku komunikacije '0', je potrebno uporabiti sekvenco Z za ta bit in za vse naslednje '0' bite;

- konec komunikacije: logična '0', ki ji sledi zaporedje Y.



Slika 7. Izsek iz signala, kjer se uporablja Millerjevo kodiranje.

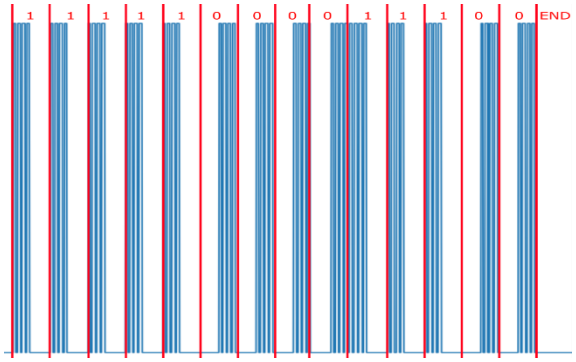
3.2 Komunikacija PICC do PCD

Tudi tukaj mora bitna hitrost f_b biti 106 kbit/s. PICC mora iz nosilca generirati podnosilec s simbolno frekvenco f_s, ki je enaka $f_c/16 \approx 847\ kHz$. Ustrezno temu je trajanje enega bita ekvivalentno 8 periodam podnosilca. Podnosilec je moduliran z OOK (On/Off Keying) modulacijo, z zaporedji:

- zaporedje D: nosilec je moduliran s podnosilcem prvo polovico trajanja bita;
- zaporedje E: nosilec je moduliran s podnosilcem drugo polovico trajanja bita;
- zaporedje F: nosilec skozi celotno periodo trajanja bita ni moduliran.

Uporablja se kodiranje Manchester (slika 8), ki je v standardu definirano na naslednji način:

- logična '1': zaporedje D
- logična '0': zaporedje E
- začetek komunikacije: zaporedje D
- konec komunikacije: zaporedje F.



Slika 8. Izsek iz signala, kjer se uporablja kodiranje Manchester.

Povejmo še nekaj o samem podnosilcu. Če pogledamo osnovni, nemodulirani signal, vidimo, da imamo pravokotne pulze s simbolno frekvenco $f_s = 847\ kHz$. Rekli pa smo, da je bitna hitrost $f_b = 106\ kHz$. To pomeni, da vsak simbol predstavlja le osmino bita. Če tak signal moduliramo, se nam frekvenčni spekter prestavi v desno, s centrom v frekvenci nosilca (13,56MHz). Okoli njega pa v na levo in desno vidimo vrhove, ki predstavljajo bitno frekvenco in simbolno frekvenco, ter njihove večkratnike.

3.3 Inicializacija in antikolizija

V standardu ISO/IEC 14443 v tretjem delu je opisana začetna faza komunikacije med PCD in PICC, katere cilj je pridobitev UID-ja. Vsak PICC ima svoj UID (Unique IDentification). V primeru, da je v magnetnem polju PCD-ja hkrati več kartic, PCD izvaja antikolizijsko zanko (Anticollision loop), s katero izbere samo eno točno določeno kartico.

Mi smo uporabljali le eno kartico, zato se antikolizijska zanka ni izvedla. Inicializacija je potekala v naslednjih korakih:

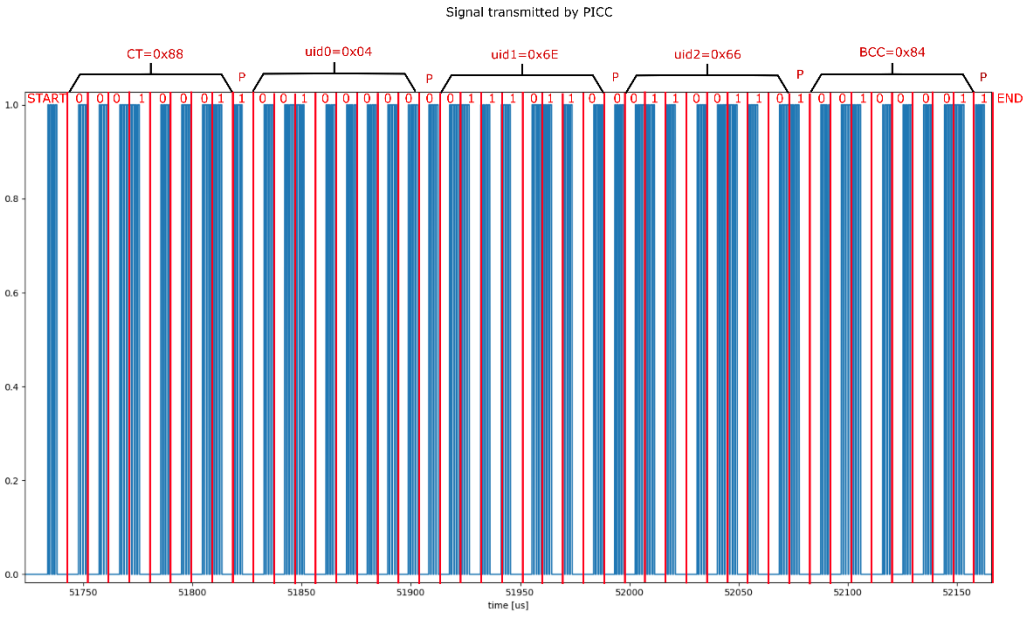
1. PCD pošlje ukaz REQA (Request Command, Type A).
2. PICC, ki je znotraj polja, odgovarja z ATQA (Answer To Request of Type A), v katerem so kodirani velikost UID-ja in preostali biti, pomembni za antikolizijo.

Velikost UID-ja določa, koliko t. i. zaporednih stopenj (CL – Cascade Level) bo potrebno, da se prenese celoten UID. Na vsaki zaporedni stopnji *n* PICC pošlje del UID-ja, ki ga označimo kot UID CLn. Maksimalno število zaporednih stopenj je tri ($3 \geq n \geq 1$).

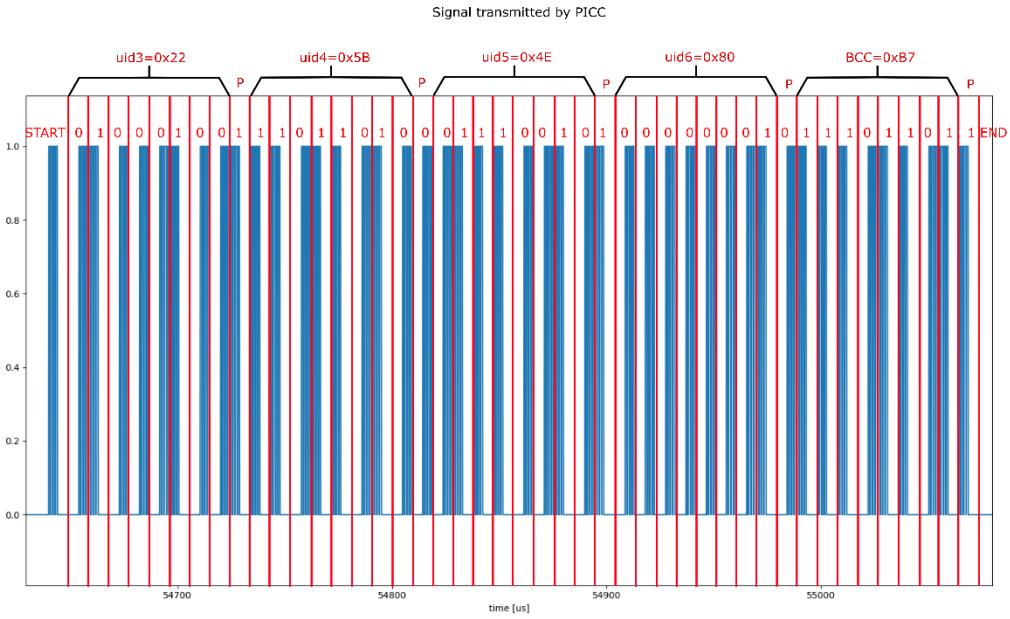
V našem primeru smo iz ATQA razbrali, da je velikost UID-ja naše kartice double oz. 7 bajtov, zato bo UID poslan v dveh delih.

3. PCD pošlje ukaz sestavljen iz bajtov SEL (Select Code) in NVB (Number of Valid Bits). V SEL je zakodirana kaskadna stopnja *n*, v tem primeru $n = 1$, NVB pa ima vrednost 0x20, kar pomeni, da je PCD-ju celoten UID CL1 še neznan.
4. PICC se odzove s svojim UID CL1 (slika).
5. PCD v NVB postavi vrednost 0x70, kar pomeni, da je bil poslan celoten UID CL1. PCD pošlje ukaz, sestavljen iz bajtov SEL, NVB, CT (Cascade Tag, '88'), UID CL1, BCC (Block Check Character, izračunan z logično operacijo XOR nad prejšnjimi 4 bajti) in dveh bajtov CRC (Cyclic Redundancy Check error detection code).
6. PICC (ki ima enak UID CL1) se odzove s SAK (Select Acknowledge). Ker PICC še ni poslal celotnega UID, je v SAK postavljen zaporedni bit.
7. PCD preveri zaporedni bit. Ker je postavljen, poveča kaskadno stopnjo *n* na 2. Odpošlje SEL in NVB z vrednostjo 0x20, kar pomeni, da še nima podatka za UID CL2.
8. PICC se odzove s svojim UID CL2 (slika 10).
9. PCD poleg drugih bajtov vrne UID CL2.
10. PICC se odzove s SAK, ki ima resetiran zaporedni bit, saj je bil PCD-ju poslan celoten UID.

Tako smo uspešno razbrali UID naše kartice, ki znaša 04 6E 66 22 5B 4E 80.



Slika 9. PICC pošlje prvi del svojega UID.



Slika 10. PICC pošlje drugi del svojega UID.

4 Zaključek

Na žalost velika večina varnostnih sistemov še vedno uporablja samo UID kodo za identifikacijo osebe. Kot smo demonstrirali v tej kratki seminarski nalogi, je s prisluškovanjem H polja v okolici RFID kartice dokaj enostavno mogoče razbrati UID kodo. Napadalec bi lahko z informacijo o UID kartico reproduciral in ukradel identiteto neke osebe.

Literatura

[1] https://lastminuteengineers.com/how-rfid-works-rc522-arduino-tutorial/

[2] https://www.iso.org/standard/73599.html

[3] https://en.wikipedia.org/wiki/ISO/IEC_14443