Bežični sistem za sigurnosnu identifikaciju

Nenad Jovičić
Katedra za Elektroniku
Elektrotehnički fakultet
Beograd, Srbija
nenad@etf.rs

Vladimir Rajović
Katedra za Elektroniku
Elektrotehnički fakultet
Beograd, Srbija
rajo@etf.rs

Milijan Ćelić
Krajina Klas doo
Banja Luka, BiH
milijanc@gmail.com

Slavko Bojić
Procontrol doo
Banja Luka, BiH
slavko.bojic@gmail.com

Sadržaj—**U radu je predstavljena realizacija sistema za identifikaciju prisustva baziranog na upotrebi bežične komunikacije. Najčešća primena sistema ovog tipa je elektronsko osiguranje kofera za prenos novca, ali to ne isključuje druge slične namene. Sistem se sastoji iz sigurnosnog kofera, prijemne jedinice unutar kofera i predajne jedinice koja se nalazi kod nekog od lica koja su u pratnji kofera. U slučaju pljačke i udaljavanja kofera od lica iz obezbeđenja kod koga se nalazi predajnik, dolazi do prekida bežične komunikacije sa prijemnikom, koji nakon toga uključuje alarmni signal. Alarmni signal se najčešće koristi za aktiviranje eksplozivne smeše koja uzrokuje ispuštanje specijalnog mastila velikom brzinom u prostor sa novcem. Na taj način obojeni novac postaje bezvredan pljačkašima, a osiguravajuće kuće pokrivaju troškove zamene novca od strane centralne banke. Akcenat u ovom radu je stavljen na realizaciju sistema i rešavanje osnovnih problema kad je u pitanju siguran bežični prenos informacija.**

Ključne reči - bežična komunikacija, kontrola pristupa

I. UVOD

Najpoznatiji proizvođač sigurnosnih sistema za skladištenje i prenos novca je švajcarska kompanija GEHRER AG [1]. Ova kompanija poseduje spektar proizvoda od kojih se većina odlikuje kvalitetnom mehaničkom zaštitom, a samo oni najsofisticiraniji imaju mogućnost rada u režimu sa daljinskom bežičnom kontrolom. Osnovna karakteristika Gehrer-ovog i sličnih rešenja je proaktivno korišćenje bežične komunikacije. Naime, bežična komunikacija se u regularnom režimu rada ne koristi. Prijemna jedinica je stalno aktivna i očekuje eventualni signal od predajne jedinice. U slučaju neovlašćenog odnošenja kofera, osoba kod koje se nalazi predajnik može da daljinski aktivira alarm, tj. sistem za bojenje novca. Bitno ograničenje ovakvog sistema je što prisustvo bilo kakvih smetnji, pa i onih namerno napravljenih, može da onemogući daljinsko aktiviranje u slučaju pljačke. Najjednostavniji primer namerno indukovane smetnje je kontinualna emisija nosioca u blizini prijemnika, što se postiže jednostavnim elektronskim napravama.

Do detaljnijih informacija o ovom i sličnim rešenjima se teško dolazi, jer proizvođači nerado odaju informacije u cilju zaštite svojih rešenja. U svakom slučaju u ovakvom sistemu najznačajnija je implementacija sigurne bežične komunikacije. Poslednjih godina istraživanja u oblasti bežičnih senzorskih mreža su veoma obimna [2]. Osim u telekomunikacijama, bežične senzorske mreže se koriste u medicini [3][4], poljoprivredi [5], industriji [6] i slično. Kako se vremenom broj korisnika deljenog medijuma povećava, sve su značajnije metode obezbeđivanja koegzistencije različitih sistema. Do sada se o sigurnosti najviše vodilo računa u industrijskim aplikacijama [7], i ideja kombinovanog vremenskog multipleksa i frekvencijskog skakanja je iskorišćena i u ovom radu.

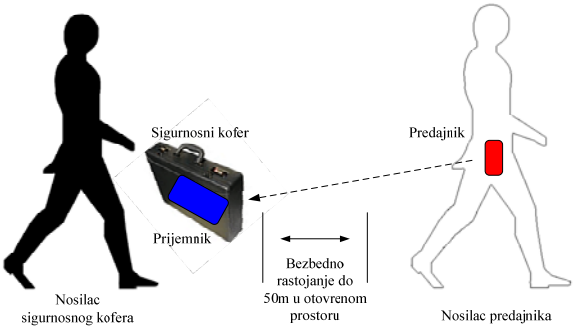
Što se tiče samih algoritama zaštite prenosa podataka, u literaturi postoji mnoštvo radova koji se bave ovom tematikom [8][9], a neke realizacije su vezane i za ovakve primene [10].

II. REALIZACIJA

A. Opis sistema

Sistem projektovan u okviru ovog projekta je izveden kao dodatna funkcionalnost na već postojeći kofer sa mehaničko-elektronskim zaključavanjem. Blok dijagram kompletnog sistema prikazan je na slici 1. Postojeći elektronski sklop u okviru sigurnosnog kofera poseduje interfejs koji omogućava povezivanje prijemne bežične jedinice. Prijemna jedinica preko nekoliko digitalnih linija obaveštava sklop kofera u kakvom je stanju komunikacija sa predajnom jedinicom. Osim veze sa elektronskim sklopom kofera, prijemna jedinica poseduje žični interfejs koji služi za početnu sinhronizaciju sa predajnom jedinicom. Žični interfejs je izveden preko DIN konektora dostupnog sa spoljnje strane kofera. Prijemna jedinica se napaja iz elektronskog sklopa kofera na koji je povezana.

Prijemna jedinica ima prijemnu antenu koja je napravljena u vidu „sloted dipol“ antene i izvedena je direktno na metanom kućištu prijemne jedinice, ili samog kofera.



Slika 1. Blok dijagram sistema.

Procedura zaključavanja kofera je sledeća: Nakon smeštanja novca u kofer, najpre se vrši mehaničko a zatim i elektronsko zaključavanje samog kofera korišćenjem odgovarajućih kodnih ključeva, i to spada u standardne metode zaštite ovakvih sistema. Potom se vrši inicijalizacija bežičnog sistema za zaštitu, povezivanjem predajnika i prijemnika žičnom vezom. Na taj način se vrši razmena identifikacionih kodova koji se koriste za zaštitu bežične komunikacije. Nakon uspostavljanja bežične zaštićene veze sa predajnikom, prijemnik signalizira elektronskom sklopu kofera da je inicijalizacija uspešno izvršena i kofer je spreman za upotrebu. U zavisnosti od konkretne realizacije, kofer može da bude opremljen različitim signalizacionim mehanizmima, uključujući i generisanje glasovnih poruka koje korisnike obaveštavaju o uspešnoj inicijalizaciji sistema, kako je i realizovano u ovom slučaju.

Nakon ove procedure sistem je spreman za transport. Po pristizanju na odredište, sekvenca otključavanja podrazumeva jednostavnu upotrebu elektronskog ključa kojim je kofer prethodno i zaključan. U fazi otključavanja ne postoji posebna procedura bežične deaktivacije sistema.

Ukoliko prilikom transporta dođe do gubitka komunikacije, prijemni uređaj daje alarmni signal koji sklop elektronike koristi za aktiviranje dimne smeše koja boji novac.

Izgled prototipa predajnika i prijemnika je prikazan na slici 2. Prijemnik je namenjen za korišćenje u postojećim koferima za prenos novca tako da je realizovan kao zaseban uređaj u aluminijumskom kućištu, sa odgovarajućim otvorima za zvučnik, konektore, izlaz dimne smeše i slično.

B. Bežična komunikacija

U koferu se nalazi prijemna jedinica povezana na elektronski sklop kofera koji se koristi za aktiviranje alarma i sistema za bojenje novca. Kod iste ili druge osobe iz pratnje pošiljke se nalazi predajna jedinica koja je u stalnoj komunikaciji sa prijemnom jedinicom u koferu. U slučaju gubitka komunikacije aktivira se alarm kofera i sistem za bojenje novca.

Veza između predajnika i prijemnika može biti u nekoliko stanja:

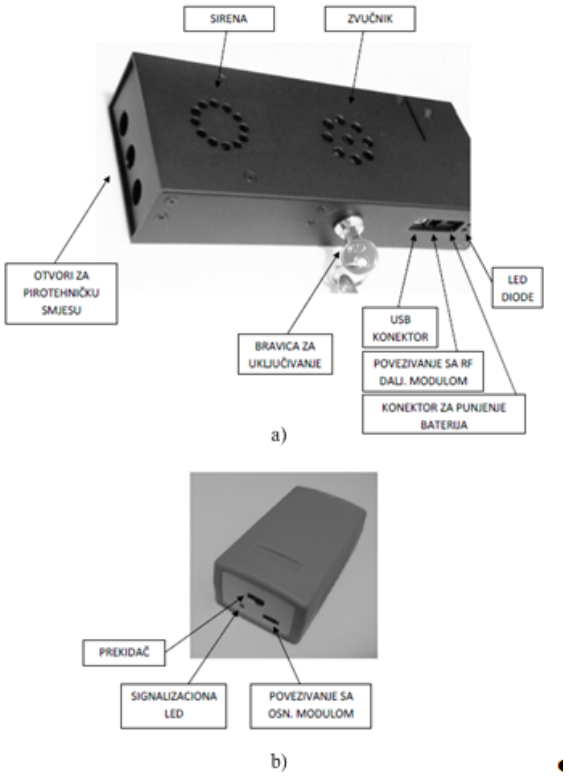
a) Link neinicijalizovan.

b) Link regularan – kontinualna komunikacija prisutna.

c) Prisutna smetnja na nekim kanalima (mogućnost lineranog jamming-a).

d) Prekid komunikacije duži od predefinisanog vremena.

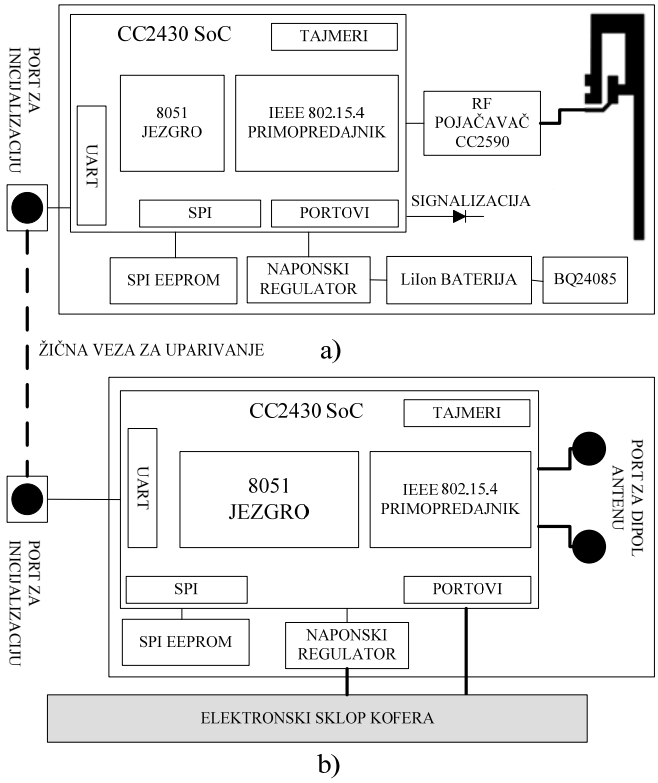
Bežična komunikacija se obavlja kroz nekoliko kanala u okviru 2.4GHz ISM opsega po standardu IEEE 802.15.4. sa maksimalnom snagom emisije od 100 mW. Komunikacija podrazumeva slanje kratkih poruka sa odgovarajućim faktorom ispunjenosti u vremenskom multipleksu takvom da je moguće da se u istom kanalu odvija komunikacija više nezavisnih uparenih sistema za prenos novca. Kolizija u okviru istog kanala se izbegava dodavanjem slučajnog odstupanja (jitter) od unapred definisanog perioda javljanja. U slučaju zagušenosti kanala, koja može biti detektovana i od strane prijemnika i od strane predajnika, vrši se frekvencijski skok na unapred definisan drugi kanal. Sekvenca skakanja je određena slučajno u vreme inicijalizacije, i po pravilu odstupa od linearne sekvence. Ovo je veoma bitno, jer se na taj način izbegava ometanje nosiocem koji vrši emisiju linerano po kanalima. Takođe, sekvenca skakanja ima dugačku periodu ponavljanja tako da se izbegava mogućnost neovlašćenog dekodiranja sekvence. Komunikacija je jednosmerna, bazirana na inkrementalnim plivajućim kodovima. Neovlašćeno ponavljanje neke od prethodnih poruka nema efekta.



Slika 2. Realizovani prototip: a) prijemna i b) predajna jedinica.

C. Hardver

Dizajn predajnika i prijemnika je baziran na mikrokontroleru CC2430 (Texas Instruments). Glavna prednost CC2430 je njegova arhitektura koja ga čini pravim sistemom na čipu (System on Chip - SoC), i u sebi sadrži jezgro bazirano na optimizovanom 8051 mikrokontroleru, veliki broj integrisanih periferija i radio primopredajnik koji podržava komunikaciju po IEEE802.15.4 standardu u 2.4GHz ISM (Industrial Scientific Medical) opsegu. Na slici 3 je prikazana blokovska šema obe komponente.



Slika 3. Blok šema hardvera.

Predajnik shodno svom osnovnom zadatku poseduje izlazni pojačavač CC2590 (Texas Instruments) koji mu obezbeđuje emisionu snagu od 20dBm i siguran domet u svim uslovima. Male dimenzije uređaja diktiraju korišćenje efikasne štampane antene „Invertovano F“, koja ima dosta homogen dijagram zračenja što je bitno za ovakve aplikacije. Predajnik je baterijski napajan iz jednoćelijske Li-Ion baterije. Punjenje baterije se vrši preko konektora koji istovremeno služi za uparivanje predajnika sa prijemnikom, a sama kontrola punjenja je prepuštena kolu BQ24085 (Texas Instruments). S obzirom da je uređaj baterijski napajan, na samom uređaju postoji prekidač kojim se uređaj isključuje ili uključuje. Da bi se osigurao rad sistema i u slučaju kada bi u toku rada došlo do namernog ili nenamernog isključivanja ili reseta predajnika, svi sinhronizacioni podaci, razmenjeni ili generisani u toku žične inicijalizacije i uparivanja predajnika i prijemnika se čuvaju u spoljašnjoj EEPROM memoriji koja se sa mikrokontrolerom povezuje preko SPI interfejsa. Žična komunikacija predajnika i prijemnika je izvedena korišćenjem serijske komunikacije implementirane pomoću integrisanih UART primopredajnika. Predajnik osim navedenih periferija poseduje i odgovarajući broj signalizacionih LED dioda.

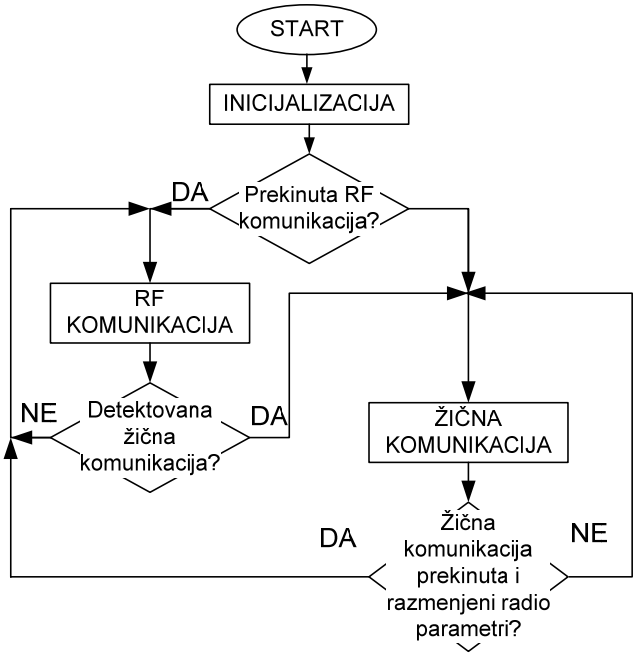
Blok šema prijemnika je prikazana na slici 3b. Po svojoj strukturi prijemnik je sličan predajniku. Iz istih sigurnosnih razloga EEPROM memorija je obavezan deo prijemnika. Osnovna razlika je u tome što prijemnik nema izlazni pojačavač, jer nikada ne radi na predaji, a malošumni pojačavač (LNA) u kolu CC2590 neznatno pojačava ulazni signal. Druga bitna razlika je kolo za prilagođenje, jer se u slučaju predajnika kao antena koristi deo kućišta samog prijemnika, i to u formi dipol antene sa prorezom.

D. Softver

Na slici 4 prikazan je algoritam izvršavanja glavnog programa, koji je isti na predajnom i na prijemom uređaju.

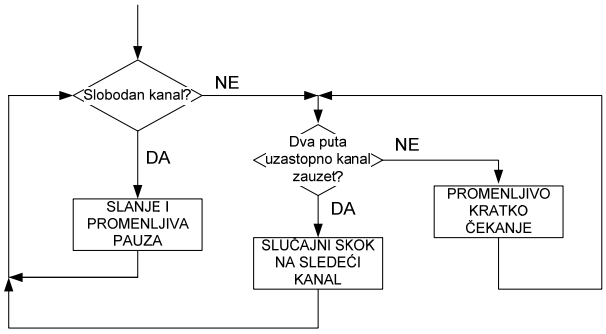
Na osnovu flega koji se čuva u EEPROM memoriji određuje se da li je do prekida napajanja ili resetovanja uređaja došlo za vreme aktivne radio komunikacije i, ukoliko jeste, komunikacija se nastavlja sa parametrima koji se restauriraju iz EEPROM memorije.

Za vreme radio komunikacije istovremeno se testira da li su preko žične veze povezani predajnik i prijemnik i, ukoliko jesu, prelazi se u režim rada u kome se dok su god povezani žičnom vezom razmenjuju uvek novi parametri za sledeću radio komunikaciju. Ovaj režim se napušta ukoliko dođe do prekida žične komunikacije nakon što su ispravno razmenjeni parametri za radio komunikaciju. Ukoliko dođe do prekida žične komunikacije a parametri za radio komunikaciju nisu ispravno razmenjeni, ne inicira se radio komunikacija, već se čeka na ponovno uspostavljanje žične komunikacije.



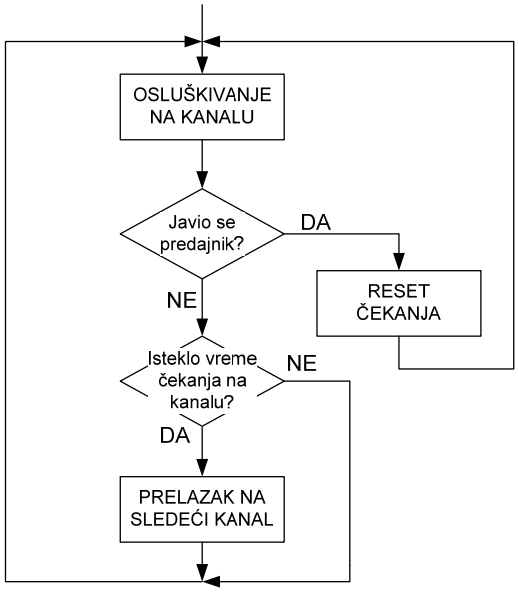
Slika 4. Algoritam izvršavanja glavnog programa.

Na slici 5 prikazan je algoritam rada predajnog uređaja za vreme radio komunikacije. Ukoliko je tekući kanal raspoloživ za emitovanje, predajni uređaj emituje poruku za prijemni uređaj. Nakon emitovanja čeka se promenljivo (u opsegu od 25 %) vreme pre nego što se ponovo emituje. Ukoliko je tekući kanal zauzet provera se na istom kanalu vrši još jednom nakon relativno kratkog promenljivog čekanja. Ukoliko je dva puta uzastopce tekući kanal bio zauzet skače se na sledeći kanal po slučajnom izboru i ponavlja se procedura.



Slika 5. Algoritam rada predajnog uređaja tokom bežične komunikacije.

Na slici 6 prikazan je algoritam rada prijemnog uređaja za vreme radio komunikacije. Ukoliko na trenutnom kanalu unapred predefinisano vreme nema emitovanja predajnog uređaja skače se na sledeći kanal i procedura ponavlja ispočetka. Elektronskom sklopu kofera se preko digitalnih linija šalju informacije o stanju bežične komunikacije tj. o tome da li je predajni uređaj u opsegu prijemnika, kao i da li je prisutan ometač. Na osnovu ovih informacija elektronski sklop kofera odlučuje da li bi trebalo aktivirati uslov alarma.



Slika 6. Algoritam rada prijemnog uređaja tokom bežične komunikacije.

III. TESTIRANJE

Za potrebe testiranja u sistem je povezano deset parova uređaja server/klijent. I serveri i klijenti su povezani na računar preko jedinstvene USB veze, pomoću koje je računaru signaliziran status veze svakog pojedinačnog para server/klijent, kao i broj kanala na kome se nalazi svaki od uređaja.

Potom je u sistem uveden i uskopojasni linearni ometač kontrolisan preko računara, i eksperiment je ponovljen. Sistem je pokazao pouzdan rad u svim testovima.

ZAHVALNICA

Projekat je rađen pod pokroviteljstvom kompanije Procontrol doo iz Banja Luke, Republika Srpska, i projekta Ministarstva prosvete nauke i tehnološkog razvoja Republike Srbije broj TR32043.

Autori se zahvaljuju akademiku Prof. dr. Antoniju Đorđeviću, profesoru Elektrotehničkog fakulteta Univerziteta u Beogradu, na savetima i pomoći koje im je pružio prilikom projektovanja sistema.

LITERATURA

[1] www.gehrer.com (pristupano januara 2013)

[2] K. Akkaya and M. Younis: "A survey on routing protocols for wireless sensor networks", Ad Hoc Networks, Volume 3, Issue 3, pp. 325-349, May 2005.

[3] N. Jovičić, L. Saranovac, and D. Popović; „Wireless distributed functional electrical stimulation system", Journal of Neuroengineering and Rehabilitation, Volume 9, Issue 54, August 2012.

[4] J. Y. Khan, M. R. Yuce, G. Bulger, and B. Harding, „Wireless body area network (WBAN) design techniques and performance evaluation", J Med Syst, Volume 36, Issue 3, pp. 1441-1457, June 2012.

[5] T. Kalaivani, "A survey on Zigbee based wireless sensor networks in agriculture", The 3rd International Conference on Trends in Information Sciences and Computing, 8-9 Dec. 2011, Salem, India , pp. 85 – 89.

[6] K. S. Low, "Wireless Sensor Networks for Industrial Environments", International Conference on Computational Intelligence for Modelling, Control and Automation and International Conference on Intelligent Agents, Web Technologies and Internet Commerce, 28-30 Nov. 2005, Intelligent Systems Centre, Nanyang Technology University, Volume 2, pp. 271 – 276.

[7] J. Song, S. Han, A. K. Mok, D. Chen, M. Lucas, M. Nixon, and W. Pratt, "WirelessHART: Applying wireless technology in real-time industrial process control", IEEE Real-Time and Embedded Technology and Applications Symposium, 22-24 April 2008, Saint Louis, Missouri, pp. 377 – 386.

[8] Y. Hu, Y. Zhang, and B. Sun, "Design of RKE system based on KEELOQ encryption technology", Workshop on Fault Diagnosis and Tolerance in Cryptography, 7-8 November 2009, Shanghai, China, Volume 1, pp. 324 – 327.

[9] C. Paar, T. Eisenbarth, M. Kasper, T. Kasper, and A. Moradi, "KeeLoq and side-channel analysis— Evolution of an attack", Workshop on Fault Diagnosis and Tolerance in Cryptography, 6-6 Sept. 2009, Lausanne, Switzerland, pp. 65 – 69.

[10] A. Moradi and T. Kasper, "A new remote keyless entry system resistant to power analysis attacks", The 7th International Conference on Information, Communications and Signal Processing Macau, China, December 8-10 Dec. 2009, pp. 1 – 6.

ABSTRACT

A realization of a system for identification of presence based on wireless communication is presented in the paper. The most often application of systems of the kind is electronic security of cash transport suitcases, but other applications are possible as well. The system consists of security suitcase, receiver unit within the suitcase, and transmitter unit with one of the suitcase escort. In a case of robbery and displacement of the suitcase from the escort carrying the transmitter unit a disruption to the wireless communication between the two units occurs, and an alarm signal is generated within the suitcase. The signal is in most cases used for activation of an explosive mixture causing fast expansion of a special ink in the space where cash is stored. The colored cash has no value for the robbers, and insurance companies cover the expenditures for cash reimbursement at the central bank authority. The system realization and the approach to the fundamental problems concerning secure wireless data transmission are addressed in the paper.

A WIRELESS SYSTEM FOR SECURITY IDENTIFICATION

Nenad Jovičić, Vladimir Rajović, Milijan Ćelić, Slavko Bojić