Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 621.31
DOI: https://doi.org/10.24867/28BE17Micic

PAMETNE BEŽIČNE KOMUNIKACIONE TEHNOLOGIJE U SISTEMU ELEKTRIČNOG VOZILA

SMART WIRELESS COMMUNICATION TECHNOLOGIES IN ELECTRIC VEHICLE SYSTEM

Ana Mićić, Vladimir Popović, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *Ovaj rad istražuje integraciju Ultra-Wideband (UWB), Near Field Communication (NFC), i Bluetooth tehnologije unutar automobilskog okruženja koristeći IEEE 802.15 standard, posebno implementiran u CoSmA tehnologijama. Rad istražuje praktične primene i posledice proučavanja inkorporacije ovih bežičnih komunikacionih protokola u vozilu. Naglašavajući specifičnu impelemtaciju unutar CoSmA okvira, studija istražuje kako ova integracija poboljšava sigurnost, povezanost i pametne funkcije mobilnosti u automobilima, doprinoseći razvoju inteligentnih sistema za transport.*

Ključne reči: *komunikacioni protokoli, UWB, CoSmA, digitalni ključ;*

Abstract – *This paper examines the integration of Ultra-Wideband (UWB), Near Field Communication (NFC), and Bluetooth technologies within the automotive context, utilizing the IEEE 802.15 standard, particularly implemented in CoSmA technology. The research investigates the practical applications and implications of incorporating these wireless communication protocols in vehicles. Emphasizing the specific implementation within the CoSmA framework, the study explores how this integration enhances security, connectivity, and smart mobility features in automobiles, contributing to the advancement of intelligent transportation systems.*

Keywords: *communication protocols, UWB, CoSmA, digital Key;*

1. UVOD

U savremenom društvu, postizanje besprekorne povezanosti i efikasne komunikacije između uređaja postalo je ključno za uspeh različitih tehnoloških aplikacija. Sa stalnim napretkom bežičnih komunikacionih tehnologija, istraživači i inženjeri suočavaju se s izazovom pronalaženja optimalnih rešenja koja zadovoljavaju zahteve brze, pouzdane i sigurne komunikacije.
U tom kontekstu, protokoli kao što su *Ultra-Wideband*, *Bluetooth* i *Near Field Communication* se izdvajaju kao ključni akteri u digitalnom ekosistemu. *UWB*, s svojom sposobnošću slanja podataka širokim frekvencijskim opsegom, otvara vrata za visoko precizne i brze prenose podataka, čime se pruža izuzetna osnova za raznovrsne primene, od lokalizacije do bežične povezanosti visoke propusnosti [1].
S druge strane, *Bluetooth*, dugogodišnji lider u bežičnoj tehnologiji, nastavlja evoluirati kako bi zadovoljio potrebe povezivanja uređaja u različitim scenarijima, od pametnih telefona do pametnih kuća [2].
Sa svoje strane, *NFC* pruža jednostavno i intuitivno povezivanje na kratkim udaljenostima, čime se često koristi u raznim aplikacijama poput mobilnog plaćanja i deljenja informacija [3].
CoSmA (*engl. Continental Digital Access*) tehnologija se oslanja na sinergiju ovih bežičnih protokola kako bi omogućila koordiniranu komunikaciju između vozila, infrastrukture i drugih povezanih uređaja u saobraćaju [4].

2. KOMUNIKACIONI PROTOKOLI

U nastavku se daje pregled bežičnih komunikacionih protokola koji se koriste za implementaciju digitalnog ključa vozila integrisanih u *CoSmA* tehnologije.

2.1 UWB tehnologija

UWB je bežična komunikaciona tehnologija koja koristi širokopojasne signale sa frekvencijskim opsegom iznad 1 GHz. Za razliku od tradicionalnih komunikacionih sistema koji koriste sinusoidalne nosioce, *UWB* se oslanja na uske pulsirajuće signale nesinusoidnog oblika na nivou nanosekunde za prenos podataka.

Jedna od glavnih prednosti *UWB* tehnologije je niska složenost sistema, kao i niska spektralna gustina snage signala pri odašiljanju. Takođe, *UWB* je manje osjetljiv na probleme poput gubitka signala, omogućava visoku preciznost pozicioniranja i ima veliku sposobnost prodiranja kroz prepreke.

S obzirom na čestu pojavu krađe automobila uz pomoć prenosa signala, mnogi razvojni inženjeri razmatraju koji bežični interfejs može rešiti ovaj problem. Standard *IEEE 802.15.4-2020* je ažurirao fizički sloj (*PHY*) i *MAC (engl. Media Access Control)* sloj tehnologije za visoko precizne, sigurne primene merenja rastojanja.

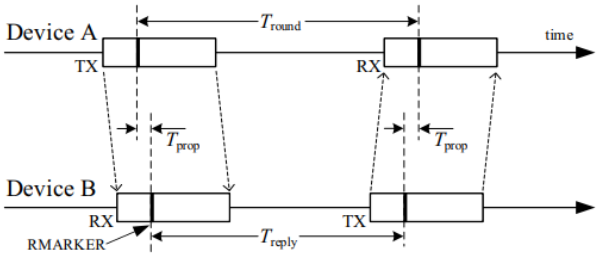
HRP UWB sistem za merenje rastojanja se zasniva na ToF (*engl. Time of Flight)* i AoA (*engl. Angle of Arrival)* merenjima kako bi obezbedio pouzdane i čvrste vremenske oznake merenja za precizno merenje udaljenosti i smera između uređaja [1].

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Vladimir Popović, doc.

Delovi procesa nazivaju se:

- *Inicijator*: Uređaj sposoban za određivanje rastojanja - koji započinje razmenu za određivanje rastojanja slanjem prvog okvira za određivanje rastojanja
- *Odgovor*: Uređaj sposoban za određivanje rastojanja - koji reaguje na inicijaciju za određivanje rastojanja putem

SS-TWR (*engl. single-sided two-way ranging)* obuhvata merenje vremena kašnjenja u oba smera za jednu poruku od jednog uređaja do drugog, s tim što drugi uređaj šalje odgovor nazad prvom. Funkcioniše kao što je prikazano na 0, gde uređaj A pokreće razmenu, a uređaj B odgovara da bi je završio. T_{prop} označava vreme propagacije tj. vreme koje signalu treba da putuje od jednog mesta do drugog, oznake za određivanje rastojanja *RMARKER*-a (*engl. ranging marker*) između uređaja.



Slika 1. Opis mehanizma za merenje rastojanja

Svaki uređaj precizno meri vremena slanja i prijema poruka, pa može izračunati vremena T_{round} i T_{reply} jednostavnim oduzimanjem. Na osnovu toga, rezultirajuće vreme leta *ToF* može se proceniti prema sledećoj jednačini.

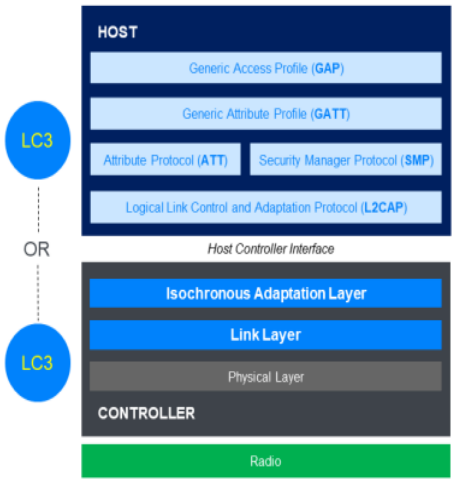
$$\hat{T}_{prop} = \frac{1}{2} \cdot (T_{round} - T_{reply}) \qquad (1)$$

2.2 Bluetooth bežični protokol

Bluetooth Low Energy prvi put se pojavila u verziji 4.0 *Bluetooth Core Specification*. Ova varijanta podržava različite topologije komunikacije, uključujući režim emitovanja, gde jedan uređaj može prenositi podatke neograničenom broju prijemnika istovremeno.

Takođe, *Bluetooth Low Energy* je osnova za *Bluetooth mesh* mreže, koje omogućavaju stvaranje mreža sa desetinama hiljada uređaja, omogućavajući svakom uređaju da komunicira sa bilo kojim drugim uređajem u mreži. *Bluetooth Low Energy*, sa svojom ekonomičnom infrastrukturom niske potrošnje energije i svojom širokom dostupnošću u pametnim telefonima, postao je važan alat za proizvođače automobila.

Na primer, *BLE* se može koristiti kao alternativa tradicionalnim *LIN (engl. Local Interconnect Network)* i *CAN (engl. Controller area network)* mrežama, zamenjujući teške kablove bežičnom povezanošću. U hibridnim i potpuno električnim vozilima, *BLE* se može koristiti za slanje podataka o temperaturi i naponu iz baterijskih paketa glavnom računaru vozila, kao deo sistema upravljanja baterijom. *Bluetooth LE* stek sastoji se od nekoliko slojeva i funkcionalnih modula, prikazano na slici 2. Ovi delovi steka su raspoređeni u okviru dva glavna arhitektonska bloka poznata kao domaćin (*engl. host*) i kontroler (*engl. controller*), a standardni logički interfejs definiše način na koji ove dve komponente mogu komunicirati. Domaćin je često nešto poput operativnog sistema, a kontroler je često sistem na čipu.



Slika 2. Opis Bluetooth LE Stack mehanizma

2.3 NFC komunikacioni protokol

Near Field Communication (*NFC*) je bežična komunikaciona tehnologija koja radi na radio talasima sa osnovnom frekvencijom od 13,56 MHz, sa tipičnim dometom do 2 cm i brzinom prenosa podataka od 46 kbit/s do 1,7 Mbit/s. NFC je tehnologija u usponu razvijena na osnovu RFID-a (*engl. Radio-frequency identification – RFID)* na način da se sastoji od interfejsa i protokola koji se zasnivaju na RFID-u. Veza između *NFC* i induktivnog sprezanja ima ključnu ulogu u strukturi bežične komunikacije koja se koristi u različitim kontekstima, posebno u aplikacijama gde je važna blizina uređaja.

Ova tehnika se oslanja na princip induktivnog sprezanja, gde se magnetna polja generišu u blizini dva provodnička kalema – jednog u inicijatoru i drugog u ciljnom uređaju (uređaju za slušanje). U osnovi, *NFC* koristi sličan princip kao transformatori, gde se magnetno polje jednog kalema koristi za indukovanje napona u drugom kalemu, omogućavajući prenos energije i podataka.

Ova komunikacija može biti aktivna, pasivna ili kombinacija oba, pri čemu *NFC* radi korišćenjem magnetskog sprezanja između uređaja. Uređaj koji može generisati svoje sopstveno radio-frekventno polje naziva se aktivni uređaj, dok se uređaj koji za prenos podataka koristi induktivno sprezanje naziva pasivnim uređajem.

3. COSMA TEHNOLOGIJA

Povećanje ponude pristupnih uređaja došlo je s razvojem *Key-as-a-Service (KaaS)*, sistemom koji se temelji na cloud tehnologiji, kao i sa *Continental Digital Access (CoSmA). CoSmA* je digitalno rešenje za pristup vozilu koje se koristi putem pametnog telefona.

Bezbednost sistema za pristup vozilu zavisi od nekoliko faktora, uključujući karakteristike fizičkog sloja za bezbedno određivanje opsega, kriptografske bezbednosti

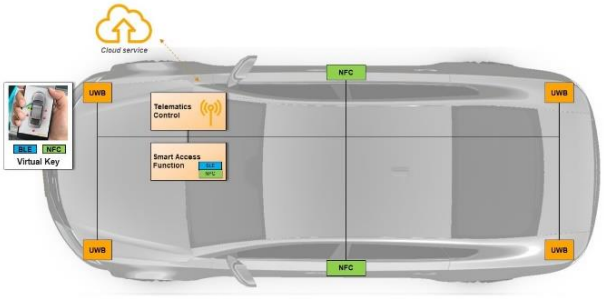
u softverskom steku i hardversku arhitekturu. Ključno je kako se ovi faktori kombinuju kako bi se efikasno odbranili od zlonamernih napada na nivou mreže ili uređaja. Postoji nekoliko načina kojima se ugrožava bezbednost sistema beskontaktnog ulaska [4]:

- *Relay* ili *man-in-the-middle* napadi, gde hakeri presreću radio talase automobila i proširuju njihov domet. Postavljaju drugi uređaj pored ključa kako bi preneli prošireni signal. To aktivira ključ, koji zatim šalje signal za otključavanje automobila. Analogni bežični signal obmanjuje vozilo da vlasnik stoji pored njega.
- Hakovanje dijagnostičkog porta na vozilu za pristup informacijama o šiframa ključa automobila - lopov može programirati novi ključ koji će pokrenuti automobil.
- Ometanje sistema - tehnika blokiranja signala koji dolazi sa ključa. Korisnik misli da je automobil zaključan, ali signal zapravo nije stigao do vozila. Lopov može otvoriti vozilo i nastaviti sa krađom

Na osnovu karakteristika različitih komunikacionih protokola u upotrebi za pristup vozilima, *UWB* je pokazao impresivne performanse za rešavanje trenutnih bezbednosnih problema.

Arhitektura obično obuhvata nekoliko komponenti i funkcionalnosti, opisano na slici 3:

- Elektronska kontrolna jedinica: Srce *CoSmA* sistema predstavlja softver koji efikasno upravlja različitim uređajima i funkcijama.
- Pametni telefoni: Ovlašćeni uređaji opremljeni *UWB* čipovima ili modulima deluju kao digitalni ključevi.
- Telematska kontrolna jedinica (TCU): U automobilskoj industriji je ugrađeni sistem na vozilu koji bežično povezuje vozilo sa uslugama u *cloud*-u ili drugim vozilima putem *V2X* standarda preko mobilne mreže.
- BLE/UWB primopredajni moduli: Predstavljaju neophodne elemente u okviru *Smart Access* sistema. Njihova uloga jeste omogućavanje komunikacije sa pametnim uređajem. Pozicioniranjem *BLE*/*UWB* satelita na strateškim mestima unutar vozila, sistem stiče sposobnost lociranja pametnog uređaja unutar i izvan vozila.
- NFC čitači:Uobičajeno je da se *NFC* antena integriše u ručku vrata ili A/B stub vozila.
- Usluge backend-a: *CoSmA* obično povezuje sa uslugama pozadine koje pružaju proizvođač originalne opreme. Ove usluge upravljaju upravljanjem ključevima, procesima autorizacije i autentifikacije.



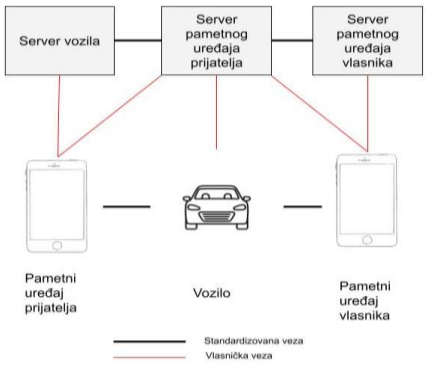
Slika 3. Arhitektura pametnog sistema pristupa [4]

4. OPIS PROTOTIPA SISTEMA ZA IMPLEMENTACIJU KONCEPTA COSMA

Sistem pristupa vozilu putem pametnog telefona (*CoSmA*), koristi pametni telefon kompatibilan sa *UWB*-om koji je programiran da funkcioniše kao ključ. Virtuelni ključ predstavlja ključnu komponentu sistema jer sadrži autorizaciju za pristup određenom vozilu. Pristup je moguć samo nakon uspešne autentifikacije putem upravljanja pravima na *cloud* sistemu. Stoga, unutar vozila su raspoređena najviše četiri UWB i četiri kombinovana *UWB* i *Bluetooth Low Energy* primopredajna modula. Sistem ih koristi kako bi locirao ovlašćeni pametni telefon putem *UWB*-a. Kada se autorizovani virtuelni ključ detektuje, sistem omogućava otključavanje vozila i pokretanje motora.

4.1 CCC Digitalni ključ

CCC Digital Key označava digitalni ključ koji je deo ekosistema *Car Connectivity Consortium* (CCC), [5]. To je tehnologija koja omogućava mobilnim uređajima da čuvaju, autentifikuju i dele digitalne ključeve za vozila na siguran način, čak i kada je baterija pametnog telefona slaba. *CCC Digital Key* je standardizovan kako bi bio kompatibilan sa različitim proizvođačima vozila i tipovima operativnih sistema, nudeći siguran i jednostavan način pristupa vozilima. Digitalni ključ omogućava potrošačima da lako i pouzdano koriste svoje mobilne uređaje, bez obzira na proizvođača ili tip operativnog sistema, kako bi pristupili vozilima. Pored snažnih mogućnosti i praktičnosti, nudi unapređenu sigurnost i zaštitu privatnosti.



Slika 4. Ekosistem Digitalnog ključa

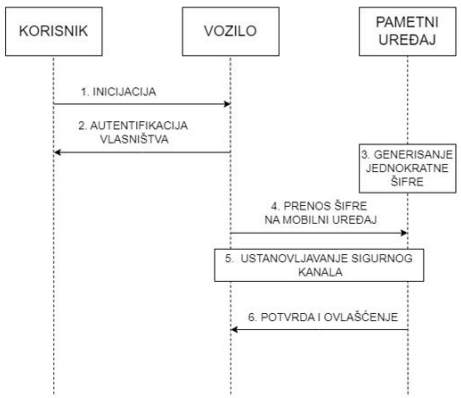
Ekosistem CCC digitalnog ključa sastoji se od:

- Vozila;
- Servera proizvođača vozila;
- Mobilnih uređaja;
- Servera mobilnih uređaja;

4.2 Uparivanje vlasnika

Vlasnik mora dokazati posedovanje vozila (metod zavisi od proizvođača automobila) i može pokrenuti proces uparivanja u aplikaciji proizvođača automobila koristeći *email* link primljen od proizvođača automobila ili iz menija vozila. U svim slučajevima, vlasnik mora predstaviti tajnu jednokratnu šifru za uparivanje *iPhone*-u, koja se koristi za generisanje sigurnog kanala uparivanja koristeći

SPAKE2+ protokol sa *NIST P-256* krivom [5]. Prilikom korišćenja aplikacije ili *email* linka, šifra se automatski prenosi na iPhone, gde se mora ručno uneti prilikom pokretanja uparivanja sa vozilom, slika 5.



Slika 5. Blok dijagram algoritma procesa uparivanja vlasnika

Standard Car Connectivity Consortium (CCC) za uparivanje vlasnika obično obuhvata sledeće faze:

1. *Inicijacija:* Vlasnik vozila pokreće proces uparivanja vlasnika, često putem aplikacije proizvođača ili specifične opcije u meniju vozila.
2. *Autentikacija vlasništva:* Korak gde se proverava ovlašćenje ili vlasništvo nad vozilom. Verifikuje da osoba koja pokreće proces uparivanja ima prava da upari mobilni uređaj sa vozilom.
3. *Generisanje jednokratne šifre za uparivanje:* Generiše se tajna jednokratna šifra za uparivanje. Ova šifra je ključni element koji se koristi za uspostavljanje sigurne veze između mobilnog uređaja i vozila.
4. *Prenos šifre na mobilni uređaj*: Generisana jednokratna šifra za uparivanje se bezbedno prenosi na mobilni uređaj.
5. *Ustanovljavanje sigurnog kanala:* Korišćenjem određenih sigurnosnih protokola definisanih CCC standardima, kao što je SPAKE2+ , mobilni uređaj i vozilo uspostavljaju siguran i enkriptovan komunikacioni kanal. Ovaj kanal osigurava poverljivost tokom interakcija.
6. *Potvrda i ovlašćenje:* Kada se uspešno uspostavi siguran kanal, vozilo potvrđuje i ovlašćuje mobilni uređaj kao 'uređaj vlasnika'. Ovo ovlašćenje daje uparenom mobilnom uređaju potpunu kontrolu i ovlašćenje nad funkcijama.

6. ZAKLJUČAK

U ovom radu detaljno su istraženi protokoli *UWB, BLE* i *NFC*, analizirajući njihove karakteristike, prednosti i primene. Poseban fokus je usmeren ka integraciji ovih tehnologija u okviru *CoSmA*, istražujući načine kako ova integracija transformiše automobilsku industriju. Protokol *UWB*, sa svojom sposobnošću preciznog određivanja raspona i visokog stepena propusnosti, izdvaja se kao ključni igrač u oblastima poput lokalizacije, praćenja i brze bežične povezanosti.

Integracija ovih tehnologija omogućila je precizno praćenje vozila, personalizovano povezivanje i sigurnu identifikaciju, stvarajući tako sveobuhvatan sistem koji ide iznad tradicionalnih granica automobilske sigurnosti. Ovo je posebno važno u kontekstu smanjenja krađe automobila, gde kombinacija lokacijskih informacija iz *UWB*-a, personalizovane veze putem *Bluetooth*-a i identifikacije putem *NFC*-a stvara složen sistem odbrane.

7. LITERATURA

[1] 802.15.4z-2020 - IEEE Standard for Low-Rate Wireless Networks, Amendment 1: Enhanced Ultra Widebandv(UWB) Physical Layers (PHYs) and Associated Ranging Techniques, June 2020.

[2] The Bluetooth® Low Energy Primer, Document Version: 1.1.0, January 2023.

[3] Naser Hossein Motlagh, Near Field Communication (NFC) - A technical Overview, Master´s thesis for the degree of Master of Science in Technology, Vaasa, 28th of May 2012.

[4] Access Systems for Security and Convenience, preuzeto sa https://conti-engineering.com/

[5] Car Connectivity Consortium Digital Key Release 3, Version 0.2.6, 2021.

Kratka biografija:

Ana Mićić rođena je u Valjevu, 1996. godine. Diplomirala na Fakultetu tehničkih nauka u Novom Sadu 2020. Godine iz oblasti Elektrotehnike i računarstva – Energetska elektronika i elekrične mašine

Vladimir Popović rođen je u Somboru 1990. god. Doktorsku disertaciju na Fakultetu tehničkih nauka iz naučne oblasti Elektrotehnike i računarstva –odbranio je 2020. god, i u zvanju je docenta na Fakultetu tehničkih nauka. Oblast interesovanja su regulacija elektromotornih pogona i digitalna kontrola sistema automatskog upravljanja.