Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 621.39
DOI: https://doi.org/10.24867/15BE26Gojic

ARHITEKTURA I BEZBJEDNOSNI ZAHTJEVI 5G MOBILNIH MREŽA

ARCHITECTURE AND SECURITY REQUIREMENTS OF 5G MOBILE NETWORKS

Jovan Gojić, Željen Trpovski, Dejan Nemec, *Fakultet tehničkih nauka, Novi Sad*

Oblast – TELEKOMUNIKACIONI SISTEMI

Kratak sadržaj – *U radu su opisane dvije ključne tehnologije koje se koriste u arhitekturi 5G sistema, a to su: softversko definisano umrežavanje (SDN) i virtualizacija mrežnih funkcija (NFV). Pored toga, prikazani su konkretni primjeri ugrožavanja bezbjednosti usluge, kao i bezbjednosni mehanizmi koji će omogućiti da korisnik pristupa uslugama bez rizika od gubitka autentičnosti, povjerljivosti, dostupnosti usluge i integriteta.*

Ključne riječi: *softversko definisano umrežavanje (SDN), virtualizacija mrežnih funkcija (NFV), 5G mobilna mreža*

Abstract – *The paper presents two key technologies used in the architecture of fifth generation networks, namely: software defined networking (SDN) and virtualization of network functions (NFV). In addition, concrete examples of endangering the security of the service are presented, as well as security mechanisms that will allow the user to access the services without the risk of losing the authenticity, confidentiality, availability of the service and integrity.*

Keywords: *software defined networking (SDN), network function virtualization (NFV), 5G mobile network,*

1. UVOD

U poslednjih tridesetak godina došlo je do intenzivnog razvoja više generacija mobilnih komunikacionih sistema, koji su sa sobom donosili novosti i poboljšanja u odnosu na prethodnu generaciju. Trenutno se kod nas i u svetu koristi četvrta generacija mobilnih komunikacionih sistema (4G) ili LTE (*Long Term Evolution*). Međutim, već se uveliko razvija novi mobilni komunikacioni sistem pete generacije. Paketski audio i video striming su sve popularnije usluge, To zahtijeva sve veće brzine prenosa podataka i manja kašnjenja. 5G sistemi se projektuju da zadovolje te zahtjeve a donese i nove funkcije.

Savremeni tempo života nužno donosi automatizaciju u gotovo svim aspektima života i rada ljudi. Osim toga, sve veći broj uređaja se povezuje u mrežu, i gradi koncept Internet stvari, IoT (*Internet of Things*).

Ovo je zapravo mreža uređaja koja ima zadatak da omogući razvoj takozvanih „pametnih kuća", a nakon toga i „pametnih gradova", „pametnih vozila" i slično. Da bi ovo bilo ostvareno, potrebno je implementirati novu, petu generaciju mobilnih komunikacionih sistema (5G). 5G je uveliko u fazi istraživanja i razvoja, a neke države su i implementirale 5G sisteme na nekim područjima.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Željen Trpovski, vanr. prof.

Tehnologije potrebne za njenu implementaciju svakodnevno se usavršavaju, kako bi pružile adekvatan kvalitet usluge. Četvrta generacija mobilnih komunikacionih sistema već ima zavidan kapacitet, brzinu i mala kašnjenja, ali se od pete generacije očekuje napredak u svim nabrojanim aspektima. Osim toga, od pete generacije se očekuje i manja potrošnja energije.

Softversko definisano umrežavanje (SDN) je nova tehnologija koja olakšava upravljanje i programabilnost mrežog sistema, što mrežu čini pouzdanijom centralizujući odvajanje upravljačke od ravni prosleđivanja podataka. Najvažnije prednosti SDN tehnologije ogledaju se u mogućnosti globalnog pregleda mreže, čime se omogućava centralizacija i prikupljanje podataka o mrežnom saobraćaju, a samim tim se poboljšava i kontrola nad mrežom. Centralizovanim pregledom mreže lakše se uočavaju greške i moguće opasnosti, pa je jednostavnije i brže pravovremeno reagovanje u cilju otklanjanja istih. Kod SDN tehnologije, pored prednosti, postoje i određeni bezbjednosni nedostaci.

SDN tehnologija olakšava DDoS (Distributed Denial of Service) i MITM (*Man In The Middle***)** napade, a mogu se očekivati napadi i na kontrolni sistem. Osim toga, s obzirom da je kontrola nad mrežom centralizovana, upad u sistem može kompromitovati cjelokupnu mrežu. Veliki bezbjednosni izazov predstavlja i očekivani ogromni broj korisnika, te će morati biti posvećena naročita pažnja u održanju funkcionalnosti i integriteta mreže.

Jedno od inovativnih rješenja za zaštitu od napada na kontrolni sistem bila bi replikacija lažnih kontrolera, čime bi se potencijalnom napadaču otežao pronalazak stvarnog kontrolera. Ovo nije savršeno rješenje, ali na ovaj način kontrolni sistem će barem donekle moći biti zaštićen. Ipak, potrebni su dodatni zaštitni sistemi, kako bi se osigurala bezbjednost SDN tehnologije. Paketi podataka kod SDN mreža se štite tehnikama kodiranja.

Međutim, kodiranje ne predstavlja zaštitu od distribuiranog uskraćivanja usluge, koje ima za cilj preopterećenje mrežnih resursa ogromnim brojem zahtjeva.

Rješenje za ovaj problem može biti uvođenje vremenskih markera, uz pomoć kojih bi mogao biti prepoznat DoS i DDoS napad [1].

2. PREDLOŽENA BEZBJEDNOSNA ARHITEKTURA 5G MOBILNIH MREŽA

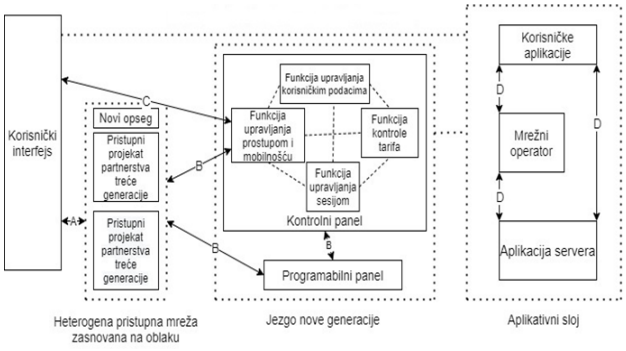
Bezbjednosna arhitektura mora biti realizovana tako da se prilagodi mrežnoj arhitekturi, ali mora da odgovori i na bezbjednosne izazove koje sa sobom nose 5G sistemi. Ona mora biti osmišljena tako da bude efikasna, ne opterećuje mrežne resurse i da bude adaptivna, kako bi se mogla prilagoditi trenutnim potrebama. Takođe, bezbjednosna arhitektura mora biti otporna na različite

prijetnje i akcije koje mogu kompromitovati bezbjednost podataka koji se šalju i primaju i korisnika koji komuniciraju.
Osim toga, mora se uzeti u obzir i činjenica da se od mobilnih mreža pete generacije očekuje da podrži veliki broj uređaja i korisnika. Zato se moraju osmisliti bezbjednosni mehanizmi koji će moći podržati ovako veliki broj uređaja i korisnika. Zbog tako velikog broja uređaja i korisnika, koji do sada nije viđen ni u jednoj mobilnoj mreži starije generacije, moraju se koristiti znatno napredniji bezbjednosni mehanizmi od ranije implementiranih. Svakako, treba se uzeti u obzir i potreba za izuzetno malim kašnjenjem zbog primene u sistemima za autonomnu vožnju, gdje reakcije u saobraćaju moraju biti brze i pravovremene.
S obzirom na ove zahtjeve, predlaže se razdvajanje ravni prosleđivanja podataka od kontrolne ravni, čime bi se omogućilo kodiranje podataka tako da budu fleksibilniji, da upravljanje mrežom i mrežnim saobraćajem postane jednostavnije, kao i da se ubrza proces provjere bezbjednosnih aspekata.

Najvažnije mrežne funkcije kontrolnog sloja jesu:

- Funkcija upravljanja pristupom i mobilnošću AMF (*Access and Mobility Management Function*). AMF nije uvijek neophodna, već zavisi od različitih primjena.
- Funkcija upravljanja sesijom, SMF (*Session Management Function*). Može postojati više SMF funkcija koje upravljaju različitim sesijama jednog korisnika za jedan AMF.
- Funkcija objedinjenog upravljanja podacima UDM (*Unified Data Management*). Ova funkcija takođe upravlja profilima za fiksni i mobilni pristup u 5G mreži.
- Funkcija kontrole politike PCF (*Policy Control Function*). Ovom funkcijom omogućava se upravljanje mobilnošću, kvalitetom usluge, romingom i sl. PCF funkcija vrši kontrolu AMF i SMF funkcija.

U 5G mrežama postoje četiri bezbjednosna domena, organizovana na sličan način kao u mobilnim mrežama starijih generacija.
Na slici 1. prikazana je bezbjednosna arhitektura sa četiri bezbjednosna domena, označenih sa A, B, C i D.



Slika 1. *Bezbjednosna arhitektura mobilne mreže [2]*

Bezbjednosni domen označen sa A, sačinjen je od bezbjednosnih funkcija koje obezbjeđuju bezbjedan pristup mreži, uz zaštitu od različitih vrsta napada. S obzirom na to da se u novom fizičkom sloju primjenjuju tehnologije kao HetNet, D2D (*Device-to-Device*), MIMO (*Multiple-Input and Multiple-Output*) i druge, pojavljuju se i problemi sa bezbjednošću koji se moraju sanirati i prevenirati.
Bezbjednosni domen označen sa B sačinjen je od funkcija čija je uloga zaštita od napada na klasični kablovski dio mreže, koji otežavaju bezbjednu razmjenu podataka. Bezbjednosni domen B nalazi se između RAN (*Radio Access Network*) i jezgra mreže nove generacije, kontrolnog i korisničkog sloja. Autentičnost, povjerljivost podataka i integritet predstavljaju najvažnije aspekte koji se provjeravaju u ovom bezbjednosnom domenu.
Bezbjednosni domen označen sa C sačinjen je od bezbjednosnih funkcija čija je uloga da obezbijede obostranu provjeru između jezgra mreže nove generacije i korisničkog interfejsa i to prije nego sam kontrolni sloj pristupi korisničkom interfejsu. Na ovaj način se vrši provjera autentičnosti.
Bezbjednosni domen označen sa D predstavlja bezbjednosne funkcije čija je uloga obezbjeđenje bezbjednosti poruka koje se razmjenjuju između korisničkog interfejsa i pružaoca usluge, ali i između korisnika i mrežnog operatora.

3. BEZBJEDNOSNI MEHANIZMI U 5G MOBILNOJ MREŽI

U cilju ostvarivanja bezbjednosnih zahtjeva 5G sistema neophodno je izvršiti unaprijeđenje postojećih bezbjednosnih mehanizama i iznaći nova rješenja koja će biti namjenski napravljena za primjenu u 5G sistemima. Inovativna arhitektura koju sa sobom donosi mobilna mreža pete generacije zahtijeva unaprijeđenje bezbjednosnih protokola, mali memorijski prostor i veoma brzu obradu podataka, u cilju smanjenja kašnjenja u procesu komunikacije. Osim toga, bezbjednosni mehanizmi moraju imati osobinu adaptivnosti, kako bi se mogli prilagoditi različitim vrstama napada i drugim bezbjednosnim prijetnjama.
Neke od bezbjednosnih tehnika koje bi mogle unaprijediti nivo bezbjednosti u mobilnim komunikacionim sistemima pete generacije jesu:

- provjera autentičnosti,
- održavanje povjerljivosti komunikacije,
- obezbjeđenje dostupnosti usluga i
- zadržavanje integriteta.

3.1. Provjera autentičnosti

Provjera autentičnosti se može vršiti na dva načina i to provjerom osobe i provjerom poruke. Provjera osobe ima za cilj da nesumnjivo utvrdi autentičnost strana u komunikaciji, dok s druge strane provjera poruke ima za cilj provjeru autentičnosti samog sadržaja komunikacije.
Postoje tri načina na koje se može izvršiti provjera autentičnosti. To su:

- provjerom same mreže,
- provjerom pružaoca usluge i
- provjerom i mreže i pružaoca usluge [6].

Kod SDN mreža preporučuje se brza provjera autentičnosti, koja ne upotrebljava kriptografske algoritme (koji neminovno oduzimaju vrijeme za provjeru autentičnosti), u cilju povećanja efikasnosti kod velikog broja zahtjeva. U poređenju sa digitalnom kriptografijom,

ovaj metod je teže potpuno kompromitovati. Metod se realizuje u više bezbjednosnih slojeva, pa je i stepen bezbjednosti veći [7].

3.2. Povjerljivost

Dva su aspekta koja čine povjerljivu komunikaciju, a to su povjerljivost podataka i privatnost. Povjerljivost podataka štiti podatke u toku prenosa od različitih vrsta pasivnih napada na način da ograničava pristup podacima samo ovlašćenim korisnicima. Privatnost s druge strane utiče na sprečavanje kontrolisanja i uticanja na samu informaciju, odnosno sprečava se pristup analitičkim podacima mogućim napadačima.

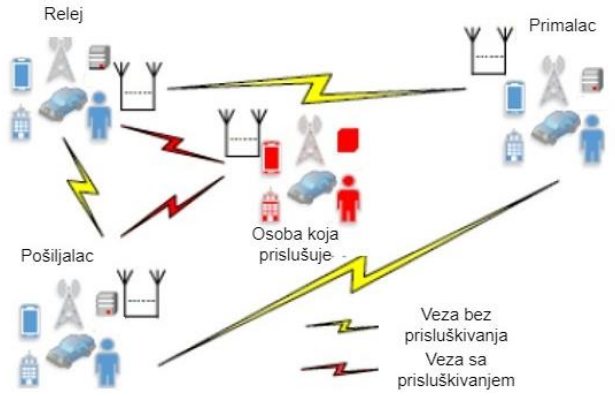
Za zaštitu povjerljivosti podataka i privatnosti najčešće se koristi metoda kodiranja. Metod kodiranja sprečava neovlašćen pristup i upotrebu podataka. Za kodiranje poruka veoma često se koristi metod simetričnog ključa. Princip simetričnog ključa zasniva se na tome da svaka strana u komunikaciji ima privatni ključ, pomoću kojeg se kodira i dekodira poruka. Privatni ključ mora biti distribuiran na bezbjedan način, kako bi se spriječilo da komunikacija bude kompromitovana. Metod simetričnog ključa je bezbjedan za slučajeve napada gdje napadač ima limitirane računarske resurse, pa ne može probiti šifru.

Da bi bio postignut visok nivo povjerljivosti podataka koji se u toku komunikacije razmjenjuju, potrebno je koristiti sledeće metode:

- upravljanje snagom,
- sigurnosni relej,
- vještački šum,
- obrada signala.

Upravljanje snagom signala je neophodno kako bi se otežala ili onemogućila rekonstrukcija komunikacionog signala i kako bi se na taj način izbjeglo presretanje i prisluškivanje komunikacije za neovlašćene osobe. Snaga signala prilagođava se smjeru komunikacije, sa ciljem da signal nosilac podataka dođe na odredište, odnosno do primaoca kojem je i namijenjen. Na ovaj način može znatno biti smanjena količina podataka koji su dostupni neovlašćenim licima.

Sigurnosni relej može biti posrednik u komunikaciji između dvije osobe. Sigurnosni relej pomaže pošiljaocu da bezbjedno prenese podatke do primaoca, kao što je to prikazano na slici 2.



Slika 2. *Princip rada sigurnosnog releja kao mehanizma zaštite poslanih poketa* [8]

3.3. Dostupnost

Pojam dostupnosti može se definisati kao stepen pristupačnosti usluge korisnicima, kao i u kom fizičkom dijelu teritorije je usluga pristupačna korisnicima. Dostupnost se može smatrati mjerom robustnosti sistema u slučaju napada. DoS i DDoS napadi predstavljaju zapravo napade na dostupnost usluge, a oni mogu onemogućiti korišćenje usluga koje pruža mrežni operator. Osim navedenog, ometanje takođe negativno utiče na dostupnost mreže, otežavajući komunikaciju. U 5G mrežama postojaće veliki broj čvorova, koji su potrebni za IoT, a to predstavlja veliki izazov u sprečavanju ometanja i DDoS napada, kako bi se obezbijedila dostupnost mreže [7].

3.4. Integritet

Bez obzira na činjenicu da se u svakoj komunikaciji vrši provjera autentičnosti poruke, čiji je zadatak provjeriti legitimitet izvora poruke, potrebno je takođe provjeriti da li je poruka u procesu prenosa izmijenjena ili duplifikovana. Zbog toga je od velikog značaja koristiti dodatni bezbjednosni mehanizam, čija je funkcija provjera integriteta poruke. Zadatak ovakvog mehanizma je da spriječi nepoželjno umnožavanje poruke, čime se zagušuje komunikacioni kanal, odnosno sistem, ali i da spriječi aktivne napade na komunikaciju, koje imaju za cilj da izmijene poslatu poruku. Apsolutan integritet poruke obezbjeđuje se na način da se obavlja obostrana provjera uz pomoć ključeva namijenjenih za provjeru integriteta.

4. ZAKLJUČAK ISTRAŽIVANJA NA OSNOVU KONTRAPRIMJERA RADI „OBARANJA“ HIPOTEZE

Ovaj rad je proizašao iz master rada, te su analizirane bezbjednosne prijetnje kao i kontraprimjeri obaranja polazne hipoteze za 5G sisteme. Na osnovu njih ponuđena su rješenja za zaštitu komunikacije u ovim sistemima. Kao prvi kontraprimjer se navodi aktivno prisluškivanje koje na osnovu povećanja broja antena (M>50) unutar bazne stanice ugrožava kapacitet tajnosti korisnika.

Dakle, aktivnom prisluškivaču kapacitet tajnosti je porastao i samim tim ugrozio legalnog korisnika. Drugi kontraprimjer se odnosi na distubuirani napad uskraćivanja usluge, gdje je jasno prikazano da se sav saobraćaj obustavlja, jer je došlo do zagušenja servera, a to se desilo nakon 3 sata od početka simulacije. Treći, ujedno i poslednji kontraprimjer se odnosi na slučaj „čovjek u sredini” (MITM), gdje „napadač” na osnovu URL adrese pristupa istom serveru kao i „žrtva” te uspijeva da preuzme odgovarajuće informacije.

preuzete informacije su napadaču neophodne za uspješan napad, uz pomoć unaprijed određenog pseudokoda.

Ipak, za obezbjeđenje maksimalne sigurnosti komunikacije pored navedenih kontraprimjera za obaranje hipoteze, biće potrebno implementirati tehnologije mobilnih mreža pete generacije u većoj mjeri – kao mreže sa velikim brojem korisnika.

Tokom implementacije vjerovatno će biti uočene i prijetnje i nedostaci, koje nije moguće uočiti prije samog realnog korišćenja. U ovom slučaju, adaptivni bezbjednosni mehanizmi mogli bi igrati ključnu ulogu za bezbjednu komunikaciju.

5. ZAKLJUČAK

Iz prethodnog izlaganja vidljivo je da svaka nova generacija mobilnih komunikacionih sistema nastaje kao rezultat potrebe za unapriđeđenjem postojećih mobilnih komuni-

kacionih sistema. Stoga je peta generacija mobilnih komunikacionih sistema nastala kao posljedica potrebe za razvojem mobilnih komunikacionih sistema četvrte generacije. Međutim, ona nije samo jednostavno unaprijeđenje LTE sistema, već je u svojoj osnovi bazirana na drugačijoj, naprednijoj arhitekturi i namijenjena je za znatno drugačije potrebe korisnika.
Mobilni komunikacioni sistemi pete generacije trebalo bi da u velikoj mjeri:

- ubrzaju prenos podataka,
- kašnjenja smanje na najmanju fizički moguću mjeru,
- pruže velikom broju korisnika na malom fizičkom području pristup širokopojasnoj Internet vezi,
- unaprijede pokrivenost signalom i
- unaprijede energetsku efikasnost sistema.

Da bi svi ovi, često kontradiktorni zahtjevi, bili mogući, potrebno je razviti tehnologije koje će razdvojiti hardverske i softverske funkcije i omogućiti virtualizaciju mrežnih funkcija.
Na taj način mobilne mreže pete generacije postaju daleko fleksibilnije i efikasnije, jer će postati moguće dijeliti mrežu na manje logičke cjeline, koje će biti konfigurisane u zavisnosti od potreba korisnika. Jezgro mreže, koje je u mobilnim komunikacionim sistemima starije generacije bila jedinstvena logička cjelina, u 5G mrežama moći će biti podijeljena na više jezgara, koja će obavljati funkcije bliže korisnicima, čime će se kašnjenje svesti na minimum.
Može se zaključiti da će mobilni komunikacioni sistemi pete generacije u prvih pet godina aktivnog rada imati ogroman broj korisnika, čime će se visoka ulaganja u razvoj istih isplatiti.
Uzevši u obzir naprijed navedeno, jasno je da su bezbjednosni zahtjevi 5G sistema znatno veći nego kod bilo kojeg drugog mobilnog komunikacionog sistema starije generacije.
Bezbjednost dakle, predstavlja izuzetno važno pitanje za mobilne komunikacione sisteme pete generacije. Ipak, imajući u vidu uspjeh ranijih generacija mobilnih komunikacionih sistema, može se očekivati da će razvojni timovi 5G sistema uspješno odgovoriti na sve izazove i projektovati sisteme bezbjedne, brze i pouzdane za krajnje korisnike.

6. LITERATURA

[1] „What is NFV: network functions virtualization basics“, dostupno na: https://www.electronics-notes.com/articles/connectivity/nfv-network-functionsvirtualisation/what-is-nfv-basics.php

[2] Eftychia Datsika : Radio resource management techniques for QoS provision in 5G networks PhD thesis dissertation, Universitat Politècnica de Catalunya (UPC), Barcelona, 2018

[3] Fernando Rodriguez, Ugo Dias, Divanilson Campelo, Robson Albuquerque, Se-Jung Lim and Luis Villalba, (2019): QoS Management and Flexible Traffic Detection Architecture for 5G Mobile Networks

[4] A., Kumar, Y., Liu, J. Sengupta: Evolution of Mobile Wireless Communication Networks: 1G to 4G, 2010

[5] Konstantinos Liolis, Alexander Geurtz, Ray Sperber, Detlef Schulz, Simon Watts, Georgia Poziopoulou, Barry Evans, Ning Wang, Oriol Vidal , Boris Tiomela Jou , Michael Fitch (2019): Use cases and scenarios of 5G integrated satellite-terrestrial networks for enhanced mobile broadband: The SaT5G approach, Journal of satellite communications and networking

[6] “5G Security: Forward Thinking Huawei White Paper”, HUAWEI WHITE PAPER, 2015.

[7] Dongfeng Fang, Yi Qian, Rose Qingyang Hu, „Security for 5G Mobile Wireless Networks“, IEEE, August 2017.,str. 5 - 6. [15] Dongfeng Fang, Yi Qian, Rose Qingyang Hu, „Security for 5G Mobile Wireless Networks“, IEEE, August 2017., Figure 12., str. 15

[8] [8] Robert W. Heath Jr., „Heterogeneous Networks“ , University of Texas at Austi

[9] Ankit Nilesh Ganatra (2017): Developments of 5G Technology, Master of Science Thesis, Governors State University

[10] Manuel Sainz (2015): 5G Techniques - Proof-of-concept Testbed , Master of Science Thesis, Aallborg University

[11] Konpal Shaukat Ali (2018): Modeling, Analysis, and Design of 5G Networks using Stochastic Geometry, King Abdullah University of Science and Technology Thuwal, Kingdom of Saudi Arabia

Kratka biografija:

Jovan Gojić, rođen je u Doboju 1994. god. Osnovnu i srednju školu završio u Doboju, gdje je završio i I cuklus studija na Saobraćajnom fakultetu. Master rad na Fakultetu tehničkih nauka iz oblasti Elektrotehnika i računarstva – Telekomunikacioni sistemi odbranio je 2021. god.
Kontakt: jgojic950@hotmail.com

Željen Trpovski rođen je u Rijeci 1957. godine. Doktorirao je na Fakultetu tehničkih nauka 1998. god. Oblast interesovanja su telekomunikacije i obrada signala.

Dejan Nemec rođen je 1972. god. Diplomirao, specijalizirao i magistrirao je na Fakultetu tehničkih nauka iz oblasti Elektrotehnike i računarstva. Oblast interesovanja su telekomunikacije i obrada signala.

Zahvalnica:
Izradu ovog rada pomogao je Fakultet tehničkih nauka u Novom Sadu, Departman za energetiku elektroniku i telekomunikacije, u okviru projekta pod nazivom: "Istraživanja u oblasti energetike, elektronike, telekomunikacija i primenjenih informacionih sistema u cilju modernizacije studijskih programa".