Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 4.9
DOI: https://doi.org/10.24867/32BE12Mladenovic

PRIMENA TEHNIKA MAŠINSKOG UČENJA NA PROBLEM KLASIFIKACIJE RAZLIČITIH SCENARIJA BOTNET NAPADA

APPLICATION OF MACHINE LEARNING TECHNIQUES ON THE PROBLEM OF CLASSIFICATION OF DIFFERENT SCENARIOS OF BOTNET ATTACKS

Luka Mladenović, *Fakultet tehničkih nauka, Novi Sad*

Oblast – SOFTVERSKO INŽINJERSTVO, INTELIGENTNI SISTEMI

Kratak sadržaj – *Sajber napadi postaju deo svakodnevice, a sa učestalošću raste i njihova sofisticiranost. Upravo zato je potrebno više napretka i kontinuirane inovacije u odbrambenim strategijama. Tradicionalne metode otkrivanja upada i dubinske inspekcije paketa, iako se još uvek u velikoj meri koriste i preporučuju, više nisu dovoljne da zadovolje zahteve rastućih pretnji po bezbednost.*

Ključne reči: *Mašinsko učenje, klasifikacija, botnet, sajber bezbednost*

Abstract – *Cyber attacks are becoming part of everyday life, and their sophistication is increasing with frequency. This is precisely why more progress and continuous innovation in defense strategies is needed. Traditional methods of intrusion detection and deep packet inspection, although still widely used and recommended, are no longer sufficient to meet the demands of growing security threats.*

Keywords: *Machine learning, classification, botnet, cyber security*

1. UVOD

Sajber bezbednost je stalno u razvoju, ali i stopa sajber kriminala stalno raste. Sofisticirani napadi se smatraju delom svakodnevice jer postaju sve češći i rasprostranjeniji [1]. Ova stalna evolucija takođe zahteva inovacije u sajber bezbednosti.

Postoje rešenja i kombinacije metoda koje se i dalje široko koriste. Sistemi za otkrivanje i prevenciju upada u mrežu (IDS/IPS) prate zlonamerne aktivnosti ili kršenja pravila postavljenih u datoj mreži [2]. IDS zasnovan na potpisima oslanja se na poznate potpise i efikasan je u otkrivanju malvera koji odgovaraju tim potpisima. IDS zasnovan na ponašanju, s druge strane, uči šta je normalno za sistem i izveštava o svakom događaju koji odstupa od norme [3].
Analiza celokupnih podataka paketa je još jedna opcija, ali je i računski preskupa i nosi rizik izlaganja osetljivih korisničkih informacija. U ovom radu se koriste Netflow podaci za analizu. Netflow zapisi pružaju dovoljno informacija da jedinstveno identifikuju saobraćaj koristeći atribute kao što su 5-tuples i druga polja, ali ne otkrivaju privatne ili lično identifikovane informacije (PII) [4].
Netflow, zajedno sa svojom otvorenom standardnom verzijom IPFIH, već se široko koristi za nadzor i upravljanje mrežom. Dostupnost Netflow podataka zajedno sa funkcijama privatnosti čini ga najadektvanijim izborom [6].

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

2. CILJ RADA I METODOLOGIJA

Glavni cilj ovog projekta je otkrivanje malvera ili botnet saobraćaja iz Netflow skupa podataka koristeći različite pristupe mašinskog učenja. Konkretno, ovaj predloženi pristup ima za cilj da:

1. Otkriva malver ili botnet saobraćaj iz Netflow podataka. Sistem bi trebalo da uzme bilo koji Netflow skup podataka bilo koje veličine, čist ili sa malverom, i klasifikuje ga kao normalan ili napadački saobraćaj.
2. Uporedi različite metode mašinskog učenja i preporuči odgovarajuću za specifične slučajeve upotrebe.

Da bi se postigli gore navedeni ciljevi, sledi se metodologija opisana u nastavku.

1.Odabir skupa podataka: Prvi deo metodologije je prikupljanje podataka o protoku saobraćaja. To se može uraditi tako što će se dobiti stvarni saobraćaj iz poznate organizacije i izvući Netflow-ovi.. Ovaj rad koristi CTU-13 u odnosu na druge javne skupove podataka jer je veoma dostupan i široko korišćen za mnoge slične istraživačke studije u prošlosti. Zatim statistički se ispituje skup podataka kako bi se identifikovale zajedničke karakteristike i frekvencije. Karakteristike su sirovi atributi u Netflow podacima - StartTime, Duration, Proto, SrcAddr, Sport, Dir, DstAddr, Dport, State, sTos, dTos, TotPkts, TotBytes, SrcBytes i Label. Ova grupa karakteristika opisuje tokove.

2.Ekstrakcija karakteristika: Iz odabranog skupa podataka identifikuju se i izdvajaju karakteristike Netflow podaci sadrže kategorijalne karakteristike koje moraju biti kodirane u numeričke ili boolean vrednosti, što bi rezultiralo matricom prevelike veličine i izazvalo probleme sa memorijom. Da bi se smanjila količina podataka za obradu, koristi se šema za uzorkovanje Netflow saobraćaja koristeći vremenski prozor. Odabran je vremenski prozor od 2 minuta sa korakom od 1 minuta. Zatim se obrađuje dvosmerni Netflow skup podataka i izdvajaju kategorijalne i numeričke karakteristike koje opisuju skup podataka unutar datog vremenskog prozora

3.Selekcija karakteristika: Uključuje korišćenje tehnika selekcije karakteristika kako bi se smanjila dimenzija ulazne matrice za obuku. Filtriranje karakteristika kroz Pirsonovu korelaciju, metode omotača koristeći eliminaciju karakteristika unazad, ugrađene metode unutar Random Forest klasifikatora, analiza glavnih komponenti (PCA) i t-distribuirano stohastičko ugrađivanje suseda (t-SNE) su različite tehnike koje se koriste u ovu svrhu.

4.Poređenje algoritama: Odlučeno je da je svrishodno upoređivanje pet odabranih algoritama. Različiti modeli mašinskog učenja koji će biti obučeni u ovom koraku su: logistička regresija, Support Vector Machine (SVM), Random Forest klasifikator, gradient boosting i gusta neuronska mreža

5.Detekcija botneta: Poslednji korak u ovoj metodologiji uključuje testiranje modela kako bi se saznalo da li je moguće uspešno detektovati botnet saobraćaj iz CTU-13 skupa podataka. Ukupna performansa detekcije botneta se određuje na osnovu f1 skora gorepomenutih modela

Rad sa podacima o mrežnoj bezbednosti donosi mnogo izazova. Prvo, podaci su veoma neuravnoteženi jer je većina saobraćaja bezopasna, a samo mali deo je zlonameran. To otežava modelu da nauči šta je štetno. Pored toga, rizik od prekomernog prilagođavanja tokom procesa obuke je visok jer struktura mreže utiče na način na koji model uči, dok se želi algoritam koji je nezavisan od mreže.

Pored toga, analiza saobraćaja se bavi mrežom koja je dinamična struktura; komunikacije zavise od vremena, a veze između servera mogu se pojaviti i nestati sa novim zahtevima i novim korisnicima u mreži [5].

2.2. Analiza podataka

CTU-13 skup podataka je označen skup podataka koji se koristi u literaturi za obuku algoritama za detekciju botneta (vidi na primer [9] i [7]. Kreirao ga je CTU univerzitet 2011. godine i beleži stvarni botnet saobraćaj pomešan sa normalnim saobraćajem i pozadinskim saobraćajem.

CTU-13 skup podataka se sastoji od 13 snimaka različitih uzoraka botneta sažetih u 13 dvosmernih Netflov5 fajlova.

Glavni problem sa Netflow podacima je što je većina informacija u obliku kategorijalnih karakteristika. Pokušaj transformacije kategorija u boolean kolone rezultira eksplozijom veličine matrice, što izaziva greške u memoriji (čak i nakon korišćenja komprimovane retke matrice). Popularna ideja je sažimanje podataka unutar vremenskog prozora. Ovo je opravdano činjenicom da botneti "imaju tendenciju ponašanja sa vremenskom lokalnošću" [7]. Pored toga, omogućava da se smanji količina podataka i da se isporuči detektor botneta koji daje rezultate uživo nakon svakog vremenskog prozora (u zamenu za detalje ulaznih podataka) [8].

Glavni problem je odrediti širinu i korak vremenskog prozora. Pregledana literatura predlaže različite opcije (2 minuta u metodi detekcije BCLus u [7], 3 sekunde u algoritmu MINDS u [12], 5 minuta u algoritmu Xu u [9], ali su ovi predlozi često empirijski. U ovom slučaju, odabrana je širina vremenskog prozora od 2 minuta i korak od 1 minuta.

Još jedan problem je da vremenski prozor prikuplja Netflow komunikacije prema vremenu početka veze. Korišćenje statusa komunikacije (aktivna ili završena) rezultiralo je eksplozijom veličine podataka, pa je korišćeno trajanje komunikacije kao dodatna karakteristika.

Izdvojene karakteristike pokušavaju da predstave Netflow komunikacije unutar vremenskog prozora. Da bi se to postiglo, podaci vremenskog prozora se prikupljaju prema izvornoj adresi. Postoje 2 karakteristike izdvojene iz svake kategorijalne Netflow karakteristike (u ovom slučaju: izvorni portovi, odredišne adrese i odredišni portovi):

- broj jedinstvenih pojava u podgrupi
- normalizovana entropija podgrupe

Što se tiče numeričkih Netflow karakteristika (u ovom slučaju: trajanje komunikacije, ukupan broj razmenjenih bajtova, broj bajtova poslatih od strane izvora), izdvojeno je 5 karakteristika: suma, srednja vred, stand. dev, maksimum, medijana.

Međutim, one mogu biti redundantne ili irelevantne za detekciju botneta, pa je potrebna selekcija karakteristika.

Odabir karakteristika vršio se uspomoć Filler i Wrapper metoda. Ispitana je takođe i korelacija između svih karakteristika. Takođe upotrebljene su i tzv. Embedded metode, kao što su Lasso i Ridge logistička regresija kao i SVM sa rekurzivnom eliminacijom karakteristika. Ispitana je i važnost svake karakteristike prema Random Forest klasifikatoru. Takođe, primenje su i tehnike redukcije dimenzionalnosti, kao što su PCA i tSNE.

2.3. Rezultati rada

Da bi se uporedili rezultati različitih algoritama, potrebno je odabrati neke metrike za evaluaciju performansi metoda.Treba imati na umu da je za ovaj projekat detekcije zlonamernog softvera imati nizak recall gore nego imati nisku preciznost, jer to znači da su većina detektovanih komunikacija botneti (preciznost), ali većina botnet komunikacija ostaje neotkrivena (recall). Naravno, imati dobar recall je lako jer sve što treba uraditi je označiti svaku komunikaciju kao botnet. Dakle, odabrani kompromis je maksimizacija f1 skora uz proveru da recall nije previše nizak.

Metoda logističke regresije je algoritam koji koristi linearnu kombinaciju karakteristika za klasifikaciju tokova. Kros-validacija je neophodna za podešavanje parametara modela. Konačno odabrani parametri su C = 550 i Weighton-botnet = 0.044.

Najbolji SVM parametri za detekciju botneta u prvom scenariju CTU-13 su polinomski kernel sa stepenom 2.

Random Forest je algoritam koji koristi nekoliko klasifikatora odlučujućih stabala za predviđanje klase svakog ulaznog toka. Odabrani broj stabala u šumi je 100.

Metoda Gradient Boosting je algoritam koji takođe koristi klasifikatore odlučujućih stabala, ali pokušava da postepeno poboljša obuku koristeći skor jednog stabla za izgradnju drugog. Dva glavna parametra moraju biti podešena: funkcija gubitka i maksimalna dubina stabala (odabrani broj stabala je 100). Odabran je eksponencijalni gubitak sa maksimalnom dubinom klasifikatora 4.

U poslednje vreme, neuronske mreže su stekle popularnost jer daju vrlo dobre rezultate kada je dostupno mnogo podataka. Ovde je testirana jednostavna gusta (ili potpuno

povezana) neuronska mreža sa 2 skrivena sloja: prvi ima 256 neurona, a drugi ima 128. Parametri neuronske mreže sastoje se od batch-normalizacije, bez dropout ReLU aktivacione funkcije (osim za izlazni sloj gde se koristi sigmoid funkcija). Model ima 39.681 parametar za obuku i 768 parametara koji se ne obučavaju.

Radi upoređivanja algoritama, modeli se obučavaju sa 2/3 skupa podataka (Netflow-ovi su nasumično odabrani) i testirana sa preostalih 1/3.

Tabela 1. Botnet Neris rezultati

Algorithms	Training			Test		
	Precision	Recall	f_1 Score	Precision	Recall	f_1 Score
Logistic Regression	0.74	0.97	0.83	0.74	0.96	0.84
Support Vector Machine	0.94	0.80	0.86	0.91	0.78	0.86
Random Forest	1.0	1.0	1.0	1.0	0.95	0.98
Gradient Boosting	1.0	0.99	1.0	0.98	0.96	0.97
Dense Neural Network	0.90	0.98	0.94	0.96	0.99	0.98

Tabela 1. pokazuje da Random Forest, Gradient Boosting i gusta neuronska mreža nadmašuju druge testirane algoritme u detekciji botneta među mrežnim saobraćajem sa f1 skorom od 0.97. Ipak, metode logističke regresije i Support Vector Machine uspevaju da postignu f1 skor od 0.85, jedna sa niskom preciznošću, druga sa niskim recall-om. Kako je Random Forest najbrži algoritam za obuku i najmanje sklon prekomernom prilagođavanju (jer nema mnogo hiperparametara za odabir), ova tehnika će biti proučavana sa drugim scenarijima u sledećem odeljku.

Da bi se saznalo da li se rezultati Random Forest klasifikatora na scenariju 1 CTU-13 skupa podataka mogu generalizovati, testiraju se na svim ostalim scenarijima

Tabela 2. Rezultati RF klasifikatora

Botnet	Dataset		Training			Test		
	Size	Botnets	Precision	Recall	f_1 Score	Precision	Recall	f_1 Score
Neris - Scenario 1	2 226 720	1.28 ‰	1.0	1.0	1.0	1.0	0.95	0.975
Neris - Scenario 2	1 431 539	1.45 ‰	1.0	1.0	1.0	1.0	0.98	0.99
Rbot - Scenario 3	2 024 053	4.99 ‰	1.0	0.99	0.99	1.0	0.96	0.98
Rbot - Scenario 4	470 663	2.36 ‰	1.0	0.90	0.95	1.0	0.69	0.82
Virut - Scenario 5	63 643	3.46 ‰	1.0	1.0	1.0	1.0	0.25	0.4
DonBot - Scenario 6	220 863	5.57 ‰	1.0	1.0	1.0	1.0	0.9	0.95
Sogou - Scenario 7	50 629	1.38 ‰	1.0	1.0	1.0	1.0	0.25	0.4
Murlo - Scenario 8	1 643 574	6.80 ‰	1.0	1.0	1.0	1.0	0.94	0.97
Neris - Scenario 9	1 168 424	12.51 ‰	1.0	0.99	1.0	1.0	0.94	0.97
Rbot - Scenario 10	559 194	9.67 ‰	1.0	0.98	0.99	1.0	0.90	0.95
Rbot - Scenario 11	61 551	2.76 ‰	1.0	1.0	1.0	0.5	0.33	0.4
NSIS.ay - Scenario 12	156 790	10.20 ‰	1.0	0.82	0.90	0.92	0.41	0.56
Virut - Scenario 13	1 294 025	7.57 ‰	1.0	1.0	1.0	1.0	0.96	0.98

Tabela 2. pokazuje da Random Forest klasifikator uspeva da detektuje većinu botneta u 8 od 13 scenarija. Loši rezultati u preostalih 5 scenarija čini se da su povezani sa veličinom skupa podataka.

Glavni problem sa rezultatima iz Tabele 2. je što su zasnovani samo na jednom testnom skupu podataka. Dakle, ako je veličina skupa podataka premala, statistička greška može biti značajna. Stoga je napravljena statistička analiza na scenarijima koji imaju male skupove podataka.

Tabela 3. kvalifikuje rezultat iz prethodnog odeljka jer pokazuje da srednje vrednosti skora nisu tako loše kao što se može protumačiti iz Tabele 2. Naime, male veličine skupova podataka su odgovorne za značajnu statističku devijaciju. Treba napomenuti da unapredna obrada ekstrakcije karakteristika nije razlog za nedostatak podataka jer originalni skupovi podataka već imaju malo tokova (129.832 za scenario 5, 114.077 za scenario 7, 107.251 za scenario 11).

Tabela 3. Statistička analiza rezultata na 50 nasumičnih skupova test podataka

Botnet	Mean (Test)			Standard deviation (Test)		
	Precision	Recall	f_1 Score	Precision	Recall	f_1 Score
Rbot - Scenario 4	1.0	0.60	0.75	0.0	0.08	0.06
Virut - Scenario 5	1.0	0.45	0.59	0.0	0.21	0.20
DonBot - Scenario 6	1.0	0.95	0.97	0.0	0.03	0.02
Sogou - Scenario 7	1.0	0.42	0.52	0.0	0.30	0.32
Rbot - Scenario 10	0.99	0.90	0.94	0.01	0.02	0.01
Rbot - Scenario 11	0.95	0.50	0.63	0.12	0.18	0.16
NSIS.ay - Scenario 12	0.93	0.39	0.54	0.07	0.08	0.08

Može se primetiti da je prosečna preciznost za svaki scenario blizu 95%, a da je prosečan recall oko 50% ili više. Random Forest klasifikator se čini neefikasnim samo u scenarijima 4 i 12, jer statističke devijacije nisu veoma značajne, a veličine skupova podataka nisu veoma male.

Da bi se izborili sa nedostatkom podataka u nekim scenarijima, ideja je da se klasifikator obuči na jednom scenariju sa velikim skupom podataka, a zatim testira na drugom scenariju sa manjim skupom podataka.

Tabela 4. Rezultati korišćenja scenarija 3 za obuku

Botnet	Test		
	Precision	Recall	f_1 Score
Rbot - Scenario 3	1.0	0.96	0.98
Rbot - Scenario 4	0.0	0.0	0.0
Rbot - Scenario 10	0.0	0.0	0.0
Rbot - Scenario 11	0.0	0.0	0.0

Tabela 5. Rezultati korišćenja scenarija 10 za obuku

Botnet	Test		
	Precision	Recall	f_1 Score
Rbot - Scenario 3	0.0	0.0	0.0
Rbot - Scenario 4	0.6	0.02	0.05
Rbot - Scenario 10	1.0	0.90	0.95
Rbot - Scenario 11	1.0	0.41	0.58

Tabela 6. Rezultati korišćenja scenarija 13 za obuku

Botnet	Test		
	Precision	Recall	f_1 Score
Virut - Scenario 5	0.0	0.0	0.0
Virut - Scenario 13	1.0	0.96	0.98

Tabele br. 4, 5 i 6 pokazuju da obuka klasifikatora na drugom scenariju uopšte ne funkcioniše. To znači da je veoma teško ili nemoguće detektovati nove neviđene botnete sa ovim skupom podataka i ovom metodom. Šodno tome, da bi se detektovao botnet, klasifikator mora biti obučen sa skupom podataka koji sadrži taj botnet unapred.

Još jedno moguće objašnjenje loše generalizacije na druge scenarije je da svaki scenario ima botnet čija je svrha drugačija. Karakteristike Botnet napada su drugačije, pa je i logično da obuka klasifikatora sa drugim scenarijem ne daje dobre rezultate.

Još jedna ideja za rešavanje problema malih veličina skupova podataka je korišćenje metode augmentacije podataka za izgradnju većeg skupa podataka. Ovde ponovo uzorkujemo podatke za obuku koristeći bootstrap tehniku kako bismo ih učinili 10 puta (vidi Tabelu 7) i 30 puta većim (vidi Tabelu 8).

Tabela 7. Statistička analiza sa ponovnim uzokrovanjem, trening skup puta 10

Botnet	Mean (Test)			Standard deviation (Test)		
	Precision	Recall	f_1 Score	Precision	Recall	f_1 Score
Virut - Scenario 5	1.0	0.55	0.69	0.0	0.20	0.17
Sogou - Scenario 7	1.0	0.55	0.65	0.0	0.32	0.31
Rbot - Scenario 11	0.94	0.63	0.74	0.12	0.18	0.14

Tabela 8. Statistička analiza sa ponovnim uzokrovanjem, trening skup puta 30

Botnet	Mean (Test)			Standard deviation (Test)		
	Precision	Recall	f_1 Score	Precision	Recall	f_1 Score
Virut - Scenario 5	1.0	0.57	0.70	0.0	0.20	0.17
Sogou - Scenario 7	1.0	0.55	0.65	0.0	0.33	0.32
Rbot - Scenario 11	0.94	0.64	0.74	0.12	0.19	0.15

Tabele br. 7 i 8 prikazuju statističku analizu scenarija 5, 7 i 11 koristeći bootstrap metodu kao ponovo uzorkovanje. Iz tabele br. 7 se može videti da su recall i f1 skor povećani za oko 10 poena za sve scenarije. To znači da je veličina skupa podataka pravi problem za detekciju botneta. Međutim, Tabela br. 8 pokazuje da se ovaj trik sa ponovnim uzorkovanjem ne može koristiti koliko god želimo, jer rezultati dostižu tačku zasićenja, čak i ako se skup podataka za obuku povećava u veličini sa bootstrap metodom.

3. ZAKLJUČAK

Cilj ovog projekta je bila izgradnja i poređenje modela koji su sposobni da detektuju botnete u stvarnom mrežnom saobraćaju predstavljenom Netflow skupovima podataka. Nakon detaljne analize podataka i mnogih pregleda radova o mrežnoj bezbednosti, izdvojene su relevantne karakteristike. Njihov uticaj je zatim proučavan kroz proces selekcije, ali nijedna karakteristika nije bila dovoljno loša da bi bila izostavljena za deo obuke.

Zatim su testirani različiti algoritmi među kojima su logistička regresija, Support Vector Machine, Random Forest, Gradient Boosting i gusta neuronska mreža. Random Forest klasifikator je odabran za detekciju botneta u svim ostalim scenarijima, što je rezultiralo tačnošću detekcije od više od 95% botneta u 8 od 13 scenarija.

Nakon toga, fokus je bio na povećanju tačnosti za 5 najtežih scenarija. Korišćenje bootstrap metode za povećanje količine podataka rezultiralo je detekcijom više od 55% scenarija 5, 7 i 11. Samo su rezultati scenarija 4 i 12 bili teški za poboljšanje (f1 skor od 0.75 za scenario 4 i 0.54 za scenario 12). Ovo je možda zbog loše reprezentacije ponašanja botneta sa izdvojenim karakteristikama ili je potrebno koristiti složenije algoritme (kao što su rekurzivne duboke neuronske mreže).

Moguće poboljšanje rada predstavljenog ovde bilo bi pokušati modifikaciju izdvojenih karakteristika sa različitim širinama i koracima za vremenski prozor i istražiti više hiperparametara za teške scenarije. Još jedna ideja bi bila pokušati obuku i testiranje nekoliko scenarija istovremeno. Na kraju, nenadgledano učenje može biti testirano za detekciju ponašanja botneta bez korišćenja oznaka podataka

4. LITERATURA

[1] Claise, Benoit. 2004. *Cisco systems netflow services export version*.

[2] Choras, Rafal Kozik and Michal. 2017. *"Pattern Extraction Algorithm for NetFlow-Based Botnet Activities Detection".* Security and Communication Networks 2017.

[3] Cynthia Wagner, Jerome Francois, Thomas Engel, et al. 2011. *Machine learning approach for ip-flow record anomaly detection.* International Conference on Research in Networking, Springer.

[4] *Wikipedia.* Accessed 09 01, 2024. https ://en .wikipedia .org/wiki/Machine_learning

[5] Matija Stevanovic, Jens Myrup Pedersen. 2014. "An efficient flow-based botnet detection using supervised machine learning." *2014 international conference on computing, networking and* 797-801.

[6] David Santana, Shan Suthaharan, Somya Mohanty. 2018. "What we learn from learning-Understanding capabilities and limitations of machine learning in botnet attacks." *arXiv preprint*

[7] Kozik Rafal, Michal Choras, and Jorg Keller. 2019. "Balanced Efficient Lifelong Learning (B-ELLA)

[8] P Fruehwirt, S Schrittwieser, i ER Weippl. 2014. "Using machine learning techniques for traffic classification

[9] Jiangpan Hou et. 2018. "Machine Learning Based DDos Detection Through NetFlow Analysis."

Kratka biografija:

Luka Mladenović rođen je u Aleksincu 1999. god. Master rad na Fakultetu tehničkih nauka iz oblasti Softversko inžinjerstvo – Inteligentni sistemi odbranio je 2024.god.
kontakt: luka99al@gmail.com