Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.41
DOI: https://doi.org/10.24867/06BE15Eric

NAPREDNA KONTROLA PRISTUPA U PAMETNIM MREŽAMA

ADVANCED ACCESS CONTROL IN SMART GRID

Dragan Erić, *Fakultet tehničkih nauka, Novi Sad*

Oblast – Elektrotehničko i računarsko inženjerstvo

Kratak sadržaj – *Proširenje osnovne kontrole pristupa zasnovane na korisničkim ulogama (engl. Role Based Access Control - RBAC) entitetom AOR-a (engl. Area of Responsibility), uz implementaciju servisa za prikupljanje i upravljanje događajima i alarmima u pametnim mrežama.*

Ključne reči: *Kontrola pristupa, RBAC, AOR, Smart Grid*

Abstract – *Extension of Role Based Access Control (RBAC) by AOR (Area of Responsibility) with the implementation of event and alarm collection service in Smart Grid.*

Keywords: *Access Control, RBAC, AOR, Smart Grid*

1. UVOD

Pametne mreže (eng. *Smart Grid*) karakteriše veliki broj korisnika, kritičnih resursa i funkcionalnosti kojima je potrebno upravljati na adekvatan način kako bi bili dostupni svim korisnicima. Tradicionalni elektroenergetski sistemi prolaze kroz duboke promjene koje su rezultovale novim izazovima u procesu upravljanja i nadzora.

Ranije fizički izolovan sistem, sa minimalnim mjerama zaštite ljudskog elementa i uređaja na mreži, danas mora biti prilagođen novim bezbjednosnim prijetnjama. Takve bezbjednosne prijetnje nisu postojale, dok se u elektroenergetski sistem nije počeo uvoditi sve veći broj pristupnih tačaka za razmjenu podataka.

Potrebno je naglasiti važnost izuzetne moći obnovljivih izvora energije kao i njihovog priključivanja na distributivne mreže stvaranjem distribuiranih energetskih resursa (eng. *Distributed Energy Resource* – skr. DER). Na taj način je započeo tranzitivni proces prelaska tradicionalnih pasivnih distributivnih mreža do aktivnih distributivnih sistema, tako da rast entuzijazma za priključivanjem DER-ova poslednjih godina enormno raste.

Sve ovo dovodi do toga da je danas distributivna mreža veoma kompleksna i gotova nemoguća za kontrolu tradicionalnim načinima. Cilj kontrole pristupa jeste ograničenje akcija ili radnji koje legitimni korisnik računarskog sistema može da obavlja.

Korisniku pod kontrolom pristupa zasnovanoj na korisničkim ulogama (eng. *Role Based Access Control*, skr. RBAC) može biti dodijeljena samo jedna uloga u organizaciji.

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

AOR (eng. *Area Of Responsibility*) kontrola pristupa, odnosno kontrola pristupa prema oblasti odgovornosti, predstavlja određeni vid nadogradnje RBAC modela. Oblast odgovornosti podrazumijeva skup dopuštenih operacija nad objektima koji imaju zajedničke karakteristike u okviru elektroenergetskog sistema [1].

2. TEORIJSKE OSNOVE

2.1 Tradicionalni elektroenergetski sistemi

Većina postojećih elektroenergetskih sistema danas ima zajedničke karakteristike. Tri glavne cjeline elektroenergetskih sistema jesu:

- proizvodnja u velikim elektranama,
- prenosna mreža, za prenos energije na visokom naponu i na velika rastojanja do krajnje potrošnje,
- srednjenaponska i niskonaponska distributivna mreža, koja dovodi energiju do krajnjih korisnika.

Konstantan porast zavisnosti od električne energije za obavljanje svakodnevnih aktivnosti i povećanje infrastrukturnih međuzavisnosti prouzrokovali su da tradicionalni sistemi postanu neodrživi. Uvođenjem novih komunikacionih i informacionih tehnologija, pozivajući na decentralizovaniji pristup sistemskim funkcijama nadgledanja i kontrole, elektroenergetski sistem prerasta u inteligentnu mrežu (eng. *Smart Grid*).

2.2 Smart Grid

Proces modernizacije elektroenergetskih sistema podrazumijeva integraciju tradicionalnih elektroenergetskih sistema sa brojnim naprednim sistemima, kao što su nadzorno-upravljački računarski sistemi za automatizaciju procesa upravljanja električnom energijom i optimizaciju potrošnje u zavisnosti od uslova snabdijevanja, zatim napredni mjerni sistemi za upravljanje potrošnjom i brojilima električne energije, automatizovani sistemi za naplatu i drugi sistemi za upravljanje poslovnim procesima elektroenergetske kompanije.

Najveće dobiti od implementacije pametnih mreža jesu sledeći rezultati koji se mogu kvantifikovati [2]:

- Povećanje pouzdanosti, radnih performansi i cjelokupne produktivnosti.
- Efikasniji način dostavljanja električne energije do potrošača smanjuje potreban broj proizvodnih sistema i broj vodova koje treba izgraditi.
- Pouzdanija isporuka električne energije povećava energetsku efikasnost, a dovodi do smanjenja emisije ugljen-dioksida.
- Optimizacija integracije obnovljivih izvora energije.

2.3 Informaciona bezbjednost

Cilj informacione bezbjednosti jeste da se eliminišu ili smanje bezbjednosni rizici, kao i smanjenje posljedica eventualnih incidenata primjenom raznih bezbjednosnih mjera za prevenciju i detekciju napada, kao i reakciju na incidente [1]. Neke od bezbjednosnih mjera uključuju fajl permisije i korisničke kontrole pristupa (eng. *Access Controls*).

2.4 Kontrola pristupa

Cilj kontrole pristupa jeste ograničenje akcija ili radnji koje legitimni korisnik računarskog sistema može da obavlja.

2.4.1 Model kontrole pristupa zasnovan na korisničkim ulogama – RBAC model

Model kontrole pristupa zasnovan na korisničkim ulogama (eng. *Role Based Access Control* skr. RBAC), u kome se pristup zasniva na korisnikovoj funkciji unutar organizacije. Uloga (eng. *role*) predstavlja skup operacija koje korisnik ili više korisnika može izvršavati u kontekstu organizacije. Uloge su orijentisane ka grupama. Instanca korisnikove interakcije sa sistemom se zove sesija (eng. *session*) [3]. Permisije (eng. *permissions* ili *privileges*) su autorizacije za izvodenje odgovarajuće akcije u sistemu [3].

2.5 Postojeće primjene RBAC modela u pametnim mrežama

RBAC je nastao kao alternativa za DAC i MAC modele kako bi se odgovorilo zahtjevima različitih organizacija u državnom i u privatnom sektoru [4]. RBAC je jedan od najzastupljenijih modela za kontrolu pristupa u modernim informacionim sistemima, s obzirom na jednostavnost upravljanja bezbjednosnim politikama, kao i smanjenja troškova i kompleksnosti administracije.

Stoga, autori rada [5] predlažu RBAC model koji se zasniva na dodeli prava pristupa korisnicima na osnovu njihovih uloga i odgovornosti u sistemu, kao i centralizovanoj administraciji bezbjednosnih politika unutar organizacije [1].

Autori u radu [6] navode da postojeće instalacije u digitalnim mrežama često koriste koncept da obavljaju lokalni oblik RBAC-a u zavisnosti od okruženja. Komunikacija između entiteta u kontrolnom centru se, na primjer, vrši na osnovu lokalno ili centralno povezanih korisnika na grupe dozvola. Ovo osigurava da lokalno izvršavanje naredbi može biti izvršeno samo ako su odobrene odgovarajuće dozvole, ali ne mora nužno osigurati udaljenom entitetu da provjeri ko će obaviti namijenjenu operaciju. Pristup opisan u IEC 62351-8 podržava i lokalni trag revizije kroz mogućnost povezivanja informacija o identitetu i pristupu u pristupnom tokenu (eng. *access token*). U trafostanicama, lokalni fizički pristup već može biti dovoljan za pristup entitetima koji komuniciraju. Iako pristup koji koristi tokene za pristup zasnovane na X.509 ima svoje prednosti, on nije odmah primjenljiv u svim slučajevima. Takođe, treba imati na umu da je infrastruktura elektroenergetske mreže tokom godina rasla i da je životni vijek instaliranih uređaja dugačak, 20-25 godina.

Nedavno proučavani različiti sigurnosni modeli u vezi sa kontrolom pristupa koristeći svijest o kontekstu, ali različite usluge koje se nude u pametnim mrežama i kontroli pristupa u takvom okruženju i dalje imaju ozbiljne ranjivosti [6].

Kao što je navedeno u [6] veb-bazirane usluge zasnovane na XMPP su specificirane za integraciju distribuiranih (decentralizovanih) energetskih resursa (DER) u digitalnu energetsku mrežu. Ove usluge mogu iskoristiti već postojeće tehnologije koje podržavaju RBAC, kao što je OpenID Connect ili OAuth 2.0, umjesto da grade paralelnu infrastrukturu za rukovanje RBAC baziranim na X.509 [6].

Autori rada [7] navode da podjela odgovornosti između korisnika kojima je dodijeljena ista uloga smanjuje vjerovatnoću (konfiguracionih) grešaka u sistemu. RBAC96 je prilično generički model kontrole pristupa i ne zadovoljava u potpunosti sve sigurnosne zahtjeve kritičnih infrastrukturnih sistema, poput separacije dužnosti i odgovornosti korisnika u skladu sa regionalnim podjelama kritičnih sredstava. U tu svrhu je uveden pojam područja odgovornosti (AOR) još jedan nivo kontrole pristupa u Smart Grid okruženju.

3. ARHITEKTURA SMART GRID SISTEMA

Arhitekturu *Smart Grid* sistema karakteriše kompleksna arhitektura koja je nastala uvođenjem distribuiranih energetskih resursa kao što su razni tipovi baterija za skladištenje električne energije, distribuirani generatori. Aplikacija predstavlja softversku platformu koja služi za nadzor, upravljanje i regulaciju distribuiranih izvora energije odnosno *Distributed Energy Resource Management System*, skraćeno DERMS. Termin DERMS se najčešće odnosi na softver koji integriše potrebe dispečera sa mogućnostima energetskih resursa sa fleksibilnom potražnjom na kraju mreže.

Korisnik aplikacije je u mogućnosti da unese zathjevani iznos aktivne ili reaktivne snage koji želi da uzme ili da preda u mrežu. Komandovanje tj. postavljanje *setpointa* se oslanja na podatke iz dobavljene vremenske prognoze.

Network Model Service - NMS Predstavlja komponentu koja drugim servisima pruža statičke podatke o mreži.

Supervisory Control And Data Acquisition - SCADA Predstavlja sistem za nadzor i upravljanje fizičkim procesima u elektroenergetskim sistemima.

Calculation Engine – CE Centralna uloga mu je da obrađuje zahtjeve za komandovanjem, tj. zahtjeve za povećanje ili smanjenje proizvodnje aktivne i/ili reaktivne snage distribuiranih izvora električne energije.

Weather Forecast Service Daje uvid u vremensku prognozu CE servisu, gdje se analiziraju podaci do 7 dana unaprijed, na nivou jednog časa.

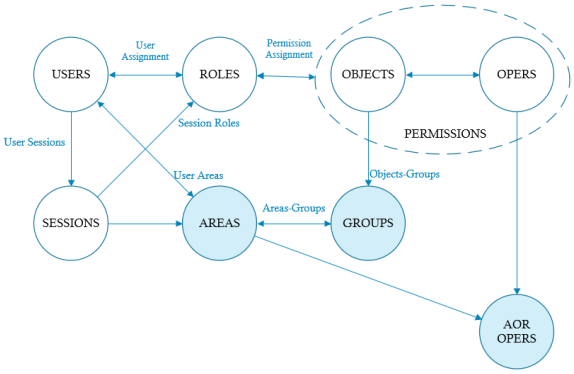
Remote Telemetry Unit – RTU Koriste se prikupljanje izmjerenih analognih i digitalnih ulaza, kao i komandno komunikacioni kontroler za uređaje u polju.

DERMS korisnički interfejs Omogućava nadzor, upravljanje i regulaciju rada distribuiranih izvora električne energije.

4. IMPLEMENTACIJA NAPREDNE KONTROLE PRISTUPA

Bezbjednosni mehanizam pristupa prema oblasti kontrole (eng. *Area Of Responsibility*, skr. AOR) predstavlja koncept podjele odgovornosti prema oblastima, najčešće geografskim, u elektroprenosnoj mreži. Pored AOR-a

implementiran je i prototip sistema za obradu alarma i događaja.



Slika 1. *Model proširenog RBAC modela*

Model kontrole pristupa demonstriran u ovom radu definiše proširenje RBAC modela, koje predstavlja segmente označene plavom bojom na slici 1. Model karakterišu tri tipična tipa aktivnosti u Smart Gridu (AOR OPERS na slici 1): **nadzor** (akcije praćenja stanja elektroenergetske mreže, statusa analognih ulaza, informacija o alarmima), **kontrola** (korektivne akcije manipulisanjem rada pojedinačnih DER-ova,upravljanje alarmnim događajima), **ažuriranje** (modifikacija statičkih podataka o elementima mreže).

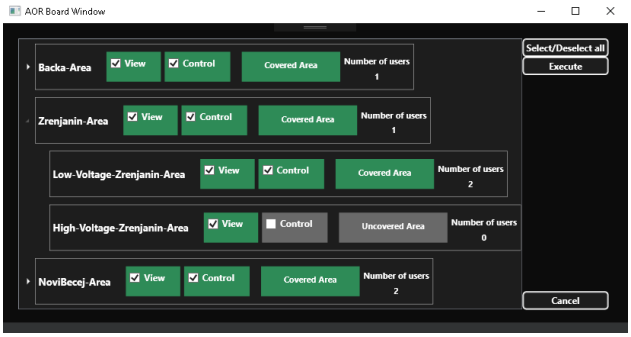
Korisniku (eng. *user*) je moguće pridružiti različite uloge (eng. *role*), od kojih svaka uloga posjeduje određene permisije (eng. *permission*). AOR oblast (eng. *area*) je sačinjena od više AOR grupa (eng. *group*) i poput korisnika posjeduje određene permisije. Operacije koje su sadržane u pripadajućem skupu AOR OPERS se mogu dozvoliti ili ne, u zavisnosti od permisija određene AOR oblasti, koje se porede sa permisijama koje posjeduje ulogovani korisnik aplikacije. Pripadnost objekta (jednog DER-a) određenoj AOR grupi se opisuje atributom objekta, odnosno relacijom „Objects-Groups“. Podaci o mapiranju AOR grupa na distribuirane energetske resurse su sadržani u Network Model servisu.

Cache komponenta je locirana unutar AOR servisa i sadrži podatke o AOR grupama, oblastima, permisijama, ulogama, korisnicima i DER-ovima. Grupa predstavlja logički skup resursa koji su blisko povezani. Skup grupa se organizuje u AOR oblasti. Jedna grupa može biti dio više oblasti i svaka oblast može biti član više grupa. Svakoj oblasti se dodjeljuje skup permisija, koje definišu prava pristupa korisnika. Jednom korisniku može biti povjereno više AOR oblasti, dok svaka AOR oblast može biti dodijeljena na više korisnika. Jednoj AOR oblasti može biti dodijeljen i proizvoljan skup drugih AOR oblasti pa na taj način nastaje hijerahija AOR oblasti. Uloga služi da grupiše određeni broj permisija i dodjeljuje se korisnicima.

Nakon logovanja korisnika se on se *publish-subscribe* mehanizma pretplaćuje na spisak AOR oblasti koje su mu dodijeljene, kako bi dobijao obavještenja kada se dese neke stvari od značaja i to u nekoj od oblasti koje su mu dodijeljene.

AOR Servis Zadužen je za autentifikaciju korisnika sistema. Služi i kao posrednik drugim servisima da dobave podatke iz AOR Cache-a.

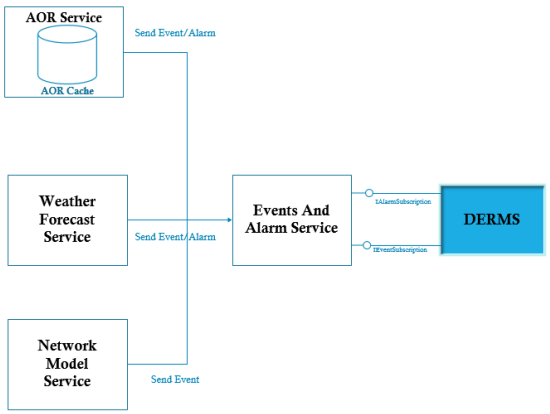
Od dodijeljenih oblasti korisnik može da izabere koje od dodijeljenih oblasti želi da nadgleda (eng. *view*) i/ili kontroliše (eng. *control*), kao što je prikazano na slici 2. Korisniku će biti prikazani samo alarmi i događaji koji se tiču njemu dodijeljenih AOR oblasti (selektovanih za nadzor ili upravljanje), dok će ostale AOR oblasti biti zanemarene.



Slika 2. *Hijerarhijski prikaz AOR oblasti*

4.3 Servis za obradu događaja i alarma

Predstavlja centralizovanu komponentu koja u sistemu agregira događaje od značaja. Funkcionisanje zasniva na mehanizmu pretplate i objave (eng. *publisher-subscriber*). Arhitektura sistema sa dodatim alarmima i događajima je prikazana na slici 3. Nakon što se korisnik pretplati na njemu dodijeljene AOR oblasti, servis čuva njegov kanal za kasnija obavještenja.



Slika 3. *Arhitektura sistema sa dodatim alarmima i događajima*

4.3.1 Obrada događaja - Event-a

Događaji mogu biti različitog tipa, obavještenje kada se uloguje novi korisnik koji ima dodijeljenu istu oblast odgovornosti, zatim izdavanja komande za manipulaciju proizvodnje DER-ova ili kada se desi model promocija (primjena novog CIM/XML fajl sa statičkim podacima mreže).

4.3.2 Obrada alarmantnih događaja - Alarma

Alarmantna notifikacija će biti poslata korisniku ukoliko nijedan korisnik (operater) u tom trenutku ne kontroliše navedenu oblast, a trenutno mu je dodijeljena.

U slučaju alarma da je jedna od oblasti ostala nepokrivena, odnosno bez nadzora, korisnik sa ulogom „Administrator“ može ručno izabrati iz liste aktivnih operatera jednog od njih i dodijeliti mu nepokrivenu oblast.

5. TESTIRANJE NAPREDNE KONTROLE PRISTUPA U OKVIRU SMART GRID APLIKACIJE

Model prezentovan u ovom radu je verifikovan simuliranjem na testnom sistemu, tj. simulirano je uprošćeno Smart Grid okruženje koje sadrži obnovljive izvore električne energije. Zbog praktičnih razloga, funcionisanje dinamičnog i kompleksnog kritičnog infrastrukturnog sistema, kao što Smart Grid svakako jeste, korišćena je simulacija segmenta njegovog rada. Korisnik, u zavisnosti od privilegija koje posjeduje, može komandovati povećanjem ili smanjenjem aktivne ili reaktivne snage određenog segmenta mreže. U simuliranom okruženju je integrisan servis koji vrši kontrolu pristupa, koja se bazira na predstavljenom modelu.

Na osnovu dostupne stručne literature moglo bi se zaključiti da postojeći modeli ne mogu na adekvatan način odgovoriti na aktuelne zahtjeve koji se postavljaju u elektroenergetskoj industriji. Prilikom donošenja odluke o pristupu nekim resursima ABAC model daje mogućnost uvažavanja velikog broja atributa koje treba uzeti u razmatranje. Ipak, ABAC model nije prihvatljiv uslijed definisanja velikog broj autorizacionih pravila, jer Smart Grid obuhvata na hiljade korisnika i opreme. Osim toga, u toku izvršavanja, kada se vrši izračunavanje vrijednosti autorizacionih pravila može doći do ozbiljne degradacije performansi sistema. Takva degradacija performansi u kritičnom sistemu Smart Grida nije prihvatljiva.

Tabela 1 prikazuje skup korisnika sistema sa pripadajućim ulogama i AOR-ima (skraćenice **O**-oblast, **N**-nadzor, **K**-kontrola, **A**-ažuriranje). U nastavku će biti prikazane neke prednosti proširenog modela, u odnosu na RBAC model. Model demonstriran u ovom radu će biti označen kao RBAC-U.

Tabela 1. *Skup korisnika sa ulogama i dodijeljenim AOR-ima*

Korisnik	Sesija	Korisnička uloga	O1 – N	O1 - K	O1 - A
Operater1	S1	Operater	✓	✓	x
Operater2	S2	Operater	✓	x	x

Kada se uspostavlja korisnička sesija operateri sistema aktiviraju dodijeljene AOR-e. Stanja sesija su demonstrirana tabelom 2 (skraćenice **O**-oblast, **N**-nadzor, **K**-kontrola, **A**-ažuriranje). U tabeli 2 su prikazani rezultati koji uporedno prikazuju RBAC model, kao i model RBAC-U. Interpretacijom rezultata zaključuje se da nepostojanje permisije uzrokuje i nemogućnost izvršenja akcije.

Kada se analiziraju korisnici koji imaju dodijeljen isti tip uloge, može se primjetiti da klasični RBAC ne podržava mogućnost podjele odgovornosti. RBAC-U omogućuje dodatni nivo kontrole pristupa, u odnosu na RBAC.

Tabela 2. *Uporedni prikaz modela kontrole pristupa*

Korisnik	Sesija	Model kontrole pristupa	N	K	A
Operater1	S1	RBAC	✓	✓	x
		RBAC-U	✓	✓	x
Operater2	S2	RBAC	✓	✓	x
		RBAC-U	✓	x	x

Operateri posjeduju pravo nadgledanja i kontrole samo nad onim dijelom mreže za koji imaju aktivirane AOR-e. (označeno simbolom ✓ u tabeli 2).

6. ZAKLJUČAK

Povećanje broja distribuiranih energetskih resursa (skr. DER) stvara decentralizovaniji elektroenergetski sistem i mijenja tradicionalnu dinamiku između lokalnih sistema distribucije i prenosnog sistema na nivou cijele regije. Informaciona bezbjednost postaje sve veća briga kako u fizičkom, tako i u elektronskom domenu. Sajber napadači se trude da pronađu i zloupotrijebe nedostatke sistema poput Smart Grida, pošto su servisi elektroenergetskog sistema od kritičnog značaja za moderno društvo. S obzirom da RBAC model nije najpogodniji model u kritičnim infrastrukturnim sistemima kao što je Smart Grid, jer npr. ne uvažava parametre koji nisu dio identiteta korisnika, iako oni mogu uticati na dozvolu pristupa određenim resursima.

Prilikom praktične primjene razvijenog modela napredne kontrole pristupa utvrđeno je da se proširenjem RBAC modela upravljanje pametnom mrežom može učiniti efikasnijim i pouzdanijim. Segmentiranjem nadzora, kontrole kao i izmjenama statičkog modela distributivnog sistema dobija se efikasniji način upravljanja kritičnom Smart Grid infrastrukturom. Hijerarhijska organizacija oblasti odgovornosti može da smanji broj oblasti koje je potrebno dodijeliti korisnicima čime se olakšava administracija modela kontrole pristupa.

7. LITERATURA

[1] Rosić D. (2017). Model kontrole pristupa u Smart Grid sistemima. Novi Sad. RS:Faculty of technical sciencs, University of Novi Sad

[2] Borlase, S. (2017). Smart grids: infrastructure, technology, and solutions. CRC press.

[3] Ferraiolo, D., Kuhn, D. R., & Chandramouli, R. (2003). Role-based access control. Artech House.

[4] Ferraiolo, D. F., Gilbert, D. M., Lynch, N. An examination of Federal and Commercial Access Control Policy Needs. 16th National Computer Security Conference. Baltimore, Maryland. 1993.

[5] David F. Ferraiolo and D. Richard Kuhn. (1992) Role-Based Access Controls Reprinted, National Institute of Standards and Technology. 15th National Computer Security Conference Baltimore, pp. 554-563

[6] Fries, S., Falk, R., & Bisale, C. (2017, May). Handling Rolebased Access Control in the Digital Grid. In ENERGY 2017: The Seventh International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies.

[7] D. Rosic, I. Lendak, S. Vukmirovic. (2015). A Role-based Access Control Model Supporting Regional Division in Smart Grid System, Acta Polytechnica Hungarica Vol. 12, No. 7

Kratka biografija:

Dragan Erić rođen je 1994. godine u Zvorniku. Završio je srednju ekonomsku školu JU SŠC u Zvorniku 2013. godine. Osnovne akademske studije završio je 2018. godine na Fakultet tehničih nauka u Novom Sadu. godine.