METODA ZA PROCENU VAŽNOSTI ELEMENATA U OKVIRU MEĐUSOBNO ZAVISNIH INFRASTRUKTURA

Nataša Gospić[1], Goran Murić[1], Dragan Bogojević[2]
[1]Saobraćajni fakultet Univerziteta u Beogradu
[2]JP Elektroprivreda Srbije, Beograd

Sadržaj: *Poslednjih godina, pitanje bezbednosti i sigurnosti infrastruktura od kojih zavisi funkcionisanje savremenog društva je postalo dominantno i pitanje krit;nih infrastruktura postaje fokus. S obzirom na to da različiti tipovi infrastruktura zavise jedni od drugih i imaju'i u vidu nivoe povezanosti, njihov međusoban uticaj postaje sve kompleksniji. To se posebno odnosi na informacionu infrastrukturu kao ključnu infrastrukturu koja prožima sve ostale i od koje zavise mnogi sistemi, procesi i organizacije. Informaciona infrastruktura se sastoji od velikog broja elemenata različitog tipa: tehnički elementi, ljudi, procesi i sl. tako da njena zaštita podrazumeva interdisciplinaran pristup. Radi procene va\nosti elemenata, u ovom radu, korišćen je pristup modelovanju infrastrukture kao jedinstvene mreže sastavljene od velikog broja elemenata (čvorova) i odnosa među elementima (linkova). Predlo\en je hibridni IENIP metod koji mo\e da se koristi za odre]ivanje va\nosti elemenata povezanih infrastruktura različitog tipa. Navedeni metod je posebno pogodan za složene sisteme kao [to je sistem za prenos i distribuciju električne energije, koji se sastoje od više različitih podsistema (Elektro enegretske mreže i telekomunikacione mreže)*

Ključne reči: *kritična infrsatruktura, kritična informaciona infrastruktura, IENIP metod, hibridni IENIP metod*

1. Uvod

Kritična infrastruktura predstavlja fizičke i sajber sisteme[1] koji su neophodni za minimum operacija u državnoj upravi i ekonomskom sektoru. Ovi sistemi su tako

[1] Jasna razlika između fizičke bezbednosti i sajber bezbednosti se ne može uvek precizno identifikovati. Na primer, fizičke komponente elektro-energetskog sistema čine elektro centrale, transformatori i električni vodovi. Računarski hardver koji je deo sistema i koji se koristi za kontrolu proizvodnje i distribucije električne energije se može posmatrati i kao fizički i kao sajber segment. Podaci koji se prenose kroz informacioni sistem koji koristi elektro-energetska kompanija, kao i softver za upravljanje se smatra sajber segmentom. Fizička bezbednost obično podrazumeva zaštitu fizičkih sredstava (uključijući i računarski hardver) od oštećenja izazvanim fizičkim silama kao što su eksplozije, udar groma, vatra. Sajber-bezbednost obično podrazumeva zaštitu i fizičkih i sajber elemenata od fizičke štete ili štete nastale neovlašćenim pristupom operativnom softveru i podacima. Obezbeđivanje kritične infrastrukture obično zahteva kombinaciju fizičkih i sajber mera (od instalacije ograde do instalacije zaštitnog softvera)

značajni, da bi njihovo onesposobljavanje ili uništenje imalo veoma negativan uticaj na odbrambenu moć ili ekonomiju zemlje. [1-3]

U poslednjoj dekadi načinjeni su značajni koraci da se elementi kritične infrastrukture analiziraju sa aspekta rizika i pripreme za događaje koji mogu omesti njihov rad kroz izradu planova zaštite, tako da se ublaži ugroženost sistema na svim nivoima (regionalni, nacionalni i lokalni). Ipak, strategije koje su usmerene ka uspešnoj prevenciji krajnje negativnih scenarija (terorističkih napada ili prirodnih katastrofa većih razmera) iako veoma efikasne, ne moraju da znače da je izvršena optimalna alokacija resursa koji su potrebni za zaštitu. Ovo veoma složeno pitanje nivoa ugroženosti predstavlja veliki izazov za pravilno planiranje odgovora na prirodne ili druge nepogode.[4]

Sa obzirom na to da kritične infrastrukture pokazuju visok stepen povezanosti i međuzavisnosti, razvijeni su modeli koji za svoju osnovu imaju teoriju mreža. Na osnovu tih modela, u ovom radu predstavljen je jedan metod zaštite povezanih kritičnih infrastruktura.

2. Teorija mreža i modelovanje kritične infrastrukture

Koncept teorije mreža je da pomogne u kreiranju modela mreža koje već postoje u stvarnom svetu i da opiše njihov oblik i funkciju. Teorija mreža je korišćena za ispitivanje širokog spektra sistema [5] kao što su društvene mreže, tehničke mreže (Internet, elektro-mreže, mreže mobilne telefonije), kao i za ispitivanje pisanog i govornog jezika kod ljudi. Za teoretsko razmatranje tehničkih sistema obično se modeluju samo osnovne karakteristike date mreže, i u principu se izbegava uključivanje drugih aspekata složenih sistema. To podrazumeva da se složeni sistem infrastrukturnih elemenata svede na mrežu koja ima relativno jednostavne odnose (linkove) između čvorova, iako njihovi odnosi mogu biti prilično kompleksni.

Uzimajući u obzir prethodno opisanu međuzavisnost kod infrastruktura, dolazimo do zaključka da se iste mogu predstaviti u obliku mreže, gde pojedini elementi infrastrukture predstavljaju čvorove, a odnosi (zavisnosti) među njima linkove date mreže.

Ideja koja stoji iza koncepta korišćenja teorije mreža u modelovanju kritičnih infrastruktura je da je moguće izvući korisne zaključke o datom sistemu samo na osnovu poznavanja topologije, koja je predstavljena u obliku grafa. Merenjem različitih kvantitativnih osobina mreže, posebno u slučajevima kada se topologija ili osobine čvorova menjaju, može se doći do saznanja o važnosti pojedinih čvorova ili segmenata mreže.

Inicijalni problem kod ovakve vrste modelovanja kritičnih infrastruktura jeste određivanje elemenata, jer treba razumeti da nisu svi elementi kritične infrastrukture sami po sebi kritični, a i oni koji su kritični nemaju isti nivo važnosti.

Sa obzirom na to da ni jedan složeni sistem u okviru nacionalne ili regionalne infrastrukture nije isključivo tehnički [6], ni elementi koje treba uzeti u obzir za zaštitu ne treba da budu samo tehnički. Većina metodologija razvijenih u svrhu definisanja kritičnih elemenata kritičnih infrastruktura, generalno ne uključuju društvenu i organizacionu komponentu u okviru analize fizičkih sistema.[7] Bez obzira na veličinu sistema, oni se sastoje od različitih tipova elemenata koje obično možemo podeliti u tri grupe: fizičke, sajber i ljudske. [8]

Pod fizičkim elementima podrazumevamo postrojenja, tj. prostorije ili zgrade u kojima se elementi nalaze. Sajber elementi su uređaji i softveri koji služe za obavljanje misije infrastrukture, dok su ljudski elementi osobe odgovorne za svakodnevno funkcionisanje infrastrukture. Svi ovi elementi su međuzavisni i sa aspekta analize se ne mogu posmatrati potpuno odvojeno iako je pristup zaštiti ovih grupa drugačiji.

Svaki od ovih elemenata, bez obzira na tip, predstavlja čvor u mreži, a međuzavisnosti se mogu modelovati vezama među čvorovima koje mogu imati težinski faktor koji predstavlja nivo međuzavisnosti. U najednostavnijem slučaju težinski faktor je jedan i svi elementi podjednako i maksimalno utiču jedni na druge. [9] Međutim, u nekim radovima isključivo se bave tehničkim sistemima, pri tom ne uzimajući u obzir ljudski faktor [10], dok se u drugim radovima uzima u razmatranje i ljudski faktor i uloga ljudi u okviru tehničkih sistema [11].

Koncept mera centraliteta

Sa metodološkog aspekta, matematičko modelovanje korišćenjem teorije mreža je predloženo u mnogim metodama modelovanja kritičnih infrastruktura [7]. U ovim metodama, teorija mreža se koristi da se opišu različiti sistemi, od informacionih i telekomunikacionih do sistema operatora distribucionog sistema ili transportne infrastrukture.

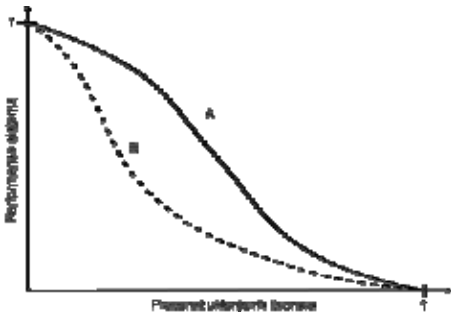
Da bi se procenili različiti potencijalni scenariji napada i njihovi uticaji na funkcionisanje stvarnih mreža u većini metoda se koriste mere centraliteta. Mera centraliteta je osnovni koncept u analizi mreža još od prvog pojavljivanja u oblasti sociologije [12]. Mere centraliteta služe da opišu mrežu i njene osobine. Uklanjanjem čvorova (nasumično ili po nekom pravilu) i istovremeno mereći osobine mreže, možemo da odredimo u kom slučaju je uklanjanje imalo najsnažniji, odnosno najdegradirajući uticaj na mrežu.

Autori [13] ovakav pristup proceni otpornosti mreže nazivaju dinamika mrežnog modela. Postoji veliki broj mogućih strategija napada koje su uglavnom zasnovane ili na određenom nasumičnom principu ili na principu koji koristi već poznate mere u okviru mreže i utiče samo određene čvorove i to po određenom redosledu. Važnost određenog čvora se meri nekom merom centraliteta koja važi za celu mrežu. Mera centraliteta se uglavnom odnosi na neku globalnu osobinu mreže kao na primer prosečno inverzno geodetsko rastojanje (eng. average inverse geodesic length)[2] [14] koje se računa sukcesivno nakon svakog koraka napada. Pored prosečnog inverznog geodetskog rastojanja mogu se koristiti druge mere poznate u teoriji mreža kao što su globalna efikasnost mreže (eng. global efficiency of the network), veličina najvećeg povezanog podgrafa (eng. size of the largest connected subgraph), prečnik mreže (eng. diameter of the network) i sl. [15]

Na slici 1 je dat primer jednog ovakvog pristupa u proceni otpornosti mreže. Globalna efikasnost mreže, koja se meri, ima zadatak da prikaže performanse mreže u

[2] Slu i da opi e u kojoj meri su povezani parovi čvorova u mre i. N je broj čvorova, a $d(v,w)$ je rastojanje, tj. du ina najkraće putanje između čvorova v i w. - $l^{-1} = \frac{1}{N(N-1)} \sum_{v \neq w} \frac{1}{d(v,w)}$

slučajevima različitih strategija napada. Mereći performanse date mreže u toku različitih vrsta napada, možemo doći do korisnih informacija o njenoj otpornosti.



Slika 1. *Merenje performansi sistema tokom simulacije napada na mrežu* [13]

Na slici 1 na vertikalnoj osi je predstavljen nivo performanse sistema meren u datom vremenskom trenutku, dok je na horizontalnoj osi predstavljen procenat uklonjenih čvorova. Krive A i B predstavljaju nivo performanse sistema za dve različite strategije napada. Sa obzirom na to da peroformanse naglo opadaju u slučaju B, zaključujemo da je mreža otpornija u slučaju napada A.

3. Modelovanje različitih mrežnih sistema u procesu zaštite

Kao što je ranije navedeno, teorija mreža se može koristiti u modelovanju različitih vrsta kritičnih infrastruktura. Ipak ne modeluju se sve infrastrukture na isti način, tj. postoje posebni modeli za različite vrste infrastruktura, a koji će biti korišćen zavisi od prirode elemenata, kao i od funkcionalne zavisnosti među njima.

Autori su razmatrali slučaj kompanije koja se bavi distribucijom električne energije, pa je u ovom radu predstavljen metod koji se koristi za zaštitu dva tipa infrastrukture: elektroenergetsku (EE) mrežu i telekomunikacionu mrežu u okviru kompanije. U ovom radu predstavljen je hibridni metod koji omogućava procenu elemenata ovakvih heterogenih infrastruktura tj. infrastruktura sastavljenih od različitih tipova elemenata za čije modelovanje su neophodni različiti pristupi.

U prethodnoj deceniji studije sistema za distribuciju električne energije koje koriste teoriju mreža postale su veoma popularne, zbog velikog broja otkaza sistema i štete koju takvi otkazi prouzrokuju. Crucitti i Latora sa koautorima su imali značajne doprinose u oblasti teorije mreža u pogledu analize tehničkih sistema. Generalno, njihov rad se zasniva na analizi kaskadnih otkaza u kompleksnim mrežama i distribuciji opterećenja kroz date sisteme [16]. Isti autori su analizirali i prosečnu efikasnost mreže kao meru performansi u ispitivanju kako EE mreže, tako i komunikacionih mreža [17]. Time su uspeli da definišu kritične vodove u visokonaponskoj/srednjenaponkoj mreži. Iako predloženi model ima veliki potencijal i može se iskoristiti za mnoge primene, ipak je previše generalizovan i uglavnom ograničen na specifične mreže za distribuciju električne energije.

Više autora je radilo na modelovanju komunikacionih mreža iz perspektive zaštite od nasumičnih ili planiranih otkaza. Crucitti je analizirao mrežne komunikacione sisteme koristeći istu teoriju kao za mreže za distribuciju električne energije[17] i na taj

način pokazao primenjivost teorije mreža u različitim oblastima. Latora i Marchiori su razvili metod za identifikaciju kritičnih elemenata jezgrene internet mreže [18]. Nezavisno od njih, mnogi drugi autori su analizirali ranjivosti različitih tipova komunikacionih mreža, koristeći različite metode, od čega se najviše koristi princip simulacije otkaza i merenja performansi mreže tokom vremena u kom se otkazi događaju.

U svojim ranijim radovima, autori su predstavili pristup za procenu važnosti elemenata u procesu zaštite kritične infrastrukture [19, 20] nazvanog IENIP (eng. Importance of Elements in Networked Infrastructure Protection). Ovaj pristup se zasniva na osobini posmatranih mreža kod kojih se određeno stanje čvora može prenositi dalje na susedne čvorove.

U okviru zaštite umreženih elemenata kritične infrastrukture, neophodno je obratiti pažnju na prirodu same mreže. Kao što je ranije navedeno, infrastrukture su podložne kaskadnom efektu, tj. sukcesivnim otkazima većeg broja elemenata.

IENIP metod koristi teoriju mreža da bi odredio najbitnije čvorove date mreže. Polazi od pretpostavke da je najbitniji čvor onaj koji posredno ili neposredno ima uticaj na najveći broj čvorova u mreži. Metod obuhvata tri koraka i primenjuje se za mreže koje su samostalne u svom funkcionisanju, tj. kod infrastruktura istog tipa: *definisanje mreže*, *identifikacija najdužih puteva između svih parova čvorova*, *identifikacija najbitnijih čvorova.*

U slučajevu infrastruktura koje obuhvataju više tipova mreža sa različitim funkcijama i u međusobnoj interakciji, potrebno je modifikovati predloženi metod u tzv. "hibridni IENIP metod".

4. Hibridni IENIP metod

U velikim sistemima kao što su sistemi prenosa i sistemi distribucije električne energije, veliki broj elemenata komunicira i zavisi jedan od drugog. U jednom takvom sistemu funkcionišu podsistemi različitih priroda (sistem distribucije električne energije se po mnogim osobinama razlikuje od telekomunikacionog sistema) koji nisu nezavisni, tj. podsistemi utiču jedni na druge i zavise jedni od drugih. Takav scenario usložnjava problem, jer ne možemo koristiti jedan model za opis celokupnog sistema, već se različiti modeli moraju kombinovati u zavisnosti od toga koji podsistem se posmatra i u kojoj meri taj podsistem utiče na ostale.

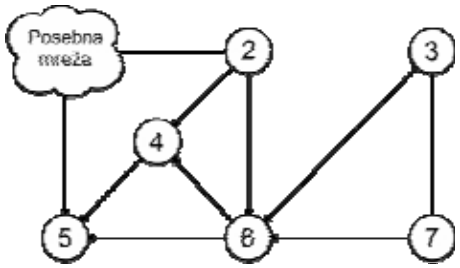
Infrastrukturni sistemi koje posmatramo predstavljaju mreže sastavljene od elemenata različitih tipova (fizički, ljudski, sajber…), tako da element može biti trafo stanica, upravnik sektora, ruter, server i sl. Različite mreže u okviru složenog sistema se na sebi svojstven način ponašaju u slučaju napada tj. otkaza pojedinih elemenata. To je osnovni razlog zbog koga je neophodno svaku od ovih mreža analizirati pojedinačno koristeći različite metode. Drugi razlog za uvođenje hibridnog metoda je potencijalna nemogućnost uvida u stanje nekog dela mreže. Na primer, deo mreže može biti tajan i nepoznat analitičaru[3] ili je analizu neophodno uraditi za kratko vreme i uz ograničena finansijska sredstva.

U ovim slučajevima, analizi značajnosti elemenata mreže možemo pristupiti koristeći princip crne kutije, tj. ne ulazeći u detaljnu analizu segmenata mreže, već posmatrajući date segmente kao jedinstvene elemente. Naravno, ovako uvedene nove

[3] Pod pojmom „analitičar" podrazumevamo osobu ili tim stručnjaka koji za zadatak ima da za titi kritičnu infrastrukturu.

elemente treba razlikovati od već definisanih elemenata iste mreže. Time se dolazi do hibridnog metoda kojim se, u odnosu na IENIP metod, čvorovima dodeljuju težine koje određuju važnost ovih elemenata koja je ranije prepoznata.

Na slici 2 je predstavljena ilustracija hipotetičke mreže koju ispitujemo.

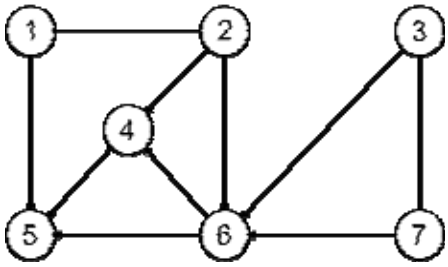


Slika 2. *Ilustracija hipotetičke mreže u okviru kritične infrastrukture*

Ceo postupak se sada svodi na četiri koraka:

Prvi korak – Enkapsulacija

Sa obzirom na to da je jedan deo mreže nepoznat ili ne želimo da ga detaljno ispitujemo u datom trenutku, njega posmatramo kao posebnu celinu i svodimo ga na nivo elementa. U ovom slučaju, ceo segment mreže koji je, u suštini, posebna mreža, svodimo na jedan čvor (Slika 3).



Slika 3. *Posebna mreža je predstavljena kao jedan čvor*

Drugi korak – Definisanje mreže

Mreža elemenata u okviru kritične infrastrukture ima N čvorova i K linkova. Graf koji se dobija preslikavanjem mreže se može opisati matricom pripadnosti A (izraz 1), čiji elementi a_{ij} su jednaki jedinici u slučaju da postoji link između i i j.

$$A = \begin{bmatrix} 0 & 1 & - & - & 1 & - & - \\ 1 & 0 & - & 1 & - & 1 & - \\ - & - & 0 & - & - & 1 & 1 \\ - & - & - & 0 & 1 & - & - \\ - & - & - & - & 0 & - & - \\ - & - & - & 1 & 1 & 0 & - \\ - & - & 1 & - & - & 1 & 0 \end{bmatrix} \quad (1)$$

Treći korak – Identifikacija ruta

U trećem koraku identifikujemo najduže rute između svih parova čvorova, koje predstavljaju kritične puteve. Postoji više algoritama na osnovu kojih možemo doći do rešenja ovakvog problema. Možemo koristiti algoritam koji je razvio Pollack 1961 godine [21] ili njegovo unapređenje koje je predstavio Yen 10 godina kasnije. [22] Svi se zasnivaju na varijacijama algoritama koji rešavaju problem pronalaženja najkraćih ruta kao što su "Floyd-Warshall", "Bellman-Ford" ili "Dijkstra". [23-26] Rezultat možemo predstaviti u obliku 2 matrice. Prva je matrica *D* (Izraz 2) koja predstavlja dužine najdužih puteva između svih parova čvorova, gde je d_{ij} najduži put između čvora *i* i *j*. Druga matrica *Q* (Izraz 3) sadrži informacije o najdužoj ruti, gde je q_{ij} prvi prethodnik čvora *j* u ruti od *i* do *j*.

$$D = \begin{bmatrix} 0 & 1 & - & 3 & 4 & 2 & - \\ 1 & 0 & - & 2 & 3 & 1 & - \\ - & - & 0 & 3 & 4 & 2 & 1 \\ - & - & - & 0 & 1 & - & - \\ - & - & - & - & 0 & - & - \\ - & - & - & 1 & 2 & 0 & - \\ - & - & 1 & 3 & 4 & 2 & 0 \end{bmatrix} \quad (2) \qquad Q = \begin{bmatrix} - & 1 & - & 6 & 4 & 2 & - \\ 2 & - & - & 6 & 4 & 2 & - \\ - & - & - & 6 & 4 & 7 & 3 \\ - & - & - & - & 4 & - & - \\ - & - & - & - & - & - & - \\ - & - & - & 6 & 4 & - & - \\ - & - & 7 & 6 & 4 & 3 & - \end{bmatrix} \quad (3)$$

Posmatrajući matricu *D*, i uzimajući u obzir izraz $i_{first} = i\,[\max\{(\sum_j \equiv \{d_{ij}\})\}]$, gde je i_{first} čvor najvećeg značaja, dolazimo do rešenja koje kaže da su najbitniji čvorovi u mreži podjednako čvorovi 1, 3 i 7. Za njima slede čvorovi 2, 6, 4 i 5 respektivno.

Četvrti korak – Dodeljivanje težina i identifikacija najbitnijih čvorova

Elementi nastali enkapsulacijom su po prirodi stvari značajni, jer mogu da predstavljaju zasebne mreže koje dalje čine veće delove sistema. Iz tog razloga, takve elemente ne možemo posmatrati na isti način kao i ostale elemente u mreži koju ispitujemo. Takvim elementima se pridaje posebna pažnja i određuje se mera koja predstavlja težinu elementa. U slučaju da element predstavlja veliki segment mreže, tj. posebnu podmrežu koja zavisi i koja utiče na mrežu koju posmatramo, dodeljeni težinski faktor treba da bude dovoljan da uvaži značajnost elementa. Analitičar je taj koji treba da odredi koja se težina dodeljuje tom elementu. Na primer, ako posmatramo sistem za distribuciju električne energije, on se najčešće sastoji od više mreža različitog tipa koje funkcionišu zajedno, kao što su komunikaciona mreža za prenos podataka i mreža za prenos energije. Ako posmatramo mrežu za prenos električne energije kao primarnu,

onda celu mrežu za prenos podataka treba da enkapsuliramo u zavistan element, kome će biti pridružen veliki težinski faktor.

Prethodno dobijene matrice modifikujemo uzimajući u obzir dodeljeni težinski faktor. Modifikacija se vrši na sledeći način: posmatramo matricu Q i notiramo sve elemente matrice gde se pojavljuje element mreže kome je dodeljen težinski faktor W_n, tj. identifikujemo sve najduže puteve gde se pojavljuje enkapsulirani element. Zatim modifikujemo matricu D tako što na odgovarajuće elemente matrice dodamo vrednost težinskog faktora i dobijamo D_1 (Izraz 4), tako da $d_{1ij} = d_{ij} + w_n$, za svako i i j gde je $q_{ij} = n \vee q_{ij} = n$

Gde je:

- d_{ij} element matrice D,
- w_n težinski faktor za element mreže n
- q_{ij} element matrice Q
- n enkapsulirani element mreže

Na ovaj način, težinski faktor čvora konvertujemo u veličinu koja u ovoj metodi ima odlučujuću ulogu, a to je dužina puta. U primeru koji je naveden, enkapsulirani element je čvor 1 i njemu treba dodeliti veliki težinski faktor. Kao što je već navedeno, vrednost težinskog faktora zavisi od odluke analitičara, ali u slučaju da je podmreža veoma važna, taj faktor ne bi trebalo da bude manji od vrednosti najduže rute u posmatranoj mreži. Čvoru 1 dodeljujemo težinski faktor 4 i dobijamo matricu D_1.

$$D_1 = \begin{bmatrix} 4 & 5 & 4 & 7 & 8 & 6 & 4 \\ 5 & 0 & - & 2 & 3 & 1 & - \\ - & - & 0 & 3 & 4 & 2 & 1 \\ - & - & - & 0 & 1 & - & - \\ - & - & - & - & 0 & - & - \\ - & - & - & 1 & 2 & 0 & - \\ - & - & 1 & 3 & 4 & 2 & 0 \end{bmatrix} \quad (4)$$

Posmatrajući dobijenu matricu D_1, po formuli $i_1first = i \mid \max\left(\left(\sum_j \left(d_{1ij}\right)\right)\right)$ možemo izvesti novi redosled značajnosti čvorova. Najbitniji čvor postaje čvor 1, zatim ga sledi čvor 2, a nakon njih svi ostali.

5. Zaključak

U ovom radu je započeta primena Hibridnog IENIP metoda na umrežene kritične infrastrukture, sa posebnim naglaskom na sisteme za prenos i distribuciju električne energije koje u sebi imaju kompleksne komunikacione mreže. U najjednostavnijem slučaju sekundarne mreže se tretiraju kao čvor, ali u praksi one sadrže najmanje stotine komunikaconih puteva (linkova) koje povezuju desetine energetskih objekata (npr. trafostanica) sa centrima upravljanja u kojima postoje različita upravljačka (SCADA sistemi) i komunikaciona oprema (SDH/DWDM uređaji za sisteme prenosa, oprema za paketski prenos podataka, WAN i LAN mreže u organizacionim jedinicama), sistemski i aplikativni softver, sistemi za nadzor i upravljanje i sl. Zato će jedan od pravaca daljeg istraživanja biti usmeren ka određivanju reprezentativnog skupa elemenata

u komunikacionoj (ili elektroenergetskoj) mreži elektrodistributivnih kompanija koji su najvažniji u kritičnoj infrastrukturi.

Zahvalnost:

Ovo istraživanje je deo projekta "Upravljanje kritičnom infrastrukturom za održivi razvoj u poštanskom, komunikacionom i Železničkom sektoru Republike Srbije", podržanog od strane Ministarstva prosvete, nauke i tehnološkog razvoja u okviru naučnih istraživačkih projekata 2011-2014, Telekoma Srbije, Pošte Srbije i Železnice Srbije.

Literatura

[1.] Utilities, T.I.o.P., *Technical Assistance Briefs: Utility and Network Interdependencies: What State Regulators Need to Know*. 2005, The National Association of Regulatory Utility Commissioners.
[2.] Clinton, W.J., *Executive Order 13010*. 1996.
[3.] Clinton, W.J., *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive No. 63*. 1998.
[4.] Nataša Gospić, Goran Murić, and Dragan Bogojević, *Definisanje kritične telekomunikacione infrastrukture u Srbiji*, in *PosTel 2012 - XXX Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju*. 2012: Beograd.
[5.] Albert, R. and A.-L. Barabasi, *Statistical mechanics of complex networks*. Reviews of modern physics, 2002. **74**.
[6.] Bea, R., et al., *A new approach to risk: The implications of E3* Risk Management, 2009. **11**(1): p. 30-43.
[7.] Solano, E., *Methods for Assessing Vulnerability of Critical Infrastructure*. 2010, Institute for Homeland Security Solutions.
[8.] Schaffer, G., T.M. Keil, and R. Mayer, *Communications Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*. 2010, Homeland Security.
[9.] Murić, G., et al. *Jedan pristup zaštiti kritične infrastrukture*. in *Konferencija o bezbednosti informacija BISEC 2013*. 2013.
[10.] Jönsson, H., J. Johansson, and H. Johansson, *Identifying Critical Components in Technical Infrastructure Networks.* Journal of Risk and Reliability, 2008. **222**: p. 235-243.
[11.] Wilhelmsson, A. and J. Johansson. *Assessing Response System Capabilities of Socio-Technical Systems*. in *The International Emergency Management Society (TIEMS2009)*. 2009. Istanbul, Turkey.
[12.] Crucitti, P., V. Latora, and S. Porta, *Centrality measures in spatial networks of urban streets.* Physical Review E, 2006. **73**.
[13.] Johansson, J., *Risk and Vulnerability Analysis of Interdependent Technical Infrastructures: Addressing Socio-Technical Systems*, in *Industrial Automation Department of Measurement Technology and Industrial Electrical Engineering, Faculty of Engineering, LTH* 2010, Lund University: Lund, Sweden. p. 189.
[14.] Latora, V. and M. Marchiori, *Efficient Behavior of Small-World Networks.* Physical Review Letters, 2001. **87**(19).
[15.] Johansson, J., H. Jönsson, and H. Johansson, *Analysing the vulnerability of electric distribution systems: a step towards incorporating the societal consequences of disruptions.* Int. J. Emergency Management, 2007. **4**(1).
[16.] Crucitti, P., V. Latora, and M. Marchiori, *Model for cascading failures in complex networks.* Rapid Communications, 2004.

[17.] Crucitti, P., et al., *Efficiency of scale-free networks: error and attack tolerance.* Physica A, 2003. **320**: p. 622-642.
[18.] Latora, V. and M. Marchiori, *Vulnerability and protection of infrastructure networks.* Physical Review E, 2005. **71**.
[19.] Murić, G., et al. *An Approach to Assess Criticality of Elements in the Process of Information Infrastructure Protection*. in *International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services - TELSIKS*. 2013. Niš, Serbia.
[20.] Murić, G., N. Gospić, and M. Šelmić. *Protecting Critical Information Infrastructures by Increasing its Resilience*. in *International conference on Applied Internet and Information Technologies*. 2013. Zrenjanin, Serbia.
[21.] Pollack, M., *The kth Best Route Through a Network.* Operations Research, 1961. **9**(4): p. 578-580.
[22.] Yen, J.Y., *Finding the K Shortest Loopless Paths in a Network.* Management Science, 1971. **17**(11): p. 712-716.
[23.] Floyd, R.W., *Algorithm 97: Shortest Path.* Communications of the ACM, 1962. **5**(6).
[24.] Bellman, R., *On a routing problem.* Quarterly of Applied Mathematics, 1958. **16**.
[25.] Dijkstra, E.W., *A Note on Two Problems in Connexion with Graphs.* Numerische Mathematlk, 1959. **1**.
[26.] Larson, R.C. and A.R. Odoni, *Urban Operation Researches*. 1981, Massachusetts Institute of Technology.

Abstract: *Recently, the security and safety issues in infrastructures became dominant as those infrastructures are essential for modern society functioning and critical infrastructures are in focus. Various types of infrastructures depend on each other, and regarding the level of their interdependency, the mutual influence becomes more complex. That is especially case with information infrastructure, as a key infrastructure to all others and essential for many systems, processes and organizations. Information infrastructure consists of numerous elements of various types: technical, human, business processes and others and its protection demands interdisciplinary approach. In this paper, authors use the concept of infrastructure modeling which considers the infrastructure as network composed of many elements (nodes) and relations among them (links). The hybrid IENIP method used for protection of interdependet infrastructures of different types is proposed. The hybrid method is a variation of authors' proposed IENIP method and is suitable for complex systems such as distribution of electricity, which includes both electrical networks and telecommunication networks.*
Keywords: *critical infrastructure, critical information infrastructure, hybrid IENIP method*

THE METHOD FOR IMPORTANCE OF ELEMENTS ASSESSMENT WITHIN THE INTERDEPENDENT INFRASTRUCTURES

Nataša Gospić, Goran Murić, Dragan Bogojević