



# Simulacija DDoS napada i strategija odbrane korištenjem SimEvents alata

Amer Mujalo

# Motivacija

---

- **Razlog istraživanja:** Razvoj alata za odbranu od DDoS napada.
- **Problem:** Smanjenje ili uklanjanje dostupnosti usluga za legitimne korisnike.
- **Rješenje:** Prepoznavanje devijacija od normalnog ponašanja sistema.
- **Cilj:** Pravovremeno otkrivanje i prevencija DDoS napada.

# Šta je DDoS napad?

---

*"Distribuirani napad uskraćivanja usluge (DDoS) je cyber napad koji cilja na preopterećenje mrežnih resursa ili servera, uzrokujući smanjenje ili potpunu nedostupnost usluga."*

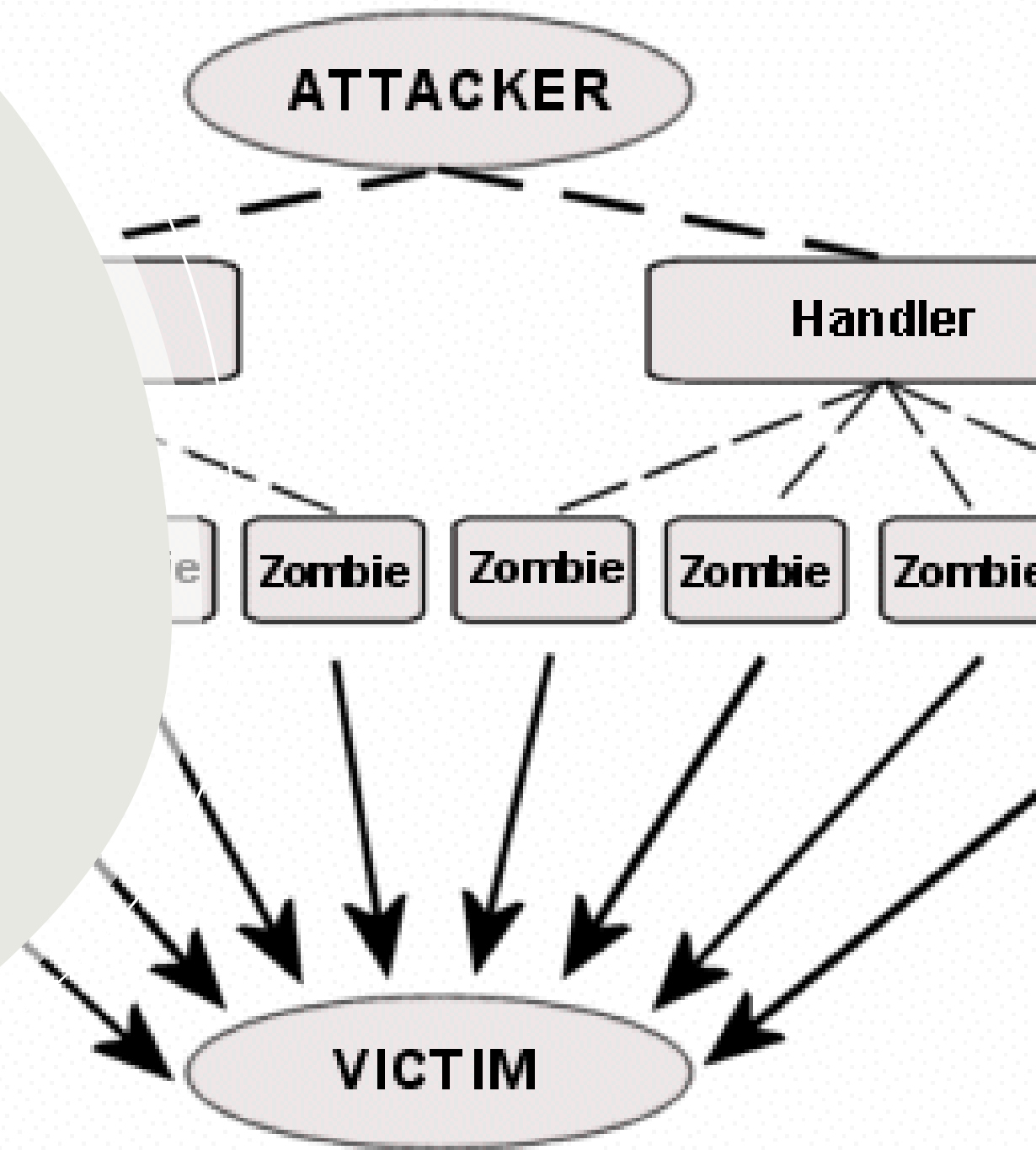
# Komponente DDoS napada

**Napadači:** To su subjekti ili grupe koji planiraju i izvršavaju napade. Njihova uloga je da kreiraju maliciozni softver i kompromituju mrežne uređaje.

**Rukovatelji (Handler):** Ovo su sistemi koje je kompromitirao ili hakirao napadač na mreži, on koristi sumnjive metode za instaliranje DDoS napadačkih alata na njihov sistem.

**Zombie uređaji (Agenti):** Ovo su uređaji čiji su vlasnici nesvjesni da su kompromitovani. Napadači koriste ove uređaje za slanje velikog broja zahtjeva prema ciljanom serveru.

**Žrtva:** Žrtva je server, mrežna infrastruktura ili aplikacija koju napadač želi onemogućiti.



# Metode DDoS napada

**Smurf napad:** Napadač šalje lažnu ICMP echo paket na broadcast adresu ranjivih mreža, što uzrokuje da svi sistemi na mreži odgovore na žrtvu, čime se iscrpljuje propusni opseg mreže i onemogućava pristup legitimnim korisnicima.

## Types of smurf attacks

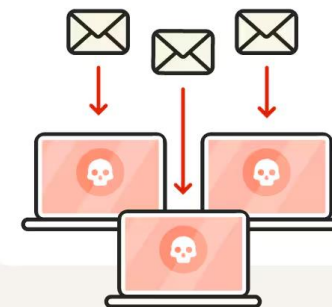
### Basic

Overwhelms a single network with infinite ICMP packets



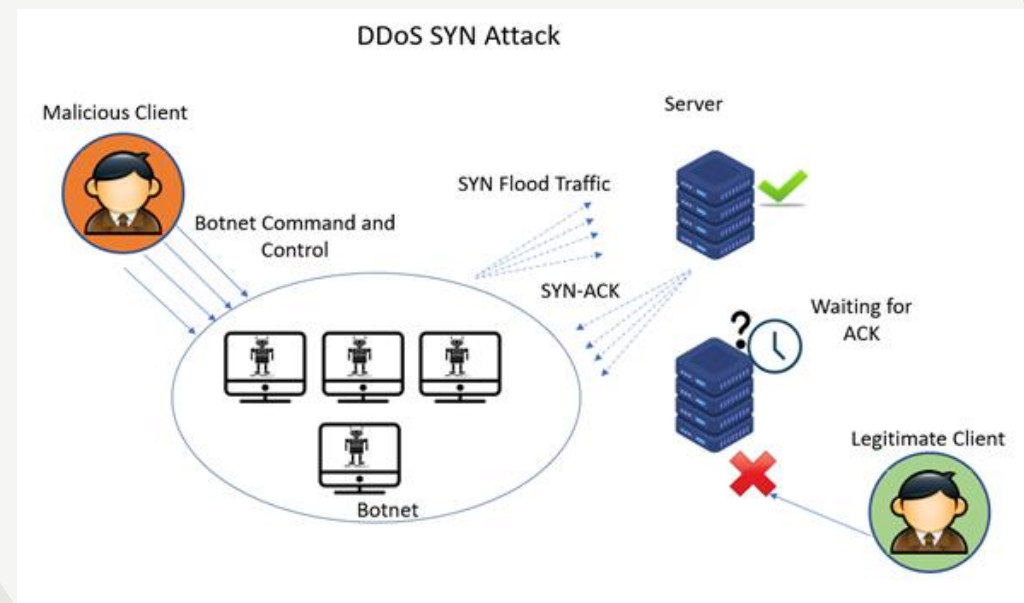
### Advanced

Targets multiple networks simultaneously



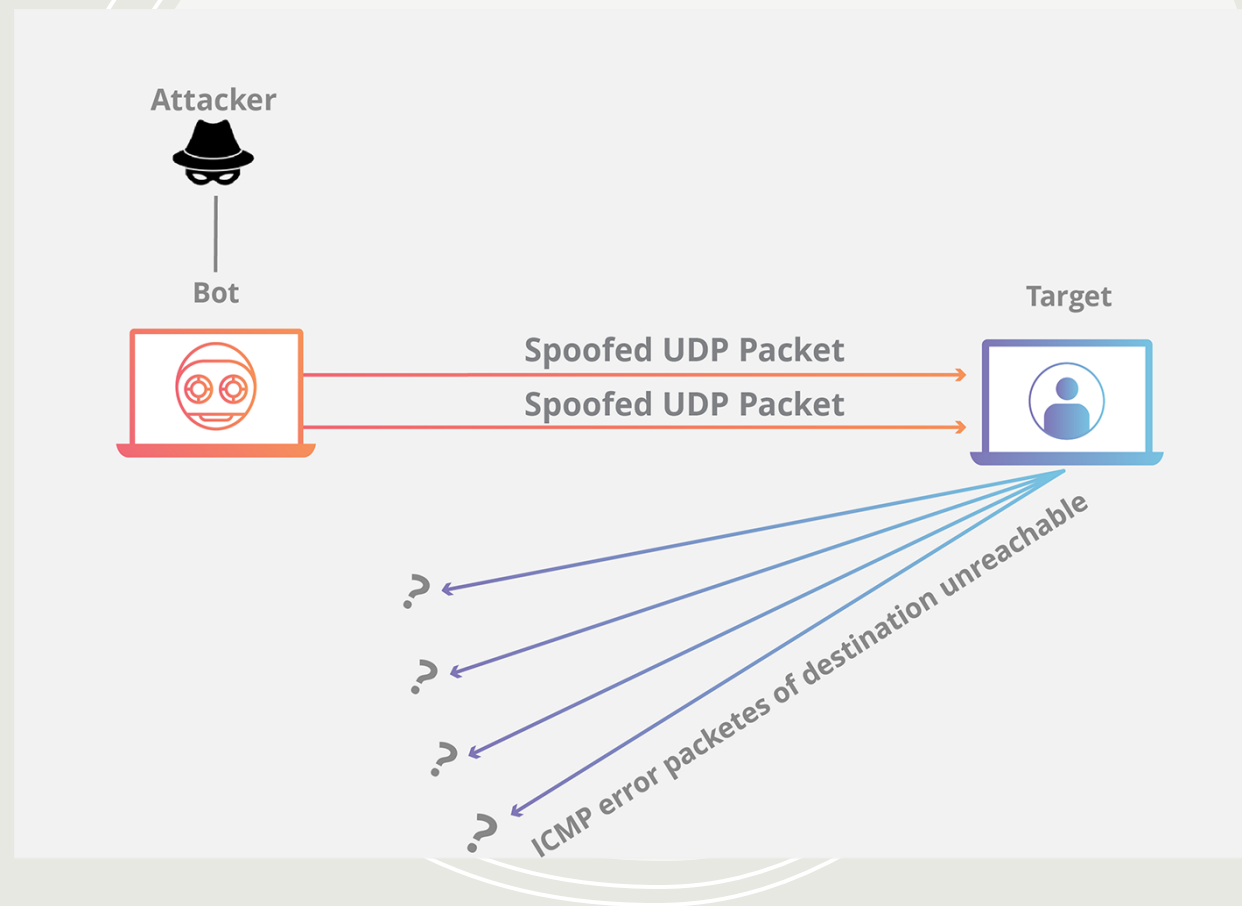
# Metode DDoS napada

**TCP SYN napad:** Napadač iskorištava slabost u TCP trostrukoj vezi slanjem zahtjeva prema serveru s nedostupnim izvorom paketa. Server ne može završiti vezu, što rezultira potrošnjom resursa servera i njegovim eventualnim padom.



# Metode DDoS napada

**UDP napad:** Napadač šalje UDP paket na nasumičnu port adresu na serveru žrtve. Kada server primi paket, pokušava pronaći aplikaciju koja čeka na tom portu. Ako aplikacija nije pronađena, server šalje ICMP paket, što može dovesti do pada sistema ako napadač pošalje dovoljno paketa.




# DDoS napadi u Bosni i Hercegovini

**Napadi na medijske portale** Tokom 2020. i 2021. godine, web stranice poput **Žurnal.info**, **Buka.com** i **Face.tv** bile su mete snažnih DDoS napada koji su ometali njihovo funkcionisanje. Ovi napadi su često povezivani s pokušajima gušenja slobode medija i političkim pritiscima. Također, **Nezavisne novine** su prijavile DDoS napad na njihov portal 10. 08. 2021. godine.



# Struktura modela

**Normalno stanje:** Sistem funkcioniše u optimalnim uslovima. Korisnici šalju zahtjeve serveru u pravilnim vremenskim intervalima. Ti zahtjevi se procesuiraju prema redoslijedu dolaska.



**Stanje napada:** Tokom napada, dodatni zahtjevi dolaze od napadača i zombi uređaja. Ovi zahtjevi preplavljaju server, uzrokujući pad njegove dostupnosti i smanjenje performansi.

# Struktura modela

- Tok simulacije DDoS napada implementira se pomoću alata SimEvents u Simulinku-u. SimEvents je alat koji omogućava modeliranje i simulaciju diskretnih događaja u različitim sistemima. Simulacija obuhvata ključne elemente za modeliranje mreže i napada, omogućavajući praćenje toka podataka od generacije zahtjeva do njihovog procesuiranja na serveru. Ključni elementi simulacije su:

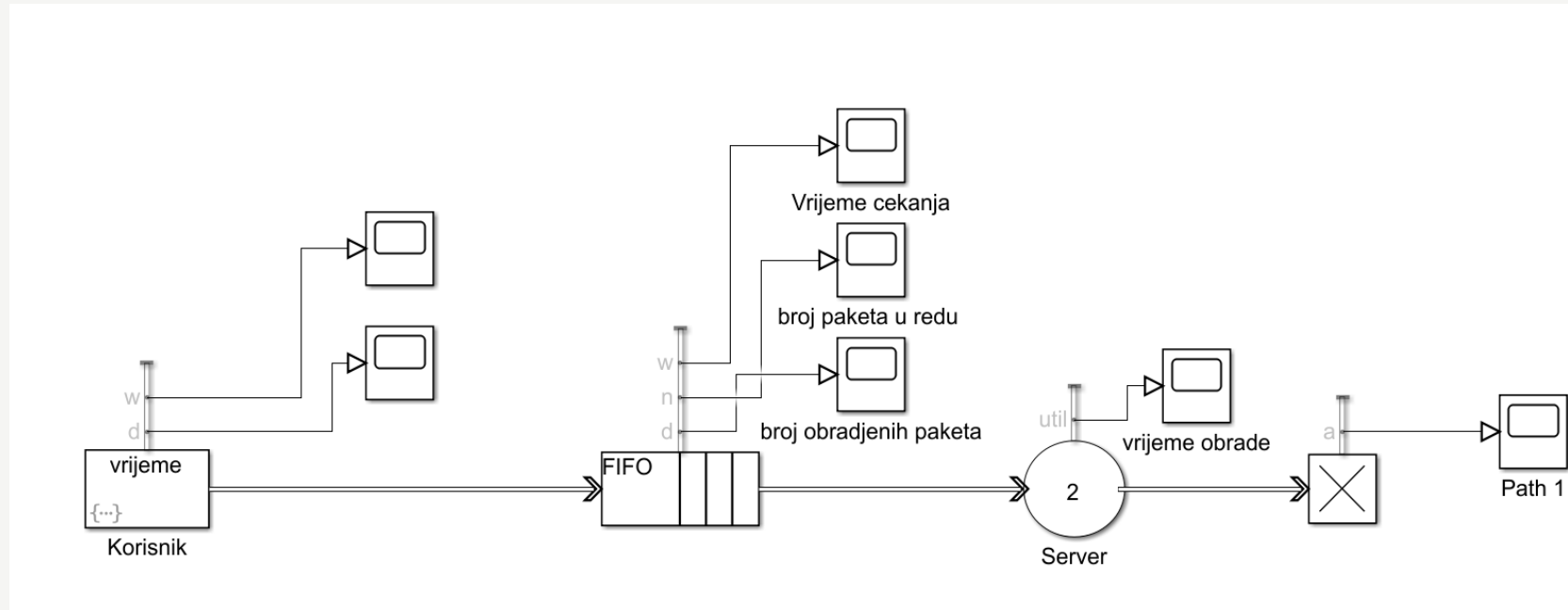
**Generacija entiteta (Entity Generator):** Kreiranje zahtjeva.

**Red za čekanje (Entity Queue):** Upravljanje dolaznim zahtjevima.

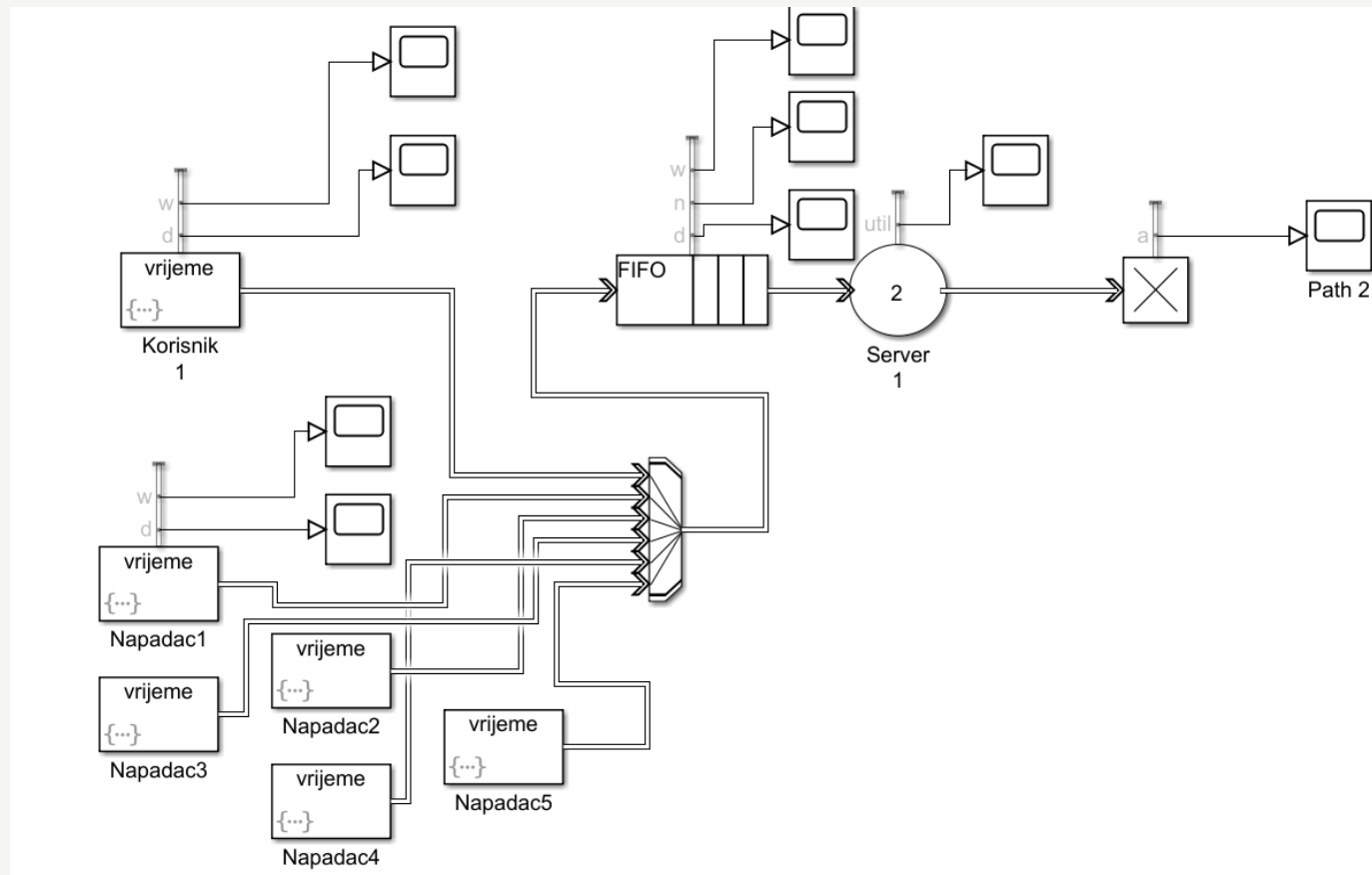
**Server:** Obrada zahtjeva.

**Entity terminator:** Završavanje obrade entiteta.

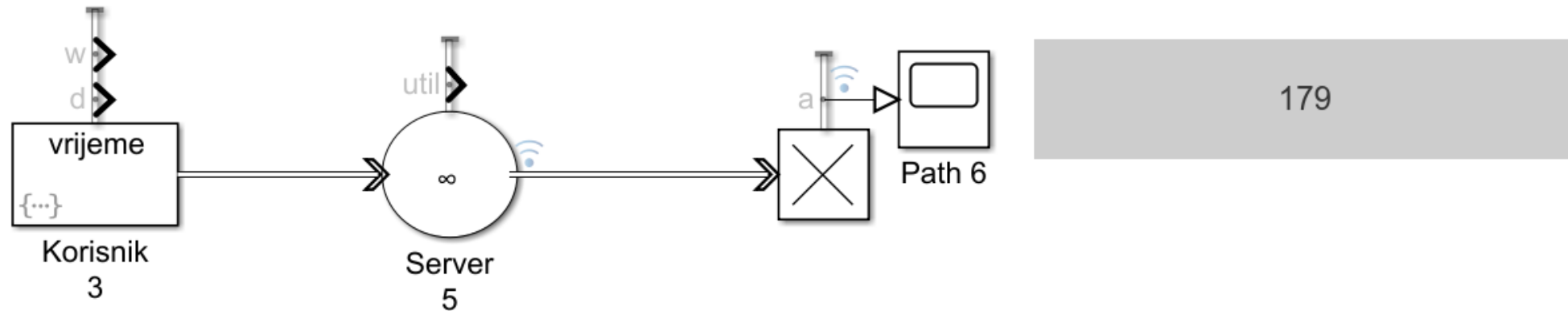
**Scope:** Vizualizacija toka podataka.



**Normalno stanje:** Regularni korisnici generiraju zahtjeve u definisanim intervalima, server funkcioniše optimalno i svi zahtjevi se procesiraju unutar raspoloživih resursa.

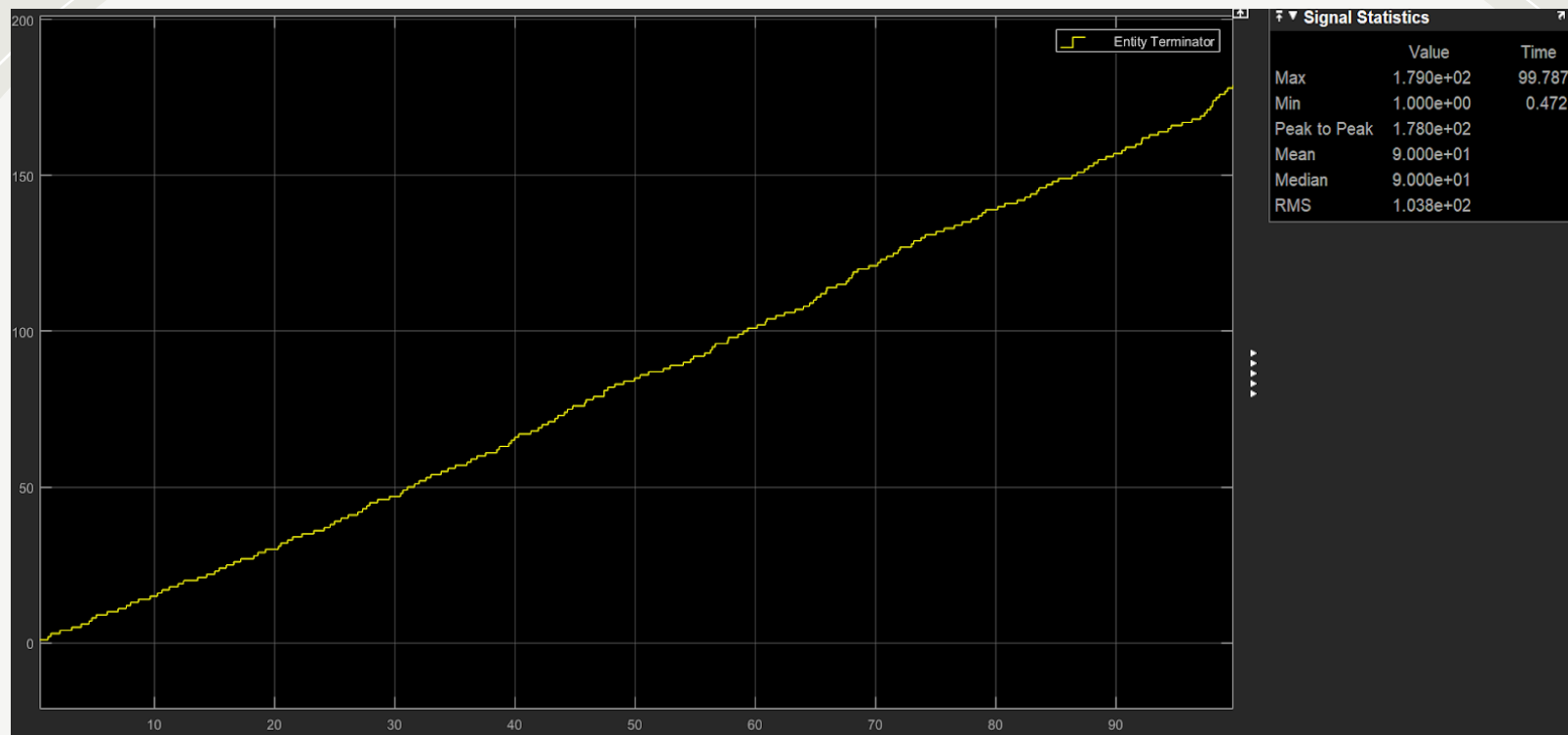


**Stanje napada:** Dodatni entiteti (napadački zahtjevi) generiraju se u visokoj frekvenciji. Red za čekanje se brzo puni, a server dostiže maksimalni kapacitet, što dovodi do pada performansi.



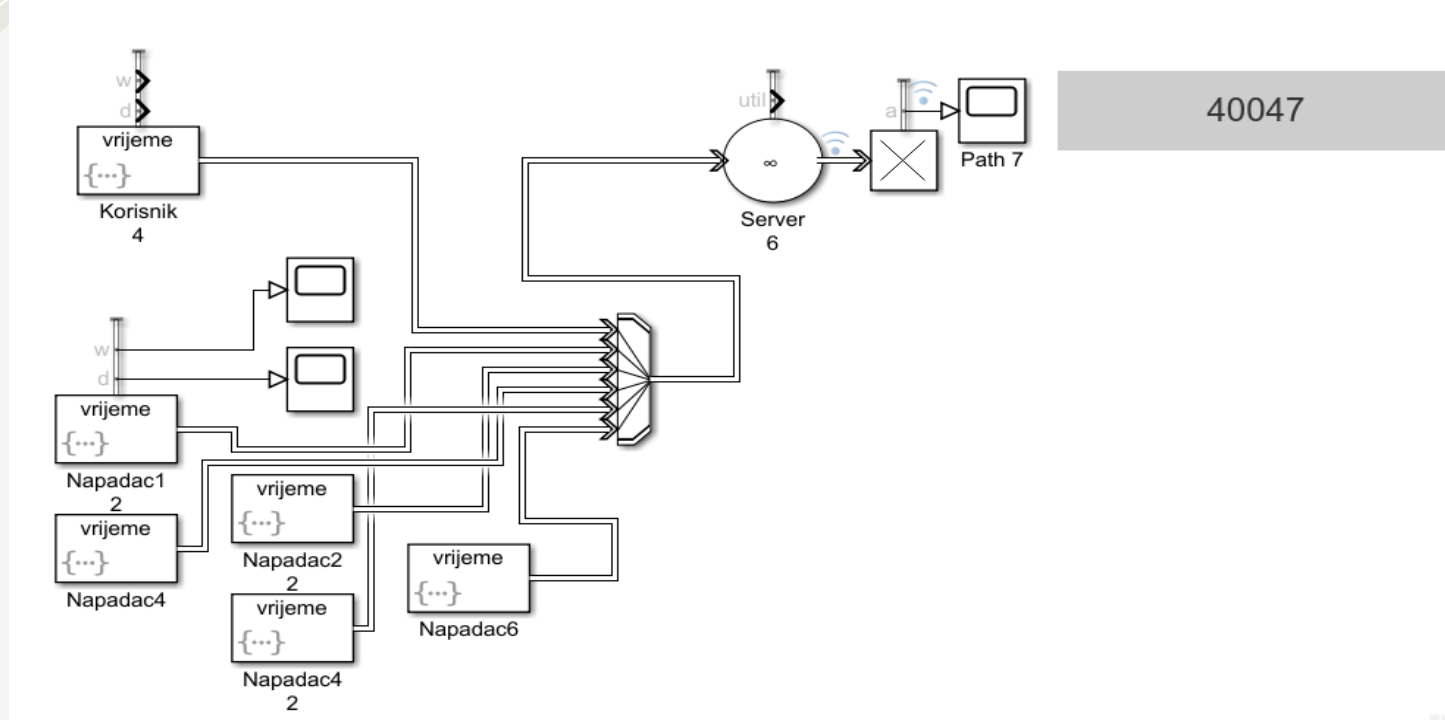
### Mjerenje performansi

Za simulaciju apsolutnog slučaja, gdje brojimo ukupan broj paketa koje je korisnik poslao u periodu od 100 sekundi, eliminirali smo red za čekanje jer nam nije bio potreban u ovom jednostavnom modelu. Također, postavili smo kapacitet procesora (jezgra) na beskonačno, što znači da server može simultano procesirati neograničen broj zahtjeva bez ikakvih kašnjenja izazvanih zagušenjem.



## Mjerenje performansi

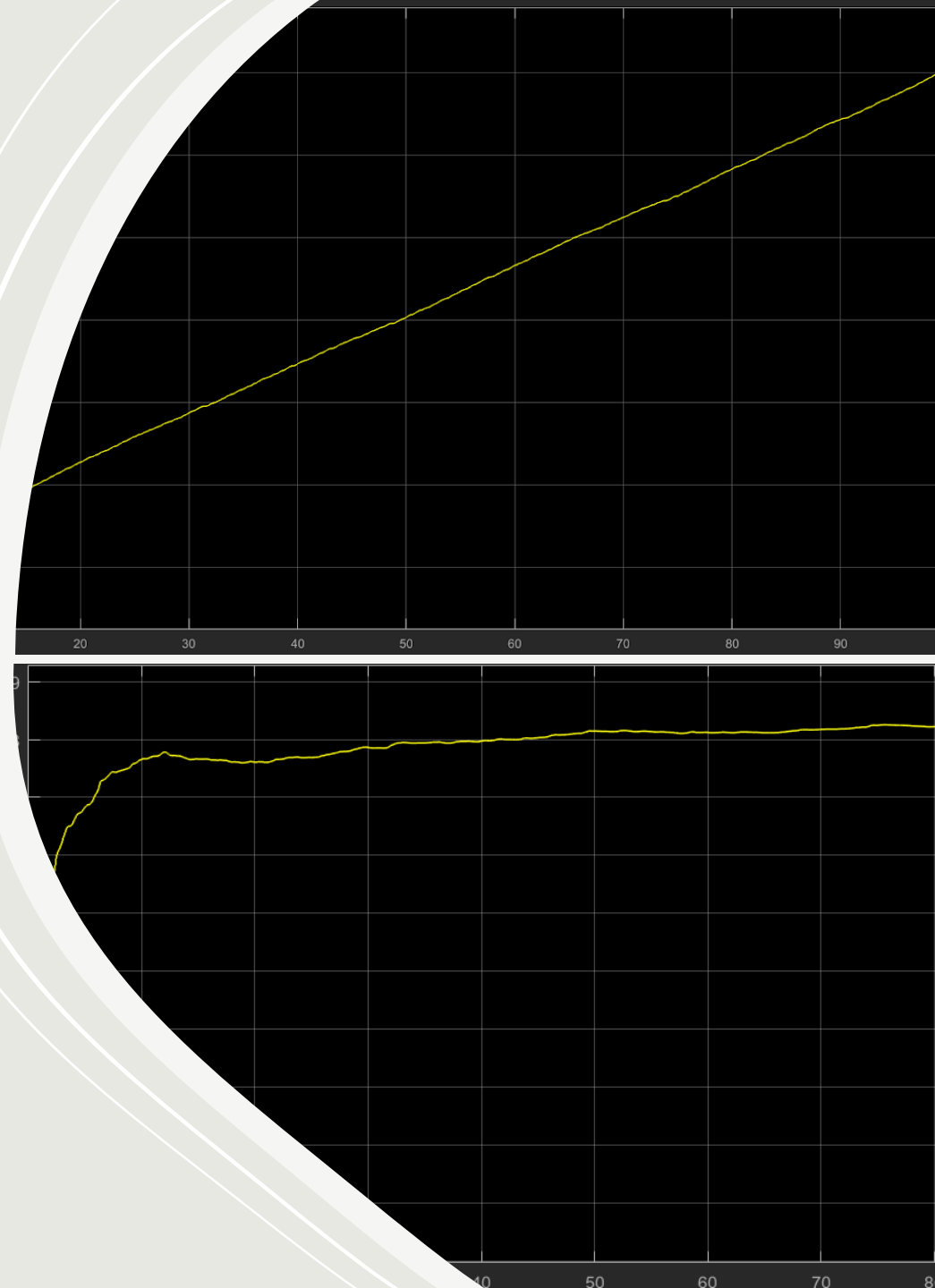
Kada smo testirali model u normalnom stanju, broj paketa koji je korisnik poslao bio je jednak apsolutnom broju paketa, što nam potvrđuje da je model adekvatan za simulaciju u uvjetima bez napada. U ovom stanju, red čekanja je bio prazan (jednak nuli), jer server nije bio preopterećen, te je mogao procesirati sve zahtjeve odmah, što potvrđuje da su svi generirani paketi uspješno prošli kroz sistem bez zastoja.



## Mjerenje performansi

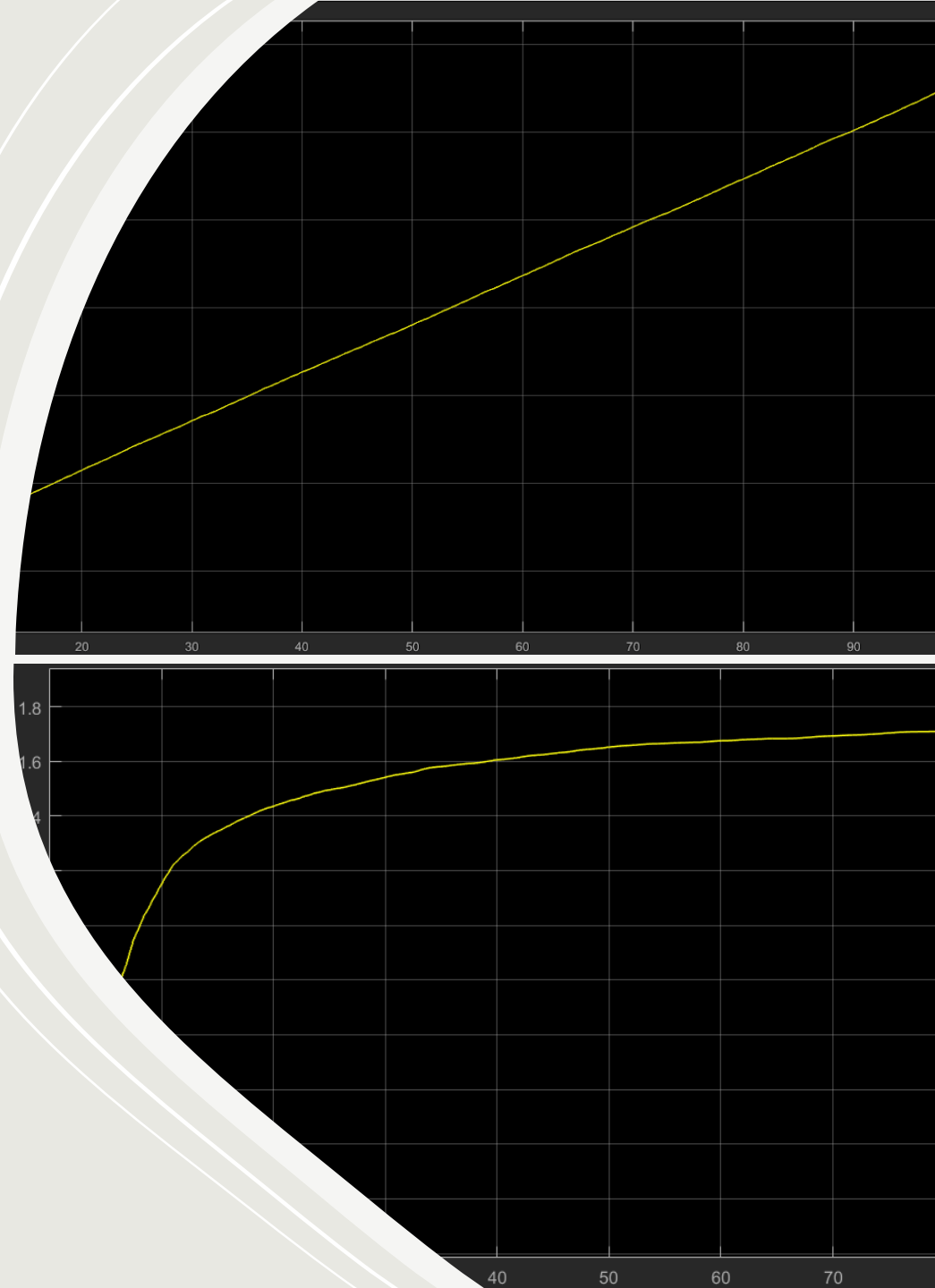
U napadnom stanju, osim regularnog korisnika, napadači također generiraju zahtjeve koji ulaze u server putem *Entity Input Switch*. Server, sa neograničenim brojem jezgri, može simultano procesirati sve zahtjeve, uključujući napadačke.

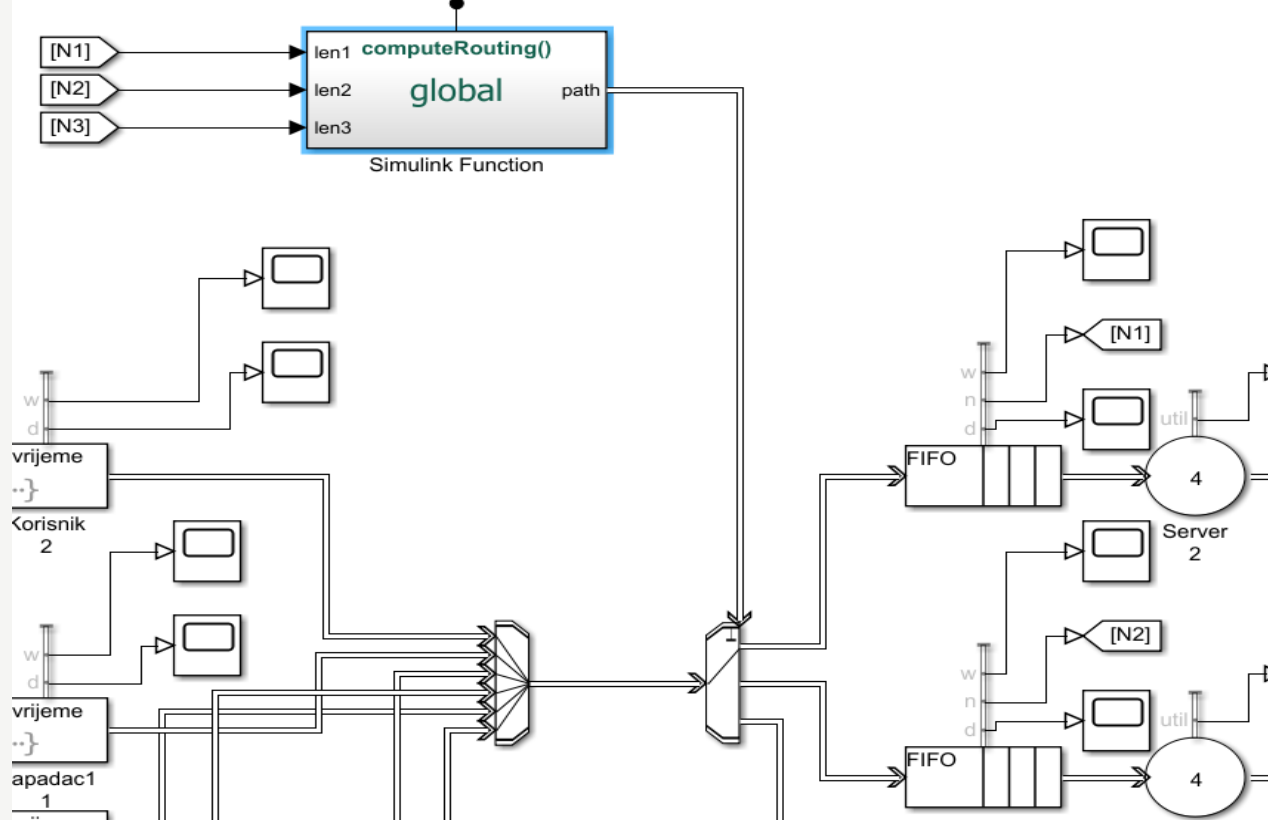
U standardnom stanju napada, gdje je kapacitet reda čekanja postavljen na **100** i server ima **2** jezgra, server je uspio obraditi oko **12,000** zahtjeva. Ovo predstavlja pad od približno **70%** u odnosu na apsolutni slučaj, gdje smo obradili oko **40,000** paketa. Ova značajna razlika ukazuje na drastičan pad u obradivosti zahtjeva zbog preopterećenja uzrokovano napadačkim saobraćajem. Također, red čekanja konvergira prema vrijednosti **0.8s**, što dodatno pokazuje zagušenje sistema i smanjenje performansi tokom napada.



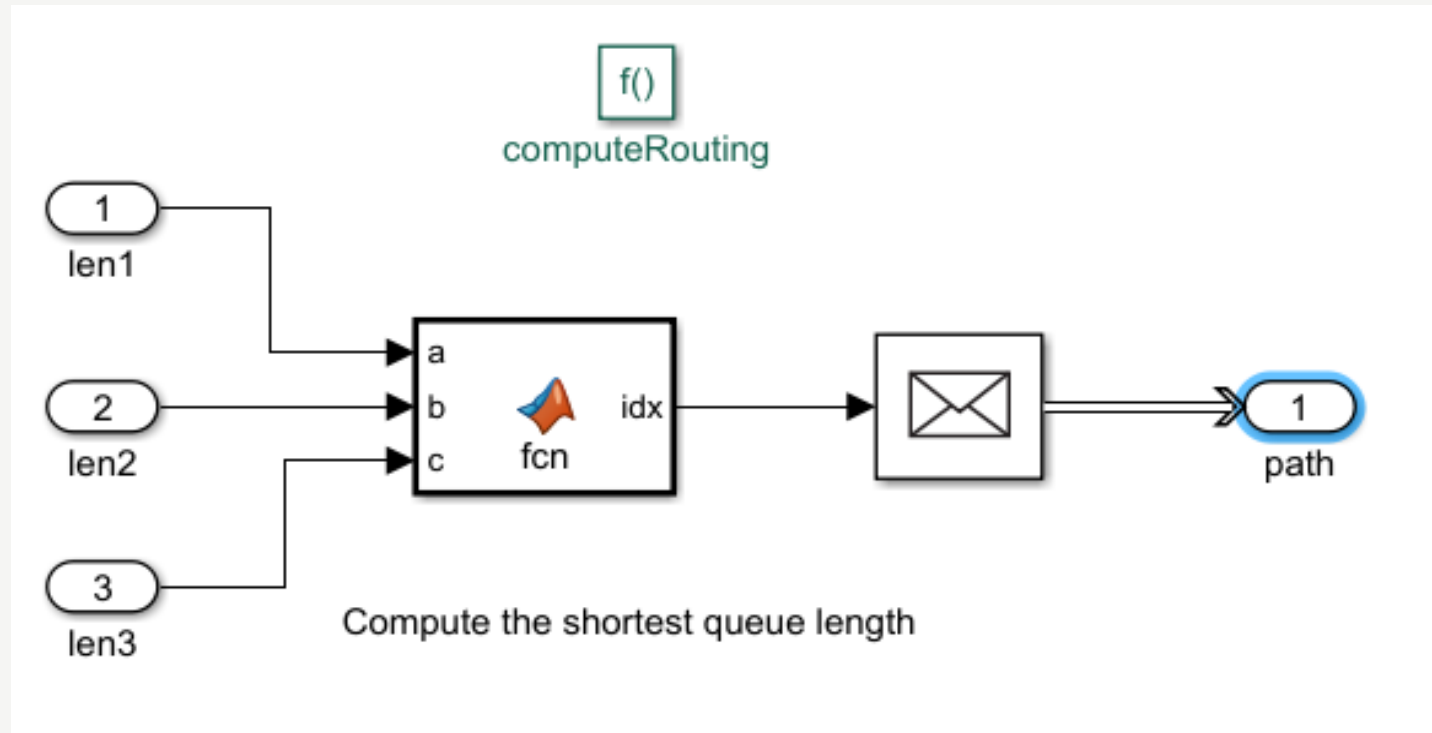


U ovom slučaju, kada smo povećali broj jezgri na serveru sa 2 na **4**, postigli smo značajno poboljšanje u performansama, obradivši skoro **28,000** paketa. Ovo predstavlja povećanje od oko **133%** u odnosu na prethodni scenario, gdje je server obradio samo **12,000** paketa. Red čekanja je sada konvergirao prema vrijednosti **1.7**, što pokazuje da je povećanje broja jezgri omogućilo bolju paralelnu obradu zahtjeva, iako još uvijek postoji zagušenje.



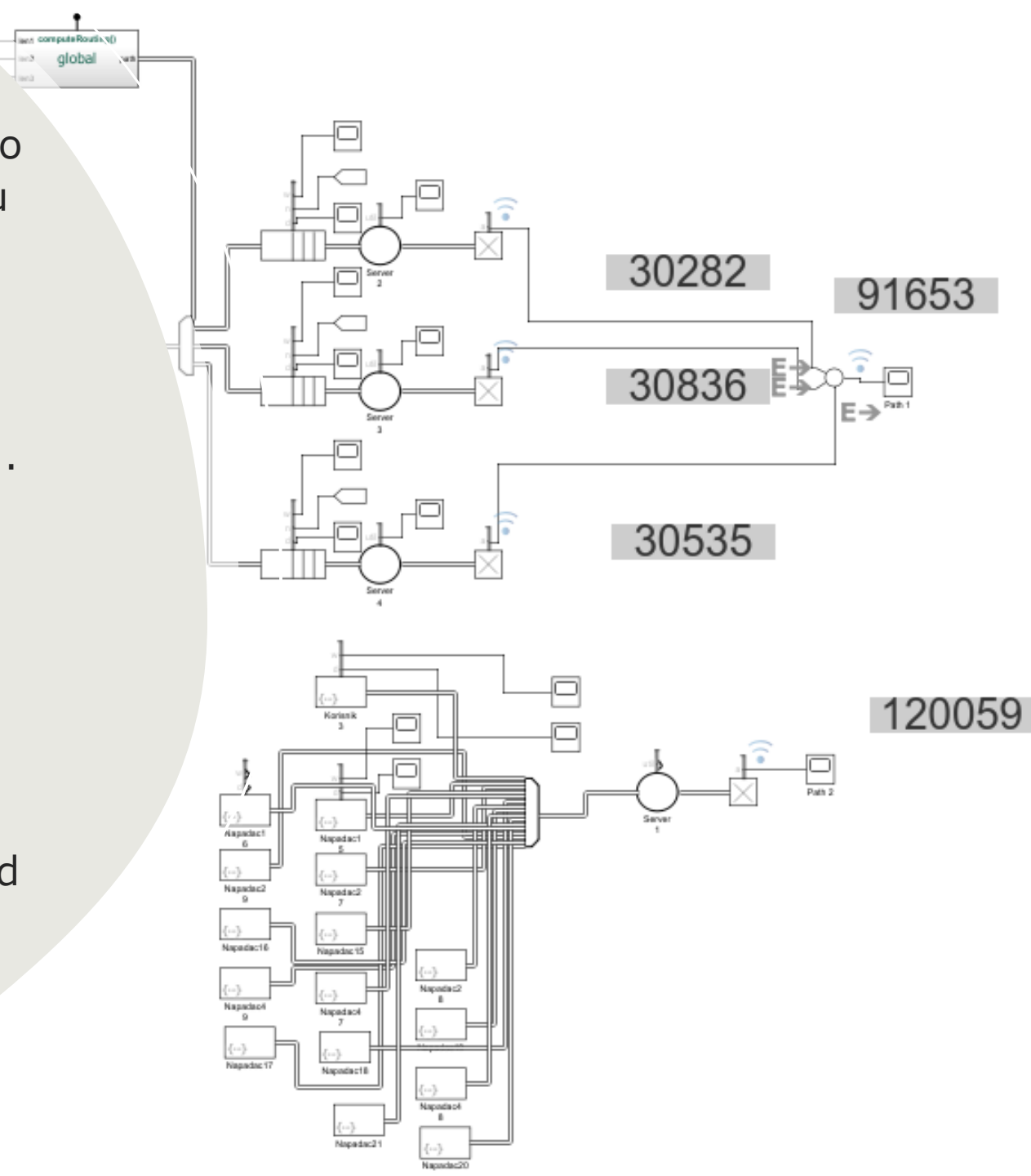


Naredno unapređenje u simulaciji uključuje korištenje tri servera umjesto jednog, svaki s 4 jezgra i kapacitetom reda čekanja od 500 paketa. Odabir servera za usmjerenje paketa vršit ćemo pomoću rutiranja, gdje će paket biti usmjeren na server s najmanjim brojem paketa u redu čekanja.



Funkcija `fcn` uzima tri vrijednosti (broj paketa u redu čekanja za svaki od tri servera) i vraća indeks servera s najmanjim brojem paketa. Taj indeks se koristi za usmjeravanje paketa prema odgovarajućem serveru putem Entity Output Switch komponente, koja će paket odrediti prema serveru na temelju izračunatog indeksa.

Testiranjem sistema s 10 napadača nismo uočili nikakvu razliku u performansama u odnosu na apsolutni slučaj. Sistem je uspješno obradio isti broj paketa, oko **80,000**, što potvrđuje da je model dovoljno robustan da podnese ovo opterećenje bez degradacije performansi. Međutim, kada smo povećali broj napadača na **15**, sistem je počeo pokazivati znakove preopterećenja. U apsolutnom slučaju, generisano je oko **120,000** paketa, dok je naš model obradio približno **92,000** paketa. Ovo predstavlja razliku od oko **23.33%**, što ukazuje na određeni pad performansi pod ekstremnim opterećenjem.



# Zaključak

---

- Ključne lekcije:
  - Utjecaj kapaciteta servera: Veći broj procesorskih jezgri smanjuje zagušenje i povećava otpornost.
  - Raspodjela opterećenja: Optimizirano rutiranje prema redovima čekanja sprječava zagušenja.
  - *Ograničenja sistema: Obrada 92,000 zahtjeva pri opterećenju s 15 napadača ukazuje na potrebu za dodatnim resursima.*
- Poređenje s realnim uvjetima: Simulacija približava stvarne scenarije, ali pojednostavljuje mrežne protokole i dinamiku napada.
- Zaključak: Strateško povećanje resursa i efikasno balansiranje ključni su za otpornost sistema.
- Značaj simulacije: Pruža uvide za optimizaciju performansi i sigurnosti mreža.