# Sybil napadi u društvenim mrežama i zaštita od njih

Antun Razum
Voditelj: prof. dr. sc. Siniša Srbljić

19. svibnja 2016.

Fakultet elektrotehnike i računarstva

# Sadržaj

# Uvod

# Sybil napadi

- *Sybil* – prema istoimenoj knjizi o ženi s disocijativnim poremećajem osobnosti
- napadi na distribuiranim sustavima poput senzorskih i *peer-to-peer* mreža
- napadač stvara velik broj lažnih identiteta preko kojih utječe na ponašanje sustava
- danas veoma aktualno na društvenim mrežama

# Primjeri

- širenje spam sadržaja na društvenim mrežama – često maliciozni sadržaj
- korištenje velikog broja lažnih identiteta za postizanje nekih "ciljeva", npr. glasanje, podizanje reputacije, lažno prijavljivanje sadržaja
- prosječno 20% zahtjeva za prijateljstvo od lažnih profila bude prihvaćeno

# Povijest i motivacija

# Središnji autoritet

- izdaje i provjerava podatke jedinstvene stvarnom čovjeku
- zahtijevanje osobnih podataka (npr. broj osobne iskaznice) ili plaćanje registracije
- nepoželjno jer odbija velik broj korisnika
- problem oko odabira središnjeg autoriteta
- može biti *signle point of failure*

# Decentralizirani pristupi

- povezivanje korisnika s IP adresom – lagano se može ukrasti i iskoristiti veći broj različitih IP adresa
- zagonetke koje zahtijevaju ljudski napor (npr. *CAPTCHA*) – predstavljanje na vlastitoj stranici ili plaćanje jeftinih servisa za rješavanje

# Motivacija

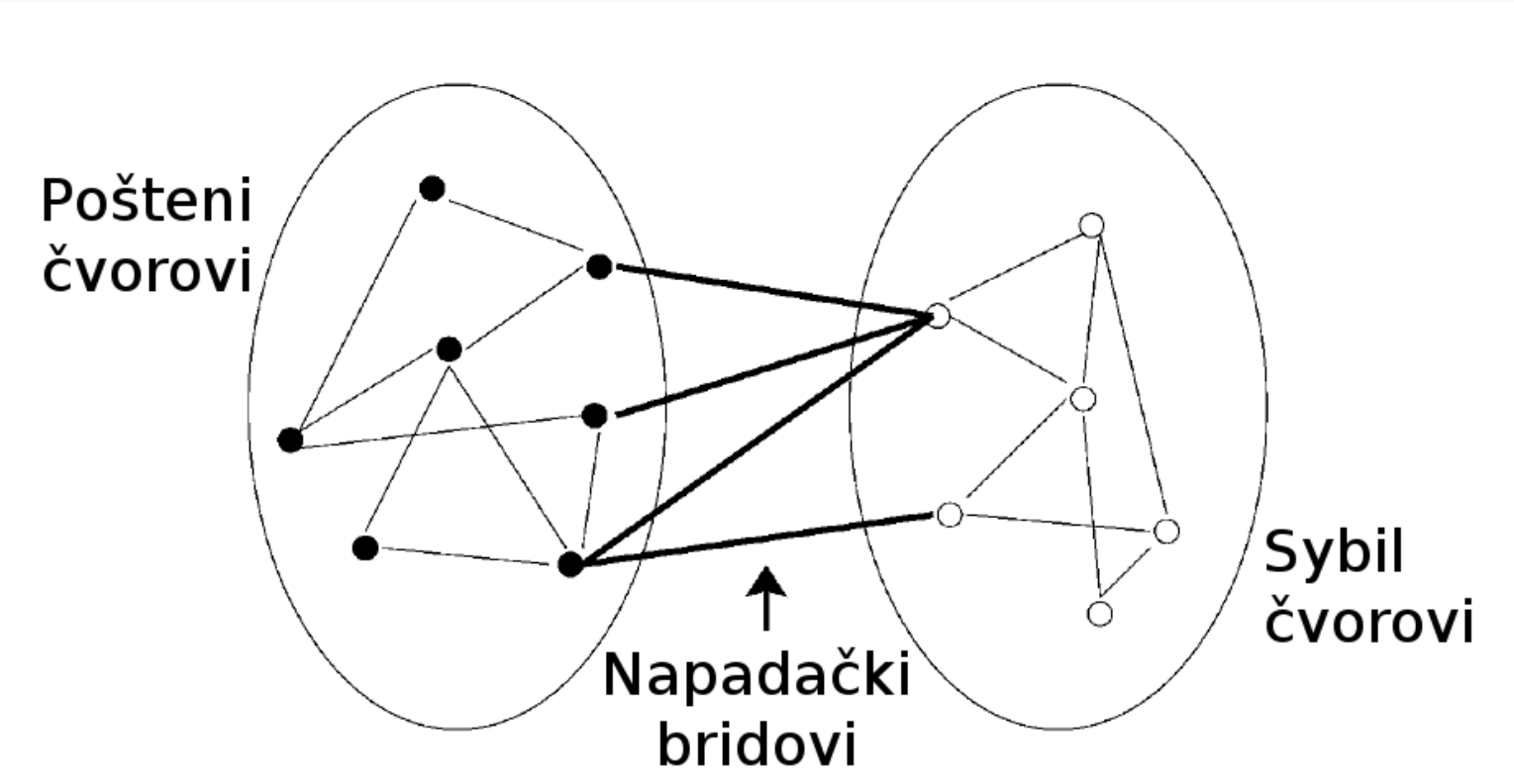
- predložene metode su ograničene
- omogućuju smanjenje, ali ne i eliminaciju sybil napada
- potrebna obrana temeljena na analizi grafa društvene mreže

# Pojmovi i definicije

# Model društvene mreže

- neusmjereni bezteˇzinski graf – cˇvorovi su korisnici, a bridovi odnosi među njima, npr. prijateljstva
- *pošteni cˇvorovi* – predstavljaju stvarne korisnike mreže
- *sybil cˇvorovi* – lažni identiteti stvoreni od strane napadača
- *napadački bridovi* – bridovi između sybil cˇvorova i poštenih cˇvorova
- *sybil regija* sastoji se od svih sybil cˇvorova, a *poštena regija* od svih poštenih cˇvorova

# Model društvene mreže



# Slučajne šetnje

- *slučajna šetnja* – šetnja u grafu s nasumično odabranim prijelazima
- slučajne šetnje su *ergodične* – konvergiraju prema *stacionarnoj distribuciji* kada im duljina teži u beskonačnost

# Vrijeme miješanja

- definira se kao najmanja duljina slučajne šetnje kojom se postiže stacionarna distribucija do neke mjere $\epsilon$:

$$T(\epsilon) = \max_i \min\{t : |\pi - \pi^{(i)} P^t|_1 < \epsilon\}$$

- graf s $n$ čvorova je *brzo miješajući* ako je:

$$T(\epsilon) = O(\log n)$$

- dobro povezani grafovi su brzo miješajući

# Obrana od sybil napada

# Pretpostavke algoritma

# Identifikacija sybil čvorova

# Pronalazak sybil grupa

# Rezultati

# Korištene metode i skupovi podataka

# Rezultati

# Zaključak

# Zaključak

# Pitanja?

# Hvala na pažnji!