სოციალური ქსელის ინფორმაციული დაცვის იმიტაციური მოდელები

ელენე კამკამიძე
პროფესორი საქ. ტექნიკური უნივერსიტეტი
ეკატერინე გვარამია
ასოც. პროფესორი საქ. ტექნიკური უნივერსიტეტი

რეზიუმე

შემუშავებულია იმიტაციური მოდელები, რომელიც საშუალებას იძლევა მისაღებ დროში მივიღოთ აკრძალული ინფორმაციის გავრცელების მოდელირების შედეგები საინფორმაციო ქსელებში განაწილებული გამომთვლელი რესურსების გამოყენებით. შემუშავებული პროგრამული უზრუნველყოფის დახმარებით ჩატარებული იყო ექსპერიმენტალური კვლევა, რომლის ამოცანაა სოციალურ ქსელში კვანძების ძიების ავტომატიზაცია, რომლებიც წარმოადგენენ აკრძალული ინფორმაციის პოტენციალურ გამავრცელებლებს.

ИММИТАЦИОННЫЕ МОДЕЛИ ИНФОРМАЦИОННОЙ ЗАЩИТЫ СОЦИАЛЬНОЙ СЕТИ

Резюме

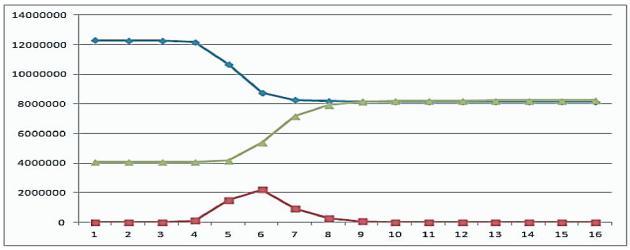
Разработаны имитационные модели, позволяющие моделировать процесс распространения запрещенной информации в социальных сетях с использованием вычислительных ресурсов распределенной информационной сети. Проведено экспериментальное исследование с использованием разработанного специального программного обеспечения с целью автоматизации поиска в социальной сети узлов, представляющих потенциальную угрозу распространения запрещенной информации.

* * * *

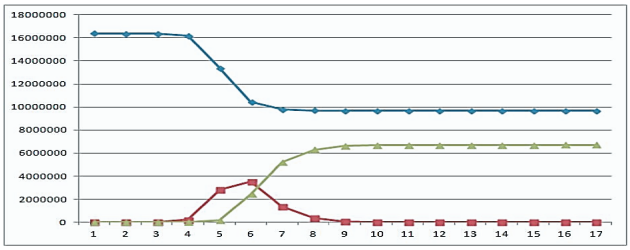
საინფორმაციო ქსელებში აკრძალული ინფორმაციის გავრცელების მოდელირება წარმოადგენს შრომატევად ამოცანას. მისი ამოხსნა მისაღებ ვადებში და აქტუალური შედეგების მიღება შესაძლებელია მხოლოდ განაწილებული გამოთვლითი რესურსების გამოყენებით. აკრძალული ინფორმაციის ექსპერიმენტალური გამოკვლევა საინფორმაციო ქსელებში ხორციელდება იმიტაციური მოდელის საფუძველზე. იმიტაციური მოდელი რეალიზირებულია დამუშავებული პროგრამული უზრუნველყოფის სახით. გრაფზე პარალელური გამოთვლის რეალიზაციისთვის გამოყენებული იყო ბიბლიოთეკა Parallel Boost Graph Library. ბიბლიოთეკა არის თავისუფლად გავრცელებადი და თავისი ფუნქციონალური საშუალებებით არ გააჩნია ალტერნატივა. Parallel Boost Graph Library (PBGL) წარმოადგენს გრაფის კონცეფციის დრეკად და ეფექტურ რეალიზაციას. გამოთვლითი კვანძების ჯგუფები: (4კვანძი, 2 პროცესორი, RAM 2Gb Hdd 160 Gb), short (14 კვანძი, 2 პროცესორი RAM 2Gb Hdd 160 Gb), Long (14 კვანძი, ორი პროცესორი RAM 2Gb Hdd 160 Gb), Work (32 კვანძი, 2 პროცესორი RAM 2Gb Hdd 160 Gb). ყველა კვანძი დაკავშირებულია ერთმანეთთან ორი დამოუკიდებელი ქსელით: სისტემური ქსელი: Infini Band DDR (Fat Tree: 6x12 პორტი; ლატენტურობა MPI-ს დონეზე : 1,3-1,95მკ/წმ; გავლის სიჩქარე MPI-s დონეზე: 1540 მეგა ბაიტი/წმ) და დამხმარე/მმართველი ქსელი: Gigabit Ethernet (2x(44+4x10G)). დამუშავებული პროგრამული უზრუნველყოფა დაწერილია Microsoft Visual Studio 2008-ის გარემოში. გრაფის წარმოდგენისთვის გამოთვლითი სისტემის მეხსიერებაში გამოიყენებოდა განაწილებული მიდგომა Parallel Boost Graph Library ბიბლიოთეკის გამოყენებით. შემავალი მონაცემების ფორმატი - ტექნიკური ფაილი, რომელშიც ყველა სტრიქონში ჩაწერილია კვანძის იდენთიფიკატორი. გამომავალ ფაილში ფიქსირდება აკრძალული ინფორმაციის დინამიკის მონაცემები, რომელიც წარმოდგენილია შემტევი და დაცული კვანძების სიაში ყოველი დროის კვანტში. ქსელში არსებობს სამი სახის კვანძები. პირველი - შემტევი კვანძები, მეორე - დაცული კვანძები, ეს კვანძები ხასიათდება იმით, რომ არასდროს არ ღებულობენ მონაწილეობას აკრძალული ინფორმაციის გავრცელებაში. მესამე - პოტენციურად დაუცველი. ასეთი ტიპის კვანძები არ მონაწილეობენ საშიშროების გავრცელებაში, მაგრამ შეიძლება დაექვემდებარონ ნეგატიურ ზემოქმედებას შემტევი კვანძების მხრიდან და შეუძლიათ გაავრცელონ აკრძალული ინფორმაცია.

განვიხილოთ ამოცანა. მოცემულია N - კვანძების რაოდენობა, რომელიც ტოლია ქსელში აბონენტების რაოდენობის, Io - აბონენტების რაოდენობა, რომლებიც არიან დასაწყისი შემტევი ზემოქმედების, y - პარამეტრი, რომელიც ასახავს საშიშროების უკუქმედების ხარისხს. φ - ტოპოლოგიურად ქსელის დაუცველობის კოეფიციენტი, რომელიც ასახავს საინფორმაციო ქსელების შინაგან თვისებებს, რომელიც დაფუძნებულია მისი ტოპოლოგიის ხასიათზე და შესაძლებელს ხდის გაავრცელოს აკრძალული ინფორმაცია, t - პროცესის დრო. ანალიტიკური მოდ-

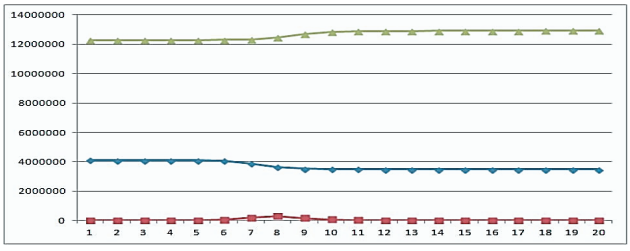
ელების დამუშავების მეთოდიკა შეიცავს შემდეგი მოქმედებების მიმდევრობას: ბიჯი 1. აკრძალული ინფორმაციის გავრცელების ინიცირებას აკეთებს რომელიღაც აბონენტი - ბოროტმზრახველი, რომელიც ავრცელებს ინფორმაციას მისი საკონტაქტო სიიდან. შეტევა შეიძლება დაიწყოს ერთმა ბოროტმზრახველმა ან ჯგუფმა. ბიჯი 2. მიმღები აბონენტები, რომლებმაც მიიღეს შეტყობინება, კითხულობენ მას და ერთვებიან შეტევის პროცესში, რომელსაც ავრცელებენ მას თავის კონტაქტების სიაში ან იგნორირებას უკეთებენ ან საერთოდ იშორებს ინფორმაციას. შეტევის პროცესი მიმდინარეობს ჩვეულებრივ ზავისებურად. შემტევი აბონენტები არ ამთავრებენ შეტევას. შეტევის ფანჯარა, როგორც წესი გრძელდება დროის დიდ მონაკვეთში და დამოკიდებულია მოწოდების ტიპზე. ბიჯი 3. აბონენტებს შეუძლიათ შეწყვიტონ აღთქმა და შესაბამისად გაავრცელონ, გამომდინარე დაცვის მექანიზმის ზემოქმედებით, ამიტომ შეტყობინება შემტევი აბონენტებიდან იქნება მუდმივად უკუგდებული. ბიჯი 4. პროცესი გრძელდება მანამდე, სანამ ქსელში იქნება აბონენტი ბოროტმზრახველი, ან არის პოტენციურად დაუცველი კვანძები.



ნახ.1.ექსპერიმენტი 1. φ =200, β=0.2, y=0.8, Io=l, Ro=0.



ნახ.2. ექსპერიმენტი 2. φ =200, β=0.2, y=0.8, Io=1, Ro =0.25.



ნახ.3.ექსპერიმენტი 3. φ =200, β =0.2, y=0.8, Io=l, Ro=0,75 N.

აღწერილი ალგორითმის საფუძველზე შემუშავდა საინფორმაციო ქსელებში აკრძალული ინფორმაციის გავრცელების იმიტაციური მოდელი, რომელიც შედგება ModelGraph დამუშავებული პროგრამისგან და მონაცემებით, რომლებიც შეიძლება იყვნენ გენერირებული აკრძალული ინფორმაციის საშუალებით. კვანძები შეტევის მიდრეკილებით (So) განისაზღვრება: So=N-Io-Ro, N არის ქსელში კვანძების საერთო რაოდენობა. ჩატარებული მოდელირების შედეგების გრაფიკები, რომელიც ეხება აკრძალული ინფორმაციის გავრცელებას ჭაცებოოკ სოციალურ ქსელში ტოპოლოგიურ ფრაგმენტებში, მოცემულია ნახაზებზე.

ექსპერიმენტიდან შეიძლება გავაკეთოთ შემდეგი დასკვნა: უკვე ერთ შემტევ კვანძს შეუძლია გამოიწვიოს „აფეთქება“ ქსელში დაცვის დიდი ალბათობის შემთხვევაშიც; საწყისი დაცული კვანძების რიცხვის ზრდისას, შემტევი კვანძების მაქსიმალური რაოდენობა ეცემა.

გამოყენებული ლიტერატურა:

1. კონსტანტინე კამკამიძე, მიხეილ დვალიშვილი, ელენე კამკამიძე. ტელეკომუნიკაციური ქსელის პარამეტრების კვლევის ანალიტიკური მოდელის ფორმირება. შრომები მართვის ავტომატიზებული სისტემები. N1 (21), 2016, 25-30გვ.

2. ელენე კამკამიძე, ირინა ხომერიკი. ტელეკომუნიკაციური ქსელის ტოპოლოგიის სრული გრაფის აგების ალგორითმი. შრომები მართვის ავტომატიზებული სისტემები. N1 (21), 2016, 31-37გვ.

3. Бреер, В.В. Стохастические модели социальных сетей / В.В. Бреер; Управление большими системами, № 27. – 2014. - С. 169-204.