

ՀՀ ԳԱԱ ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈՔԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

ԴԱՐԲԻՆՅԱՆ ՎԱՀՐԱՄ ՀՐԱՅՐԻ

ԹՎԱՅԻՆ ՀՐԱՊԱՐԱԿՈՒՄՆԵՐԻ ԾԱՌԱՅՈՒԹՅՈՒՆՆԵՐԻ ՊԱՇՏՊԱՆՎԱԾՈՒԹՅԱՆ ԵՎ
ԱՐԱԳԱԳՈՐԾՈՒԹՅԱՆ ԲԱՐՁՐԱՑՄԱՆ ՄԻՋՈՑՆԵՐԻ ՀԵՏԱԶՈՏՈՒՄ ԵՎ ՄՇԱԿՈՒՄ

Ե.13.04-«Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի
մաթեմատիկական և ծրագրային ապահովում» մասնագիտությամբ տեխնիկական
գիտությունների թեկնածուի զիտական աստիճանի հայցման ատենախոսության

Ս Ե Ղ Մ Ա Գ Ի Ր

ԵՐԵՎԱՆ 2014

ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ НАН РА

ДАРБИНЯН ВАГРАМ ГРАЙРОВИЧ

ИССЛЕДОВАНИЕ И РАЗРАБОТКА СРЕДСТВ ПОВЫШЕНИЯ ЗАЩИЩЁННОСТИ И
БЫСТРОДЕЙСТВИЯ СЕРВИСОВ ЦИФРОВЫХ ПУБЛИКАЦИЙ

А В Т О Р Е Ф Е Р А Т

диссертации на соискание ученой степени кандидата технических наук по
специальности 05.13.04 – «Математическое и программное обеспечение вычислительных
машин, комплексов и сетей»

ЕРЕВАН 2014

Ատենախոսության թեման հաստատվել է Հայաստանի Պետական Ճարտարագիտական Համալսարանում (Պոլիտեխնիկ)

Գիտական ղեկավար՝	տեխ.գիտ.թեկնածու	Գ.Ի. Մարգարով
Պաշտոնական ընդդիմախոսներ՝	ֆիզ.մաթ.գիտ. դոկտոր	Ս.Կ. Շուքրյան
	տեխ.գիտ.թեկնածու	Ս.Կ. Զարգարյան

Առաջատար կազմակերպություն՝ Երևանի կապի միջոցների գիտահետազոտական ինստիտուտ

Պաշտպանությունը կայանալու է 2014թ. հունիսի 17-ին, ժ. 16:00-ին ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում գործող 037 «Ինֆորմատիկա և հաշվողական համակարգեր» մասնագիտական խորհրդի նիստում հետևյալ հասցեով՝ Երևան, 0014, Պ. Սևակի 1:

Ատենախոսությանը կարելի է ծանոթանալ ՀՀ ԳԱԱ ԻԱՊԻ գրադարանում:

Սեղմագիրը առաքված է 2014թ. մայիսի 17-ին:

Մասնագիտական խորհրդի
գիտական քարտուղար, ֆ.մ.գ.դ.



Հ. Գ. Սարգսյան

Тема диссертации утверждена в Государственном инженерном университете Армении (Политехник)

Научный руководитель:	кандидат тех. наук	Г.И. Маргаров
Официальные оппоненты:	доктор физ.-мат.наук	С.К. Шукурян
	кандидат тех. наук	Т.К. Заргарян

Ведущая организация: Ереванский научно-исследовательского институт средств связи

Защита состоится 17 июня 2014г. в 16:00 на заседании специализированного совета 037 «Информатика и вычислительные системы» Института проблем информатики и автоматизации НАН РА по адресу: 0014, г. Ереван, ул. П. Севака 1.

С диссертацией можно ознакомиться в библиотеке ИПИА НАН РА.

Автореферат разослан 17 мая 2014г.

Ученый секретарь специализированного
совета, д.ф.м.н.



А. Г. Сарухянян

ԱՇԽԱՏԱՆՔԻ ԸՆԴՀԱՆՈՒՐ ԲՆՈՒԹԱԳԻՐԸ

Թեմայի արդիականությունը. Վերջին տարիներին ինտերնետի բնագավառը արագորեն փոփոխվում է՝ ներառելով նորանոր կիրառություններ: Վեբ տեխնոլոգիաների առաջընթացը թույլ տվեց հրապարակողներին (համալսարաններին, գրքերի և ամսագրերի հրատարակչություններին և այլոց) սկսել անցում կատարել ավանդական տպագրական միջավայրից դեպի առցանց թվային հրապարակումներ, արագացնելով հրապարակման գործընթացը և նվազեցնելով ծախսերը: Մասնավորապես թվային ինտերակտիվ հրապարակումները լինելով ավելի հարմարեցված օգտագործողին, հրապարակման ժամանակակից մեթոդները մեծ հետաքրքրություն են առաջացնում օգտագործողների, հրատարակողների և գովազդատուների մոտ: Թվային ինտերակտիվ հրապարակումները նույնպես հանդիսանում են առցանց գովազդի շատ արագորեն զարգացող միջավայր: Նշենք, որ 2013թ առցանց գովազդների 42 միլիարդ դոլլարի շրջանառությունը պատմության մեջ առաջին անգամ գերազանցել է հեռուստատեսայինի շրջանառությանը (2013 - 39 միլիարդ)¹:

Առցանց գովազդը ունենալով ավանդականի նկատմամբ ավելի մեծ վերադարձի գործակից, ունի նույնպես իր թերությունները, որոնցից հիմնականն են կեղծ դիտումները: Կեղծ դիտումները շատ մեծ կորուստներ են հասցնում հրատարակողներին և առցանց հրապարակումների ծավալների մեծացման հետ մեկ տեղ, կորուստները աճում են նույնպես: Համաձայն, առցանց գովազդի բնագավառում առաջատարներից մեկը հանդիսացող՝ Google, կազմակերպության հրատարակած տվյալների, արցանց դիտումների 10%-ը հանդիսանում են կեղծ²: Այդպիսի դիտումները հաճախ իրագործվում են Denial of Service (DoS) հարձակման սկզբունքով, երբ մեծածավալ հարցումներ են ուղարկվում վեբ ռեսուրսի վրա և նույնիսկ, եթե ռեսուրսը շարքից դուրս չի գալիս, գրանցում է գովազդի դիտումների շատ մեծ ծավալ, առաջացնելով համապատասխան ծախսեր: DoS հարձակման հայտնաբերման հետ կապված հիմնական խնդիրը այն է, որ հարձակվողը օգտագործում է օրինական հարցումների տարափ, թիրախ համակարգը հեղեղելու համար: Այս իսկ պատճառով բարդ է տարբերակել հարձակումը, հարձակման մաս չկազմող օրինական հարցումներից: Խնդիր է առաջանում որևէ եղանակով տարբերակել օրինական օգտագործողներին, ինչը իր հերթին հանդիսանում է բարդ խնդիր, քանի որ հարձակման ժամանակ օգտագործվող չարամիտ ծրագրերը (բոթերը) օրեցօր զարգացվում են և ավելի հմուտ են դառնում վեբ օգտագործողի վարգաքիծը նմանակելու գործում: Թվային ինտերակտիվ հրապարակումներում, ի տարբերություն սովորական վեբ կայքերի, օգտագործողի վարքագիծը ավելի կանխագուշակելի է, ինչը ունի օրինական օգտագործողին բոթից տարբերակելու միջոց դառնալու պոտենցիալ: Թվային ինտերակտիվ հրապարակումների շուկայի աճը մեծ հետաքրքրություն է առաջացնում առցանց գովազդատուների մոտ, քանի որ շատ հրատարակումներ անցում են կատարում ավանդական տպագրվածից, իրենց հրապարակման առցանց տարբերակի:

¹“IAB internet advertising revenue report 2013 full year results”, April 2014; PwC, <http://www.pwc.com/e&M>. <http://www.forbes.com/sites/roberthof/2014/04/10/online-ad-revenues-blow-past-broadcast-tv-thanks-to-mobile-and-video/>

²<http://www.google.com/ads/adtrafficquality/>

Ավանդական տպագրված տարբերակից, հրապարակումների թվայինի անցնելը իր հետ բերում է օգտագործելիության խնդիր: Օգտագործողները ակնկալում են թվային հրապարակումից լինել նույնքան հասանելի, որքան տպագրվածն է և ապահովել ընթերցման աստիճան և դյուրին ընթացք: Շատ օգտագործողներ պատրաստ չեն երկար սպասել հրապարակման էջերի բեռնմանը և կնախընտրեն տպագրված տարբերակը, քանի դեռ նմանատիպ խնդիրներ առկա են: Այսպիսով արդիական է թվային ինտերակտիվ հրապարակումների ծառայության օգտագործողներին բոթերից առանձնացնելու և ծառայությունը DoS հարձակումներից պաշտպանվածության և արագագործության բարձրացման միջոցների հետազոտումը և մշակումը:

Աշխատանքի նպատակն է մշակել թվային ինտերակտիվ հրապարակումների ծառայությունների արագագործության և DoS հարձակումներից պաշտպանվածության բարձրացման միջոցներ՝ հիմնված թվային ինտերակտիվ հրապարակումների ծառայության օգտագործողի վարքագծի վրա: Նշված նպատակին հասնելու համար աշխատանքում դրվել և լուծվել են հետևյալ խնդիրները՝

- Հետազոտել թվային հրապարակումների ծառայությունների համակարգերը, ինչի հիման վրա մշակել օգտագործողի վարքագծի նկարագրության միջոց և օգտագործողի վարքագծի մոդել:
- Մշակել թվային հրապարակումների ծառայությունների վրա կատարվող DoS հարձակումների հայտնաբերման մեթոդ, որը հաշվի կառնի միջավայրի առանձնահատկությունները, իրագործել համապատասխան ծրագրային ապահովում:
- Մշակել թվային հրապարակումների ծառայությունների արագագործության բարձրացման միջոց, իրագործել համապատասխան ծրագրային ապահովում:

Հետազոտման օբյեկտ է հանդիսանում թվային հրապարակումների ծառայությունները, նրանցում օգտագործողների վարքագիծը, վարքագծի հավանականային ու սիմուլացիոն մոդելները, DoS հարձակումները և նրանցից պաշտպանության միջոցները:

Հետազոտման մեթոդներ. Աշխատանքի ընթացքում օգտագործվել են օբյեկտա-կողմնորոշված ծրագրավորման, հավանականային և սիմուլացիոն մոդելավորման մեթոդներ:

Արդյունքների գիտական նորությունը:

- Առաջարկվել է թվային ինտերակտիվ հրապարակումների ծառայությունների օգտագործողի վարքագծի նկարագրության մեթոդ, որը հիմնված է վիճակագրական տվյալների վրա և թույլ է տալիս կանխագուշակել օգտագործողի հերթական գործողությունը:
- Մշակվել է թվային ինտերակտիվ հրապարակումների ծառայությունների օգտագործողի ուղղորդման հավանականային մոդել, որը անկախ վիճակագրական տվյալներից թույլ է տալիս կանխագուշակել օգտագործողի հերթական գործողությունը:
- Առաջարկվել է թվային ինտերակտիվ հրապարակումների ծառայությունների վրա կատարվող DoS հարձակումների հայտնաբերման մեթոդ, հիմնված օգտագործողի

վարքագծի յուրահատկությունների վրա:

Ստացված արդյունքների կիրառական նշանակությունը:

- Նախագծվել և իրագործվել է թվային ինտերակտիվ հրապարակումների ծառայությունների օգտագործողի վարքագծի հիման վրա օգտագործողի հերթական գործողության կանխագուշակման ծրագրային մոդուլ:
- Նախագծվել և իրագործվել է օգտագործողի հերթական գործողության կանխագուշակման մոդուլի վրա հիմնված ծրագրային մոդուլ, որը թույլ է տալիս բարձրացնել համակարգի արագագործությունը, ռեսուրսների նախորոք բեռնման միջոցով:
- Նախագծվել է թվային ինտերակտիվ հրապարակումների ծառայությունների վրա կատարվող DoS հարձակումների հայտնաբերման ալգորիթմ, որը ապահովում է բոթերի հայտնաբերման 20-80% ավելի բարձր ճշտություն, հրապարակմանը հարմարվող լինելու շնորհիվ: Ալգորիթմը իրագործվել է ծրագրային մոդուլի տեսքով:

Ներդրումներ. Ատենախոսությունում նախագծված լուծումների հիման վրա ստեղծվել է ծրագրային փաթեթ, որը օգտագործվում է համակարգի արագագործության բարձրացման և DoS հարձակումներից պաշտպանության համար: Ստեղծված ծրագրային փաթեթը օգտագործվում է վերոհիշյալ նպատակներով Joomla ցեղ ծառայությունում (<http://www.joomag.com>): Համակարգի կայունության փորձարկումները ցույց են տվել, որ չարամիտ հարցումների հայտնաբերումը և առանձնացումը օրինական հարցումներից բարելավվել է 76%-ով: Փորձաշրջանի ընթացքում կատարված վիճակագրության արդյունքում պարզվել է, որ պարունակության նախորոք բեռնման շնորհիվ, պարունակության բեռնմանը սպասելու միջին ժամանակը նվազել է 31%-ով, իսկ չարամիտ հարցումների կողմից հասցրած վնասները 27%-ով: Վերոհիշյալ փաստը հաստատված է համապատասխան փաստաթղթերով:

Ուշադասությանը ներկայացվում են հետևյալ դրույթները.

- Թվային ինտերակտիվ հրապարակումների ծառայության օգտագործողի վարքագծի նկարագրության մեթոդը, որը հիմնված է վիճակագրական տվյալների վրա և թույլ է տալիս կանխագուշակել օգտագործողի հերթական գործողությունը:
- Թվային ինտերակտիվ հրապարակումների ծառայությունների վրա կատարվող DoS հարձակումների հայտնաբերման մեթոդը, որը հիմնված է օգտագործողի վարքագծի յուրահատկությունների վրա:
- Թվային ինտերակտիվ հրապարակումների ծառայությունների օգտագործողի ուղղորդման հավանականային մոդելը, որը թույլ է տալիս, անկախ վիճակագրական տվյալներից, կանխագուշակել օգտագործողի հերթական գործողությունը:
- Թվային ինտերակտիվ հրապարակումների ծառայությունների օգտագործողի վարքագծի հիման վրա օգտագործողի հերթական գործողության կանխագուշակման և թվային ինտերակտիվ հրապարակումների ծառայությունների վրա կատարվող DoS հարձակումների հայտնաբերման ալգորիթմները և ծրագրային մոդուլները:

Ստացված արդյունքների ապրոքացիան. Աշխատանքի հիմնական արդյունքները ներկայացվել և քննարկվել են “Computer Science and Information Technologies (CSIT)”

միջազգային կոնֆերանսին (2013թ., ք. Երևան), Կասպերսկու լաբորտորիայի կողմից անցկացվող “It Security For The New Generation 2013” (2013թ., ք. Երևան) և “It Security For The New Generation 2013” (2013թ., ք. Լոնդոն) ուսանողական կոնֆերանսներին, վերջինի ընթացքում աշխատանքը ստացել է Best Paper մրցանակը: Աշխատանքը նաև քննարկել է ՀՊՃՀ ՏԱԾԱ ամբիոնի գիտական սեմինարների ընթացքում (2011-2014թ., ք. Երևան) և ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտի ընդհանուր սեմինարին:

Հրատարակումներ. Աշխատանքի հիմնական արդյունքները հրատարակվել են 3 գիտական աշխատություններում, որոնք բերված են սեղմագրի վերջում:

Ատենախոսության կառուցվածքը և ծավալը. Ատենախոսական աշխատանքը կազմված է ներածությունից, երեք գլուխներից, վերջաբանից, օգտագործված գրականության ցանկից և հավելվածից: Աշխատանքի ընդհանուր ծավալն է 119 էջ, ինչը ներառում է 25 նկար: Գրականության ցանկը կազմում է 45 վերնագիր, իսկ հավելվածների ընդհանուր ցավալն է 4 էջ:

ԱՇԽԱՏԱՆՔԻ ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆԸ

Ներածության մեջ հիմնավորված է թեմայի արդիականությունը, ձևակերպված են աշխատանքի նպատակը, գիտական նորությունները, պաշտպանության ներկայացվող հիմնական դրույթները:

Առաջին գլխում հետազոտվել են թվային ինտերակտիվ հրապարակումների ծառայությունները, նրանց զարգացման ուղիները և սպառնացող վտանգները:

Անց է կացվել DoS հարձակումների ուսումնասիրություն, հետազոտվել են հարձակումների հիմնական տեսակները, նրանցից պաշտպանության ընդունված միջոցները: Դիտարկվել են հարձակումներից պաշտպանության միջոցների թերությունները:

Վերջում, կատարված ուսումնասիրությունների հիման վրա, ձևակերպվել է ատենախոսական աշխատանքի նպատակը և դրվել են դրան հասնելու խնդիրները:

Երկրորդ գլխում հետազոտվել են վեբ օգտագործողի և թվային ինտերակտիվ հրապարակման ծառայության օգտագործողի վարքագծերը: Հետազոտության արդյունքում բացահայտվել են վարքագծերի առանձնահատկությունները:

Հետազոտված է թվային ինտերակտիվ հրապարակման ծառայության օգտագործողի վարքագիծը տարբեր միջավայրներում (աշխատանք, ժամանց) և տարբեր օգտագործողի սարքավորումների վրա:

Առաջարկված է թվային ինտերակտիվ հրապարակման ծառայության օգտագործողի վարքագծի նկարագրության մեթոդ, հիմնված վրձակագրական տվյալների վերլուծության վրա: Մեթոդը հիմնված է հետևյալ տվյալների վրա՝

- Ամսագրի եզակի նույնարկիչ
- Ընթացիկ էջ
- Նախորդ էջեր
- Օգտագործողի սարքավորման տեսակ
- Ուղղորդման ռեժիմ (հաջորդական կամ հղումներով)
- Ինտերնետ կապի արագություն
- Hit ratio
- Լրացուցիչ տվյալներ (օրինակ աշխարհագրական դիրք)

Հրապարակման նույնարկիչը օգտագործվում է սեսիայում օբյեկտը տարբերակելու նպատակով, քանի որ միաժամանակ տարբեր հրապարակումներ կարող են ընթերցվել: Ընթացիկ էջը այն էջն է, որը պետք է վերլուծվի հղումներ և ակտիվ կոմպոնենտներ հայտնաբերելու համար, որոնք թույլ կտան կանխագուշակել օգտագործողի հերթական գրոծողությունը:

Օգտագործողի սարքավորման տեսակը օգտագործվում է մոդելում ուղղորդման առաջնահերթությունը որոշելու համար, երբ սկզբնական տվյալները հասանելի չեն: Այս չափանիշը առանձին չի օգտարծվում: Ինտերնետի միացման արագությունը հաշվի է առնվում այս չափանիշը օգտագործելիս: Օրինակ, երբ օգտագործողը բացել է հրապարակումը պլանշետ սարքի վրա, ուղղորդման ռեժիմը կհամարվի հաջորդական և սերվերը կպատրաստի հաջորդ էջը մատուցման, սակայն համացանցին միացման ցածր

արագության դեպքում (երբ առաջին էջը բեռնելը երկար ժամանակ է պահանջել) ուղղորդման ռեժիմը կփոխվի հղումայինի:

Ուղղորդման ռեժիմը, ինչպես երևում է վերը նկարագրված օրինակում, դրոշակ է, որը որոշում է, որ հերթական գրոծողությունն է ավելի հավանական տվյալ պահին՝ հաջորդ էջ անցնելը, թե մեկ այլ էջ անցումը հղման միջոցով: Երբ էջի վրա հղումներ չեն պարունակվում, ուղղորդման ռեժիմը համարվում է հաջորդական:

Լրացուցիչ տվյալները (օրինակ օգտագործողի աշխարհագրական դիրքը) կարող են ավելացնել կանխագուշակման ճշտությունը և պետք է ամեն տվյալի համար իրագործվեն առանձին ֆունկցիոնալության տեսքով: Աշխարհագրական դիրքի դեպքում տվյալ հրապարակման նախորդ ընթերցումների մասին տվյալները պետք է մշակվեն:

Hit ratio-ն օգտագործողի սեսիայում պահվող մոդելի օբյեկտի կարևոր մասերից է: Այն սկզբնարժեքավորվում է նեյտրալ արժեքով (0.5 կամ 50, 100 միավորանոց սանդղակում) և թարմացնում իր արժեքը կախված օգտագործողի գրոծողությունների կանխագուշակման հաջողությունից: Կարելի է որոշել շեմային արժեք, որից իջնելու դեպքում ուղղորդման ռեժիմը կփոփոխվի, քանի որ դա կնշանակի տվյալ կանխագուշակման մոտեցումը իրեն չի արդարեցնում տվյալ օգտագործողի համար:

Օգտագործելով թվային ինտերակտիվ հրապարակումների ծառայության օգտարժողի վարքագծի միտումները կարող ենք ստեղծել ծրագրային ապահովում, որը թույլ կտա կանխագուշակել օգտագործողի հերթական գրոծողությունը:

Քանի որ թվային ինտերակտիվ հրապարակման վիճակագրական տվյալները միշտ չէ, որ հասանելի են, գլխում դիտարկվում են առանց վիճակագրական տվյալների օգտագործողի վարքագծի կանխորոշման մեթոդների մշակման հնարավոր տարբերակները:

Գլխում դիտարկված են վեբ օգտագործողի վարքագծի գոյություն ունեցող մաթեմատիկական մոդելները և նրանց կիրառելիությունը թվային ինտերակտիվ հրապարակումների համար: Առաջարկված է թվային ինտերակտիվ հրապարակումների ծառայության օգտագործողի ուղղորդման հավանականային մոդել, որը ավելի ճշգրիտ է արտահայտում օգտագործողի վարքագծի տենդենցները, հաշվի առնելով հրապարակման վերաբերյալ այնպիսի տվյալներ, ինչպիսիք են հրապարակման տեսակը և նրա կառուցվածքը՝ էջից էջ տանող հղումները:

Հրապարակման x էջից դեպի y էջը ուղղորդումը մոդելավորելիս, պետք է հաշվի առնել ոչ միայն x էջի վրա դեպի y էջ տանող հղման առկայության փաստը, այլև այդ հղման օբյեկտի չափը և դիրքը էջի վրա: Ավելի մեծ հղումները ավելի մեծ հավանականություն ունեն քանեցվելու քան ավելի փոքրերը: Հղումները նույնպես կարող են տեղադրված լինել արմող էջի մակերեսով, ինչը դարձնում է նրանց օգտագործման հավանականությունը էլ ավելի մեծ (այս հղումները հաճախ օգտագործվում են սխալմամբ):

Դիցուկ x էջից վրա կա հղումների որոշակի բազմություն: Նշանակենք այդ բազմությունը L^x : Այն կարող է լինել դատարկ բազմություն, կամ կարող է արտահայտված լինել ինչպես $L^x = \{l_1^x, \dots, l_n^x\}$, որտեղ $n_x - p$ է էջի վրա հղումների քանակն է: Ենթադրեք y -ը մի էջ է, ուր տանում են L^x բազմության հղումներից մի քանիսը: Անվանենք այդ բազմությունը L_y^x

$L_y^x = \{l_{y_1}^x, \dots, l_{y_m}^x\}$, որտեղ m -ը դեպի y տանող հղումների քանակն է: x էջից դեպի y էջ հղումով տեղափոխվելու շանսը փոխկապակցված է x էջի վրա դեպի y էջ տանող

հղումների գումարային մակերեսին: Այդ շանքը նշանակենք $Fs(x,y)$: x էջից դեպի y էջ տանող հղում օբյեկտների մակերեսների գումարը նշանակենք $S(x,y)$:

$$S(x,y) = \sum_{i=1}^m sur(L_{y_i}^x)$$

որտեղ i -ն L_y^x բազմությունից $L_{y_i}^x$ հղում օբյեկտի համարն է, իսկ $sur(L_{y_i}^x)$ այդ հղում օբյեկտի մակերեսը: $Fs(x,y)$ -ը հաշվարկելու համար անհրաժեշտ է x էջի բոլոր հղում օբյեկտների մակերեսների գումարը, որը նշանակենք $S(x)$

$$S(x) = \sum_{j=1}^{n_x} sur(L_j^x)$$

որտեղ $sur(L_j^x)$ -ը L^x բազմությունից L_j^x հղում օբյեկտի մակերեսն է: Վերջապես $Fs(x,y)$ -ը կհաշվարկվի հետևյալ բանաձևով՝

$$Fs(x,y) = \begin{cases} \frac{S(x,y)}{S(x)}, & S(x) > 0, \\ 0, & S(x) = 0 \end{cases}$$

Օգտագործողի x էջից հղումով դեպի y էջ անցնելու շանքը կախված է հետևյալ գործոններից՝

- Հրապարակման տեսակ
- Ընթացիկ էջ
- Արդյոք ընթացիկ էջը հանդիսանում է դիտարկվող էջի նախորդ կամ հաջորդ էջը
- Ընթացիկ էջից դեպի դիտարկվող էջ տանող հղումները՝ նրանց չափը և քանակը

Երբ օգտագործողը գտնվում է x էջի վրա, նա կարող է կատարել երեք գործողություն ուղղորդման տեսակետից՝

- Թերթել դեպի հաջորդ էջ
- Թերթել դեպի նախորդ էջ
- Օգտագործե հղում այլ էջ ուղղորդվելու համար:

Որպեսզի կարողանանք կանխագուշակել, թե որ էջն է հարցվելու օգտագործողի քանի դեռ նա գտնվում է x էջի վրա, պետք է հաշվարկենք բոլոր էջերի հարցված լինելու շանքը: Այս նպատակով կհաշվարկենք անցումային արժեքներ ամեն էջի վրա, որոնք կանվանենք կշիռներ: Որքան մեծ է էջի կշիռը, այնքան մեծ է ընթացիկ էջից, այդ էջի հարցված լինելու շանքը:

w_n արժեքը կներկայացնի y էջի x -ի հաջորդ էջը լինելու փաստը: Երբ y -ը հանդիսանում է x -ի հաջորդ էջը, w_n -ի արժեքը կլինի 1, իսկ հակառակ դեպքում 0: Նմանապես կօգտագործենք w_p արժեքը, y էջի x -ի նախորդ էջը լինելու փաստը նկարագրելու համար: Էջ x -ից դեպի y հղման առկայությունը կավելացնի y էջի կշիռը w_l -ով, որը կհաշվարկենք՝

$$w_l = Fs(x,y) * L(x,Nm),$$

Որտեղ $L(x,Nm)$ -ը հղում օգտագործելու գործակից է, որի արժեքը կախված է ընթացիկ էջի համարից և ուղղորդման ռեժիմից (navigation mode – Nm)՝

	$Nm = 1$	$Nm = 2$
$x = 1$	0.36	0.52
$x \neq 1$	0.21	0.46

$Nm = 1$ – հաջորդական ուղղորդում, $Nm = 2$ – հղումային ուղղորդում:

Այսպիսով y էջի համար գումարային կշիռը կհաշվարկենք գումարելով այդ արժեքները և բազմապատկելով համապատասխան գործակիցներով:

$$W_y = k_n w_n + k_p w_p + k_l w_l,$$

որտեղ k_n, k_p և k_l գործակիցները կարող են լինել կամ հաստատուն արժեքներ, հաշվարկված վիճակագրական տվյալներից, կամ կարող են լինել սկզբնարժեքավորված որոշակի նեյտրալ արժեքներով և հետագայում ճշգրտվեն մոդելի աշխատանքի ընթացքում:

Այսպիսով, երբ օգտագործողը x էջի վրա է, x -ից բացի բոլոր էջերի համար հաշվարկվում է x էջից անցման կշիռները: Կշիռներից հավանականությունների անցում կատարելու համար պետք է հաշվարկել x -ից տարբեր բոլոր էջերի գումարային W_T կշիռը՝

$$W_T = \sum_{i=1, i \neq x} W_i,$$

որտեղ n -ը տվյալ հրապարակման էջերի քանակն է:

Հրապարակման y էջի հարցված լինելու $p_y(x)$ հավանականությունը այն դեպքում, երբ օգտագործողը գտնվում է x էջի վրա, կհաշվարկենք հետևյալ բանաձևով՝

$$p_y(x) = \frac{W_y}{W_T}.$$

որտեղ W_y -ն y էջի կշիռն է:

Ունենալով բոլոր էջերի համար հարցված լինելու հավանականությունները, կարող ենք դրանք դասակարգել նվազման կարգով և օրինակ նախաբեռնել այդ էջերի պատկերման համար անհրաժեշտ ռեսուրսները:

Հիմնված թվային ինտերակտիվ հրապարակման օգտագործողի հերթական գործողությունը կանխագուշակելու հնարավորության վրա, գլխում առաջարկված է թվային ինտերակտիվ հրապարակումների ծառայության վրա իրագործված DDoS հարձակումների հայտնաբերման մոտեցում: Առաջարկված է էջից էջ անցումների գրաֆ, որը նկարագրում է թե կամայական էջի վրա գտնվելու պարագայում, որ էջ անցումն է ամեա հանանականը: Էջերի անցումների գրաֆը անընդհատ թարմացվում է հիմնված օգտագործողների կողմից կատարված հարցումների հիման վրա: Որևէ էջի համար գրաֆում գործակիցը շատ արագ փոփոխվել սկսելը կարող է համարվել DDoS հարձակման նշան: Որոշակի ընդմիջումով, հաշվարկվում է էջերի անցման նոր գրաֆ և համեմատվում արդեն հաշվարկվածի հետ, կտրուկ փոփոխությունները կհամարվեն DDoS հարձակման նշան:

Երրորդ գույքը նվիրված է առաջարկված մեթոդների պրակտիկ իրագործմանը: Գլխում նկարագրված է թվային ինտերակտիվ հրապարակման վիճակագրական տվյալների կուտակման և վերլուծության եղանակները:

Նկարագրված են 3 ծրագրային մոդուլների իրագործումը՝

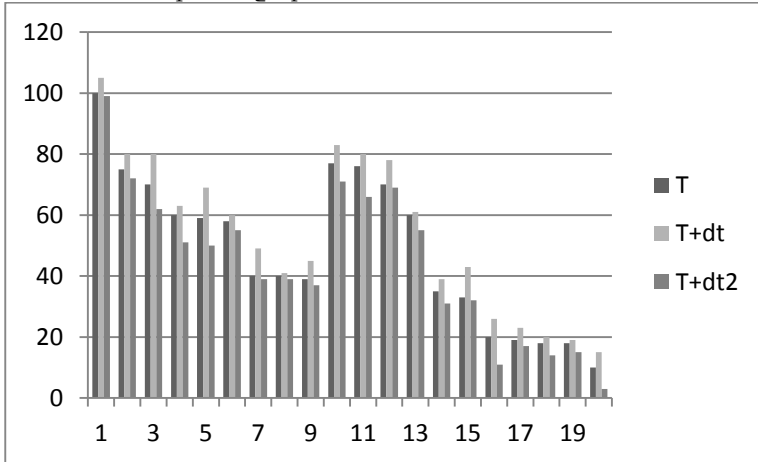
- Օգտագործողի հերթական գործողության կանխագուշակման AP (action prediction) մոդուլ;
- AP մոդուլի վրա հիմնված ռեսուրսների նախաբեռնման մոդուլ, որը թույլ է տալիս, ենթադրություն անելով օգտագործողի ուղղորդման մասին, նախապես բեռնել հաջորդ էջը արտապատկերելու համար անհրաժեշտ ռեսուրսները և բարելավել թվային ինտերակտիվ հրապարակումը

ընթերցելու փորձը՝ կրճատել ռեսուրսների բեռնմանը սպասելու ժամանակը:

- DoS հարձակումներ հայտնաբերող BBDD (Behavior Based DDoS Detector) մոդուլ:

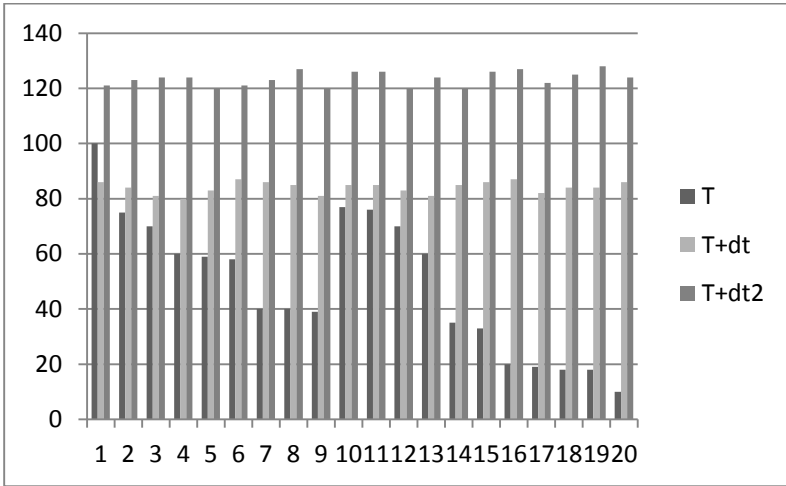
Ստեղծված ծրագրային մոդուլը օգտագործում է վիճակագրական տվյալներ այն դեպքում երբ տվյալները հասանելի են, իսկ երբ տվյալները հասանելի չեն (օրինակ նոր հրապարակված հրապարակման դեպքում) օգտագործում է AP մոդուլի վիճակագրական տվյալներ սիմուլացնելու ունակությունը, որը թույլ է տալիս ստանալ վիճակագրական տվյալների փոխարինիչ:

Ցանկացած հրապարակման հրատարակվելուց հետո, վերջինումն օգտագործողի վարքագիծը ձեռք է բերում որոշակի տեսք և զգալիորեն չի փոխվում հրապարակման բոլոր ընթերցումների ընթացքում: Այս իսկ պատճառով, իմանալով, որ հրապարակման X էջը որոշակի ժամանակահատվածում հարցվում է N անգամ, կարող ենք ենթադրել, որ հաջորդ նույն ժամանակահատվածում հարցումների քանակը չի կարող փոփոխվել շատ կտրուկ: Այն կարող է աճել կամ նվազել, բայց այդ փոփոխությունը բնականոն օգտագործման ժամանակ համաչափ է:



Նկար 1: Էջերի հարցումների քանակությունները T , $T+dt$, $T+dt2$ պահերին՝ բնական աճ

Նկար 1 գրաֆիկում ներկայացված են ժամանակի T , $T+dt$ և $T+dt2$ պահերին, հրապարակման էջերի հարցումների քանակությունները: T -ն ընդունելով բազային վիճակ, համեմատենք $T+dt$ և $T+dt2$ վիճակների հետ: $T+dt$ պահին ինչպես երևում է գրաֆիկից, հարցումների քանակությունը աճել է: Հրապարակման բոլոր էջերը ընթերցվել են ավելի շատ անգամ, բայց ինչպես երևում է գրաֆիկից քանակության ընթերցումը համաչափ է, և գրաֆիկի տեսքը զգալիորեն չի փոխվել: Համեմատելով ժամանակի T պահին վիճակը $T+dt2$ պահին վիճակի հետ, տեսնում ենք որ ընթերցումների քանակը նվազել է, բայց կրկին անգամ փոփոխվել է համաչափ, ինչը վկայում է օգտագործման բնականոն լինելու մասին:

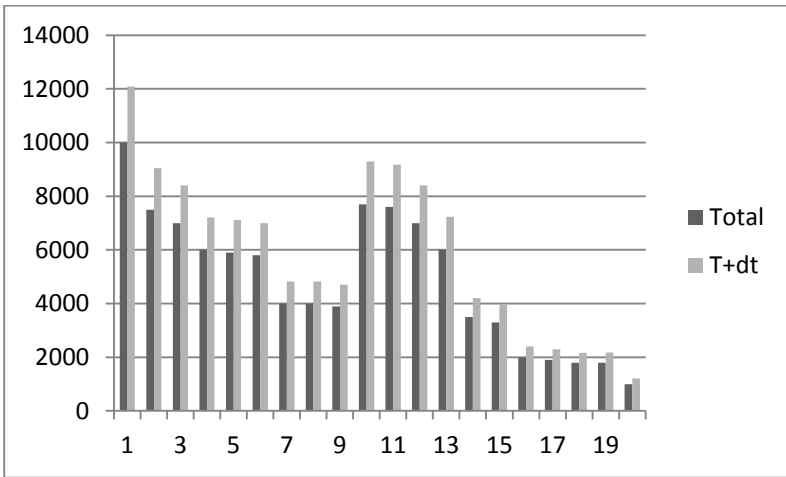


Նկար 2: Էջերի հարցումների քանակությունները T, T+dt, T+dt2 պահերին՝ անբնական փոփոխություն

Նկար 2 գրաֆիկում համեմատենք ժամանակի T պահին ինտերակտիվ թվային հրապարակման էջերին կատարվող հարցումների քանակությունները այլ T+dt և T+dt2 պահերին քանակությունների հետ: Այս դեպքում երևում է, որ հարցումների քանակությունը ավելացել է ոչ համաչափ: Այն էջերը, որոնք հարցվում էին մեծ քանակությամբ, շարունակում են շատ հարցվել, բայց հարցումների փոքր քանակություն ունեցող էջերը, նույնպես հարցվում են շատ, ինչը վկայում է օգտագործման անբնական լինելու մասին, մեծ հավանականությամբ տեղի ունեցողը հարձակում է: Այս պնդումը հիմնավորվում է նրանով, որ այն էջերը, որոնք չէին վայելում մեծ համբավ և անհետաքրքիր էին ընթերցողների համար, չեն կարող հանկարծակիորեն դառնալ հետաքրքիր: Հետևաբար այդ էջերի հարցումները կրում են ահրեստական բնույթ:

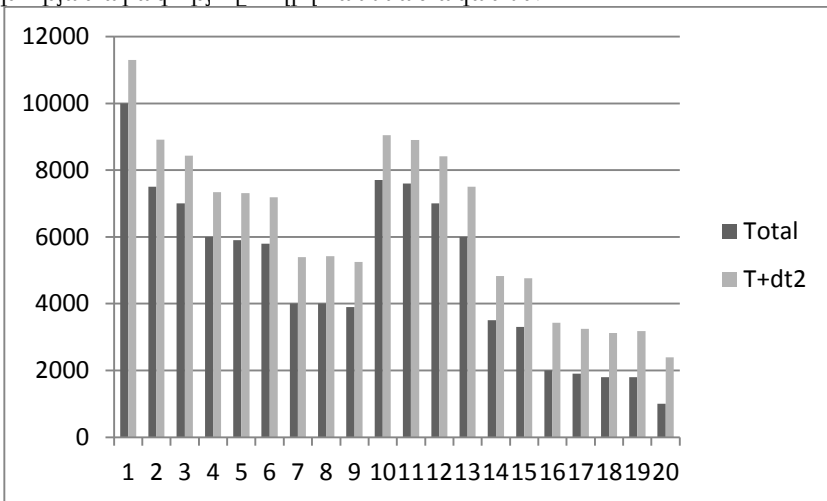
Մակայն միշտ չէ, որ հարմար է պահել ամեն հրապարակման բոլոր էջերի հարցումների քանակությունները ժամանակի ցանկացած պահի: Ինչը կարող է պայմանավորված լինել հիշողություն խնայելու նկատառումով: Այս պատճառով կարող ենք նվազեցնել սերվեի մասում պահպանվող և մշակվող ռեսուրսների ծավալը օգտագործելով միայն թվային ինտերակտիվ հրապարակման էջերին կատարված հարցումների ընդհանուր քանակությունը, խուսափելով snapshot-ներ պահելուց: Սա թույլ կտա զգալիորեն նվազեցնել հիշողությունում պահվող տվյալերի քանակը, սակայն կմեծացնի հաշվողական ռեսուրսների ծախսը, քանի որ ցանկալի արդյունքները ստանալու համար անհրաժեշտ մշակման ենթակա տվյալների ծավալը կմեծանա:

Նկար 3 գրաֆիկում ներկայացված են Total շարքում թվային ինտերակտիվ հրապարակման էջերին կատարված հարցումների ընդհանուր քանակը, ժամանակի T պահին, հրապարակումից 1 ժամ անց: T+dt շարքում ներկայացված է հարցումների քանակությունը ժամանակի T+dt պահին: Հարցումների ընդհանուր քանակը նվազել չի կարող: Ինչպես երևում է գրաֆիկից, հարցումների քանակությունը աճել է:



Նկար 3: Էջերի հարցումների ընդհանուր քանակությունները T և T+dt պահերին՝ բնական աճ

Գրաֆիկից նույնպես երևում է, որ հարցումների քանակության աճը այն էջերի համար որոնք ավելի հետաքրքիր պարունակություն ունենին, և հետևաբար ավելի մեծ քանակությամբ հարցումներ, ավելի մեծ է քան ավելի քիչ հարցումներ ունեցող էջերի համար: Այսինքն հարցումների քանակությունը և հարցումների քանակության փոփոխության արագությունը ուղիղ համեմատական են:

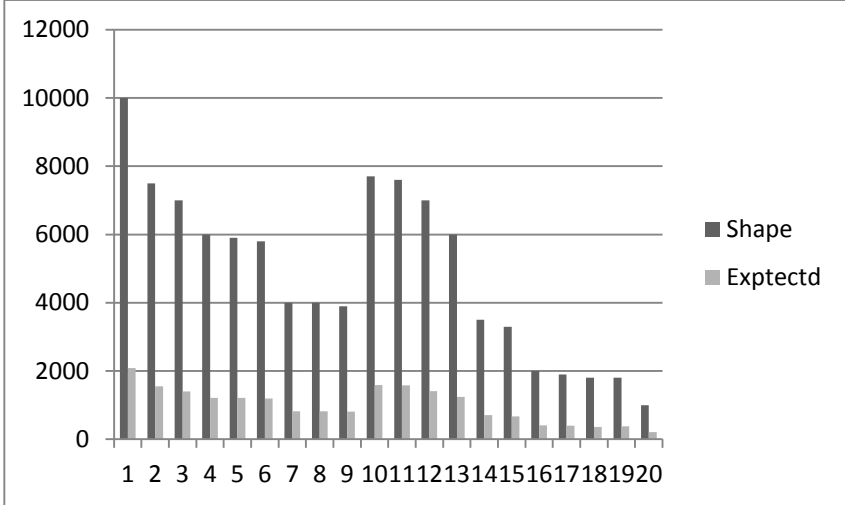


Նկար 4: Էջերի հարցումների ընդհանուր քանակությունները T և T+dt2 պահերին՝ անբնական աճ

Նկար 4 գրաֆիկի T+dt2 շարքում ներկայացված է իրադարձությունների մեկ այլ ընթացք, որի դեպքում հարցումներ քանակությունը բոլոր էջերի համար ավելանում է նույն չափով: Իրադարձությունների այս ընթացքը ոչ բնականոն օգտագործման արդյունք

է և էջերին կատարված հարցումների քանակությունների համաչափ աճը հանդիսանում է DoS հարձակման նշան:

Հանենք $T+dt$ և շարքերի արժեքներից Total շարքի արժեքները: Ստացված արժեքները, Total շարքի արժեքների հետ մեկ տեղ, ներկայացված են ստորև բերված գրաֆիկում:



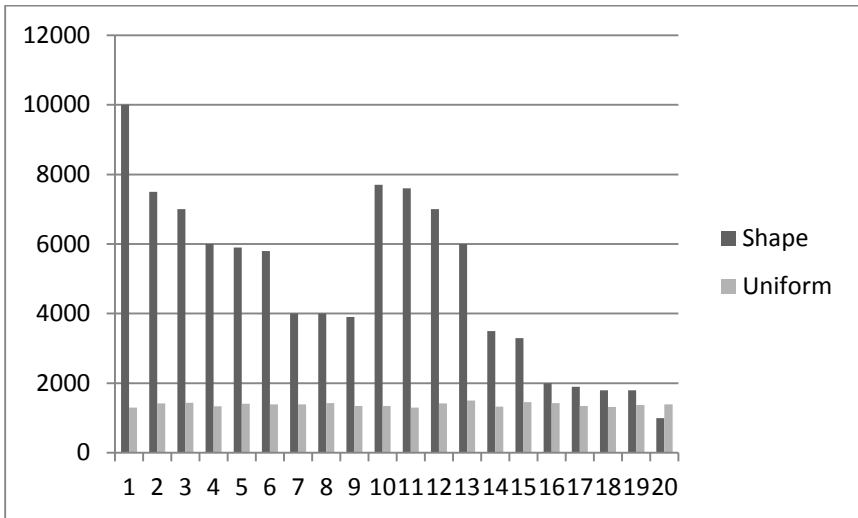
Նկար 5: էջերի հարցումների ընդհանուր քանակությունները համեմատած բնական աճի հետ

Ինչպես երևում է ստացված գրաֆիկից հարցումների քանակության աճի գրաֆիկի տեսքը նման է ընդհանուր հարցումների գրաֆիկին, ինչը իր հերթին խոսում է բնականոն օգտագործման մասին:

Հանենք $T+dt$ և $T+dt2$ շարքերի արժեքներից Total շարքի արժեքները և ներկայացնենք նրանք ստորև բերված գրաֆիկում համեմատելով Total շարքի արժեքների հետ:

Նկար 6 գրաֆիկում երևում է, որ փոփոխությունը բոլոր էջերի համար կազմել է նույնատիպ քանակություն: Գրաֆիկների տեսքերի իրար նման չեն: Այս փաստն էլ խոսում է նրա մասին որ հարցումները կատարված են եղել ոչ թե, մարդկային վարքագրծ ունեցող, մարդկանց այլ նախապես ծրագրավորված վարքագիծ ունեցող բոթերի կողմից: Այս մոտեցման դեպքում կարող ենք պահել սերվերի հիշողությունում թվային ինտերակտիվ հրապարակման էջերի ընթերցման հարցումների ընդհանուր քանակությունը և միավոր ժամանակ առաջ վիճակի snapshot: Համեմատելով ամեն էջի հարցումների քանակի փոփոխությունը էջերի հարցումների քանակի հետ, կարող ենք գնահատել արդյոք օգտագործումը գտնվում է նորմայի սահմաններում թե ոչ:

Հետագայում գլխում կատարված է մշակված մոդուլների արդյունավետության գնահատում, ինչի արդյունքում ստացվել է, որ DoS հարձակումների հայտնաբերման առաջարկված մոտեցումը թվային ինտերակտիվ հրապարակումների ծառայությունների համար գերազանցում է գոյություն ունեցող մեթոդները 20-80%-ով կախված կարգաբերումից և ծառայության տեսակից:



Նկար 6: էջերի հարցումների ընդհանուր քանակությունները համեմատած անբնական աճի հետ

Աշխատանքի հիմնական արդյունքները հետևյալն են՝

- Առաջարկվել է թվային ինտերակտիվ հրապարակումների ծառայությունների օգտագործողի վարքագծի նկարագրության մեթոդ, որը հիմնված է վիճակագրական տվյալների վրա և թույլ է տալիս կանխագուշակել օգտագործողի հերթական գործողությունը: [1,2]
- Մշակվել է թվային ինտերակտիվ հրապարակումների ծառայությունների օգտագործողի ուղղորդման հավանականային մոդել, որը անկախ վիճակագրական տվյալներից թույլ է տալիս կանխագուշակել օգտագործողի հերթական գործողությունը: [3]
- Առաջարկվել է թվային ինտերակտիվ հրապարակումների ծառայությունների վրա կատարվող DoS հարձակումների հայտնաբերման մեթոդ, հիմնված օգտագործողի վարքագծի յուրահատկությունների վրա: [1,2]
- Նախագծվել և իրագործվել է թվային ինտերակտիվ հրապարակումների ծառայությունների օգտագործողի վարքագծի հիման վրա օգտագործողի հերթական գործողության կանխագուշակման ծրագրային մոդուլ: [2]
- Նախագծվել և իրագործվել է օգտագործողի հերթական գործողության կանխագուշակման մոդուլի վրա հիմնված ծրագրային մոդուլ, որը թույլ է տալիս բարձրացնել համակարգի արագագործությունը, ռեսուրսների նախորոք բեռնման միջոցով: [3]
- Նախագծվել է թվային ինտերակտիվ հրապարակումների ծառայությունների վրա կատարվող DoS հարձակումների հայտնաբերման ալգորիթմ, որը ապահովում է բոթերի հայտնաբերման 20-80% ավելի բարձր ճշտություն, հրապարակմանը հարմարվող լինելու շնորհիվ: Ալգորիթմը իրագործվել է ծրագրային մոդուլի տեսքով: [1,2,3]

**ԱՏԵՆԱԽՈՍՈՒԹՅԱՆ ԹԵՄԱՅԻ ՇՐՋԱՆԱԿՆԵՐՈՒՄ ՀՐԱՊԱՐԱԿՎԱԾ
ԱՇԽԱՏՈՒԹՅՈՒՆՆԵՐԻ ՑԱՆԿ**

- [1] V. H. Darbinyan; R. H. Vardanyan, "Detecting DDoS attacks on Digital Interactive Publication Hosting Services", Proceedings of SEUA Series "Information technologies, Electronics, Radio engineering" Issue 15, pp. 20-25, Yerevan, Armenia, 2012.
- [2] V. H. Darbinyan, "Analysis of user behavior when reading Digital Interactive Magazine online on various devices", CSIT Proceedings of the conference, Sep 23-27, pp. 445-446, Yerevan, Armenia, 2013.
- [3] V.H. Darbinyan, "A Probabilistic Model of User Navigation in a Digital Interactive Publication", Transactions of IIAP NAS RA, Mathematical Problems of Computer Science, vol. 41, pp 93-102, Yerevan, Armenia, 2014.

ИССЛЕДОВАНИЕ И РАЗРАБОТКА СРЕДСТВ ПОВЫШЕНИЯ ЗАЩИЩЁННОСТИ И БЫСТРОДЕЙСТВИЯ СЕРВИСОВ ЦИФРОВЫХ ПУБЛИКАЦИЙ

РЕЗЮМЕ

В последние годы интернет технологии стремительно развиваются, включая в себя новые приложения. Развитие веб технологий позволили создателям печатной продукции (университетам, издательским домам, частным издателям и т.д.) начать переход от существующих традиционных печатных издательских технологий к функционирующим в режиме онлайн и основанным на возможностях веб технологиям тем самым сократить время подготовки и дистрибуции публикации и стоимость ее создания. В частности, цифровые интерактивные публикации, являясь более адаптированными к пользователям, представляют большой интерес для пользователей, издателей и рекламодателей. Цифровые интерактивные публикации также являются быстро развивающейся средой для онлайн рекламы. Заметим, что оборот онлайн реклам на 2013г составил 42 миллиарда долларов, тем самым в первые превзошел оборот телевизионной рекламы (39 миллиардов). Онлайн реклама имея более высокий фактор возврата по сравнению с традиционной рекламой, также имеет свои недостатки, основным из которых является Кликфрод. Кликфрод причиняет большие расходы издателям и рекламодателям, и вместе с ростом объёмов онлайн рекламы, затраты на кликфрод тоже увеличиваются. По данным компании Google – одного из лидеров в сфере онлайн рекламы, порядка 10% кликов на рекламы является кликфродом. Кликфрод часто выполняется по принципу Denial of Service (DoS) атак, когда многочисленные запросы посылаются на веб ресурс, и даже если веб ресурс не выходит из строя, то регистрируется большое количество запросов на рекламу, что приводит к большим затратам. Основная проблема при обнаружении DoS в том, что атакующая сторона использует легитимные запросы для того чтобы заполнить мишень и сложно отличить запрос сделанный ботом от запроса сделанного пользователем. И так есть задача каким-либо способом отличить легитимных пользователей от ботов, что довольно сложно, так-как боты быстро развиваются и улучшают свою способность имитировать поведение пользователя. В цифровых интерактивных публикациях, в отличии от обычных веб страниц, поведение пользователя более предсказуемое. Этот факт имеет потенциал стать средством обнаружения ботов. Стремительный рост рынка цифровых интерактивных публикаций представляет большой интерес для онлайн рекламодателей, поскольку многие издания переходят от традиционных печатных публикаций к цифровым. Переход от традиционных печатных публикаций к цифровым, приносит с собой проблему удобства пользователя. Пользователи ожидают что цифровые издания были такими же доступными как печатные, и чтоб чтение было бы плавным и непрерывным. Многие пользователи не готовы долго ждать загрузки публикации и предпочитают печатный вариант, до тех пор, пока проблемы с загрузкой существуют. Исходя из вышесказанного актуально исследование и разработка средств отделения запросов сделанных ботами от запросов пользователей, а так же методов повышения быстродействия сервиса цифровых интерактивных публикаций.

Цель и задачи работы – исследование и разработка средств повышения быстродействия и защищенности от DoS атак сервисов интерактивных цифровых публикаций. Для достижения указанной цели в работе ставятся и решаются следующие основные задачи:

- Исследование сервисов цифровых публикаций, разработка средств описания поведения пользователя и создание модели поведения пользователя.
- Разработка метода и программного обеспечения обнаружения DoS атак на сервисы цифровых интерактивных публикаций, который будет учитывать особенности среды.
- Разработка метода и программного обеспечения повышения быстродействия сервисов цифровых интерактивных публикаций.

Основные результаты и выводы

1. Предложен метод описания поведения пользователя сервисов цифровых интерактивных публикаций на основе статистических данных, который позволяет предугадывать очередное действие пользователя [1,2].
2. Разработана вероятностная модель поведения пользователя сервисов цифровых интерактивных публикаций, которая позволяет предугадывать очередное действие пользователя вне зависимости от статистических данных [3].
3. Предложен метод обнаружения DoS атак на сервисы цифровых интерактивных публикаций, на основе особенностей поведения пользователя [1,2].
4. Разработан программный модуль предугадывания очередного действия пользователя сервисов цифровых интерактивных публикаций на основе поведения пользователя [2].
5. На основе программного модуля предугадывания действий, разработан программный модуль, позволяющий повысить быстродействие сервисов цифровых интерактивных публикаций, способом предварительной загрузки данных [3].
6. Разработан алгоритм и программный модуль обнаружения DoS атак на сервисы цифровых интерактивных публикаций, который обеспечивает 20-80% более высокую точность в обнаружения ботов за счет адаптации к публикациям [1,2,3].

Vahram Darbinyan
RESEARCH AND DEVELOPMENT OF MEANS FOR SPEED AND SECURITY
IMPROVEMENT IN DIGITAL PUBLICATION SERVICES

RESUME

In recent years, Internet technologies are evolving rapidly, including more applications every day. Development of web of technologies has allowed the publishers of printed materials (universities, publishing houses, private publishers, etc.) to begin the transition from the existing traditional print publishing technology to ones functioning online and based on the capabilities of the Web technologies, thereby saving on the preparation and distribution of publications and reducing the cost of creation. In particular, interactive digital publications, being more adapted to the users are of great interest to users, publishers and advertisers. Digital interactive publications are also a fast-paced environment for online advertising. Note that the turnover of online advertising in 2013 was \$42 billion, which for the first time surpassed television advertising turnover (\$39 billion).

Online advertising has higher return factor compared to traditional advertising, but it also has its drawbacks, the main one being click fraud. Click fraud causes great expense to publishers and advertisers, and with increasing volumes of online advertising expenses on click fraud are also increasing. According to the company Google - one of the leaders in online advertising, about 10% of clicks on advertising are fraudulent. Click fraud is often performed on the same principle of Denial of Service (DoS) Attacks, when multiple requests are sent to a web resource, and even if the web resource does not fail, a large number of requests on advertising is recorded, which leads to higher costs. The main problem with detecting DoS is that the attacker uses legitimate requests to flood the target and it's hard to distinguish requests made by a bot from requests made by the user. Thus there is the problem of distinguishing legitimate users from bots, which is quite difficult, as bots develop rapidly and improve their ability to mimic the behavior of a user. In interactive digital publications, unlike conventional web pages, user behavior is more predictable. This fact has the potential to become a means for detecting bots. The rapid growth in the market of digital interactive publications is of great interest for online advertisers, as many publications are moving from traditional print publications to digital.

The transition from traditional print publications to digital, brings with it the problem of usability. Users expect digital publications to be available as printed, and to provide smooth and uninterrupted use experience while reading. Many users are not willing to wait long for the publication to download and would prefer a printed version, as long as there are problems with loading. Based on the aforementioned it is relevant to conduct research and development of means of telling requests made by bots from user requests, as well as methods for increasing the speed of digital interactive publication services.

The purpose and objectives

The main purpose of the work is research and development of means to improve the performance and protection from DoS attacks for digital interactive publication services. To achieve this goal, the following tasks must be solved:

- Research of digital publishing services, the development of means of user behavior description and creation of a user behavior model.
- Development of a method and software of DoS attack detection on services of interactive digital publications, which will take into account the characteristics of the environment.
- Development of a method and software to improve the performance of digital interactive publications services.

The main results are:

1. A method for describing the user's behavior in digital interactive publications services has been proposed, which is based on use of statistical data and allows predicting the next user action [1,2].
2. A probabilistic model of user behavior in digital interactive publishing services has been developed that allows predicting the next action of the user, regardless of the availability of statistical data [3].
3. A method of detecting DoS attacks on interactive digital publications services has been proposed, which is based on user behavior analysis [1,2].
4. A software module has been developed that allows prediction of the next user action in digital interactive publishing services based on user behavior [2].
5. Based on action prediction software, a software module has been developed for improving performance of digital interactive publication services, by means of data pre-loading [3].
6. An algorithm and software module for detecting DoS attacks on digital interactive publication services is developed, which provides 20-80% higher accuracy in detecting bots by being adoptive to the publication [1,2,3].

Ծավալը՝ 20 էջ: Տպաքանակը՝ 100:
ՀՀ ԳԱԱ ԻԱՊԻ կոմպյուտերային պոլիգրաֆիայի լաբորատորիա:
Երևան, Պ. Սևակի 1