

Պաշտոնական ընդհանրասի կարծիք

Թիմուր Զամղարյանի

«Տեղեկատվական ցանցում տվյալների ամբողջականության ապահովման համակարգի մշակումը» թեմայով Ե.13.04 «Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի մաթեմատիկական և ծրագրային ապահովում» մասնագիտությամբ տեխնիկական գիտությունների գիտական աստիճանի հայցման ատենախոսության վերաբերյալ

Տեխնոլոգիաների կատարելագործմանը զուգընթաց, մեծանում են դրանց չարամիտ գործադրմամբ հարձակումներ իրականացնելու հնարավորությունները տեղեկատվական ցանցերում, մինչդեռ, այդ կրիտիկական ենթակառուցվածքների հուսալիության խաթարումները հղի են մեծ կորուստներով: Զամղարյանի հետազոտության առարկան տեղեկատվական ցանցերում տվյալների ամբողջականության ապահովումն է նոր ի հայտ եկող սպառնալիքների պայմաններում: Դրանք կապված են մեքենայական ուսուցման (ՄՈւ) բերած հնարավորություններով ցանցային գրոհներ կազմակերպելու հետ: Այդ առումով, նրա աշխատությունը ներկայացնում է նման բարդ ներխուժումների հայտնաբերման նոր մեթոդներ և համակարգեր, որոնք նաև ներդրված են կիրառության մեջ: Այս լուծումները նույնպես հենված են ՄՈւ վրա:

Ըստ կառուցվածքի, ատենախոսության հիմնական նյութը շարադրված է 4 գլուխներում: Այն ունի համառոտ ներածություն և գրականության ցանկ 98 աղբյուրներով:

Ներածությունը անդրադառնում է ցանցերի անվտանգության ապահովման նորոշյա խնդիրներին, մատնանշում այն մարտահրավերները, որոնց բախվում են համակարգի պատասխանատուները: Դրանց թվում է մեքենայական ուսուցման գործիքակազմով հարձակումների դեմ պայքարի կանխավ որոշված սխեմաներով հայտնաբերման անարդյունավետությունը, որի պատճառով, ներխուժման հայտնաբերման համակարգերը ստիպված են անցնել ՄՈւ-ով արդիականացված եղանակների: Ըստ այդմ, հեղինակը սահմանում է այն գիտական նպատակը, որի իրականացման ուղղությամբ կատարած աշխատանքի նկարագրությունը ընդգրկում է ատենախոսության մյուս երեք գլուխները: Դա ՄՈւ միջոցներով հարձակման ենթարկված ցանցերում ներխուժման հայտնաբերման այնպիսի համակարգի նախագծումն է, որն արդյունավետ կերպով աշխատում է ցանցի միջուկի մակարդակում: Այս խնդրի լուծման բեռն ընկած է ցանցն օգտագործող կազմակերպությունների, ոչ թե ցանցային օպերատորների վրա:

Ատենախոսության առաջին գլխում վերլուծվում են ժամանակակից ցանցային ճարտարապետությունները, այս ենթակառուցվածքներում հարձակումների եղանակները, դրանցում ներխուժման հայտնաբերման համակարգերը: Մասնավորապես, քննարկվում են հայտնաբերման գործող համակարգերի

սահմանափակումները՝ տվյալների ամբողջականության նկատմամբ ՄՈւ միջոցներով կատարվող հարձակումների պարագայում: Այս հեղինակը անդրադառնում է այս բնագավառում առաջացած հիմնական խնդիրներին, դրանց լուծման ուղղությամբ իր սույն ձեռնարկին ու ստացած արդյունքներին:

Երկրորդ գլխում մշակվում է ցանցի կայունությունը գնահատելու ու փոխանցվող տվյալների ամբողջականության ապահովման մոդել: Նկարագրվում է նաև ՄՈւ միջոցներով կազմակերպված գրոհի մոդել: Անհրաժեշտ է եղել պատշաճ կերպով (augmentation and boosting) գեներացնել հնարավոր վնասարար ծրագրային ապահովումից եկող տվյալների հավաքածուներ՝ հարձակումները կանխատեսող նեյրոնային ցանցերի ուսուցման համար: Ներկայացվում է նաև համապատասխան լուծումների ծրագրային ապահովումը:

Երրորդ գլուխը քննարկում է որոշ տիպերի նեյրոնային ցանցերի (ռեկուրենտ, փաթույթային, գեներատիվ-մրցակցային և պարկուճային) կիրառմամբ վնասարար ծրագրերի հայտնաբերման մեթոդներ: Այստեղ հետազոտվում է նաև softmax ֆունկցիայի օպտիմիզացիայի միջոցով նեյրոնային ցանցերի ճանաչողական որակները նշանակալի բարձրացնելու խնդիրը: Գրականության մեջ հայտնի մեթոդների համեմատությամբ, հեղինակի մշակումները տալիս են 11-19% բարելավում:

Չորրորդ գլխում հեղինակը անդրադառնում է բուն ներխուժման հայտնաբերման համակարգի հուսալիության բարձրացման խնդրին, դրա ամբողջականության նկատմամբ հնարավոր հարձակման դեպքում: Առաջարկվում է լուծում, համապատասխան ծրագրային ապահովում: Այստեղ նույնպես, ՄՈւ մոտեցումները առանցքային են, օգտագործվել է k մոտակա հարևանների ալգորիթմը: Դրա շրջանակում, մշակվել է ներխուժման հայտնաբերման համակարգի արտադրողականության գնահատման ալգորիթմ:

Ի մի բերելով վերոհիշյալ գլուխներում տեղ գտած նյութը, ատենախոսության հիմնական արդյունքներն են.

- 1) Հիմնավորվել է ցանցերում վնասարար պոլիմորֆ ծրագրային ապահովման հայտնաբերման նոր մեթոդ, որն իր ճշգրտությամբ գերազանցում է մինչ այդ եղած մեթոդները, որոնք իրականացնում են փոխանցվող տվյալների ամբողջականության խախտման հայտնաբերում:
- 2) Հիմնավորվել է փոխանցվող տվյալների ամբողջականությունը խախտող վնասարար մթագրված և յուրացված ծրագրային ապահովման հայտնաբերման նոր մեթոդ, որն իր ճշգրտությամբ գերազանցում է մինչ այդ եղած համապատասխան մեթոդները:
- 3) Առաջարկվել է ցանցային ենթակառուցվածքներում շրջանառվող տվյալների և ներխուժումների հայտնաբերման համակարգի ամբողջականության խախտման ճանաչման ավելի արագ մեթոդ, քան եղածները:
- 4) Կառուցվել են վերոհիշյալ արդյունքները ապահով ծրագրային փաթեթերները, դրանք ինտեգրվել են ավելի մեծ անվտանգային համակարգի մեջ:

Այս տեսակետից, հատկանշական է այն հանգամանքը, որ այս լուծումները կիրառության են դրվել ռազմավարական կարևորության համակարգի («Ձինված ուժերի տեղեկատվական անվտանգության») մեջ:

Այդուհանդերձ, հետազոտության նյութի տեսակետից առաջին հայացքից կարևոր որոշ ասպեկտներ քննության չեն ենթարկվել աշխատության մեջ: Դրանք են՝

- ներդրված համակարգերի արդյունավետության մոնիտորինգից բխող դիտարկումներ ու եզրակացություններ,
- ցանցային ներխուժման միջադեպերի հայտնաբերման ընթացքում առաջացող պահանջներից լուծումների շարունակական կատարելագործման հնարավորությունները,
- ՄՈւ բացատրելի մոդելների կառուցման կարևորության հարցը դիտարկվող խնդիրներում: Արդյոք չի առաջանում փոփոխված տվյալները տեղորոշելու, ոչ միայն դրանց ամբողջականության հարցը կանխատեսելու առաջադրանքը:

Ցանկալի կլիներ տեսնել նաև հեղինակի աշխատանքների ապրոքացիան լայն միջազգային ու մասնագիտական հարթակներում, թե գիտաժողովների, թե հողվածների առումով:

Սակայն, նշենք, որ այս հանգամանքը չեն նսեմացնում ատենախոսության կշիռն ու կարևորությունը, ինչի վկայությունն են ձեռք բերված արդյունքների հիման վրա տպագրված թվով 14 աշխատանքներն ու արտադրության մեջ դրված լուծումները:

Ըստ ամենայնի, Թիմուր Ջամդարյանի աշխատությունը քննության է ենթարկում տեղեկատվական ցանցերի անվտանգությանը վերաբերող կարևոր կիրառական խնդիրներ և առաջարկում արժեքավոր լուծումներ: Այն ավարտուն գիտական նյութ է, իսկ նրա հեղինակը արժանի է 05.13.04 «Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի մաթեմատիկական և ծրագրային ապահովում» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի շնորհմանը:

Պաշտոնական ընդդիմախոս՝

Ֆիզ.մաթ.գիտ.թեկնածու

Աշոտ Նշանի Հարությունյան

ՀՀ ԳԱԱ ԻԱՊԻ գիտաշխատող Ա.Ն. Հարությունյանի ստորագրությունը հավաստում եմ՝

ՀՀ ԳԱԱ ԻԱՊԻ գիտքարտուղար՝

Հ. Սահակյան

19.01.24

