ՀԱՍՏԱՏՈՒՄ ԵՄ
«Երևանի Կապի միջոցների ԳՀԻ» ՓԲԸ
տնօրեն, տ.գ.դ., պրոֆեսոր

Մ.Վ. Մարկոսյան

«18» հունվարի 2024 թ.

ԱՌԱՋԱՏԱՐ ԿԱԶՄԱԿԵՐՊՈՒԹՅԱՆ ԿԱՐԾԻՔ

Թիմուր Վյաչեսլավի Ջամղարյանի *«Տեղեկատվական ցանցում տվյալների ամբողջականության ապահովման համակարգի մշակումը» թեմայով Ե.13.04 - «Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի մաթեմատիկական և ծրագրային ապահովում» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանների հայցման ատենախոսության վերաբերյալ:*

Ատենախոսության թեմայի արդիականությունը

Թ.Վ. Ջամղարյանի ատենախոսական աշխատանքի արդիականությունը կասկած չի հարուցում և պայմանավորված է մի շարք հանգամանքներով, որոնցից հարկ է առանձնացնել մեքենայական ուսուցման (Machine Learning, ML) տեխնոլոգիայի բուռն զարգացումը և կիրառումը տարբեր ոլորտներում: Հարկ է նշել, որ ML մեթոդների կիրառմամբ, չարագործները կարող են գործնական իրականացնել CIA (Confidentiality, Integrity, Availability, CIA) մոդելի համաձայն գրոհները, չլինելով հայտնաբերված «դետերմինիստիկ» պաշտպանողական համակարգերով: Ցանցային ենթակառուցվածքի (ՑԵ) անվտանգությունը նախագծող ճարտարապետների առջև ծառացած կարևոր խնդիրներից մեկը ՑԵ-ում փոխանցվող տվյալների, ամբողջականությունն ապահովելն է: Տարբեր մեխանիզմներ և մեթոդներ, որոնք ապահովում են տվյալների ամբողջականությունը ՑԵ դառնում են ոչ արդյունավետ, երբ չարագործը, որպես գրոհի գործիք կիրառում է ML-ի վրա հիմնված մեթոդներ: Արդյունքում, ՑԵ-ի և համակարգային

անվտանգության հետազոտողները սկսեցին ակտիվորեն ուսումնասիրել ML օգտագործումը ներխուժման հայտնաբերման համակարգերում: Սակայն, ներխուժման հայտնաբերման համակարգերի մեծամասնությունը (ինչպես «դետերմինիստիկ», այնպես էլ ML-ի բաղադրիչներով) գործում են ՑԵ մուտքի և/կամ բաշխման մակարդակներում: Ցանցային ենթակառուցվածքի միջուկի մակարդակը, որի հիման վրա է ձևավորվում ինքնավար համակարգը (Autonomous System, AS), որպես կանոն, պաշտպանված չէ, քանի որ հեռահաղորդակցության օպերատորները, որոնք ձևավորում են ՑԵ միջուկի մակարդակը, միշտ չէ, որ տեղադրում են ներխուժման հայտնաբերման համակարգեր՝ պատասխանատու լինելով միայն մեծ ծավալների տվյալների փոխանցման համար: Համապատասխանաբար, չարագործների դեմ պայքարը, ովքեր նպատակ ունեն փոփոխել (խախտել ամբողջականությունը) ՑԵ միջուկի մակարդակում փոխանցվող տվյալները, դրվում է վերջնական կազմակերպությանը: Տեղեկատվական համակարգում չբացահայտված ներխուժումը, կարող է խաթարել դրանում փոխանցվող տվյալների ամբողջականությունը: Տեղեկատվական համակարգերում տվյալների ամբողջականությանը սպառնացող վտանգները չեզոքացնելու համար անհրաժեշտ է հարձակումը հայտնաբերել վաղ փուլում՝ մինչև դրա ակտիվ զարգացումը:

Հաշվի առնելով այս հանգամանքը՝ արդիական է դառնում ML-ով ներխուժման հայտնաբերման համակարգի մշակումը, որն ի վիճակի է հայտնաբերել փոխանցված տվյալների ամբողջականության խախտումները ցանցի միջուկի մակարդակում: Այս առումով ներկայացված ատենախոսական աշխատանքը հեռանկարային է՝ արդիական, և ունի կարևոր գործնական նշանակություն:

Ատենախոսական աշխատանքի կառուցվածքը համաատասխանում է հետազոտության նպատակին և խնդիրներին: Ատենախոսությունը բաղկացած է ներածությունից, 4 գլխից, եզրակացությունից, 98 անուն օգտագործված գրականության ցանկից և 6 հավելվածից: Աշխատանքը ներառում է 74 նկար և 16 աղյուսակ: Աշխատանքի ընդհանուր ծավալը 138 էջ է: Աշխատանքը գրված է ռուսերեն լեզվով:

Ներածությունում հեղինակի կողմից հիմնավորված է ընտրված թեմայի արդիականությունը, սահմանված են հետազոտության նպատակը, խնդիրները և մեթոդները, գիտական նորույթը և գործնական նշանակությունը, ձևակերպված են պաշտպանության ներկայացվող հիմնական գիտական դրույթները:

Առաջին գլուխը ներկայացնում է հետազոտվող ոլորտի հիմնական խնդիրները, կոշտ տրամաբանությամբ և մեքենայական ուսուցումով ներխուժումների հայտնաբերման համակարգերի հիմնական չլուծված խնդիրները: Կատարվել է տարբեր ցանցային ենթակառուցվածքների կառուցման ճարտարետության և բաց ելակետային կոդով ներխուժման հայտնաբերման համակարգերի ուսումնասիրություն: Առանձին վերլուծվել է մեքենայական ուսուցումով ներխուժման հայտնաբերման համակարգերի ոլորտում կատարված հետազոտությունները: Կատարվել է ամբողջականության դեմ գրոհները հայտնաբերող նեյրոնային ցանցերի ընտրությունը: Ձևակերպվել է հետազոտության խնդրի դրվածքը:

Երկրորդ գլուխը նվիրված է ՑԵ-ի կայունության և փոխանցվող տվյալների ամբողջականության ապահովմանը: Մշակվել է ՑԵ բազմաչափորոշիչային մաթեմատիկական մոդել: Սահմանվել է ՑԵ փոխանցվող տվյալների ամբողջականության դեմ հաջող գրոհի պայմանները, չարագործի կողմից ML մեթոդների կիրառման դեպքում: Նեյրանային ցանցերի ուսուցման և տվյալների հավաքածուների նախապատրաստման համար, մշակվել է հաշվեկարգ և ծրագրային ապահովում: Նեյրոնային ցանցերով ՑԵ փոխանցվող տվյալների ամբողջականության խախտումները, ավելի ճշգրիտ հայտնաբերելու համար, մշակվել է հաշվեկարգ և ծրագրային ապահովում:

Երրորդ գլուխը նվիրված է տարբեր տեսակի մթագրված և/կամ յուրացված վնասաբեր ծրագրային ապահովման հայտնաբերմանը, որը կարող է խախտել ՑԵ-ում փոխանցվող տվյալների ամբողջականությունը: Մշակվել է ծրագրային ապահովում և հաշվեկարգ վնասաբեր պոլիմորֆ ծրագրային ապահովում հայտնաբերելու համար: Կատարվել է մշակված «իրավիճակների մատրիցների» հիման վրա վնասաբեր պոլիմորֆ ծրագրային ապահովման հայտնաբերման արդյունավետության չափումը, «իրավիճակների մատրիցների» տարբեր կարգերի դեպքում:

Չորրորդ գլուխը նվիրված է մշակված ներխուժման հայտնաբերման համակարգում մշակվող և ելքային տվյալների հավաստիության բարձրացմանը: Կատարվել մշակված ներխուժման հայտնաբերման համակարգի ինտեգրումը Snort բաց ելակետային կոդով կոշտ տրամաբանությամբ ներխուժման հայտնաբերման համակարգի հետ: Մշակվել և ծրագրային իրագործվել է ներխուժման հայտնաբերման համակարգի արտադրողականությունը գնահատող մաթեմատիկական մոդելը: Կատարվել է ներխուժման հայտնաբերման համակարգի կազմի մեջ մտնող նեյրոնային ցանցերի արդյունավետության գնահատումը:

Եզրահանգման մեջ շարադրված են ատենախոսական աշխատանքի հետազոտական և կիրառական հիմնական արդյունքները:

Ատենախոսական աշխատանքի բովանդակությունն օժտված է ներքին միասնականությամբ և նվիրված է հետազոտության խնդիրների լուծմանը:

Ատենախոսության սեղմագիրը համապատասխանում է ատենախոսական հետազոտության բովանդակությանը:

Ատենախոսության գիտական արդյունքների նորույթը

- Առաջարկվել է վնասաբեր պոլիմորֆ ծրագրային ապահովման հայտնաբերման մեթոդ, որը գերազանցում է գոյություն ունեցող մեթոդների վրա հիմնված արդյունքները, ինչը հնարավորություն է տալիս ավելի արդյունավետ հայտնաբերել փոխանցվող տվյալների ամբողջականության խախտումը:
- Առաջարկվել է փոխանցվող տվյալների ամբողջականությունը խախտող վնասաբեր մթագրված և յուրացված ծրագրային ապահովման հայտնաբերման մեթոդ, որը գերազանցում է գոյություն ունեցող մեթոդների արդյունքները, ինչը հնարավորություն է տալիս ավելի արդյունավետ հայտնաբերել փոխանցվող տվյալների ամբողջականության խախտումը:
- Առաջարկվել է ՑԵ շրջանառվող տվյալների և ներխուժումների հայտնաբերման համակարգի ամբողջականության (այլ հավասար պայմանների դեպքում) խախտման դեպքում հայտնաբերման մեթոդ, որն ապահովում է ներխուժման հայտնաբերումն ավելի արագ, քան գոյություն ունեցող մեթոդները:
- Ձեռք բերված գիտական արդյունքների հիման վրա, բարելավվել է «սպառնալիքների մոդելը» ՑԵ շրջանառվող տվյալների ամբողջականության բարձրացման շրջանակներում, իր բազմաչափորոշիչային, ստրատիֆիկացված բարելավման ժամանակ, դինամիկ վերակազմավորման ռեժիմում:

Ատենախոսության հիմնական արդյունքները հրապարակվել են 14 գիտական հոդվածներում, որոնցից 11-ը ընդգրկված են ԲՈԿ-ի համար ընդունելի գիտական պարբերականների ցանկում, 1-ը Scopus շտեմարանում, 2-ը այլ պարբերականներում, ստացվել է հետազոտության արդյունքների կիրառական նշանակությունը հաստատող ներդրման ակտ:

Ատենախոսական աշխատանքի վերաբերյալ դիտողություններ

1. Ատենախոսության մեջ ներկայացված ոչ բոլոր նեյրոնային ցանցերի ուսուցման դարաշրջանների արդյունքներն են մանրամասնորեն նկարագրված:
2. Աշխատանքը էականորեն կշահեր, եթե կատարվեին նաև համակարգի արդյունավետության գնահատումը ցանցային ենթակառուցվածքի մուտքի և բաշխման մակարդակներում:

3. Առկա են տեխնիկական գործընթացների նկարագրման անգլերեն-ռուսերեն կիրառվող խրթին, լավ չհասկացվող բացատրություններ:

Եզրակացություն

Նշված դիտողությունները չեն ազդում ատենախոսական աշխատանքի ընդհանուր բարձր դրական գնահատականի վրա: Թ. Վ. Ջամղարյանի թեկնածուական ատենախոսությունն ավարտուն գիտա-հետազոտական աշխատանք է, որն իր արդիականությամբ, ձևավորմամբ, ստացված գիտական և կիրառական արդյունքներով լիովին բավարարում է ՀՀ ԲՈԿ-ի կողմից թեկնածուական ատենախոսություններին ներկայացվող պահանջներին, իսկ աշխատանքի հեղինակ Թիմուր Վյաչեսլավի Ջամղարյանը արժանի է Ե.13.04 «Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի մաթեմատիկական և ծրագրային ապահովում» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի շնորհմանը:

Ատենախոսությունը զեկուցվել, մանրամասն քննարկվել և հավանության է արժանացել «Երևանի կապի միջոցների գիտահետազոտական ինստիտուտ» ՓԲԸ-ի 2024 թ. հունվարի 16-ին կայացած գիտական սեմինարում: Ներկա էին՝ 9 անձ՝ տ.գ.դ. Մ. Մարկոսյանը, տ.գ.դ. Վ. Ավետիսյանը, տ.գ.թ. Ա. Ահարոնյանը, բաժնի վարիչներ՝ Հ. Մարտիրոսյանը, Ա. Մակարյանը, լաբ. վարիչ՝ Ա. Հովհաննիսյանը, առաջատար ճարտարագետներ՝ Հ. Գրիգորյանը, Գ. Սուղյանը, ճարտարագետ - ծրագրավորող Ա. Սմբատյանը:

ԵրԿՄԳՀՀԻ-ի գիտական գծով փոխտնօրեն,
տ.գ.դ., պրոֆեսոր՝ Վ.Ավետիսյան

Գիտական քարտուղար՝ Ա. Մակարյան

Ստորագրությունները հաստատում եմ՝
կազմակերպության կադրերի բաժնի վարիչ Ա. Նաշալյան