«ՀԱՍՏԱՏՈՒՄ ԵՄ»

«Երևանի կապի միջոցների ԳՀԻ» ՓԲԸ

Տնօրեն՝

_____ Ֆ.Է. Լազարյան

«19» մայիսի 2026թ.

ԱՌԱՋԱՏԱՐ ԿԱԶՄԱԿԵՐՊՈՒԹՅԱՆ ԿԱՐԾԻՔ

<u>Համբարձում Դավթի Մինասյանի</u> «Իրերի համացանցի սարքավորումների անվտանգության ապահովման մեթոդների և գործիքամիջոցների մշակումը» թեմայով Ե.13.04 «Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի մաթեմատիկական և ծրագրային ապահովում» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսության վերաբերյալ:

<u>Թեմայի արդիականությունը</u>

Իրերի համացանցի (Internet of Things - IoT) սարքերի մեծ տեմպերով զարգացումը և դրանց կիրառման ոլորտների ընդլայնումը հանգեցրել են կիբեռանվտանգության նոր մարտահրավերների առաջացմանը: IoT էկոհամակարգը թիրախավորող ժամանակակից կիբեռհարձակումները դարձել են բազմաշերտ և բարդ, մինչդեռ ներկայումս կիրառվող սարքերի զգալի մասը կա՛մ չունի ներկառուցված անվտանգության մեխանիզմներ, կա՛մ հիմնվում է կենտրոնացված ամպային լուծումների վրա. այն պահանջում է մշտական կապ, ինչը անիրագործելի է իրական կիրառությունների մեծ մասի դեպքում: IoT սարքերին բնորոշ ռեսուրսների սահմանափակումները՝ հաշվողական հզորության, հիշողության և էներգիայի սպառման տեսանկյուններից, էլ ավելի են բարդացնում

անվտանգության ավանդական մոտեցումների կիրառումը: Առկա է հիմնարար հակասություն տեղեկատվության պաշտպանության խիստ պահանջների և IoT ապարատային ապահովման սահմանափակ հնարավորությունների միջև: Թեև ժամանակակից բջջային IoT պլատֆորմները (օրինակ՝ Nordic nRF9161) ինտեգրում են ապարատային անվտանգության մոդուլներ (ARM CryptoCell-310, TrustZone), սակայն բացակայում են դրանց արդյունավետ օգտագործման համակարգված մեթոդները՝ սարքի կիրառման ամբողջական կենսացիկլի գործունեության համար: Միևնույն ժամանակ, RFC 9783 ստանդարտի (PSA ատեստավորման տոկեն) վերջին հրապարակումը ստեղծում է հնարավորություն՝ սարքերի կարգավիճակի գնահատման համար, սակայն դրա կիրառելիությունը սահմանափակ ռեսուրսներով սարքերի վրա դեռևս գործնականում հաստատված չէ: Վերոնշյալ խնդիրների լուծմանն ուղղված մեթոդների և գործիքների մշակման անհրաժեշտությունն է սույն ատենախոսական աշխատանքի արդիականության հիմնավորումը:

Այսպիսով, իրերի համացանցի սարքավորումների համար նախատեսված գաղտնագրման համակարգերի մշակման խնդիրն արդիական է թե՛ գիտական հետաքրքրություն ներկայացնող խնդիրների լուծման, և թե՛ կիրառական նշանակություն ունեցող ավտոմատացված կառավարում պահանջող համակարգերի նախագծման տեսանկյունից:

<u>Ատենախոսական աշխատանքի բովանդակությունը</u>

Ատենախոսությունը բաղկացած է ներածությունից, չորս գլուխներից, եզրահանգումից, 119 անուն գրականության ցանկից, թվով 1 հավելվածից և հապավումների ցանկից: Ատենախոսության ծավալը կազմում է 118 էջ, իսկ հավելվածի, նկարների և աղյուսակների ցանկի հետ միասին 131 էջ:

Ներածություն: Ներածության մեջ հիմնավորված է թեմայի արդիականությունը, ձևակերպված են աշխատանքի նպատակները, գիտական նորույթները և հիմնական դրույթները, որոնք ներկայացվում են պաշտպանության:

Գլուխ 1-ում ներկայացվում է ատենախոսությունում կիրառված տեխնոլոգիաների և մոտեցումների նկարագրությունը: Աշխատանքի այս

հատվածում ներկայացվել է առկա հետազոտություններում հինգ կարևոր բացթողում. բանալիների կառավարման համապարփակ՝ ապարատային արագացմամբ շրջանակների բացակայությունը, բանալիների կառավարման նախագծման մեջ էներգիա-անվտանգություն փոխզիջումներին ոչ բավարար ուշադրությունը, մառախլապատ (fog-assisted) անվտանգության ճարտարապետությունների սահմանափակ մասշտաբայնությունը, IoT սահմանափակումներին հարմարեցված սարքերի ստանդարտացված հավաստագրման բացակայությունը և գաղտնիությունը պահպանող ու քվանտային կայուն մեխանիզմների ոչ բավարար ինտեգրումը:

Գլուխ 2-ում ներկայացվել են սահմանափակ ռեսուրսներով IoT սարքերի վրա ապարատային գաղտնագրման համակարգերի մոդելավորման և քանակական գնահատման համար մաթեմատիկական մոդելներ: Ներկայացված համակարգը հնարավորություն է տալիս կազմել էներգիայի սպառման, անվտանգության մակարդակի, հիշողության օգտագործման և հաշվողական ծախսերի միջև կապերը՝ օպտիմալացման մոդելի միջոցով, որը ենթարկվում է անվտանգության և ռեսուրսների հստակ սահմանափակումների:

Գլուխ 3-ում ներկայացվել է երեք փոխկապակցված մեթոդ, որոնք միասին լուծում են լայնածավալ բջջային IoT տեղակայումների բանալիների կառավարման և տվյալների անվտանգության ապահովման պահանջները:

Գլուխ 4-ում ներկայացվել է մշակված գործիքների և առաջարկվող մեթոդների համապարփակ փորձարարական վավերացում: ARM TF-M-ի (Trusted Firmware-M) վրա կիրառվել է RFC 9783 PSA հավաստագրման թոքենների համակարգը՝ ապահովելով իրական ժամանակում սարքի կարգավիճակի մշտադիտարկում:

<u>Հետազոտության հիմնական նպատակն</u> է մշակել մեթոդներ և գործիքներ՝ իրերի համացանցի սարքերի անվտանգության ապահովման համար: Նշված նպատակին հասնելու համար աշխատանքում դրվել և լուծվել են հետևյալ խնդիրները.

- Մշակել իրերի համացանցի սարքավորումների գաղտնակայունության գնահատման մաթեմատիկական մոդել.

- Մշակել գաղտնագրման բանալիների գեներացման, պահպանման և փոխանակման ապահովման մեթոդներ.
- Մշակել իրական ժամանակում իրերի համացանցի սարքավորումների կարգավիճակի և անվտանգության մակարդակի գնահատման մեթոդ:

<u>Հեղինակի կոնկրետ մասնաբաժինը ստացված արդյունքներում</u>

Աշխատանքի հիմնական արդյունքները և եզրակացությունները ստացված են անձամբ հեղինակի կողմից: Նրա կողմից ձևակերպված են հետազոտությունների նպատակը, խնդիրները, իրականացված են հետազոտությունները և մշակումները, վերլուծության են ենթարկված ստացված արդյունքները:

<u>Հետազոտության արդյունքների հավաստիությունը</u>

Ատենախոսության մեջ շարադրված գիտական դրույթներն ու տեսական եզրահանգումները ձևակերպվել են հեղինակի կողմից ինքնուրույն և առաջին անգամ. դրանց գիտական հիմնավորումն ապահովված է մանրակրկիտ փորձնական ստուգմամբ, ստացված արդյունքների վիճակագրական վերլուծությամբ ու հավաստիության համակողմանի գնահատմամբ, ինչն ապահովում է ատենախոսության հիմնական պնդումների վստահելիությունը:

<u>Հետազոտության գիտական նորույթը</u>

- Մշակվել է գաղտնագրման համակարգի արդյունավետության գնահատման մաթեմատիկական մոդել, որն ի տարբերություն առկա լուծումների՝ ինտեգրում է էներգասպառումը, հաշվարկային ցիկլերը և հիշողության սահմանափակումները:
- Առաջարկվել են իրերի համացանցի սարքավորումների գաղտնագրման համար օգտագործվող բանալիների գեներացման, պահպանման և փոխանակման մեթոդներ, որոնք, ի տարբերություն առկա լուծումների, չեն պահանջում կենտրոնացված համակարգեր և հիմնված են ապարատային լուծման վրա:
- Առաջարկվել է իրերի համացանցի սարքավորումների վիճակի և անվտանգության մակարդակի գնահատման մեթոդ, որն ի տարբերություն առկա լուծումների՝ կատարում է սարքավորման վարքագծի իրական ժամանակում վերլուծություն և հնարավորություն է տալիս՝ կատարելու հեռահար մշտադիտարկում:

Հրապարակումները

Ատենախոսության հիմնական արդյունքները հրապարակվել են հեղինակի 7 գիտական աշխատանքներում: Սեղմագիրը լիովին համապատասխանում է ատենախոսությանը և արտացոլում է դրա հիմնական բովանդակությունը:

Հետազոտության արդյունքների կիրառական նշանակությունը

Ատենախոսության շրջանակներում մշակված բանալիների կառավարման և սարքերի կարգավիճակի գնահատման համակարգերը ներդրվել են «Ար Փի Ի Քնթրոլս» ՍՊԸ-ում (RPE Controls LLC)՝ խելացի կառավարվող լուծումների անվտանգության մակարդակի բարձրացման նպատակով: Գաղտնագրման գործընթացի կայունության գնահատման մաթեմատիկական մոդելը և դրա ծրագրային իրականացումն օգտագործվում են Հայաստանի ազգային պոլիտեխնիկական համալսարանի «Տեղեկատվական անվտանգության և ծրագրային ապահովման» ամբիոնի ուսումնական գործընթացում:

Ատենախոսության թերությունները.

1. Որոշ դեպքերում անհրաժեշտ է ավելի մանրամասն համեմատություն կատարել այլ ժամանակակից գաղտնագրային արձանագրությունների հետ, ինչը կհարստացներ ատենախոսության համեմատական վերլուծությունը:

2. Առաջարկվող համակարգում դիֆերենցիալ գաղտնիության պարամետրի (ε=0.5) ընտրության հիմնավորումը կարող էր ավելի մանրամասն լինել՝ ներառելով օգտակարություն - գաղտնիություն փոխզիջման քանակական վերլուծությունը:

Նշված դիտողությունները չեն ազդում աշխատանքի ընդհանուր գնահատականի վրա:

Ատենախոսությունը իր ծավալով, գիտական մակարդակով և ձևակերպմամբ լիովին համապատասխանում է **ՀՀ ԿԳՄՍՆ բարձրագույն կրթության և գիտության կոմիտե**ի կողմից թեկնածուական ատենախոսություններին ներկայացվող պահանջներին, բովանդակությամբ համապատասխանում է Ե.13.04 «Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի մաթեմատիկական և ծրագրային ապահովում» մասնագիտությանը, իսկ հեղինակն արժանի է տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի շնորհմանը:

Ատենախոսությունը զեկուցվել, մանրամասն քննարկվել և հավանության է արժանացել «Երևանի կապի միջոցների գիտահետազոտական ինստիտուտ» ՓԲԸ-ի 2026թ. մայիսի 18-ին կայացած գիտական սեմինարում:

Ներկա էին՝ 8 անձ՝ տ.գ.դ. Ա. Մարկոսյանը, տ.գ.թ. Ա. Ահարոնյանը, փոխ. տնօրեն Հ. Մարտիրոսյանը, բաժնի վարիչներ՝ Ֆ. Տեր-Զաքարյանը, Ա. Մակարյանը, լաբ. վարիչ՝ Ա. Զարգարյանը, առաջատար ճարտարագետ Լ. Մանուչարյանը, ճարտարագետ ծրագրավորող Ա. Կայծակովը:

ԵրԿՄԳՀԻ-ի գիտխորհրդի նախագահ,
տ.գ.դ., պրոֆեսոր՝ Մ. Մարկոսյան

Գիտական քարտուղար՝ Ա. Մակարյան

Ստորագրությունները հաստատում եմ
Կազմակերպության կադրերի բաժնի վարիչ՝ Ի. Վանդունց