ՊԱՇՏՈՆԱԿԱՆ ԸՆԴԴԻՄԱԽՈՍԻ ԿԱՐԾԻՔ

Համբարձում Դավթի Մինասյանի

«Իրերի համացանցի սարքավորումների անվտանգության ապահովման մեթոդների և գործիքների մշակումը» թեմայով Ե.13.04 «Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի մաթեմատիկական և ծրագրային ապահովում» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսության վերաբերյալ:

Ատենախոսությունը նվիրված է իրերի համացանցի սարքավորումների անվտանգության ապահովման արդիական և կարևոր խնդիրներին, որոնք ժամանակակից թվային ենթակառուցվածքների զարգացման պայմաններում ունեն առանձնահատուկ նշանակություն: Աշխատանքում դիտարկվում են IoT սարքերի անվտանգության ապահովման տարբեր ասպեկտներ՝ ներառյալ գաղտնագրային մեթոդների արդյունավետության գնահատումը, բանալիների կառավարման մեխանիզմների մշակումը և սարքերի անվտանգության վիճակի մշտադիտարկումը:

1. Աշխատանքի արդիականություն

Աշխատանքի արդիականությունը պայմանավորված է իրերի համացանցի (IoT) տեխնոլոգիաների արագ զարգացմամբ և դրանց լայն կիրառմամբ արդյունաբերության, տրանսպորտի, առողջապահության, էներգետիկայի, խելացի քաղաքների և ռազմական նշանակության համակարգերում: Վերջին տարիներին նկատվում է IoT սարքերի քանակի աճ, և հետևաբար մեծանում է դրանց միջոցով փոխանցվող և մշակվող տվյալների քանակի: Այս պայմաններում IoT ենթակառուցվածքների անվտանգությունը վերածվել է ոչ միայն տեղեկատվական անվտանգության, այլ նաև ազգային և հանրային անվտանգության կարևոր հնդրի: Միաժամանակ IoT սարքերի մեծ մասը նախագծվում են սահմանափակ հաշվողական և էներգետիկ ռեսուրսներով սարքեր, ինչը դժվարացնում է դասական գաղտնագրային և պաշտպանական մեխանիզմների կիրառումը: Գործնականում լայն տարածում ունեն այնպիսի խնդիրներ, ինչպիսիք են՝ նույնականացումը, անվտանգ բանալիների պահպանման բացակայությունը, ծրագրային ապահովման ուշ թարմացումները և հեռավար հսկողության սահմանափակ հնարավորությունները: Նման խնդիրները մեծացնում են «գրոհի մակերեսը» ինչը բերում է լայնածավալ կիբեռհարձակումների:

Արդիական է դառնում ապարատային արագացմամբ անվտանգության մեխանիզմների կիրառումը, որոնք հնարավորություն են տալիս ապահովել

գաղտնակայություն՝ սահմանափակ էներգիայի աղբյուրի պայմաններում: Վերոնշյալ խնդիրները պայմանավորում են IoT սարքերի անվտանգության ապահովման նոր մեթոդների և գործիքների մշակման անհրաժեշտությունը, ինչը և հիմնավորում է ներկայացված ատենախոսական աշխատանքի արդիականությունը:

2. Ատենախոսության կառուցվածքը և բովանդակությունը

Ատենախոսությունը բաղկացած է ներածությունից, չորս գլուխներից, եզրակացությունից, օգտագործված գրականության ցանկից և հավելվածից: Աշխատանքի ընդհանուր ծավալը կազմում է 130 էջ՝ ներառյալ նկարները, աղյուսակները և օգտագործված գրականության ցանկը:

Ներածությունում հիմնավորվել է թեմայի արդիականությունը, ձևակերպվել են հետազոտության նպատակը և խնդիրները, ներկայացվել են աշխատանքի գիտական նորույթը, գործնական նշանակությունը, հետազոտության մեթոդները, ինչպես նաև պաշտպանության ներկայացվող հիմնական դրույթները:

Առաջին գլխում կատարվել է իրերի համացանցի սարքերի անվտանգության խնդիրների համակողմանի վերլուծություն: Ներկայացվել են IoT էկոհամակարգի ճարտարապետական առանձնահատկությունները, ժամանակակից կիբեռ-սպառնալիքները, սահմանափակ ռեսուրսներով սարքերի անվտանգության խնդիրները, ինչպես նաև իրականացվել է գաղտնագրման մեթոդների և բանալիների կառավարման համակարգերի համեմատական ուսումնասիրություն: Գլխում առանձնացվել են առկա լուծումների հիմնական սահմանափակումները:

Երկրորդ գլխում մշակվել է IoT սարքերի գաղտնագրային հաշվեկարգ: Վերլուծվել է էներգիայի սպառման, հիշողության ծախսի և անվտանգության մակարդակի փոխկախվածությունը, իրականացվել է գաղտնագրային ալգորիթմների մոդելավորում և կատարվել է մոդելի տեսական վավերացում:

Երրորդ գլխում ներկայացվել են ապարատային արագացմամբ բանալիների կառավարման և տվյալների անվտանգ մշակման մեթոդները: Մշակվել են բանալիների գեներացման և պահպանման մեխանիզմներ՝ ARM CryptoCell-310 տեխնոլոգիայի կիրառմամբ:

Չորրորդ գլխում ներկայացվել են IoT սարքերի անվտանգության վիճակի մշտադիտարկման գործիքները և դրանց փորձարարական գնահատման արդյունքները: Իրականացվել է RFC 9783 PSA թոկենի վրա հիմնված հեռավար ատեստավորման համակարգ, ներկայացվել են մշակված մեթոդների փորձարկման արդյունքները և կատարվել է արդյունավետության համեմատական գնահատում:

Եզրակացությունում ամփոփվել են աշխատանքի հիմնական գիտական և գործնական արդյունքները, ձևակերպվել են ստացված եզրահանգումները:

3. Աշխատանքի գիտական արդյունքները

Առաջին գիտական արդյունքը վերաբերում է գաղտնագրային համակարգերի արդյունավետության գնահատման մաթեմատիկական մոդելին, որը հնարավորություն է տալիս համալիր կերպով գնահատել էներգիայի սպառման, հիշողության ծախսի և անվտանգության մակարդակի փոխկապակցվածությունը: Առաջարկված մոտեցումը հնարավորություն է տալիս քանակական գնահատել IoT սարքերում կիրառվող գաղտնագրային ալգորիթմների արդյունավետությունը:

Երկրորդ գիտական արդյունքը վերաբերում է ապարատային արագացմամբ բանալիների կառավարման մեթոդների մշակմանը: Առաջարկված լուծումները հնարավորություն են տալիս ապահովել բանալիների գեներացում, պահպանում և փոխանակում՝ առանց կենտրոնացված կառավարման համակարգերից կախվածության:

Երրորդ գիտական արդյունքը վերաբերում է իրական ժամանակում IoT սարքերի անվտանգության վիճակի գնահատման : Մշակված գործիքները հնարավորություն են տալիս իրականացնել սարքերի մշտադիտարկումը:

4. Փորձարարական արդյունքներ և վավերացում

Աշխատանքում ներկայացված են մշակված մեթոդների և գործիքների համապարփակ փորձարարական արդյունքները: Հեղինակը իրականացրել է փորձարկումներ տարբեր, սահմանված ապարատային հարթակների վրա և ցույց տվել, որ ապարատային արագացմամբ իրականացումները զգալիորեն նվազեցնում են էներգիայի սպառումը և հիշողության օգտագործումը՝ միաժամանակ բարձրացնելով համակարգի արտադրողականությունը:

Դրական է նաև այն, որ աշխատանքի շրջանակներում կիրառվել են տեսական վավերացման ժամանակակից միջոցներ՝ Coq, Isabelle/HOL և ProVerif գործիքները, որոնք բարձրացնում են ստացված արդյունքների հիմնավորվածությունը և վստահելիությունը:

5. Հրապարակումներ

Ատենախոսության հիմնական արդյունքները հրապարակվել են 7 գիտական աշխատանքներում: Հրատարակությունները ներառում են ինչպես Հայաստանի Հանրապետության, այնպես էլ միջազգային հեղինակավոր գիտական

հարթակներ՝ ամսագրեր, միջազգային կոնֆերանսներ, գիտաժողովներ: Աշխատանքի արդյունքների ներկայացումը նման հեղինակավոր գիտական հարթակներում վկայում է դրանց արդիականության, գիտական արժեքի և միջազգային մասնագիտական հանրության կողմից ընդունելիության մասին:

6. Աշխատանքի դիտողություններ և առաջարկություններ

Չնայած աշխատանքի բարձր գիտական և կիրառական արժեքին, կարելի է նշել որոշակի դիտողություններ:

1. Աշխատանքում սպառնալիքների և չարագործի մոդելները բավարար չափով դիտարկված չեն: Ցանկալի կլիներ առավել հստակ սահմանել չարագործի հնարավորությունները, ինչպես նաև դիտարկվող կիբերհարձակումների տեսակները, ինչը կուժեղացներ աշխատանքի տեսական հիմնավորվածությունը:
2. Գաղտնագրային ալգորիթմների արդյունավետության գնահատման ընթացքում հիմնական շեշտը դրված է արտադրողականության ցուցանիշների՝ էներգասպառման, հիշողության և թողունակության վրա, մինչդեռ գաղտնագրային կայունության քանակական գնահատականները բավարար խորությամբ ներկայացված չեն: Ցանկալի կլիներ ներառել նաև անվտանգության մակարդակի տեսական գնահատումներ՝ բարդության տեսության կամ հարձակման հավանականության մոդելների կիրառմամբ:
3. Աշխատանքում ներկայացված փորձարարական հետազոտությունները հաստատում են առաջարկված լուծումների գործնական արդյունավետությունը, սակայն չեն դիտարկվում ակտիվ չարագործի մասնակցությամբ սցենարներ, գաղտնավերլուծական հարձակումների մոդելավորում կամ հանգույցների կոմպրոմետացման պայմաններում համակարգի կայունության գնահատում: Նման վերլուծությունը հնարավորություն կտար առավել ամբողջական գնահատել առաջարկված ճարտարապետության իրական անվտանգության մակարդակը:

Եզրակացություն

Նշված դիտողությունները չեն նվազեցնում ատենախոսության գիտական արժեքը և ստացված արդյունքների կարևորությունը: Ատենախոսությունը հանդիսանում է ավարտուն գիտահետազոտական աշխատանք, որտեղ լուծված են իրերի համացանցի սարքերի անվտանգության ապահովման կարևոր խնդիրներ: Ստացված արդյունքները ունեն ինչպես տեսական, այնպես էլ գործնական նշանակություն և կարող են կիրառվել տարբեր IoT համակարգերում:

Սեղմագիրը համապատասխանում է ատենախոսության բովանդակությանը և արտացոլում է աշխատանքի հիմնական դրույթներն ու արդյունքները:

Հաշվի առնելով աշխատանքի արդիականությունը, գիտական նորույթը, ստացված արդյունքների հիմնավորվածությունն ու կիրառական նշանակությունը՝ գտնում եմ, որ **Համբարձում Դավթի Մինասյանի ատենախոսությունը բավարարում** է Ե.13.04 «Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի մաթեմատիկական և ծրագրային ապահովում» մասնագիտությամբ թեկնածուական ատենախոսություններին ներկայացվող պահանջներին, իսկ հեղինակը **արժանի է** տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի շնորհմանը:

Պաշտոնական ընդդիմախոս՝ տ.գ.թ Թ.Ջամղարայն

ՀԱՊՀ գիտքարտուղար Ծ.Ս.Հովհաննիսյան

«20» 05 2026