ՀՀ ԳԱԱ ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

Հովսեփյան Վլադիմիր Հովսեփի

ԱՄՊԱՅԻՆ ՏԵԽՆՈԼՈԳԻԱՆԵՐՈՎ ԱՆՎՏԱՆԳ ԱՇԽԱՏԵԼՈՒ ԼՐԱՑՈՒՑԻՉ ՄԻՋՈՑՆԵՐԻ ՄՇԱԿՈՒՄ

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

Ս Ե Ղ Մ Ա Գ Ի Ր

Երևան – 2017

ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ НАН РА

Овсепян Владимир Овсепович

РАЗРАБОТКА ДОПОЛНИТЕЛЬНЫХ СРЕДСТВ ДЛЯ БЕЗОПАСНОЙ РАБОТЫ С ОБЛАЧНЫМИ ТЕХНОЛОГИЯМИ

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, систем и сетей»

Ереван – 2017

Ատենախոսության թեման հաստատվել է Հայաստանի ազգային պոլիտեխնիկական համալսարանում:

Գիտական ղեկավար՝	տեխ.գիտ.թեկնածու	Գ. Ի. Մարգարով
Պաշտոնական ընդդիմախոսներ՝	տեխ.գիտ.դոկտոր	Հ.Հ.Հարությունյան
	տեխ.գիտ.թեկնածու	Վ. Հ. Դարբինյան
Առաջատար կազմակերպություն՝	Երևանի կապի միջոցների գիտահետազոտական ինստիտուտ	

Պաշտպանությունը կայանալու է 2017թ. հունիսի 15-ին, ժ. 16:00-ին ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում գործող 037 «Ինֆորմատիկա» մասնագիտական խորհրդի նիստում, հետևյալ հասցեով՝ Երևան, 0014, Պ. Սևակի 1:
Ատենախոսությանը կարելի է ծանոթանալ ՀՀ ԳԱԱ ԻԱՊԻ գրադարանում:
Սեղմագիրը առաքված է 2017թ. մայիսի 15-ին:

037 Մասնագիտական խորհրդի
գիտական քարտուղար ֆ.մ.գ.դ. Հ.Գ.Սարուխանյան

Тема диссертации утверждена в Национальном политехническом университете Армении.

Научный руководитель:	кандидат тех. наук	Г.И.Маргаров
Официальные оппоненты:	доктор тех. наук	Г.А.Арутюнян
	кандидат тех. наук	В.Г.Дарбинян
Ведущая организация:	Ереванский научно-исследовательский институт средств связи	

Защита состоится 15-ого июня 2017г. в 16:00 на заседании специализированного совета 037 «Информатика» 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 15-ого мая 2017г.

Ученый секретарь,
Специализированного совета 037
доктор физ.-мат.наук А.Г.Саруханян

ԱՇԽԱՏԱՆՔԻ ԸՆԴՀԱՆՈՒՐ ԲՆՈՒԹԱԳԻՐԸ

Աշխատանքի արդիականությունը: Ժամանակակից տեղեկատվական տեխնոլոգիաների և հեռահաղորդակցության համակարգերի զարգացումը, մասնավորապես՝ ամպային տեխնոլոգիաների լայնամասշտաբ ներգրավումը մարդկային կենսագործունեության բոլոր բնագավառներում, նոր պահանջներ է առաջադրում տեղեկատվական անվտանգության ապահովմանը, առանց որի հնարավոր չէ այդ բնագավառների հետագա զարգացումը:

Ամպային տեխնոլոգիաների բուռն զարգացող ոլորտներից է իրերի ինտերնետը: Ամպային ինտերնետ իրերի միջև փոխադարձ կապը հնարավորություն է տալիս կառավարել և ավտոմատացնել ընթացող գործառույթները: Ինտերնետ իրերը ստեղծված են որոշակի գործառույթ իրականացնելու համար և, որպես կանոն, ունեն համեմատաբար ցածր հաշվողական հզորություն: Մյուս կողմից՝ իրերի արտադրությամբ զբաղվող ընկերությունները, ստեղծելով պարզ կիրառության և քիչ ռեսուրսներ օգտագործող ինտերնետ սարքեր, իրենց առջև տեղեկատվական անվտանգության ապահովման խնդիրներ չեն դնում: Տեղեկատվական անվտանգության տեսանկյունից վերոհիշյալ խնդիրն ունեցող ինտերնետ իրերը դասակարգվում են երկու դասի՝ սարքեր, որոնք ունակ են իրականացնել գաղտնագրային գործառույթներ, և սարքեր, որոնցում անհնար է կատարել գաղտնագրային որևէ գործառույթ՝ սահմանափակ հաշվողական ռեսուրսների պատճառով: Վերոհիշյալ ցածր արտադրողականության սարքերը կարելի է անվանել նաև պարզ ինտերնետ իրեր:

Գաղտնագրային համակարգերի սահմանափակումները տարատեսակ իրերի ինտերնետ միջավայրում պահանջում են ինտերնետ իրերի համաձայնեցում գաղտնագրային համակարգի հետ՝ նախքան ամպային ցանցին միանալը: Վերոհիշյալ հանգամանքն անխուսափելիորեն բացասական ազդեցություն է թողնում ամպային միջավայրի արդյունավետության վրա, միևնույն ժամանակ ինտերնետ իրերի գերակշիռ զանգվածի համար բանալիների բաշխման հայտնի համակարգերը կիրառելի չեն, քանի որ դրանք նախատեսված են միատեսակ սարքերի համար, մինչդեռ իրերի ինտերնետ միջավայրը ներառում է տարատեսակ սարքեր:

Ինչպես նշվել է, գոյություն ունեն ինտերնետ իրերի այնպիսի տեսակներ, որոնք թույլ չեն տալիս կիրառել գաղտնագրային գործառույթներ՝ որոշակի տեխնիկական պահանջների կամ համապատասխան ծրագրային ապահովման անհամատեղելիության պատճառով: Այս բարդությունը շրջանցելու մոտեցումներից մեկը կարող է լինել ինտերնետ իրերում տեխնիկական փոփոխությունների իրականացումը, որը սակայն անխուսափելիորեն կբերի իրերի ինքնարժեքի բարձրացմանը: Ուստի անհրաժեշտություն է առաջանում տվյալ խնդրի համար գտնել այնպիսի լուծում, որը չի պարտադրի սարքերի տեխնիկական կամ ծրագրային փոփոխություններ:

Ինտերնետ իրերին հատուկ է նաև դրանց ֆիզիկական ազդեցությունը արտաքին միջավայրի վրա, որի պատճառով կարևորվում է իրերի կողմից իրականացվող գործառույթների ամբողջականության ապահովումը: Գործառույթների ամբողջականության ապահովման արգելք է հանդիսանում նաև ինտերնետ իրերի խոցելիությունը ցանցային գրոհների, մասնավորապես՝ ներխուժումների և DDoS

գրոհների նկատմամբ: Իրերի ինտերնետ միջավայրում վերոհիշյալ սպառնալիքների չեզոքացումը հեռակառավարման հնարավորություն ունեցող սարքերի քանակի աճին զուգընթաց դառնում է ավելի ու ավելի կարևոր: Այս ասպարեզում մինչ այժմ գոյություն ունեցող լուծումները հիմնականում ծրագրային են, իրականացված են, որպես կանոն, կենտրոնացված սերվերային միջավայրի համար և պահանջում են զգալի հաշվողական ռեսուրսներ:

Աշխատանքի նպատակն է մշակել ամպային տեխնոլոգիաներով անվտանգ աշխատելու լրացուցիչ միջոցներ՝ տվյալների անվտանգ փոխանակման, գործառույթների ամբողջականության ապահովման և ցանցային գրոհներից պաշտպանվելու համար: Այդ նպատակին հասնելու համար դրվել և լուծվել են հետևյալ խնդիրները՝

- Մշակել գաղտնագրային բանալիների կառավարման մեթոդ, որն ապահովում է միջավայրին միացվող սարքերի ինքնակարգավորումը և դրանց միջև տվյալների անվտանգ փոխանակումը:
- Մշակել անվտանգ հաղորդակցման մեթոդ ամպային միջավայրում պարզ սարքերի համար, որոնք սահմանափակ ռեսուրսների պատճառով գաղտնագրային ընթացակարգեր չեն ապահովում:
- Մշակել ամպային բաշխված ցանցերում գործառույթների ամբողջականությունն ապահովող մեթոդ, որը նաև կիրականացնի ամպային միջավայրի վրա հատուկ գրոհների բացահայտումը և դրանց կանխարգելումը:

Գիտական նորույթ:

- Մշակվել է տարատեսակ իրերի ինտերնետ միջավայրում բանալիների կառավարման մեթոդ, որն, ի տարբերություն գոյություն ունեցող լուծումների, տվյալների անվտանգ փոխանակման համար սարքերի նախնական կարգաբերում չի ենթադրում:
- Մշակվել է գաղտնահամակարգ՝ ամպային միջավայրում պարզ ինտերնետ իրերի հետ անվտանգ հաղորդակցման ապահովման նպատակով, որը, ի տարբերություն ոլորտում առկա լուծումների, ապահովում է անհրաժեշտ անվտանգություն և սարքերի տեխնիկական բնութագրերի փոփոխություն չի պահանջում:
- Մշակվել է բաշխված ցանցերում գործառույթների ամբողջականության ու անվտանգության ապահովման մեթոդ, որը կենտրոնացված սերվերի օգտագործում չի պահանջում և ապահովում է ինտերնետ իրերի տեղեկատվական անվտանգությունը միջավայրին բնորոշ գրոհների նկատմամբ:

Աշխատանքի գործնական նշանակությունը:

- Մշակվել է IKS ծրագրային համակարգը, որը հիմնված է բանալիների բաշխման մեթոդի վրա և հնարավորություն է ընձեռում ապահովել տվյալների անվտանգ փոխանակում տարատեսակ ինտերնետ իրերի միջև:
- Մշակվել է SIT ծրագրային համակարգը, որի ներդրումը համապատասխան սարքում ապահովում է տվյալների անվտանգ փոխանակում այն ինտերնետ իրերի համար, որոնք գաղտնագրային ընթացակարգեր չեն ապահովում:

- Մշակվել է իրերի ինտերնետ միջավայրում գործառույթների ամբողջականությունն ապահովող ծրագրային գործիքամիջոց, որն օգտագործելով մշակված արձանագրությունը, ապահովում է ինտերնետ իրերի անվտանգությունը միջավայրին հատուկ գրոհների նկատմամբ:

Պաշտպանության են ներկայացվում հետևյալ դրույթները.

- Գաղտնագրային բանալիների կառավարման մեթոդ, որն աշխատում է առանց նախնական կարգաբերման անհրաժեշտության և ապահովում է իրտերնետ իրերի միջև տվյալների անվտանգ փոխանակումը:
- Ամպային միջավայրում ինտերնետ իրերի հետ անվտանգ հաղորդակցման մեթոդ, որը կիրառելի է գաղտնագրային ընթացակարգերից զուրկ ինտերնետ իրերի համար:
- Բաշխված ցանցերում գործառույթների ամբողջականության ու անվտանգության ապահովման մեթոդ, որը նաև ապահովում է ինտերնետ իրերի տեղեկատվական անվտանգությունը միջավայրին բնորոշ գրոհների նկատմամբ:

Ներդրումները:

Ատենախոսության արդյունքները կիրառվում են.

- Կանխարգելիչ սրտաբանության կենտրոնում առօրյա պայմաններում հիվանդի առողջական վիճակի հետազոտության տվյալների անվտանգ փոխանցման գործընթացներում:
- «Կորիզ» ՍՊԸ-ում՝ ինտերակտիվ խաղային հարթակում ինտերնետ իրերի հետ կապված գործառույթների անվտանգության ապահովման նպատակով:

Աշխատանքի արդյունքները զեկուցվել են. ՀԱՊՀ տարեկան գիտաժողովում (2015թ., ք. Երևան), «ՆԱՏՕ առաջադեմ հետազոտական աշխատաժողով»-ում (NATO ARW, 2015թ., գ. Աղվերան, ՀՀ), «Քոմփյութերային գիտությունների և տեղեկատվական տեխնոլոգիաների» միջազգային գիտաժողովում (CSIT 2015թ., ք. Երևան), «Միջազգային գիտափորձնական ուսանողների և երիտասարդ գիտնականների գիտաժողով»-ում (Ազգային ավիացիոն համալսարան, 2016թ. ք. Կիև, Ուկրաինա), «Ինտերնետ անվտանգության համաշխարհային կոնգրես»-ում (WorldCIS-2016, 2016թ. ք. Լոնդոն, Մեծ Բրիտանիա), ՀԱՊՀ ՏԱԾԱ ամբիոնի գիտատեխնիկական սեմինարներում (2014-2017թ., ք. Երևան):

Հետազոտման օբյեկտներն են բանալիների բաշխման մեթոդները, բանալիների ենթակառուցվածքի ձևավորման մոդելները, գաղտնագրային համակարգերը և քաոսային հեշավորման ֆունկցիաները:

Հրապարակումներ: Ատենախոսության հիմնական արդյունքները տպագրված են 6 գիտական աշխատություններում, որոնք թվարկված են սեղմագրի վերջում:

Աշխատանքի կառուցվածքը և ծավալը: Ատենախոսությունը բաղկացած է ներածությունից, չորս գլխից, եզրակացությունից և 67 անուն օգտագործված գրականության ցանկից: Աշխատանքի ընդհանուր ծավալն է 110 էջ՝ ներառյալ 20 նկար: Հավելվածները կազմում են 2 էջ:

ԱՇԽԱՏԱՆՔԻ ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆԸ

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

Առաջին գլխում դիտարկված է, որ ամպային տեխնոլոգիաներում մասնավորապես, տարատեսակ իրերի ինտերնետում առկա կարևորագույն խնդիրը տեղեկատվական անվտանգության ապահովումն է: Դիտարկվել են ամպային տեխնոլոգիաների տեղեկատվական անվտանգության հիմնախնդիրները: Առաջադրված խնդիրների լուծման նպատակով հետազոտվել են գաղտնիքի բաշխման գոյություն ունեցող սխեմաները՝ իրերի ինտերնետ միջավայրում դրանց կիրառման նպատակահարմարության տեսանկյունից և բացահայտվել են կիրառվող սխեմաների թերությունները: Միաժամանակ ուսումնասիրվել և կարևորվել է ինտերնետ իրերի գործառույթների ամբողջականության ապահովումը, որի համար հիմնական խոչընդոտը ինտերնետ իրերի խոցելիությունն է հարձակումների նկատմամբ: Իրերի ինտերնետ միջավայրի տեղեկատվական անվտանգության՝ պահանջվող մակարդակի ապահովման համար այս գլխում առաջարկվել է մշակել գաղտնի բանալիների բաշխման, հարձակումների բացահայտման և դրանցից պաշտպանվելու նոր մեթոդ:

Կատարված հետազոտությունների հիման վրա ձևավորվել է աշխատանքի նպատակը և դրվել են այն խնդիրները, որոնք անհրաժեշտ է լուծել այդ նպատակին հասնելու համար:

Երկրորդ գլխում հետազոտվել են տարատեսակ ինտերնետ իրերը՝ միմյանց հետ փոխազդելու եզակի գլոբալ հասցեավորման սխեմայի և ծառայությունների տրամադրման մեխանիզմների բացահայտման նպատակով: Իրերի ինտերնետ ցանցը դիտարկվում է որպես կամայականորեն բաշխված միատեսակ և տարատեսակ իրերի ընդլայնվող ցանց, որտեղ նշված իրերի կարևոր գործառույթներից են՝ ֆիզիկական շրջապատից տվյալների հավաքագրումը և գրանցումը: Հիմնվելով իրերի ինտերնետ միջավայրում իրերի բնութագրերի վրա՝ առաջարկվել է բանալիների կառավարման անվտանգ սխեմա՝ տարատեսակ իրերի միջև անվտանգ կապի հաստատման նպատակով: Ընդունվել է, որ բանալիների կառավարման առաջարկված սխեմայում յուրաքանչյուր ինտերնետ իր ընտրվում է որպես ծառայության հանգույց, այլընտրանքային ծառայության հանգույց կամ աշխատանքային հանգույց՝ ինքնակարգավորման մշակված ալգորիթմի միջոցով: Ընտրման գործընթացից անմիջապես հետո ծառայության հանգույցները գեներացնում են բանալիների ենթակառուցվածք՝ համապատասխան աշխատանքային հանգույցների համար: Արդյունքում զույգ աշխատանքային հանգույցները հաշվարկում են ընդհանուր բանալին:

Հաշվի առնելով հանգույցների հիշողության գերբեռնման և հարցումների սպասարկման N պարամետրի սահմանափակ լինելու հետ կապված խնդիրները՝ անհրաժեշտություն է առաջանում մշակել բանալիների բաշխման և կառավարման նոր սխեմա, որով կարելի կլինի անվտանգ կառավարել տարատեսակ ինտերնետ իրերը:

Ինտերնետ իրերի նման դասակարգումը հնարավորություն է տալիս խուսափել հիշողության գերբեռնումից և հարցումների սպասարկման ցածր արտադրողականությունից՝ ծառայության հանգույց ընտրելով այն հանգույցը, որը տվյալ

պահին տեխնիկապես (կախված իրի ֆիզիկական պարամետրերից) ավելի նպատակահարմար է:

Առաջադրված խնդրի լուծման նպատակով մշակվել է ալգորիթմ հետևյալ հաջորդականությամբ.

1. Յուրաքանչյուր հանգույց ընտրվում է որպես՝
   - ծառայության հանգույց,
   - այլընտրանքային հանգույց,
   - աշխատանքային հանգույց:
2. Ծառայության հանգույցի կողմից ստեղծվում է բանալիների ենթակառուցվածք՝ համապատասխան աշխատանքային հանգույցների համար:
3. Աշխատանքային հանգույցի և դրա հետ կապված ծառայության հանգույցի միջև հաստատվում է անվտանգ կապուղի, որի միջոցով աշխատանքային հանգույցները բանալու վերաբերյալ ամբողջական ինֆորմացիա են ստանում համապատասխան ծառայության հանգույցներից:
4. Միևնույն ծառայության հանգույցի հետ կապված աշխատանքային հանգույցները ստանում են ընդհանուր/բաշխված բանալի, որով ապահովվում է կապի անվտանգությունն այդ հանգույցների միջև:

Ենթադրվում է, որ հանգույցների որոշ պարամետրեր նախասահմանված և նախաբեռնված են՝ նախքան հանգույցի տեղակայվելը ցանցում, ինչպես նշված է աղյուսակ 1-ում:

Աղյուսակ 1. Հանգույցների նախասահմանված և նախաբեռնված պարամետրերը

Պարամետրերը	Պարզաբանումը/նկարագրումը
T_s,	Ծառայության հանգույցի ընտրության մեկ փուլի ժամանակը
a, b	Երկու պարզ թիվ՝ բանալիների ենթակառուցվածքի գեներացման համար՝ Ռաբինի անհամաչափ գաղտնահամակարգի բանալու օգտագործմամբ
λ	Ծառայության հանգույցի կողմից սպասարկվող հանգույցների առավելագույն քանակը
H	Վերահասցեավորման սահմանային արժեքը
Ps	Որպես ծառայության հանգույց ընտրվելու հավանականությունը
UID	Հանգույցի եզակի նույնականացման նշիչը՝ 6LowPAN
T_{total}	Գործընթացի գործարկման առավելագույն ժամանակը

Բանալիների բաշխման գործընթացը մեկնարկում է յուրաքանչյուր հանգույցին իր սպասելու T_{total} առավելագույն ժամանակի, ծառայության հանգույցի ընտրության համար մեկ T_s փուլի և λ առավելագույն քանակի նախաբեռնմամբ՝ հստակեցնելով

սպասարկվող աշխատանքային այն հանգույցների քանակը, որոնք ծառայության հանգույց են դառնում:

Հանգույցի նույնականացման համար ենթադրվում է, որ յուրաքանչյուր հանգույց ունի անհատական IPv6 հասցե: Այդ դեպքում, օգտվելով 6LoWPAN տեխնոլոգիայից, հնարավոր է ստանալ նույնականացման եզակի ցուցիչ (UID): Կարելի է նշել, որ 6LoWPAN-ն փոքր հզորություն օգտագործող անլար բաշխված ցանց է, որտեղ ամեն մի հանգույց ունի IPv6 հասցե՝ ինտերնետի հետ ուղղակի կապ հաստատելու համար:

Ինչպես հայտնի է, անհամաչափ գաղտնահամակարգերը անվտանգության հիմնարար գործառույթ են ապահովում անլար ցանցերում և օգտագործվում են նաև իրերը իրերի հետ կապի անվտանգությունն ապահովելու նպատակով: Մյուս կողմից՝ իրերի ինտերնետում միատեսակ հանգույցների ռեսուրսների սահմանափակությունը լուրջ արգելք է բանալիների զույգերի կառավարման ավանդական մեթոդների համար՝ բաց բանալիով գաղտնագրման և բանալու բաշխման կենտրոնի (Key Distribution Center)-ի կիրառելիս:

Մինչ այժմ անհամաչափ գաղտնահամակարգերում կիրառվում են բաշխված բանալիների ենթակառուցվածքի ստեղծման դասական երկու մոդել՝ բազմանդամային և մատրիցային:

Բազմանդամային հիմքով նախագծված բանալիների ենթակառուցվածքի ստեղծման համար օգտագործվում է ստորև բերված λ-աստիճանի բազմանդամը՝

$$\boldsymbol{f(x,y) = f\,(y,x) = \sum_{i,j=0}^{\lambda} a_{ij} x^i y^j} \quad , \qquad (1)$$

կառուցված Fq վերջավոր դաշտի վրա, որտեղ q-ն պարզ թիվ է, որի արժեքը բավարար մեծ է և օգտագործվում որպես բանալու արժեք՝ հարկավոր գաղտնակայունություն ապահովելու համար: Իրերի ինտերնետ անլար ցանցում օգտագործելով հանգույցի նույնականացման եզակի նշիչը՝ կարելի է ստանալ բանալու վերաբերյալ ամբողջական ինֆորմացիա, որը փոխանցվում է հանգույցին: Այսպիսով, I հանգույցին բանալին հասանելի է տվյալ f (i, j) ֆունկցիայի հաշվարկման արդյունքում:

Հետևաբար, երկու հանգույց կարող են հաշվարկել ընդհանուր բանալին իրենց բանալիների ինֆորմացիայից՝ որպես f(x,y) = f(y,x): f(x,y) բազմանդամային հիմք ունեցող բանալիների ենթակառուցվածքի ստեղծումը հիմնված է Բլունդոյի և մյուսների կողմից ներմուծված սխեմայի վրա:

Մատրիցային հիմքով նախագծված բանալիների ենթակառուցվածքի մոդելն օգտագործում է (λ + 1) × (λ + 1) հանրային G մատրիցը և (λ + 1) × (λ + 1) գաղտնի D մատրիցը՝ դարձյալ վերջավոր Fq դաշտի վրա, որտեղ q-ն նույնպես պարզ թիվ է: Վերոհիշյալ երկու մատրիցն օգտագործվում են երրորդ A մատրիցը գեներացնելու համար:

$$\mathbf{A} = (\mathbf{D} \cdot \mathbf{G})^{\boldsymbol{T}} \qquad (2)$$

Ակնհայտ է, որ եթե D մատրիցը համաչափ է, ապա K մատրիցը նույնպես համաչափ է, որը հաշվարկվում է հետևյալ ձևով.

$$\mathbf{K} = \mathbf{A} \cdot \mathbf{G} \qquad (3)$$

(3) հավասարումից կարող ենք ստանալ $k_{ij} = k_{ji}$, որտեղ k_{ij}-ն K մատրիցի i-րդ տողի և j-րդ սյան տարրն է՝ i, j = 1,2,3, … , λ + 1:

Եթե I հանգույցին հատկացված է ընդհանուր բանալի, որը պարունակում է A-ի i-րդ տողը և G-ի i-րդ տողը, ապա i և j երկու հանգույցները կարող են հաշվարկել իրենց ընդհանուր kij բանալին՝ G-ի սյունակների փոխանակման միջոցով:

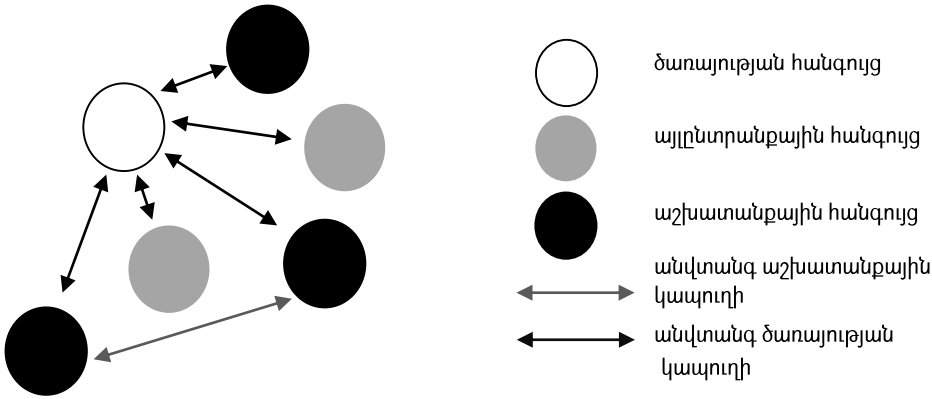
Բացի այդ, եթե G մատրիցը նախագծված է Vander Monde Matrix-ի կիրառմամբ, ապա միայն որոշ մասը պետք է փոխանցվի հանգույցների միջև ողջ սյունակի փոխարեն:

Հարկ է նշել, որ բանալու կառավարման առաջարկված սխեման կարող է աշխատել բանալիների ենթակառուցվածքի գեներացման երկու մոդելի հետ:

Իրերի ինտերնետ միջավայրի առաջարկվող մոդելում հանգույցների գործարկումը կատարվում է ինքնաբերաբար, որի ընթացքում հանգույցներին վերագրվում են համապատասխան դերակատարումներ (նկ.1):

Հանգույցը ցանցին միանալուն պես՝ փորձում է ընտրել իրեն որպես ծառայության հանգույց՝ Ալգորիթմ 1-ում բերված քայլերի համաձայն, երբ տվյալ հանգույցը կարող է ընտրվել որպես ծառայության, այլընտրանքային կամ աշխատանքային հանգույց: Պարզության համար ենթադրենք, որ $T_{total} = T_s \cdot t$, որտեղ t-ն հանգույցի ընտրության և ինքնակարգավորման փուլերի ընդհանուր թիվն է: Հարկ է նշել, որ ինքնակարգավորումը բխում է հանգույցների ինքնակազմակերպվող բնույթից:

Այսպիսով, N_i-րդ հանգույցը նախ փորձում է ինքնուրույն ընտրել իրեն որպես ծառայության հանգույց՝ P_s հավանականությամբ: Եթե փորձը հաջողություն է ունենում, N_i-րդ հանգույցը դառնում է ծառայության հանգույցի թեկնածու և ստեղծում է համապատասխան KP_i բանալու ենթակառուցվածքը: Այնուհետև, N_i-րդ հանգույցը ստուգում է, թե արդյոք գոյություն ունի՞ հեռարձակված հաղորդագրություն:



Նկ. 1. Ցանցային հանգույցները և դրանց կապերը

Եթե N_i հանգույցը ստանում է հեռարձակման հաղորդագրություն, նշանակում է (H-1) ցատկ միջակայքում առկա է ծառայության հանգույց: Հանգույցի ամբողջ հաշվողական ռեսուրսի օգտագործման համար N_i-րդ հանգույցն ընտրվում է որպես այլընտրանքային ծառայության հանգույց:

Եթե N_i հանգույցը հեռարձակման հաղորդագրություն չի ստանում, ապա N_i–րդ հանգույցը դառնում է ծառայության հանգույց, որից հետո այն իր կարգավիճակի վերաբերյալ տեղեկությունը փոխանցում է H ցատկ միջակայքի իր հարևաններին, որից հետո հանգույցում ավարտվում է դերակատարության ընտրության ընթացակարգը:

Եթե հանգույցը չի ընտրվում որպես ծառայության հանգույց, ապա նրան վերագրվում է աշխատանքային հանգույցի կարգավիճակ: N_i –րդ հանգույցը ստուգում է, թե արդյոք առկա՞ է եղել ծառայության հանգույց, որն արդեն գոյություն է ունեցել (H-1) ցատկ միջակայքում: Եթե ընթացիկ փուլում ոչ մի ծառայության հանգույց չի հայտնաբերվում (H-1) ցատկ միջակայքում, ապա N_i–րդ հանգույցը մասնակցում է հաջորդ փուլին, և՝ այդպես շարունակ:

Նախքան աշխատանքային հանգույցները իրենց համապատասխանող ծառայության հանգույցներից կպահանջեն բանալու ինֆորմացիա, հաստատվում է անվտանգ կապուղի դեպի ծառայության հանգույցը:

Ինչպես ցույց է տրված նկ.1-ում, նախ հեռարձակվում է հանգույցի նույնականացման եզակի նշիչը և n բաց բանալին՝ իրեն համապատասխանող հանգույցների միջակայքում: Այնուհետև՝ աշխատանքային հանգույցը ընտրում է պատահական k թիվ և գաղտնագրում է պահանջված հաղորդագրությունը՝ օգտագործելով անհամաչափ գաղտնահամակարգը

$$\mathbf{En}\,(\mathbf{k}\,||\,\mathbf{B}) \;=\; (\mathbf{k}\,||\,\mathbf{B})\mathbf{2}\ \mathbf{mod}\ \boldsymbol{n} \qquad (4)$$

(4) հավասարման լուծման արդյունքում E_n (k || B) || B գաղտնագիրն ուղարկվում է ծառայության հանգույցին՝ կցելով այն ուղարկվող փաթեթին: Ի վերջո, ծառայության հանգույցը վերծանում է պահանջված բանալու ինֆորմացիան՝ հաշվարկելով $D_{p,a}$ (E_n (k || B)):

Այսպիսով, k-ն կարող է օգտագործվել որպես գաղտնի բանալի՝ աշխատանքային հանգույցի և դրան համապատասխանող ծառայության հանգույցի միջև:

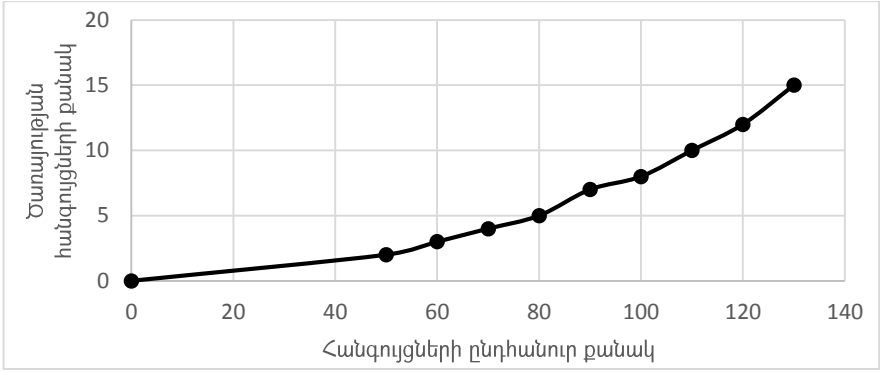
Բանալու ինֆորմացիայի բաշխման ընթացակարգը բեռնվում է անլար ցանցի յուրաքանչյուր հանգույցում՝ հետևայլ կերպ.

Նախ՝ ծառայության հանգույցը հեռարձակում է իր UID և n-ը համապատասխան միջակայքում գտնվող հանգույցներին: Այնուհետև, ծառայության հանգույցը մեկնարկում է աշխատանքային հանգույցների կամ այլընտրանքային ծառայության հանգույցների կողմից ուղարկվող հարցումների սպասարկումը՝ քանի դեռ այդ հարցումների քանակը չի գերազանցում λ մեծությունը:

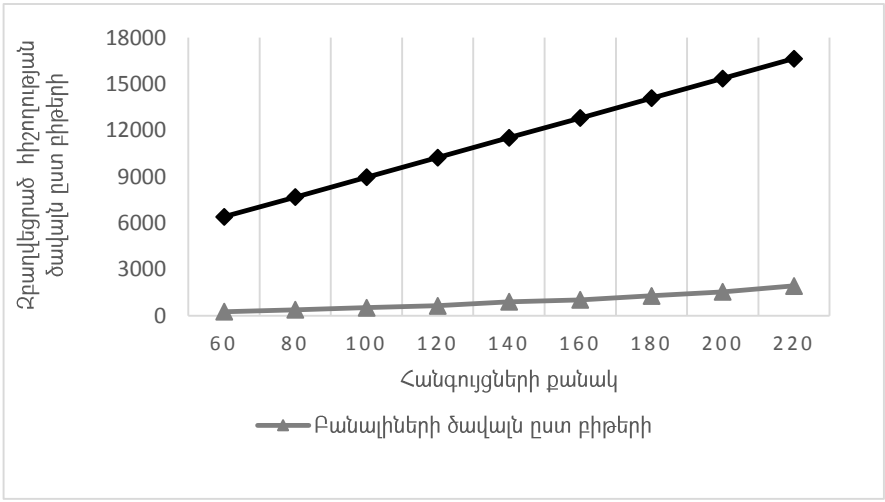
Եթե ստացված հարցման հաղորդագրությունն ուղարկված է աշխատանքային հանգույցից, ապա ծառայության հանգույցը վերծանում է հաղորդագրությունը, այնուհետև գտնում է չօգտագործած բանալի տվյալ հարցման համար և ուղարկում այն համապատասխան աշխատանքային հանգույցին:

Գնահատվել է նաև առաջարկված սխեմայի պիտանելիությունը՝ հիշողության, հաղորդակցման, հաշվողական գերբեռնվածության և հարձակումների նկատմամբ դիմացկունության չափանիշներով: Նկար 2-ում պատկերված է ծառայության հանգույցների քանակական հարաբերակցությունը հանգույցների ընդհանուր քանակի նկատմամբ: Ինչպես նաև նկար 3-ում բերված է բանալիների պահպանման համար

անհրաժեշտ հիշողության ծավալը՝ համեմատած դասական բանալիների պահպանման մեթոդի հետ:



Նկ.2. Ծառայության հանգույցների քանակի կախվածությունն հանգույցների ընդհանուր քանակից



Նկ.3. Բանալիների պահպանման համար անհրաժեշտ հիշողության ծավալի համեմատականը դասական և առաջարկված մեթոդների դեպքում

Երկրորդ գլխում առաջարկվել է նաև գաղտնահամակարգ, որն ապահովում է ամպային միջավայրում պարզ ինտերնետ իրերի հետ անվտանգ հաղորդակցումը: Գաղտնահամակարգը ներառում է նաև լրացուցիչ սարքի կիրառում, որը, տրամադրելով պարզ ինտերնետ իրերի համար հատուկ անլար ցանց, ապահովում է այդ ցանցից ուղարկված և ստացված հարցումների անվտանգությունը: Այդ նպատակով առաջարկվում է, որպես գործառույթների մեկնարկման հրամանների անուններ օգտագործել նախօրոք հեշավորված հաստատուն հրամանների անունները, որտեղ

հեշավորման բանալին անհատական է ամեն սարքի համար և ունի 2^k բարդության աստիճան: Հեշավորման նպատակով օգտագործելով hashcash ֆունկցիան հնարավոր է նախքան հարցումները պարզ սարքերի կողմից ընդունել և վավերականացնել այդ հարցումներում առկա հրամանները:

Երրորդ գլխում մշակվել է ինտերնետ իրերի բաշխված ցանցի կառավարման և գործառույթների անվտանգ իրականացման ամբողջական մոդել:

Իրերի ինտերնետ միջավայրը տարատեսակ իրերից բաղկացած բաշխված ցանց է, որի կողմից տրամադրվող գործառույթը/ծառայությունն իր հերթին բաղկացած է տարբեր իրերի կողմից կատարած գործառույթներից: Վերոնշյալ բաշխված ցանցի կառավարումը, գործառույթների հաջորդականության վերահսկումը և գործառույթների ամբողջականության ապահովումը կարևոր խնդիր է:

Հաշվի առնելով վերոգրյալը՝ առաջարկվում է իրերի ինտերնետի մոդելը կառուցել ուղղորդված ծառի տեսքով, որտեղ հանգույցներն ինքնակազմակերպվող են, իսկ հրահանգների և տվյալների փոխանակումը հանգույցների միջև վերահսկվում է տեղեկատվության անվտանգության և ամբողջականության մեխանիզմներով:

Այդ նպատակով՝ միջավայրի գործառույթների ավտոմատացման համար առաջարկվում է ներմուծել հանգույցներին հաղորդվող հաղորդագրությունների հետևյալ ձևաչափը, որը ներկայացնում է նաև յուրաքանչյուր հանգույցին ուղղված գաղտնիքի (մյուսների համար անվերծանելի) մասնաբաժինը:

Աղյուսակ 2. Հաղորդագրության գլխամասի ձևաչափը

Առանձին հանգույցների գաղտնագրված տվյալները					Գլխամաս
E_1	E_2	E_3	E_4	E_5	Hashcash, N_1 -N_m

Առաջարկվող մոդելն օգտագործում է իրերի ինտերնետ միջավայրի համար մշակված արձանագրությունը և ձևաչափը, որը հնարավորություն է տալիս իրագործել.

Գործառույթների կառավարում, որը կատարվում է ձևաչափում նկարագրված հաջորդականության շնորհիվ: Գործառույթների հաջորդականությունը նկարագրվում է շնորհիվ զանգվածի, որը բաղկացած է 168 բայթ երկարություն ունեցող տեղեկատվությունից, որտեղ առաջին 128 բայթը եզակի նշիչ(UID) է կամ IP6 հասցե: Հաջորդող 32 բայթ երկարությամբ L տվյալը ցույց է տալիս ձևաչափի մարմնում գտնվող գաղտնագրված տեղեկատվության չափը: Վերջին 8 բայթը՝ D-ն ցույց է տալիս համապատասխան ինտերնետ իրի գործառույթի խորությունը գործառույթների ծառում:

Աղյուսակ 3. Հաղորդագրության մարմնի ձևաչափը

N_1 գործառույթ			N_2 գործառույթ			N_m գործառույթ		
UID | IP6	L	D	UID | IP6	L	D	UID | IP6	L	D
128բ	32բ	8բ	128բ	32բ	8բ	128բ	32բ	8բ

Տվյալների գաղտնագրում, որը կատարվում է 1-ից մինչև N քանակի բանալիներով, որտեղ N պարամետրը փոքր կամ հավասար է ցանցում առկա ինտերնետ իրերի թվին: Շնորհիվ տարբեր բանալիների կիրառության՝ հնարավոր է ապահովել առանձին ինտերնետ իրերին պատկանող գաղտնագրված ինֆորմացիայի անվտանգությունը ցանցում՝ նույնիսկ այլ ինտերնետ իրերի խոցելիության դեպքում: Գաղտնագրման բանալու ստեղծման համար օգտագործվում է հետևալ բանաձևը՝ $K = H * K_i$, որտեղ K_i-ն ինտերնետ իրում նախաբեռնված բանալին է, իսկ H պարամետրը՝ տվյալ ինտերնետ իրին հարցում ուղարկած հանգույցին պատկանող բաց տվյալների հեշ արժեքը, որը հանգույցը ուղարկում է հարցման ժամանակ: Շնորհիվ L պարամետրի՝ հաղորդագրության ձևաչափի մարմնում կարելի է գտնել կոնկրետ ինտերնետ իրի հաղորդագրության սկզբնական և վերջնական արժեքները հետևյալ բանաձևով

$$L_{start} = L_0 + L_1 + \cdots + L_{i-1},\ L_{end} = L_{start} + L_{end},\qquad D(N_i) = L_{start}, \ldots, L_{end} \tag{5}$$

Հարցում ուղարկող հանգույցը գտնվում է D–1 կամ D +1 խորության վրա, որտեղ D-ն դա տվյալ հանգույցի խորությունն է: Նկարագրած ձևաչափի կիրառումը հնարավորություն է տալիս ապահովել ինտերնետ իրերին պատկանող տեղեկատվական անվտանգությունն այլ ինտերնետ իրերից:

Սխալների հայտնաբերում և գործառույթների չեղարկում, որը կատարվում է՝ հիմնվելով գաղտնագրված տեղեկատվության վերծանման արդյունքի վրա: Ինչպես նշվել է, ինտերնետ իրերին պատկանող տեղեկատվության վերծանման համար անհրաժեշտ է D–1 ինտերնետ իրերին պատկանող բաց տվյալի հեշավորումը և տվյալ ինտերնետ իրերի բանալին: Հեշավորման բացակայության կամ սխալ վերծանման դեպքում, օգտվելով ստուգող կոդերից, ինտերնետ իրը սկսում է գործառույթի չեղարկման գործառույթը, որտեղ չեղարկման հարցումները կատարվում են հակառակ ուղղությամբ:

Այսպիսով, ներկայացրած արձանագրության շնորհիվ, հարցումից կախված, ինֆորմացիան փոխանցվում է ցանցի հանգույցին, որը

- իրեն հասանելի մասնաբաժնի համար իրականացնում է վերծանում և դրան համապատասխան գործառույթ,
- ձևավորում է վերծանված մասնաբաժնի հեշը, որը հավելվում է վերոհիշյալ հաղորդագրության մեջ՝ գաղտնիքի մասնաբաժնի ամբողջականության վերահսկման նպատակով:

Քանի որ ձևաչափը տեղեկություն է պարունակում տվյալ հանգույցից դեպի այլ՝ տրամաբանորեն հաջորդ հանգույց տանող ճանապարհի վերաբերյալ, որը փաստորեն ենթադրում է "նավարկում" դեպի ծառի ավելի ստորին մակարդակում/մակարդակներում տեղակայված մեկ կամ մի քանի հանգույցներ, ապա ստորին մակարդակի ամեն հանգույց՝ ստանալով նշված ձևաչափի հաղորդագրությունը, նախ՝ փորձում է իր կարգային համարը գտնել այդ հաղորդագրության մեջ, որից հետո վերծանելով գաղտնիքի իր մասնաբաժինը և արտադրելով համապատասխան հեշը, կառավարումը փոխանցում է հաջորդ հանգույցին: Արդյունքում բոլոր անհրաժեշտ հանգույցների կողմից մշակված և արտադրված հեշ արժեքների հավաքածուն վերահսկում է ցանցով փոխանակվող տվյալների և գործառույթների ամբողջականությունը, իսկ բաշխվող

բանալիների ենթակառուցվածքը՝ այդ նույն տվյալների և գործառույթների անվտանգությունը:

Հարկ է նշել, որ ցանցով տվյալների և հրահանգների փոխանակման առաջարկվող մոդելը հաջորդական է և ենթադրում է սեսսիոն բանալիների ենթակառուցվածք, որը բաշխում է սեսսիոն բանալիները՝ ծառի մակարդակներին համապատասխան:

Այն դեպքում, երբ հանգույցը, որին փոխանցվել է վերոհիշյալ ձևաչափի հաղորդագրությունը և որն իր կարգային համարը չի հայտնաբերում այդ հաղորդագրության մեջ, ուստի ազատ է գաղտնիքի որև է մասնաբաժին վերծանելուց, կառավարումը փոխանցում է հաջորդ հանգույցին՝ ապահովելով միայն հեշավորումը:

Հեշ արժեքների ստուգման անհաջողության դեպքում տվյալ հանգույցի գործառույթի ամբողջ շղթան, չեղարկման հետ, ազդանշան է ուղարկվում նույն հաջորդականությամբ:

Հաջողության դեպքում հանգույցը որոշում է ստացված հաղորդագրությունը փոխանցել անհրաժեշտ հանգույցին՝ ըստ UID-ի: Ամեն հաջորդ հանգույցում ձևավորված հեշերի շղթան երաշխիք է՝ հավաստիացնելու համար ցանցի գործողությունների վավեր լինելը:

Այսպիսով, առաջարկվել են իրերի ինտերնետ միջավայրի համար մշակված արձանագրությունը և ձևաչափը, որն ունակ է տեղեկություն հաղորդել այլ հանգույցների՝ տվյալ հանգույցում անոմալիաների իրազեկման համար և արգելակել ամբողջ համակարգի աշխատանքը՝ թույլ օղակի գործոնով՝ բացառելով համակարգի հետագա գործողությունը:

Չորրորդ գլխում ատենախոսության մեջ բերված հետազոտությունների հիման վրա ներկայացվել են մշակված ծրագրային լուծումները, որոնք ներառում են՝ IKS բանալիների բաշխման մոդուլը, SIT մոդուլը և Իրերի ինտերնետ միջավայրում գործառույթների ամբողջականությունը ապահովող մոդուլը: Վերոհիշյալ ծրագրային լուծումների փորձարկման համար ստեղծվել է համապատասխան վիրտուալացման համակարգ, որը հիմնված է Docker ծրագրային միջավայրի վրա: Այն հնարավորություն է տալիս ստեղծել արհեստական իրերի ինտերնետ միջավայր, որտեղ օգտատերն առաջադրում է գործարկվող հանգույցների թիվը և կարողանում է հետևել համակարգի աշխատանքին իրական ժամանակում: Մեկուսացման հիմքում ընկած են Linux միջավայրի հետևալ հասկացությունները՝ cgroup, union ֆայլային տիրույթը և ՕՀ միջուկի գործընթացների անունների տարածությունը:

Վիրտուալացման միջավայրի բնութագրման համար օգտագործվում են պատկերները (images), որոնք պարունակում են վիրտուալացրած միջավայրի ծրագրային անհրաժեշտ կարգավորումները և հավելվածները: Ստեղծվել են 4 տարբեր տեսակի պատկերներ.

- Պատահական տարատեսակ, որը նախատեսված է գլուխ 2-ում նկարագրած բանալիների բաշխման սխեմայի հիման վրա ստեղծված IKS ծրագրի փորձարկման համար: Տվյալ տեսակի հանգույցում տեղադրվում է IKS բանալիների բաշխման ծրագրային մոդուլը՝ անհրաժեշտ նախաբեռնված կարգավորումներով, որոնք հնարավոր է փոփոխել վիրտուալացումից առաջ

համապատասխան պատուհանում: Նշված տեսակի հանգույցի տեխնիկական բնութագրերը, մասնավորապես՝ հիշողությունը և պրոցեսորի արտադրողականությունն ընտրվում են պատահականության սկզբունքով ՝ տարատեսակ միջավայր ստանալու նպատակով:

- Ցածր արտադրողականության, որը նախատեսված է քիչ ռեսուրսներ ունեցող իրերի ինտերնետի վիրտուալացման համար: Տվյալ տիպի հանգույցները զուրկ են գաղտնագրման որևէ գործառույթներից և հասարակ հարցումներ են կատարում շարժական բանալուն որոշակի պարբերականությամբ: Եթե ընտրված է գոնե մեկ ցածր արտադրողականության հանգույց, դա նշանակում է, որ կստեղծվի շարժական բանալու վերտուալացում ևս:
- Շարժական բանալու պատկերը, որի մեջ նախապես ներդրված SIT ծրագրային իրականացումը շնորհիվ ցածր արտադրողականություն ունեցող հանգույցներից ստացված և դեպի այդ հանգույցներ ուղարկված տվյալները գաղտնագրվում և վերծանվում են ապահովելով տվյալների անվտանգ փոխանակման գործընթացը: Շարժական բանալու վեբ գրաֆիկական կառավարման վահանակը հասանելի կլինի ամեն հանգույցում լոկալ հասցեում 8086 պորտի միջոցով:
- Գործառույթների ամբողջականությունը և անվտանգությունը ապահովող համակարգ, որը մշակված արձանագրության շնորհիվ ապահովում է բոլոր հանգույցների միջև կատարվող գործառույթների ամբողջականությունը և գաղտնիությունը: Իրերի ինտերնետ վերտուալացրած միջավայրում տվյալ հանգույցը կարող է գոյություն ունենալ մինչև 15 օրինակով:

Միաժամանակ ցույց է տրվել, որ հետազոտական նպատակների համար նախատեսված ծրագիրը հնարավորություն է տալիս վերտուալացնել իրերի ինտերնետ միջավայրը համակարգչում և կատարել փորձեր, ուսումնասիրել բանալիների բաշխման, շարժական բանալու և ներխուժումների բացահայտման սխեմաները:

ԱՇԽԱՏԱՆՔԻ ՀԻՄՆԱԿԱՆ ԱՐԴՅՈՒՆՔՆԵՐԸ

- Մշակվել է գաղտնագրային բանալիների կառավարման մեթոդ, որն ապահովում է սարքերի ինքնակարգավորումը և տվյալների անվտանգ փոխանակումը:

- Մշակվել է գաղտնահամակարգ՝ ամպային միջավայրում պարզ ինտերնետ իրերի հետ անվտանգ հաղորդակցման ապահովման նպատակով, որն ապահովելով անհրաժեշտ անվտանգություն, սարքերի տեխնիկական բնութագրերի փոփոխություն չի պահանջում:

- Մշակվել է ամպային բաշխված ցանցերում գործառույթների ամբողջականությունն ապահովող մեթոդ, որը բացահայտում և կանխարգելում է ամպային միջավայրին ուղղված հատուկ գրոհները:

- Մշակվել է բանալիների կառավարման IKS ծրագրային մոդուլը, որը հնարավորություն է ընձեռում առանց սարքի նախնական կարգաբերման, միացնել այն ցանցին և ապահովել այլ ինտերնետ իրերի հետ անվտանգ կապը: Գաղտնագրման հնարավորություններից զուրկ սարքերի միջև անվտանգ տվյալների փոխանակման նպատակով ստեղծվել է SIT ծրագրային ապահովումը, որը ներդրվում է ցանցում գտնվող լրացուցիչ սարքում և ապահովում է գաղտնագրման գործառույթները: Մշակվել է նաև գլուխ 3-ում նկարագրված արձանագրության ծրագրային իրացումը, որի կիրառման արդյունքում հնարավոր է ապահովել իրերի ինտերնետ միջավայրում կատարվող գործառույթների անվտանգությունը և ամբողջականությունը:

ՀՐԱՏԱՐԱԿՎԱԾ ԱՇԽԱՏՈՒԹՅՈՒՆՆԵՐԸ

[1] Hovsepyan V., " Secure Real-Time Data Transfer in the Cloud", Meeting Security Challenges Through Data Analytics and Decision Support. “NATO Science for Peace and Security” Series - D: Information and Communication Security – 2016, Vaolume47, pp. 271-276.

[2] Հովսեփյան Վ., "Շարժական բանալու կիրառումը ամպային միջավայրում", ՀԱՊՀ Լրաբեր, գիտական և մեթոդական հոդվածների ժողովածու, Երևան, Հայաստան, 2016, pp. 162-167:

[3] Hovsepyan V., “Files pfull life cycle protection and secure distribution”, Proceedings of the Conference Computer Science and Information Technologies (CSIT-2015), Yerevan 2016, pp. 217-219.

[4] Hovsepyan V., “Securing of IOT environment”, Тезисы докладов международной научно-практической конференции молодых ученых и студентов, Киев, Украина, 2016, С. 224-226.

[5] Hovsepyan V., “Securing data transfer in IOT environment”, Науковий журнал Безпека інформації, Киев, Украина, pp. 131-134, Kiev, Ukraine 2016

[6] Hovsepyan V., Khemchyan A., Atayan B. “Data Security and Backup in Cloud Envirement”, Proceedings of the Conference World Congress on Internet security (WorldCIS2016) – London, United Kingdom, 2016, P. 101-105

Hovsepyan Vladimir Hovsep

DEVELOPMENT OF ADDITIONAL TOOLS FOR SAFETY WORK OF CLOUD TECHNOLOGY

RESUME

The development trends of modern information technologies and telecommunication systems, in particular, the large-scale introduction of cloud technologies in all the spheres of human activity, puts forward new requirements to ensuring the information security without which it would be impossible to provide the further progress of those fields.

The Internet of things is one of the fastest developing spheres of cloud technology. The interrelation of the cloud Internet of things enables to control and automate the transactions taking place. The devices of that class are produced to perform certain functions, and as a rule their computation capacity is relatively low. On the other hand, the companies engaged in the production of things, try to create easy-to-use and less resource consuming internet devices without paying adequate attention to ensuring the information security. The internet things, having such a problem from the viewpoint of information security, can be classified in two groups: various devices which are able to perform enciphering, and devices in which it is impossible to perform enciphering due to low capacity. Low productivity of these devices can be called simple Internet things.

Restrictions on cryptographic systems in variety of Internet things require a coordination within Internet of things and the cryptographic system, before joining to the cloud network. This fact will have an unavoidable negative impact on the flexibility of the cloud environment. At the same time, the already known key distribution systems for the vast array of Internet things are not applicable, as they are designed for uniform devices, while the production environment includes a wide variety of Internet devices.

As was mentioned, there are different types of internet things not allowing to apply encryption technics due to incompatibility of some technical requirements or adequate software. One of the approaches to overcome that difficulty is to make technical changes in the device which will actually increase its initial cost. It is necessary to find a solution for this problem without making technical or software changes in already produced devices.

The Internet of things may also have a physical impact on the external environment, that is why, ensuring the integrity of transactions taking place is mostly important. The main obstacle while ensuring the integrity of transactions is the vulnerability of the internet of things against network attacks, in particular, to intrusions and DDoS attacks. The neutralization of these threats along with the increase in the number of items in the Internet environment with remote control devices becomes more and more important. Experience shows that the majority of Internet things provides only basic security requirements, through the identification and protection against network attacks. Existing solutions in this area are mainly software solutions which are carried out usually for a centralized server environment and require significant computing resources.

The goal of the work is to develop additional security tools allowing to implement secure data exchange in order to ensure full functionality and protection from network attacks.

To achieve that goal, the following tasks have been put forward and solved:

- A method for managing cryptographic keys which will ensure self-regulation of devices connected to the network and secure data exchange between them, has been developed;
- A secure method in the cloud environment for simple devices, which, due to limited resources, do not provide cryptographic procedures, has been developed;
- A method ensuring the integrity of transactions in cloud distributed network which will reveal the attacks against the cloud environment and preventing them, has been developed.

The main results are:

- A new cryptographic key management method has been developed which ensures self-regulation of devices, also provides secure data exchange;
- A cryptographic system for ensuring secure communication of simple things in the cloud environment has been developed, which by ensuring the required security, do not require changes in technical parameters [1, 3];
- A method to ensure the transactions integrity has been developed for a cloud-based distributed network which detects and prevents attacks specific for the cloud environment [2];
- Based on the obtained scientific results, IKS a software of the key control method has been developed allowing to connect the device to the network without its preliminary adaptation and to ensure a secure link with other internet things. SIT module has been developed, which, being introduced in the additional device inside the network, ensures secure data exchange between the devices which do not support encryption. Also, a software implementation of the protocol, presented in the third chapter, was created to ensure the integrity and security of the transactions of the Internet of things [4, 5, 6].

ОВСЕПЯН ВЛАДИМИР ОВСЕПОВИЧ

РАЗРАБОТКА ДОПОЛНИТЕЛЬНЫХ СРЕДСТВ ДЛЯ БЕЗОПАСНОЙ РАБОТЫ С ОБЛАЧНЫМИ ТЕХНОЛОГИЯМИ

РЕЗЮМЕ

Развитие современных информационных технологий и телекоммуникационных систем, в частности, широкомасштабное проникновение облачных технологий во все сферы человеческой деятельности предъявляет новые требования к обеспечению информационной безопасности, без чего невозможно дальнейшее развитие указанных областей.

Облачная реализация среды интернет вещей является одной из стремительно развивающихся отраслей информационных технологий. Взаимосвязанность облачных интернет вещей даёт возможность управлять транзакциями и автоматизировать процессы. Устройства такого рода в основном созданы для осуществления определённых функций и имеют малую мощность. С другой стороны, предприятия, выпускающие устройства, пытаются создать интернет вещи, которые удобны в эксплуатации и потребляют малые ресурсы, часто не задумываясь над проблемами безопасности. Интернет вещи, имеющие вышеуказанную проблему, делятся на две группы: устройства, способные выполнять криптографические функции, и устройства, лишенные этих функций из-за нехватки вычислительных способностей.

Разнородные интернет вещи, способные выполнять криптографические функции, требуют адаптации устройств ещё до присоединения к облачной сети, что неизбежно имеет негативное влияние на расширяемость облачной среды. С другой стороны, для преобладающей массы интернет вещей существующие системы распределения ключей неприемлемы, так как они предусмотрены для однородных устройств, тогда как интернет-среда состоит из разнородных элементов.

Как было отмечено, есть виды интернет вещей, которые решены возможности выполнять криптографические функции по причине несовместимости технических требований или программного обеспечения. Это проблема может привести к необходимости технических изменений устройств, что приведёт к повышению их себестоимости. Следовательно, необходимо найти такое решение проблемы, которое не требует технических или программных изменений устройств.

Заметим, что интернет вещам свойственно физическое воздействие на внешнюю среду, поэтому целостность транзакции интернет вещей имеет огромное значение. Препятствием в обеспечении этой целостности служит уязвимость интернет вещей к различного рода атакам, в частности, проникновениям и DoS атакам. Критическое значение этих угроз для интернет вещей увеличивается с умножением количества телеуправляемых устройств. Опыт показывает, что большинство интернет вещей удовлетворяют только простейшие требования безопасности посредством идентификации и не защищены от атак. Существующие до сих пор решения основаны

на программном обеспечении, которое разработано в основном для централизованной серверной среды и требуют больших вычислительных ресурсов.

Цель работы. Разработать дополнительные средства безопасности для работы с облачными технологиями с целью обеспечения безопасного обмена данными, целостности транзакция и устойчивости к сетевым атакам.

Для достижения этой цели были поставлены и решены следующие задачи:

- Разработать метод управления криптографическими ключами, который обеспечивает саморегулирование соединяемых устройств среды и безопасный обмен данными между ними.
- Разработать безопасный коммуникационный метод в облачной среде для тех устройств, которые из-за ограниченности ресурсов не обеспечивают криптографические процедуры.
- Разработать метод для обеспечения целостности транзакций облачных распределенных сетей, который также обнаруживает и предотвращает атаки, присущие облачной среде.

Основные результаты диссертационной работы следующие:

- Разработан новый метод управления ключами, который обеспечивает самоконфигурирование интернет вещей и безопасную среду для обмена данными.
- Разработана криптосистема для безопасного обмена данными между облачными интернет вещами, которая обеспечивая необходимую безопасность, не требует изменений их технических параметров.
- Разработан метод, обеспечивающий целостность транзакции в облачных распределенных сетях, который предотвращает свойственные облачной среде атаки и предотвращает их.
- На основании полученных научных результатов разработано программное обеспечение IKS для управления ключами, что даёт возможность подключения устройства к сети и работы с интернет вещами без предварительной адаптации и настройки. Наряду с этим, создано программное обеспечение SIT, позволяющее установить дополнительное устройство в сети и, обеспечивающее безопасность тех устройств, которые не могут обеспечить криптографические процедуры. Также создана программная реализация протокола, которая обеспечивает целостность и безопасность транзакций интернет вещей.