ԵՐԵՎԱՆԻ ՊԵՏԱԿԱՆ ՀԱՄԱԼՍԱՐԱՆ

Ասլանյան Հակոբ Լևոնի

ԱՆԼԱՐ ՑԱՆՑԵՐԻ ՄԱԹԵՄԱՏԻԿԱԿԱՆ ՄՈԴԵԼՆԵՐՈՒՄ ԱԼԳՈՐԻԹՄԱԿԱՆ ԽՆԴԻՐՆԵՐԻ ՀԵՏԱԶՈՏՈՒՄ

Ա.01.09 –«Մաթեմատիկական կիբեռնետիկա և մաթեմատիկական տրամաբանություն» մասնագիտությամբ

ֆիզիկամաթեմատիկական գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսության

ՍԵՂՄԱԳԻՐ

ԵՐԵՎԱՆ — 2010

ЕРЕВАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Асланян Акоп Левонович

ИССЛЕДОВАНИЕ АЛГОРИТМИЧЕСКИХ ПРОБЛЕМ В МАТЕМАТИЧЕСКИХ МОДЕЛЯХ БЕСПРОВОДНЫХ СЕТЕЙ

АВТОРЕФЕРАТ

Диссертации на соискание ученой степени кандидата физикоматематических наук по специальности 01.01.09 - “Математическая кибернетика и математическая логика”

ЕРЕВАН – 2010

Ատենախոսության թեման հաստատվել է Երևանի պետական համալսարանում:

Գիտական ղեկավար՝	ֆ.մ.գ.դ. Ա. Ա. Ալեքսանյան
Պաշտոնական ընդդիմախոսներ՝	ֆ.մ.գ.դ. Հ. Բ. Մարանջյան ֆ.մ.գ.թ. Ռ. Ն. Տոնոյան
Առաջատար կազմակերպություն՝	ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտ

Պաշտպանությունը կայանալու է 2010թ., հունիսի 7-ին ժ.14:00-ին ԵՊՀ-ում գործող ԲՈՀ-ի 044 «Մաթեմատիկական կիբեռնետիկա և մաթեմատիկական տրամաբանություն» մասնագիտական խորհրդի նիստում, հետևյալ հասցեում՝ Երևան, 0025, Ալեք Մանուկյան, 1:

Ատենախոսությանը կարելի է ծանոթանալ Երևանի պետական համալսարանի գրադարանում:

Սեղմագիրն առաքվել է 2010թ. մայիսի 6-ին

Մասնագիտական խորհրդի գիտական քարտուղար
Ֆիզ. մաթ. գիտ.թեկնածու Վ. Ժ. Դումանյան

Тема диссертации утверждена в Ереванском государственном университете.

Научный руководитель:	д.ф.м.н А. А. Алексанян
Официальные оппоненты	д.ф.м.н. Г. Б. Маранджян к.ф.м.н. Р. Н. Тоноян
Ведущая организация:	Институт проблем информатики и автоматизации НАН РА

Защита состоится 7 июня 2010 г. в 14:00 на заседании специализированного совета 044 “Математическая кибернетика и математическая логика” ВАК при ЕГУ по адресу: 0025, г. Ереван, ул. Алека Манукяна 1.

С диссертацией можно ознакомиться в библиотеке Ереванского государственного института .

Автореферат разослан 6 мая 2010 г.
Ученый секретарь специализированного совета
кандидат физ. мат. наук: В. Ж. Думанян

ԱՏԵՆԱԽՈՍՈՒԹՅԱՆ ԸՆԴՀԱՆՈՒՐ ԲՆՈՒԹԱԳԻՐԸ

Ներկայացվող աշխատանքը նվիրված է ժամանակակից համակարգչային ցանցերի նորագույն մաթեմատիկական մոդելների և ալգորիթմական խնդիրների ուսումնասիրմանը:

Ինֆորմացիոն տեխնոլոգիաները, որոնք բիո և նանոտեխնոլոգիաների հետ մեկտեղ համարվում են տնտեսության զարգացման ներկայիս կարևորագույն գործոնները, բնութագրվում են այնպիսի ձեռքբերումներով, ինչպիսիք են նորագույն ցանցերը (ինտերնետ, բջջային ցանց, գլոբալ տեղադրվածության համակարգեր, շարժական և ռադիո կապի ցանցեր), բարձր արդյունավետության և էլեկտրոնային սարքերը և համակարգերը (տերաբիթանոց կապ, GRID համակարգեր, անհատական օգտագործման սարքերի նոր սերունդ), էլեկտրոնային բովանդակության համակարգերը (սոցիալական ցանցեր, էլեկտրոնային գրադարաններ) և այլն: Տիրույթի հաջողությունները պայմանավորված են միկրոէլեկտրոնիկայի զարգացմամբ և, համամասնորեն, մաթեմատիկական նոր գիտելիքի ձևավորմամբ: Վերջիններիս թվում են բազմանդամային նորանգույն ալգորիթմները՝ գծային ծրագրավորում և թվի պարզության ստուգում, հայտնի դասական խնդիրների լուծման նոր ալգորիթմներ, ստորին գնահատականների բարելավում՝ մոնոտոն սխեմաների բարդություն, հոմոմորֆիկ կրիպտոմոդելի ստեղծում, ապրոքսիմացիոն ալգորիթմների ստացում և այլն: Այս ամենին զուգահեռ առաջանում են նոր մաթմատիկական մոդելներ, որոնց ուսումնասիրումն առաջ է բերում նոր ալգորիթմական խնդիրներ: Նման առանձնահատուկ օրինակ է անլար սենսորային ցանցերի գիտատեխնիկական տիրույթը:

Սենսորային ցանցի հանգույցները ինքնավար սարքեր են, կազմված զարգացած տեխնիկական համակարգերից՝ սենսորներ, ռադիո կապի հնարավորություն, հաշվող սարք և սնուցում: Սրանք լինելով միկրո-սարքեր, ունեն սահմանափակ ռեսուրսներ և պահանջում են օպտիմալ կառավարում երկարաժամկետ գործունեության ապահովման համար: Երկրորդ կարևորագույն առանձնահատկությունը ինքնակառավարման կարգընթացների անհրաժեշտությունն է այն կապակցությամբ, որ ցանցի կառուցվածքը ի սկզբանե անհայտ է և որ այն կարող է կազմվել լոկալ գործընթացների արդյունքում, ինչն ինքնակառավարման դասական սցենար է: Սենսորային ցանցը սովորաբար աշխատում է վտանգավոր կամ անհասանելի տարածության մեջ և ի վիճակի է լուծել կարևորագույն խնդիրներ՝ գյուղատնտեսական տարածքի մոնիտորինգ, անհասանելի տարածքի հետախուզում, բարդ ֆիզիկական համակարգի տեխնիկական ստուգում և այլն: Մաթեմատիկական խնդիրները, որոնք առաջանում են անլար սենսորային ցանցերում, բացի ավանդական ալգորիթմներից պահանջում են նոր խնդիրների լուծում և նոր ալգորիթմների մշակում:

Կարևորագույն խնդիրները դրանք ցանցի կապակցվածության ձևավորումն ու ապահովումն է, նպատակային տիրույթի ծածկումն է, կրիպտոգրաֆիկ պարզագույն, բայց բավարար կայուն սխեմաների մշակումն ու կիրառումն է և, որ ամենակարևորն է, այս ամենի համատեղ իրականացնումն է մինիմալ էներգիայի օգտագործման պայմաններում: Առաջ են գալիս առանձնահատուկ խնդիրներ՝ օրինակ

ինտերֆերենցիան, որը ռադիո հասանելիության պատիկությանն է նվիրված: Խնդիրը առավել բարդ խնդիրներից է և համարվում է չլուծված:

Ներկա աշխատանքը դիտարկում է երեք հիմնական խնդիր:

Առաջին մասը նվիրված է ինտերֆերենցիայի խնդրի լուծմանը: Այստեղ համատեղվում են տիրույթի ծածկման և հասանելիության պատիկության մինիմիզացիայի պահանջները: Ֆորմալ մակարդակում նախ ապացուցվում է համապատասխան ալգորիթմական խնդրի *NP* դժվար լինելը: Այնուհետև կառուցվում է խնդրի լուծման մոտարկող իտերատիվ ալգորիթմ և գնահատվում են նրա ճշգրտության աստիճանը և հաշվման իտերատիվ փուլերի քանակը:

Երկրորդ մասը դա ավտոնոմ ծրագրային ագենտների քանակական բնութագրերի ստացումն է կոմբինատոր տերմիններով: Խնդիրը հավանականային է: Իրականացվում է ինֆորմացիայի հավաքում պատահականորեն տեղաբաշխված n սենսորային հանգույցներում m ագենտների միջոցով, որոնցից յուրաքանչյուրն իր հերթին պատահականորեն կարող է ցատկել թվով k հանգույցների մեջ: Հարկավոր է գտնել մինիմալ m և k, որոնք կապահովեն պահանջվող ինֆորմացիայի հավաքումը: Մինչ այժմ այս պարամետրերի միջև հայտնի առնչությունները բարդ են, չապահովելով խնդրի կիրառական լուծումը և այս մասում աշխատանքի արդյունքը համապատասխան նոր բանաձևերի դուրսբերումն է:

Երրորդ հատվածը ցանցի ծածկագրման ապահովումն է: Օգտագործվում է հանրահաշվական մի կառուցվածք՝ պարզագույն սիմետրիկ ծածկագրման ալգորիթմի սինթեզման համար: Ապացուցվում է կոդավորման դարձելիության ճշտությունը: Ներկայացվում է բանալիների բաշխման ալգորիթմ և հիմնավորվում է նրա աշխատանքի ճշտությունը:

Թեմայի հրատապությունը

Կիրառական – ծրագրային համակարգերը իրենց հիմքում ունեն բազմաթիվ ալգորիթմական լուծումներ և նրանց աշխատանքի վերջնական արդյունավետությունը էապես է կախված այս ալգորիթմների բարդությունից:

Ինֆորմացիոն տեխնոլոգիական ժամանակակից բազմաթիվ կիրառական խնդիրներ - կերպարների վերծանում, հակադարձ խնդիրների լուծում, ծածկագրման խնդիրներ, աշխատանքների պլանավորում և այլն, առնչվում են ալգորիթմների հետ, որոնց համար պարզ, բազմանդամային բարդության լուծումներ հայտնի չեն: Այս խնդիրների մի մասը կազմում է ալգորիթմորեն բարդ *NP* դասը: Այլ խնդիրների համար նույնիսկ *NP* դասին պատկանելիությունը հայտնի չէ, ինչը ևս նշանակում է, որ սրանք էլ այսօր չունեն պարզ լուծումներ: Այսպիսով, նման խնդիրների հետ առնչվող կիրառական համակարգերը ունեն առանձնակի բարդություն, և սա պահանջում է խնդիրների մոտավոր կամ հավանականային լուծումների այլընտրանքի ուսումնասիրումը, ինչը հրատապ և բարդ խնդիր է: Միևնույն ժամանակ, որոշ խնդիրների համար մոտարկման ալգորիթմներ այսօր հայտնի են: Խնդիրների մեծ մասի լուծումը հիմնվում է էվրիստիկ ալգորիթմների վրա, որոնք գնահատված արդյունք չեն երաշխավորում, բայց և հատարկման միակ այլընտրանքն են:

Կան մեծ թվով տիպային խնդիրներ, որոնց սովորաբար (բազմանդամային

բարդությամբ) հանգեցվում են NP դասի խնդիրները: Հիմնական օրինակը կոնյունկտիվ նորմալ ձևի իրագործելիության խնդիրն է: Այս հանգեցումները խնդիրները բերում են բուլյան ֆունկցիաների և տրամաբանական նորմալ ձևերի տերմինների: Նման ունիվերսալ խնդրի դեր է տանում նաև ամբողջարժեք գծային ծրագրավորման մոդելը: Կոմբինատոր օպտիմիզացման բազմաթիվ խնդիրներ բնականորեն հանգեցվում են ամբողջարժեք գծային ծրագրավորման խնդիրներին: Այս ոլորտի կարևորագույն արդյունքը գծային ծրագրավորման խնդրի բազմանդամային բարդությունն է ըստ Լ. Խաչիյանի: Սակայն ստացվող ռացիոնալ լուծումը հեշտությամբ չի վերածվում ամբողջարժեք լուծման, մասնավորապես, քանի որ նման կետի անմիջական շրջակայքում կարող են լինել թվով ցուցչային ամբողջարժեք կետեր: Տիրույթում հայտնի են պատահական կլորացման և Լագրանժյան ռելաքսացիայի (թուլացման) մեթոդները: Սրանք բարդ լուծումներ են, որոնց արդյունքը մի քայլ ավելի է մոտեցնում նախնական խնդրի լուծմանը: Այս մոտեցումների կիրառման համար խնդիրը պետք է ճիշտ նախապատրաստել և պետք է ստանալ մի շարք ուղեկցող խնդիրների լուծումը: Խնդիրների մյուս դասը, որը կարևոր նշանակություն ունի ներկա ուսումնասիրության մեջ, դա բազմության ենթաբազմությունների միջոցով ծածկելու խնդիրն է: Սա հիմնական *NP*-լրիվ խնդիրներից մեկն է: Հայտնի է, որ խնդիրը թույլ է տալիս լոգարիթմական ապրոքսիմացիա, օրինակ, գրադիենտ (ագահ) ալգորիթմի միջոցով: Նշված և բազմաթիվ այլ ալգորիթմներ միասին կազմում են նաև ժամանակակից ցանցային մոդելի հիմքը: Արձանագրությունները, որոնք ապահովում են կապը, տիրույթի ծածկումը, կապի անվտանգությունը, ծախսվող էներգիայի նվազեցումը և այլ պահանջվող բնութագրեր, բարդ համակցում են կիրառական ալգորիթմների, որոնք ի լրումն ամենի ունեն լրացուցիչ առանձնահատկություններ և նոր պահանջներ:

Աշխատանքի նպատակն ու խնդիրները

Աշխատանքի նպատակը ալգորիթմական լուծումների ստացումն է, որոնք անհրաժեշտ են ցանցային մոդելների նախագծման և իրականացման համար: Առաջնահերթ նպատակը դա ինտերֆերենցիայի լուծման ուղղությամբ նոր գիտելիքի ձևավորումն է: Ինտերֆերենցիայի խնդիրը, որը տիրույթում հիմնական չլուծված խնդիրն է, դիտարկում է ցանցի կապակցվածությունը այնպես, որ գագաթների (ընդունիչի) մյուս գագաթներից (հաղորդիչի) հասանելիության պատիկությունը լինի մինիմալ: Օգտագործվող ռեսուրսները՝ դա ինֆորմացիայի ցրման շառավղի ընտրությունն է, և դրանից հետո, որոշակի ավելցուկային կապերի ընդհատումն է: Համապատասխան մաթեմատիկական մոդելը, որը սահմանվում է աշխատանքի շրջանակներում, մինիմալ մասնակի մասնակցությամբ բազմության մասնակի ծածկույթ (ՄՄՄԲՄԾ) խնդիրն է: Նպատակը այս խնդրի մոտարկման ալգորիթմի կառուցումն է:

Կապակցվածության խնդրի մյուս բաղադրիչը ցանցով տեղափոխվող տվյալների պաշտպանվածության ապահովումն է: Այստեղ առաջացող ոչ ստանդարտ կրիպտոգրաֆիկ խնդիրն այն է, որ կապակցվածությունը հնարավոր է լոկալ դրվագներով և, որ հարկ չկա կիրառել ծածկագրման բանալիների համատարած փոխանակման մոդել՝ բավարար է բանալիների փոխանակում հարևան, կապակցող հանգույցների միջև: Բացի այդ, բանալիների փոխանակումը իրականացվում է ցանցի

տեղադրման սկզբնական կարճաժամկետ հատվածում և բանալիների փոխանակման գործողության կայունությունը հարկ է ապահովել սոսկ այդ դրվագում: Հետագա ծածկագրումը դա մի սիմետրիկ սխեմա է, որը պետք է լինի ինչպես կայուն, այնպես էլ պարզագույն՝ էներգիայի մինիմալ սպառմանը համապատասխանելու իմաստով: Այս խնդրի լուծումը սովորաբար տարվում է հայտնի սխեմաների պարզեցված տարբերակների մշակման և կիրառման ճանապարհով: Աշխատանքը, որպես այլընտրանք, նպատակ ունի այս մասում սկսել հայտնի պարզ տեսական առնչություններից, դրանք կիրառելով ծածկագրման պարզեցված համակարգերի տեսքով:

Գապակցվածության և ծածկագրված կապակցվածության կողքին աշխատանքը դիտարկում է ցանցում հասանելի տվյալների ամբողջականության ապահովման խնդիրը, որը նպատակ ունի պարզաբանել անհրաժեշտ մինիմալ ռեսուրսը, որի դեպքում ցանցը դեռ ի վիճակի է հավաքել անհրաժեշտ ծավալի հասանելի ինֆորմացիան: Կիրառվող մոդելը ծրագրային ինքնավար ագենտների ճկուն մոդելն է, որի ուսումնասիրման մեխանիզմը կոմբինատոր և հավանականային մակարդակի գնահատականներն են:

Հետազոտության օբյեկտը

Հետազոտման հիմնական առարկան ցանցերն են (գրաֆներ)՝ տարբեր սահմանափակումներով և լրացուցիչ պայմաններով: Ցանցերը, որոնց գործունեությունը հիմնված է նման գրաֆների վրա կիրառվող տարբեր օպտիմիզացիոն ալգորիթմների բազմության վրա, կարիք ունեն գլոբալ նախագծման և օպտիմիզացիայի: Աշխատանքում ուսումնասիրվում են այդ ալգորիթմների այնպիսի դասեր, որոնք առայժմ չունեն բավարար արդյունավետ լուծումներ: Դրանք կապակցման և ծածկման պարզ խնդիրներ են՝ ծածկագրման, հավելյալ կապակցվածության վերացման և նպատակային ինֆորմացիայի հավաքման մինիմալ ռեսուրսների մասին տերմիններով:

Հետազոտության մեթոդները

Հետազոտման մեթոդները ընդգրկում են խմբերի տեսության տարրերը, մասնավորապես տեղադրությունների խմբերի և նրա ծնիչների ուժեղ բազմության հետ կապված հայտնի Սիմսի ալգորիթմի կիրառման տեսքով, ամբողջարժեք գծային ծրագրավորման մոտեցումները, այդ թվում փոփոխականների թուլացման տեխնիկան և պատահական կլորացման մեթոդը, ինչպես նաև կոմբինատոր և հավանականային մեթոդներ՝ կցման և արտաքսման մեթոդը, հավանականային բաշխումների մոտարկման տեխնիկան և Ստիրլինգի երկրորդ սեռի թվերի կիրառումը քանակական բնութագրերի հաշվարկման մեջ:

Արդյունքների նորությունը

Ինքնավար ագենտների և ինֆորմացիայի հավաքման մոդելը և նրա

գնահատումը[1] հիմնված լինելով ներդրված գումարների և փոփոխական գումարման տիրույթներով բանաձևերի վրա, վերջ ի վերջո հիմնվում էր փորձարարական կորերի կառուցման և ուսումնասիրման վրա: Աշխատանքում փուլ առ փուլ ստացված հանգեցումները, նախ, կցման արտաքսման մեթոդին, հետո առավել պարզեցված մի մոդելի և, վերջապես, Ստիրլինգի երկրորդ սեռի թվերով բանաձևերին էական առաջընթաց է այս խնդիրներում: Ինտերֆերենցիայի խնդրում նորությունը պարտադիր ծածկման և մինիմալ ծածկման տիրույթների սահմանազատումն է և այդ կտրվածքով ծածկույթների խնդրի բարելավված ալգորիթմների ստացումը: Տվյալների պահպանման մոդելում Սիմսի ալգորիթմի կիրառումը նոր մոտեցում է, որը հաշվի է առնում սենսորի էներգիայի մինիմալ սպառման անհրաժեշտությունը:

Ստացված արդյունքների կիրառական նշանակությունը

Աշխատանքում ուսումնասիրված ալգորիթմական խնդիրներն ունեն ընդգծված կիրառական բնույթ: Նրանք բոլորն ուղղված են անլար սենսորային ցանցերի նախագծման օպտիմիզացիային և նրանց գործունեության արդյունավետության բարձրացմանը: Ավելորդ չէ մեկ անգամ ևս նշել հենց իրենց՝ անլար սենսորային ցանկերի կարևոր կիրառական նշանակությունը: Սրանք նորագույն տեխնիկական համակարգեր են, որոնք կարող են ունենալ, բայց և կարող են չունենալ նախապես նախագծված կառուցվածք: Սենսորները կարող են տեղադրված լինեն կամրջային կառուցվածքի տարբեր մասերում, կամ կարող են տարածվել ինքնաթիռով հետախուզման որոշակի տարածքի վրա: Ցանցի աշխատանքը պահանջում է, որ այն կապակցված լինի կողերի միջոցով, որոնք կապում են փոխադարձաբար հասանելի հանգույցների զույգերը: Հարևան հանգույցների կապը պետք է ծածկագրված լինի բանալիների փոխանակման պարզ հաշվողական համակարգերի միջոցով և այլն: Ներկա աշխատանքը նպատակ ունի բարելավել այս հույժ կարևոր համակարգերի տեխնիկական բնութագրերը:

Առաջինը դա ծածկագրման բանալիների փոխանակման արդյունավետ համակարգն է պարզագույն, բայց կայուն ծածկագրման հետ մեկտեղ: Երկրորդը դա ինտերֆերենցիայի մինիմիզացման ալգորիթմներն են, որոնք ունեն գնահատված մոտարկման գործակից: Եվ վերջապես, ցանցում ինֆորմացիայի հավաքման մինիմալ ռեժիմի բնութագրումն է՝ կոմբինատոր հավանականային տերմիններով: Մշակված ալգորիթմների նախնական տեստավորումը իրականացվել է համապատասխան ծրագրային էքսպերիմենտի միջոցով:

Ներդրումներ

Աշխատանքների նախնական փուլը կապված է եղել INTAS 00-626 'Data Mining Algorithm Incubator' նախագծի հետ: Աշխատանքների հիմնական մասը իրականացվել

[1] Ira S. Moskowitz, Myong H. Kang, LiWu Chang, and Garth E. Longdon. Randomly roving agents for intrusion detection. Technical report, Naval research laboratory, Washington D.C., 2001.

են համագործակցությամբ AEOLUS Integrated Project FP6 IST-015964 'Algorithmic Principles for Building Efficient Overal Computers' նախագծի:

Պաշտպանությանը ներկայացվում են հետևյալ դրույթները

- Դիտարկվել է մինիմալ մասնակցությամբ բազմության ծածկույթ (ՄՄԲԾ) NP-լրիվ խնդրի ձևափոխված տարբերակը՝ մինիմալ մասնակի մասնակցությամբ բազմության մասնակի ծածկույթ (ՄՄՄԲՄԾ) խնդիրը և ապացուցվել է նրա NP-լրիվությունը:
- Ցույց է տրվել, որ ՄՄԲԾ խնդրի մոտավոր ալգորիթմը մոտարկում է ՄՄՄՄԲԾ խնդրի օպտիմալ լուծումը միևնույն գործակցով՝ ինչ-որ ՄՄԲԾ-ինը:
- Անլար ցանցերում ինտերֆերենսի մինիմիզացիայի խնդիրը (որը NP-դժվար է) ձևակերպվել է գրաֆների և բազմությունների համակարգերի լեզվով և նրա համար առաջարկվել մոտավոր իտերատիվ ալգորիթմ, որը աշխատանքի յուրաքանչյուր փուլում գործ է ունենում դիտարկված ՄՄՄԲՄԾ խնդրի հետ:
- Ստացվել է ցանցերում բավարար ինֆորմացիայի կորզման թափառող ագենտների քանակական բնութագիրը ներկայացնող բանաձև, որը գոյություն ունեցող բանաձևից անհամեմատ պարզ է:
- Բարելավվել է ցանցում բավարար ինֆորմացիայի կորզման թափառող ագենտների մոդելը և գտնվել է առնչություն դիտարկված երկու մոդելների քանակական բնութագրերի միջև:
- Գտնվել է պարզեցված մոդելի քանակական բնութագիրը ներկայացնող բանաձև, որը արտահայտվում է հայտնի Ստիրլինգի երկրորդ կարգի թվերի միջոցով:
- Մշակվել է տվյալների ծածկագրման սխեմա, որի բանալին տեղադրությունների խմբի ծնիչների ուժեղ բազմությունն է: Առաջարկված ծածկագրման սխեման կարելի է օգտագործել նաև որպես ինքնության հաստատման սխեմա:
- Մշակվել է անլար սենսորային ցանցերում բանալիների բաժանման նոր սխեմա:
- Կազմվել է շարժական հանգույցներով անլար սենսորային ցանցից տվյալների հավաքման ալգորիթմ, որի արդյունավետությունը ցույց է տրվել ալգորիթմի ծրագրային իրականացման միջոցով: Գրանցված արդյունքները գերազանցում են գոյություն ունեցեղ ալգորիթմի արդյունքներին:

Ստացված արդյունքների ապրոբացիան

Հիմնական դրույթներն ու արդյունքները զեկուցվել են CSIT-2003 և CSIT-2005 գիտաժողովներում http://www.csit.am, ԵՊՀ Ինֆորմատիկայի և կիրառական մաթեմատիկայի ֆակուլտետի ընդհանուր սեմինարում, ՀՀ ԳԱԱ ԻԱՊԻ սեմինարներում:

Հրատարակությունները

Ատենախոսության թեմայով հրատարակված են 6 գիտական հոդված, որոնցից 4-ը ընդգրկում են աշխատանքի հիմնական արդյունքները:

Աշխատանքի կառուցվածքը և ծավալը

Ատենախոսությունը բաղկացած է ներածությունից, 5 գլուխներից, եզրահանգումից և օգտագործված գրականության ցանկից: Աշխատանքի ծավալը 101 էջ է, որի մեջ ներառված են նաև նկարներ և օգտագործված գրականության ցանկը:

ԱՇԽԱՏԱՆՔԻ ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆԸ

Ներածության մեջ հիմնավորված են թեմայի հրատապությունն ու արդիականությունը, հետազոտության նպատակն ու հիմնական խնդիրները, ձևակերպված են ուսումնասիրման օբյեկտը և մեթոդները:

Առաջին գլխում բերվում են աշխատանքում օգտագործված հիմնական հասկացությունները, դիտարկվում են հարակից խնդիրների դասերի ուսումնասիրությունը և նրանց առնչությունը աշխատանքում դիտարկվող խնդիրների հետ:

Քանի որ աշխատանքում դիտարկվող որոշ խնդիրների լուծման համար օգտագործվում է ամբողջարժեք գծային ծրագրավորման խնդրի մոդելը, ապա առաջին գլխում, տիրույթի դասական շարադրանքների հիման վրա ներկայացվում են գծային և ամբողջարժեք ծրագրավորման խնդիրները, բերվում են հիմնական անհրաժեշտ սահմանումները, լուծման հայտնի մեթոդները, ինչպես նաև մոտավոր լուծումներ կառուցելու փոփոխականների թուլացման և փոփոխականների պատահական-հավանականային կլորացման մեթոդները:

Այս գլխում նշվում են նաև ուսումնասիրման մյուս տիրույթների հիմնական գաղափարները և արդյունքները: Դրանք են՝ հանրահաշվական դրույթներ կապված խմբի ծնիչ բազմության և Սիմսի ալգորիթմի հետ, հավանականությունների հաշվարկման և գնահատման մոտեցումներ, բազմության ենթաբազմությունների միջոցով ծածկման խնդիրներ և Ստիրլինգի երկրորդ կարգի թվի հաշվման մեթոդներ ու ասիմպտոտիկ գնահատականներ: Որոշ դեպքերում շարադրանքի համապատասխան մասը տեղափոխվել է համապատասխան գլուխ, որտեղ շարադրված է դրա հետ կապված կոնկրետ հետազոտությունը:

Երկրորդ գլխում կառուցվել է անլար ցանցերում ինտերֆերենսի մինիմիզացման մոտավոր ալգորիթմը: Խնդիրը ձևակերպվում է հետևյալ կերպ.

Խնդիր 2.1 (Ինտերֆերենսի մինիմիզացման խնդիր): Տրված է $G=(V,E)$ կապակցված գրաֆը: Գտնել G-ի ենթագրաֆ $H=(V,E')$ այնպես, որ H-ը լինի կապակցված և $\max\limits_{u\in V}|\{v/d(u,v)\le \max\limits_{(v,w)\in E'}\{d(v,w)\}\}|$ մեծությունը $H=(V,E')$ գրաֆի համար (ինտերֆերենսը) լինի մինիմալ հնարավորը, որտեղ $d(u,v)$-ն (u,v) կողի երկարությունն է:

Խնդրի լուծման համար դիտարկվել է մինիմալ մասնակի մասնակցությամբ բազմության մասնակի ծածկույթ (ՄՄՄԲՄԾ) խնդիրը, որը սերտորեն կապված է

մինիմալ մասնակցությամբ բազմության ծածկույթ (ՄՄԲԾ) խնդրի հետ: Վերջինս հետևյալն է.

Խնդիր 2.2 (ՄՄԲԾ): Տրված է՝ S բազմությունը և S-ի ենթաբազմությունների C հավաքածուն: Գտնել՝ $C' \subseteq C$, որ $S = \bigcup_{c \in C'} c$ և $\max_{s \in S} |\{c \in C' \setminus s \in c\}|$-ն մինիմալ է:

Թեորեմ 2.1 [18][2] Հայտնի է մինիմալ մասնակցությամբ բազմության ծածկույթ խնդիրը լուծող մոտավոր ալգորիթմ, որը բազմանդամային ժամանակում խնդրի օպտիմալ արժեքը մոտարկում է $O(\log(|S|)$ գործակցով:

Խնդիր 2.3 (ՄՄՄԲՄԾ): Տրված է՝ $S = S_1 \cup S_2$ բազմությունը, որտեղ $S_1 \cap S_2 = \varnothing$ և S-ի ենթաբազմությունների C հավաքածուն: Գտնել՝ $C'' \subseteq C$, որ $S_1 \subseteq \bigcup_{c \in C''} c$ և $\max_{s \in S_2} |\{c \in C'' \setminus s \in c\}|$-ը մինիմալ է:

Թեորեմ 2.2: Մինիմալ մասնակի մասնակցությամբ բազմության մասնակի ծածկույթ խնդրի ճանաչման տարբերակը *NP*-լրիվ է:

Թեորեմ 2.3: Մինիմալ մասնակի մասնակցությամբ բազմության մասնակի ծածկույթ խնդիրը լուծող պատահական կլորացումների մոտավոր ալգորիթմը խնդրի օպտիմալ արժեքը մոտարկում է բազմանդամային ժամանակում $O(\log(\max\{|S_1|, |S_2|\})$ գործակցով:

Ինտերֆերենսի մինիմիզացման խնդրի (Խնդիր 2.1) համար առաջին մոտավոր ալգորիթմը հաջողվել է ստանալ մեկ չափանի էվկլիդյան տարածությունում տրված ցանցերի համար: Այն տրված n գագաթանոց ցանցի մինիմալ ինտերֆերենսի կառուցումը մոտարկում է $\sqrt[4]{n}$ գործակցով [15]: Հետագայում ընդլայնելով այս արդյունքը ստացվել է ալգորիթմ, որը երկչափ մետրիկական տարածությունում տրված ցանցից կառուցում է ցանցի ինտերֆերենսի առավելագույնը $\sqrt{n}$ գործակցով մոտարկում, իսկ երկուսից մեծ, հաստատուն չափողականությամբ մետրիկական տարածությունում տրված ցանցի համար՝ առավելագույնը $\sqrt{n \log n}$ գործակցով մոտարկում [16]: Միայն այս արդյունքները ստանալուց հետո է հաջողվում ապացուցել ինտերֆերենսի մինիմիզացման խնդրի NP-դժվար լինելը: Ստացվել է նաև արդյունք ինտերֆերենսի մինիմիզացմամբ կապակցվածության ալգորիթմի մոտարկման դժվար լինելու մասին. խնդիրը հնարավոր չէ մոտարկել $O(\ln n)$ գործակցով, եթե միայն NP դասը թույլ գերբազմանդամային ժամանակի դաս է [17]: Այս պնդումն ապացուցվել է կապի արժեքի ֆունկցիայի տերմիններով, ինչը կարող է և մետրիկա չլինել: Անցնենք սույն աշխատանքի հիմնական արդյունքներից մեկին:

Ալգորիթմ 2.1: Ինտերֆերենսի մինիմիզացման մոտավոր ալգորիթմ:

[2] տես ատենախոսության գրականությունը

1. Ալգորիթմն աշխատանքը սկսում է $G_0 = (V, E_0)$ գրաֆից, որտեղ $E_0 = \varnothing$:
2. Ալգորիթմի l-րդ փուլում կառուցվում է նախորդ փուլում ստացված $G_{l-1} = (V, E_{l-1})$ գրաֆի կապակցված կոմպոնենտների $CP(G_{l-1}) = \{C_{l-1}^1, ..., C_{l-1}^{k_l}\}$ բազմությունը:
3. Կառուցվում է միջկոմպոնենտային կողերի բազմությունը $H_l = \{(u,v) / (u,v) \in E \setminus E_{l-1},\ \ u \in C_{l-1}^p, v \in C_{l-1}^q, p \neq q\}$
4. Կառուցվում է բազմությունների $\mathrm{T}_l = \{T_l(u,v) / (u,v) \in H_l\}$ հավաքածու, որտեղ $T_l(u,v) = \{C_{l-1}^p\} \cup \{C_{l-1}^q\} \cup \{w \in V / \min\{d(u,w), d(v,w)\} \le d(u,v))\}$ և թե $u \in C_{l-1}^p, v \in C_{l-1}^q, C_{l-1}^p, C_{l-1}^p \in CP(G_{l-1})$:
5. Կազմվում է $S_1 = CP(G_{l-1})$, $S_2 = V$, $C = T_l$ ՄՄՄԲՄԾ խնդիրը:
6. Մոտավոր ալգորիթմի օգնությամբ գտնվում է ՄՄՄԲՄԾ խնդրի $W_l \subseteq T_l$ լուծումը:
7. Կառուցվում են կողերի $F_l = \{(u,v) / T_l(u,v) \in W_l\}$ և $E_l = E_{l-1} \cup F_l$ բազմությունները:
8. Եթե $G_l = (V, E_l)$ գրաֆը կապակցված է, ապա ագորիթմն ավարտում է աշխատանքը, հակառակ դեպքում անցում է $l+1$-րդ փուլի կատարմանը:

Թեորեմ 2.4: Ալգորիթմի յուրաքանչյուր քայլում (փուլում) կապակցված կոմպոնենտների քանակը կրճատվում է առնվազն երկու անգամ՝ $|C(G_{l-1})| / |C(G_l)| \ge 2,\ \ l \ge 1$:

Հետևանք 2.1: Ալգորիթմը կատարում է առավելագույնը $\log_2 n$ փուլ:

Թեորեմ 2.5: $G^l = (V, F_l)$ գրաֆի համար $\max\limits_{u \in V} |\{v / d(u,v) \le \max\limits_{(v,w) \in F_l} \{d(v,w)\}\}| \le O(opt^2 \cdot \ln n)$, որտեղ opt-ն ինտերֆերենսի մինիմիզացման խնդրի օպտիմալ արժեքն է:

Թեորեմ 2.6: Ալգորիթմով կառուցված $G_l = (V, E_l)$ գրաֆի համար՝ $\max\limits_{u \in V} |\{v / d(u,v) \le \max\limits_{(v,w) \in E_l} \{d(v,w)\}\}| \le O(opt^2 \cdot \ln^2 n)$:

Երրորդ գլուխում դիտարկվել է ինքնավար ագենտների միջոցով ցանցից ինֆորմացիայի հավաքման երկու մոդել:

Խնդիր 3.1: Տրված է n տարր պարունակող S բազմությունը և S-ից պատահականորեն ընտրված $S_1, ..., S_k$ ենթաբազմությունները, որոնցից

յուրաքանչյուրը պարունակում է ճիշտ m տարր $|S_i|=m, i=1,\ldots,k$: Անհրաժեշտ է հաշվել հավանականությունը այն բանի, որ $S_1,\ldots,S_k$ ենթաբազմությունների միավորումը կպարունակի ճիշտ t տարր. $P_k(n,m,t)=\Pr\left(\left|\bigcup_{i=1}^{k} S_i\right|=t\right)$:

(3.1) խնդրի համար գոյություն ունի հետևյալ հարակից արդյունքը.

Թեորեմ 3.1 [3]:

$$P_k(n,m,t)=\binom{n}{m}^{-(k-1)}\sum_{m_2,m_3,\ldots,m_{k-1}=0}^{m}\left\{\binom{m}{m_2}\binom{n-m}{m-m_2}\binom{2m-m_2}{m_3}\binom{n-2m+m_2}{m-m_3}\cdots\right.$$

$$\cdots\binom{(k-2)m-m_2-\ldots-m_{k-2}}{m_{k-1}}\binom{n-(k-2)m+m_2+\ldots+m_{k-2}}{m-m_{k-1}}\cdot$$

$$\left.\cdot\binom{(k-1)m-m_2-\ldots-m_{k-1}}{km-t-m_2-\ldots-m_{k-1}}\binom{n-(k-1)m+m_2+\ldots+m_{k-1}}{t-(k-1)m+m_2+\ldots+m_{k-1}}\right\},\ k\geq 4$$

Աշխատանքում (3.1) խնդիրը բերվել է $k\times n$ չափանի այն բինար մատրիցների քանակի հաշվմանը, որոնք պարունակում են ճիշտ t ոչ զրոական սյուն և միաժամանակ յուրաքանչյուր տողում պարունակում են ճիշտ m հատ 1: Արդյունքում, հենվելով կոմբինատոր կցման-արտաքսման սկզբմունքի վրա, ստացվել է $P_k(n,m,t)$ հավանականության հաշվման անհամեմատ պարզ բանաձև.

Թեորեմ 3.2:

$$P_k(n,m,t)=\frac{C_n^t\cdot\sum_{i=0}^{t-m}(-1)^i C_t^i\cdot\left(C_{t-i}^m\right)^k}{\left(C_n^m\right)^k}:$$

Խնդիր 3.2: Տրված է n տարր պարունակող S բազմությունը և S-ի պատահական ընտրված $S_1,\ldots,S_k$ ենթաբազմությունները, որոնցից յուրաքանչյուրը պարունակում է ամենաշատը m տարր $|S_i|\leq m, i=1,\ldots,k$: Սա կանվանենք նաև 3.2 մոդել: Անհրաժեշտ է հաշվել հավանականությունը այն բանի, որ $S_1,\ldots,S_k$ ենթաբազմությունների միավորումը պարունակի ճիշտ t տարր.

$$P_k^*(n,m,t)=\Pr\left(\left|\bigcup_{i=1}^{k} S_i\right|=t\right):$$

Թեորեմ 3.3: Եթե $kC_m^2/n \underset{k,n,m\to\infty}{\longrightarrow} 0$, ապա

$P_k(n,m,t)\cdot P \le P_k^*(n,m,t)$, որտեղ $P \to 1$:

P հավանականությունը 3.2 մոդելի ներքին պարամետր է:

Թեորեմ 3.1:

$$P_k^*(n,m,t) = \frac{C_n^t \cdot t! S(mk,t)}{n^{mk}}:$$

Որտեղ $S(N,K) = \frac{1}{K!}\sum_{j=0}^{K}(-1)^j C_K^j (K-j)^N$ -ն Ստիրլինգի երկրորդ կարգի թիվն է:

Նրա համար գոյություն ունեն ասիմպտոտիկ տարբեր գնահատականներ և ռեկուրենտ հաշվման բանաձևեր, որոնք կարող են օգտագործվել նախագծման համար:

<u>Չորրորդ գլխում</u> դիտարկվել են անլար սենսորային ցանցերի ապահովության խնդիրներ: Մասնավորապես մշակվել են տվյալների ծածկագրման և բանալիների բաժանման սխեմաներ:

Տվյալների ծածկագրման սխեման որպես բանալի օգտագործում է տեղադրությունների խմբի ծնիչների ուժեղ բազմությունը, որը տրվում է աղյուսակի տեսքով: Մուտքային տվյալները բաժանվում են N երկարության (N բայթ պարունակող) բլոկերի և յուրաքանչյուր բլոկ ծածկագրվում է առանձին: N երկարության բլոկեր ծածկագրելու համար օգտագործվում է $2N+1$ տարրանոց տեղադրությունների խմբի ծնիչների ուժեղ որևէ բազմություն: Բլոկի ծածկագրման ժամանակ նրա յուրաքանչյուր բայթի համար ծնիչների ուժեղ բազմությունից (աղյուսակից) ֆիքսվում են երկու տեղադրություն: Ինչի արդյունքում ողջ բլոկի համար ֆիքսվում են $2N$ տեղադրություն, որոնց արտադրյալն էլ հանդիսանում է բլոկի ծածկագրման արդյունքը: Այսպիսով, տվյալների N երկարության բլոկի ծածկագրումից ստացվում է $2N+1$ տարրանոց մեկ տեղադրություն:

Բլոկի վերականգնման ժամանակ տրված $2N+1$ տարրանոց տեղադրությունից վերականգնվում է ինֆորմացիայի N բայթ:

Սխեմայի աշխատանքը բավականին պարզ է, չի պահանջում բարդ հաշվարկներ, ինչը հնարավոր է դարձնում նրա օգտագործումը անլար սենսորային ցանցերում:

Մշակված բանալիների բաժանման սխեման նույնպես պարզ է և, հաշվի առնելով անլար սենսորային ցանցերի բոլոր առանձնահատկությունները, ապահովում է բանալիների բաժանման ապահով սխեմա:

<u>Չինգերորդ գլխում</u> դիտարկվել է շարժական հանգույցներով անլար սենսորային ցանցերում ինֆորմացիայի հավաքման խնդիրը: Դիտարկված մոդելում ցանցի հանգույցները գտնվում են քաոսային շարժման մեջ և յուրաքանչյուր հանգույց ժամանակ առ ժամանակ գրանցում է ինչ-որ տվյալ: Խնդիրը գրանցված տվյալները հավաքման կայանին հասցնելն է:

Մշակված ալգորիթմը աշխատում է ցանցում գրանցված յուրաքանչյուր տվյալ ցրել ցանցի հանգույցների այնպիսի բազմության վրա, որ հավանականությունը, որ տվյալը կրող հանգույցներից գոնե մեկը այն կհասցնի կայանին քիչ չէ, քան նախօրոք որոշված 1-ին մոտ թիվը:

Ալգորիթմի արդյունավետությունը ցույց է տրվել ծրագրային փորձարկումների միջոցով: Այն ապահովում է ցանցում գրանցված տվյալների կայան հասցման բարձր տոկոս՝ *97-99%*, մինչդեռ գոյություն ունեցող ալգորիթմները ապահովում էին տվյալների *70-75%*- առաքում:

Հիմնական արդյունքներն ու եզրահանգումները

Դիտարկվել է մինիմալ մասնակի մասնակցությամբ բազմության մասնակի ծածկույթ (ՄՄՄԲՄԾ) խնդիրը և ապացուցվել է նրա NP-լրիվությունը: Կառուցվել է այս խնդրի լուծման բազմանդամային բարդությամբ մոտարկող ալգորիթմ և գնահատվել է մոտարկման գործակիցը:

Անլար ցանցերում ինտերֆերենցիայի մինիմիզացիայի խնդիրը ձևակերպվել է բազմությունների ընտանիքի լեզվով և նրա լուծման համար առաջարկվել մոտավոր իտերատիվ ալգորիթմ, որն աշխատանքի յուրաքանչյուր փուլում գործ է ունենում դիտարկված ՄՄՄԲՄԾ խնդրի հետ:

Ստացվել է ցանցերում թափառող ագենտների քանակական բնութագիրը ներկայացնող բանաձև, որը գոյություն ունեցող բանաձևից անհամեմատ պարզ է:

Բարելավվել է ցանցում բավարար ինֆորմացիայի կորզման թափառող ագենտների մոդելը և գտնվել է առնչություն դիտարկված երկու մոդելների քանակական բնութագրերի միջև:

Գտնվել է դիտարկված համարժեք մոդելի քանակական բնութագիրը ներկայացնող բանաձև, որը արտահայտվում է հայտնի Ստիրլինգի երկրորդ կարգի թվի միջոցով:

Մշակվել է տվյալների ծածկագրման սխեմա, որի բանալին տեղադրությունների խմբի ծնիչների ուժեղ բազմությունն է: Առաջարկված ծածկագրման սխեման կարելի է օգտագործել նաև որպես ինքնության հաստատման սխեմա: Մշակվել է անլար սենսորային ցանցերում բանալիների բաժանման սխեմա:

Ատենախոսության թեմայի շրջանակներում հրատարակված աշխատությունների ցանկ

1. H. Aslanyan, “Approximation Algorithm for Wireless Network Interference Minimization”, Mathematical Problems of Computer Science, Transactions of IPIA NAS RA, vol33, 2010, ISSN 0131-4645, pp. 162-171
2. A. Alexanyan, H. Aslanyan and A. Soghoyan, “Data Encryption, Authentication and Key Predistribution Schemes for Wireless Sensor Networks”, Mathematical Problems of Computer Science, Transactions of IPIA NAS RA, vol33, 2010, ISSN 0131-4645, pp. 127-134.
3. H. Aslanyan, “Quantitative Framework of Randomly Roving Agents”, Գիտական տեղեկագիր, ԵՊՀ, h. 2, 2010, էջ. 29-34.
4. H. Aslanyan, “Greedy Set Cover Estimations”, Computer Science and Information Technologies conference, Yerevan, September 22-26, 2003, pp. 143-144.

Резюме

Асланян Акоп Левонович

Исследование алгоритмических проблем математических моделей беспроводных сенсорных сетей

Работа посвящена исследованию моделей беспроводных сенсорных сетей. Этот новый тип сетей имеет важные приложения в критических системах мониторинга и управления. Сенсоры являются автономными звеньями сетей и обладают измерительными, вычислительными и коммуникационными функциями при значительно ограниченом обьеме питания. Сенсоры, случайным образом распределенные на территории, снабжены протоколами, которые упавляют процессом конфигурации пар связанных вершин в сети, снабжают вершины секретными ключами коммуникации и следят за тем, чтобы снизить ненужное проникновение радиоволн коммуникации (интерференция) при минимальной используемой энергии.

Рассматриваются здачи связности и покрытия целевой области, которые в математической формулировке сводятся к задачам поиска связного подграфа с некоторыми ограничениями, задачам минимального покрытия множества подмножествами и построении легких криптомоделей, например на основе простых алгебраических алгоритмов.

Одна группа основных результатов посвящена минимизации интерференции, для которой построен алгоритм, основанный на итеративном обращении к задаче частичного покрытия с частичным участием. Доказывается NP полната этой задачи. Проводится анализ построенного алгоритма доказывая, что число шагов является логарифмом от числа вершин графа и, что полученная интерференция не превосходит квадрата минимума и логарифма числа вершин.

Из группы задач покрытия целевой области рассматривается модель, где информацию собирают автономные агенты, равномерно блуждающие по сети. Рассмотрен ряд таких моделей, доказывается их эквивалентность и выводятся формулы вероятностей, эквивалентные комбинаторным числам Стирлинг второго рода.

Рассматривается также задача защиты коммуникации в сети. Строится “легкая” схема симметичной криптографии основанная на сильных порождающих множествах.

Основным выводом является то, что применение комбинаторной, алгебраической и вероятностной теорий позволяет построить эффективные алгоритмы проектирования оптимальных беспроводных сетей, решив основные задачи связности сети и покрытия целевой области при учете требования минимизации используемой энергии.

Hakob L. Aslanyan

Studies on Algorithmic Problems of
Wireless Sensor Network Mathematical Models