UDK 004.415

# TARMOQ STEGANOGRAFIYASI USULLARINING TAHLILI

*Ganiyev A.A.* [1], *Allanov O.M.*[1], *Mavlonov O.N.*[1]

[1] Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, Toshkent, O‘zbekiston

abduhalilganiev58@gmail.com, orif_allanov@mail.ru, mavlonov8686@gmail.com

**Annotatsiya**. *Ushbu maqolada OSI modelining transport sathida ishlovchi TCP/IP protokoliga maxfiy xabarlarni yashirish usullari haqida ma’lumotlar berilgan. Shuningdek, tarmoq steganografiyasi usullari imkoniyatlari bo‘yicha tahlil qilingan. Tahlil natijalariga ko‘ra axborot yashirish imkoniyati yuqori va ruxsatsiz aniqlanish ko‘rsatkichi past bo‘lgan tarmoq steganografiyasi usullari aniqlangan.*

**Kalit so‘zlar:** *Tarmoq steganografiyasi, IP, VOIP, LACK, RSTEG, SCTP, HICCUPS, TCP/IP, HTTP.*

## I. KIRISH

Bugungi raqamli texnologiyalar rivojlangan dunyoda steganografiya turli maqsadlarga ega bo‘lishi mumkin – xavfsiz va xavfli hattoki jinoiy. Xususan, steganografiyaning tinchlik yo‘lidagi eng mashhur foydalanishligi mumkin bo‘lgan jihati bu mualliflik huquqini himoya qilishdir, steganografiya usullari bilan kiritilgan “suv belgisi” dan foydalanganda siz ma’lumotlar mualifini aniqlashingiz mumkin.

Steganografiya raqamli kutubxonalar va bulutli omborlardagi materiallarni raqamli belgilash uchun ishlatilishi mumkin. Steganografik biriktirma hatto ma’lum darajada elektron imzo o‘rnini bosishi mumkin, chunki u uzatilgan ma’lumotning yaxlitligini isbotlash imkonini beradi. Boshqa tomondan, steganografiya yordamida tajovuzkor tarmoqda o‘rnatilgan barcha filtrlarni chetlab o‘tib, maxfiy ma’lumotlarni ochiq aloqa kanallari orqali uzatishi mumkin. Shuning uchun bugungu kunda steganografiya va stegoanaliz usullari ayniqsa diqqat bilan o‘rganishni talab etadi [1].

Tarmoq steganografiyasi katta hajmdagi ma’lumotlarni real vaqtda yashirib uzatish imkonini beradi. Tarmoq steganografiyasi paketini modifikatsiyalash, paketlarni uzatilayotganda strukturasini modifikatsiyalash va gibrid(aralash) usullarga bo‘linadi.

## II. ASOSIY QISM

Tarmoq steganografiyasining paketlar modifikatsiyasilash usullarining asosiy g‘oyasi steganogramma qo‘shish uchun sarlavha maydonlarini o‘zgartirishga asoslanadi. Buni amalga oshirishda maydonlardagi ba’zi ortiqcha foydalanilmaydigan jaylardan, ya’ni paketlarni uzatishda ahamiyatga ega bo‘lmagan maydonlardan foydalaniladi. Eng ko‘p ishlatiladigan sarlavha maydonlari IP va TCP protokollari tarkibida mavjud.

IP sarlavhalari maydonlarini o‘zgartirishga asoslangan bunday usulning namunasi 1-rasmda ko‘rsatilgan.


**1-rasm**. IP sarlavhasi maydonini o‘zgartirish usuli

1-rasmda ma’lumotlarni steganografik yashirish uchun ishlatilishi mumkin bo‘lgan maydonlar(osti chizilgan) holatda ko‘rsatilgan [2].

IP-paket Identifikatsiya maydonining qiymati jo‘natuvchi tomonida hosil bo‘ladi. Bu raqam paket yaratilganda hosil bo‘ladigan tasodifiy sonni o‘z ichiga oladi. Identifikatsiya maydoni faqat fragmentlash bajarilganda ishlatiladi. Shuning uchun, ushbu usuldan foydalanishda tarmoqdagi uzatiladigan paketlarning maksimal uzatish birligi (MTU-The maximum transmission unit) qiymatini bilish kerak va uzatish paytida paket fragmentlanmasligi (parchalanmasligi) uchun uning hajmi belilangan maksimal qiymatdan oshib ketmasligi kerak. Paketni qismlarga ajratish zarurati bo‘lmasa, Don't Fragment (DF) bayrog‘ini o‘rnatish uchun javob beradigan ikkinchi bitda "Bayroqlar" maydonida ma’lum bir ortiqcha maydon bo‘sh bo‘ladi. Yuboruvchi paketni qismlarga ajratishni istamasligini ko‘rsatish uchun bayroqni belgilashi mumkin. Agar steganogramma paketi kattaligi tufayli bo‘linmasa, ma’lumotni DoNotFragmentBit bayroq maydonida yashirish mumkin. Ushbu usuldan foydalanish xar bir paket tarkibida 1 bit ma’lumotni yashirish imkonini beradi.

Ushbu usulning afzalligi ma’lumotni jo‘natuvchidan qabul qiluvchiga o‘zgarmagan holda uzatishdir. Lekin u yuborilgan ma’lumotlar hajmini ham cheklaydi. Ushbu usulga asoslangan steganografiyani amalga oshirish oson, yaxshi o‘tkazuvchanlikka ega. Chunki kiritilgan o‘zgarishlar bilan ko‘plab IP-paketlarni yuborishi mumkin va paketning funksionalligi buzilmaydigan maydonlardan foydalanish tufayli narxi arzon. Agar marshrut tanlansa, uzatish davomida paket yo‘q parchalanib ketgan bo‘lsa bu usul juda keng qo‘llanilishi mumkin. Kamchiliklar qatorida shuni ta’kidlash kerakki, uzatilgan ma’lumotlar aniq matnda mavjud va kuzatuvchi tomonidan osongina o‘qilishi mumkin (garchi himoyani qo‘shimcha ravishda kriptografiya yordamida kuchaytirish mumkin).

Tarmoq paketlarini o‘zgartirishning yana bir usuli Transcoding steganography **(TranSteg) bo‘lib**, IP orqali audio (VoIP yoki IP telefoniya) xabarlar paketining foydali yuk maydonini o‘zgartirishga asoslanadi. TranSteg usulidan shuningdek, ochiq ma’lumotlarni siqish imkoniyati mavjud bo‘lgan boshqa ilovalar yoki xizmatlarda masalan, video xabarlar oqimlarida foydalanish mumkin.

Steganografiyadagi odatiy yondashuvida uzatiladigan ma’lumotlarning hajmini kamaytirish uchun ma’lumotlar siqiladi, chunki yashirin aloqa kanalidan foydalanganda o‘tkazish qobiliyati cheklangan bo‘ladi.

TranSteg usulida ham steganogrammani yuborishga joy ochish uchun ma’lumotlarni siqishdan foydalanadi. Bunda ovozli ma’lumotlarni yuqori bit tezligidan pastroq bit tezligiga, agar imkoni bo‘lsa ovoz sifatini minimal yo‘qotgan holda transkodlash (yo‘qotilgan siqish) amalga oshiriladi. Ovozli ma’lumotlar siqilgandan so‘ng steganogrammalar paketli yuklash sohasining bo‘sh joylarga kiritiladi. Umuman olganda, ushbu usul paketni kechiktirishdagi yeng kichik 32 kb/s lik farq bilan steganografik o‘tkazuvchanlikni olish imkonini beradi.

Polsha olimlarining tajribalari shuni ko‘rsatdiki, TranSteg yordamida VoIP paketini uzatishdagi kechikish steganogrammasiz paketdan farqli ravishda (1ms) bir millisekundga ortadi [3].

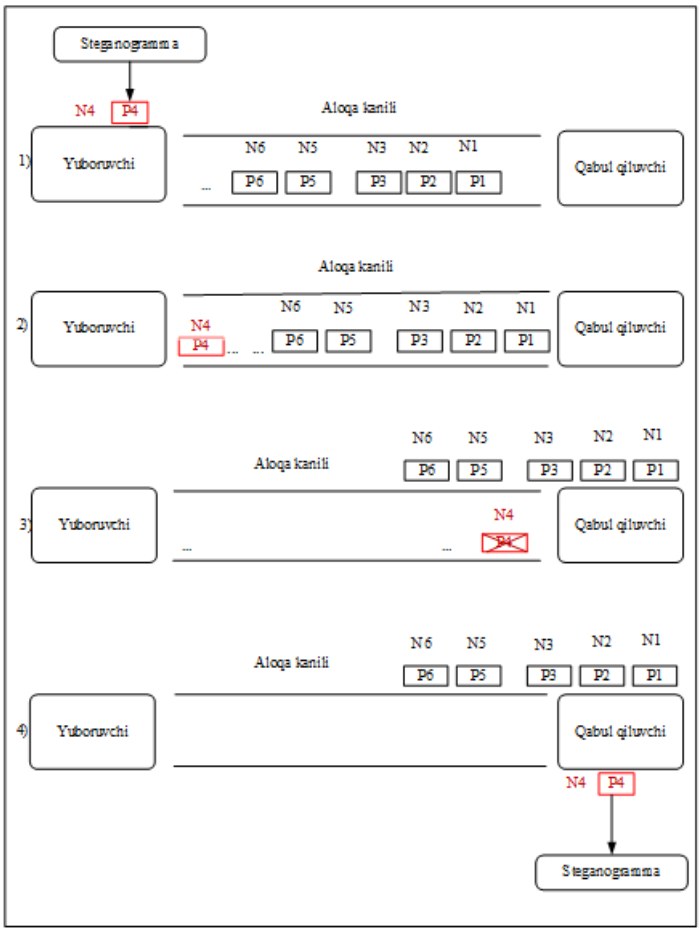
TranSteg usulida aniqlashning murakkabligi to‘g‘ridan-to‘g‘ri ssenariyni tanlashga va tashqi kuzatuvchining shartlariga bog‘liq. Kamchiliklaridan yana shuni aytish mumkinki, bu usulni amalga oshirish juda qiyin. Sababi ovozli aloqada qanday kodeklardan foydalanilishini bilish, nutq sifatini yo‘qotishda yeng kam farqli kodeklarni tanlash shu bilan birga steganogrammani joylashtirish uchun ko‘proq joy ajratish yo‘llarini bilish kerak. Bundan tashqari uzatiladigan nutq ma’lumotlari siqilganda sifati yo‘qolishini hisobga olish kerak.

VoIP protokoli imkoniyatlaridan foydalanib xabarni yashirin uzatish usullaridan yana biri *LACK* (*Lost Audio Packets Steganography*) hisoblanadi.

IP-telefoniya orqali aloqa ikki qismdan signal (xizmat) va suhbatdan iborat bo‘ladi. Ikkala qismda ham ma’lumotlar har ikki yo‘nalishda ham uzatiladi. Signal uzatish uchun *SIP* (*Session Initiation Protocol*) va suhbatni amalga oshirish uchun *RTP* (*Real-time Transport Protocol*) protokollaridan foydalaniladi. Bu shuni anglatadiki, qo‘ng‘iroqning signalizatsiya bosqichida foydalanuvchi agentlar SIP xabarlarini almashadilar. Odatda, SIP xabarlari SIP serverlari orqali o‘tadi va foydalanuvchilarga bir-birini qidirish va topish imkonini beradi. Ulanish o‘rnatilgandan so‘ng, suhbat bosqichi boshlanadi va bu yerda RTP audio oqimi qo‘ng‘iroq qiluvchilar o‘rtasida har ikki yo‘nalishda ovozli xabar almashishni ta’minlaydi. Ovozli xabarlaga maxfiy ma’lumotlarni samarali yashirish usullaridan biri LACK hisoblanadi. *LACK* usulining ishlash printsipiga ko‘ra transmitter ovozli oqim paketlaridan birini tanlaydi va uning foydali yukini maxfiy xabarning bitlari bilan almashtiriladi. Keyin tanlangan paket ataylab kechiktiriladi. Har safar haddan tashqari kechiktirilgan paket steganografik protsedura bilan tanish bo‘lmagan qabul qiluvchiga yetib borganida, u yo‘q qilinadi. Biroq, agar qabul qiluvchi yashirin ulanish haqida bilsa u qabul qilingan RTP paketlarini o‘chirish o‘rniga yashirin ularni qabul qiladi va yashirib uzatilgan ma’lumotga ega bo‘ladi. Qasddan yo‘qotishlarni keltirib chiqarganda aloqa sifati yomonlashadi. Bu esa oddiy foydalanuvchilarda ham, tinglovchi kuzatuvchilarda ham shubha uyg‘otishi mumkin. LACK usulining stegoanalizining taqdim etilgan natijalariga asoslanib, ushbu usul o‘rtacha aniqlash murakkabligiga ega degan xulosaga kelish mumkin. Bu usuldan foydalanish juda murakkab va ba’zi operatsion tizimlarda amalga oshirilmasligi mumkin [8].

Quyidagi 2-rasmda LACK usuli funksiyasi batafsil tavsiflangan. Transmitterda RTP oqimidan bitta paket tanlanadi va uning audio yuki (ovozli ma’lumot) steganogrammaning bitlari birinchi qadamdagidek o‘zgartiriladi. Tanlangan tovush paketi uzatilgunga

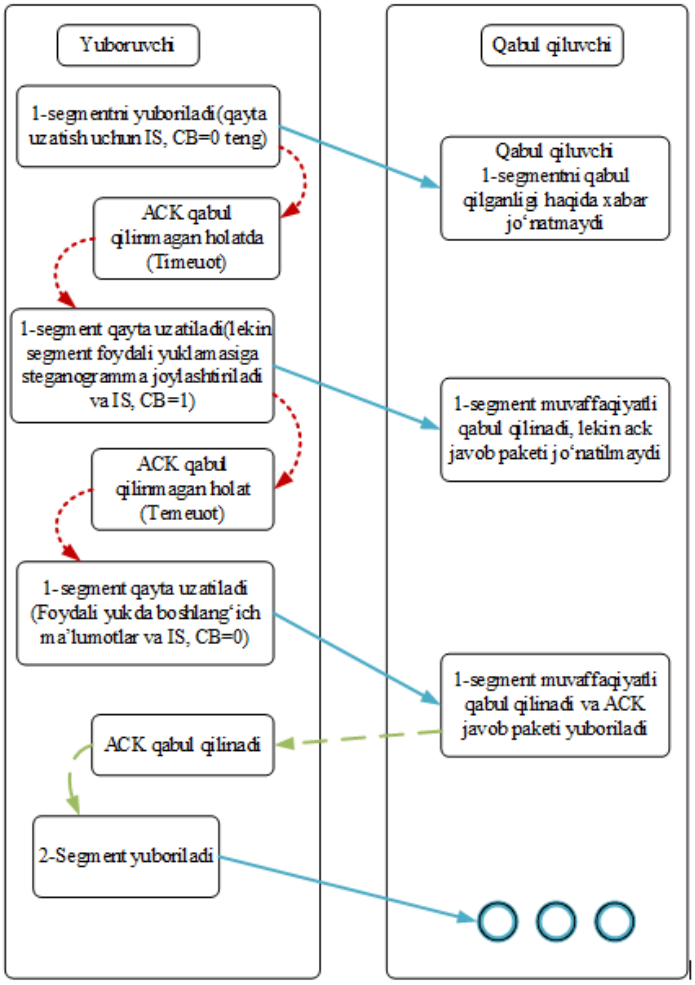
qadar ikkinchi qadamda ko‘rsatilganidek ataylab kechiktiriladi. Agar kechikish muddati oshib ketgan paket steganografik protseduradan bexabar bo‘lgan qabul qiluvchiga yetib borsa, u uchunchi qadamda keltirilganidek uni o‘chiradi. Chunki yashirin ma’lumotlar qabul qiluvchilar uchun "ko‘rinmas" hisoblanadi. Biroq, agar qabul qiluvchi yashirin xabar kelishini bilsa, u paketni o‘chirish o‘rniga to‘rtinchi qadamda keltirilganidek yashirin ("foydali yuk")ni qabul qiladi. Qasddan kechiktirilgan paketlarning yashirin foydali yuki protseduradan xabardor bo‘lgan qabul qiluvchilarga maxfiy ma’lumotlarni yetkazish uchun ishlatilganligi sababli, qo‘shimcha paketlar yaratilmaydi [6].




**2-rasm**. LACK usulining ishlash prinsipi

LACK usuli haqida keltirilgan ma’lumotlardan ko‘rish mumkinki uzatlayotgan ovozli paketga maxfiy ma’lumotni yuklash va uni oddiy foydalanuvchiga bildirmaslik maqsadida ataylab kechiktiriladi. Bunda uzatilayotgan paketga to‘liq maxfiy ma’lumotni yuklash imkoniyati LACK usulining maxfiy ma’lumotlarni tarmoqda uzatilishining samaradorligini ta’minlaydi. Sababi uzatilayotgan paketga to‘liq maxfiy ma’lumotni yashirib uzatish imkoniyati mavjud [11].

Paketlarni qayta uzatish mexanizmiga asoslangan steganografik usullardan yana biri *RSTEG* (*Retransmission Steganography*) hisoblanadi. Ushbu usulni quyidagi 3-rasmda keltirilganidek ifodalash mumkin.




**3-rasm**. RSTEG usulining ishlash prinsipi

Bu yerda IS(Identifying Sequence) - ketma-ketlikni aniqlash va CB uzatilayotgan paketlar tartib raqami hisoblanadi.

RSTEG usulida dastlab ma’lumot yuboruvchi paketni jo‘natadi, lekin qabul qiluvchi tasdiq(ACK) paketi bilan javob bermaydi. Natijada paketlarni qayta jo‘natish mexanizmi ishga tushadi. Qayta jo‘natish paytida paket ichiga steganogramma joylashtirib uzatiladi. Qabul qiluvchi ichida steganogramma mavjud paketni qabul qiladi, lekin yana tasdiq(ACK) paketini yuboruvchiga jo‘natmaydi. Yana paketlarni qayta jo‘natish mexanizmi ishga tushganda asl paket qo‘shimchalarsiz uzatiladi va qabul qiluvchi ma’lumotni olgandan so‘ng tasdiq(ACK) paketini yuboruvchiga jo‘natadi. Natijada tasdiq(ACK) paketini yuborilmasdan qayta uzatilganda ma’lumotlar steganografik yashirib uzatiladi.

RSTEG usulining unumdorligi paket yuki hajmi va segmentlar hosil bo‘lish chastotasiga bog‘liq hisoblanadi.

Steganografiyaning haqiqiy usullaridan hech biri mukammal emas. Qanday usul bo‘lishidan qat’i nazar, yashirin ma’lumotni aniqlash mumkin. Ma’lumotlar oqimiga qancha yashirin ma’lumot kiritilsa, uni stegoanaliz qilish usullari bilan aniqlash ehtimoli shunchalik yuqori bo‘ladi. Bundan tashqari, yashirin ma’lumotlarni yuborish uchun qancha paketlar ishlatilsa, aniqlash chastotasi ortadi. Yashirin aloqa kanalini aniqlashni sezilarli darajada osonlashtiradigan vositalar relayli paketlar hisoblanadi. Bundan tashqari, tarmoqdagi paketlarning yo‘qolishi nazorat qilinadi va

RSTEG qonuniy trafikdan foydalanadi. Bu esa umumiy yo‘qotishni oshiradi. Tarmoqdagi umumiy paket yo‘qotilishi normal bo‘lishini va RSTEG ulushi bir xil tarmoqdagi boshqa ulanishlar bilan solishtirganda juda yuqori bo‘lmasligini ta’minlash uchun steganografiya qatlamini nazorat qilish va dinamik moslashtirish kerak [5].

RSTEG gibrid usul hisoblanadi. Shuning uchun uning steganografik o‘tkazuvchanligi taxminan paketlarni o‘zgartirish usullarining o‘tkazuvchanligiga teng va shu bilan birga paketlarni qayta tartiblash usullaridan yuqori. Aniqlash va o‘tkazishning murakkabligi to‘g‘ridan-to‘g‘ri usulni amalga oshirish uchun ishlatiladigan mexanizmga bog‘liq. RTO(Recovery Time Objective) asosidagi RSTEG usuli aniqlanishning yuqori murakkabligi va past o‘tkazish qobiliyati bilan tavsiflanadi. Xuddi shu usulga asoslangan SACK (Selective acknowledgment RSTEG uchun maksimal o‘tkazish qobiliyatiga ega, ammo uni aniqlash oson [9].

RSTEG usuli TCP/IP protoklida ishlatish uchun juda mos keladi va o‘rtacha darajadagi uzatish bilan bu usul kuzatuvchida shubha uyg‘otmaydi. Ammo bu usulni amalga oshirish juda qiyin, ayniqsa uning oddiy foydalanuvchilarning paketlarini ushlash va tuzatishga asoslangan algoritmlari. O‘tkazilayotgan paketlar chastotasining keskin oshishi yoki uzatishda g‘ayrioddiy kechikishlarning paydo bo‘lishi tufayli steganogrammalar tashqi kuzatuvchida shubha tug‘dirishi mumkin [8].

Tarmoq steganografiya usullaridan biri SCTP (Stream control transport protocol) protokoliga asoslangan usul hisoblanadi. SCTP paketlarni boshqarish transport protokoli bo‘lib u BSD, Linux, HP-UX va SunSolaris kabi operatsion tizimlarda idhlatiladi. Shuningdek, Cisco IOS operatsion tizimining tarmoq qurilmalarini qo‘llab-quvvatlaydi va Windows tizimida ham ishlatilishi mumkin.

SCTP steganografiyasi ushbu protokolning ko‘p tarmoqli va bir nechta interfeyslardan foydalanish (multi-homing) kabi yangi xususiyatlaridan foydalanadi. Ba’zi yangi tahdidlar va taklif qilingan qarshi choralar SCTP dagi hujumlarni tavsiflovchi RFC 5062 ga qo‘shimcha sifatida ishlatilishi mumkin.

SCTP steganografiya usullarini uch guruhga ajratish mumkin [10]:

1. SCTP paketlari tarkibini o‘zgartirish usullari;
2. SCTP paketlarini uzatish ketma-ketligi o‘zgartiriladigan usullar;
3. Paketlarning mazmuniga ham, uzatish vaqtida ularning tartibiga ham ta’sir qiluvchi(gibrid) usullar.

SCTP paketlari tarkibini o‘zgartirish usullari har bir STCP paketi qismlardan iborat bo‘lishiga asoslanadi va bu qismlarning har biri o‘zgaruvchan parametrlarni o‘z ichiga oladi. Amalga oshirishdan qat’i nazar, yo‘naltirilgan bloklar uchun ishlatiladigan NIC manzillarining statistik tahlili yashirin havolalarni aniqlashga yordam beradi. Ushbu steganografiya usulini qo‘llash imkoniyatini yo‘q qilish qayta yuborilgan blokda joylashgan tasodifiy tanlangan paketdagi jo‘natuvchi va qabul qiluvchining manzilini o‘zgartirish orqali amalga oshirilishi mumkin.

SCTP protokoliga asoslangan gibrid usulning mohiyati oqimdagi paketlarni qayta jo‘natmasdan qasddan o‘tkazib yuborishni tashkil qilish imkonini beruvchi ma’lum protokol mexanizmlaridan foydalanishdir. Gibrid usul yordamida paket modifikatsiya qilinadi,

bu paketga steganogramma qo‘shiladi va u qayta yuboriladi.

Tarmoq steganografiyasi usullaridan foydalanib yaratilgan va bugungi kunda foydalaniladigan kompleks tizimlar ham mavjud. Ulardan biri *HICCUPS* (*Hidden Communication system for Corrupted Networks*) bo‘lib, umumiy ma’lumotlarni uzatish vositasi (umumiy muhit) bo‘lgan tarmoqlar uchun o‘tkazish qobiliyatini taqsimlash steganografik tizimi. HICCUPS ma’lumotlarning buzilishining tabiiy sabablari bo‘lgan uzatish muhitining kamchiliklari shovqinlardan foydalanadi [14].

Media tarmoqlari, ayniqsa LAN larda mediaga kirishning turli mexanizmlaridan foydalanadi. Masalan CSMA (Carrier Sense Multiple Access), CSMA/CD (CSMA with Collision Detection), CSMA/CA (CSMA with Collision Avoidance) va Token Bus tarmoq texnologiyalarida**.** Barcha qayd yetilgan mexanizmlarning umumiy xususiyati bu tashuvchida uzatiladigan ma’lumotlar oqimlarini "tinglash" qobiliyatidir. Kadrlarni ushlab turishning zaruriy sharti jismoniy muhitga ruxsatsiz kirishdir.

Atrof-muhitda uzatiladigan barcha ma’lumotlar oqimlarida "tinglash" va tuzatish kodlarining noto‘g‘ri qiymatlari bilan buzilgan kadrlarni yuborish qobiliyati HICCUPS uchun yeng muhim tarmoq funksiyalaridan hisoblanadi. Jumladan, simsiz tarmoqlarda "sun’iy" buzilgan oqimlarni kiritish imkoniyatini yaratadigan o‘zgaruvchan bit xato tezligini (BER) radio uzatishidan foydalanadi.

Umuman olganda, HICCUPS ning yangiligi quyidagilardan iborat:

1. Steganografik tizimni yaratish uchun kriptografik mexanizmlar bilan jihozlangan xavfsiz telekommunikatsiya tarmog‘idan foydalanish;
2. Buzilgan oqimlar asosida steganografik maqsadlar uchun tarmoq kengligi taqsimoti bilan yangi qoidalar yaratish.

Taklif etilayotgan tizim quyidagi xususiyatlarga ega bo‘lgan muhitda amalga oshirish uchun mo‘ljallangan:

1. Kadrlarni ushlab turish imkoniyati bilan birgalikda ma’lumotlarni uzatish vositasi;
2. Shifrlash algoritmini ishga tushirishning taniqli usuli, masalan, ishga tushirish vektorlari bilan;
3. Shifrlangan oqimlar uchun yaxlitlik mexanizmlari, masalan, bir tomonlama xesh funksiyasi, CRC(Cyclic redundancy check) kodlar.

Ta’riflangan xususiyatlarga ega tarmoqda MAC oqimida uchta yashirin ma’lumotlar kanalini yaratish mumkin:

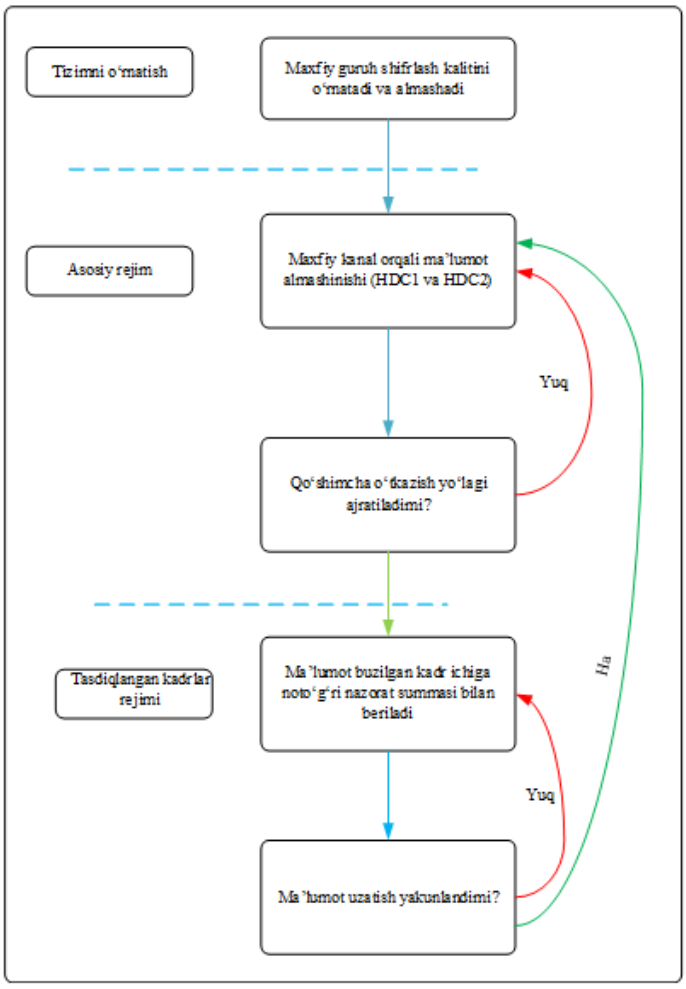
- HDC1 shifrni ishga tushirish vektorlariga asoslangan kanal;
- HDC2 MAC ga asoslangan kanal;
- HDC3 yaxlitlik mexanizmi qiymatlariga asoslangan kanal (masalan, oqim nazorat summasi).

Xavfsizlik ta’minlanmagan tarmoqlarda faqat HDC2 va HDC3 ishlatiladi. Ko‘pgina simli tarmoqlar MAC darajasidagi xavfsizlikni qo‘llab-quvvatlamaydi [12].

HICCUPS tizimining umumiy sxemasi quyidagi 4-rasmda ifodalangan. Unda uchta o‘rnatish, asosiy va tasdiqlangan kadrlar rejimlari mavjud. Ushbu tizim umumiy tarmoqlar, ayniqsa simsiz LAN uchun mo‘ljallangan, past o‘tkazish qobiliyatiga (tarmoqqa bog‘liq), noqulay amalga oshirish, past steganografik xarajat va yuqori aniqlash murakkabligiga ega. Biroq, noto‘g‘ri nazorat summasi bo‘lgan freymlarni tahlil qilish orqali ushbu usuldan

foydalanganib yashirin uzatilgan xabarni aniqlash mumkin [4].

Tizim ishga tushirilganda, yashirin guruhga kiritilgan barcha stansiyalar steganografik tizimga o‘rnatilgan shifrlash uchun maxfiy kalitni o‘rnatadilar. Taklif etilayotgan tizim uchun unicast(1:1 - bitta jo‘natuvchidan bitta qabul qiluvchiga), multicast(1: N - birdan ko‘pga yoki M:N- ko‘pdan ko‘pga) yoki translyatsiya ulanishi bilan cheklanmaydi. Yechim har qanday guruhlash tartib-qoidalari, asosiy kelishuv yoki kalit almashinuv protokoli uchun ochiq hisoblanadi.




**4-rasm**. HICCUPS ishining umumiy sxemasi

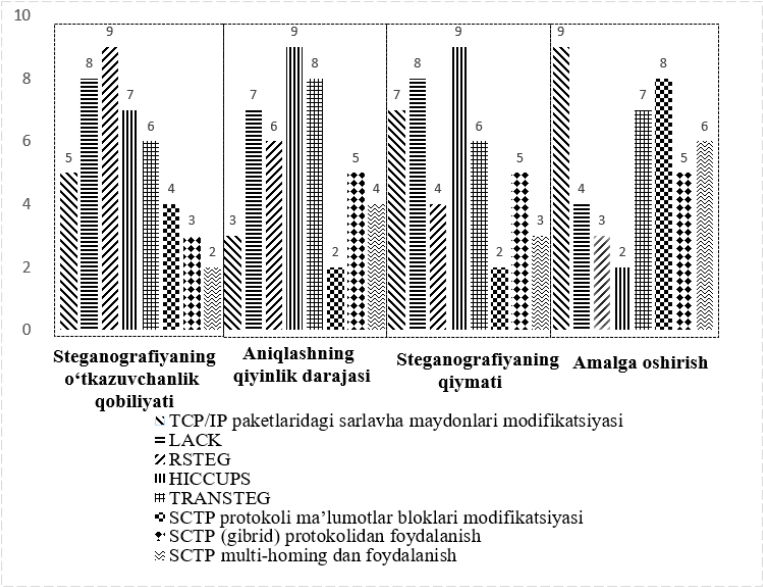
HICCUPS tizimining asosiy ishlash rejimi shifrni ishga tushirish vektorlari (HDC1) va MAC manzillari (HDC2) asosida ma'lumotlar almashinuvini hosil qilishdir. Ushbu yashirin aloqa kanallari past o‘tkazish qobiliyati bilan ajralib turadi va mavjud oqim hajmining 1% dan kamrog‘ini tashkil qiladi. Ular yashirin ish stansiyalari o‘rtasida nazorat xabarlarini almashish uchun va past tarmoq kengligi aloqalari uchun ishlatilishi mumkin. HDC1 yoki HDC2 orqali uzatiladigan belgilangan ketma-ketlik uchun yashirin guruh stansiyalari qo‘shimcha tarmoq kengligi buzilgan oqim rejimiga o‘tadi.

Buzilgan oqim rejimida ma’lumotlar ataylab yaratilgan noto‘g‘ri nazorat summalari (HDC3)bilan freymlarning foydali yuki doirasida uzatiladi. Ushbu rejim ma’lum vaqt davomida deyarli 100% o‘tkazish qobiliyatini ta’minlaydi. Odatda, yashirin guruhga tegishli bo‘lmagan stansiyalar noto‘g‘ri nazorat

summalari bilan buzilgan oqimlarni yo‘q qiladi. HDC1-HDC3 almashish rejimlarini ketma-ket sanab o‘tish asosiy rejimga qaytishga olib keladi. Buzilgan oqim rejimida ishlaydigan tarmoq adapterlari mediadan barcha freymlarni (hatto kadrlar nazorat summasi xatosi bo‘lganlar ham) kuzatilishi kerak.

HICCUPS va shunga o‘xshash ko‘pchilik steganografik tizimlarda kriptografik algoritmlar birgalikda ishlatiladi. Sababi stegoanaliz qilinga yashirilgan axborot oshkor bo‘lishi mumkin. Ushbu holatda maxfiy xabar oshkor bo‘lmasligi uchun steganografik usullar bilan kriptografik algoritmlarni birga qo‘llash yashirin uzatilgan maxfiy xabarlarning oshkor bo‘lishini qiyinlashtiradi.

Yuqorida keltirilgan tarmoq steganografiya usullarining imkoniyat-larini 10 ballik tizimda baholansa quyidagi 5-rasmda keltirilgan qiyosiy tavsiflar paydo bo‘ladi. Steganografiya usullarini o‘tkazish qobiliyati, aniqlash murakkabligi, xarajat va amalga oshirishning murakkabligi jihatidan taqqoslandi. Usullar reytingi nisbiy birliklarda amalga oshiriladi va miqdoriy xususiyatlarni aks ettirmaydi. Diagram-mada ko‘rsatilgan mos keladigan usulning parametri qanchalik katta bo‘lsa, uning xarakteristikasi shunchalik yuqori bo‘ladi. Misol uchun, RSTEG usuli eng yuqori o‘tkazish qobiliyatiga ega va HICCUPS tizimi eng yuqori aniqlash murakkabligiga ega. Shu bilan birga, RSTEG va HICCUPS tizimi oson amalga oshirish murakkabligiga ega. Lekin narx jihatidan HICCUPS tizimi eng qimmat ekanligini ko‘rish mumkin. Aslida tarmoq steganografiyasi tizimi o‘tkazuvchanligi yuqori, aniqlash murakkabligi yuqori, narxi arzon va amalga oshirish oson bo‘lganda optimal bo‘ladi. Biroq, bu parametrlarning barchasini bir vaqtning o‘zida ta’minlash murakkab masala hisoblanadi. Shuning uchun asosiy parametrlar hisoblangan o‘tkazish qobiliyati va aniqlash murakkabligi yuqori bo‘lgan tizimlar tarmoq steganografiyasida samarali hisoblanadi. Tahlil natijalaridan ko‘rish mumkinki tarmoq steganografiyasining gibrid usullaridan bo‘lgan RSTEG va LACK usullarining axborotni yaxshirib uzatish qobiliyati yuqori, lekin aniqlashning qiyinlik darajasi yuqori emas. Shuningdek narx va amalga oshirish murakkabligi bo‘yicha ko‘rsatkichlari talab darajasida.




**5- rasm**. Tarmoq steganografiyasi usullarining qiyosiy tahlili

## III. XULOSA

Shundan kelib chiqib RSTEG va LACK usullarida ruxsatsiz aniqlashning qiyinlik darajasini oshirilsa, barcha ko‘rsatkkichlar bo‘yicha talabga javob beruvchi usullar hosil bo‘ladi. Shuning uchun tadqiqotning keyingi bosqichlarida tarmoq steganografiyasining gibrid usullarini takomillashni amalga oshirish maqsadga muvofiq hisoblanadi [12].

RSTEG usuli TCP/IP protokolida, LACK usuli VoIP protokilida amalga oshiriladi. Biroq, tarmoqda amaliy sathda xabarlar asosan HTTP prototokolda uzatiladi. Ushu protokolda ham xabarlarni steganografik yashirib uzatish mumkin. Shuning uchun keyingi ilmiy izlanishlarda xabarlarni HTTP prototokolida stega-nografik yashirish usullariga e’tibor qaratiladi.

## ADABIYOTLAR

[1] *Белкина, Т. А.* Аналитический обзор применения сетевой стеганографии для решения задач информационной безопас-ности / Молодой ученый. — 2018. — № 11 (197). — С. 36-44.

[2] *Zseby T. et al.* A network steganography lab on detecting TCP/IP covert channels //IEEE Transactions on Education. – 2016. – Т. 59. – №. 3. – S. 224-232

[3] *Wojciech Mazurczyk, Paweł Szaga, Krzysztof Szczypiorski.* Using Transcoding for Hidden Communication in IP Telephony. Warsaw University of Technology, Institute of Telecommunications. http://arxiv.org/pdf/1111

[4] *L. Ji, W. Jiang, B. Dai, X. Niu*, A novel covert channel based on length of message. In proceedings of 2009 International symposium on information engineering and electronic commerce. 2009, pp. 445-450.

[5] *L. Yao, X. Zi, L. Pan and J. Li.* A study of on/off timing channel based on packet delay distribution. Computers & Security, 2009,28(8), pp.785-794.

[6] W. *Mazurczyk, M. Smolarczyk, K. Szczypiorski.* Retransmission steganography and its detection. Soft Computing. 2009, 15(3), pp. 505-515.

[7] *K. Szczypiorski* — HICCUPS: Hidden Communication System for Corrupted Networks <http://krzysiek. tele. pw. edu. pl/pdf/acs2003-hiccups. pdf>.

[8] W. *Mazurczyk, J. Lubacz, K. Szczypiorski* — On steganography in lost audio packets. Интернет: < https://arxiv.org/ftp/arxiv/papers/ 1102/1102.0023. pdf>

[9] *W. Frączek, W. Mazurczyk, K. Szczypiorski.* Stream Control Transmission Protocol Steganography. //Warsaw University of Technology, Institute of Telecommunications http://arxiv.org/abs/1006.0247

[10] *Wojciech Mazurczyk, Paweł Szaga, Krzysztof Szczypiorski.* Using Transcoding for Hidden Communication in IP Telephony./ Warsaw University of Technology, Institute of Telecommunications http://arxiv.org/pdf/1111.1250v1. pdf

[11] *Wojciech Mazurczyk, Paweł Szaga, Krzysztof Szczypiorski.* Using Transcoding for Hidden Communication in IP Telephony. / Warsaw University of Technology, Institute of Telecommunications http://arxiv.org/pdf/1111.

[12] *W. Frączek, W. Mazurczyk, K. Szczypiorski.* Stream Control Transmission Protocol Steganography. //Warsaw University of

Technology, Institute of Telecommunications. URL: http://arxiv.org/abs/1006.0247

[13] *Anderson B. et al.* Limitless HTTP in an HTTPS World: Inferring the Semantics of the HTTPS Protocol without Decryption //Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy. – 2019. – S. 267-278.

[14] *Akasiadis C., Pitsilis V., Spyropoulos C. D.* A multi-protocol IoT platform based on open-source frameworks //Sensors. – 2019. – T. 19. – №. 19. – S. 4217.

*Поступила в редакцию 16.01.2023*

**Citation**: *Ganiyev A.A., Allanov O.M., Mavlonov O.N.* (2023). Tarmoq steganografiyasi usullarining tahlili. Raqamli texnologiyalarning nazariy va amaliy masalalari xalqaro jurnali. 2(4). – B. 62-72.

# ANALYSIS OF NETWORK STEGANOGRAPHY METHODS

*Ganiyev A.A.* [1], *Allanov O.M.*[1], *Mavlonov O.N.*[1]

[1] Tashkent University of information technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan
abduhalilganiev58@gmail.com, orif_allanov@mail.ru, mavlonov8686@gmail.com

**Abstract**. *This article provides information about methods for hiding secret messages in the TCP / IP protocol operating at the transport layer of the OSI model. The possibilities of network steganography methods were also analyzed. Based on the results of the analysis, methods of network steganography with a high probability of hiding information and a low rate of unauthorized detection were identified.*

**Keywords**: *Network steganography, IP, VOIP, LACK, RSTEG, SCTP, HICCUPS, TCP/IP, HTTP.*

# АНАЛИЗ МЕТОДОВ СЕТЕВОЙ СТЕГАНОГРАФИИ

*Ганиев А.А.* [1], *Алланов О.М.*[1], *Мавлонов О.Н.*[1]

[1]Ташкентский университет информационных технологий имени Мухаммада ал-Хорезми, Ташкент, Узбекистан
abduhalilganiev58@gmail.com, orif_allanov@mail.ru, mavlonov8686@gmail.com

**Аннотация**. *В данной статье представлена информация о методах сокрытия секретных сообщений в протоколе TCP/IP, работающем на транспортном уровне модели OSI. Также были проанализированы возможности методов сетевой стеганографии. По результатам анализа определены методы сетевой стеганографии с высокой вероятностью сокрытия информации и низким показателем несанкционированного обнаружения.*

**Ключевые слова:** *Сетевая стеганография, IP, VOIP, LACK, RSTEG, SCTP, HICCUPS, TCP/IP, HTTP.*