GSM UYALI ALOQA TIZIMLARIDA IDENTIFIKATSIYALASHNI KLONLASH ORQALI MA'LUMOTLARNI YECHIB OLISH USULI VA MUAMMOLARI

O'R MV Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti
AKT va AHI radioyelektron razvetka va kurash kafedrasi kapitan
Axunov A.A
AKT va AHI radioyelektron razvetka va kurash kafedrasi kursanti
Alimardonov Sh.E

Annotatsiya: *Ushbu maqolada GSM uyali aloqa standarti tashkiliy tuzilishi, ma'lumotlar xavfsizligini ta'milash, SIM karta orqali tarmoqqa ulanishda haqiqiylikni teklshirish jarayonlari, SIM kartani klonlashtirish usullar ko'rib chiqilgan bo'lib, ushbu usullarning afzalligi va kamchiligi qiyosiy tahlili keltirilgan.*

Kalit so'zlar: *uyali aloqa, GSM standarti, kanllarni vaqt bo'yicha ajratish, kanllarni chastota bo'yicha ajratish, abonent terminali, bazaviy stansiya, autentifikatsiya, autentifikatsiya markazi, individual kalit.*

Аннотация: *В данной статье рассмотрена организационная структура стандарта сотовой связи GSM, обеспечение безопасности данных, процессы аутентификации при подключении к сети с использованием SIM-карты, методы клонирования SIM-карт, а также представлено сравнительный анализ преимуществ и недостатков этих методов.*

Ключевые слова: *сотовая связь, стандарт GSM, выделение каналов по времени, выделение каналов по частоте, абонентский терминал, базовая станция, аутентификация, центр аутентификации, индивидуальный ключ.*

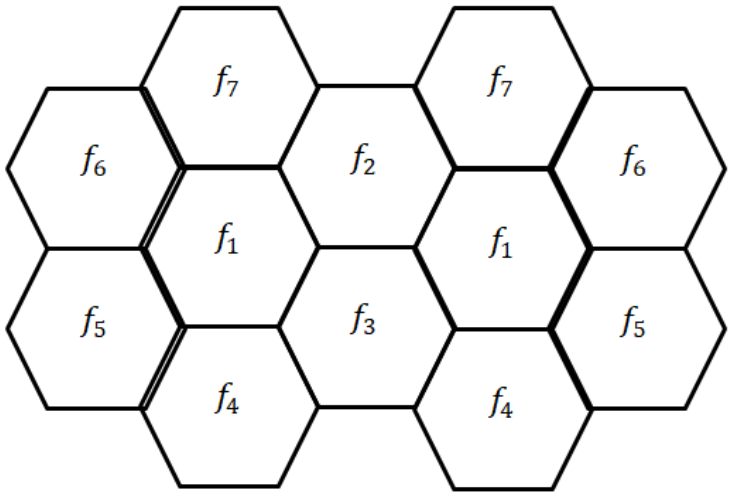
Abstract: *This article discusses the organizational structure of the GSM cellular communication standard, ensuring data security, authentication processes when connecting to a network using a SIM card, methods for cloning SIM cards, and also presents a comparative analysis of the advantages and disadvantages of these methods.*

Key words: *cellular communications, GSM standard, allocation of channels by time, allocation of channels by frequency, subscriber terminal, base station, authentication, authentication center, individual key.*

XXI asr bu axborot texnologiyalar asri bo'lib, hozirgi kunda jadal rivojlanib borayotgan texnologiyalar barcha sohalarga kirib bordi. Bugungi kunni yuqori texnologiyalar, jumladan uyali aloqa vositalarsiz tasavvur qilib bo'lmaydi. Sababi axborot texnologiyalar, xususan uyali aloqa tizimlariga bo'lgan talab oshib bormoqda va mobil aloqa tizimlariga bo'lgan talab 10 yil avvalgi holatdan keskin farq qiladi. Avvallari aloqaning o'ziga talab yuqori bo'lgan bo'lsa, hozirgi kunga kelib, nafaqat aloqaga, balki aloqaning tezligi, uning sifati, qo'shimcha xizmatlariga va eng muhimi aloqaning xavfsizligiga talab ortib bormoqda.

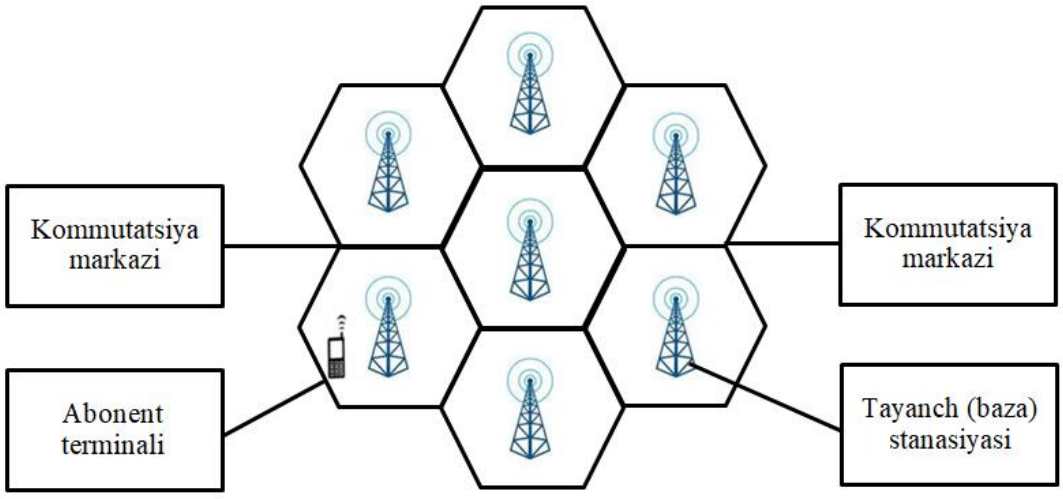
Hozirgi vaqtda uyali aloqa vositalarida turli xil aloqa turlarini (uyali, sun'iy yo‘ldosh, televizor va boshqalar) integratsiyalashuvi davom etmoqda, gibrid qurilmalar, shu jumladan PDA paydo bo‘ldi, videokamera, IoT qurilmalari, albatta, 5G tarmoqlarining keng tarqalishiga olib keldi [2].

Uyali aloqa tizimlarining joriy etilishi xabarlarni bir xil chastotalarda uzatish orqali ajratilgan radiochastota diapazonidan tejamkor foydalanish muammosini hal qilish va telekommunikatsiya tarmoqlarining o‘tkazuvchanligini oshirish imkonini berdi. Ular o‘z nomlarini aloqani tashkil etishning uyali printsipiga muvofiq oldilar, unga ko‘ra xizmat ko‘rsatish hududi (shahar yoki viloyat hududi) uyalarga (uyalarga) bo‘linadi. Nisbatan yaqinda paydo bo‘lgan ushbu uyali aloqa tizimlari aloqa tizimlarining mutlaqo yangi turidir, chunki ular uyali aloqaga muvofiq qurilgan: xizmat ko‘rsatish hududi bo‘yicha chastotalarni taqsimlash printsipi (hududiy chastotani rejalashtirish) va radio bilan ta’minlash uchun mo‘ljallangan.



1-rasm. Hududiy chastotani rejalashtirish

Uyalarning har biriga tayanch stantsiya deb ataladigan ko‘p kanalli qabul qiluvchi qurilma xizmat ko‘rsatadi. Bu uyali telefon va mobil kommutatsiya markazi o‘rtasidagi o‘ziga xos interfeys bo‘lib xizmat qiladi, bu erda radioto‘lqinlar an'anaviy telefon tarmog‘ida simlar rolini o‘ynaydi. Asosiy stansiya kanallarining soni odatda 8 ga ko‘paytiriladi, masalan, 8, 16, 32... Kanallardan biri boshqaruv kanalidir. Ba’zi hollarda uni chaqiruv kanali deb ham atash mumkin. Ushbu kanalda mobil tarmoq abonentiga qo‘ng‘iroq qilishda to‘g‘ridan-to‘g‘ri ulanish o‘rnatiladi va suhbatning o‘zi faqat hozirgi vaqtda bepul kanal topilgandan va unga o‘tish sodir bo‘lgandan keyin boshlanadi. Bu jarayonlarning barchasi juda tez va shuning uchun abonent uchun sezilmaydigan tarzda sodir bo‘ladi. U faqat kerakli telefon raqamini teradi va oddiy telefondagi kabi gaplashadi.

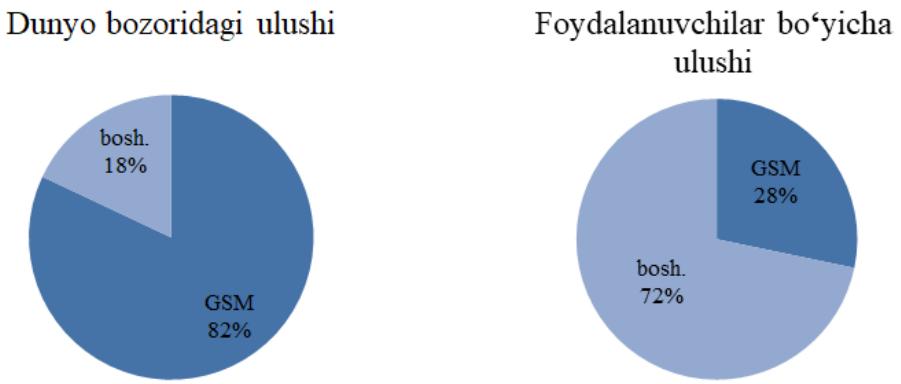


Har qanday uyali aloqa kanallari dupleks aloqa uchun chastotalar juftligi, ya'ni tayanch va mobil stansiyalarning chastotalari ajratilgan. Bu signalni filtrlashni yaxshilash va transmitterning bir vaqtning o‘zida ishlayotgan bir xil qurilmaning qabul qiluvchisiga o‘zaro ta'sirini bartaraf etish uchun amalga oshiriladi.

Barcha tayanch stansiyalar maxsus simli yoki radioreleyli aloqa kanallari orqali mobil kommutatsiya markaziga (kommutator) ulangan MSC barcha tarmoqni boshqarish funktsiyalarini ta’minlovchi uyali telefon stantsiyasidir. U doimiy ravishda mobil stansiyalarni kuzatib boradi, ularning releli uzatilishini tashkil qiladi, bunda aloqa uzluksizligiga mobil stansiya bir uyadan uyaga o‘tganda va xalaqit yoki nosozliklar yuzaga kelganda yacheykadagi ishchi kanallarni almashtirishda erishiladi, mobil abonentni unga kerak bo‘lganiga ulaydi.

Uyali aloqa standartlarining xilma-xilligiga qaramay, mavjud funksiyalardan qat’iy nazar, ularning ishlash algoritmlari asosan o‘xshashdir. Hozirgi kunga kelib dunyo bo‘ylab keng tarqalgan uyali aloqa standarti GSM hisoblanadi.

GSM - (Global System for Mobile Communications) mobil uyali aloqa uchun raqamli standart bo‘lib, chastota kanali FDMA va vaqt bo‘yicha TDMA printsipiga ko‘ra bo‘linadi va o‘rtacha xavfsizlik darajasiga ega. GSM XX asr 80-yillarning oxirida Yevropa telekommunikatsiya standartlari instituti (ETSI) tomonidan ishlab chiqilgan. GSM hozirgacha eng keng tarqalgan aloqa standartidir. GSM assotsiatsiyasi (GSMA) ma’lumotlariga ko‘ra, ushbu standart global mobil aloqa bozorining 82 foizini tashkil qiladi, dunyo aholisining 29 foizi global GSM texnologiyalaridan foydalanadi. GSMA hozirda 210 dan ortiq mamlakat va hududlardagi operatorlarni o‘z ichiga oladi.

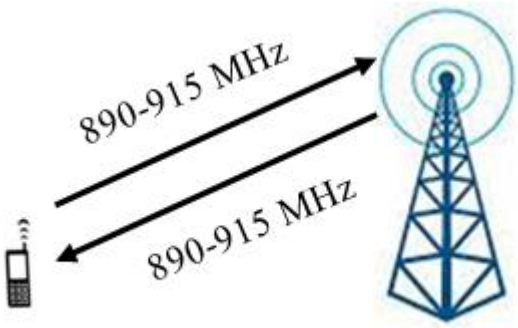


3-rasm. GSM standartining dunyo bozoridagi umumiy ulushi

GSM standarti boshqa uyali aloqa standartlarida ishlatilmaydigan (yoki to‘liq ishlatilmaydigan) qator xizmatlarni o‘z foydalanuvchilariga taqdim etadi. Ularga quyidagilar kiradi:

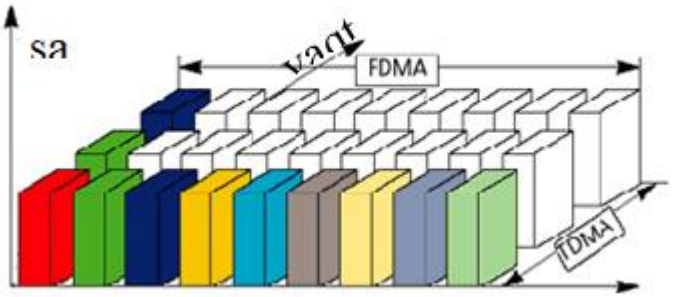
- kanal va aloqa xizmatlariga ulanish uchun intellektual SIM- kartalardan foydalanish;
- uzatiladigan xabarlarni shifrlash;
- yashirin eshitishga yopiq radiointerfeys mavjudligi;
- abonentni autentifikatsiyalash va abonentlar qurilmalarini kriptografik algoritmlar bo‘yicha identifikatsiya qilish;
- signalizatsiya kanallari bo‘yicha uzatiladigan qisqa xabarlar xizmati;
- milliy va xalqaro ko‘lamlarda turli GSM tarmoqlarini abonentlarining avtomatik roumingi;

1980-yildagi SERT tavsiyalariga muvofiq, GSM standartidagi harakatdagi aloqa uchun 862 - 960 MHz diapazondagi chastotalar spektri ajratilgan. Harakatdagi stansiyadan bazaviy stansiyaga uzatish uchun 890 - 915 MHz chastotalar polosasi va bazaviy stansiyadan harakatdagi stansiyaga (abonentga) uzatish uchun 935 - 960 MHz chastotalar polosasi ishlatiladi. Aloqa seansi vaqtida kanallarning qayta ulanishida bu chastotalar orasidagi farq o‘zgarmas va 45 MHzga teng. Qo‘shni aloqa kanallari orasidagi chastotalar farqi 200 kHzni tashkil etadi. Shunday qilib, qabul qilish/uzatish uchun ajratilgan 25 MHz chastotalar polosasida 124 ta aloqa kanallari joylashadi.



3-rasm. GSM standartida abonent terminali va baza stansiyasi orasida chastotalar polosasi taqsimlanishi

GSM standartida vaqt bo‘yicha tor polosali ko‘p stansiyali ulanish (TDMA va FDMA) ishlatiladi, bu bitta tashuvchi chastotada bir vaqtda 8 tagacha nutq kanallarini joylashtirishga imkon beradi. Nutqni o‘zgartirish qurilmasi sifatida munatazam impulsli qo‘zg‘atishli (yuqori chastotali vibrator) va 13 Kbit/s nutqni o‘zgartirish tezligini RPE – LTP nutq koderi ishlatiladi.



4-rasm. GSM standartida vaqt bo‘yicha tor polosali ko‘p stansiyali ulanish (TDMA va FDMA)

Bu standartda nutqqa ishlov berish uchun qabul qilingan nutqni uzlukli uzatish - DTX (Discontinuous Transmission) tizimi doirasida amalga oshiriladi, u faqat signal bo‘lganida uzatkich yoqilishini ta’minlaydi, pauzalarda va so‘zlashuvning oxirida uzatkich o‘chiriladi. DTX tizimi nutqning aktivligi detektori - VAD (Voice Activity Detector) ni boshqaradi, u hatto shovqin sathi nutqning sathiga teng bo‘ladigan holarda shovqinli nutq va shovqinsiz nutq intervallarini aniqlash va ajratishni ta’minlaydi.

Radiokanallarda vujudga keladigan xatoliklardan himoyalash uchun o‘rin alamshtirishli blokli va o‘ramli kodlash qo‘llaniladi. Harakatdagi stansiyalarning kichik harakatlanish tezligida kodlash va o‘rin almashtirishning samaradorligini oshirishga aloqa seansi jarayonida ishchi chastotalarni sekin (sekundiga 217 sakrashlar tezligida) qayta ulash bilan erishiladi.

Shahar sharoitlarida radioto‘lqinlarning ko‘p nurli tarqalishi keltirib chiqaradigan qabul qilingan signallarning interferension so‘nishlari bilan kurashish uchun aloqa apparaturalarida impulsli signallarni kechikish vaqtining 16 mksgacha o‘rtacha kvadratik og‘ishi bilan tekislashni ta’minlaydigan ekvalayzerlar ishlatiladi. Qurilmalarni sinxronlashtirish tizimi signallarni kechikishi absolyut vaqtini kompensatsiyalashga (233 mks gacha) mo‘ljallangan. Bu 35 km (uyaning radiusi) maksimal aloqa masofasiga mos keladi.

Radiosignalni modulyatsiyalash uchun minimal chastotaviy surishli spektral-samarador gauss chastotaviy manipulyatsiyalash (GMSK) qo‘llanadi. Bunday nomlash axborot bitlari ketma-ketligi modulyatorgacha gauss amplitudaviy-chastotaviy xarakteristikasiga ega bo‘lgan past chastotalar filtridan o‘tishiga bog‘liq, bu nurlantiriladign signal chastotasi kengligining sezilarli kamayishiga olib keladi.

GMSK radiosignalni shakllantirish bitta bitga mos keladigan intervalda tashuvchining fazasi 90° ga o‘zgaradigan tarzda bo‘lib o‘tadi. Bu bunday turdagi manipulyatsiyalashda

aniqlanishi mumkin bo‘lgan fazaning eng kichik o‘zgarishi hisoblanadi. Faza uzluksiz o‘zgaradigan chiqish signali chastota diskret o‘zgaradigan chastotaviy modulyatsiyalash natijasida olingan signalga o‘xshash bo‘ladi.

1-jadval

GSM standarti umumiy tavsifi

Harakatdagi stansiyaning uzatish chastotasi va bazaviy stansiyaning qabulqilish chastotasi, MHz	890 - 915
Harakatdagi stansiyaning qabul qilish chastotasi va bazaviy stansiyaning uzatish chastotasi, MHz	935 - 960
Qabul qilish va uzatish chastotalarining dupleks ajratilishi, MHz	45
Radiokanalda ma’lumotlarni uzatish tezligi, kbit/s	270, 883
Nutq kodekining o‘zgartirish tezligi, kbit/s	13
Aloqa kanali polosasining kengligi, kHz	200
Aloqa kanallarining maksimal soni	124
Bazaviy stansiyada tashkil etiladigan kanallarning maksimal soni	16 - 20
Modulyatsiyalash turi	GMSK
Modulyatsiyalashindeksi	BT 0,3
Modulyatsiyalashdan oldingi gauss filtri polosasining kengligi, kHz	81,2
Chastota bo‘yicha sekundiga sakrashlar soni	217
Harakatdagi aloqa uchun TDMA kadr (uzatish/ qabul qilish) intervallarida vaqt bo‘yicha ajratish	2
Nutq koderining turi	RPE/LTR
Uyaning maksimal radiusi, km	35 gacha
Kanallarni tashkil etish sxemasi	Kombinatsiyalangan TDMA/FDMA

GSM tizimida ma’lumotlarni uzatish xavfsizligini ta’minlash uchun quyidagi choralar ko‘riladi:

foydalanuvchining haqiqiyligini tekshirish asosida tarmoqqa kirishni amalga oshirish;

shifrlash yordamida uzatiladigan ma’lumotlarni (nutq signallari, ma’lumotlar, fakslar va boshqaruv signallari) tasniflash;

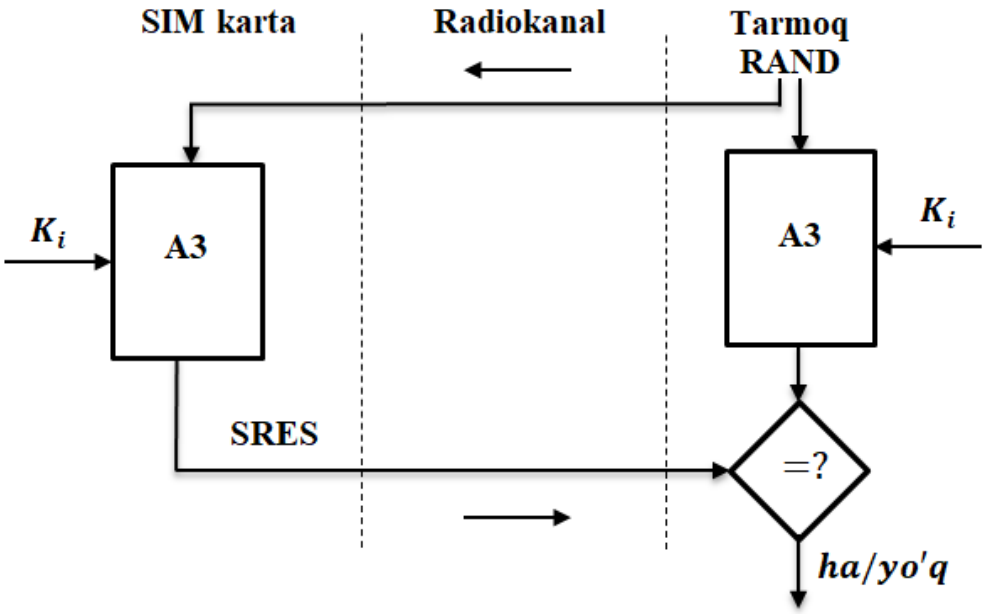
tarmoq ichida mobil abonentning vaqtinchalik identifikatsiya raqamidan foydalanish tufayli abonentlarning anonimligini ta’minlash.

GSM tizimida maxfiylikni ta’minlashning muhim elementi abonentni identifikatsiya qilish moduli (ingl. Subscriber Identity Module) - SIM karta hisoblanadi.

Ro‘yxatdan o‘tish jarayonida tarmoq haqiqiyligini tekshirishni boshlaydi

(5-rasm). Ko‘chma stansiyaga 128 bitli RAND psevdo tasodifiy raqami yuboriladi. A3 shifrlash algoritmi yordamida va foydalanuvchi uchun individual kaliti KI tarmoq va SIM-

karta 32 bitli SRES elektron imzoni (ingl. signed response) hisoblaydi. Harakatlanuvchi stantsiya tomonidan hisoblangan SRES imzosi tarmoqning belgilangan qismiga uzatiladi, bu yerda ikkala imzo ham taqqoslanadi. Agar ular bir-biriga mos kelsa, autentifikatsiya jarayoni tugallangan deb hisoblanadi. Keyingi bosqichda VLR foydalanuvchiga TMSI va LAI ni ajratadi. Ikkala raqam ham mobil stantsiyaga shifrlangan shaklda uzatiladi va SIM-kartada saqlanadi. Shaxsiy IMSi raqami foydalanuvchi mavjudligi davomida bir marta uzatiladi. Bu harakatlanuvchi stantsiya birinchi marta tarmoqda ro‘yxatdan o‘tganida va VLR registrida bu haqda hech qanday ma’lumot bo‘lmaganida sodir bo‘ladi.



5-rasm. GSM tarmog‘ida ro‘yxatdan o‘tish jarayonida haqiqiylikni tekshirish

Yuqorida ta’kidlab o‘tilganidek, ulanishni o‘rnatishning ma’lum bir bosqichidan boshlab foydalanuvchi ma’lumotlari va boshqaruv signallari shifrlangan shaklda uzatiladi. Shifrlash jarayoni Yevropada standartlashtirilgan A5 ochiq kalitli shifrlash algoritmidan foydalanadi. Ushbu algoritmga faqat uyali aloqa uskunalari ishlab chiqaruvchilari kirishlari mumkin. Uzatilayotgan ma’lumotlarning maxfiyligi nafaqat shifrlash algoritmiga kirishni cheklashga, balki birinchi navbatda hech qachon radiokanallar orqali uzatilmaydigan shifrlash kalitidan foydalanishga asoslangan.

Bugungi kunga kelib uyali aloqa vositalari keng qo‘llanilayotgani, ma’lumotlar oqimining ortib borishi radiokanalni kuzatish va monitoring qilish jarayonida bevosita obyektlar va manbaalar soni oritishiga olib keldi. Shu jixatdan xavfsizlikni ta’minlash jarayonida kuzatuv obyektlarining uyali aloqa vositalariga yashirincha ulanish va kuzatishni talab etadi. Natijada uyali aloqa kanalini kuzatish va monitoring qilishda turli darajadagi qiyinchiliklarni keltirib chiqaradi. Lekin uyali tarmoqqa va abonent terminaliga ulanish, qo‘ng‘iroqlarni tinglash va qisqa xabarlarni tutishning bir nechta usullari ishlab chiqilgan. Quyida shunday usullardan biri hisoblangan SIM kartani klonlashtirish usuli va turlarini ko‘rib o‘tamiz.

GSM standartida ma’lumotlarni olish usullaridan biri SIM kartani klonlashtirish hisoblanadi. Internetda tez-tez kartani klonlashtirishning oson yo‘llari haqida e’lonlarni va SIM Card Seizure ga o‘xshash utilitlarni uchratish mumkin.

Klonlashtirishdan asosiy maqsad qilib odatda SIM-karta egasining hisobidan bepul qo‘ng‘iroqlarni amalga oshirish va ularning so‘zlashuvlarini eshitish ko‘rsatiladi.

Hozirgi vaqtga kelib SIM kartani klonlashtirishning bir necha usullari ishlab chiqilgan bo‘lib, ushbu jarayonda asosiy muammo KI individual kalitni qo‘lga kiritish hisoblanadi.

Yuqorida SIM-kartaning haqiqiylikka tekshirish jarayoni ta’riflangan edi. Bu jarayondagi asosiy parametrlar IMSI va KI individual kalit edi. Klon AUC da autentifikatsiyadan o‘tishi uchun u yuqoridagi parametrlarni bilishi zarur. IMSI ni aniqlash oson chunki u kartaning o‘zida yozilgan bo‘lishi yoki unga biriktirilishi mumkin. Uni SIM-karta o‘qiydigan qurilma orqali aniqlash mumkin. Ammo KI ga kelsak jarayon oson kechmaydi.

Ma’lumki KI individual kalit ikki joyda ya’ni SIM-karta xotirasi va AUC xotirasida saqlanadi. KI individual kalit hech qachon ochiq ko‘rinishda uzatilmaydi va uni autentifikatsiya jarayonida tutib olishning imkoni yo‘q. Hujum amalga oshiruvchilarda KI individual kalitni olish uchun 4 ta variant bor.

Birinchisi kompaniya-operatordagi insayder. Bu variant qulayroq bo‘lib birdaniga bir nechta kartalar haqida ma’lumot olish mumkin. Ushbu variantning kamchiliklari KI individual kalitning ahamiyati bilan bog‘liq bo‘lib uning ko‘rsatkichlariga ruxsat cheklangan va ko‘p hajmdagi ma’lumotlar chiqib ketganda insayder darrov aniqlanadi. Undan tashqari AUCda KI individual kalitni o‘qish uchun mo‘ljallangan funkisonal xavfsizlik nuqtai nazaridan mavjud bo‘lmaydi.

Ikkinchi variant KI individual kalitni o‘g‘irlash bilan bog‘liq bo‘lib bu odatda ishlab chiqaruvchidan SIM-karta olingan zahoti amalga oshiriladi. Mazkur variantda ham muammolar avvalgi variantdagidek: ma’lumotlarga ruxsat berilgan shaxslar soni cheklangan.

Uchinchi variant: KI individual kalitni SIM-karta xotirasidan olish. Boshlanishiga obyekt kartasini qo‘lga kiritish zarur (uni biror operatsiya bajarish orqali xizmatni yaxshilash bahonasida telefondan chiqarish va PIN kodni aniqlash lozim). Muhim kamchilik: SIM-kartadan KI individual kalitni o‘qish yoki o‘zgartirish mumkin bo‘lgan interfeys mavjud emas.

Va nihoyat oxirgi variant: KI individual kalitni olish uchun hujum amalga oshiruvchi operator tomonidan foydalaniladigan A3 algoritmi haqida ma’lumotlarga ega bo‘lishi kerak. Bunda SRES da RAND natijalarining vujudga kelishini kuzatish orqali KI individual kalitni aniqlash mumkin. Buning uchun RAND ni avtomatlashmagan holda transformatsiya qilinadi, algoritm chaqiriladi va unga RAND beriladi. Bu jarayonni SimScan va WoronScan kabi dasturlar orqali avtomatlashtiriladi.

SIM-karta klonlari birinchi marta aynan shu tarzda olingan. Bu COMP128 deb ataluvchi A3 algoritmi haqidagi ma’lumotlar tarmoqqa chiqib ketganidan so‘ng sodir

bo‘lgan. Algortimda kamchiliklar aniqlangan, ya’ni ko‘p sonli terishlarni amalga oshirish usuli orqali KI individual kalitni aniqlash imkoni yuzaga kelgan. Ushbu zaiflik aniqlangandan so‘ng ko‘pgina operatorlar uni mustahkamrog‘iga almashtirishdi. Hozirgi kunda COMP128 ni 3 ta versiyasi mavjud. Ikkinchi va uchinchi versiyalari hozirgi kunda ochib bo‘lmas hisoblanadi. Albatta tarmoqda ushbu veriyalarni buzish imkoniyatiga ega bo‘lgan dasturlar haqida ko‘pgina ma’lumotlar bor ammo ushbu dasturlarni yuklab olgan foydalanuvchilar amalda ular o‘rniga (trojan) viruslari bilan to‘qnashadilar.

Agar hujum amalga oshiruvchi A3 algoritmining tashkiliy tuzilishi haqida ma’lumotga ega bo‘lmasa u KI individual kalitni terib ko‘rish (brute force) orqali amalga oshirishga urinib ko‘rishi mumkin. Bunda yana bitta to‘siq yuzaga keladi: KI individual kalitni terib ko‘rish uchun urinishlar soni cheklangan. SIM-kartada A3 ning chaqirishlar sonini cheklovchi hisoblagich o‘rnatilgan bo‘lib, ma’lum bir urinishlar soniga yetgach (65535) karta bloklanadi va registratsiya uchun so‘rovlarga javob bermay qo‘yadi (lekin boshqa funksiyalari faoliyat ko‘rsatishda davom etadi, masalan telefon kitobi (abonentlar ro‘yxati)). Doimiy xizmat ko‘rsatish jarayonida, SIM-karta har gal tarmoqda registratsiyadan o‘tkazilganda A3 chaqiruvi amalga oshiriladi, undagi cheklovlar abonentga halaqit bermaydi. Lekin KI individual kalitni olish uchun ko‘proq urinishlar kerak bo‘lishi mumkin.

Agar hujum amalga oshiruvchi KI individual kalitni topishni uddalasa u boshqa abonent hisobidan qo‘ng‘iroqlarni amalga oshirish imkoniyatiga ega bo‘ladi. Ammo bu yerda bir nechta cheklovchi faktorlar mavjud. Birinchidan abonent hisobidagi pullar odatdagidan tezroq sarflana boshlaydi va SIM-karta egasi buni katta ehtimol bilan payqaydi. Qo‘ng‘iroqlar tarixi ro‘yxati operator tomonidan olinganda ortiqcha qo‘ng‘iroqlar darrov aniqlanadi. Bu “cheksiz” tarif rejalaridagi abonentlarda ham bilinadi, chunki ularda ham ma’lum bir cheklovlar saqlanib qolgan (chet davlatlarga qo‘ng‘iroqlarni amalga oshirish). Shuning uchun hujum amalga oshiruvchi mavjud balansdagi mablag‘ni tugatib SIM-karta klonidan tezroq xalos bolishga harakat qiladi. Ikkinchidan, agar ikkala karta ham tarmoqda ro‘yxatdan o‘tgan bo‘lsa, kirish qo‘ng‘iroqlari oxirgi avtorizatsiyadan o‘tgan yoki oxirgi chiqish qo‘ng‘irog‘i amalga oshirilgan abonentga keladi. Bunda faol bo‘lagan abonent unga kutilayotgan qo‘ng‘iroqlar kelmayotganidan bilib olishi mumkin. Hujum amalga oshiruvchilar yashirinlikni ta’minlash uchun qo‘ng‘iroqlarga javob bermasligi maqbul hisoblanadi. Aks holda abonent muhbirlarni hujum amalga oshiruvchini darhol aniqlashadi. Uchinchidan operator cheklangan vaqt oralig‘ida tarmoqda ro‘yxatdan o‘tgan SIM-kartalarni geografik jihatdan har xil joydaligini aniqlashi mumkin va klonlashtirilganlikda gumon qilinayotgan kartani bloklab abonentga yangi karta beradi.

2-jadval.

SIM kartani klonlanshtirish uchun zarur bo‘lgan KI individual kalitni
qo‘lga kiritish usullari qiyosiy tahlili

K_I individual kalitni olish usullari	Afzalligi	Kamchiligi
1-variant kompaniya-operatordagi insayder	birdaniga bir nechta kartalar haqida ma'lumot olish mumkin	ko'p hajmdagi ma'lumotlar chiqib ketganda insayder darrov aniqlanishi
2-variant individual kalitni o'g'irlash	SIM-karta olingan zahoti amalga oshiriladi	ma'lumotlarga ruxsat berilgan shaxslar soni cheklangan
3-variant individual kalitni SIM-karta xotirasidan olish	SIM-kartani bevosita qo'lga kiritish	SIM-kartadan K_I ni o'qish yoki o'zgartirish mumkin bo'lgan interfeys mavjud emas
4-variant hujum amalga oshirish	A3 algoritmi haqida oldindan ma'lumotlarga ega bo'lish (SRES, RAND)	SIM-kartada A3 ning chaqirishlar sonini cheklovchi hisoblagich o'rnatilgan

Xulosa qilib aytish mumkinki SIM-kartalarni klonlashtrish mumkin, ammo juda qiyin. Agarda operator o'z vaqtida A3 ni modernizatsiyasini amalga oshirgan va uning hodimlari o'z kasbiga va ishiga sodiq bo'lishsa, abonentlar SIM-kartalari klonlashtirilishidan qo'rqmasliklari mumkin. Bundan tashqari bunday hujum amalga oshirish darajasi abonentlar tomonidan o'z qurilmalari va ma'lumotlari xavfzislik siyosatini to'g'ri amalga oshirishlari, begona shaxslarga qurilmalarini bermasliklari, doimiy tarzda parollar siyosatini to'g'ri amalga oshirishlari orqali pasaytirilishi mumkin.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

[1] "Uyali aloq tizimi GSM standartida axborot xavfsizligini ta'minlashning kriptografik jihatlari", A.A. Axunov, "Harbiy aloqa va Akt xabarlari" 4(8),Toshkent,2021-y.// (M), 37-60 b.

[2] "GSM va mobil tarmoqlarni boshqarish". Madaminov H.X., Ibraimov R.R., Khatamov A.P., Khotamov A., Xakimov Z.T. – "Nihol Print" OK nashriyoti, 2021-y.

[3] Сети мобильной связи. Частотно-территориальное планирование. Учебное пособие для вузов / В. Ю. Бабков, М. А. Вознюк, П. А. Михайлов. - 2-е изд., испр. - М.: Горячая линия-Телеком, 2007 г.,-224 с.: ил.

[4] Андреев В.А. Обзор системы GSM. Харьковский национальный университет радиоэлектроники. https://studfiles.net/preview/

[5] Веселовский Кшиштоф. Системы подвижной радиосвязи. – М.: Горячая линия – Телеком, 2006 г., 536с.