Б Ъ Л Г А Р С К А А К А Д Е М И Я Н А Н А У К И Т Е

ИНСТИТУТ ПО ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ

Илиян Грозданов Илиев

ОПТИМИЗАЦИЯ НА ПРЕХОДА ОТ УПРАВЛЕНИЕ НА АСЕТИ КЪМ УПРАВЛЕНИЕ НА УСЛУГИ В СЛОЖНИ ФЕДЕРИРАНИ СИСТЕМИ В ПУБЛИЧНИЯ СЕКТОР

ДИСЕРТАЦИЯ

за придобиване на образователната и научна степен „доктор“

по докторска програма „Компютърни системи, комплекси и мрежи“

професионално направление 5.3. “Комуникационна и компютърна техника“

Научен ръководител: доц. д-р Велизар Шаламанов

София, 2026 г

Съдържание

Списък на използвани съкращения и термини

Асет – asset – идентифицируем технически, информационен или организационен ресурс, който има стойност за организацията и участва в предоставянето на услуги.

ИТ – информационни технологии.

AI – Artificial Intelligence – Изкуствен интелект.

АТЦ – автоматична телефонна централа – комутационна система, която автоматично свързва абонати в телефонна мрежа, без нужда от човек-оператор.

ISP – Internet Service Provider – доставчик на Интернет достъп.

Credentials – идентификационни данни – данни за удостоверяване на потребител или система, например потребителско име и парола, сертификат или биометрични данни.

Dial-up – комутируем достъп – метод за достъп до интернет чрез обществена комутируема телефонна мрежа и аналогов модем.

Call – повикване – двупосочно взаимодействие в реално време между страните по телефонна или IP мрежа.

QoE – Quality of Experience – качество на потребителското изживяване; субективна оценка за възприетото качество на услугата.

NIST – National Institute of Standards and Technology – Национален институт за стандарти и технологии на САЩ.

AIS – Automatic Identification System – автоматична идентификационна система за обмен на навигационни данни.

VTS – Vessel Traffic Service – служба за управление и наблюдение на корабния трафик.

AS – Autonomous System – автономна система; в дисертацията – автономен административен домейн или оператор.

NMEA 0183 – National Marine Electronics Association 0183 – сериен текстов интерфейс, широко използван при AIS и други морски системи.

!AIVDM – Automatic Identification System VHF Data-link Message – NMEA 0183 формат за капсулиране на AIS съобщения.

POP – Point of Presence – точка на присъствие; физическа мрежова точка за достъп и обмен на трафик.

HLS – HTTP Live Streaming – протокол за адаптивно мултимедийно разпространение по HTTP.

STB – Set-top-Box – устройство за декодиране и визуализиране на съдържание на телевизор.

SSO – Single Sign-On – единичен вход; механизъм за достъп до множество приложения с единна автентикация.

VOD – Video on Demand – видео по заявка; модел за избор и гледане на съдържание в избран от потребителя момент.

CDN – Content Delivery Network – мрежа за доставка на съдържание; разпределена инфраструктура за по-бързо и устойчиво обслужване на крайни потребители.

CUDA – Compute Unified Device Architecture – платформа на NVIDIA за паралелни изчисления върху графични процесори.

GPUaaS – GPU as a Service – графичен процесор като услуга; модел за предоставяне на GPU ресурси при поискване.

GeoJSON – Geographic JavaScript Object Notation – JSON-базиран формат за представяне на географски обекти и атрибути.

GIS – Geographic Information System – географска информационна система.

WebSocket – WebSocket – протокол за двупосочна комуникация в реално време между клиент и сървър по една дълготрайна TCP връзка.

VoIP – Voice over Internet Protocol – технология за предаване на глас и мултимедия през IP мрежи.

SIP – Session Initiation Protocol – протокол за сигнализация за установяване, управление и прекратяване на мултимедийни сесии.

WebRTC – Web Real-Time Communication – технология за комуникация в реално време в браузъри и приложения.

RTP – Real-time Transport Protocol – протокол за пренос на аудио и видео в реално време.

SRTP – Secure Real-time Transport Protocol – защитена версия на RTP с криптиране и защита на целостта.

DTLS-SRTP – Datagram Transport Layer Security – Secure Real-time Transport Protocol – механизъм за сигурно договаряне на ключове и защита на медийни потоци.

IPsec – Internet Protocol Security – набор от протоколи за защита на IP комуникация чрез удостоверяване и криптиране.

Opus – аудио кодек с ниска латентност, широко използван при VoIP и стрийминг.

Regional ISP – Regional Internet Service Provider – регионален доставчик на интернет услуги.

Asterisk PBX – Asterisk private branch exchange – софтуерна платформа за IP телефонни централи.

P2P – Peer-to-Peer – децентрализирана архитектура за директен обмен на данни между участници.

ZeroTier – софтуерно дефинирана мрежова платформа за виртуална peer-to-peer свързаност.

Network Performance – производителност на мрежата – съвкупност от показатели за качество, скорост и надеждност на мрежовата комуникация.

Latency – латентност – времево закъснение при преноса на данни между източник и получател.

Jitter – трептене – вариация в закъснението при пристигането на пакетите.

Packet Loss – загуба на пакети – недоставяне на един или повече пакети до местоназначението им.

Фарватер – fairway (англ.), Fahrwasser (нем.), chenal navigable (фр.), vaarwater (нидерл.) – навигационно пригодната и обичайно обозначена част от плавателния път, в рамките на която са осигурени необходимите дълбочина, широчина и безопасни условия за движение на плавателни съдове.

УВОД

Системите за управление на ефективността в мрежите на публичния сектор са изправени пред специфични предизвикателства, произтичащи от разпределеното управление, хетерогенността на участниците и динамично променящите се обществени и политически приоритети. Широкото внедряване и комбиниране на цифрови технологии във всички сфери на обществения и икономическия живот води до цялостно дигитално преобразование, което налага преход от управление на асети към управление на услуги.

Този преход има и по-дълбока историческа логика. В по-ранните етапи на развитие на комуникационните системи беше достатъчно до крайния потребител да бъде осигурена преносна среда, чрез която той да достига до централен изчислителен ресурс. При този модел обработката, съхранението и управлението на данните са концентрирани в центъра, а мрежата изпълнява преди всичко ролята на канал за вход и изход. С нарастването на обема на данните, изискванията към качеството на услугите, необходимостта от сигурност и чувствителността към латентност този модел започва да показва ограничения, които не могат да бъдат преодолени единствено чрез още по-голяма централизация.

Съвременната дигитална трансформация в публичния сектор не се изчерпва с внедряване на отделни технологии, а представлява преосмисляне на начина, по който се планират, предоставят и управляват цифровите услуги. Този преход е особено сложен във федерирани системи, където множество автономни административни, комуникационни и изчислителни домейни трябва да взаимодействат при различни правила на управление, нееднородна инфраструктура и ограничен контрол върху свързаността, сигурността и капацитета.

В традиционния централизиращ модел акцентът е поставен върху самата инфраструктура и върху поддържането на отделни технически компоненти. В модела, ориентиран към услугите, фокусът се измества към стойността за крайния потребител, качеството на предоставяната услуга и способността на системата да използва наличните асети по гъвкав, координиран и мащабируем начин. В такава среда основният въпрос вече не е само кои технологии се използват, а как те се организират така, че крайният

резултат да бъде надеждна, сигурна и икономически оправдана услуга, способна да работи и извън логиката на абсолютната централизация.

По тази причина настоящото изследване разглежда ориентиран към услуги подход, при който изчислителните, мрежовите и организационните асети се предоставят при поискване, комбинират се динамично и се управляват чрез архитектурни механизми, ориентирани към нивото на услугата, а не към отделния хардуерен или софтуерен компонент. В този смисъл дисертационният труд е посветен на преосмисляне на подхода за използване на цифровите технологии при тяхното проникване във всички сфери на икономическия и социалния живот.

Изследванията в дисертационния труд са насочени към разработване на по-ефективни модели за предоставяне на обществени услуги, автоматизирано разгръщане на асети при поискване, оптимизиране на разходите и повишаване на сигурността на услугите във федерирани системи от публичния сектор.

Дисертационният труд разглежда четири представителни класа цифрови услуги: адаптивно мултимедийно разпространение чрез HLS, GPU-базирани изчислителни услуги чрез API и WebSocket, VoIP архитектури с директен медиен обмен и федеративен AIS облак за периферно събиране и обработка на телеметрия в реално време. Тези казуси са различни по приложение, но споделят общи архитектурни проблеми: необходимост от разделение между управляващ слой и слой за данни, работа в хетерогенна и често NAT-ограничена среда, защита на идентичности и данни, както и ефективно използване на ограничени комуникационни и изчислителни асети.

В рамките на настоящото изследване оптимизацията се разбира като инженерно подобряване на прехода към модел, ориентиран към услугите, според няколко основни критерия: намаляване на латентността и подобряване на отзивчивостта на услугите; повишаване на надеждността и устойчивостта при разпределена работа; защита на комуникацията, съдържанието и личните данни; по-ефективно използване на споделени мрежови и изчислителни асети; и организационна приложимост в условията на публичния сектор, включително при ограничени бюджети, наследена инфраструктура и разпределена отговорност.

На тази основа дисертацията търси общи принципи за проектиране и управление на услуги във федерирани среди, вместо да разглежда отделните технологии като самоцел. Основната теза е, че независимо дали става дума за видео стрийминг,

високопроизводителна обработка на данни, комуникация в реално време или морска телеметрия, успешният преход от управление на асети към управление на услуги изисква архитектурно разделение на функциите, динамично осигуряване на асети при поискване, ясно дефинирани граници на отговорност и сигурност, вградена в самия модел на услугата.

В този смисъл представените решения имат двоен характер. От една страна, те адресират конкретни практически проблеми в публичния сектор и в регионални комуникационни среди. От друга страна, те служат като валидиращи казуси за формулиране на по-общ модел за преход от управление на асети към управление на услуги в сложни федерирани системи.

Структура на дисертацията

Дисертационният труд е структуриран в пет глави, увод, заключение, списък на използваните литературни източници и приложения.

В **първа глава** са разгледани историческите, технологичните и организационните предпоставки за дигитализацията на услугите във федерирани системи в публичния сектор. Проследено е развитието на комуникационната инфраструктура, анализирани са основните класове услуги, релевантни за изследването, и е обоснована необходимостта от преход от управление на асети към управление на услуги. В края на главата са формулирани целта, задачите, обектът, предметът и методите на изследването.

Във **втора глава** са разгледани въпросите, свързани със сигурността и надеждността на комуникационните услуги в разпределена среда. Анализирани са ограниченията на RSA при недостатъчна ентропия, аргументиран е изборът на ECC за разглежданите в дисертацията услуги и е очертана перспективата за развитие към пост-квантови криптографски подходи в контекста на защитени цифрови услуги.

В **трета глава** са изследвани подходи за достъп до защитено съдържание, защита на личните данни и сигурно предоставяне на мултимедийни услуги. Разгледани са архитектурни решения за уеб стрийминг, механизми за удостоверяване и криптиране, както и модели за локално и регионално разпространение на съдържание в среда на разпределени мрежи и регионални интернет доставчици.

В **четвърта глава** е изследван преходът към предоставяне на цифрови услуги в публичния сектор чрез три взаимосвързани направления: платформа за административни услуги, високопроизводителни изчислителни услуги и федеративна услуга за събиране и предварителна обработка на потокова телеметрия в реално време. Разгледани са API-базиран достъп до услуги, обработка на големи обеми от структурирани и геопространствени данни, използването на GPU асети като основа за предоставяне на изчислителна услуга при поискване, както и архитектурните принципи на федеративен AIS облак за предоставяне на услуги.

В **пета глава** са предложени архитектурни решения за оптимизиране на прехода от управление на асети към управление на услуги в сложни федерирани системи.

Представени са хибридно VoIP решение за комуникация в среда с NAT ограничения и федеративен AIS облак като модел за оптимизация на предоставянето на навигационна телеметрия като услуга. Акцентът е поставен върху формализацията на ресурсния ефект, върху проблемите, които решенията адресират в реална среда, и върху техния системен ефект, включително в контекста на морската сигурност и на бъдещи приложения като DANRISS 2.

В **заключението** са обобщени резултатите от изследването, формулирани са основните научни и научно-приложни приноси и са очертани насоки за бъдещи изследвания по темата. Представен е списък с научни публикации по темата и забелязани цитирания.

Дисертационният труд съдържа 153 страници, 49 фигури, 6 таблици и 127 литературни източника.

ГЛАВА 1. Дигитализация на услугите във федерирани системи в публичния сектор

1.1. Въведение

Обзорът на настоящата дисертация ще започне по леко нетрадиционен начин. Когато в обществото се говори за дигитализация в публичния сектор, най-често се мисли за е-услуги, онлайн платформи, регистри, мобилни приложения, обществени поръчки и възможността административни дейности да се извършват без посещение на гише. По-задълбоченият поглед обаче показва, че тези видими проявления са само повърхността на много по-сложен процес. Зад тях стоят не само технологии, проекти, администрации и изпълнители, а преди всичко натрупани исторически дефицити, инфраструктурни ограничения, обществени очаквания и нови изисквания към сигурност, капацитет и свързаност. Именно тук възниква същинският въпрос: **кой е двигателят на процесите** на дигитална трансформация в публичния сектор?

Заслужава си този въпрос да бъде разгледан в историческа перспектива. Съвременният човек е свикнал с Интернет до такава степен, че почти не си задава въпроса как тази свързаност изобщо достига до устройството му. Тя се възприема като естествена даденост – в дома, в джоба, на улицата, на работното място – и то с достатъчен капацитет и достатъчно ниска латентност, за да бъдат възможни поточно видео с високо качество, интерактивни услуги и комуникация в реално време. Именно затова Североизточна България е особено показателен пример за регион, в който глобалният технологичен напредък и изградените обществени очаквания дълго време не се материализират в същата степен, както в други части на страната. Изследването (Iliev and Blagoev, 2025) разглежда именно този проблем – ниския капацитет за обмен на данни и високата латентност дори между географски близки точки.

Не е случайно, че в конкретика се спирам именно на този регион. Изборът не се основава само на технически наблюдения, а и на дългогодишно лично опознаване на Северното Черноморие, Дунавския бряг и Делтата – на пътищата, населените места, музеите, забележителностите и обектите от критичната инфраструктура. Освен прякото изследване на автоматичната идентификационна система AIS по море и по Дунав, самото придвижване през тези територии, срещата с техните географски, културни и исторически пластове носят емоционален заряд, който неизбежно участва в изграждането на изследователския мироглед. В този смисъл събирането на данни от AIS

за плавателни съдове и навигационни съоръжения, приемани както от морския, така и от Дунавския бряг, не е само техническа дейност, а част от по-широко и натрупвано с години опознаване на регион със силна историко-географска, инфраструктурна и културна значимост (Фиг. 1.1, Фиг. 1.2).

Фиг. 1.1. Районът на Фар Шабла, изследване на AIS покритието с мобилната установка, включваща AIS receiver Em-Trak R300, VHF23 Marine Antenna и Raspberry Pi 5

Фиг. 1.2. Степна местност в района на нос Калиакра

1.1.1. Исторически предпоставки и натрупване на регионален разлом

До 1989 г. държавната структура „Български пощи и далекосъобщения“ отговаря за пощи, телеграф, телекс и телефон. Телефонното покритие е осигурено на практика на 100% в цялата страна. Няма населено място и адрес без телефон – шахта до всеки блок, комутационен шкаф във всяка отдалечена махала, стълбове – дървени, стоманени, стоманобетонни за телефонни кабели до дворовете на хората, пощенска станция в почти всяко село. Линията от абоната до централата е медна усукана двойка, предава се аналогов глас в честотна лента 300-3400Hz. До 70-те години централите са автоматични, но реализирани с електромеханична релейна логика, след това се цифровизират самите АТЦ с времеделение TDM и PCM канали 64kbps. Цифровото кодиране на звука е G.711, 8bit, 8kHz. Линията до абоната остава аналогова. Именно тогава се появява първият бум и желание у по-събудените граждани за интернет достъп, осъществен с т.нар. dial-up модеми. Тези модеми работят в същата звукова честота като гласа 300-3400Hz, на практика няма значение за централата, дали се предава глас или интернет достъп. Модемът прозвънява специален номер в централата, тя го свързва с модем от модемни банки, започва междумодемен разговор с кодиране FSK / QAM според стандарта V.xx., и след това комуникацията напуска централата, обичайно се пренася по цифрово трасе – ISDN или наета линия до реалното ISP. Респективно, за абонатите от отдалечените села, аналоговият пренос може да премине през няколко пощенски станции, докато стигне централа, цифрово свързана с интернет доставчиците. Постепенно светът се развива, подобряват се стандартите V.xx и се вдигат скоростите на модема. И тук започва да се появява **разлом.**

Държавната структура „Български пощи и далекосъобщения“ след 1990 г. се разделя на „Български пощи“ и „Българска Телекомуникационна Компания“ (Център за изследване на демокрацията, Телекомуникационната политика на България юни 1995 г.), (World Bank – меморандум, март 1993 г.).

Времената са трудни, белязани от края на Студената война, Източният блок се разпада, наличие на множество фалирали предприятия, сериозни нива на инфлация, обезценявания на парите и това е само част от политикономическата картина. Започват да се оформят слаборазвити райони. Емиграцията е огромна, вътрешна – към големите градове и столицата, и външна – към западните страни. При това говорим за емиграция с огромна част от будните хора. В целия този дух на промени, след 90-те години БТК

„забравя“ модернизацията на АТЦ в малките градове и села поради икономическа нецелесъобразност. Същите продължават да функционират с електромеханиката, влияеща пряко върху внасянето на електромагнитни шумове по линията и освен това остават географски далеч от най-близките цифрови централи. Ако в голям град скоростите достигат теоретичните 56 kbit/s при последните генерации dial-up модеми, то в отдалечен район са от порядъци на 1-5 kbit/s. Няма висши образователни и научни институции, няма будни граждани, само местен бизнес, предимно малък, няма го вече интелектуалният двигател, който да изисква високоскоростен интернет. Банковите клонове и държавните администрации използват скъпоструващи ISDN или наети линии, аналогови линии използват по-малки администрации, за които скоростите им са достатъчни, а прекъсванията не представляват сериозна спънка в работата им, на принципа – „и утре е ден“.

Бумът на модемите отшумява в края на 90-те, началото на 2000-те. Това явление е в световен мащаб и напълно обяснимо. Ако до края на 90-те обичайно се разменяха електронна поща, текстови документи, текстов чат, то в края на 90-те вече започнаха да се разпространяват все по-широко мултимедийните формати. Аналоговите линии вече не отговарят на тези нужди на обществото. Един пълнометражен филм в стандартно качество и резолюция при тогавашните схеми за кодиране и компресия се сваля за дни и нощи. Тепърва се появяват и динамичните уеб страници, които изискват презареждане всеки път поради предаване на credentials (пълномощия) за достъп – бисквитки, появява се първообразът на криптираните връзки и използването на цифров сертификат, където времевият прозорец за процеса на удостоверяване е участваща величина и от съществено значение. Това са все тежки обремененост за dial-up връзката.

Традиционните телекоми поеха пътя към цифрови линии до крайния абонат. У нас БТК е приватизирана от Виваком през 2004 г., а през 2006 г. имплементират ADSL услуга в над 140 града (Консолидиран финансов отчет на БТК, декември 2008, публикуван от Vivacom).

DSL използва същите медни двойки, но качва сигнала в по-висок и по-широк честотен диапазон, вече цифрово кодиран с OFDM. Тук се корени историята на появилият се технически термин Broadband Internet. Скоростите се вдигат чувствително до няколко мегабита, но отдалечените райони продължават да са проблемни поради електромагнитна зашуменост по трасетата – самите кабели и връзки са стари, има течове в комутационните шкафове и окислявания. В този период – края на 90-те, началото на

2000-те се появи алтернативен метод за Интернет достъп, белязан от бума на кварталните ЛАН доставчици, които решиха проблема със свалянето на обемни файлове, естествено по неособено законен начин. Идеята е следната – изгражда се Ethernet/Fast Ethernet LAN в даден район по стандарт 10/100 мегабита/секунда, използващ 2 двойки проводници в режим Full duplex TX+/TX-, RX+/RX-,а самият ЛАН доставчик е свързан към телеком. Така услугата им беше двукомпонентна – ЛАН свързаност и Интернет свързаност. Дори имаше тарифа само за ЛАН свързаност, която е от два до три пъти по-евтина от комплекта ЛАН+Интернет свързаността. Кабелите висяха от блок на блок, фасадите бяха „облечени“ с кабели, а където се ползваха шахти, то имаше проблем със законността и правото на използване на готовите кабелни трасета, защото те не бяха собственост на ЛАН доставчиците. Тази част от проблематиката е по-безобидната част и касае територията на общината, където оперират. По-сериозният криминален аспект беше в разпространението на съдържание без платени лицензи (софтуер) и авторски права (музика, филми, др.). Всъщност, първоначалната идея не е в нарушението на правата. Всеки „уважаващ себе си“ ЛАН доставчик поддържаше FTP сървър в мазето си, пълен с музика, филми, софтуер и друго съдържание. Така редуцира интернетския трафик. Вместо всеки потребител да сваля един и същ аудио файл във формат MP3 от интернет с абсолютно същия хеш, при това бавно, всеки би предпочел да го свали от локалния FTP сървър със скорост 80-100 мегабита/секунда. Скорост, която беше недостижима за предлаганите интернет свързаности в дома в онези времена. Нещо повече – в ЛАН имаше и P2P обмен между потребителите – споделени директории (file sharing), DC++ и тн., понеже свързването с потребители на същия физически сегмент (суич, хъб), понякога беше по-високоскоростно от ползването на централизираното FTP през 5 квартала. Колкото до авторските права – ако самият потребител иска да ги наруши, така или иначе ще си намери незаконно съдържание из Интернет. В края на краищата беше по-удобно да се използва ЛАН свързаността, където е достатъчно един потребител да свали съдържание от Интернет бавно и да го предостави за останалите, които ще го свалят от него бързо. Разбира се, като всяко положително нещо, има и отрицателни страни – поради отворения характер на мрежата, за да съществува обменът безпрекословно и без ограничения между потребителите, то разпространението на вируси беше бич за потребителите с по-слаби компютърни познания. Второ – всеки можеше да комуникира по каквито си протоколи поиска. Това е положително – играеха се всякакви мултиплейър игри в ЛАН мрежата, но негативната страна се състоеше в пускане на злонамерен флууд (първообразът на DDOS) без никаква финансова изгода. Тук като тривиално обяснение

бихме приели, че съществуваха особена порода потребители тогава, които бяха социопати в реалния живот, когато тепърва се изграждаше общественият образ на дигитален виртуален свят в мрежата.

На пазара оперираха и трети вид доставчици, които са в нишата между телеком и ЛАН, или поне идеологически са по-близо до телекоми като инфраструктура до крайния клиент. Това са изначално стартирали като класически ТВ доставчици, които впоследствие използват коаксиалната си кабелна мрежа за транспорт на телефония и данни, заедно с аналоговата PAL TV и по-късно цифрова DVB-C телевизия. Става дума за стандарта DOCSIS, при които нови версии се постигат скорости от гигабит и повече. Модулацията е OFDM, като се използват честотни ленти между ТВ каналите за пренос на данни или глас. Въпреки, че днес технологията се смята за отмираща, все още в някои отдалечени райони може да бъде забелязана работеща Интернет услуга по коаксиална ТВ кабелна мрежа (Фиг. 1.3) (КРС, Приложение към Решение № 246/22.02.2011 г.).

Фиг. 1.3. Кафене в гр. Каварна, ноември 2025 г., функциониращ рутер с вграден кабелен модем

Вземайки предвид всичко това, и че правните рамки все повече се насищат в насока – цифровизация, използване на Интернет, права и задължения на доставчици и потребители, около средата на 2000-те започнаха организирани акции на службите. Маскираните отряди провеждаха наказателни акции и нахлуваха по мазетата на всеки ЛАН доставчик, за да изземват оборудвания, съхраняващи и предоставящи незаконно съдържание, както или излъчващи ТВ канали с неуредени права. Народната мъдрост

ясно гласи – което не става доброволно, става с насилствени методи. Останки от такава дейност бяха документирани дори през 2025 г. (Фиг. 1.4).

ГДБОП са претърсвали офис на местна фирма за ТВ и Нет услуги в Балчик

Про Нюз Добрич 21.02.2025 | 12:18 6017

Претърсване в офис на телекомуникационна фирма в град Балчик е било проведено вчера около 10:30 часа, научи от свои източници Про Нюз Добрич. Действията са част от разследване срещу кабелен оператор, заподозрян в незаконно разпространение на телевизионни програми без необходимите права.

Фиг 1.4. ГДБОП и Европол в апартамент на блок, ж.к. Балик, гр. Балчик, превърнато в сървърно помещение на ТВ+интернет доставчик, 20.02.2025 г.

Уж, облечени в правна рамка, тези акции през 2000-те доведоха до следното:

- Упадък на ЛАН доставчиците в края на 2000-те. На практика без FTP и P2P в LAN, те трябваше да вдигат интернет скоростите, за да отговорят на нуждите на потребителите. Така им се спря развитието в посока разширение на мрежата. Нещо повече – незаконните кабели също бяха премахнати. Това допълнително им покачи разходите за изграждане на законна инфраструктура, доколкото това е практически възможно. Като резултат – покритието им се сви, започнаха да разпродават мрежата си на телекомите.
- Изгубили пазарния си дял в края на 90-те, телекомите започнаха да набират скорост след спецакциите, придобивайки квартални ЛАН доставчици с най-ценния актив – клиентите им. Процесът продължи основно цяло десетилетие 2010-2020.

По този начин към края на първото десетилетие на XXI век се оформя устойчива двойнствена картина: от една страна нараства общественото очакване за модерна

цифрова свързаност, а от друга – в редица региони, включително в Североизточна България, се натрупва инфраструктурен и дигитален разлом, който не е преодолян от досегашния модел на развитие.

1.1.2. Преход към широколентова свързаност и съвременна линия на развитие

Още преди най-новата вълна от стратегически проекти в Черноморския регион вече е налице материализирана линия на подводна цифрова свързаност. От 2008 г. между Поти и Балчик функционира Caucasus Cable System (Фиг. 1.5) – приблизително 1200 km подводен оптичен кабел, който осигурява пряка връзка между Грузия и българския бряг. Самото му съществуване е важно, защото показва, че западното Черноморие не е извън големите цифрови коридори, а участва в тях като транзитно пространство между Европа и Кавказ. В същото време този факт не действа като магическа пръчица за преодоляване на вътрешнорегионалния разлом. Наличието на международен подводен кабел не води автоматично до равномерна широколентова достъпност, когато на сушата липсват достатъчно развити локални оптични мрежи и архитектури за изнасяне на услуги по-близо до крайния потребител. По тази причина значението на такива кабели следва да се разглежда двойствено: едновременно като реална стъпка към широколентова свързаност и като напомняне, че транзитната инфраструктура сама по себе си не отменя необходимостта от регионална наземна интеграция.

Фиг. 1.5. Caucasus Cable System, 21.11.2008

Именно на този фон през периода 2010–2020 започва нов етап на развитие, при който техническата еволюция на мрежите и външните икономически и геополитически

фактори постепенно променят условията за преодоляване на натрупания регионален разлом. Резюмето на десетилетието 2010-2020 в обобщен вид:

- Преход от медна свързаност (UTP, коаксиален кабел) към FTTH пасивна оптика по някой от PON стандартите GPON, EPON, XGPON (КРС, Определяне, анализ и оценка на ПАЗАРА НА ЕДРО НА ЛОКАЛЕН ДОСТЪП В ОПРЕДЕЛЕНО МЕСТОПОЛОЖЕНИЕ), (Министерство на транспорта и съобщенията, National Broadband Infrastructure Plan for Next Generation Access Decree № 435/ 26.06. 2014), (Valentina Petrova, 2018).
- Поради изчезването на традиционната аналогова телефонната услуга, а от друга страна слаб интерес към VDSL, тъй като този стандарт вече не може да отговори на потребностите на десетилетието, БТК закрива АТЦ-та, оттам VDSL достъп на практика няма. Отрязани са цели райони, които навремето са имали само телефонна услуга, днес нямат достъп до Интернет.
- Бившите ЛАН доставчици, вече известни като местни ISP трудно разширяват мрежата си. Цените са високи за крайния клиент, оттам – по-малко потребители, а оттам по-бавно разширение на мрежата, ниски скорости.
- ЛАН достъпът между точки еволюира в корпоративна услуга с права и задължения между страните клиент-доставчик. Поддържат го определен кръг доставчици. Физически LAN или VLAN услуги се явяват лукс за обикновени потребители. Алтернатива за ЛАН свързаност между обикновени потребители е възможна с VPN механизми през Интернет.

Водейки се от икономическите фактори, слаборазвитите райони биха останали без Интернет или адекватен такъв, отговарящ на съвременните потребности още дълго, докато свят светува. Но по правило – глобалните фактори променят картината. Тъй като беше поставен въпроса – кой е двигателят на процесите, настоящото десетилетие е едва преполовено, а на преден план изпъкват 2 големи фактора – Глобалната пандемия, причинена от КОВИД 19 и пълномащабната военна операция в Украйна.

Първата стъпка към целта – интернет покритие за малки населени места, е направена по време на Пандемията. И тя не е значима толкова като действия при доставчиците, колкото се създава психологически ефект у тях. Много хора се завръщат по родните си места, или избират спокойствието на селото, за да работят отдалечено. Голяма част са изгубили реална представа за родните си места, понеже посещенията им са главно по празници или отпуски, т.е. с цел почивка, а не с цел работа. И така се наложи

да се сблъскат пряко с дигиталния упадък на района си. Нещо повече – преди 20 г. те евентуално са били интернет ентусиасти или геймъри, не им е трябвал интернет за професионални цели, нито им е зависело препитанието от него, приемали са нещата такива, каквито са – с всичките позитиви и негативи, които обрисувахме – било в конкретиката на dial-up, ADSL, интернет по LAN или коаксиален ТВ кабел. И така през 2020 г. се сблъскват с проблеми, които са неприемливи за съвремието, но са факт. Първото и най-елементарно, с което се сблъскаха работещите отдалечено по естествен път, бяха трудностите по време на отдалечена среща или разговор (meeting, call). Дистанционните обаждания станаха такъв хит, че по време на Пандемията заемаха почти цялото работно време на служителите. В технически аспект, платформите за meeting – Teams, Zoom, Google Meet и тн. изискват голям капацитет за високо качество, а и отварят голям pool от TCP криптирани сесии. При струпване на много потребители в обаждане в рамките на един доставчик, нерядко се случва да се достигнат лимитите на сесии при доставчика и в резултат на това се появяват прекъсвания. Второ – качеството се превключва на по-ниско с цел пестене на капацитет. И трето – разработчиците на платформите умишлено са избрали подход с много сесии, точно да се справят в среда на малки доставчици. Ако връзката беше по класическия подход – една сесия, тогава прекъсванията биха били още по-осезаеми, понеже установяването на нов канал отнема време. Очевидно – балансът брой сесии/капацитет не е панацея и доставчиците не бяха подготвени за завръщането на хората.

Но КОВИД вълната попремина и внесените подобрения при доставчиците бяха откъслечни и мимолетни. Повече с цел спасяване и закърпване на текущото положение, отколкото изграждане на визия за бъдещето. И тогава се появи на сцената доста по-сериозен фактор, а именно – пълномащабната военна операция в Украйна. След нейното начало въпросът за оптичната и широколентовата свързаност придобива и ясно изразено измерение на устойчива гражданско-военна инфраструктура. Комуникационните мрежи и транспортните системи обслужват едновременно гражданските услуги и действията при криза, поради което НАТО ги разглежда като ключови елементи на националната устойчивост, а експертните форуми ги описват като част от сложни гражданско-военни системи (NATO, 2024).

1.1.3. Морска сигурност, подводна свързаност и Черноморски хъб

В този контекст въпросът за свързаността престава да бъде обсъждан само в технически или пазарен аспект и преминава в полето на морската сигурност (Съвет на Европейския съюз, 2025). В официалната рамка на Европейския съюз морската сигурност обхваща не само сигурност и отбрана, включително киберсигурност, но и критична инфраструктура, риболов, търговия и корабоплаване, енергетика, транспорт и туризъм. Същата рамка подчертава, че над 80% от световната търговия се осъществява по море и че до 99% от глобалните потоци от данни се предават по подводни кабели. Това означава, че широколентовата и оптичната свързаност по Черноморието не може да бъде разглеждана само като удобство за крайния потребител, а като част от по-широка система на икономическа, технологична и стратегическа устойчивост.

Именно затова новият стратегически подход на ЕС към Черноморския регион поставя на преден план идеята за Black Sea Maritime Security Hub (EU strategic approach to the Black Sea region, 2025). В тази рамка хъбът е мислен като инструмент за повишаване на морската ситуационна осведоменост, обмен на информация в реално време, защита на критичната морска инфраструктура и разширяване на координацията между крайбрежните държави и бреговите служби. Изрично е посочено, че той следва да подпомага наблюдението от космоса до морското дъно и да защитава инфраструктура като офшорни инсталации и подводни кабели. По този начин Черноморският хъб не е странична политическа инициатива, а институционална рамка, в която цифровата свързаност, морската сигурност и регионалната устойчивост се събират в една обща логика.

На този фон е уместно развитието на подводната черноморска свързаност да се представи като последователна еволюция, а не като единичен инфраструктурен акт. Ако Caucasus Cable System маркира по-ранния етап на директна връзка между грузинския и българския бряг, то Kardesa (Submarine Networks, 2026) вече се очертава като следващо поколение проект, който разширява хоризонта към по-цялостно западно черноморско окабеляване. Според официалната комуникация на Vodafone (Vodafone Group, 2025) Kardesa е нов висококапацитетен кабелен проект с точки към България, Грузия, Турция и Украйна, с капацитет над 500 Tbps и с амбиция да създаде нов цифров коридор между Европа и Азия (Фиг. 1.6.). В специализираното инфраструктурно отразяване проектът е описан и като нова цифрова високоскоростна магистрала „digital highway“ и катализатор

за регионален растеж „catalyst for regional growth“. В академичния текст това позволява да покаже преходът от единичен подводен маршрут към по-широка концепция за черноморска цифрова мрежа.

Фиг. 1.6. Карта на трите оптични трасета в Черно море релевантни към Black Sea Maritime Security Hub, източник на графиката: submarinecablemap.com

На сушата същата логика вече намира израз и в национални проекти за довеждаща и регионална инфраструктура. През юли 2025 г. в предаване по БНР бяха проведени интервюта с жители и кметове на села и малки градове, в които достъпът до интернет остава единствен чрез мобилно покритие и зависим от локални особености на релефа. Именно на този фон Виваком обявява мащабен проект за изграждане на високоскоростна оптична инфраструктура в над 150 малки населени места и общински центрове в Североизточна и Югоизточна България, както и към стратегически гранични пунктове, с финансиране по националния план за възстановяване и устойчивост ПВУ чрез NextGenerationEU (Vivacom, 2025). В инфраструктурно отношение тези два района се очертават не просто като зони на покритие, а като регионални оптични пръстени с морски разклонения. При Североизточна България особено значение има и оформянето на свързващото ребро Дунав – Черно море, което придава на проекта не само социално, но и ясно транспортно, логистично и стратегическо измерение. Така сухоземната оптична експанзия може да бъде прочетена не като изолирана социална мярка, а като естествено наземно продължение на подводните цифрови магистрали и като предпоставка за изграждане на по-плътна регионална архитектура от тип оптичен пръстен. Фигури 1.7, 1.8, 1.9 показват моменти от работата на терен.

Фиг. 1.7. Полагане на HDPE тръба и оптичен сноп по магистрално трасе Варна – Балчик – ГКПП Дуранкулак, с. Хаджи Димитър, община Каварна, ноември 2025 г.

Фиг. 1.8. Подготовка за полагане на оптично магистрално трасе Тутракан – Дулово – Тервел – Добрич, община Главиница, декември 2025 г.

Фиг. 1.9. Сплайсинг за ШМ (шахта-муфа): разклонение от магистрално трасе Варна – Балчик – ГКПП Дуранкулак, с. Оброчище, община Балчик; начало на клон за Добрич, януари 2026 г.

Линията на развитие показва преход от ранни форми на интернет достъп – dial-up, ограничено LAN и кабелно покритие, а в по-късен етап и частично FTTH PON – към нов етап на мащабно оптично изграждане. Ако в предходните периоди свързаността се характеризираше с ниски скорости, високи месечни разходи и неравномерно териториално покритие, то в настоящия етап се наблюдава опит за стратегическо преодоляване на този разлом чрез инфраструктурен проект с широк регионален обхват. Поради това трасето следва да се разбира не само като телекомуникационно разширение, а и като част от по-широка логика на устойчивост, морска сигурност и защита на

гранични и стратегически райони, в които са разположени обекти със значение за националната сигурност, включително военни бази, радиолокационни системи и други елементи на критичната инфраструктура.

Така описаната инфраструктурна и стратегическа трансформация създава условия мрежата да престане да бъде само транспортна среда и да се превърне в основа за изнасяне, координация и федерация на цифрови услуги.

1.2. От управление на комуникационни асети към управление на услуги

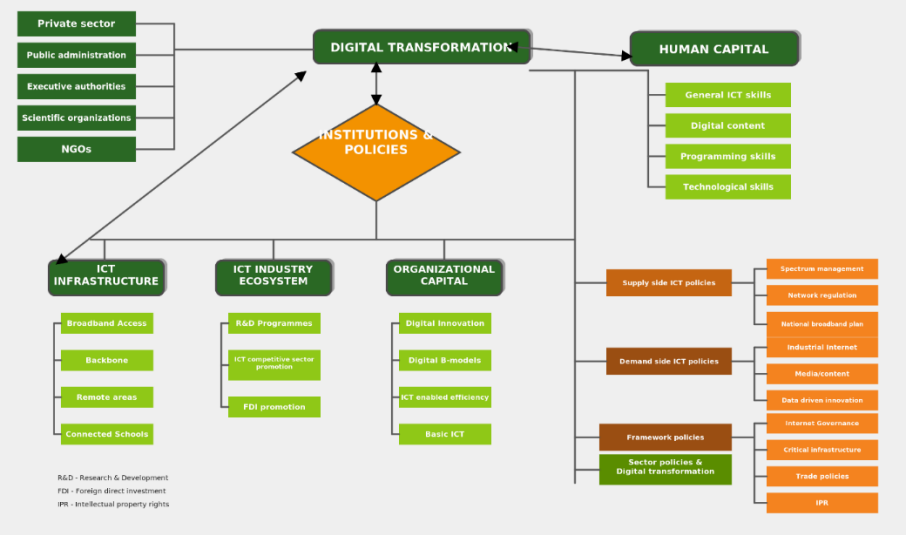
Историческото развитие на комуникационните системи показва, че в ранните етапи на цифровизацията основната задача е била да се осигури достъп от крайния потребител до централен изчислителен ресурс. При този модел обработката на данните, съхранението на файловете и логиката на приложенията са концентрирани в центъра, докато крайната точка изпълнява предимно ролята на средство за вход и изход. В този смисъл мрежата се възприема основно като преносна среда, а не като среда, в която самата услуга може да бъде организирана по разпределен начин.

Тази логика ясно се вижда както при мейнфрейм системите и отдалечените терминали, така и при по-късните модемни връзки. Първоначално модемът по същество продължава ролята на отдалечения терминал – крайното устройство осъществява връзка с конкретна система, към която подава команди и данни, а резултатът се формира и връща от центъра обратно към крайното устройство. С развитието на V.xx стандартите се извършва съществен архитектурен преход: физическата телефонна линия престава да служи само за връзка с точно определен сървър и започва да пренася логически мрежови връзки, така върху една и съща физическа среда става възможно капсулиране на мрежови протоколи, получаване на мрежова адресация и достъп до множество различни услуги и крайни точки, а не само до един централен хост. Именно този преход превръща модемната връзка от средство за терминален достъп в потребителски ориентиран мрежов интерфейс за уеб, електронна поща и други интернет приложения.

В ранните етапи на развитие и употреба на класическите клиент–сървър приложения, включително уеб приложенията, латентността и капацитетът дълго време

не се възприемат като определящи ограничения. Когато крайната точка служи основно за достъп до централизирана система, а услугите са сравнително леки, наличната инфраструктура, дори телефонните линии, е достатъчна. С навлизането на мултимедийни формати, интерактивни услуги, реалновремеви комуникации, големи масиви от данни и чувствителни към закъснение приложения, този централизиращ модел започва да разкрива своите ограничения. Не всяка услуга може да бъде предоставяна ефективно, когато всички данни, всички функции и всички управленски механизми са концентрирани в един център.

Точно тук се проявява и описаният в дисертационния труд регионален разлом. Докато в едни зони комуникационната инфраструктура се развива сравнително бързо и последователно, в други – включително в Североизточна България – дълго време се натрупва изоставане по отношение на широколентовата свързаност, капацитета и качеството на услугите. В съвременните условия този разлом започва да се запълва под въздействието на нови икономически, технологични и геополитически фактори, включително развитието на регионална оптична инфраструктура, необходимостта от устойчива цифрова свързаност и потребността от по-гъвкави модели за предоставяне на услуги.



Фиг. 1.10. Дигитална трансформация, с основните участници и тяхната взаимосвързаност– източник: Министерство на транспорта и съобщенията, Digital Transformation of Bulgaria for the Period 2020-2030.

Показаната на Фиг. 1.10 взаимосвързаност между основните участници в процеса на дигитална трансформация е особено важна за настоящото изследване. Тя показва, че съвременните цифрови услуги не възникват в изолиран център, а в среда на зависимост между инфраструктура, институции, доставчици и крайни потребители. Именно затова фокусът постепенно се измества от управление на отделни асети към управление на услуги, а в по-сложните случаи – към федеративни модели на взаимодействие. Това развитие води до архитектурно противопоставяне между познатия централизиращ модел и по-новите service-centric и федеративни подходи.

Централизацията не изчезва като принцип, но престава да бъде универсално решение.

Когато услугите стават чувствителни към латентност, обемът на пренасяните данни нараства, а регионалната инфраструктура придобива достатъчен локален капацитет, все по-логично е част от функциите да се изнесат по-близо до източника на данни или до крайния потребител. В този смисъл мрежата престава да бъде само транспортен канал към централен ресурс и започва да се превръща в среда за организиране на самите услуги.

Подобна практическа фаза на преход към service-centric среда се наблюдава в Румъния, където трансформацията на морските възли все по-ясно се обвързва не само с инфраструктурно разширяване, а с изграждане на цифрови услуги, базирани на непрекъснат поток от данни, предсказващ мониторинг и обработка в реално време. Burmambet отбелязва, че в Констанца се наблюдава постепенен, но стратегически напредък към дигитализация чрез IoT-базирани системи за проследяване, AI-ориентирано управление на трафика, развитие на платформи за данни в реално време и отдалечен мониторинг за управление на флот и инфраструктура, както и усилия за Port Community System, насочени към консолидиране на информационните потоци и намаляване на бумацината (Burmambet, 2025). На по-общо равнище Gasparotti, Попеску и др. разглеждат румънските морски пристанища през логиката на smart-port трансформацията и подчертават, че автоматизацията, дигитализацията, IoT, киберсигурността, интегрираните цифрови платформи и мониторингът в реално време са именно онези механизми, чрез които инфраструктурата престава да бъде само физическа среда за пренос и започва да функционира като среда за координирани услуги, данни и оперативни процеси (Gasparotti et al., 2026). В този смисъл румънският пример е

важен не толкова като транспортна аналогия, а като свидетелство, че при достатъчно зряла инфраструктурна и организационна среда преходът от asset-centric към service-centric логика вече навлиза в практическа фаза.

Именно тук възниква преходът от управление на комуникационни асети към управление на услуги. В традиционния модел основен фокус са отделните асети – линии, маршрутизатори, приемници, сървъри, точки за достъп. В service-centric модела фокусът се измества към начина, по който тези асети се комбинират, координират и предоставят като цялостна услуга с определени характеристики – сигурност, надеждност, отзивчивост, мащабируемост и организационна приложимост. Това означава, че не е достатъчно да съществува свързаност; необходимо е тя да бъде организирана така, че да поддържа реални цифрови функции при различни ограничения и изисквания.

Федерираните архитектури се явяват естествен отговор на тази промяна. Те позволяват различни автономни участници да запазят част от своята независимост, но същевременно да предоставят услуги съвместно чрез споделени правила, интерфейси и механизми за доверие. По този начин се преодолява едновременно ограничението на абсолютната централизация и слабостта на напълно разпокъсаните локални решения. Точно тази логика се проследява и в следващите глави на дисертационния труд – от криптографската основа на удостоверяването и сигурния достъп, през защитено видео разпространение и изчислителни услуги при поискване, до реалновремеви комуникации и федеративен облак за AIS телеметрия.

В тази дисертация се разглеждат следните четири класа цифрови услуги:

1. адаптивно мултимедийно разпространение по HTTP (HLS), при което защитата на съдържанието и удостоверяването чрез трета страна изграждат техническата основа за кооперативен модел между правоносител, регионален разпространител и краен потребител;
2. високопроизводителни изчислителни услуги с GPU ускорение, предоставяни чрез програмни интерфейси като услуга при поискване за обработка на големи геопространствени масиви от данни;
3. VoIP услуги в реално време, при които централизираното управление на сигнализацията се комбинира с директен P2P пренос на медия в контролирана и криптографски защитена мрежова среда;

4. федеративен AIS облак, в който приемането, пречистването, маршрутизирането и предоставянето на навигационна телеметрия се реализират като координирана разпределена услуга.

Стандартите (RFC, ITU-R, NIST) се използват като референтни източници за протоколи и архитектурни дефиниции.

1.3. Федерирани системи

Федерираните системи са архитектури, в които независими и автономни организации или системи си сътрудничат за постигане на общи цели. Тези системи позволяват на различни организации да споделят ресурси, информация и услуги, без да е необходим централизиран контрол (Gu Z et al., 2024).

Същност и роля на федерираните системи:

- Децентрализация: Федерираните системи избягват централизирана структура, като позволяват на участниците да запазят автономност.
- Оперативна съвместимост: Те улесняват оперативната съвместимост между различни системи и организации, дори когато използват различни технологии или стандарти (Buyya et al., 2010).
- Сигурност и доверие: Чрез установяване на стандартни политики и протоколи, федерираните системи осигуряват сигурен обмен на информация между участниците (Bernsmed et al., 2012).

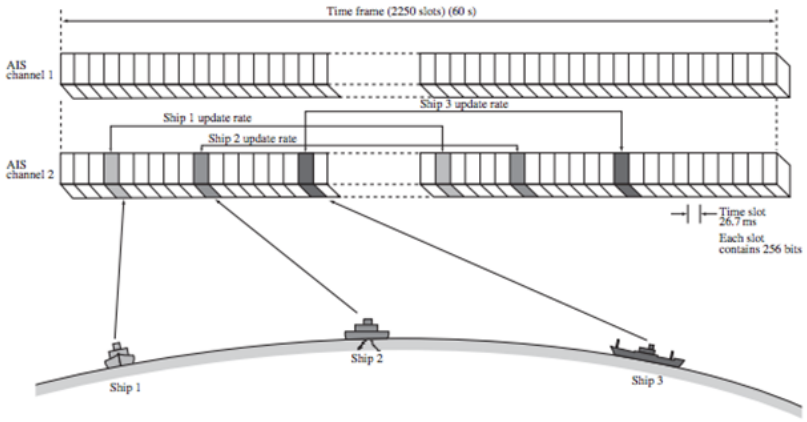
Проблеми, които федерираните системи решават за организациите:

- Оперативна съвместимост на системите: Позволяват интеграция на различни ИТ системи, което улеснява обмена на данни и услуги между организациите.

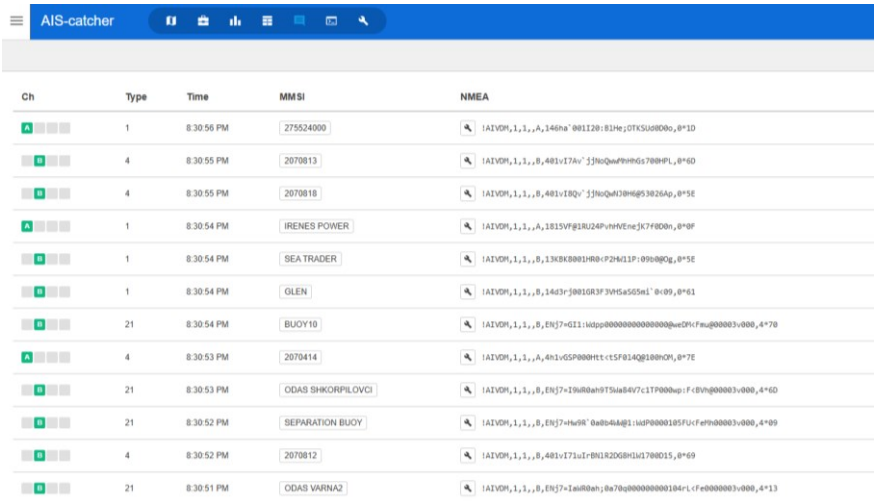
- Управление на идентичността: Федерираните системи предоставят механизми за унифицирано управление на потребителските идентичности, намалявайки необходимостта от множество входове и пароли.
- Сигурност на данните: Чрез споделени стандарти и протоколи те осигуряват сигурен обмен на информация между участниците.
- Намаляване на разходите: Споделянето на ресурси и услуги между организациите води до оптимизиране на разходите и повишена ефективност.

Пример на федерирана система

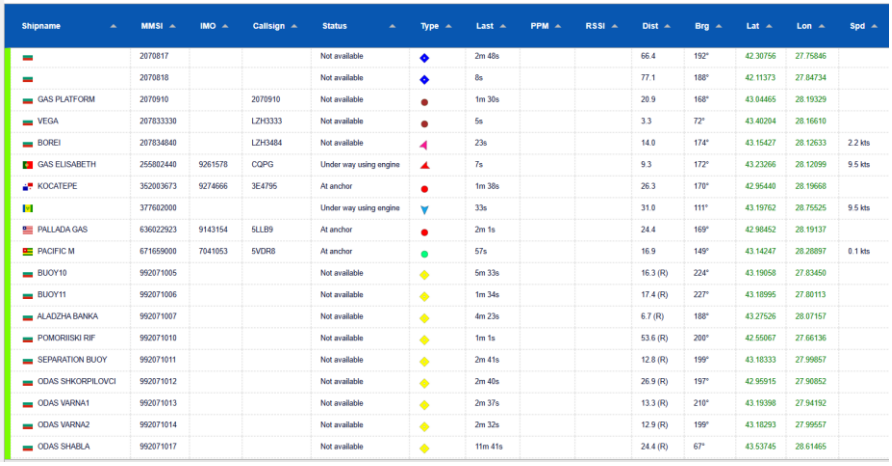
Като пример на федерираната система може да се посочи автоматична идентификационна система AIS – Automatic Identification System. AIS е критична система за морска ситуационна осведоменост и безопасност, в която корабите и бреговите станции обменят стандартизирани съобщения по VHF с TDMA достъп (ITU-R Recommendation M.1371), (Фиг. 1.11). На брега данните обикновено се приемат от радиоприемник и се предоставят към софтуер като текстови NMEA 0183 sentences (изречения), най-често `!AIVDM/!AIVDO` (Фиг. 1.12), които могат да бъдат пренесени по сериен порт RS232, USB или по IP мрежа към интернет платформи (NMEA 0183 Interface Standard).



Фиг. 1.11. AIS слотове, принципи на TDMA (Wu, Daniel & Aarsnes, Marion, 2017)



Фиг. 1.12. NMEA 0183 изречения, приети от лична AIS станция в района на гр. Балчик



Фиг. 1.13. Извадка от статистика на приема – базови станции, плавателни съдове, знаци

Т.нар. marine платформи (напр. MarineTraffic, AISHub и тн.) стъпват върху краудсорснат “сензорен слой”: те агрегират AIS съобщения от разпределена мрежа наземни приемници, които в голяма степен се поддържат от оператори в общността. Практическият модел е „даваш покритие (Фиг. 1.13) → получаваш стойност“: доброволци инсталират и държат онлайн AIS станция и подават поток (фийд) към платформата, а в замяна получават привилегии (достъп/планове/признание), а понякога и оборудване след подбор. Това позволява на платформата бързо да разширява покритието по крайбрежията, без да изгради физически всяка точка сама (D. Memos, 2017).

Моделът „станция → платформа“ е успешен поради ниския праг за участие: потребителят често трябва само да свърже приемника и да настрои адрес/порт. При по-

сложни инсталации обаче се появяват системни ограничения: 1) множество приемници в близък район слушат едни и същи съобщения и генерират дубликати; 2) нестабилни домашни ISP връзки правят UDP доставка ненадеждна; 3) разрастващите се платформи трябва да инвестират в edge ingestion и тежка дедуп инфраструктура; 4) възниква нужда от по-гъвкаво рутиране (към различни цели, през различни посредници) и отчетност.

Целта на един федеративен облак е да предложи междинен слой: да „събере“ множество физически станции в един логически фийд, да премахне дубликатите максимално близо до източника и да достави чист поток към платформи – без да изисква от крайния потребител да изгражда сложни тунели или да управлява сървърна инфраструктура.

Наземният (terrestrial, shore-based) AIS е проектиран като „реална картина“ в рамките на VHF радиохоризонта: корабите и бреговите станции обменят динамични репорти с честота от няколко секунди до минути, като за тактически задачи (наблюдение в близка околност, VTS) се изискват обновявания от порядъка на 2–10 s. На практика качеството на крайбрежната „AIS картина“ зависи силно от плътността и разположението на наземните приемници (антена/приемник/линк): повече точки на прием редуцират сенките от релеф, увеличават вероятността за прием при ниско SNR и осигуряват по-равномерна „свежест“ на потока. Цената на това са повече дубликати, които трябва да се отстраняват възможно най-близо до източника, преди публикуване към платформа (European Commission (EC) No 415/2007), (Plass et al., 2015).

Сателитният AIS (S-AIS) е силно допълващ — дава глобалност там, където липсва наземна инфраструктура, но има вродени ограничения в натоварени райони. Те са свързани с ограничена „навременност“ поради непостоянна видимост и допълнителни стъпки по детекция/обработка/доставка, и по-ниска вероятност за декодиране заради ниска приета мощност и висока колизионност: TDMA механизмът е оптимизиран за ship-to-ship/ship-to-shore, а големият сателитен footprint събира множество независими „локални“ TDMA домейни, които преизползват слотове и се „сблъскват“ на приемника (Kapeliaris et al., 2023), (Šakan et al., 2018), (IALA Recommendation A-124).

1.4. Характеристика на разглежданите услуги

1.4.1. HLS – адаптивно мултимедийно разпространение

Разглежданата в дисертационния труд HLS услуга има две взаимосвързани части. Първата част е насочена към сигурното предоставяне на уеб видео стрийминг през интернет, при което удостоверяването на крайния потребител се изнася към външна услуга за доверие. По този начин самото съдържание и процесът по идентификация и оторизация се разделят функционално, което позволява видео дистрибуторът да не обработва чувствителните лични данни на потребителите, а достъпът до защитеното съдържание да се реализира чрез удостоверяване през трета страна и контролирано предоставяне на ключов материал.

Втората част е насочена към локално и регионално разпространение на същата услуга в среда на регионален интернет доставчик, където външната интернет свързаност може да е ограничена, а локалната PON инфраструктура да разполага със значително по-висок капацитет. При такъв сценарий доставчикът може да приеме един висококачествен входящ поток и да го преразпространи локално чрез multicast, така че да се намали външният трафик и едновременно с това да се осигури гледане с по-високо качество в локалната мрежа.

Тази логика има историческа аналогия с модела на LAN доставчиците от края на 90-те и началото на 2000-те, при които локалната мрежа се използваше за по-бърза дистрибуция на съдържание в сравнение с външния интернет. В разглеждания тук случай обаче подходът е реализиран в рамките на законна и регламентирана услуга, при която регионалният оператор не разпространява произволно съдържание, а работи в кооперативен модел с правоимащата страна. Техническото сърце на тази кооперативност е схемата за удостоверяване и управление на ключове: дори когато криптираният трафик достигне до абонатната точка, неоторизиран потребител не може да го декриптира без валидно удостоверяване и получаване на съответния персонализиран ключ.

В този смисъл HLS услугата в дисертационния труд не се разглежда само като протокол за адаптивно мултимедийно разпространение, а като архитектурен модел, който съчетава удостоверяване през трета страна, криптиране на съдържанието, контрол на достъпа и ефективно използване на локалния капацитет в регионална мрежова среда.

1.4.2. CUDA анализи през API/WebSocket – „GPU като услуга“

CUDA е паралелна платформа и програмен модел за общо предназначение изчисления върху GPU, предназначена да ускорява изчислително-интензивни задачи чрез масивен паралелизъм (Nickolls et al., 2008). Когато CUDA се предлага като услуга, контролният слой обичайно е реализиран чрез API, а двупосочните канали за статус/телеметрия често се реализират с WebSocket за ефективни съобщения над TCP (Fette and Melnikov, 2011). Входно-изходните данни се пренасят отделно (напр. обектно съхранение или стрийминг), за да не се „заключи“ контролният канал.

В разглеждания сценарий входните данни за GPU обработка са големи GeoJSON файлове, които описват геопространствени обекти (Feature/FeatureCollection) и атрибути. (Butler et al., 2016). На практика парсингът/валидацията и преобразуването към компактно бинарно представяне (напр. WKB/Arrow) често се изпълняват на CPU, докато числените геометрични операции (филтриране, трансформации, пространствени индекси и joins) се ускоряват на GPU чрез паралелни ядра, с внимание към разхода за пренос на данни host↔device.

1.4.3. VoIP direct P2P – комуникация в реално време

VoIP технологиите се превърнаха в жизненоважен инструмент за корпоративна комуникация, позволявайки оптимизиране на разходите и безпроблемна интеграция с множество цифрови услуги. Качеството им обаче силно зависи от интернет инфраструктурата, което създава предизвикателства за използването им в региони с ограничени ресурси. Това изследване разглежда основните проблеми, свързани с внедряването на VoIP телефония в среда с регионални доставчици на интернет услуги, липса на публични IP адреси, невъзможност за изграждане на MAN връзки и повишена латентност. Като решение се предлага хибридна архитектура, при която Asterisk PBX в център за данни изпълнява функцията на централен SIP сървър. В същото време, RTP аудио потоци се предават по peer-to-peer модел през защитени тунели. Валидирането на подхода е извършено чрез експериментални измервания на латентност, трептене и загуба на пакети, както и чрез анализ на SIP и RTP трафик с Wireshark. Резултатите показват, че архитектурата позволява надеждна VoIP телефония с високо качество на разговорите, въпреки ограниченията на регионалните интернет доставчици, и може да бъде внедрена като модел за други организации с подобни предизвикателства.

Предложената VoIP архитектура е насочена към сценарий, при който организационно свързани, предварително известни локации трябва да осъществяват разговори в реално време при ограничения на регионалната интернет среда. При този модел централната инфраструктура изпълнява функциите по сигнализация, управление на сесиите и прилагане на политики, докато преносът на медията се реализира по директен peer-to-peer път между крайните точки. Това намалява натоварването върху централния сървър и съкращава пътя на аудио трафика, което е особено важно при чувствителни към закъснение услуги. В уеб контекста WebRTC предоставя утвърден сигурен медиен стек, при който RTP потоците се защитават чрез SRTP, а ключовете се договарят чрез DTLS-SRTP (Rescorla, 2021), (Baugher et al., 2004), (McGrew and Rescorla, 2010). Кодекът Opus е широко използван при интерактивна реч поради своята адаптивност и устойчивост при загуби на пакети (Valin and Vos, 2012). В организационен контекст такава архитектура може да се разглежда като хибриден модел, при който централизираната сигнализация се съчетава с директен медиен обмен върху вече изградена и криптографски защитена IP свързаност между локациите (Kent and Seo, 2005), (Kaufman et al., 2014).

1.4.4. Федеративен AIS облак – периферно събиране и федерация на телеметрия

AIS (Automatic Identification System) е VHF базирана TDMA система за идентификация и обмен на навигационни съобщения; Rec. ITU-R M.1371 описва техническите характеристики и формата на съобщенията (ITU-R M.1371-5, 2014). Наред с ролята на NMEA 0183 като стандартен формат за пренос на навигационни съобщения, съществуват и подходи, при които самата протоколна информация се използва като източник за повишаване на точността на навигационната оценка. Bao et al. предлагат MT-e&R – допълващ NMEA протокола алгоритъм за високоточна навигация, базиран на оценка на GNSS грешката чрез multitask learning, като показват, че NMEA потокът може да има стойност не само като транспортен интерфейс, но и като вход към по-висок слой на аналитична обработка (Bao et al., 2022). Това е още един аргумент, че при федеративен AIS облак ранната нормализация и запазването на семантично значимите полета в телеметрията имат значение не само за маршрутизацията и дедупликацията, но и за последващи интелигентни навигационни услуги. В контекста на настоящата дисертация федеративният AIS облак надгражда физическия слой чрез разпределено събиране от

множество приемни точки, нормализация, пречистване и дедупликация на съобщения, добавяне на метаданни и маршрутизация към множество цели или абонати.

Ключова роля в този модел има периферната обработка, разбирана като изнасяне на част от изчислителните и логическите функции по-близо до източника на данни. В литературата тази парадигма е известна като edge computing и се свързва с намаляване на латентността, ограничаване на излишния трафик към централната инфраструктура и по-бърза реакция в разпределени среди (Shi et al., 2016), (Satyanarayanan et al., 2017). В случая с AIS това означава, че първичните функции по приемане, нормализация, времево подреждане и предварителна дедупликация могат да се изпълняват близо до точката на приемане, преди потокът да бъде препратен към по-горни нива на федеративната система.

Архитектурно този подход комбинира именно принципите на периферната обработка с федеративни облачни модели, при които автономни домейни координират услуги и политики, без да се отказват напълно от собствената си независимост (Lee et al., 2020). По този начин федеративният AIS облак не представлява просто централен агрегатор на потоци, а координирана разпределена услуга, в която различни участници могат да изпълняват отделни роли по приемане, пречистване, пренос и предоставяне на данни.

В контекста на потоковата обработка на неограничени и потенциално непоследователно пристигащи събития особено значение имат семантиките за event-time и прозорците за обработка, тъй като именно те позволяват коректна дедупликация, агрегиране и синхронизация между различните източници (Akidau et al., 2015). Това прави федеративния AIS облак не само комуникационна, но и изчислително-организационна архитектура за управление на навигационна телеметрия в реално време.

1.4.5. Сравнителна таблица

Характеристиките на разглежданите услуги могат да бъдат обобщени в сравнителен вид, така че по-ясно да се открояят техните различни оптимизационни цели, изисквания към латентността и ролята на разделението между управляващите функции и полезния трафик (Таблица 1.1).

Таблица 1.1. Съпоставка между разглежданите класове цифрови услуги

Клас услуга	Основна оптимизационна цел	Тип на потока/ обработката	Разделение на функциите	Толеранс към латентност	Федеративен потенциал
HLS видео услуга	Устойчиво потребителско изживяване и контрол върху достъпа до съдържание	Сегментиран мултимедиен поток по HTTP	Разделение между доставка на съдържание, удостоверяване и предоставяне на ключов материал	Секундна латентност е допустима	Възможно е регионално разпространение и кооперативен модел между правоносител, разпространител и краен потребител
GPU услуга при поискване	Съкращаване на времето за изпълнение на изчислително-интензивни задачи	Пакетна или заявъчна обработка на големи геопространствени данни	Разделение между контролен интерфейс (API/WebSocket) и пренос/обработка на данните	По-висока латентност е допустима	Може да еволюира от централизирана към федеративна услуга при нарастване на обхвата
VoIP услуга в реално време	Минимизиране на латентност, трептене и загуба на пакети при разговор	Непрекъснат двупосочен медиен поток	Разделение между SIP сигнализация и RTP пренос на медия	Много ниска латентност е критична	Поддържа хибридно съчетание на централно управление и пряк пренос между крайните точки
Федеративен AIS облак	Близост до източника, дедупликация и координирано споделяне на телеметрия	Непрекъснат поток от събитийни навигационни данни	Разделение между управляващ слой и слой за данни, както и между роли за приемане, дедупликация, транзит и доставка	Ниска латентност и устойчивост на потока са важни	По замисъл представлява федеративна услуга между множество автономни системи

1.5. Анализ на сходства и различия на разглежданите услуги

Четирите класа услуги се различават по оптимизационна цел и допустими компромиси. HLS оптимизира устойчивото потребителско изживяване (QoE) чрез сегментиране, буфериране и CDN кеширане, като приема секундни латентности и вариации на пропускателната способност. CUDA-as-a-service оптимизира време за изпълнение на паралелни задачи чрез масивен хардуерен паралелизъм и често отделя контролния канал (API/WS) от преноса на обемни данни (напр. големи GeoJSON обекти) (Nickolls et al., 2008), (Fette and Melnikov, 2011), (Butler, et al., 2016). P2P VoIP оптимизира end-to-end латентност и jitter в контролирана топология от предварително известни точки, свързани чрез ZeroTier и допълнителен IPsec слой; директната медийна връзка между локациите намалява натоварването на централата (Rescorla,2021), (Baugher et al.,

2004), (McGrew and Rescorla, 2010), (Valin and Vos, 2012), (Kent and Seo, 2005), (Kaufman et al., 2014). Федеративният AIS облак оптимизира близост до източника (edge), качество и уникалност на събитийните данни (нормализация, дедупликация и времеви прозорци), както и многопосочно споделяне между автономни домейни в рамките на федеративна архитектура (ITU-R M.1371-5, 2014), (Mell and Grance, 2011), (Lee et al., 2020), (Shi et al.,. 2016), (Satyanarayanan, 2017), (Akidau et al., 2015). Общ мотив и при четирите е разделянето между управляващ слой - control-plane (идентичности, политики, конфигурация) и слой за данни - data-plane (поток/медия/задачи), но системните изисквания към латентност и консистентност са различни: HLS и CUDA толерират по-големи закъснения, докато VoIP и AIS са чувствителни към динамиката на мрежата и изискват стабилна обработка на непрекъснати потоци.

1.5.1. Критерии за оптимизация на прехода към управление на услуги

За целите на настоящия дисертационен труд оптимизацията на прехода от управление на асети към управление на услуги се разглежда като многокритериална задача, включваща взаимосвързани инженерни и организационни подобрения.

Първият критерий е латентност и отзивчивост на услугата, което е особено съществено при комуникация в реално време, видео стрийминг и интерактивни изчислителни заявки.

Вторият критерий е надеждност и устойчивост, разбирани като способност на системата да поддържа услугата при инфраструктурни ограничения, откази на отделни възли и променливи мрежови условия.

Третият критерий е сигурност, включваща защита на комуникацията, съдържанието, идентичностите и личните данни, както и ограничаване на последствията при компрометиране на отделни компоненти.

Четвъртият критерий е ефективност при използване на асетите, тоест възможност наличните мрежови, изчислителни и организационни асети да бъдат комбинирани и предоставяни така, че да се постигне по-висока стойност на услугата при ограничени ресурси.

Петият критерий е организационна приложимост, която е особено важна в публичния сектор, където решенията трябва да работят в условия на наследена инфраструктура, ограничени бюджети, разпределена отговорност и необходимост от оперативна съвместимост между автономни участници.

Въз основа на тези критерии в следващите глави се оценяват предложените архитектурни решения и се проследява как те допринасят за оптимизиране на прехода от управление на асети към управление на услуги в различни класове цифрови услуги.

1.6. Изводи

В първа глава беше проследено историческото развитие на комуникационната инфраструктура и бяха изведени причините, поради които в съвременната дигитална среда се налага преход от управление на асети към управление на услуги. Показано бе, че историческите инфраструктурни разломи, ограничената регионална свързаност, нарастващите изисквания към латентност, капацитет и сигурност, както и необходимостта от оперативна съвместимост между автономни участници правят класическия централизиращ модел все по-малко достатъчен.

Анализът на разгледаните класове услуги показа, че независимо от различията помежду им, те споделят общи архитектурни проблеми: необходимост от ясно разграничение между управляващи и информационни функции, защита на идентичности и данни, ефективно използване на комуникационните и изчислителните асети и възможност за предоставяне на функции като услуги, а не само като локално притежавани ресурси.

На тази основа федерираните системи се явяват естествена архитектурна посока за развитие, тъй като позволяват съчетаване на автономност, координация и споделяне на услуги между различни домейни. Именно в този контекст следващите глави разглеждат последователно криптографската основа на доверието, сигурното предоставяне на защитено съдържание, изчислителните услуги при поискване и архитектурните решения за комуникация и федеративна телеметрия в реално време.

1.7. Цел, задачи, обект, предмет и методи на изследване в дисертационния труд

Цел на дисертационния труд

Въз основа на извършения обзор на развитието на цифровите технологии, нарастващата роля на дигиталната трансформация в публичния сектор и необходимостта от координирано функциониране на хетерогенни цифрови среди, може да бъде формулирана основната цел на дисертационния труд:

Да се разработят подходи за оптимизиране на прехода от управление на асети към управление на услуги в сложни федерирани системи в публичния сектор.

В настоящия дисертационен труд оптимизацията се дефинира като инженерно и организационно усъвършенстване на жизнения цикъл на дигиталните асети/активи. Тя обхваща тяхното ефективно съчетаване и предоставяне като услуги с цел постигане на минимална латентност, висока надеждност и сигурност, както и максимална приложимост в реалната практика на публичния сектор.

Задачи на дисертационния труд:

1. **Да се анализират** предпоставките за преход от управление на асети към управление на услуги в публичния сектор, включително историческите, технологичните и организационните фактори, които определят необходимостта от такъв преход във федерирани среди, и на тази основа **да се формулират общи принципи и архитектурен модел за управление на услуги в сложни федерирани системи**, приложим към различни класове цифрови услуги в публичния сектор.
2. **Да се анализират криптографските рискове** в компютърните системи за повишаване на сигурността и надеждността на комуникационните услуги.
3. **Да се разработят методи за сигурен достъп до защитено съдържание** и защита на личните данни при предоставяне на цифрови услуги.

4. **Да се разработи архитектура за предоставяне на административни** и изчислителни услуги при поискване за обработка на големи обеми от данни в публичния сектор.
5. **Да се разработи хибридна архитектура** за предоставяне на комуникационна услуга в среда с инфраструктурни ограничения.
6. **Да се предложи архитектурно решение** за телеметрия в реално време в сложни федерирани среди.

Обект на дисертационния труд

Обект на дисертационния труд са сложните федерирани системи в публичния сектор, в които множество автономни административни, комуникационни и изчислителни домейни взаимодействат при предоставянето на цифрови услуги.

Предмет на дисертационния труд

Предмет на дисертационния труд са подходите, архитектурните модели и технологичните механизми за оптимизиране на прехода от управление на асети към управление на услуги в такива системи, разгледани чрез представителни казуси в областта на мултимедийното разпространение, високопроизводителните изчисления, комуникацията в реално време и федеративната телеметрия.

Методи на изследване

За реализиране на поставената цел и задачи са използвани следните **методи на изследване:**

- системен и сравнителен анализ на съществуващи технологии, архитектури и модели за предоставяне на цифрови услуги;

- исторически и контекстен анализ на развитието на комуникационната и цифровата инфраструктура;
- архитектурно моделиране на услуги и взаимодействия между автономни домейни във федерирана среда;
- анализ на сигурността и надеждността на комуникационни и изчислителни решения;
- проектиране и изследване на практически приложими решения, базирани на реално разработени и внедрени услуги;
- обобщаване на резултатите в общ модел за преход към управление на услуги.

1.8. Връзка между целта, задачите, главите и очакваните резултати

Поставената цел за оптимизиране на прехода от управление на асети към управление на услуги в сложни федерирани системи се реализира чрез последователно решаване на взаимосвързани задачи, разгърнати в отделните глави на дисертационния труд.

Първата задача, свързана с анализ на предпоставките за преход от управление на асети към управление на услуги в публичния сектор и с формулиране на общи принципи и архитектурен модел за управление на услуги в сложни федерирани системи, е разгледана основно в **глава първа** и намира завършен израз чрез общия синтез на резултатите в **заключението**. В тази част са изследвани историческите, технологичните и организационните фактори, които обуславят необходимостта от нов модел на управление в условията на дигитална трансформация и федерирани среди. Като резултат са изведени приложими принципи за архитектурен дизайн на service-centric и федеративни системи, които служат като основа за останалите изследвания в дисертационния труд.

Втората задача, свързана с анализ на криптографските рискове в компютърните системи и с аргументиране на избора на ECC като по-подходяща криптографска основа за повишаване на сигурността и надеждността на разглежданите комуникационни услуги, е разработена в **глава втора**. Извършен е анализ на слабостите на RSA, произтичащи от

качеството на ентропията, и е аргументиран изборът на ECC като по-подходяща основа за разглежданите в дисертацията разпределени и ресурсно ограничени цифрови услуги. Като резултат са предложени конкретни технологични стъпки за повишаване на киберустойчивостта на Linux-базирани системи и е очертана перспектива за пост-квантова устойчивост.

Третата задача, насочена към разработване на методи за сигурен достъп до защитено съдържание и защита на личните данни, е реализирана в **глава трета**. В тази част са предложени методи за сигурен видео стрийминг, разделяне на съдържанието от удостоверяването, внедряване на SSO услуга и изграждане на локална услуга за стрийминг на защитено съдържание. Като резултат е постигнат модел, който едновременно повишава киберустойчивостта и намалява зависимостта на регионалните оператори от ограниченията на мрежовата инфраструктура.

Четвъртата задача, свързана с разработване на архитектура за предоставяне на административни и изчислителни услуги при поискване, е разгърната в **глава четвърта**. В нея са разгледани платформа за административни услуги, централизирана обработка на сложни геопространствени изчисления чрез API-базиран достъп и използване на GPU асети, както и архитектурен подход за организиране на услуга върху потокова телеметрия. Като основен практически резултат е разработен и внедрен демонът *insightd*, който реализира паралелна обработка на данни чрез графични процесори и позволява прехвърляне на тежките изчисления към специализирана централизирана услуга.

Петата задача, насочена към разработване на хибридна архитектура за комуникация в реално време в сложни федерирани среди, е реализирана в **глава пета** чрез казуса за хибридна VoIP архитектура. В тази част е предложен модел за предоставяне на комуникационна услуга в среда с NAT ограничения, повишена латентност и инфраструктурни ограничения при регионални доставчици. Като резултат е показано, че чрез съчетаване на централизирана SIP сигнализация и директен пренос на медия може да се постигне по-ниска латентност, по-добро качество на комуникацията и по-висока практическа приложимост в реални регионални условия.

Шестата задача, насочена към предлагане на архитектурно решение за телеметрия в реално време в сложни федерирани среди, е реализирана в **глави четвърта и пета** чрез казуса за федеративен AIS облак. В тази част са разгледани edge събиране, дедупликация, нормализация, маршрутизация и координирано предоставяне на навигационна

телеметрия като услуга. В резултат са изведени ресурсният ефект на федеративния подход, практическите проблеми, които той решава, и системният ефект от предоставянето на координирана телеметрична услуга при запазване на автономността на отделните участници.

По този начин поставените задачи се реализират в конкретни части на дисертационния труд, а съвкупността от получените резултати формира общ модел за оптимизиране на прехода от управление на асети към управление на услуги в сложни федерирани системи в публичния сектор.

ГЛАВА 2. Методи за осигуряване на надеждност при управление на комуникационни услуги

2.1. Осигуряване на надеждност при комуникация

По-бързото развитие на съвременните общества води до по-голяма дигитализация. Все повече дейности и процеси стават по-продуктивни и по-ефективно управлявани чрез участието на технологиите. Тези процеси допълнително се ускориха и доказаха своята стойност, когато светът беше засегнат от глобалната пандемия от КОВИД 19. Трансформация, която при други обстоятелства би отнела години, трябваше да се случи в рамките на месеци. Обществата бяха подтикнати да търсят различни начини на живот и работа, много по-тясно свързани с цифровите технологии. Именно тук обаче се откроi и другата страна на процеса: не всички инфраструктури, организации и региони навлязоха в тази ускорена дигитализация с еднаква степен на технологична и киберзрялост. Там, където развитието е било непоследователно, фрагментирано или дълго време подчинено на частични и закъснели решения, се натрупват не само ограничения в свързаността и капацитета, но и уязвимости в сигурността. В този смисъл ескалацията на киберпрестъпленията, посегателствата върху лични данни, финансовите злоупотреби, загубата на информация и изнудването, свързано с нея, не са просто страничен ефект от по-широкото използване на технологии, а индикатор, че дигиталната трансформация често протича при неравномерно изградена киберустойчивост. Това показва, че наред с инфраструктурния разлом съществува и взаимосвързан разлом в киберсигурността, който изисква не изолирани мерки, а последователен архитектурен подход към надеждността и защитата на комуникационните услуги. (Jang-Jaccard and Nepal, 2014), (Kostadinov and Atanasova, 2019), (Dineva and Atanasova, 2019).

2.2. Изследване на RSA, дължащи се на Генератори за случайни числа

Спазването на изискванията за киберсигурност е предпоставка за сигурността и безопасността на ИТ инфраструктурите, цифровите ресурси и защитата на личните данни. В това отношение темите за криптографията и достатъчно надеждното генериране на случайни числа, които са в основата на всяка система за криптиране, са от особен интерес (Shalamanov, 2020).

За нуждите на съвременната криптография се използват два вида генератори на случайни числа - истински генератор на случайни числа (TRNG) и генератор на псевдослучайни числа (PRNG) (DiCarlo, 2012).

Генератор на истински случайни числа (TRNG): прилага се, когато RNG трябва да генерира стойности в даден момент, които трябва да са уникални и да не се повтарят в последващи RNG извиквания (Carr, 2003), (L'Ecuyer, 2007). Числата, получени с този тип RNG, се прилагат за операции, които изискват уникални/неповтарящи се числови стойности, генерирани във времето. (Jin, 2004), (Camara, 2019) Пример за такава ситуация е генерирането на криптографски ключ за кодиране/декодиране на данни, инициализиращи вектори, начални числови стойности (seed) за контролирани RNG и др. (Ergün, 2015), (Ryabko et al., 2016)

Генератор на псевдослучайни числа (PRNG): Като основа за този генератор се използва начално случайно число от микро или макро света (seed), а за следващите числа се използва математическа формула. От началната стойност, чрез прилагане на определен алгоритъм, произлизат всички генерирани впоследствие случайни числа. Последващите стойности, по реда им, са възпроизводими. Единствената неочаквана и тайна стойност, която трябва да бъде възможно най-непредсказуема, е началното число, което е „коренът" в основата на тази поредица и инициира генерирането на цялата числова поредица. От тази технология са заимствани удостоверяването с еднократна парола (OTP), генерирането на криптографски ключове, получени от главния коренов ключ (прилага се при съставянето на портфейли в BlockChain - технология на разпределения регистър), удостоверяването чрез HMAC и други.

Традиционните мерки за сигурност на генератора на случайни числа (RNG) са предимно обобщени статистики, свързани с отклонения от математическата случайност. (Trappe and Washington, 2006).

Хардуерният генератор на случайни числа (HRNG) (Dichtl, 2003) или по-скоро истинският генератор на случайни числа (TRNG) е устройство, което генерира случайни числа от физически процес, а не чрез алгоритъм. Този тип генератори са коренно различни от обсъжданите досега, защото такива устройства често се основават на явления в микросвета, които генерират на ниско ниво статистически случайни „шумови" сигнали, като топлинен шум, фотоелектричен ефект, включително разделител на лъча и други квантови явления. Тези стохастични процеси се считат за напълно непредсказуеми

на теория, за разлика от парадигмата за генериране на псевдослучайни числа, често прилагана в компютърните програми. Като цяло са известни два основни източника на практически квантово-механични физически вероятности: квантова механика на атомно или субатомно ниво и топлинен шум (някои от които са с квантово-механичен произход). Квантовата механика твърди, че някои физически явления, като например ядрения разпад на атомите, са фундаментално случайни и като цяло непредсказуеми.

Тъй като резултатът от квантово-механичните събития не може да бъде предвиден, те се считат за „златен стандарт“ за генериране на случайни числа.

Всъщност, един от най-добрите генератори на случайни числа за сървърни системи се счита за квантовите генератори от фотонен тип. Те са достатъчно компактни и могат да се поберат на печатна платка, като същевременно имат много висока производителност. Според някои изследвания, в много случаи такъв хардуерен модул има капацитета да захранва повече от един сървър за обществени услуги с качествени случайни числа.

Независимо кой от генераторите на случайни числа се прилага (неконтролиран или контролиран), общият успех на системата зависи от статистическите качества на произведените числа (Lavasani and Eghlidos, 2009). Бързо нарастващото търсене на честотни ленти, нарастващите обеми на съхраняваните данни и извършването на изчисления, съчетани с нарастващия спектър от киберзаплахи, гарантират, че нуждата ни от надеждни и непредсказуеми случайни числа само ще нараства в бъдеще. (Hart et al., 2017)

2.2.1. Значимост на проблема

Проблеми с генератора на случайни числа (RNG) са в основата на недостатъка в цифровия сертификат на тайвански гражданин. Бернщайн, Чанг, Ченг, Чоу, Хенингер, Ланге и ван Сомерен представиха доклад по време на Asiacrypt 2013 (Bernstein et al., 2013), в който показаха, че официалните смарт карти за идентификация на граждани, издадени от тайванското правителство, са дефектни. Резултатите им се основават на изследването на (Heninger et al., 2012) върху ключове за сигурност с ниска ентропия. Къде те изследват ключовете за сигурност с ниска ентропия и дали подобни недостатъци могат да бъдат открити в тайванската база данни „Citizen Digital Certificate“? Изследователите са водили проучването с 2 милиона 1024-битови RSA ключа от

тайванската база данни „Citizen Digital Certificate“ и са установили, че 184 от тези ключове са тривиални за изчисляване в рамките на няколко часа. Те отдават тези слаби RSA ключове на фатален недостатък в хардуерния генератор на случайни числа (RNG). Случайността, използвана за генериране на RSA ключове, е съдържала недостатъчна ентропия и е създала предвидими модели за RSA прости числа.

Изследователите показаха, че смарт картите, съдържащи тази фатална уязвимост при генерирането на ключове, вече се използват от тайвански граждани. Смарт картите са били използвани за чувствителни към сигурността процеси, като например:

- данъци върху доходите на физическите лица,
- актуализации на регистрацията на автомобили,
- за транзакции с държавни агенции (регистри на имоти, национално трудово осигуряване, обществена безопасност и имиграция),
- заявления за безвъзмездни средства,
- компании, които взаимодействат.

Също така, тази уязвимост може да е кибер инструмент за злонамерени страни, тъй като е замесена значителна сума пари.

Всеки може да факторизира простите числа на RSA ключа и след това да компрометира основния ключ, като по този начин може да фалшифицира цифровия подпис на притежателя на смарт картата и да открадне самоличността му.

2.2.2. Слаби ключове при мрежови устройства

В статия, публикувана през 2012 г. (Heninger et al., 2012), е показана слабост в TLS (Transport Layer Security) и SSH (Secure Shell) сървъри, включваща слаби ключове за сигурност. Те разкриват, че неправилно функциониращите генератори на случайни числа (RNG) водят до ниска ентропия на случайността за RSA и DSA сървърните ключове, което е причина за компрометирана криптография. Изследователите посочват, че тази уязвимост се дължи на наличието на дупка в ентропията в RNG (/dev/random и /dev/urandom). По време на зареждане /dev/random използва данни, останали от предишното зареждане, за пула на ентропията. Но когато системата е била изключена за дълго време и паметта се върне в основното си състояние, тези данни са предвидими.

Накрая, изследователите показват, че когато ядрото на Linux извлича ентропията от пул, то хешира съдържанието на пула и смесва част от резултата обратно в пула. Когато множество нишки извършват тази ентропия едновременно, това създава значителна ентропия поради непредсказуемостта в поведението на паралелизъм. Но изследователите показват също, че когато ядрото е принудено да използва само една физическа нишка, този метод не е достатъчен за генериране на ентропия за пула.

Уязвимостите в генерираните стойности на случайността водят до това, че голям брой TLS сертификати и SSH ключове лесно се факторизират и след това се компрометират. Изследователите показват, че някои частни RSA ключове са получени, защото техните публични ключове споделят нетривиални общи фактори поради тези проблеми с ентропията. Получаването на тези ключове за сигурност компрометира целите TLS и SSH системи и следователно това е проблем с голямо въздействие върху сървърите, използващи тези компрометирани системи. Те показват важността на наличието на случайност с висока ентропия по време на генериране на криптографски ключове и важността на решаването на проблема със събитията с ниска ентропия в Linux RNG.

2.2.3. Случайност в RSA криптографията

Същността на RSA криптирането е, че то използва само информация, която е публично достъпна. С публичния ключ всеки може да криптира съобщение, което иска да изпрати до собственика на частния ключ. Това е възможно, защото без да знае стойностите на p и q, никой освен собственика на частния ключ не може да декодира съобщението. Въпреки че всеки знае публичния ключ $x = p * q$, това не му дава ефективен начин да намери стойности за p или q. Според група изследователи преди години се е смятало, че дори откриването на 232-цифрено число би отнело повече от 1500 години изчислително време (разпределено между стотици компютри), за да се компрометира такъв частен ключ.

На пръв поглед RSA криптирането изглежда неуязвимо. Може да се каже дотук, но с изключение на един малък проблем, почти всички използват едни и същи генератори на случайни числа. Необходим е отличен източник на ентропия, за да се генерират висококачествените прости числа, които съставляват криптографските ключове в RSA. В конвенционалните компютърни системи източниците на качествена ентропия са

сравнително оскъдни за подобна задача. Поради тази причина, seeds, получени от качествена ентропия, се използват широко от години. Изчисленията за новите RSA ключове след това се извършват чрез генератори на псевдослучайни числа.

Като се вземат предвид фактите, можем да се обърнем към изследване от последните години, според което се появява нова идея, разглеждайки отново добре познатия пример: Да предположим, че Боб и Алис публикуват публични ключове онлайн. Тъй като и двамата са използвали една и съща програма за генериране на случайни прости числа, е по-вероятно техните публични ключове да имат общ прост делител. Факторизирането на публичните ключове на Боб или Алис поотделно би било почти невъзможно, но намирането на общи делители между тях е много по-лесно. Всъщност времето, необходимо за изчисляване на най-големия общ делител между две числа, е близко до пропорционалното спрямо броя цифри в двете числа. След като общият делител между ключовете на Боб и Алис е идентифициран, може да се изчисли основната факторизация на двата ключа. От тази гледна точка е възможно да се декодират всякакви съобщения, изпратени до Боб или Алис.

Въоръжени с тази идея, изследователите сканирали интернет и започнали да събират публични ключове, за да приложат алгоритъма. За тази цел те събрали 6,2 милиона реални публични ключа. След това изчислили най-големия общ делител между двойките ключове, компрометирайки ключ всеки път, когато той споделя общ делител с други ключове. В този експеримент те успели да разбият 12 934 RSA ключа. С други думи, ако технологията се използва небрежно и описаните слабости не бъдат преодолени, RSA криптирането осигурява по-малко от 99,8% сигурност.

На пръв поглед това изглежда като цялата история. По-подробното четене на изследванията по темата “Рон грешал, Уит е прав” (Arjen Lenstra et al., 2012) разкрива нещо по-тревожно. Според авторите, те са успели да извършат цялото изчисление за няколко часа на машина с един процесор. Погледнато през теоретичната основа на RSA, трябва да се предположи, че ще са необходими години, за да се изчисли НОД (най-голям общ делител) между 36 трилиона двойки ключове, а не часове, според проучването.

Как са го направили? В бележка под линия авторите намекват, че тяхното изчисление се основава на асимптотично бърз алгоритъм, който им позволява да намалят времето за извършване на изчисленията до почти линейно. Действителното описание на алгоритъма се пази в тайна от читателя, може би за да се предотврати злонамерена

употреба. Само няколко месеца след публикуването на статията, последващи доклади вече обсъждат подробно различни подходи, представящи бързи алгоритми (като това изследване: Квазилинейно изчисление на GCD и факторизиране на RSA модули и дори показва как да се използват графични процесори, за да се извърши изчислението с груба сила по-бързо (Scharfglass, 2012).

Вероятно може да се каже тук, че не е добре да се споменават неща, ако искаме да останат в тайна. От друга страна, ако слабостите в криптографските функции не бъдат подчертани, рискуваме да бъдат използвани от злонамерени лица без знанието на другите. В този случай, за да стигнем до резултатите от изследването, трябва да се обърнем към алгоритмите.

Предвид характеристиките на криптографията и предложения подход, алгоритъмът ще борави с цели числа с асимптотично голям брой цифри. Следователно, събирането и умножението няма да се считат за фиксирани и относително времеви операции.

За n-битови числа се приема $O(n)$ време. Използвайки операция за умножение, умножението изглежда отнема $O(n^2)$ време. Оказва се обаче, че има алгоритъм (алгоритъм на Шьонхеге-Щрасен), който работи във времето $O(nlog2\ nloglogn)$. Изчисляването на НОД с помощта на евклидовия алгоритъм отнема време $O(n2\ lognloglogn)$. За пореден път обаче изследователите са открили по-добър алгоритъм, който работи във времето $O(nlog2\ nloglogn)$. За щастие, всички тези алгоритми вече са имплементирани в GMP (GNU MP Sub quadratic), C++ библиотеката за работа с големи числа. За останалата част от изследването ще използваме нотацията Õ, вариант на нотацията Big-O, който игнорира логаритмичните множители. Например, докато изчисляването на НОД отнема време $O(nlog2\ nloglogn)$, в нотацията пишем, че отнема време Õ(n).

2.2.4. Трансформация на проблема

Дефинираме множеството от публични RSA ключове с k_1.....k_n, където всеки ключ е произведението на две големи прости числа. Обърнете внимание, че n е общият брой ключове. Вместо да изчисляваме НОД на всяка двойка ключове, можем да изчислим за всеки ключ k_1 НОД на него и произведението на всички останали ключове.

$\prod_{t=1} K_t$. Ако ключът k_i споделя един главен фактор с други ключове, тогава това ще даде главния фактор. Ако обаче и двата главни фактора на k_i са споделени с други ключове, изчислението няма да може действително да извлече отделните прости фактори. Този случай може да е достатъчно рядък и не си струва да му се обръща особено внимание.

2.2.5. Алгоритъм

Алгоритъмът има леко необичайна рекурсивна структура, тъй като рекурсията се случва в средата на алгоритъма, а не в края.

В началото на алгоритъма разполагаме само с ключовете:$k_1 \ldots k_2 \ldots k_3 \ldots$

Първата стъпка на алгоритъма е да се свържат ключовете и да се изчислят резултатите от тях:

$j_1 = k_1 . K_2,$

$j_2 = k_3 . K_4,$

$j_1 = k_5 . K_6, \ldots$

След това, чрез рекурсия върху поредицата от числа $j_1, \ldots\ldots, j_n$се изчислява:

$r_1 = GCD(j_1, \prod_{t \neq 1} j_t),$

$r_2 = GCD(j_2, \prod_{t \neq 2} j_t),$

$r_3 = GCD(j3, \prod_{t \neq 3} j_t), \ldots\ldots\ldots$

Целта е да се изчисли $si = GCD(ki, \prod t \neq ikt)$ за всеки *kj* ключ. Важното тук е, че когато *i* е нечетно, *si* може да се изрази като

$s_i = GCD(k_i, r_{(i+1)/2}.k_{i+1})$

И че когато i е четно, *si* може да се изрази като

$s_i = GCD(k_i, r_{i/2}.k_{i-1})$

За да се разбере защо е така, може да се провери дали изразът от дясната страна на *GCD* е гарантирано кратен на $si = GCD(ki, \prod t \neq ikt)$, докато същевременно е делител на $\prod t \neq ikt$. Това от своя страна предполага, че изчислението *на GCD* ще бъде *точно*

$GCD(ki, \prod t \neq ikt)$, както се очаква.

Време на изпълнение:

Нека m означава общия брой битове, необходими за записване на$k_1 \ldots k_n$. Всеки път, когато алгоритъмът се повтори, се гарантира, че общият брой битове в рекурсния запис не надвишава предишното ниво на рекурсия. Това е така, защото новите записи са произведения на двойки елементи от стари. Следователно всяко от нивата на $O(\log n)$ на рекурсията действа върху входа с общ размер $O(m)$ битове. Освен това, аритметичните операции във всяко ниво на рекурсия отнемат най-много време $\tilde{O}(m)$. Следователно общото време на работа на алгоритъма също е $\tilde{O}(m)$ (тъй като рекурсионните нива $O(\log n)$ могат да се научат в нотацията O-tilde).

Ако разширим работното време в стандартната Big-O нотация, получаваме $O(m \log 3\ m \log \log m)$.

2.2.6. Приложимост на подхода

На пръв поглед тройният логаритмичен фактор може да изглежда като пречка за използването на този алгоритъм. Но в друго проучване се оказва, че това представяне е доста разумно. Статията (Cloostermans, 2012) установява, че алгоритъмът отнема приблизително 7,65 секунди на хиляда ключа, което означава, че ще са необходими малко над 13 часа за изпълнение на 6,2 милиона ключа.

Оказва се също, че един от LOG факторите може да бъде елиминиран с помощта на друг подход, който избягва напълно изчисленията на GCD, освен на първото ниво на рекурсия, например статията (Heninger et al., 2012). Този подобрен алгоритъм отнема около 4,5 секунди на хиляда ключа, което води до общо време за изпълнение от около 7,5 часа за работа с 6,2 милиона ключа. Така че изчислението, което би трябвало да отнеме години, се свежда до часове. Всичко, което е необходимо, е прилагането на рекурсия, анализ на времеви серии, за да се използва слабостта при генерирането на случайни числа в системите.

В заключение може да се каже, че слабостите не произтичат от грешка в аритметиката на RSA. Те идват от технологичната слабост, с която се имплементира RSA. Компютърните системи, ако са от по-ново поколение, имат хардуерни и софтуерни подобрения, които им позволяват да генерират качествени случайни числа. Опасността от тази уязвимост обаче остава. Защото RSA се нуждае от наистина големи случайни числа. Настоящият критерий за надежден RSA ключ е минимум 2048 бита, а

препоръчителната дължина е дори 4096 бита. Други проучвания също така установяват, че между 4096, 8192 и 16384 бита на RSA ключ, по-голямата сигурност на по-големите ключове е минимална. Причината идва и от ограниченията на генераторите на случайни числа. По-големите RSA ключове изискват изключително големи реални случайни числа. Което е изключително трудно да се получи в компютърна система. Дори ако за тази цел се използва силициевият модул за HWRNG, буферът за ентропия е 4096 бита и се натрупва бавно, като ограниченията идват от технологията. При използване на RSA криптография, в системи със значително по-малко хардуер, като например IoT, генерирането на RSA ключове ще бъде още по-слабо. Отново, причините са едни и същи и този тип устройства често нямат специализиран хардуер за обогатяване на ентропията. Поради тази причина много такива устройства често стават лесни жертви на кибератаки.

Както се казва, в основата на всяка система за криптиране, е алгоритъм и генератор на случайни числа. Следователно, независимо колко сложни алгоритми за криптиране се прилагат, те се считат за толкова уязвими, колкото и генераторът на случайни числа, който е в основата на тази система.

Ефективността на генератора на случайни числа (RNG) се измерва със степента на ентропия за генериране на случайни числа.

Сложността на анализа на даден генератор на случайни числа е функция на качеството на неговата ентропия, сезонност и склонност към сблъсъци. Това са моментите, в които генераторът на случайни числа ще генерира стойност, която е циклична или стойностна, което води до повторение или генериране на нова, но очаквана стойност. Чрез математиката на времевите редове е възможно да се определи ентропията във времето и е вероятно да се изчисли (предскаже) евентуалното бъдещо повторно появяване на данните. Откриването на сезонност в получените стойности, отклонения или сблъсъци може също да показва слабости на генератора на случайни числа. Ако генераторът е с добро качество, тогава той ще следва анализа на много голям брой статистически стойности от генериран от него числен масив с висока степен на ентропия и непредсказуемост, което ще бъде много ресурсоемко и сложно. Това ще го направи и много устойчив на атаки в цялата криптография, свързана с този генератор.

2.3. Възможни начини за решаване на проблема с ентропията на случайния генератор в компютърните системи

2.3.1. Операционни системи, базирани на Linux и Debian

В операционни системи, базирани на Linux и Debian, ентропията на случайните числа се увеличава с използване на технологията HwRNG на процесора на Intel.

Името на модула за генериране на случайни числа е Intel Secure Key, предишното му кодово име е Bull Mountain Technology. Следователно, трябва да се провери дали текущата система разполага с такива процесори и дали конфигурацията ѝ може да бъде надградена. При наличие на компютърна система с операционна система Linux, проверката може да се извърши освен чрез техническата документация на чиповете от производителя и чрез следната комбинация от команди:

```
$ cat /proc/cpuinfo | grep -i rdrand | echo $?
```

В резултат на това, `0` означава, че е наличен RDRAND флаг и процесорът може да бъде включен, за да подобри криптографските функции на системата, както следва:

```
# apt install rng-tools-debian
# /etc/init.d/rng-tools-debian start
# /etc/init.d/rng-tools-debian status
* rng-tools-debian.service - LSB: rng-tools (Debian variant)
Loaded: loaded (/etc/init.d/rng-tools-debian; generated)
Active: active (running) since Fri 2021-09-28 17:30:54 EET;
2min 15s ago
Docs: man:systemd-sysv-generator(8)
Tasks: 4 (limit: 4915)
Memory: 1.3M
CGroup: /system.slice/rng-tools-debian.service
’-3597 /usr/sbin/rngd -r /dev/hwrng
$ cat /proc/sys/kernel/random/entropy_avail
4038
```

Резултатите показват, че скоростта на събиране на ентропия в нашия случай надвишава скоростта на нейното потребление.

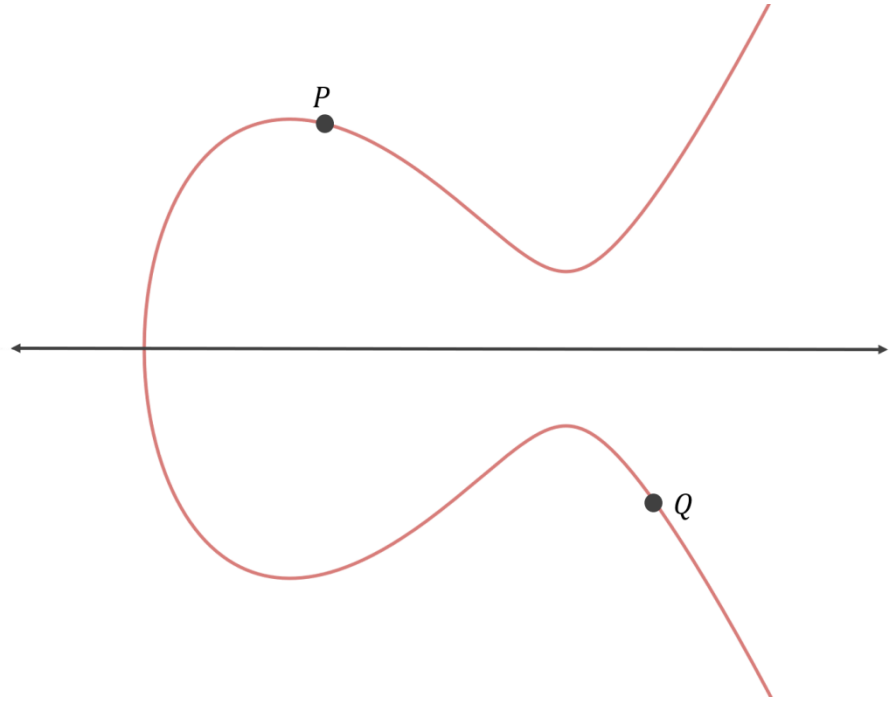
2.3.2. Избор на ECC в разглеждания контекст

В рамките на настоящия дисертационен труд преходът от RSA към ECC не се разглежда като универсална подмяна на всички асиметрични криптографски схеми, а като по-подходящ инженерен избор за разглежданите цифрови услуги. При услуги, работещи в разпределена среда, върху вградени или ресурсно ограничени устройства, и при необходимост от чести операции по удостоверяване, подписване и договаряне на ключове, ECC осигурява по-добър баланс между криптографска устойчивост, размер на ключовете, трафичен overhead и изчислително натоварване. По тази причина в контекста на разглежданите в дисертацията service-centric и федеративни сценарии практичният преход е именно от RSA към ECC.

RSA алгоритъмът се характеризира с по-големи размери на ключовете и по-високо изчислително натоварване, особено при среди, в които се използват вградени устройства, edge възли или системи с ограничени ресурси. Именно това прави ECC по-практичен избор за разглежданите в настоящото изследване услуги.

2.3.3. ECC криптография

ECC (криптографията на елиптичните криви) се заражда, когато двама математици на име Нийл Коблиц и Виктор С. Милър предлагат използването на елиптични криви в криптографията (Afreen and Mehrotra, 2011). ECC в криптографията с публичен ключ използва елиптични криви върху крайни полета. Тази техника използва теорията на елиптичните криви. Елиптичната крива представлява множеството от точки, които удовлетворяват математическо уравнение ($y^2 = x^3 + ax + b$). Графичната репрезентацията на елиптична крива е показана на Фиг. 2.1.



Фиг. 2.1. Елиптична крива (Sarkar et al., 2021)

Ще илюстрираме примерза Q = d·P при елиптични криви (ECC) по идеята на Коблиц (Koblitz, 1987).

1. Избираме крива и параметри

За визуализация (интуиция върху реалните числа) избираме елиптичната крива:

$E: y^2 = x^3 - 7x + 10$ *(Фиг. 2.2)*

Избираме базова точка (генератор) и малък скалар за примера:

$P = (1, 2)$

$d = 3$

$Q = d \cdot P = 3P = (9, -26)$

Забележка: В реалната ECC изчисленията са над крайно поле (mod p или mod 2^m), но груповият закон и идеята с права/допирателна и отражение остават същите като конструкция.

2. Геометрична конструкция (как P „се умножава“ по d)

Умножението по скалар d се реализира чрез последователно събиране на точки. Геометрично, сборът $P + R$ се получава така: права през P и R пресича кривата в трета точка $-S$, а отражението ѝ спрямо оста x дава $S = P + R$.

2.1 Дублиране (2P)

Допирателната в P пресича кривата в трета точка $-(2P)$, след което отразяваме по оста x.

Резултат: $2P = (-1, -4)$

2.2 Събиране (3P = P + 2P)

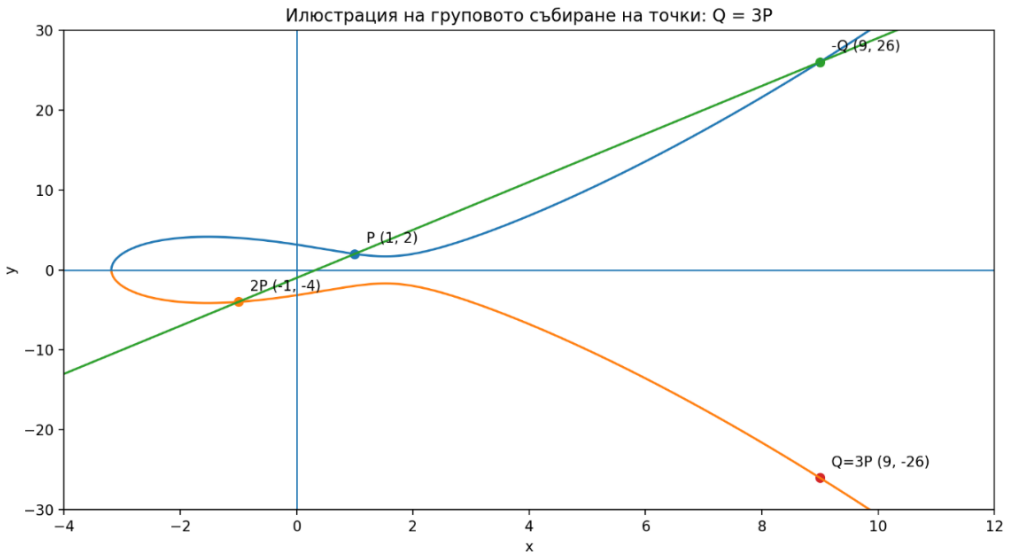
Правата през P и $2P$ е: $y = 3x - 1$

Тя пресича кривата в трета точка: $-Q = (9, 26)$

Отражение по x-оста дава публичната точка: $Q = (9, -26) = 3P$

3. Геометрична илюстрация

Фигура 3.2 показва кривата E, правата през P и $2P$, точката $-Q$ (третото пресичане) и отражението $Q = 3P$.



Фиг 2.2. Геометрична илюстрация на Q = 3P върху E: $y^2 = x^3 - 7x + 10$

4. Какво е „тайната“ в ECC в този контекст

Публично са известни P и Q. Тайната (частният ключ) е скаларът d в равенството $Q = d \cdot P$. Да се изчисли Q от (P, d) е лесно, но да се възстанови d от (P, Q) е трудно при коректно избрани параметри и достатъчно голям порядък на групата, известно в математиката като проблем за дискретния логаритъм върху елиптични криви. ECDLP е фундаментална твърда математическа задача, на която се крепи сигурността на

съвременната криптография с елиптични криви (ECC). За “обратния път” в ECC (да се намери d от Q = d·P) стандартният аргумент за трудност е, че в общия модел всяка атака срещу дискретния логаритъм изисква поне $\Omega(\sqrt{p})$ групови операции, където p е най-големият прост делител на реда на групата — т.е. на практика расте като квадратен корен от размера на групата и става непосилно при правилно избрани параметри (Shoup, 1997).

Методът на елиптични кривиECC може да се използва за създаване на по-малки, много по-бързи и по-ефективни криптографски ключове. Вместо да използва традиционен метод за генериране на произведение от много големи прости числа, той използва уравнение на елиптична крива за генериране на ключове. ECC се използва във всички основни блокчейн криптовалути, а една от добре познатите е Bitcoin. За хакерите е наистина трудно да разбият ECDLP.

RSA	ECC
Има бавен алгоритъм и може да използва максимално компютърни ресурси като батерия и др.	Алгоритъмът е бърз, тъй като размерите на ключовете са по-малки, което натоварва по-малко системните ресурси.
Той е уязвим срещу квантови компютри и атаки с груба сила.	Използва ECC алгоритъм, който работи по проблема с елиптични криви и дискретен логаритъм (ECDLP), което е доста трудно за хакерите да го разгадаят, затова е много сигурен
В RSA може да са необходими по-дълги ключове за по-висока сигурност.	Благодарение на по-късите си ключове, ECDSA предлага много по-добра производителност в сравнение с RSA.
В RSA мащабируемостта не е оптимална.	Мащабируемостта се подобрява, тъй като по-високият трафик може да се обработва от сървъра благодарение на по-ниските режийни разходи
RSA зависи повече от RNG ограниченията	По-малките ключове и математическите специфики правят ECC по-сигурен в настоящите възможности за RNG

Таблица 3.1.Бързо сравнение между RSA и ECC.

2.3.4. ECDSA/ECDH върху NIST елиптични криви: компактност, производителност и ниво на сигурност

За автономни системи от федеративния AIS облак, които често работят върху вградени устройства (Raspberry Pi, edge приемници/форвардъри), е важно асиметричните операции да са бързи и да не „надуват“ трафика. Алгоритмите базирани на криптографията на елиптичните криви – ECDSA за подписи и ECDH за договаряне на ключ, дават еквивалентна криптографска устойчивост при значително по-къси ключове и подписи спрямо RSA, което е практично за защита от край до край при транспорт между възлите в облака.

NIST Digital Signature Standard (FIPS 186-5) дефинира ECDSA и утвърдените „NIST криви“ P-256, P-384 и P-521, които са широко поддържани в стандартни криптографски библиотеки и хардуерни модули.

Съгласно препоръките за еквивалентна сила на сигурност (напр. SP 800-57 Part 1), P-256 е типичен избор за около 128-битова устойчивост: публичните ключове и подписите са компактни (десетки байтове), докато RSA за сходно ниво изисква ключове от порядъка на 3072 бита, което увеличава латентността, размера на сертификатите и натоварването при подписване/верификация.

Подобни принципи – подписване на AIS съдържание за автентификация и цялост при запазване на обратна съвместимост – са демонстрирани и в Protected AIS (pAIS), където се използвасхема за съвместимост с криптография, за да се адресират известни AIS уязвимости и да се запази интероперабилност с немодифицирани AIS устройства (Gary Kessler, 2020).

2.4. Перспективно направление на изследвания - През времето и квантовите компютри

В момента и двата алгоритъма (RSA, ECC) не са толкова лесни за хакване, но всичко това ще се промени с евентуалното (и вероятно) въвеждане на квантови компютри в бъдеще по прогнози на NIST. При RSA публичният ключ е произведение на две големи прости числа, а тайната е частният експонент d, изчисляем от φ(N)=(p-1)(q-1). Класическата сигурност на RSA се свежда до това, че факторизацията на N е изчислително трудна при големи размери. Сходството с ECC е това, че при класическите компютри намирането на частния скалар dот публичните точки Q=dP (ECDLP) е считано за изчислително непосилно при правилно избрани параметри. Така при наличие на

квантов компютър с достатъчно кюбити, алгоритъмът на (Shor, 1994) може да факторизира N (за RSA) и да решава дискретния логаритъм (за ECC) в полиномиално време, т.е. да възстанови dот P и Q. Това прави схеми като RSA, ECDH и ECDSA квантово уязвими: от публичния ключ може да се извлече частният ключ, а оттам – да се изчисляват споделени тайни и да се фалшифицират подписи (Proos and Zalka, 2003).

2.5. Изводи

По този начин втора глава изгражда криптографската и удостоверителна основа, върху която в следващата глава се развиват модели за сигурно предоставяне на защитено мултимедийно съдържание.

Изследването на представените слабости в асиметричния RSA алгоритъм показва, че надеждността на цифровите услуги зависи в значителна степен от качеството на генераторите на случайни числа и от правилния избор на криптографска схема. Това обосновава избора на криптография на елиптичните криви (ECC) като по-подходяща основа за разглежданите в дисертацията удостоверителни и защитни механизми, особено в разпределени, федеративни и ресурсно ограничени среди.

Разгледаните хардуерни и софтуерни подходи за повишаване на ентропията при генериране на случайни числа допълват тази линия, като показват, че сигурността не е статично свойство, а резултат от правилно съчетаване между алгоритми, източници на ентропия и реална изчислителна среда. В този смисъл втора глава не само анализира ограниченията на RSA, но и очертава практически посоки за изграждане на по-надеждна криптографска основа за цифровите услуги, разглеждани в следващите части на дисертационния труд.

Съдържанието на тази глава е отразено в следните публикации:

1. Blagoev, I., Balabanov, T., Iliev, I. RSA Weaknesses Caused by the Specifics of Random Number Generation. Information & Security: An International Journal, 50, 2, Procon Ltd., 2021, ISSN:0861-5160, DOI:10.11610/isij.5028, 171-179 (2021)
2. Blagoev, I., Balabanov, T., Iliev, I. The Randomness in Shared Web Hostings. Extended Abstracts of 16th Annual Meeting of the Bulgarian Section of SIAM, Fastumprint, (2021), ISSN:1313-3357, 9-10

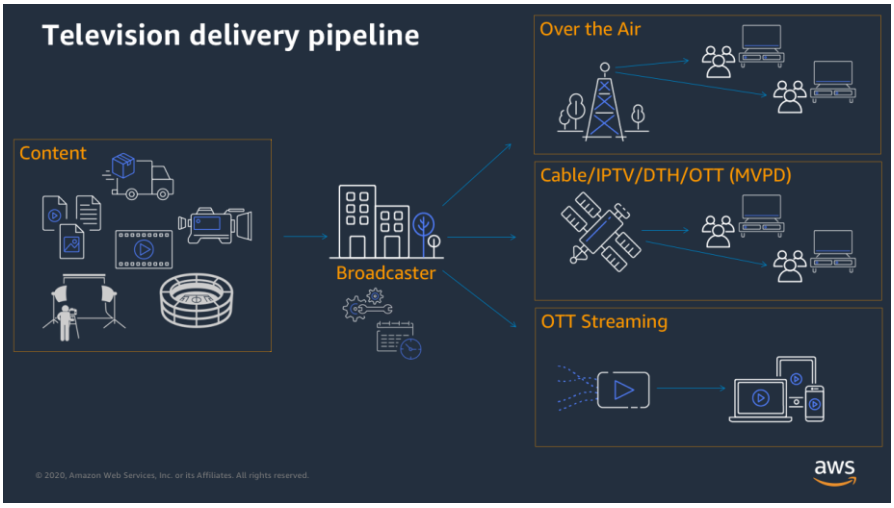
ГЛАВА 3. Методи за достъп до защитено съдържание

Изобретяването на телевизията промени света и ускори разпространението на информацията. През последните няколко години телевизионното излъчване остана само цифрово, а IP мрежите се очертаха като допълнителна опция за излъчване. В тази дисертация се предлага подход за сигурно стрийминг на видео и предотвратяване на лесно изтичане на видео съдържание поради проблеми с киберсигурността. Предложените методи обхващат и двата аспекта – самото съдържание и защитата на личните данни на абонатите при използване на услуги за стрийминг на живо.

От друга страна, гледането на услуга за стрийминг на живо през интернет с висока резолюция и високо качество генерира голям мрежов трафик, което изисква от зрителите да осигурят интернет връзка с достатъчна скорост. В днешно време има доста интернет доставчици, които не могат да предоставят високи скорости на своите абонати и в резултат на това гледането на услуга за стрийминг на живо с високо качество е невъзможно. Целта на изследването е да се предложат технически методи за разпространение на сигурна услуга за стрийминг на живо през интернет в локална интернет среда и да се разгледат съображения за сигурност, свързани с условен достъп, криптиране на съдържание и незаконно разпространение. Общото описание на разработените методи се обобщава като „съдържание е едно, а удостоверяването е друго“.

3.1. Подход за подобряване на сигурността на уеб видео стрийминга и предотвратяване на изтичане на лични данни

Обикновено дадена телевизионна продукция определя тема, като например спорт, новини, музика, филми и др., която се излъчва по съответния телевизионен канал. Наборът от канали образува пакет, който се предлага и продава на крайния потребител от телевизионния оператор и се разпространява чрез наземни, кабелни или сателитни комуникации в традиционните радиоразпръсквателни услуги. През последните няколко години радиоразпръсканата телевизия остава само цифрова, а IP мрежите набират популярност като допълнителна опция за излъчване (Фиг. 3.1).



Фиг. 3.1. Пътища за доставка на телевизионни продукции (източник Amazon).

Независимо от инфраструктурата, използвана от даден оператор, някои канали или дори специално съдържание изискват специфична схема за плащане и прилагат условен достъп. Това означава, че само абонати на услугата могат да гледат платените канали и никой друг. В миналото, по време на ерата на аналоговата телевизия, операторите са използвали техники за кодиране, като например видео шифър, за да защитят съдържанието (Фиг. 3.2). Клиентът трябва да включи декодер, за да върне аудио/видео (AV) сигналите в първоначалния им вид.

Фиг. 3.2.Video Cipher scrambler устройство, защитаващо аналогово съдържание за телевизионни оператори.

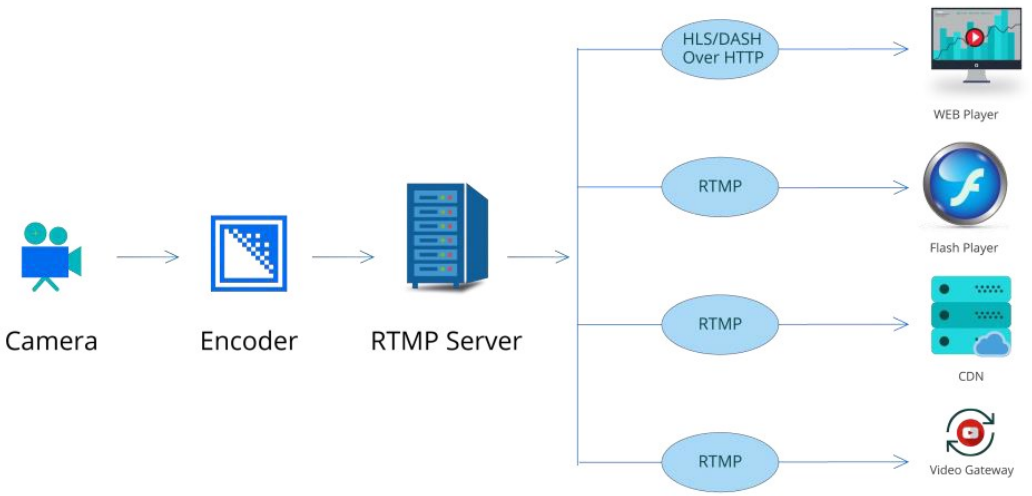
В ерата на цифровата телевизия, схемите за кодиране са се развили в схеми за криптиране, като Viaccess, Irdeto, Conax и много други. Клиентите трябва да притежават смарт карта, която защитава самоличността на потребителя и работи в устройства за декриптиране, като например модул за условен достъп (CAM) на телевизор или приемник (STB), съответстващ на схемата за криптиране.

Развитието на интернет позволява на много професионалисти и аматьори да разширят своя дигитален бизнес в глобален мащаб. Много общности и корпорации разработват специфични комуникационни протоколи, механизми за сигурност, хардуерни устройства и софтуерни платформи за различни видове дейности и реализации. Нарастващите скорости на интернет правят възможно стрийминга на видео и гледането в реално време от много места. В резултат на това конвенционалните телевизионни канали са изправени пред нова конкуренция в областта на уеб видео услугите. Така че някои организатори на спортни събития, концерти, конференции и др. предпочитат уеб стрийминг продукцията пред традиционното телевизионно отразяване нададено събитие. Тази тенденция се наблюдава най-вече при нискобюджетни събития. Въпреки че няма пряка техническа връзка между бюджета и качеството на услугата, всъщност могат да се наблюдават редица проблеми и уязвимости едновременно, причинени от ниския бюджет. Настоящото изследване не е насочено към създаването на видео съдържание, а само към съображения за сигурност по отношение на upstream ипроцес на стрийминг надолу по веригата, чиито подобрения биха проправили пътя за развитието на тези услуги.

Протокол за съобщения в реално време (RTMP)

Протоколът за съобщения в реално време (RTMP) е най-разпространеният протокол за стрийминг на видео съдържание в реално време. Този протокол е разработен от Adobe в първоначална версия за предаване на мултимедия към потребителски Flash плейъри и по-късно е доразвит като основен протокол за предавания на живо в интернет. RTMP стриймингът на живо се поддържа като функционалност в редица софтуерни и хардуерни видео енкодери за любители и професионалисти. От страна на сървъра, RTMP се поддържа като модул в някои от известните сървъри (напр. nginx) и в популярните платформи за публично споделяне на видео – FaceBook, Instragram, Youtube, TikTok, Twitch и др. (Documentation Team, “Amazon Kinesis Video Streams Developer Guide,” 2018), (Tashev et al., 2016).

Източниците на аудио и видео сигнали, които могат да бъдат камери, микрофони, музикални инструменти, миксиращи конзоли, предварително записана мултимедия и др., се обработват в един видео поток, след което се кодира съгласно подходяща схема за трансфер, например H. 264, с необходимите параметри за AV компресия. Изходният поток се изпраща през RTMP до RTMP крайна точка, която може да бъде хоствана на специален сървър или публична платформа за споделяне на видео. Настройването на собствен RTMP сървър позволява внедряване на висока защита на трафика, както и разкриване на редица възможности за разполагане на допълнителна инфраструктура, докато съдържанието достигне крайния клиент, като например клониране на трафик към други RTMP крайни точки за междуплатформено едновременно излъчване или за CDN осигуряване, т.е. постигане на географски по-близко обслужване до крайния потребител (Фиг. 3.3).



Фиг. 3.3. Диаграма, представяща процеса на RTMP стрийминг (източник synopi.com).

По отношение на киберсигурността и нискослойните транспортни протоколи, RTMP съществува в 5 варианта:

- RTMP – базовата протоколна форма на стандартен TCP порт 1935. Може да се пропусне в RTMP URL;
- RTMPS – RTMP през TLS. Няма дефиниран стандартен TCP порт, често се използва 1936 и трябва да бъде изрично споменат в RTMP URL;
- RTMPE – RTMP с механизми за криптиране на Adobe;

- RTMPT – RTMP през HTTP(S) (когато доставчикът е блокирал всички портове към дестинации с изключение на 80 и 443);
- RTMFP – P2P UDP комуникация

На практика се използват първите два варианта, а именно RTMP и RTMPS. Първият аспект на тази глава, разглеждащ защитата на специфично видео съдържание, когато то е предназначено само за строго определена група абонати, е свързан с осигуряване на сигурността на комуникацията между стрийминг студиото и крайната точка на RTMP, когато трафикът преминава през публична мрежа като Интернет. В този случай използването на RTMPS не винаги е добра идея. Причината е, че софтуерните програми или стрийминг хардуерът обикновено нямат възможността да правят специфични TLS настройки, както ида имат в наличие надежден източник на случайни числа (Blagoev, 2020).

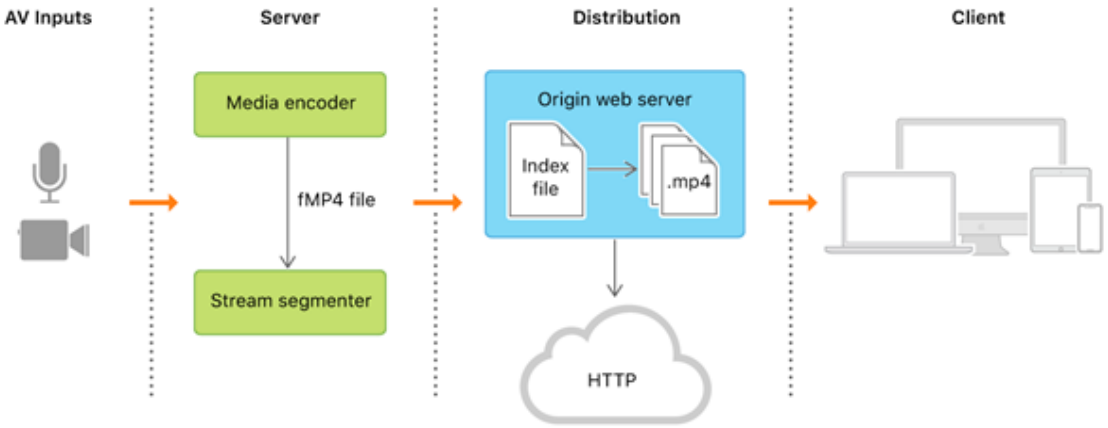
Най-добрият начин за защита на трафика е преминаването през предварително установен криптографски тунел, например IPSEC, между стрийминг студиото и крайната точка на RTMP. По този начин, RTMP трафикът в чист вид може да се пренася през тунела без проблеми (Paul Baka et al., 2021), (Benoit Badrignans et al., 2011).RTMPS трябва да се използва само когато криптографски тунел не може да бъде установен предварително по една или друга причина, най-често финансова.

HTTP протокол за стрийминг на живо (HLS)

Въпреки че RTMP позволява гледане на потока от същата крайна точка, към която се предава, това никога не се използва на практика от крайните потребители. Причините са:

- Ограничен брой плейъри поддържат RTMP комуникация;
- RTMP изисква постоянна TCP връзка, което би създало проблеми при гледане на живо чрез над 90% от конвенционалните домашни интернет доставчици и мобилни оператори;
- RTMP няма гъвкави механизми за удостоверяване на крайния потребител.

Трите проблема бяха решени с въвеждането на нов HLS протокол, разработен от Apple, който е предназначен само за гледане на видео съдържание от крайни потребители (Фиг. 3.4).



Фиг. 3.4. HLS Архитектура (източник Apple)

Къде са решени посочените проблеми:

- Поддържа се от почти всички HTML5 плейъри и браузъри;
- Подобряване на сигурността на уеб видео стрийминга и предотвратяване на изтичане на лични данни
- Потокът в реално време (RTMP в тази дисертация) се конвертира в HLS парчета, които се предоставят през HTTP(S) на крайния потребител;
- Могат да се приложат всички механизми за сигурност и удостоверяване на HTTPS връзката.

За да разгледаме механизмите за защита на трафика и удостоверяване на потребителите, е необходимо да се вгледаме по-задълбочено в HLS. Това може да се случи след стартиране на работеща крайна точка за гледане на HLS видео, което може да се реализира чрез изпълнение на следните стъпки:

- Настройване на RTMP сървър за получаване на RTMP трафик на съответната крайна точка;
- Настройка на RTMP към HLS конвертиране.

Пример с nginx конфигурационен фрагмент с компилиран nginx-rtmp-module за стъпки 1 и 2: https://github.com/arut/nginx-rtmp-module, след което следва:

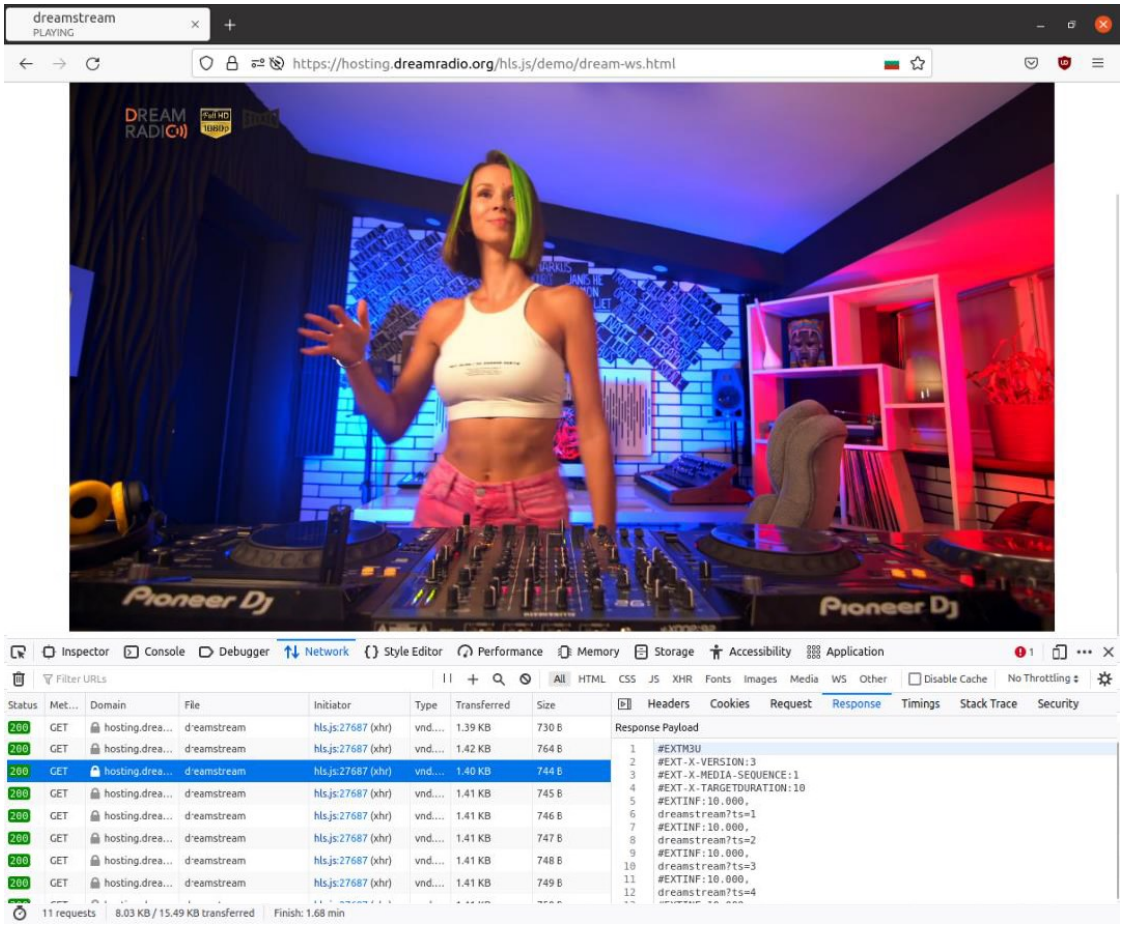
- Кодиране на входящия AV сигнал към H.264 (използвайки стрийминг програма или специфично хардуерно устройство);
- Въвеждане на RTMP крайната точка и съответния Stream Key в настройките на програмата или устройството;

- Стартиране на процеса на стрийминг;
- Разработване (клониране от хранилището) на уеб плейър, позволяващ гледане на HLS.

Примерен код на уеб hls.js проект, https://github.com/video-dev/hls.js/

- Въвеждане на HLS настройките в съответния JS файл;
- Вграждане на плейъра в основна уеб страница;
- Пускане на видеото от плейъра и отваряне на конзолата за разработчици на браузъра, за да се види трафикът.

Мрежовата работа на плейъра се свежда до отправяне на асинхронни XHR заявки към HLS крайната точка, които са разделени на 2 типа. Първият тип заявка изтегля m3u8 плейлист с Content-Type: application/vnd.apple.mpegurl (Фиг. 3.5), съдържащ крайните точки на наличните парчета, а вторият тип изтегля съответното парче с Content-Type: video/mp2t (Philip Goldie et al., 2003).



Фиг. 3.5. Асинхронно сваляне и декодиране на m3u8 плейлист.

Тук идва моментът на втория аспект на изследването, който се отнася до видео дистрибутора и разглежда защитата на видео съдържанието спрямо крайните потребители. Тъй като специфичното видео съдържание е предназначено за строго определена група потребители, следва, че HTTPS сървърът първо трябва да бъде конфигуриран съгласно най-добрите практики за сигурност (https://www.ssl.com/guide/ssl-best-practices/). След това трябва да се внедрят механизми за удостоверяване на потребителите. Опциите най-общо се свеждат до две основни:

Установяване на TLS с изискване за удостоверяване на клиента със сертификат; Управление на потребителски сесии на приложението с бисквитки или подобен метод.

Първият вариант се използва изключително рядко, защото е по-сложен от гледна точка на потребителя. Изисква се валиден клиентски TLS сертификат за удостоверяване на потребителя, подписан от Удостоверяващ орган.

Както често се изисква и специализиран криптопроцесор за защита на частния ключ на потребителя, за да бъде имплементиран правилно. Въпреки че е доста сигурен, сложността на многото елементи в него, които се предават предимно на потребителя, го прави нешироко използван за тази цел.

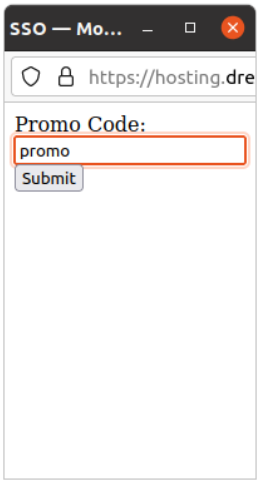
При втория вариант, парчетата, както и плейлистът, не могат да бъдат изтеглени от който и да е потребител в интернет, който има техните URL адреси, а само от оторизирани, които могат да предадат валиден токен за изтегляне на съдържанието, с други думи – тези, които са преминали процеси на удостоверяване и оторизация. В света на видео разпространението, оторизиран потребител най-често се разбира като този, който има достъп до дадено съдържание, след като е извършено плащане.

За нуждите на изследването е разработен симулатор на такива процеси в backend-а, функциониращ между „голата“ HLS услуга на nginx и крайния потребител, който се грижи за предоставянето на токен на потребителя в бисквитка след валидно удостоверяване и съответно валидира токените от клиентските заявки. Ако токенът не е подаден или е невалиден (изтекъл), бекендът връща *401 Неоторизирано* (Mueller, 2015).

Възможностите за получаване на токен са многобройни и разнообразни. Те зависят най-вече от управленските решения на организацията или групата организации.

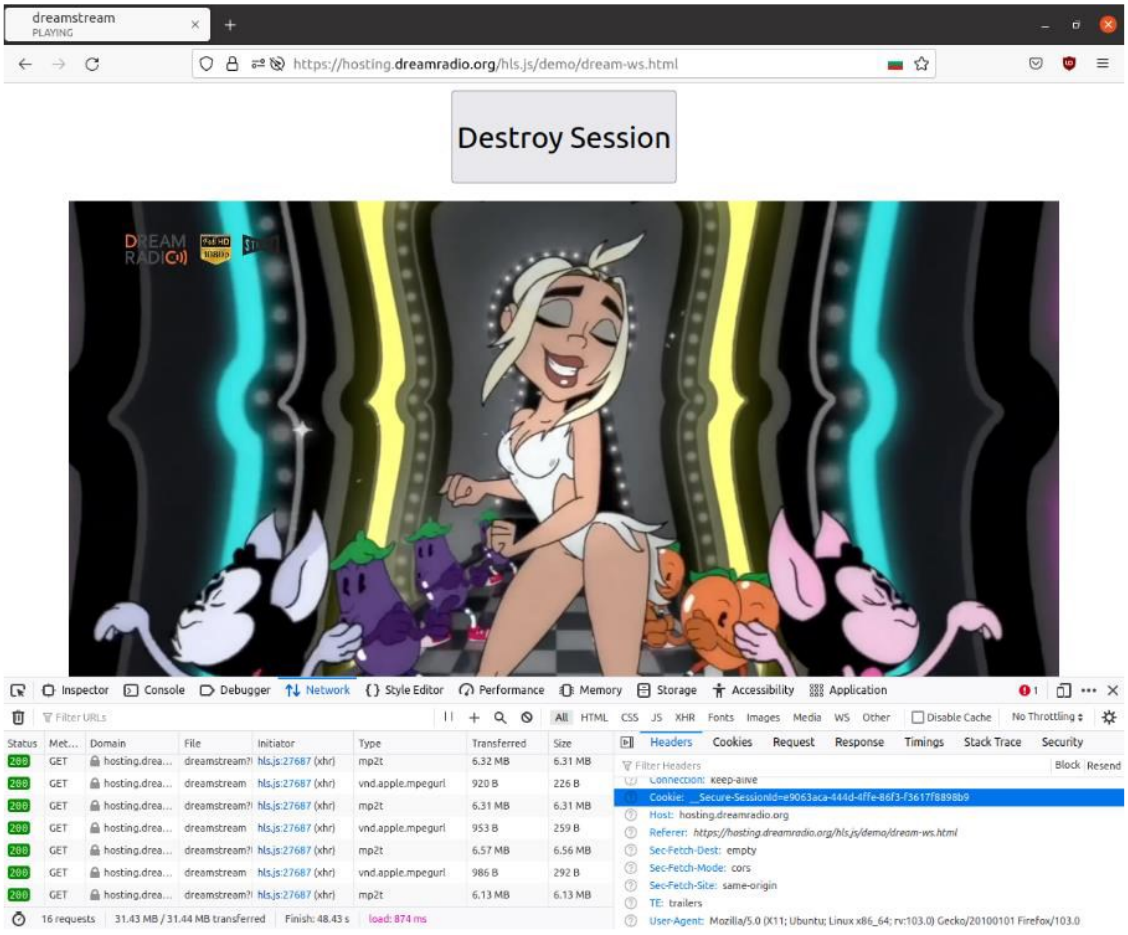
В тази дисертация е разработена семпла услуга за SSO вход за демонстрация.

След извикване на услугата SSO (Фиг. 3.6) и успешно преминаване на процеса на удостоверяване, се стартира потребителска сесия на приложението с произволно генериран криптографски защитен идентификатор и бисквитката на сесията се връща в отговора към клиента.



Фиг. 3.6. Формуляр за получаване на токен за оторизация.

Клиентът е длъжен да предостави токена, за да поддържа сесията активна (Фиг. 3.7). Времевият прозорец, през който токенът е валиден, както и времето за преиздаване, подлежат на дефиниране на управленско ниво, а не на техническо.



Фиг. 3.7. Оторизиране към стрийминг сесия с бисквитки

Внедряването на тази SSO услуга има за цел да демонстрира, че самото разпространение на видеото и удостоверяването на потребителите могат да бъдат разделени между различните организации. Това означава, че излъчващата организация и доставчикът на доверие могат да бъдат напълно разделени. Изграждането на стрийминг платформа с диференцирана услуга за доверие позволява внедряването на различни методи за удостоверяване, които могат да се извършват с:

- потребител + парола
- промо код
- клиентски сертификат със съответния частен ключ съхранен на файл или смарт карта
- мобилно приложение, което удостоверява потребителите
- чрез публична платформа – имейл, социална мрежа и др.

Освен това, изборът или промяната им от доставчика на доверие в бъдеще не изисква тежко преконфигуриране при видео дистрибутора. Второто предимство е, че

излъчващата организация е освободена от обработката на личните данни на потребителите.

Недостатъкът е, че в момента най-разпространените мобилни и настолни медийни плейъри не поддържат разширени методи за удостоверяване като SSO, Oauth2 и др., което означава, че опциите за гледане са ограничени до уеб браузър или специално проектиран плейър за мобилни и настолни устройства. Предимството на медийните плейъри пред браузърите е, че те предоставят по-голям контрол на потребителя по отношение на аудио и видео настройки, работа с пълния набор от аудио и видео устройства, свързани към системата на потребителя и др.

По този начин в дисертацията са разгледани възможностите за защита на комуникацията между стрийминг студиото и RTMP сървъра, от една страна, и HLS комуникацията между видео дистрибутора и крайния потребител, като е предложена идея за внедряване на портал за удостоверяване на потребителите, предоставен от доставчик на услуги за удостоверяване, който освобождава видео дистрибутора от обработка на лични данни и платежни средства. За целите на изследването предложеният подход беше реализиран на тестов сървър, откъдето бяха представени резултатите от изследването. Предимството на предложения подход за защита на стрийминг съдържанието е, че може да се приложи към всякакъв вид високобюджетен или нискобюджетен проект. Също така не се изисква дистрибуторите на съдържание да се грижат за администрирането на личните данни на потребителите. Това води до още по-висока киберустойчивост на предложеното решение, защото дори при всяко нарушение на сигурността на сървър, няма лични данни, които могат да бъдат откраднати.

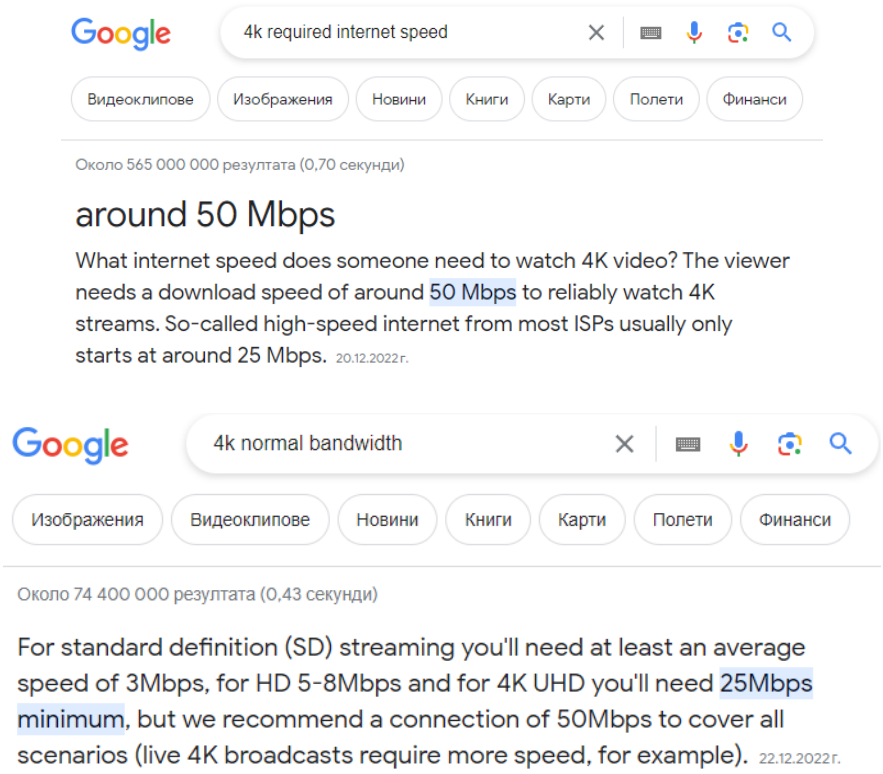
3.2. Съображения за сигурност и техники за разпространение на видео стрийминг в среда на домашни интернет доставчици

3.2.1. Проблемът с недостатъчната интернет скорост

Интернет телевизионните предавания и други създатели на съдържание напълно разчупиха границите на съвременната телевизия и медии. Ако дадена телевизионна програма е достъпна в ограничен географски регион, тя достига до своите фенове по целия свят чрез интернет. Поради това почти всяка телевизионна програма вече е достъпна и чрез интернет стрийминг. Според проучване на Nielsen за последните години

до 2022 г., делът на стрийминг излъчванията ще се увеличи в сравнение с гледането на ефирно и кабелно предаване сред потребителите (Alec Tefertiller et al., 2019).

Като допълнително предимство, със стрийминга, потребителите имат по-голям избор от устройства и свободата да избират времето за гледане на видео по заявка (VOD) съдържание. Но заедно с бързото развитие на стрийминга идват и предизвикателствата за осигуряване на достатъчно бърз интернет, необходим за качествено излъчване на стрийминг съдържание. Това е проблем, с който едва ли има потребител на видео стрийминг, който да не се е сблъсквал. За да избере своя интернет тарифа, всеки средностатистически интернет потребител, който иска да гледа стрийминг на живо, би направил едно от следните бързи търсения (Фиг. 3.8).



Фиг. 3.8. Бързо търсене в Google относно изискванията за скорост за гледане на4K video в интернет.

Скоростите, описани в резултатите, които търсачката връща, са базирани на обичайния набор от алгоритми за компресия на видео и честота на кадрите за съответната резолюция, които са внедрени в популярните стрийминг платформи. Както е известно, те адаптират тези параметри към средата на средностатистическия интернет потребител,

за да постигнат задоволително качество на видео услугата срещу минимизирани изисквания по отношение на интернет свързаността.

Дори и с така подбрани параметри, регионалните интернет доставчици в отдалечени райони, морски и планински курорти не предлагат на своите абонати достатъчни интернет скорости, за да гледат обичайно 4K видео в реално време. През последните години се наблюдава постоянна тенденция хората да местят живота си към по-спокойни и здравословни места, като същевременно хората са свикнали с някои от удобствата на големия град, което означава, че местните бизнеси трябва да се адаптират към тенденцията и да отговорят на новите нужди.

В контекста на видео услугите проблемът може да се види в голям мащаб. Ако говорим за 8K и High Frame Rate Video формати, то дори по-големите интернет доставчици в големия град или близо до него не биха предлагали такива скорости на своите абонати, а ако е така, биха били неизгодни за голяма част от потребителите.

Изследването “A Study of High Frame Rate Video Formats” (Mackin et al., 2019) хвърля интересен поглед върху предимствата на високите кадри в секунда, които не се ограничават само до зрелищност и ефекти, а напротив – пряко влияят на психофизиологията и намаляват нивото на стрес при продължително гледане.

3.2.2. Изграждане на локална стрийминг услуга независимо от интернет тарифите

В този дисертационен труд е предложен подход за изграждане на локална стрийминг услуга в централния офис на интернет доставчика за дистрибутиране на видео на живо до крайните потребители, независимо от интернет тарифите.

Преки ползи:

- Възможност за гледане на защитено видео съдържание с високо качество в средата на регионален интернет доставчик;
- Минимизиране на външния трафик на доставчика;
- Реклама на дадена стрийминг услуга сред абонати на даден интернет доставчик;

Потенциални ползи:

- Насърчаване на местни инициативи, свързани с производството на видео съдържание.

Решението за дистрибутиране на услуга за стрийминг на живо в интернет доставчик е фокусирано върху изграждането ѝ в среда на пасивна оптична мрежа (PON), тъй като PON технологиите се използват все по-често, заместващи медните кабелни мрежи (ADSL, VDSL, меден Ethernet и др.), а парадигмите за интегриране на услуги в PON са отдавна установени (Mutlu et al., 2001).

При внедряването на локална услуга за стрийминг на защитено съдържание трябва да се вземат предвид следните съображения и техники:

1. Техники за разпространение: Избягване на репликиране на трафика в 1 точка;
2. Съображения за сигурност: Удостоверяване и внедряване на обща схема за криптиране;
3. Предотвратяване на незаконно преразпределение.

Услугата за уеб стрийминг е по същество комбинация от протоколи за upstream (предаване нагоре по веригата) към стрийминг сървъра и downstream (надолу по веригата) към крайните потребители, като най-често използваният набор е RTMP + HLS. Такова разделение на протоколите се е наложило през годините поради спецификата на свързаността на потребителите. Според HLS, видео потокът се разделя на парчета, като периодично се изтегля и чете текстов плейлист в стандартизиран M3U формат, който описва парчетата, достъпни за изтегляне. За да се постигне надеждност на услугата, разпределение на натоварването и ниска латентност към крайния потребител, стрийминг платформата се изгражда на CDN схема с множество възли, които са географски разпределени.

Целта на локалния възел е, от една страна, да се свърже със специфичната стрийминг услуга, достъпна в интернет, и да поддържа синхронизация на видео фрагментите с нея, а от друга страна, да преразпредели фрагментите към локалните абонати.

3.2.3. Техники за разпространение

3.2.3.1. Unicast комбиниран със сървър-клиент

Unicast комбиниран със сървър-клиент комуникация е най-често използваният метод за консумиране на видео поток в интернет поради своята простота и надеждност, лесен за изпълнение, но при дадена локална свързаност противоречи на условието за избягване на репликация на трафика към локалния стрийминг възел.

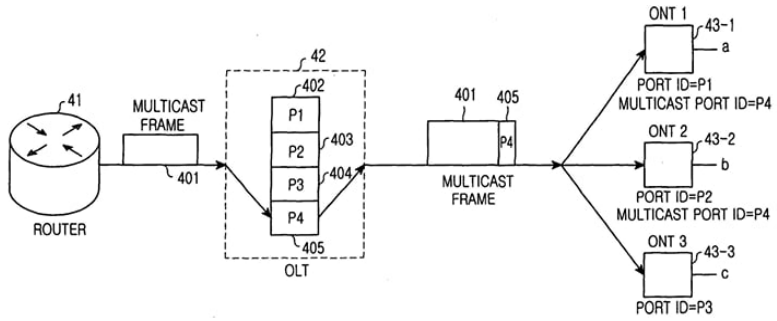
3.2.3.2. Peer-to-Peer (P2P)

Peer-to-Peer (P2P). Стар механизъм за изграждане на мрежова стратегия, избягващ концентрацията на мрежов трафик в 1 точка, първоначално реализиран в добре познати чат протоколи, споделяне на файлове, откриване на устройства и мултимедийни услуги в локална мрежа и др., но неприложим в пасивни мрежи от тип „точка-към-много-точки“ (P2M) с голям мрежов трафик по очевидни причини - споделяне на обща честотна лента между 32, 64 или 128 ONT устройства в зависимост от схемата за мултиплексиране, свързани към 1 активен OLT порт.

3.2.3.3. Multicast

Също така стар механизъм за изграждане на мрежова стратегия, избягващ репликация на трафика в една точка. Той е напълно подходящ за видео стрийминг и внедряване в съвременни PON мрежи (Фиг. 3.9).

Традиционна настройка на мултикаст за корпоративна среда с активно мрежово оборудване е описана в следния документ „МУЛТИКАСТ ЗА СТРИЙМИНГ НА ВИДЕО В КОРПОРАТИВНА СРЕДА“ (Protocols and Design Guide, 2015). Приложението на мултикаст в PON среда е базирано на традиционния метод, но с добавени функции, дължащи се на мултиплексната среда, по отношение на конструирането на мултикаст кадрите, съдържащи номерата на съответните ONT портове (Wenyang Yanget al., 2011).



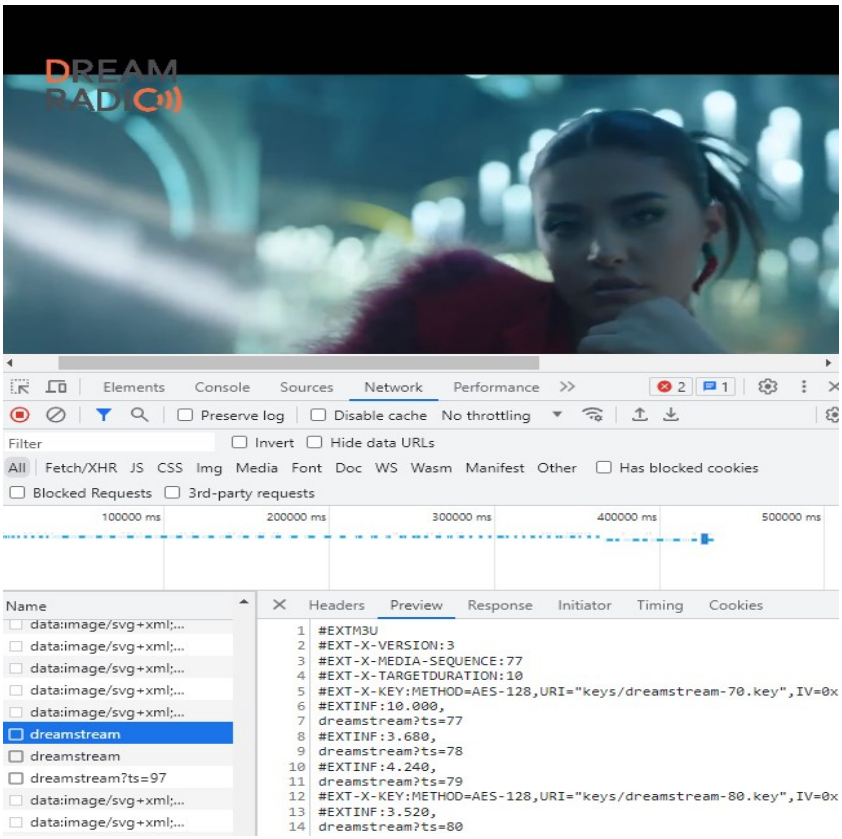
Фиг. 3.9. Multicast GPON предаване и метод за обработка на GEM кадри - multicast кадър, предаван в PON (Samsung Electronics Co, 2005).

3.2.4. Съображения за сигурност

3.2.4.1. Сигурност на комуникацията

Решението е да се внедрят споразумения за условен достъп в DVB, където алгоритмите за обмен на ключове и кодиране са отделни, но специфична схема за условен достъп (Conax, Irdeto, VideoGuard, Viaccess и др.) ги реализира заедно.

Идентични парадигми могат да бъдат приложени в спецификацията на протокола HLS, за която е предоставена схемата за AES криптиране на видео фрагменти от MPEG Transport Stream, описана в (RFC8216). Криптирането се извършва на сървъра, като клиентът извлича ключа за декриптиране от URI адреса и прилага точната крипто схема, описана в плейлиста M3U, съгласно стандарта HLS за декриптиране на TS фрагменти (Conditional-access systems for digital broadcasting, 2016) (Фиг. 3.10).



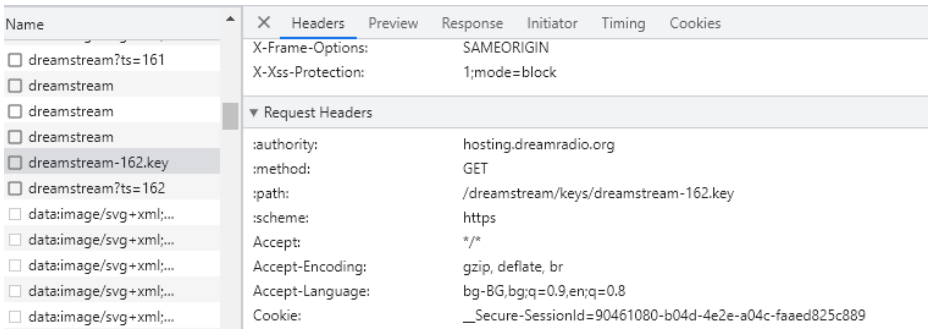
Фиг 3.10. Плейлистът M3U описва схемата за криптиране и ключовите местоположения за декриптиране на TS парчетата.

3.2.4.2. Автентификация

Като се има предвид, че криптирането на самите фрагменти е фактическата защита на канала, за да се реши задачата за удостоверяване на потребител, е достатъчно изтеглянето на ключовете да премине през процес на удостоверяване (Ralf-Philipp et al., 2005).

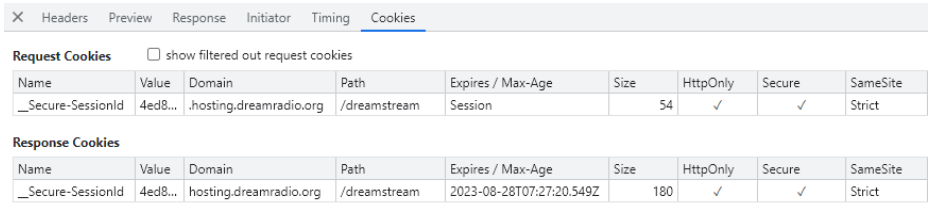
В дисертационния труд е разработен подход за подобряване на сигурността на уеб видео стрийминга и предотвратяване на изтичане на лични данни, като се обсъждат

начини за внедряване на условен достъп чрез установяване на потребителска сесия за изтегляне на видео фрагменти чрез предаване на криптографски токени от клиента към стрийминг сървъра, издадени от услуга за удостоверяване на трета страна (Iliev&Blagoev, 2022).Предлага се развитие на този авторски подход като същите тези техники се прилагат не към видео фрагментите, а към ключовете (Фиг. 3.11 и 3.12).



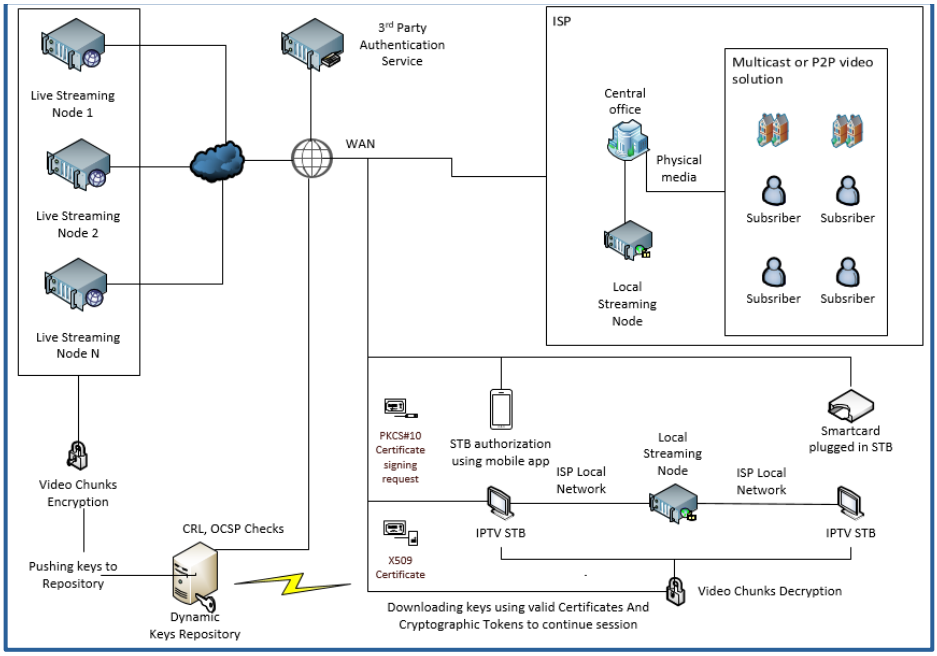
Фиг. 3.11. Заявка за ключ за изтегляне чрез HTTPS с използване на валиден токен.

По този начин, изтеглянето на всеки ключ ще бъде защитено от потребителска сесия на приложението срещу неоторизирано изтегляне.



Фиг. 3.12. Сесийна бисквитка с време на изтичане, съхранявана в браузър.

Тези примери за възпроизвеждане на криптирано HLS видео съдържание в браузър са взети от демонстрационна услуга. В реална среда на интернет доставчик, видеото ще се възпроизвежда от STB устройствата на доставчика. В обобщение, цялостната схема на решението би изглеждала така (Фиг. 3.13):



Фиг. 3.13. Обща схема за дистрибутиране на стрийминг на живо в локална интернет среда

Основни компоненти:

- Услуга за стрийминг на живо, разпространявана в облак или персонализирана платформа в интернет.
- Локален стрийминг възел, инсталиран при интернет доставчик.
- Услуга за удостоверяване на доставчик на удостоверителни услуги.
- Хранилище за ключове за декриптиране на видео трафик.
- IPTV приемник на клиента.
- Устройства за удостоверяване на потребителя – смартфон, смарт карта.
- Неилюстрирани компоненти, за които се предполага, че са интегрирани – например платежни системи.

3.2.4.3. Примерен работен сценарий за изграждане на системата

Първоначално потребителят се идентифицира пред доставчик на удостоверителни услуги, който е интегриран със системата, и създава профил за него. Обикновено идентификацията се извършва дистанционно и профилът е достъпен чрез мобилно приложение.

При наличие на предаване на живо, потребителят избира от приемника (STB) доставчик на удостоверителни услуги, интегриран със съответната стрийминг услуга.

STB генерира ECC-базирана асиметрична двойка ключове и заявка за подписване на сертификат PKCS#10 с произволно общо име, например UUID4 или подобен случаен низ с достатъчна дължина. Изборът на ECC в този сценарий е обусловен от ограничения ресурс на крайното устройство, необходимостта от компактни ключове и сертификатни структури, както и от по-ниското изчислително натоварване при удостоверяването и поддържането на защитен достъп до услугата.

На следващата стъпка STB кодира URL адреса в примерен формат:

https://trust-service-provider.tld/streaming-service-id/live-event-id/{uuid}/csr

като QR код и го показва на телевизионния дисплей.

На заден план, STB се свързва с доставчика на услуги за удостоверяване, изпраща генерирания CSR и чака издаването на x509 сертификат.

Междувременно потребителят заснема QR кода, мобилното приложение на доставчика на услуги за удостоверяване се отваря и потребителят потвърждава издаването на сертификата и го упълномощава да гледа предаването на живо срещу съответната такса. Доставчикът на услуги за удостоверяване подписва CSR, издава x509 сертификат с дата на изтичане малко след края на предаването на живо и го прехвърля към стрийминг услугата.

STB сваля x509 сертификата.

Стрийминг услугата криптира AES ключа всеки път с публичните ключове на всеки x509 сертификат, абониран за стрийма на живо, и изпраща криптираните AES ключове към хранилището.

STB инициира HTTPS заявка с частния ключ и клиентския сертификат към хранилището на ключове, за да му бъде издаден криптографски токен за иницииране на потребителска сесия. С този токен STB изтегля AES ключа за видеото, криптирано с публичния ключ от сертификата. Декриптира AES ключа с неговия частен ключ и след това декриптира видео фрагментите с AES ключа.

Веднъж стартирана, потребителската сесия не изисква TLS с удостоверяване на клиента или частния ключ на клиента, докато криптографският токен не изтече. В рамките на сесията токените се подновяват, но неактивността в рамките на определения

период на валидност на последния токен изисква иницииране на нова сесия чрез TLS, използвайки частния ключ и клиентския сертификат.

Бележка: В примерния сценарий е използван x509 сертификат като средство за удостоверяване, издаден от Удостоверяващият орган на доставчик на доверителни услуги. Видео услугите обикновено не са квалифицирани и не изискват квалифицирани процедури за идентификация и удостоверяване, съответно издадените сертификати не са квалифицирани. По този начин няма задължение частният ключ да бъде генериран, съхраняван и използван на смарт карта. Технически е възможно да се генерира на всяко компютъризирано устройство и да се повторят действията, програмирани в STB устройството. Този технически факт е от значение за незаконното разпространение.

При подготовката на сценария бяха взети предвид следните съображения:

- Всички процеси са автоматизирани, без да се отчитат манипулациите на потребителя в STB и мобилното приложение на доставчика на услуги за удостоверяване;
- Операциите с лични данни се извършват само в системите на доставчика на услуги за удостоверяване;
- Доставчикът на услуги за удостоверяване не може да свърже потребителя с неговата самоличност въз основа на директна логика.
- Хранилището с ключове може да бъде напълно отделна услуга. Никой не може да декриптира ключовете за гледане на видео без съответния частен ключ, съответстващ на оторизиран сертификат;
- Видео трафикът преминава през интернет доставчика в криптиран вид. Служителите на интернет доставчика не могат да гледат видео съдържание без ключове за оторизация и това не е необходимо, освен ако изключителна ситуация не го изисква. Основната роля на интернет доставчика е да осигури широк канал за разпространение на видео трафик през своята физическа мрежа до крайните потребители.
- Процедурите за удостоверяване, оторизация и изтегляне на ключове могат да се извършват през най-удобната интернет връзка. Няма специфични мрежови изисквания и генерираният трафик, свързан с тези операции, е незначителен.

3.2.5. Предотвратяване на незаконна дистрибуция

Това е най-интересният и ключов въпрос. Огромното предимство на цифровите пред аналоговите технологии е неограниченото копиране на информация, без да се губи оригиналната ѝ форма. Това явление е едновременно положително и отрицателно. То поставя предизвикателства при справянето с проблемите, свързани с неразрешеното копиране и разпространение на цифрова информация.

Тяхното начало датира отпреди повече от 20 години. След като законно предоставената информация достигне дори до един потребител, започва неконтролиран процес на разпространение - т.нар. дигитално пиратство.

Най-популярните и използвани мерки и до днес са правните, които в споразумение между дистрибутора и крайния потребител определят правните последици срещу незаконното копиране и разпространение. Важни правни развития относно защитата на защитено с авторски права съдържание от неразрешено копиране (Turnbull, 2001).

Технически метод срещу незаконно копиране и разпространение е воднят знак, но той е обект на тайни атаки (Lianet al., 2008).

Следващият подход за сигурност е да се позволи свързване само на отговарящи на условията устройства. Един такъв стандарт е HDCP, осигуряващ защита за HDMI, DisplayPort и DVI интерфейси. Текущата версия на стандарта е 2.3, докато старите версии са били хакнати (Lomb and Guneysu, 2011).

3.3. Коментари

Независимо от известните уязвимости, няма 100% техническа бариера срещу излъчването на защитено съдържание на обществено място, дори при наличие на съответното споразумение между страните. Няма пречки за инсталиране на легален телевизор в супермаркета или на жп гарата, откъдето може да се излъчва незаконно защитено съдържание.

В крайна сметка се получава порочен кръг – създават се сложни системи за удостоверяване, оторизация и разпространение, които правят крайния продукт много скъп, а същевременно се разчита на съвест – „моля, използвайте отговорно, неразрешеното разпространение се преследва от закона“. Икономически не е честно

спрямо тези, които са готови да си платят сами, тъй като цената на една система така или иначе трябва да се поеме отнякъде. Но животът като цяло не е справедлив. Може би с появата на квантовите технологии и този въпрос би бил решен с технически методи за по-справедлив свят.

3.4. Изводи

В този смисъл трета глава показва как върху вече изградена основа на доверие и удостоверяване може да се реализира защитена и капацитетно ефективна регионална услуга, което подготвя прехода към предоставяне на по-сложни административни и изчислителни функции като услуги в следващата глава.

Предложен е подход за реализиране на локално преразпределение на услугата за стрийминг на живо през интернет към абонати на интернет доставчици с висока степен на защита на видео трафика и личните данни. От представените примери става ясно, че предоставянето на интегрирана услуга, независима от интернет честотната лента на отделните абонати, ще намали външния трафик на доставчика. Това би позволило излъчване на видео съдържание с по-добро качество в реално време, в райони, където не е осигурена съответната интернет скорост, покриваща видео трафика. Следвайки тенденциите в технологичния свят към необходимостта от обмен на все по-големи обеми данни, въпросът за интеграцията на услуги при интернет доставчиците ще стои с нарастваща сила.

Съдържанието на тази глава е отразено в следните публикации:

1. **Iliev, I.**,Blagoev, I.. An Approach to Improve Web Video Streaming Security and Prevent Personal Data Leakage. Information & Security: An International Journal, 53, 1, Procon, 2022, ISSN:1314-2119, DOI:https://doi.org/10.11610/isij.5306, 78-88
2. **Iliev, I.**, Blagoev, I. Security Considerations and Techniques for Video Streaming Distribution in Home ISPs (International Conference on Electronics, Engineering Physics and Earth Science (EEPES 2026) which will be held on 24th-27th June, 2026 in Bandirma, Turkey).

ГЛАВА 4. Управление на услуги в сложни федерирани системи в публичния сектор

В настоящата глава се разглежда преходът към предоставяне на цифрови услуги в публичния сектор чрез три взаимосвързани направления: платформа за административни услуги, централизирана изчислителна услуга за обработка на геопространствени данни и федеративна услуга за събиране и предварителна обработка на потокова телеметрия в реално време. Акцентът е поставен върху service-centric подход, при който сложните технически функции не се реализират локално във всяка отделна администрация или приемна точка, а се организират като услуги с ясно разграничени роли, интерфейси и отговорности.

4.1. Дигиталната трансформация и регионалното развитие

Анализът на геопространствените данни е ключов фактор за дигиталната трансформация и регионалното развитие в случая на градоустройството, решавайки проблеми с трафика, включително като ясна посока за прехода към умни градове (Erskine et al, 2014). Тя е от съществено значение и за търговските организации чрез вземане на решения в редица случаи като планиране на мрежово покритие, инвестиционни изследвания, оценка на риска и анализ на пазара (Wickramasuriya et al., 2013). Така наречените услуги за онлайн аналитична обработка (OLAP) стават все по-необходими (Rivest et al., 2005), тъй като предоставят различни механизми за анализ на геоданни в отдалечени дигитални среди, позволявайки това да се извършва напълно автоматично. Човешката история многократно е показвала, че всяка промяна или революция е трудна, болезнена и се случва в продължение на дълъг период от време. Тук не се наблюдава изключение. Днес работният процес все още не е автоматизиран, въпреки всички практически изисквания за развитието на компютърните технологии в момента.

4.2. Преход към предоставяне на цифрови услуги за държавните администрации

В настоящия дисертационен труд е разработена и имплементирана услуга за анализ на геопространствени данни във формат GeoJSON, предназначена за вътрешна и външна употреба в консорциумна среда. Архитектурата включва HTTP API крайни точки за приемане на файлове и задачи, обратна WebSocket връзка за известяване в

реално време за статуса на обработката и самостоятелна фонова услуга за изпълнение на анализа, реализирана чрез демона *insightd*, който използва рамката RAPIDS за паралелни изчисления с графичен процесор (GPU).

Всички технически описания са базирани на реално разработени и работещи услуги в консорциумна среда при изпълнение на дейности по работен пакет в проект с европейско финансиране. Важно е да се отбележи, че крайните точки на интерфейса за приложно програмиране (API) са проектирани с възможност за използване и от външни организации по абонаментен модел, когато услугата бъде официално предоставена.

4.2.1. Някои от основните въпроси на дигиталната трансформация

- Липса на умения: Служителите често нямат необходимите умения за работа с нови технологии. Не-ИТ персоналът е изправен пред вид работа, която е изцяло свързана с ИТ. Понякога причината е, че оперативните бюджети изтичат, което прави наемането на ИТ персонал или външни ИТ експерти невъзможно през повечето време. Така че не-ИТ персоналът е оставен да се оправя сам.

- Непълна трансформация по дейности: Различни експерти в различни отделни офиси на организацията извършват едни и същи или подобни действия неавтоматизирано. Причината е, че няма обща услуга за дадена дейност.

- Финансови ограничения: Дигиталната трансформация може да изисква значителни инвестиции в технологии и обучение, което може да бъде проблем за някои организации. В конкретния случай съществуващият софтуер и типично хардуерно оборудване в администрациите са неподходящи или неефективни за дадена обработка, особено за големи многомерни данни (Shalamanov and Tagarev, 2021).

В резултат на това, споменатите проблеми генерират неефективност и водят до разход на значителни средства, в случай че всички локации на организацията трябва да бъдат оборудвани с много по-мощен хардуер, за да могат да се извършват необходимите изчисления на място (Dineva et al., 2022).

В този случай е необходимо да се направи преход от извършване на ежедневни дейности към предоставяне на цифрови услуги, което ще избегне някои от споменатите проблеми и ще позволи на не-ИТ експертите да се концентрират върху своите

специфични задачи. Също така, за да се реши проблемът с финансовите ограничения и изразходването на значителни средства за хардуер на различни локации на организацията, сложните изчисления биха могли да бъдат прехвърлени към централизирана система за високопроизводителни изчисления (HPC), която ще бъде подпомагана от графичен процесор (GPU) и ще се интегрира с клиентския софтуер, използвайки интерфейс за приложно програмиране (API).

4.3. Платформа за предоставяне на административни услуги

4.3.1. Описание – как работи платформата

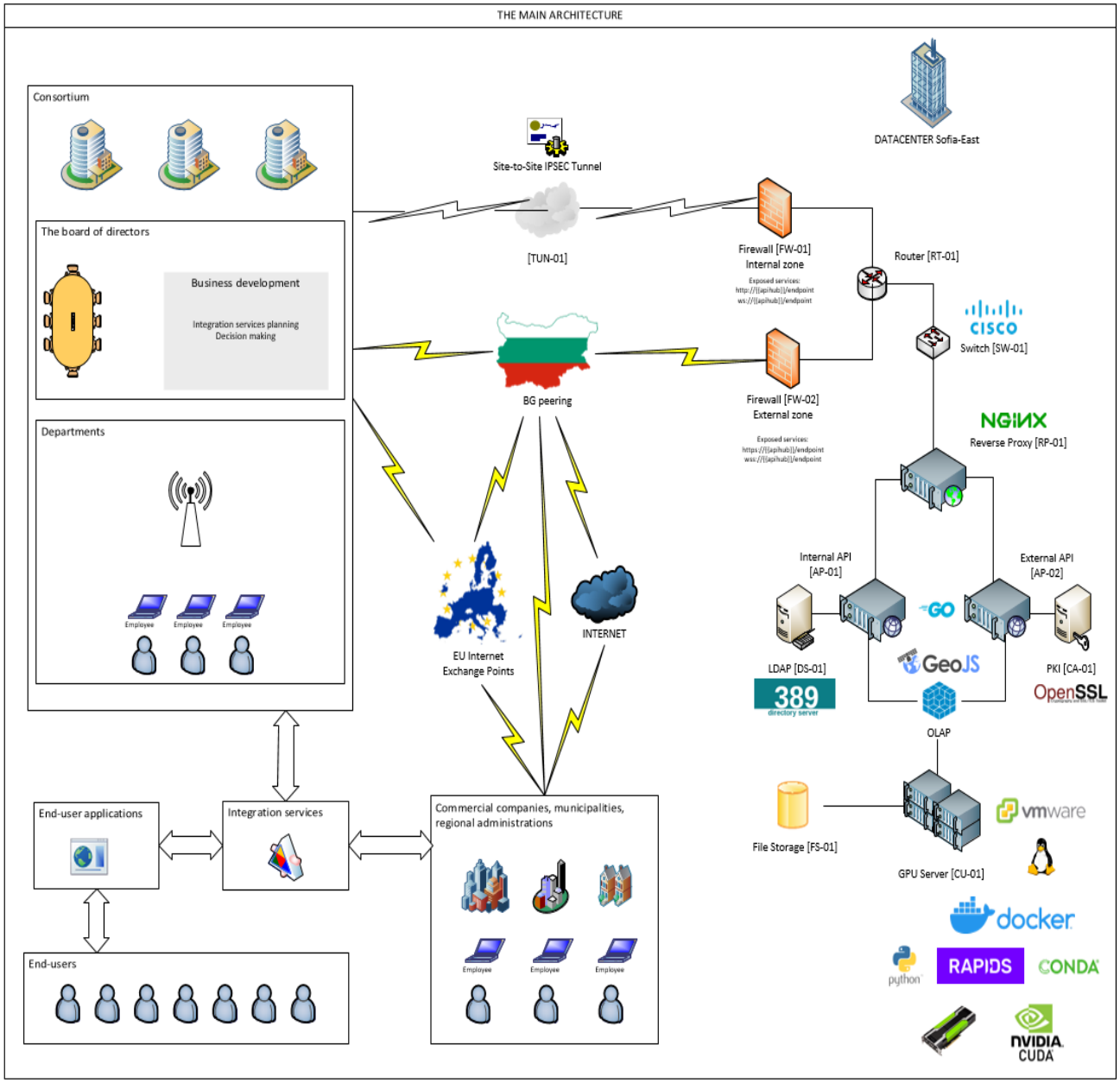
В този случай основната концепция е да се облекчат администрациите от извършването на специфични изчисления. Това означава, да се предоставят онлайн услуги за анализ на геопространствени данни (Фиг. 4.1). Същевременно партньорските организации увеличават интереса си към тази област, като създават авангардни продукти. Освен това, повечето от тях не биха искали да създават сложна инфраструктура за тази дейност и биха се отказали от разработването на собствен софтуер, който изисква задълбочени познания за многомерна обработка на данни. Следователно, те биха се съсредоточили върху разработването на високо ниво на софтуер и услуги за своя бизнес и в този случай предоставянето на онлайн аналитична услуга ще бъде чудесна възможност за това. Друг аспект на цялата картина ще бъде достъпът до данни и анонимизацията, където е необходимо.

Свързването на услуги може да бъде осъществено чрез различни комбинации от протоколи, методи, например stateful API, stateless API, grpc и много други. Това зависи от конкретната ситуация.

4.3.2. API заявки

Потребител или интеграционна услуга могат да взаимодействат с платформата съвсем чисто. Например, може да се види кратко описание на API функциите (Таблица 4.1), които обработват .json файл във формат GeoJSON, дефиниран в RFC7946. Чрез този API е възможно да се извличат обекти на свойства от масиви от характеристики, да се намират уникални ключове и да се преброи колко пъти се среща всяка уникална стойност за асоциирания ключ.

На пръв поглед този анализ не звучи особено труден за автоматизиране, но напротив, евентуалното подценяване на задачата създава потенциална възможност за вземане на напълно грешно решение относно процеса на разработка и избора на подходящи технологии за API услуги.



Фиг. 4.1. Представяне на основната архитектура на платформата, разработена в тази дисертация.

Таблица 4.1. Описание на API на GEOJSON сървъра

HTTP Method	Endpoint	Authorization	HTTP Request Body	Response
PUT	/upload	Internal – Basic Auth, LDAP back-end Scheme: **http** External – TLS Client x509 Certificate Scheme: **https**	form-data unique: optional int value (unique attributes threshold) file1: mandatory filename.json attachment Action: receives a file from the client for analysis and returns request {{uuid}}	Content-type: application/json JSON object containing status message with connection data
GET	/*{{uuid}}*/status	Internal – Basic Auth, LDAP back-end Schemes: **http, ws** External – TLS Client x509 Certificate Schemes: **https, wss**	Body: none Action: gets the current status for request {{uuid}}	Content-type: application/json JSON object containing status message with connection data
	WebSocket		Body: none Action: callback when action for request {{uuid}} is performed	Awaiting a JSON message, when the action for {{uuid}} is performed
GET	/*{{uuid}}*/download	Internal – Basic Auth, LDAP back-end Scheme: **http** External – TLS Client x509 Certificate Scheme: **https**	Body none Action: sends the result to the client for request {{uuid}}	Content-type: application/json JSON array, containing status message with connection data and result
DELETE	/*{{uuid}}*/delete	Internal – Basic Auth, LDAP back-end Scheme: **http** External – TLS Client x509 Certificate Scheme: **https**	Body none Action: immediately deletes the result for request {{uuid}} from the server explicitly from the client. The deletion process is performed on a regular basis implicitly.	Content-type: application/json JSON object containing status message with connection data

Целта на предоставянето на API услугата е, от една страна, да се даде възможност за интеграция с потенциално заинтересовани организации, които да се възползват от централизирана услуга за анализ на данни (de Castro Lima, 2018), а от друга страна, да се улеснят техническите им задачи в сравнение с това сами да предприемат действия за изграждане на собствени услуги за анализ на данни. Като важен момент трябва да се спомене, че само с изграждането на API услуги задачите по интеграция не се изчерпват, тъй като те не представляват еднократно действие във времето, а подлежат на промени и подобрения. В тази връзка е необходимо да се наблегне на CI/CD подходите, които следват установените принципи, а за организации, които не разполагат с висококвалифициран персонал, това може да бъде особено предизвикателство.

4.4. HPC услуги с техники за внедряване на CUDA

За предоставяне на високопроизводителната изчислителна услуга е разработен и имплементиран самостоятелен демон *insightd*, който работи независимо от API слоя и изпълнява аналитичните задачи върху GPU. Демонът приема подадените чрез платформата файлове с данни и заявки, извършва обработката с използване на RAPIDS/CUDA и връща резултатите към потребители или външни системи чрез междинния API/WebSocket слой. По този начин изчислителната логика е отделена от логиката по достъп, управление на заявките и известяване в реално време.

Според представения по-горе анализ на проблемите, пред които е изправена дигиталната трансформация, стана ясно, че се очаква решение за някои от често срещаните проблеми, като например високите разходи за технологии. В този конкретен случай, както и в много други, това произтича от необходимостта от компютърно оборудване с висока изчислителна мощност за множество офиси на различни места в организацията. Обработката на големи файлове изисква много RAM памет и обикновено е времеемка за процесора (Blagoev, 2018), ако се приложи добре познатата последователна итерация върху JSON обект, използваща динамични структури (напр. речници) за временно съхранение на резултата, докато цикълът завърши. Като алтернативно решение може да се избере подходът, използващ паралелни изчисления (Luebke, 2008).

За текущите услуги е разработен напълно отделен демон, който работи независимо от API услугите, чете файлове, изпратени чрез API, и извършва заявения

анализ. Демонът с име ***insightd*** е ядрото на платформата, написан е на Python и реализира 2 подхода:

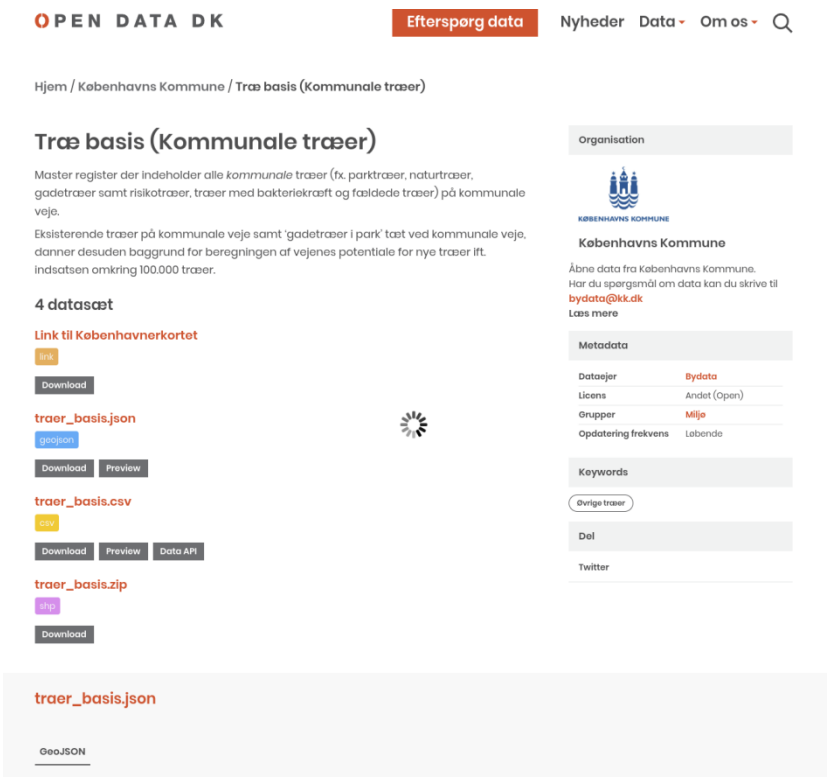
- Четенето на обекти със свойства е в стрийминг режим. Тази техника консумира минимална RAM памет. Итеративната библиотека за JSON парсер се импортира. https://pypi.org/project/ijson/
- Ключовете на свойствата се обработват паралелно. За тази техника се използва работната рамка Rapids, работеща с библиотека cudf и CUDA 6.0 съвместими графични GPU карти като минимално хардуерно изискване (Giuntaet al., 2010), (GPU Accelerated Data Science).

Използването на CUDA и RAPIDS в настоящото изследване следва да се разбира като проектно и контекстно обусловен избор, а не като универсална препоръка за всички случаи на високопроизводителни изчисления в публичния сектор. В разглеждания пилотен сценарий е използвана налична и практически достъпна NVIDIA-базирана среда, която позволява бърза реализация и проверка на концепцията за централизирана GPU-ускорена услуга. Следователно приносът на дисертационния труд е не в доказване на технологично превъзходство на конкретен доставчик, а в показване, че подобен тип изчислителна услуга може да бъде организирана и предоставяна ефективно в реална административна среда.

Чрез зареждане на свойства в паметта на графичния процесор, библиотеката преобразува линейни данни в куб с данни. За примерния файл заредените в GPU свойства изглеждат като следните редове:

```
category type
0 a park tree
1 b park tree
```

Нека видим друг пример. Файлът traer_basis.json съдържа данни за дървесно картографиране на съществуващи дървета в Копенхаген и може да бъде изтеглен от платформата за отворени данни на община Копенхаген (Фиг. 4.2), линк към ресурса: https://www.opendata.dk/city-of-copenhagen/trae-basis-kommunale-traeer.



Фиг. 4.2. Изглед на страницата за отворени данни на община Копенхаген

Размерът на този файл е достатъчен, за да изразходва ресурсите на обикновена компютърна система, но техниката за обработка CUDA позволява извършването на анализа с незначително използване на ресурсите на хост машината.

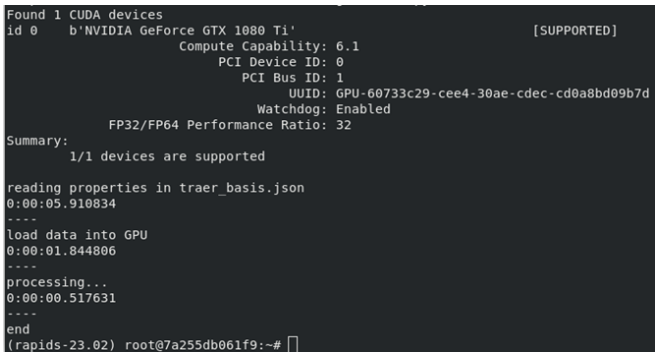
Част от куба с данни изглежда като следната таблица 4.2:

Таблица 4.2. Куб с данни

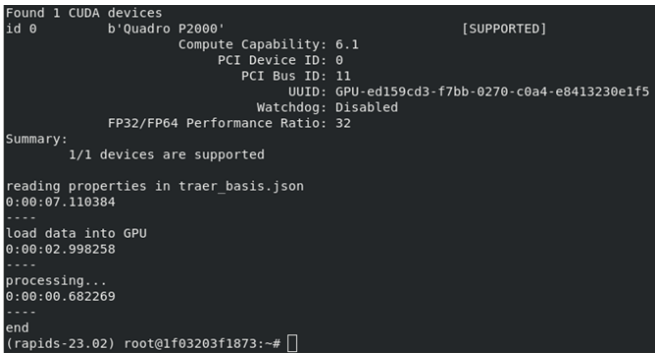
	kategori	saerligt_trae	id	type	...	torso_naeste_styning	torso_skaeres_ned_til	torso_bemaerkning	ogc_fid
0	gadetræ	nej	2667	2 Træer	...	<NA>	<NA>	<NA>	1
1	gadetræ	nej	2669	2 Træer	...	<NA>	<NA>	<NA>	2
2	gadetræ	nej	2676	2 Træer	...	<NA>	<NA>	<NA>	3
3	gadetræ	nej	2680	2 Træer	...	<NA>	<NA>	<NA>	4
4	gadetræ	nej	2681	2 Træer	...	<NA>	<NA>	<NA>	5
...	...	...	...	...	...	...	...	...	...
63737	parktræ	nej	96431	2 Træer	...	<NA>	<NA>	<NA>	63738
63738	parktræ	nej	96413	2 Træer	...	<NA>	<NA>	<NA>	63739
63739	privat træ	nej	18679	2 Træer	...	<NA>	<NA>	<NA>	63740
63740	gadetræ	nej	82463	2 Træer	...	<NA>	<NA>	<NA>	63741
63741	gadetræ	nej	100017	2 Træer	...	<NA>	<NA>	<NA>	63742

[63742 rows x 192 columns]

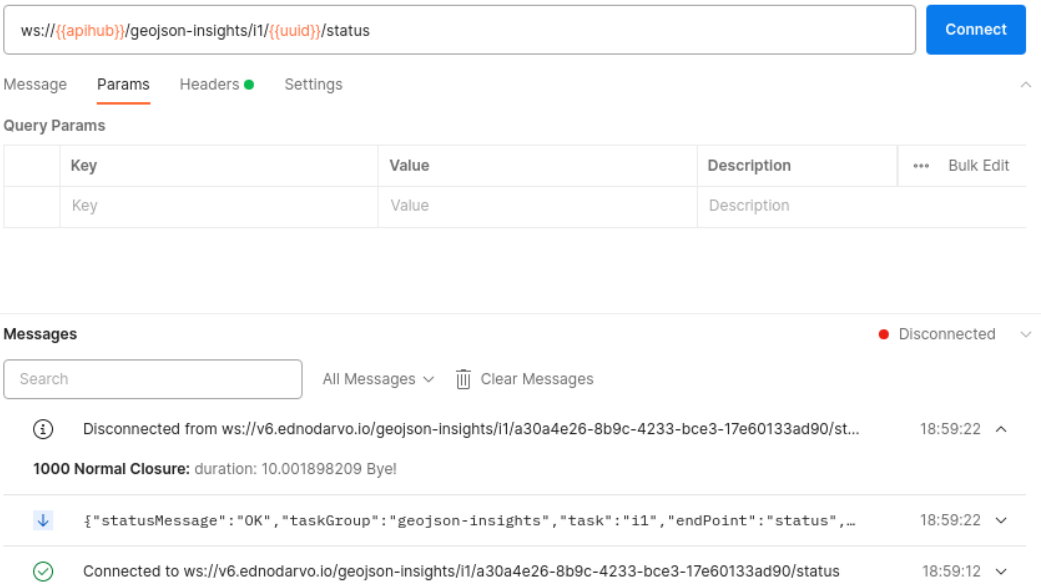
За тестовете са използвани два модела графични процесора на различни хостове, но резултатите от производителността са сходни (Фиг. 4.3, 4.4).



Фиг. 4.3. Около 8 секунди.

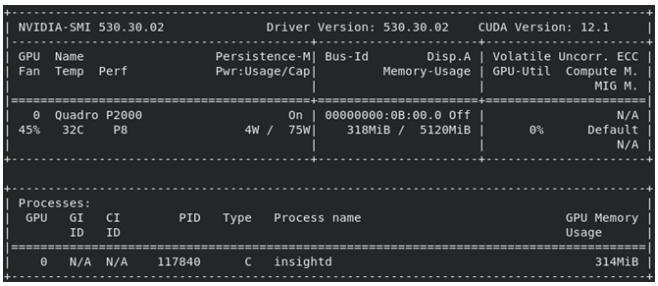


Фиг. 4.4. Около 10 секунди.



Фиг. 4.5. Съобщенията на WebSocket

Последният екран (Фиг. 4.5) показва съобщенията на WebSocket, докато обработката на traer_basis.json завършва. Тестовата среда на платформата използва Nvidia Quadro P2000 GPU и продължителността в секунди напълно съответства на тестовите скриптове.



Фиг. 4.6. При нормална работа, процесът на демона консумира между 300 и 500 MiB памет на графичния процесор.

От постигнатите в предишните глави реално резултати става ясно, че централизацията на по-сложните изчисления в този случай, като например частния облак за високопроизводителни изчисления, е полезна за решаване на няколко проблема:

- В този случай няма нужда от препроектиране и интегриране на всички софтуерни системи в организацията, за да се използва CUDA и да се добавят възможности за извършване на тези изчисления;
- При интегриране с трети страни, като например партньорски организации, приложеният подход може да се използва и разходите могат да бъдат намалени;
- Ако услугата за високопроизводителни изчисления (HPC) се нуждае от надграждане, това ще се извърши на едно място и няма да се променят множество софтуерни системи;
- Позволява интеграция със системата на различни видове устройства, дори устройства на полево ниво, не само мощни компютърни работни станции;
- Намаляване на разходите за поддръжка на софтуерните системи на организацията, които ще трябва да обработват тези данни. Защото е много по-лесно да се интегрира с API услуга, отколкото да се използват високоплатени експерти за внедряване на паралелни изчисления в системите;

- Намаляване на разходите за високопроизводителен хардуер, инсталиран локално в организацията;
- Намаляване на разходите за енергия. Централизираните решения от този тип водят до намаляване на нуждата от допълнителен хардуер, което съвсем логично води до намаляване на потреблението на електроенергия. Тези два аргумента подкрепят и усилията за намаляване на въздействието върху околната среда.

В този конкретен случай, освен дигиталната трансформация, представеният проект е част от плановете за интелигентни градове. Развитието на дигитализацията, интелигентните градове, потреблението на енергия и намаляването на разходите са от съществено значение за настоящия технологичен преход. За това може да се каже, че използването на централизирани облачни технологии за паралелни изчисления би било от решаващо значение за справяне с възникващите предизвикателства. Съвременният свят използва цифрови технологии във все по-голям мащаб и непрекъснато внедрява цифрови и комуникационни устройства във все по-широк спектър от човешки дейности. Всичко това генерира огромни количества данни, което ще създаде глад за тяхната обработка. OLAP услугите и паралелните изчисления няма да останат като малко използвани луксове, напротив, повечето организации ще обмислят внедряването им в ежедневната работа. Изследването представи само един конкретен пример, който доказва, че използването им в средата на държавните и общинските администрации е напълно възможно и от решаващо значение за справяне с възникващите предизвикателства.

4.5. Федеративен AIS облак за предоставяне на услуги

Показаният в предходния раздел модел демонстрира как натрупани в течение на времето данни могат да бъдат събрани в една точка и обработени ускорено чрез централизирана услуга с паралелни изчисления. При този тип задачи паралелизмът е вътрешен за самата обработка: голям масив от данни се разпределя върху множество изчислителни ядра, които изпълняват едни и същи операции върху различни части от

входа. При потокови услуги в реално време, каквато е AIS телеметрията, подобна логика не може да бъде пренесена механично. Там данните не се натрупват първо, за да бъдат обработени впоследствие като голям пакет, а пристигат непрекъснато от множество източници и изискват незабавни действия по приемане, нормализация, дедупликация, евентуално географско филтриране и доставка. Така паралелизмът тук ще се разглежда в различна архитектурна перспектива: не като ускоряване на една централизирана изчислителна задача, а като едновременно и координирано изпълнение на едни и същи операции върху множество логически потоци, съществуващи паралелно във времето.

4.5.1. Концептуална постановка за дизайн на федеративен AIS облак

Федеративният AIS облак трябва да бъде проектиран така, че да работи и в масовия „домашен“ интернет сценарий, включително при частни адреси, динамични IP адреси и CGNAT. Затова са необходими познати техники за преодоляване на мрежовите ограничения, включително установяване на свързаност между възли, междинно препредаване при нужда и прагматичен подход към участници, при които не може да се изисква статичен публичен адрес или ръчно отворени портове.

Необходимо е ясно разделение между управляващ слой (control-plane), който обхваща идентичностите, конфигурациите и политиките, и слоя за данни (data-plane), който пренася самия AIS поток. Подобно разграничение е в съзвучие с разгледаните по-рано услуги, при които има отделяне между плейлист и сегменти при HLS и между контролен интерфейс и изчислителен поток при API/WebSocket базираните GPU услуги (Fette and Melnikov, 2011).

Дедупликацията следва да се разглежда като потокова задача с времева семантика на събитията и с ясно дефинирани времеви прозорци. За исторически анализи са по-подходящи предварително агрегирани времеви серии и индекси, а при обработка на големи геопространствени масиви от данни могат да се използват ускорени изчислителни подходи върху GPU ресурси (Akidau et al., 2015), (Butler et al., 2016).

Сигурността следва да бъде заложена „по подразбиране“ чрез ясно дефинирани идентичности и механизми за защита срещу повторно възпроизвеждане на пакети. Слоестият подход, при който мрежовата защита и защитата на медийния или приложния слой се разглеждат като взаимно допълващи се, повишава интероперабилността и

устойчивостта в хетерогенна среда (Rescorla, 2021), (Baugher et al., 2004), (McGrew and Rescorla, 2010), (Kent and Seo, 2005).

Федеративният модел изисква и обща референтна архитектура за обмен между домейни, включително по отношение на идентичност, политики и одит. В този смисъл приложим е опитът от референтните архитектури за облачна федерация, които дефинират роли, интерфейси и правила за взаимодействие между автономни участници (Lee et al., 2020).

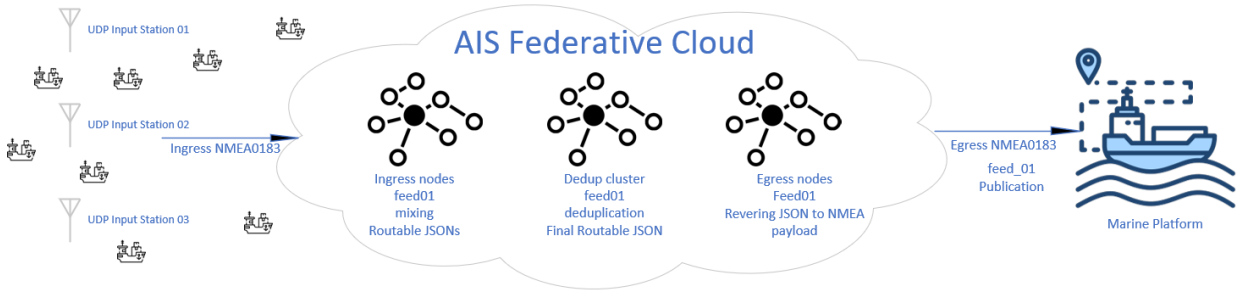
В настоящия раздел е предложена архитектура на федеративен AIS облак като пример за преход от управление на асети към управление на услуги в среда с множество автономни участници, разпределени точки за прием и необходимост от координирано предоставяне на телеметрични данни. За разлика от централизирания модел, при който всички потоци и управленски функции се концентрират в един оператор, тук се предлага федеративен подход, при който отделни автономни системи запазват своята вътрешна независимост, но взаимодействат чрез общи интерфейси, договорени роли и правила за отговорност. AIS асетите се преорганизират в среда, способна да осигури мащабируемост, устойчивост, дедупликация и контролирано споделяне на данни в сложна разпределена среда.

4.5.2. Архитектурни принципи

Под „федеративен облак“ в настоящия контекст се разбира архитектура, при която няма един централен оператор на всички данни. Вместо това множество независими оператори, разглеждани като автономни системи (AS), участват със собствени ресурси и взаимодействат чрез разделение между управляващ слой (control-plane) и слой за данни (data-plane). Управляващият слой би включвал сесии за сдвояване, откриване на съседи, маршрутни анонси, отчетност и тн. Слоят за данни включва реалния поток от AIS данни (NMEA/полета/структурирани полезни данни). Това разделение позволява слоят за данни да бъде прост и високопроизводителен, докато управляващият слой носи сложността.

Вътрешната архитектура на всяка AS е напълно автономна (може да е един процес или голям клъстер), а общото поведение се формира от стандартен външен интерфейс:

идентичност (с механизми на асиметрична криптография), функционални възможности и правила за сдвояване, отчетност.



Фиг. 4.7. Обща архитектурна схема на AIS федеративен облак, предложена в тази дисертация

4.5.3. Роли и принципи на отговорност

Ролите Ingress, Transit/bridge, Dedup/aggregator, Egress не са фиксирани за дадена AS. Една и съща AS може да изпълнява различни роли за различни логически потоци. Федеративният характер идва от това, че системата не налага един „правилен“ софтуер, всеки оператор може да избере технологичен стек, стига да поддържа интерфейса към останалите.

- Ingress (listener): приема трафик от физически станции. Типично: UDP поради простота на потребителската настройка.
- Transit/bridge: препредава между автономни системи и/или преобразува транспортни протоколи (напр. MQTT↔WS, gRPC↔AMQP).
- Dedup/aggregator: миксира множество входове, премахва дубликати, нормализира и формира чист поток. Описание на софтуер, който реализира тези функционалности https://aismixer.net/, github repository: https://github.com/iliyan85/aismixer
- Egress: доставя чист поток към морска платформа, без очакване за обратен ACK от платформата.

4.5.4. Коментари от гледна точка на практика

Тук е важно да се подчертае, че предложеният подход не разглежда свързаността от тип точка до точка като теоретична хипотеза, а като практически овладян модел на работа в среда с ограничена адресна достижимост, който ще бъде разгледан в следващата глава. Приблизителната работна хипотеза е, че ~94% от възлите биха били зад NAT с динамични адреси и без административен достъп до отваряне на портове; ~5% потенциално имат публичен IPv4 адрес и едновременно с това административни правомощия, като биха могли да управляват порт пренасочването; ~1% имат публичен IPv6 адрес или дори /64 сегмент, което означава, че могат да се сдвояват директно по IPv6. В последващата глава, където се разглежда хибридно VoIP решение, е показано, че директният обмен на полезния трафик между отдалечени локации може да бъде реализиран надеждно чрез виртуална наслагваща свързаност и директен канал между участниците, докато централен компонент изпълнява управляващи функции. В архитектурата на федеративния AIS облак същият принцип се обобщава: административното сдвояване и управляващата координация предхождат и разрешават техническия обмен между възлите, така че трафикът с полезните данни да се предава директно между съответните AS, без да имаме концентрация в транзитен преносен център.

От практическа гледна точка предложеният модел следва да отговаря едновременно на изисквания за лесно включване на нови участници, съвместимост със съществуващите морски платформи и устойчиво нарастване на броя възли без концентрация на обработката в един център:

- Plug&play за неспециалист: настройка с минимални параметри (най-често само дестинация, описана с IP+порт).
- Съвместимост с текущите морски платформи: изход като традиционен NMEA 0183 поток (!AIVDM).
- Реално време и плътно крайбрежно покритие: приоритет за минимална латентност и висока „навременност“ чрез гъста наземна мрежа и локална дедупликация;
- Мащабируемост: да работи с много станции и множество оператори без зависимост от централен възел и без формиране на единна точка на отказ.
- Доверие и проследимост: да е трудно някой да се представи за доверена страна без ключ/подпис.

- Надеждност при NAT и динамични връзки: поддръжка на P2P канали, резервни пътища и препредаване.
- Контролирана репликация: допустима преди услугата за дедупликация dedup, нежелана след dedup.
- Възможност за „пазар“ на услуги: различни автономни системи да предлагат ingress/dedup/transit/egress.

4.5.4.1. Плътност на наземните станции и „реално време“: защо облакът цели прием близо до източника

Нормативните спецификации за AIS подчертават реално-времевия характер на системата: AIS е автономен, самоорганизираща (без master), а тактическата информация трябва да се обменя непрекъснато (типично поне на 10 s, при някои маршрути до 2 s). За да се постигне подобна „жива“ картина в крайбрежни райони, решаваща е плътността на наземните приемници: всяка допълнителна антена/приемник точка не само разширява геометричното покритие, но и повишава вероятността за прием на слаби/частично закрити предавания. Проблемът е, че повече приемници означава повече повторения на едни и същи AIS репорти, които „наводняват“ изхода към платформите. Точно тук федеративният облак има системна стойност: той позволява плътна крайбрежна мрежа за прием в реално време, а едновременно с това извършва дедупликация и нормализация преди доставката към платформи.

4.5.4.2. Аналогии от интернет и разпределени системи

Междудомейн рутирането чрез BGP използва постоянно установени т.нар. peering сесии за обмен на маршрутна информация между автономни системи (RFC 4271). MPLS предлага логическа абстракция на пътя чрез етикети, полезна като метафора за „логически поток“ и класове трафик (RFC 3031). P2P DHT системи като Kademlia (Maymounkov et al., 2002) показват как децентрализирани възли откриват ресурси/пътища без централен контрол. В масовия целеви сценарий участниците в облака са малки оператори. Пътищата могат да се изменят динамично по различни причини от практиката, свързани с преконфигурирания от страната на интернет доставчика, временни прекъсвания и тн. Централната маршрутизация е анти-федерирана и често остарява; затова се предпочита търсене в локалния граф на свързаностите. Типичен алгоритъм е BFS по съседи с време на живот (TTL) спрямо лимит на скокове и с кеш на успешната следваща цел.

4.5.4.3. Защита на идентичността и данните отвъд транспортния слой

Разгледаните в предходните глави въпроси на асиметричната криптография, избора на по-леки и приложими схеми с елиптични криви, управлението на идентичности и защитата на транспортния канал са пряко релевантни и към федеративния AIS облак. Защитата само на транспортно ниво, например чрез тунелиране или криптиран канал между две точки, е необходима, но не е достатъчна в среда с множество автономни участници и с възможно преминаване на потока през повече от един възел. В подобна архитектура е необходимо произходът и целостта на данните да останат проверими и отвъд конкретния транспортен сегмент. Поради това защитата на приложно ниво може да се разглежда като естествено допълнение към транспортната защита: идентичността на участника се удостоверява чрез механизми на асиметрична криптография, а полезните данни и придружаващите ги метаданни могат да бъдат подписвани така, че да останат валидируеми по целия път на услугата. В този контекст по-леките схеми с елиптични криви са особено подходящи, тъй като позволяват практична защита в разпределена среда с ограничени ресурси. По аналогия с разгледания в предходната глава принцип за отделяне между съдържание и удостоверяване, и тук транспортът, идентичността и самите данни следва да се разглеждат като различни, макар и взаимосвързани слоеве на услугата.

4.6. Изводи

Четвърта глава показа, че преходът към управление на услуги в публичния сектор може да се реализира чрез различни, но допълващи се архитектурни режими. В първия случай сложните изчисления върху натрупани геопространствени данни се централизират и ускоряват чрез GPU-базирана услуга, при която паралелизмът е вътрешен за самата задача и води до съкращаване на времето за обработка и до намаляване на локалните изисквания към администрациите. Във втория случай, при федеративния AIS облак, паралелизмът се проявява не вътре в една изчислителна задача, а на нивото на услугата, където множество логически потоци съществуват паралелно във времето и преминават през едни и същи сервизни операции по приемане, нормализация, дедупликация и доставка. По този начин главата демонстрира два комплементарни подхода към service-centric трансформацията: централизирано изчислително ускорение

и разпределена федеративна организация на потокова услуга. От криптографска гледна точка разгледаната архитектура потвърждава, че за федеративния AIS облак ECC е по-подходящият избор спрямо RSA, тъй като позволява практична защита на приложно ниво, по-компактни подписи и по-нисък ресурсен overhead в среда с множество автономни участници и edge възли.

Именно това двойно решение подготвя и следващата глава, в която фокусът се измества от конструиране на услугата към въпроса какви проблеми в реална среда тя може да оптимизира и какъв системен ефект може да произведе, включително в контекста на морската сигурност и проект като DANRISS. Така четвърта глава извежда модела ориентиран към услуги отвъд комуникационните услуги и го подготвя за най-сложните случаи на реалновремева комуникация и федеративна телеметрия изразени формално и практически, осветяващи оптимизирането на прехода от управление на асети към управление на услуги.

Съдържанието на тази глава е отразено в следната публикация:

1. Iliev and I. Blagoev, "Centralized Parallel Computing as a Cloud Service for Solving Digital Transformation Problems in Smart Cities," 2023 4th International Conference on Communications, Information, Electronic and Energy Systems (CIEES), Plovdiv, Bulgaria, 2023, pp. 1-4, doi: 10.1109/CIEES58940.2023.10378756.

ГЛАВА 5. Оптимизация на прехода от управление на асети към управление на услуги

В настоящата глава се разглеждат архитектурни решения, чрез които преходът от управление на асети към управление на услуги се реализира в среди с реални инфраструктурни ограничения. Акцентът е поставен върху два представителни казуса: хибридно VoIP решение за комуникация в регионална среда с NAT ограничения и федеративен AIS облак за събиране, обработка и предоставяне на телеметрични данни. И в двата случая се търси не просто избор на технология, а архитектурна организация на асетите така, че да се постигнат надеждност, сигурност, ниска латентност и практическа приложимост.

5.1. Управление на услуги при регионални интернет доставчици, демонстрирано в контекста на хибридно VoIP решение

5.1.1. VoIP технологии

VoIP технологиите са се превърнали в ключов инструмент за корпоративната комуникация, като позволяват оптимизация на разходите и интеграция с множество цифрови услуги. Тяхното качество обаче е силно зависимо от интернет инфраструктурата, което създава предизвикателства при използването им в региони с ограничени ресурси. В настоящото изследване се разглеждат реалните проблеми, свързани с внедряването на VoIP телефония в среда с регионални доставчици на интернет услуги, липса на публични IP адреси, невъзможност за изграждане на MAN връзки и повишена латентност. Като решение е предложена хибридна архитектура, при която Asterisk PBX в дейта център изпълнява функцията на централен SIP сървър, докато RTP аудио потоците се предават по peer-to-peer модел чрез защитени тунели. Валидирането на подхода е извършено чрез експериментални измервания на латентност, jitter и загуба на пакети, както и чрез анализ на SIP и RTP трафика с Wireshark. Резултатите показват, че архитектурата позволява надеждна VoIP телефония с високо качество на разговорите, въпреки ограниченията на регионалните ISP, и може да бъде приложена като модел за други организации със сходни предизвикателства.

5.1.2. Постановка на проблема

VoIP, като ефикасна технология в комуникационната индустрия, трансформира гласа в данни, позволявайки му да бъде обработван, записван, криптиран и интегриран с други системи. VoIP лесно се интегрира със CRM, ERP, helpdesk и инструменти за колаборация (Teams, Slack, Zoom), поддържайки омниканална комуникация (глас, чат, видео, имейл), което е предпоставка за ускоряване на дигиталната трансформация на бизнеса чрез унифицирани комуникации (Borissova, Dimitrova, Dimitrov, 2020). От друга страна, VoIP генерира предизвикателства за анализ на данни: анализ на обажданията, анализ на настроенията, KPI за обслужване на клиенти, които могат да захранват AI решения и автоматизация (Borissova and Mustakerov, 2012), (Mustakerov and Borissova 2013).

VoIP технологиите отдавна са се утвърдили като важен инструмент за корпоративна комуникация, позволявайки оптимизиране на разходите и интеграция с множество цифрови услуги, като същевременно подобряват поверителността и споделянето на информация (Saenger et al., 2020). Ситуацията обаче е различна в регионалните и периферните населени места, където доставчиците на интернет услуги (ISP) често предлагат ограничена инфраструктура, липса на публични IP адреси, трудности при изграждането на MAN връзки и нестабилни канали за пренос на трафик. Тези ограничения пряко възпрепятстват нормалното функциониране на VoIP решенията, което води до висока латентност, загуба на пакети и невъзможност за гарантиране на качеството на услугата (Rao et al., 2024).Настоящото изследване разглежда именно този проблем, като се фокусира върху предизвикателствата пред VoIP комуникацията в условията на регионални ISP. В настоящата дисертация е представено иновативно архитектурно решение, което комбинира централизирана SIP сигнализация чрез Asterisk PBX и децентрализиран P2P пренос на RTP аудио потоци посредством защитени тунели. Подходът цели да минимизира негативните ефекти от ограниченията на регионалната интернет инфраструктура и да осигури надеждно качество на гласовата комуникация, сравнимо с това в големите градски мрежи.

5.1.3. Предложен архитектурен подход

За да се илюстрира на практика посоченият проблем, в настоящото изследване е разгледан реален случай от корпоративна среда. Логистичната и спедиторска компания, оперираща с офиси в градовете Варна и Балчик, се сблъсква с ограниченията на

регионалните интернет доставчици. Липсата на публични IP адреси, отсъствието на възможност за изграждане на MAN свързаност и нестабилните канали за данни правят невъзможно внедряването на класическо VoIP решение, базирано на централизирано маршрутизиране на аудио потоци през PBX.

В отговор на тези ограничения е разработен нетрадиционен подход, при който Asterisk PBX, разположен в дейта център в София, изпълнява единствено функцията на сигнализационен сървър (SIP), докато аудио потоците се предават директно по P2P модел между офисите чрез защитени тунели. Този модел цели да елиминира зависимостта от ограничените ресурси на регионалните ISP и да осигури надеждно и висококачествено гласово общуване в условията на реална бизнес среда.

Средното разстояние по шосе между Варна и Балчик е в порядък до 30-40 км в зависимост от избрания маршрут. Тази мярка за разстояние може да бъде взета предвид и за оптичните линии, понеже комуникационните трасета следват в максимална степен вече установени трасета, т.е. от гледна точка на телекомуникациите, географското разстояние между кои да е 2 точки в района е пренебрежимо малко. Но практиката при реализиране на логически комуникационни връзки, показва друга картина.

Въпреки близостта на Балчик до Варна и независимо от избора на интернет доставчик там – национален, варненски или местен, интернет свързаността, която се предлага за частни или бизнес клиенти в Балчик по стандартните планове е ниска (**Проблем 1**), няма практика за предоставяне на усъвършенствани L2/L3 услуги (**Проблем 2**) и е наблюдавана голяма латентност в комуникацията дори между близко разположени географски точки (**Проблем 3**).

Проблем 1 е свързан с предоставян твърде малък bandwidth на фона на съвременните нужди за Интернет свързаност (порядъци на 20-50 Мбит/с при местните ISP и 50-100 Мбит/с за националните и варненски ISP).

Проблем 2 – рядко предоставяне на публични IP адреси и никаква практика за предоставяне на услуги в MAN, като QinQ VLAN, DARKFIBER, MPLS, VPLS.

Проблем 3 е фокусът на изследването и засяга латенцията между всеки 2 комуникиращи точки през интернет доставчиците. Същата зависи от свързаността между самите доставчици. Ниска латенция може да се постигне с вътрешни маршрути, които се договарят и установяват между самите доставчици. Без тази вътрешна информация, как са се „договорили“ доставчиците, отвън е трудно да се направи бизнес планиране на

ресурсите. Вътрешните договорки са твърде остарял подход, датиращ от зората на Интернет и ранните LAN ISP.

Модерният подход за връзки между ISP се осъществява с участие в т.нар. IXP, разгледани в статиите “Impact Of Internet Exchange Points On ISPs Speeds And Latency”(Dabone at al., 2022), “Estimating the effects of Internet exchange points on fixed-broadband speed and latency” (Vakataki, 2021) и “There is More to IXPs than Meets the Eye“ (Chatzis et al., 2013). Информацията за участниците в даден IXP е публична, което означава, че може да се направи прецизно бизнес планиране при избор на доставчици, така че предварително да е известно, кои два или повече от доставчика в даден IXP, биха могли да гарантират ниска латенция между мрежовите терминиращи устройства на абонатите. Пример със списък от членове и автономните им системи във VarnaIX https://www.varnaix.net/en/members.html

Обичайната латенция между София и Варна е в порядък 11 милисекунди, измерена – 11.2 ms (Фиг. 5.1) и малко над 11 ms между София и Балчик, измерена 11.6 ms (Фиг 5.2).

ADDRESS	LOSS	SENT	LAST	AVG	BEST	WORST	STD-DEV
87.121.0.17	0%	36	0.8ms	0.9	0.3	6.3	1
212.73.157.250	0%	35	0.6ms	1.3	0.3	20.3	3.3
87.120.206.130	0%	35	0.7ms	0.7	0.5	1.2	0.1
130.204.74.2	97..	35	timeout	8.4	8.4	8.4	0
130.204.74.12	0%	35	11ms	11.2	10.9	12.1	0.2

Фиг. 5.1. Времезакъснение на сигнала между София и Варна

ADDRESS	LOSS	SENT	LAST	AVG	BEST	WORST	STD-DEV
87.121.0.17	0%	35	0.7ms	1	0.6	7.6	1.1
212.73.157.250	0%	35	0.6ms	0.7	0.6	1.9	0.3
185.1.226.144	0%	35	0.7ms	0.7	0.6	0.8	0
185.205.208.182	0%	35	11.7ms	11.7	11.7	11.8	0
46.253.1.29	0%	35	11.6ms	11.6	11.6	11.7	0

Фиг 5.2.Времезакъснение на сигнала между София и Балчик

Наблюдаваните стойности гравитират около 11 ms, което се явява и близо до теоретичната стойност за трасетата и географската отдалеченост между точките (~500 км).

От друга страна, теоретичната латенция между Балчик и Варна трябва да е между 1-2 милисекунди. Приемливо от практическа гледна точка би била и стойност 3. Но времезакъсненията между клиентски устройства в различни ISP са далеч от тези теоретични стойности. Фиг. 5.3 показва резултат от измерване на латенцията между клиентски рутер в Балчик и рутер на доставчик във Варна, а Фиг5.4 - в обратната посока.

ADDRESS	LOSS	SENT	LAST	AVG	BEST	WORST	STD-DEV
192.168.189.1	0%	35	0.4ms	0.4	0.3	1	0.1
192.168.223.1	0%	35	1.2ms	0.9	0.5	1.4	0.2
193.43.105.1	0%	35	0.9ms	0.9	0.8	1.1	0.1
84.43.190.29	0%	35	1.9ms	2	1.8	3.5	0.3
185.1.137.154	0%	35	10.9ms	10.9	10.5	11.6	0.2
130.204.74.12	0%	35	13.9ms	13.6	13.1	14.2	0.2

Фиг 5.3.Времезакъснение на сигнала между клиентски рутер в Балчик и рутер на доставчик във Варна

ADDRESS	LOSS	SENT	LAST	AVG	BEST	WORST	STD-DEV
192.168.100.1	0%	36	0.6ms	0.5	0.4	0.8	0.1
87.227.218.2	0%	36	3.4ms	3.4	3.1	4.2	0.3
78.83.181.113	91..	36	11.2ms	11	10.9	11.2	0.1
78.83.181.114	0%	35	10.9ms	11.3	10.9	11.6	0.2
84.43.190.30	0%	35	12.8ms	13	12.7	13.7	0.3
46.253.1.29	0%	35	12.9ms	13	12.7	13.4	0.1

Фиг 5.4.Времезакъснение на сигнала между рутер на доставчик във Варна и клиентски рутер в Балчик

Измерени са средни стойности от ~13 милисекунди, което е далеч от теоретичната стойност. Наблюденията сочат за нелогичен скок от 8-9 ms и в двете посоки, какъвто не би трябвало да има в рамките на такова късо трасе. Без тези скокове, латенцията би била малко над прага на теорията.

Трите проблема са взаимосвързани и са описани в статията “Peering vs. transit: Performance comparison of peering and transit interconnections” (Ahmed et al., 2017).

За да бъдат преодолени тези ограничения, беше проектирано хибридно VoIP решение, което комбинира централизирана SIP сигнализация и децентрализиран P2P пренос на аудио потоци. В следващия раздел е представена неговата архитектура и начин на работа.

5.1.4. Хибридна архитектура и решение на проблемите

За преодоляване на описаните ограничения е предложена хибридна архитектура с две функционално разграничени части: централизирана част за SIP сигнализацията и децентрализирана част за преноса на RTP аудио потоците.

Архитектура на VoIP решението:

1 Централата Asterisk PBX е инсталирана и работи в Дейта център в гр. София. Същата управлява само SIP, като не преминава RTP аудио трафик през нея (Ahmed & Mansor, 2008).

2 Изграден е VPN с топология звезда между дейта центъра и всеки офис за пренос на SIP. Защитата на трафика е с IPsec.

3 Аудио потоците се предават P2P между хардуерните телефони Cisco SPA502G и/или софтуерните MicroSIP, инсталирани и работещи в офисите на логистичната и спедиторска компания XYZ във Варна и Балчик.

4 Връзките между офисите и централата се осъществяват с P2P VPN решението ZeroTier за предаване на аудиото. Защитата на трафика е с IPsec върху ZeroTier.

Представената на диаграма на Фиг. 5.5 обобщава архитектурата на решението: Asterisk PBX е разположена в дейта център в София и обслужва само SIP сигнализацията, докато RTP аудио потоците се предават директно между офисите посредством P2P тунели през ZeroTier и IPsec защита. В тази архитектура всеки офис разполага със собствена Voice VLAN мрежа (напр. 192.168.90.0/24 във Варна и 192.168.190.0/24 в Балчик), а устройствата – хардуерни телефони и софтфони – регистрират вътрешните си номера (11XX, 12XX, …) към централата.

Изборът на ZeroTier в настоящото решение не следва да се разбира като универсално предпочитание към конкретна VPN технология, а като контекстно обусловен архитектурен избор. В целевия сценарий комуникиращите точки могат едновременно да се намират зад NAT на доставчици, без контрол върху пренасочването на портове и без гарантирано наличие на публични IP адреси. При такива условия класическите тунелни решения, които предполагат поне една управляемо адресируема крайна точка, не са достатъчни сами по себе си. Поради това е избран подход, който позволява динамично изграждане на защитени peer-to-peer канали в NAT-ограничена

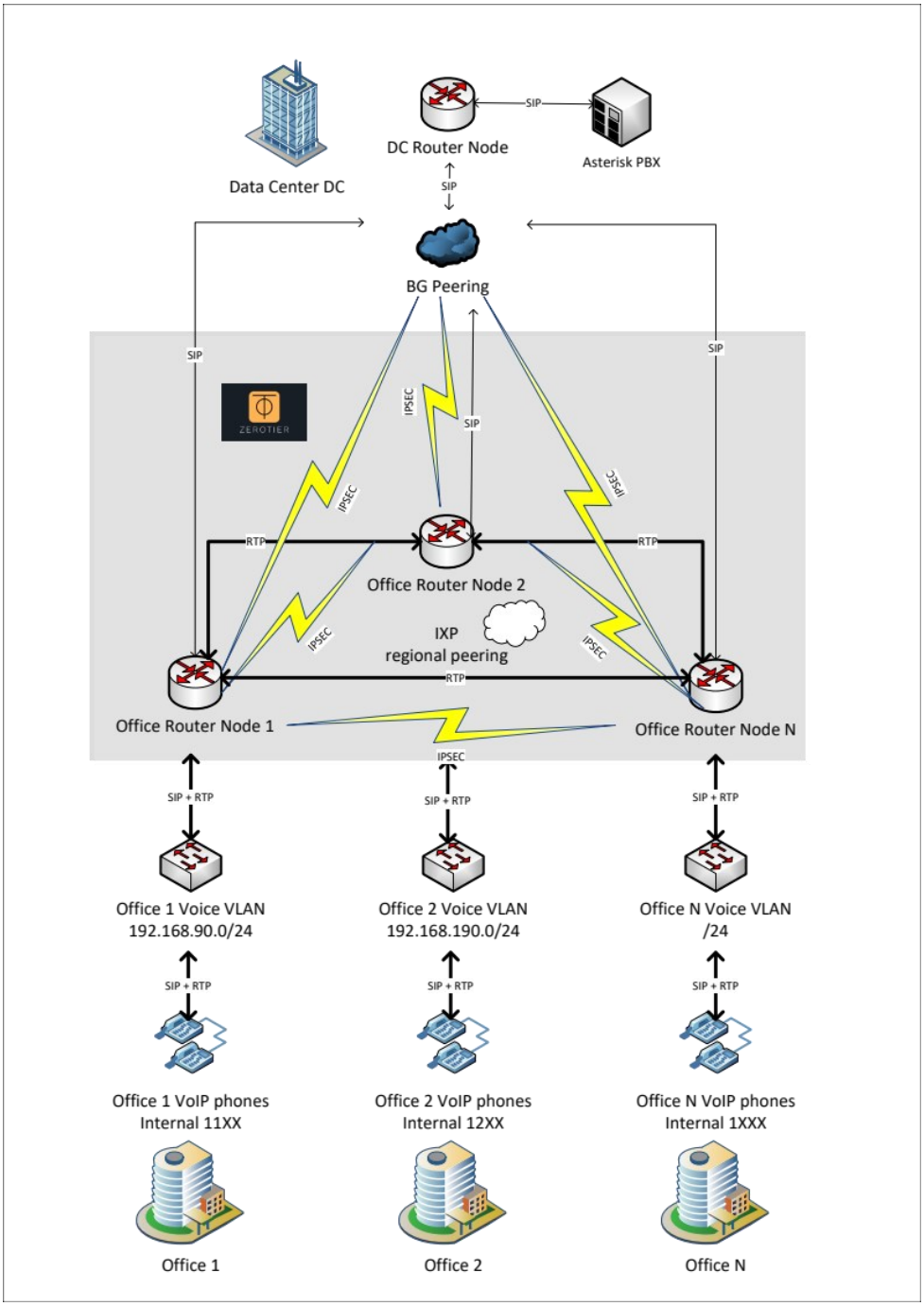
среда, като ZeroTier изпълнява ролята на практически приложим свързващ механизъм, а не на самоцелна технологична зависимост (ZeroTier. The Protocol).

ZeroTier предоставя тип край-до-край криптографски защитена peer-to-peer свързаност и по този начин адресира проблема на достижимостта в NAT-ограничена среда. В разглеждания случай обаче е избран и допълнителен защитен слой, управляван в рамките на самата организация, с цел политиките по защита на полезния трафик, удостоверяване и контрол върху защитната конфигурация да бъдат отделени от функцията по изграждане на виртуалната свързаност. Такъв подход следва логиката на многослойната защита и съответства на практиката допълнителни криптографски механизми да се използват върху вече изградена overlay свързаност, когато се търси по-ясно разграничение между транспортна достижимост и организационно контролиран защитен периметър (Gentile et al., 2024).

След установяване на виртуалната IP свързаност между локациите чрез ZeroTier възниква отделен архитектурен въпрос: кой механизъм е най-подходящ за допълнителна защита на гласовия трафик. В криптографски аспект този защитен слой следва логиката, аргументирана във втора глава, а именно че за разглежданите в дисертацията разпределени услуги ECC е по-подходящ избор от RSA, когато се търси баланс между сигурност, латентност и ресурсна ефективност. В разглеждания случай IPsec е избран не като универсално по-добро решение, а като мрежов защитен слой, който естествено работи върху вече налична IP достижимост. Изборът му е обусловен не само от защитата на Voice VLAN трафика, а и от факта, че между локациите се пренасят и други вътрешноорганизационни IP мрежи и услуги. Това позволява чрез policy routing и единен защитен канал да бъдат пренасяни множество логически мрежи, без да се изграждат отделни ad hoc решения за всяка услуга и без да се усложняват излишно статичните маршрутни таблици на маршрутизиращите устройства. При директна IP видимост IPsec защитава трафика на ниво IP чрез ESP, докато при NAT използва стандартизирания режим NAT Traversal с допълнителна капсулация и експлоатационно натоварване. WireGuard е модерна и ефективна алтернатива, но транспортът му остава UDP-базиран и след установяване на сесията, а OpenVPN е приложим, но по-тежък за този тип вече IP-ориентирана L3 свързаност. Поради това изборът на IPsec тук е обоснован от ролята му на широко поддържан мрежов стандарт за защита върху вече установена виртуална IP видимост, а не от предварително фиксирано технологично предпочитание.

Критерий	IPsec	WireGuard	OpenVPN
Основна роля в разглежданата архитектура	Мрежов защитен слой върху вече осигурена IP достижимост; естествено се вписва в L3 модел между известни точки.	Възможна алтернатива за защитен тунел върху вече осигурена IP достижимост, но не решава сам по себе си първичния проблем с достижимостта.	Приложим защитен тунел върху вече осигурена IP достижимост, но с по-голям софтуерен и транспортен overhead.
Работен слой	Мрежово ниво (L3); ESP може да работи директно върху IP, а при NAT се използва UDP капсулация чрез NAT-T.	Логически работи на мрежово ниво (L3) чрез виртуален IP интерфейс, но транспортът по мрежата остава UDP-базиран.	Потребителско ниво; обичайно работи над UDP или TCP чрез виртуален тунелен интерфейс.
Удостоверяване / идентификация	Поддържа разнообразни механизми в рамките на IKE/IKEv2, включително сертификати, EAP-базирани методи, предварително споделени ключове и вендорски разширения.	Използва предварително конфигурирани асиметрични ключове между участниците; не разчита на централен PKI механизъм в самия протокол.	Поддържа удостоверяване в рамките на TLS, най-често чрез сертификати, а при нужда и чрез потребителско име/парола или комбинирани схеми според конфигурацията.
Обмен на ключове / асиметрична криптография	Обменът на ключове и договарянето на SA се извършват чрез IKE/IKEv2; възможни са различни криптографски набори, включително ECC-базирани подходи.	Използва Curve25519 ECDH в Noise-базиран handshake; възможен е и допълнителен предварително споделен ключ.	Използва TLS за удостоверяване и обмен на ключов материал; наличните механизми зависят от поддържаното от TLS библиотеката и конфигурацията.
Криптиране на трафика / симетрична криптография	Полезният трафик се защитава симетрично чрез ESP; на практика широко се използват AES-базирани режими, но конкретният алгоритъм зависи от договорения защитен набор.	Използва ChaCha20-Poly1305 като AEAD механизъм за защита на трафика.	Каналът за данни се криптира със симетричен алгоритъм, определен от конфигурацията; в съвременните реализации често се използват AES-GCM режими чрез data-ciphers.
Цялост / хеш / интегритет	Целостта и автентичността на трафика се осигуряват чрез механизмите на ESP/AH или чрез AEAD режими; в практиката често се използват SHA-базирани хеш/HMAC механизми или AEAD интегритет.	Използва Poly1305 за удостоверена защита на трафика, а BLAKE2s и HMAC-BLAKE2s участват в хеширане и извеждане на ключове в протокола.	При не-AEAD режими може да използва HMAC за целостта; при AEAD режими интегритетът е вграден в самия алгоритъм. TLS control channel може допълнително да се защитава чрез tls-auth или tls-crypt.
Подходящост за конкретния VoIP сценарий	Много подходящ при вече установена виртуална IP видимост и нужда от широко поддържан L3 механизъм за защита между мрежови устройства.	Подходящ като компактна алтернатива, но не внася решаващо предимство в сценарий, в който достижимостта вече е осигурена по отделен механизъм.	Подходящ основно когато се търси по-универсален софтуерен тунел или съвместимост с TLS-ориентирана инфраструктура, а не минимален L3 overhead.

Таблица 5.1. Сравнение между VPN технологии, осигуряващи защита на данните: IPsec, WireGuard и OpenVPN



Фиг 5.5. Архитектура на решението

Как архитектурата (Фиг. 5.5) решава Проблем 1, Проблем 2 и Проблем 3?

Проблем 1 – не се концентрира тежкия трафик в звездата, което разтоварва изходящите канали на доставчиците към София и изходящия канал на дейтацентъра в обратна посока, което потенциално би затруднило както VoIP комуникацията, така и други услуги.

Проблем 2 – ZeroTier работи на принципа на динамичните VPN мрежи, като връзката между всеки два възела е P2P без необходимост от публични адреси (Baset et al., 2006), което носи преимуществото на приложението на технологията в среди, където доставчиците не могат да предоставят много публични адреси или изобщо – никакви. В статията "Securing IoT Environments Using ZeroTier and OPNsense" (Hriţcan et al., 2024) са изброени основните функционалности на ZeroTier.

Проблем 3 – очакваната сумарна латенция при комуникация през центъра на звездата в София би била минимум 2*11 ms = 22 ms и като се прибави и латенцията до крайните устройства във Voice VLAN-ите, стойността ще нарасне до 25 ms. Вместо това, при P2P връзка е постигната далеч по-ниска латенция ~15 ms (Фиг. 5.6 и 5.7) с използване на директните връзки между доставчиците във Варна и Балчик.

```
SEQ HOST                                    SIZE TTL TIME       STATUS
  0 192.168.190.1                             56  64 14ms819us
  1 192.168.190.1                             56  64 14ms745us
  2 192.168.190.1                             56  64 15ms631us
  3 192.168.190.1                             56  64 15ms476us
  4 192.168.190.1                             56  64 15ms619us
  5 192.168.190.1                             56  64 15ms650us
  6 192.168.190.1                             56  64 15ms619us
  7 192.168.190.1                             56  64 15ms466us
  8 192.168.190.1                             56  64 15ms528us
  9 192.168.190.1                             56  64 15ms688us
 10 192.168.190.1                             56  64 15ms410us
  sent=11 received=11 packet-loss=0% min-rtt=14ms745us avg-rtt=15ms422us max-rtt=15ms688us
```

Фиг 5.6.Времезакъснение сдиректните връзки между доставчиците във Варна и Балчик.

```
SEQ HOST                                    SIZE TTL TIME       STATUS
  0 192.168.90.1                              56  64 14ms931us
  1 192.168.90.1                              56  64 15ms856us
  2 192.168.90.1                              56  64 15ms812us
  3 192.168.90.1                              56  64 14ms922us
  4 192.168.90.1                              56  64 14ms913us
  5 192.168.90.1                              56  64 15ms420us
  6 192.168.90.1                              56  64 14ms977us
  7 192.168.90.1                              56  64 15ms678us
  8 192.168.90.1                              56  64 14ms843us
  9 192.168.90.1                              56  64 15ms40us
 10 192.168.90.1                              56  64 15ms621us
  sent=11 received=11 packet-loss=0% min-rtt=14ms843us avg-rtt=15ms273us max-rtt=15ms856us
```

Фиг. 5.7. Времезакъснение с директните връзки между доставчиците във Балчик и Варна.

Коментар: постигнатата стойност от ~15ms пред 25 ms е задоволителна и обосновава използването на P2P динамичен тунел. Освен това, очаквано би било в бъдеще местните доставчици да подобрят връзките помежду си, което би означавало сваляне под 15 ms до очаквани стойности около 3-4 ms , докато при използване на комуникация

през центъра е невъзможно да се свали латенцията под физическия праг от 22 ms, независимо от доставчиците. Освен това, използването на по-късо трасе статистически би намалило потенциалните загуби на пакети.

За да се валидира ефективността на описаната архитектура, беше извършен подробен анализ на сигнализационния и медийния трафик с помощта на Wireshark. Следващата част проследява пълния жизнен цикъл на едно VoIP обаждане.

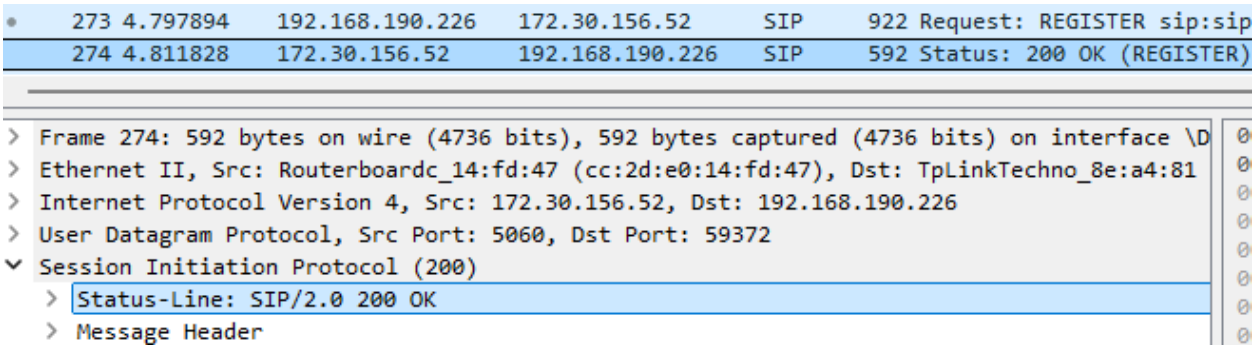
В статиите “Effects of Delay and Packet-Loss on the Conversational Quality” (Thilo and Möller, 2020) и “Effects of Delay on Nonverbal Behavior and Interpersonal Coordination in Video Conferencing” (Diao et al., 2024) се проследяват ефектите от забавянето и загубите на пакетите по време на разговорите, което предвид постигнатите резултати и очакваното подобрение по отношение на латенция и капацитет на предаване на данни между доставчиците би следвало да е възможно провеждането и на конферентни видео разговори във висока резолюция.

5.1.5. Архитектурно описание на решението

Тази схема дава общия поглед върху топологията, но за да се проследи реалното функциониране на системата е необходимо да се разгледа мрежовият трафик в динамика. За целта бяха направени Wireshark наблюдения на трафика, които показват ключовите етапи от SIP сигнализацията и RTP аудио преноса.

По своята същност VoIP телефонията е набор от протоколи, като основните включват сигналинг (SIP) и предаване на кодирано аудио в реално време (RTP) (BERNARD S. KU, 2001). В настоящата дисертация няма да се спираме на това, как работят протоколите, тъй като те са 30 годишни и за тях е изписано много в литературата. Маркираме основните моменти с дъмп на трафик – регистрация на устройство в централата (Фиг. 5.8), позвъняване, приемане на разговор, договорка за кодек G.722 и стартиране на аудиото P2P (Фиг. 5.9) Фиг. 5.10 е аналогична на Фиг. 5.9, показва P2P трафик между LAN мрежи в различни офиси.

Първият етап, който ще разгледаме, е регистрацията на VoIP терминал към Asterisk PBX (Фиг. 5.8):



Фиг. 5.8. Регистрация на устройство

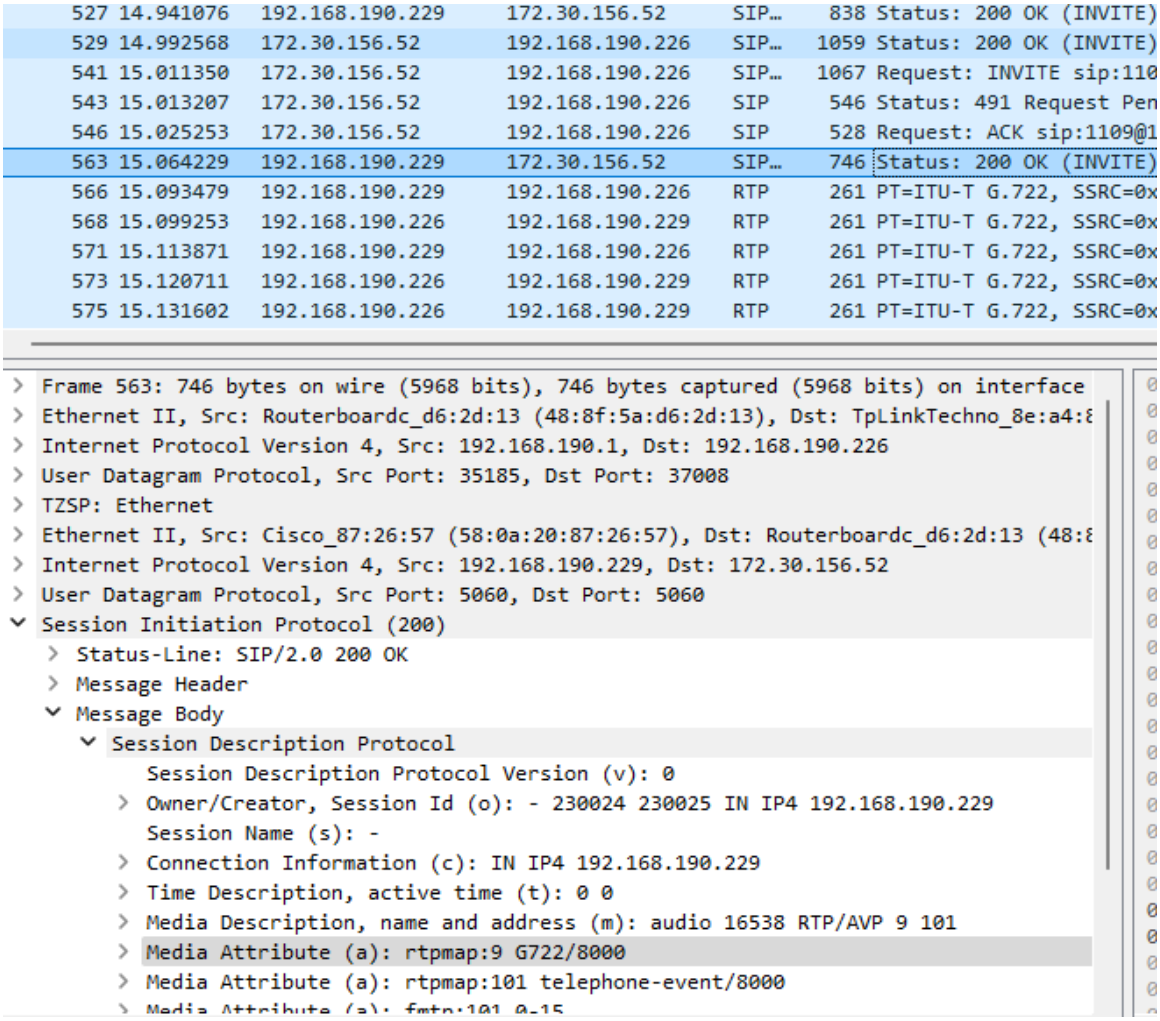
Този етап е ключов, защото именно чрез него устройството получава право да участва в сигнализационния обмен и да извършва или приема обаждания.

В мрежовия трафик се наблюдават следните стъпки:

- SIP REGISTER – терминалът изпраща заявка за регистрация към Asterisk PBX, като предоставя идентификатор (SIP URI).
- 401 Unauthorized – стандартен отговор от PBX, който изисква автентификация. Това не е грешка, а част от механизма за предизвикване на клиент за предоставяне на коректни креденшъли.
- REGISTER (с автентификация) – терминалът изпраща повторна заявка, този път съдържаща криптиран хеш на потребителското име и парола, изчислен чрез Digest Authentication.
- 200 OK – успешен отговор от страна на PBX, който потвърждава, че регистрацията е завършена.

Това демонстрира как Asterisk PBX се използва единствено за сигнализация. Успешната регистрация осигурява необходимата логическа връзка между терминалите и централата, но на този етап не се установява аудио поток. Това е фундаментална особеност на разглежданата архитектура – PBX служи за контрол и маршрутизация на обажданията, докато аудио преносът ще бъде реализиран чрез P2P механизъм, което ще се види в следващите фигури.

След успешната регистрация на терминала (Фиг. 5.8), следващият етап е осъществяването на повикване (Фиг. 5.9):



Фиг. 5.9. Иницииране на разговор и договаряне на кодек

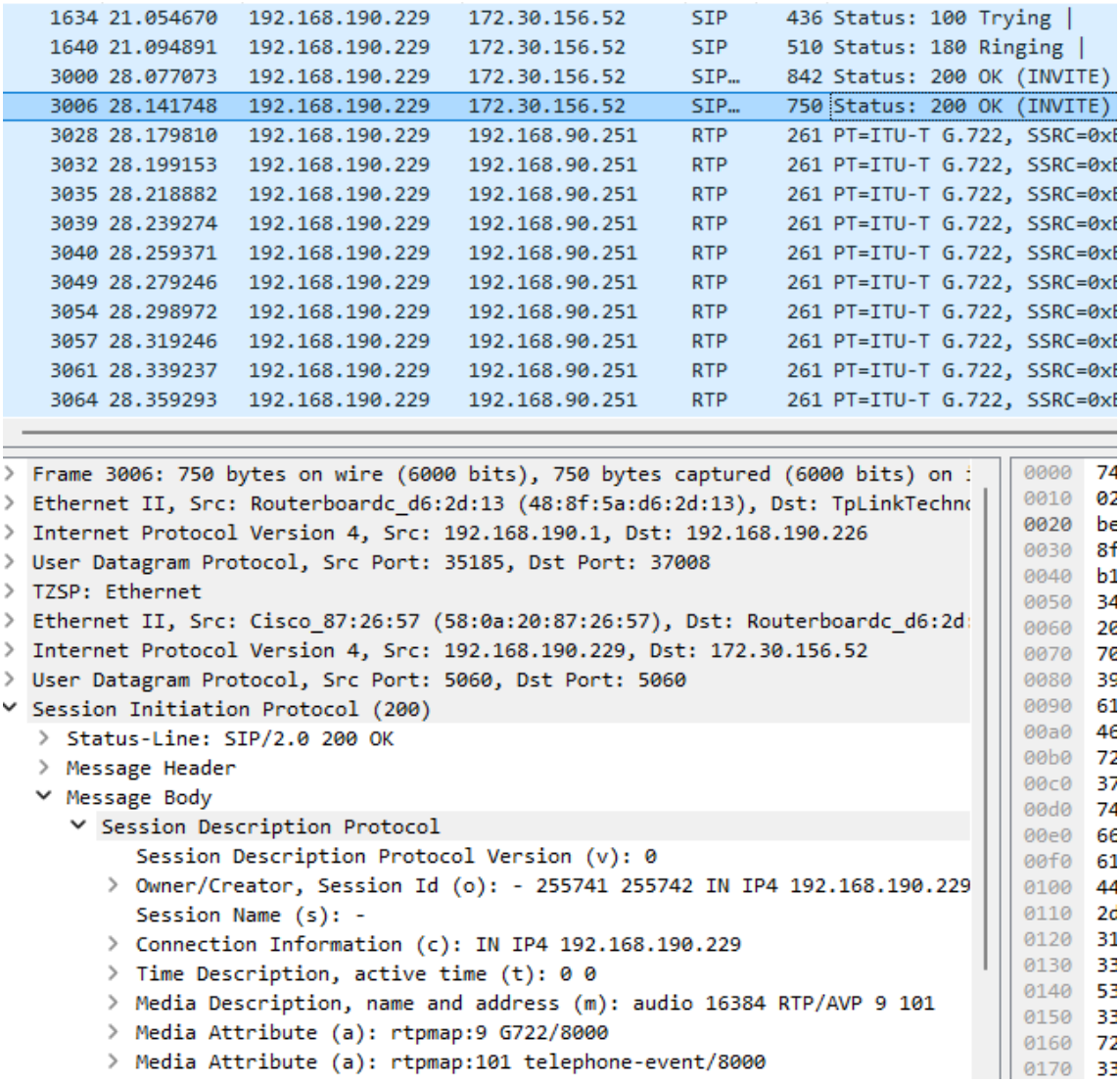
На този етап се демонстрира как SIP сигнализацията се използва за договаряне на връзката, докато самото аудио пренасяне е подготвено за директен P2P обмен.

- INVITE: Инициращият терминал изпраща SIP INVITE съобщение към Asterisk PBX, съдържащо Session Description Protocol (SDP) параметри. В тях е включен списък с поддържани кодеци – например G.711 и G.722.
- 100 Trying: PBX потвърждава, че заявката е получена и обработва повикването.
- 180 Ringing: Терминалът на отсрещната страна започва да звъни и връща междинен сигнал. Това показва, че сигнализационният канал функционира правилно.

- 200 OK: Получателят на разговора отговаря с потвърждение и предоставя свой SDP, като в този процес се извършва договаряне на кодек. В примера се избира G.722, което гарантира HD аудио качество (Catellier and Voran, 2023).
- ACK: Инициращият терминал изпраща ACK съобщение, с което двустранно се финализира установяването на сесията. На този етап сигнализационната фаза приключва.

Това илюстрира стандартния SIP процес на повикване и потвърждаване на връзка. Ключов момент е договарянето на аудио кодек, което в разглеждания случай завършва с избор на G.722. По този начин се гарантира високо качество на разговора, независимо от ограничената инфраструктура на регионалните ISP. Важно е да се подчертае, че въпреки че сигнализацията преминава през PBX, RTP потоците не се насочват през централата, а предстои да бъдат установени директно между терминалите.

След приключването на SIP сигнализацията (Фиг. 5.9) и избора на аудио кодек, започва същинският пренос на глас. Този етап е критичен за предложената архитектура, тъй като именно тук се демонстрира разликата спрямо традиционните VoIP решения – RTP аудио потоците не преминават през Asterisk PBX, а се установяват директно между двата терминала в различни офиси – Фиг. 5.10.



Фиг. 5.10. P2P RTP трафик между офисите

Описание на процеса във Фиг. 10:

1. Източник и дестинация на RTP пакетите – вместо да са адресирани към дейта центъра (PBX), те се обменят директно между IP адресите на локалните LAN мрежи (например 192.168.90.x ↔ 192.168.190.x).
2. Payload Type – стойностите в RTP заглавките потвърждават, че се използва договореният кодек G.722, осигуряващ HD качество на звука.
3. Последователност и времеви маркери – инкрементalните Sequence Number и Timestamp показват нормален и непрекъснат аудио поток без значителни загуби или закъснения.

4. P2P връзка през ZeroTier тунел – благодарение на динамичното изграждане на VPN, RTP трафикът достига директно до отсрещния офис дори при липса на публичен IP или при наличие на NAT.

Този процес потвърждава основното предимство на хибридната архитектура: SIP сигнализацията се обслужва централизирано от PBX в дейта центъра, но гласовите потоци се обменят peer-to-peer между офисите, заобикаляйки ограниченията на регионалните ISP (нисък капацитет, липса на публични IP адреси, невъзможност за MPLS). Това позволява намаляване на латентността, оптимално използване на наличната честотна лента и постигане на високо качество на разговора дори при неблагоприятни мрежови условия.

Като естествено продължение във Фиг 5.11 се обединяват двата ключови етапа от SIP комуникацията: сигнализация при позвъняване и последващия активен разговор с висококачествен аудио кодек.

Фиг. 5.11. Позвъняване и активен разговор с HD аудио

В първата част на трасето се наблюдават стандартните SIP съобщения 180 Ringing и 183 Session Progress, които показват, че терминалът на отсрещната страна успешно приема повикването и подготвя връзката за установяване. Този етап е междинно потвърждение, че PBX изпълнява функцията си на централен сигнализационен възел, координиращ обаждането, но без да участва в преноса на медия.

Тук се демонстрира пълния цикъл на обаждане: от позвъняването до активната RTP сесия. Тя затвърждава основната иновация на предложеното решение: PBX обслужва единствено SIP сигнализацията, докато аудио потоците се обменят директно между офисите чрез P2P връзка, оптимизирайки капацитета и минимизирайки латентността.

Анализът на трафика с Wireshark (Фиг. 5.8–5.10) проследява целия жизнен цикъл на едно VoIP обаждане в рамките на предложената хибридна архитектура. На Фиг. 5.8 се демонстрира процесът на регистрация, при който Asterisk PBX изпълнява ролята на централен сигнализационен сървър. Фиг. 5.9 показва установяването на повикване и договарянето на кодек G.722, което осигурява HD качество на аудиото. На Фиг. 5.10 се вижда как RTP потоците се обменят директно между офисите по P2P модел, като по този начин се заобикалят ограниченията на регионалните ISP. Накрая, Фиг. 5.11 илюстрира целия цикъл – от позвъняването до активната RTP сесия, като потвърждава, че аудио качеството се запазва високо въпреки предизвикателствата на мрежовата инфраструктура.

Wireshark трасетата доказват на практика, че архитектурата е ефективна: SIP сигнализацията се централизира през PBX, докато RTP аудио потокът се децентрализира чрез P2P обмен. Тази комбинация минимизира латентността, оптимизира използването на наличния капацитет и осигурява стабилно HD качество на разговорите, което е недостижимо при класическите VoIP реализации, зависими изцяло от инфраструктурата на регионалните ISP. Представените трасета потвърждават, че архитектурата функционира стабилно в условията на ограничена инфраструктура. Това дава основание да се обобщят основните ползи от предложеното решение.

Внедреното решение показва, че комбинацията от централизирана SIP сигнализация и децентрализиран P2P пренос на RTP аудио потоци е ефективен подход за преодоляване на ограниченията, наложени от регионалните интернет доставчици. Чрез използването на защитени тунели и динамично изграждане на връзки се постига значително намаляване на латентността и елиминиране на зависимостта от липсата на публични IP адреси и MAN свързаност. Допълнително, директният обмен на аудио пакети между офисите позволява оптимално използване на наличната честотна лента и гарантира стабилно качество на разговорите. Този модел не само отговаря на текущите нужди на разглежданата компания, но и служи като пример за внедряване на надеждна VoIP архитектура в условията на ограничена инфраструктура, приложима и за други организации със сходни предизвикателства.

От академична гледна точка изследването допринася с демонстрация на приложимостта на P2P моделите в реална корпоративна среда, извън лабораторни условия, като показва как подобен подход може да бъде използван за подобряване на качеството на услуги, зависими от интернет свързаността. На базата на тези резултати

могат да се формулират окончателните изводи и насоки за бъдещо развитие на изследването.

5.1.6. Предимствата на предложената архитектура

Подходът при изграждане на хибридното решение беше да раздели логиката на звездна архитектура и P2P архитектура, базирана на динамични тунелни връзки между възли, което разреши проблемите с капацитета за обмен, справянето с NAT среди, намали латенцията при комуникацията между крайните точки и потенциалната загуба на пакети. Освен това, подобно решение отделя слоя ISP от бизнес слоя, като позволява организиране на собствена адресация вътре в бизнес средата, собствена маршрутизация, както и имплементиране на собствена защита, в т.ч. и криптографска сигурност, като така обособената схема се явява логическа независима както от промени в самите ISP, така и в самия P2P платформен слой. По този начин решението доказва, че дори при ограниченията на регионални ISP може да се гарантира качество на корпоративна VoIP услуга, сравнимо с това в големите градски мрежи.

В бъдеще архитектурата може да бъде разширена и към други направления на корпоративната комуникация, като видеоконференции и интеграция с услуги за споделяне на съдържание в реално време. Допълнително, прилагането ѝ в условия на 5G или сателитни технологии като Starlink би позволило по-широк обхват на приложение и би осигурило надеждна свързаност за отдалечени офиси и мобилни екипи. Подобни разширения ще позволят още по-пълноценно сравнение с традиционните VoIP решения и ще дадат основа за нови изследвания върху качеството на услугата в различни мрежови среди.

5.2 Федеративен AIS облак — оптимизация на предоставянето на навигационна телеметрия като услуга

Досега разгледаните услуги в този дисертационен труд – видео стрийминга, GPU услугата при поискване, VoIP комуникацията в реално време и федеративният AIS облак представляват различни инженерни режими, но споделят обща архитектурна логика: разделение на функциите, контрол върху латентността, наблюдаемост и устойчивост при

отпадане на компоненти. Затова дизайнът на федеративния AIS облак следва да заема доказани практики от стрийминг системите, реалновремевите комуникации и федеративните облачни модели, като ги адаптира към особеностите на навигационната телеметрия и на многодомейнната среда.

5.2.1. Концептуална формализация на ресурсния ефект при федеративен AIS облак

Следващата формализация е предназначена да подпомогне архитектурното обосноваване на федеративния AIS облак, без да претендира за емпирично калибриран модел. Целта ѝ е да покаже защо при нарастване на броя на приемните възли нефедеративният подход води до акумулиране на суров поток и дедупликационно натоварване в централен ресурс, докато при федеративен подход част от пречистването се изнася по-близо до източника.

Формализацията е концептуална и не цели да описва в детайли всички особености на реалната радиосреда. Тя е насочена към най-съществената зависимост: степента на припокриване между приемните зони определя колко пъти едни и същи AIS събития се мултиплицират в сумарния суров поток, а оттам и какъв централен ресурс би бил необходим при липса на федеративна организация.

Означение	Смисъл
N	брой активни приемни възли
λu(N)	интензивност на полезния уникален поток от AIS събития
ddup(N)	среден коефициент на дублиране преди локална дедупликация
dres(N)	остатъчен коефициент на дублиране след локална или регионална дедупликация
κ	относително тегло на дедупликацията спрямо чистото приемане и пренос
Cnf(N)	нормализиран централен ресурс при нефедеративен модел
Cfed(N)	нормализиран централен ресурс при федеративен модел
G(N)	архитектурна полза от федеративния подход като отношение между двата ресурса

Таблица 5.1. Означения

Концептуално, ако λu(N) обозначава полезния уникален поток от AIS събития, а ddup(N) — средния коефициент на дублиране при приемането им от множество станции, то при нефедеративен модел централният ресурс трябва да поеме суров поток:

$$\lambda raw(N) = ddup(N) \cdot \lambda u(N)$$

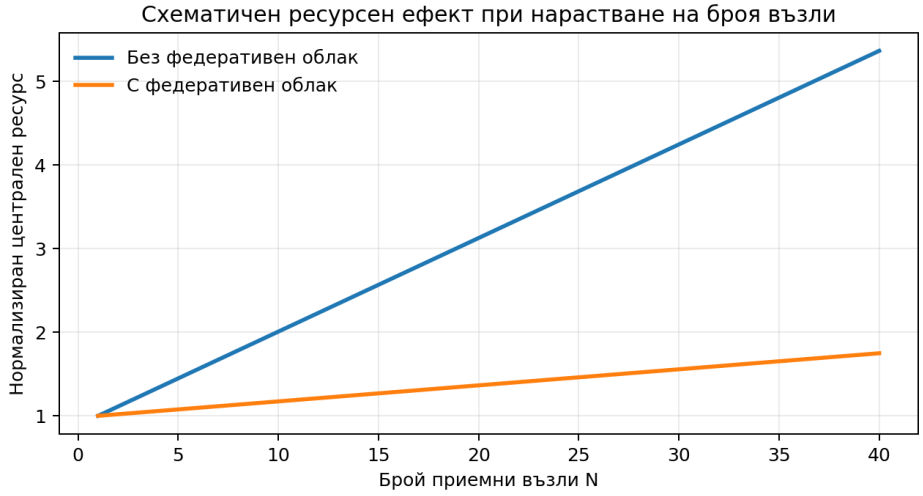
$$Cnf(N) = ddup(N) + \kappa \cdot (ddup(N) - 1)$$

където вторият член отчита допълнителната тежест по дедупликация върху централния ресурс. При федеративен модел част от пречистването се извършва близо до източника и към по-горно ниво се предава поток с остатъчен коефициент на дублиране dres(N), съществено по-малък от ddup(N), така че нормализираният централен ресурс може да бъде представен като:

$$Cfed(N) = dres(N) + \kappa \cdot (dres(N) - 1)$$

$$G(N) = Cnf(N) / Cfed(N)$$

Следователно архитектурната полза от федеративния подход нараства с увеличаване на броя на възлите и със степента на локално припокриване. Това показва, че при отсъствие на федеративен облак нарастването на броя приемни точки води до еквивалентно нарастване на необходимия централен ресурс, докато при федеративна организация част от това натоварване се абсорбира на по-ниско ниво чрез локална дедупликация и предварителна обработка.



Фиг. 5.12. Схематичен ресурсен ефект при нарастване на броя възли

Фиг. 5.12 представя схематична зависимост между броя на приемните възли и необходимия централен ресурс при два режима: без федеративен облак и с федеративен облак. За илюстрация е прието, че коефициентът на дублиране преди локална дедупликация нараства по зависимост $ddup(N)=1+0.07\cdot(N-1)$, а остатъчният коефициент след локална или регионална дедупликация — по зависимост $dres(N)=1+0.012\cdot(N-1)$, при $\kappa=0.6$. Параметрите са илюстративни и не претендират за емпирична калибрация. Те служат единствено за визуализиране на тенденцията, че при федеративен подход нарастването на необходимия централен ресурс е значително по-плавно.

5.2.1.1. Интерпретация на коефициента на дублиране

Коефициентът ddup(N) отразява степента на пространствено и времево припокриване между приемните зони. При близко разположени станции, които наблюдават сходна AIS картина, ddup(N) нараства и може да се доближи до броя на станциите в локалната група. При увеличаване на разстоянието между станциите и намаляване на припокриването на приемните зони ddup(N) намалява, като в пределен случай на практически независими AIS картини се доближава до 1.

Тази зависимост е важна, защото показва, че ресурсният ефект на федеративния подход не е функция само от броя възли, а и от това доколко техните радиохоризонти и реални области на прием се припокриват. Следователно плътното разполагане на станции в крайбрежен или речен участък увеличава не само общия входящ поток, но и относителната полза от локалната дедупликация.

5.2.1.2. Частен случай: две станции

Нека за две станции означим с U1 уникалния поток само от първата станция, с U2 — уникалния поток само от втората станция, а с O — припокриващия се поток от събития, които и двете станции приемат. Тогава:

$$\lambda raw = U1 + U2 + 2O$$

$$\lambda u = U1 + U2 + O$$

$$ddup = (U1 + U2 + 2O) / (U1 + U2 + O)$$

Оттук се вижда, че когато двете станции са близо една до друга и припокриването O е голямо, коефициентът ddup нараства и в граничен случай се доближава до 2. При постепенно раздалечаване на станциите припокриването намалява, а заедно с него ddup се приближава до 1. Именно тази проста зависимост обяснява защо централизираната

система трябва да поеме все повече суров поток, когато много близки станции изпращат към един и същ централен възел.

В по-общ случай за локална група от m близки станции, които наблюдават почти една и съща AIS картина, коефициентът ddup може концептуално да се доближи до m. Когато обаче станциите се разполагат така, че приемат все по-различни картини, коефициентът намалява към 1 и ползата от дедупликация на централно ниво естествено отслабва.

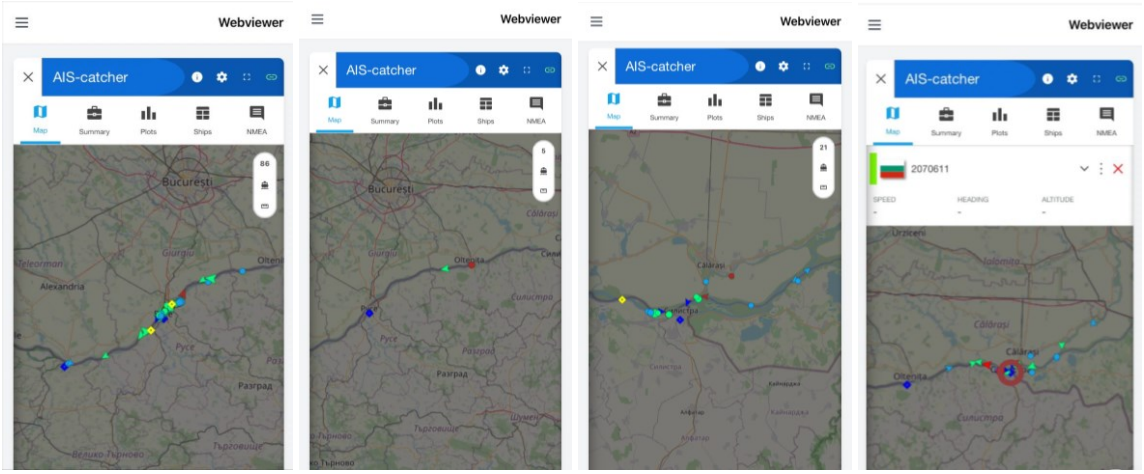
Следователно формализацията не предполага фиксиран коефициент на дублиране, а допуска той да се изменя според реалната топология на станциите, геометрията на покритието и моментната AIS картина. Това прави модела достатъчно прост за архитектурно обосноваване и едновременно достатъчно гъвкав, за да отрази прехода от силно припокриващи се локални групи към практически независими приемни зони.

5.2.2. Проблеми, които решава федеративният облак и системен ефект

Федеративният AIS облак решава едновременно технически, организационни и икономически проблеми, които възникват при прехода от модел „станция → платформа“ към по-сложна среда с множество приемни точки, автономни оператори и различни цели за предоставяне на данни. Формализацията по-горе показва ресурсния смисъл на федеративния подход; на практика този ефект се проявява като промяна в начина, по който се дефинира самата услуга. Основният системен ефект е, че физическите приемници, мрежовите връзки и изчислителните механизми вече не се разглеждат като отделни, слабо свързани компоненти, а като координирана услуга за събиране, пречистване, маршрутизиране и предоставяне на телеметрични данни. В този контекст под „пречистване“ не се разбира само премахване на повторенията, а съвкупност от операции по нормализация на входните съобщения, времево подреждане, дедупликация, географско ограничаване до поискан участък и запазване на релевантните непозиционни съобщения за съдовете, свързани със съдовете в разглеждания участък.

Показателен практически пример е дунавският участък Русе – Тутракан – Силистра. Наблюденията от приемни точки в района на Русе, Тутракан, Айдемир и Силистра показват, че отделните станции не възприемат строго изолирани навигационни

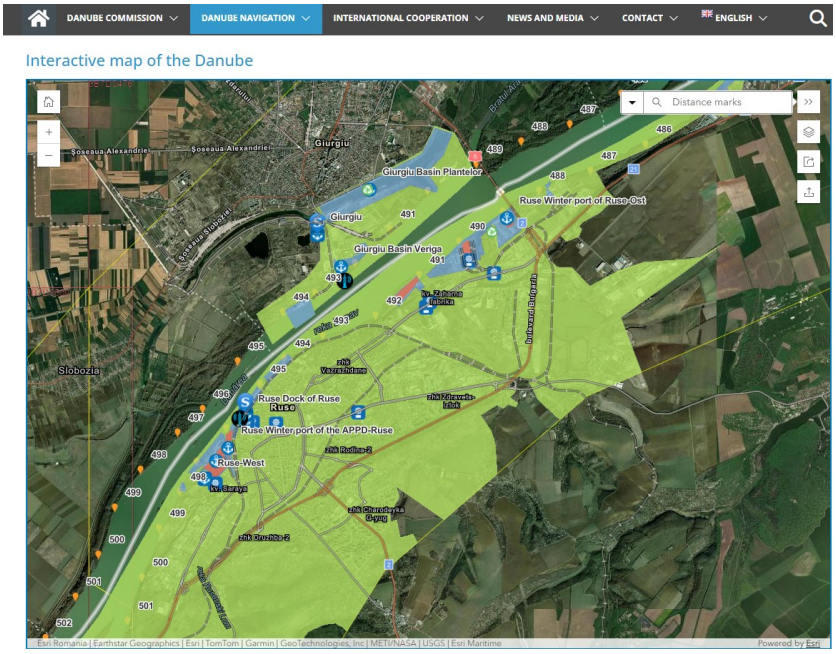
сегменти, а формират частично припокриваща се приемна картина. Поради това при традиционен модел за подаване на данни според физическите активи крайният получател не получава „чист“ поток за търсения участък, а смес от съобщения, които се отнасят и до съседни речни сегменти (Фиг. 5.13).



Фиг. 5.13. Изследване на AIS приема в района на Русе, Тутракан, Айдемир и Силистра

Илюстративните екранни снимки от тези наблюдения са направени в различни моменти и при различен мащаб и поради това не служат за количествено измерване на степента на повторяемост. Те обаче ясно показват по-съществения системен проблем: при подаване на сурови потоци по приемни точки към административния потребител достига смесена картина, която не съвпада пряко с оперативно търсения участък по фарватера.

Това води до важна промяна в начина, по който се дефинира самата услуга. Администрацията не се интересува от това къде точно са разположени антените и приемниците и кои от тях са приели съответното съобщение. За нея е от значение да получи надеждна AIS картина за определен участък от фарватера, например за отсечката Русе (490 км, Фиг. 5.14) – Тутракан (434 км), без да бъде натоварена с последващо ръчно отделяне на съобщения от участъци като Свищов – Русе или Тутракан – Силистра. Именно тук предложеният модел премества фокуса от физическите активи към услугата. Вместо да се заявяват данни от конкретни станции, заявява се услуга за конкретен пространствено определен участък.



Фиг. 5.14. Екранна снимка на интерактивната карта на Дунав и навигационния километраж в района на Дунав мост „Русе – Джурджу“, източник: Дунавска комисия

Логическият ред на обработката в този модел е следният: първо се извършват нормализация и времево подреждане на входните AIS съобщения, след това се прилага дедупликация върху вече уеднаквения поток, а едва след това се извършва географското ограничаване до искания участък. Този ред е важен, защото ако пространственото ограничаване се приложи преди дедупликацията, една и съща географска проверка ще се извършва многократно върху повтарящи се копия на едни и същи съобщения. След пространственото ограничаване може да се добави и контекстно допълване с релевантни непозиционни съобщения за вече установените съдове в участъка. По този начин към крайния потребител се подава не инфраструктурно зависима смес от сурови потоци, а селектиран и дедупликиран базов AIS поток за конкретната оперативна зона.

От гледна точка на оператора на станция предложеният модел запазва ниския праг за участие и не изисква съществена промяна в обичайния начин на работа. Запазва се познатият базов модел на свързване: антена → приемник → NMEA 0183 → домашен рутер → интернет. Една станция може да подава данни паралелно към повече от една входна точка, което повишава надеждността при нестабилна UDP свързаност и при ограничения на малки или битови интернет доставчици. Не се изискват пренасочване на портове и публичен IP адрес при крайния потребител, тъй като сложността по

преодоляване на мрежовите ограничения остава между автономните системи. Миксирането на потоците, дедупликацията и пространственото ограничаване се извършват във федеративната среда, близо до мястото на приемане, без операторът да поддържа тези функции локално. Осигурява се и проследимост на дейностите по приемане, транзит, дедупликация и доставка, без операторът на станцията да е натоварен с управление на тези компоненти.

От гледна точка на операторите на автономни системи федеративният облак въвежда по-ясни граници на отговорност и контрол. Вместо всяка страна да изпълнява едновременно ролята на приемник, агрегатор, маршрутизатор и доставчик, функциите се разделят между входни точки, транзитни възли, възли за дедупликация и изходни точки. Това позволява по-добра отчетност, по-лесно локализиране на проблеми и по-прецизно управление на доверието между участниците. От гледна точка на крайните платформи и административните потребители най-съществения ефект е намаляването на дублиращия се и шумов трафик още близо до източника. При класическия модел множество приемници от един и същи район могат да подават едни и същи AIS съобщения независимо един от друг, което води до излишно натоварване на централната инфраструктура. Федеративният облак измества значителна част от тази обработка по-близо до мястото на приемане и така предоставя по-чист, по-структуриран и по-лесен за последващо използване поток от данни.

Показателен пример за тази посока на развитие е дунавската линия на сътрудничество между българската и румънската администрация по проекта DANRiSS и неговото по-ново надграждане DANRISS 2. Първоначалният проект е насочен към повишаване на координацията между двете администрации чрез обща база данни, правила за корабоплаване, методика за оценка на риска и интегрирана информационна система за инспекции на съдове по общия българо-румънски участък на река Дунав. В актуалната линия на развитие тази основа се надгражда към интелигентна и интегрирана платформа, в която вече се включват събиране и анализ на данни, сензори, съвместен мониторинг, инфраструктурни компоненти и решения с изкуствен интелект, като изрично се търси избягване на дублирането на дейности между администрациите. Този пример показва, че дигиталната трансформация в публичния сектор не се изчерпва с електронизация на отделни процедури, а преминава към споделени цифрови услуги,

общи данни и координирани междудомейнни процеси, което е в пълно съответствие с логиката на федерираните системи, разглеждани в настоящото изследване.

Практическата релевантност на подобен подход се вижда и в европейските инициативи за интеграция на речни информационни услуги. EuRIS е реализирана като обща и централизирана точка за достъп, която събира данни от националните инфраструктури и предоставя услуги през уеб портал и програмни интерфейси, като суровите AIS данни постъпват към средата през защитена VPN свързаност (Zwicklhuber and Kaufmann, 2023). В този смисъл предложеният тук модел не отрича подобни решения, а ги надгражда, като измества акцента от централизирано събиране на инфраструктурни потоци към федеративно предоставяне на пречистена услуга според конкретен участък и конкретна административна потребност. Сходна посока се наблюдава и при DANRiSS и неговото планирано надграждане DANRISS 2, където се търси интегрирана платформа, избягване на дублирането между администрациите, използване на сензори, анализ на данни и решения с изкуствен интелект за усъвършенстван мониторинг и инспекции (Министерство на транспорта и съобщенията, 2018), (Министерство на регионалното развитие и благоустройството, 2026).

Особено важен е и по-широкият организационен ефект. Подобни AIS екосистеми често се развиват върху доброволно поддържан слой от станции, при който стимулите не са непременно финансови, а са свързани с достъп, признание, полезност и принадлежност към общност. Литературата описва този тип системи като форма на доброволно предоставяна географска информация — volunteered geographic information (VGI), тоест данни, събирани и предоставяни от граждани и ентусиасти, често срещу немонетарни стимули като признание, достъп до функции и усещане за принадлежност (Goodchild, 2007). Практиката при морските платформи показва, че мрежите от приемници се разширяват именно чрез участие на независими оператори на станции. В публикуван анализ за MarineTraffic се посочва, че мрежата от наземни приемници е изградена с подкрепата на оператори на станции на доброволни начала: платформата приема кандидатури за подобряване на покритието, провежда скрийнинг процес, а успешните кандидати могат да получат оборудване безплатно срещу ангажимент да поддържат станцията технически изправна и функционираща в онлайн режим (Memos et al., 2017). Практическата релевантност на подобен федеративен подход се потвърждава и от развитието на комерсиалните морски платформи, които вече оперират глобални AIS

мрежи, комбиниращи наземни, океански и спътникови приемници, и продължават да разчитат на общностен слой от станции. Това показва, че при нарастващ мащаб и хетерогенност на източниците възниква необходимост от по-ясно разделение на роли, обработка близо до източника, дедупликация и контролирано споделяне на данни между автономни участници (MarineTraffic, 2026).

5.3. Изводи

Пета глава показа, че оптимизацията на прехода от управление на асети към управление на услуги в сложни федерирани системи не се изчерпва с подмяна на една технология с друга, а изисква архитектурно преосмисляне на начина, по който се организират функциите, потоците и отговорностите. В случая на хибридното VoIP решение това преосмисляне се реализира чрез разделяне между централизирана сигнализация и директен пренос на медия, което позволява едновременно запазване на управляемостта и намаляване на латентността при работа в среда с NAT ограничения и регионални инфраструктурни дефицити. В случая на федеративния AIS облак същата логика се проявява чрез разделяне между управленски и информационни функции, периферно събиране и предварителна обработка на потоците, както и предоставяне на навигационна телеметрия като услуга, ориентирана не към отделната станция, а към оперативно значим резултат за конкретен участък, зона или институционален потребител от публичния сектор.

В този смисъл двата разгледани казуса очертават два комплементарни модела на оптимизация. При VoIP водеща е чувствителността към латентност и необходимостта от контролирана, но не прекомерно централизирана комуникационна архитектура. При федеративния AIS облак водещи са близостта до източника, намаляването на излишния централен ресурс, дедупликацията, възможността за пречистване на гео база, а и при запазване на автономността на отделните участници. Съществената разлика е, че федеративният AIS облак може да бъде полезен и в среда на ограничения, но неговото пълноценно разгъване зависи от наличието на по-мощна оптична основа, която да намали физически обусловените ограничения по отношение на латентност, капацитет и надеждност. Именно тук се затваря връзката с по-ранния обзор: новите подводни и сухоземни оптични проекти не са само инфраструктурен фон, а условие логическото и

приложното ниво на услугите да следват физическата логика на мрежата и да достигнат по-висока производителност, по-широк обхват и по-силен системен ефект. В криптографски аспект и двата разгледани казуса потвърждават, че за разглежданите в дисертационния труд service-centric и федеративни среди ECC е по-подходящият избор спрямо RSA, когато се търси съчетание между сигурност, нисък overhead, ограничено изчислително натоварване и приложимост в реални разпределени инфраструктури.

Федеративният AIS облак може да се разглежда и като технологична предпоставка за по-висока национална и регионална морска сигурност, тъй като създава условия за по-добра ситуационна осведоменост, наблюдение на критични участъци и по-навременна координация между административни и оперативни структури.

Съдържанието на тази глава е отразено в следните публикации:

1. **I. Iliev,** I. Blagoev and Y. Terziev, "Hybrid VoIP Solution to Address Regional ISP Challenges," 2025 6th International Conference on Communications, Information, Electronic and Energy Systems (CIEES), Ruse, Bulgaria, 2025, pp. 1-6, doi: 10.1109/CIEES66347.2025.11300241.

Заключение – резюме на постигнатите резултати

Съвременната дигитална трансформация в публичния сектор не се изчерпва с внедряване на отделни технологии, а представлява преход от управление на асети към управление на услуги. В условията на сложни федерирани системи този преход изисква координирано използване на мрежови, изчислителни и организационни асети, така че те да бъдат предоставяни като надеждни, сигурни и ефективни цифрови услуги.

В дисертационния труд е изследван именно този преход чрез няколко представителни класа услуги: адаптивно мултимедийно разпространение, високопроизводителни изчислителни услуги, комуникация в реално време и федеративна телеметрия. Въпреки различията в приложните области, разгледаните казуси показват, че успешното предоставяне на услуги във федерирани среди зависи от общи архитектурни принципи: ясно разделение на функциите, динамично предоставяне на асети при поискване, сигурност, вградена в самия модел на услугата, киберустойчивост и съобразяване с реалните ограничения на инфраструктурата.

В областта на сигурността и киберустойчивостта е аргументирана необходимостта от преход към по-съвременни механизми за защита на комуникациите и цифровите услуги. Анализът на зависимостта на RSA от качеството на ентропията показва, че сигурността не е статично състояние, а процес на постоянно технологично обновление и архитектурно съобразяване със средата. На тази основа е обоснован изборът на ECC като по-подходящо решение за разглежданите в дисертацията разпределени и ресурсно ограничени услуги, като същевременно е очертана и перспективата за бъдещо развитие към устойчивост в постквантов контекст.

В областта на мултимедийните услуги е показано, че защитата на съдържанието и защитата на личните данни могат да бъдат постигнати по-ефективно чрез разделяне между разпространението на съдържанието и удостоверяването на потребителите. Така се реализира модел, при който видео дистрибуторът пренася съдържанието, без да обработва чувствителните данни на крайния потребител, а удостоверяването се възлага на специализирана услуга за идентичност. Този подход повишава киберустойчивостта и намалява риска от компрометиране на лични данни при пробив в инфраструктурата за стрийминг.

В областта на административните и изчислителните услуги е показано, че преходът от локална обработка към централизирани услуги при поискване позволява по-ефективно използване на изчислителните асети и по-лесна интеграция с външни системи. Чрез API-базиран достъп и чрез използване на GPU-ускорена обработка се създават предпоставки за по-достъпно предоставяне на сложни аналитични услуги в публичния сектор, без необходимост всеки краен потребител да разполага със собствена високопроизводителна инфраструктура.

В областта на комуникационните услуги и телеметрията в реално време е показано, че моделът, ориентиран към услугите, е приложим и в среди с инфраструктурни ограничения, включително при NAT-ограничения, хетерогенни участници и разпределено управление. Хибридната VoIP архитектура и предложената архитектура на федеративен AIS облак демонстрират, че чрез разделение между управляващи и информационни функции, както и чрез координирано предоставяне на услуги, могат да бъдат постигнати по-висока гъвкавост, устойчивост и практическа приложимост в реални регионални среди.

Получените резултати потвърждават основната теза на дисертационния труд, че оптимизацията на прехода от управление на асети към управление на услуги в сложни федерирани системи не се изчерпва с избор на отделна технология, а изисква цялостен архитектурен подход. Такъв подход не омаловажава значението на инфраструктурата, а я поставя в правилния системен контекст. В изчислителния слой отделни функции могат да бъдат преразпределяни, консолидирани или изнесени към по-подходящи възли в зависимост от анализа на натоварването, латентността и организационните изисквания. При комуникационната инфраструктура обаче съществуват базови слоеве на свързаност, чиято роля не може да бъде компенсирана чрез механично натрупване или агрегиране на множество по-слаби връзки. Именно в този смисъл магистралната оптична свързаност остава незаменима основа за предоставяне на надеждни услуги в реално време. След дългоочаквания исторически момент на изграждане на високоскоростна свързаност в региони, които дълго време са се намирали в периферията на цифровото развитие, настъпва следващият преломен етап: тази инфраструктурна основа да започне да поражда реални регионални услуги, които впоследствие да преминават към координация, интеграция и федериране. Именно в такава еволюционна перспектива се разкрива и пълният потенциал на предложения модел. Този преход не може да бъде

осъществен мигновено, нито чрез еднократен технологичен акт, а изисква последователно, плавно и организационно обосновано развитие, при което инфраструктурата престава да бъде крайна цел и се превръща в основа за изграждане на устойчиви цифрови услуги.

Не е случайно, че настоящият дисертационен труд започва нетрадиционно – от Североизточна България като пространство с памет, география, инфраструктурни дефицити и неизползван потенциал. По същия нетрадиционен начин е избрано и неговото завършване: отново към същия регион, но вече видян през възможността върху веднъж изградена свързаност да възникват нови поколения услуги. Именно тук едновременното присъствие на дунавския коридор Русе–Тутракан–Силистра и черноморската линия Шабла–Каварна–Балчик показва как една и съща цифрова основа може да обслужва различни, но свързани процеси – наблюдение, комуникация, транспорт, рибарство, крайбрежен туризъм и регионално управление. В рамките на настоящото изследване това вече се проявява както в анализа на AIS покритието по дунавския участък и в идеята за географски пречистен NMEA поток по отделни сегменти на фарватера, така и в морските наблюдения по Северното Черноморие. Регионалната конкретика на Шабла–Каварна–Балчик, разгърната в изследване, реализирано по Оперативна програма за развитие на сектор „Рибарство“ 2007–2013, показва колко плътно на малка територия могат да се наслагват природни дадености, историческа памет, рибарски практики и туристически ресурси (Станкова, 2016). Новата научна литература, от своя страна, вече очертава и възможността AIS данните да се използват за анализ на взаимодействията между туризма с малки плавателни съдове и риболова (Ramos et al., 2025). По този начин регионалната перспектива получава и ясно междудисциплинарно продължение. Именно в тази еволюция от инфраструктурна основа към координирани и постепенно федерирани регионални услуги се разкрива и действителният потенциал на предложения модел.

На тази основа може да се направи изводът, че предложените в дисертационния труд решения и модели очертават завършена концептуална и практическа рамка за оптимизиране на прехода от управление на асети към управление на услуги в сложни федерирани системи в публичния сектор.

Приноси

Основните научни и научно-приложни приноси на дисертационния труд могат да бъдат обобщени, както следва:

1. **Разработен е общ модел за преход** от управление на асети към управление на услуги в сложни федерирани системи в публичния сектор. Моделът обединява цифрови, мрежови и изчислителни ресурси в интегрирани услуги с гарантирано качество. Това оптимизира надеждността и сигурността на процесите, като същевременно подобрява тяхната ефективност и организационна приложимост при управление на данни.
2. **Изборът на ECC (Elliptic Curve Cryptography) е аргументиран** като по-подходяща криптографска основа за разглежданите в дисертацията разпределени услуги с ограничени ресурси. Това е постигнато чрез детайлен анализ на дефицитите на RSA при ниска ентропия и формулиране на практически насоки за повишаване на криптографската устойчивост. При ECC нуждите от ентропия за генериране на сигурен ключ са значително по-ниски спрямо RSA (поради по-малкия размер на ключа за същото ниво на сигурност), което е критично за IoT устройства и „edge“ услуги, където източниците на истинска случайност често са ограничени.
3. **Разработени са методи за сигурно предоставяне** на мултимедийни услуги чрез разделяне на процесите по разпространение на съдържанието от удостоверяването на потребителите. Този подход ограничава обработката на лични данни от дистрибутора, осигурява регламентирана редистрибуция и повишава киберустойчивостта на услугата.
4. **Разработена е архитектура за предоставяне на административни** и изчислителни услуги при поискване (on-demand). Тя включва API-базиран достъп до обработка на геопространствени данни и специализиран демон insightd за централизирано GPU-ускорено изчисляване. Този подход минимизира зависимостта от скъп локален хардуер и значително улеснява интеграцията с външни системи. Използването на GPU-ускорена обработка чрез специализиран демон е ключово предимство в контекста на геопространствените данни (GIS). Комбинацията от API достъп и GPU демон архитектурно разделя интерфейса за управление от тежките изчисления. Поради високите изисквания за

паралелизация при масиви от пространствени данни, централизираните структури предлагат значително по-висока ефективност и изчислителна мощ в сравнение с капацитета на стандартните локални работни станции.

5. **Разработена е хибридна VoIP архитектура** за комуникационни услуги в среди с инфраструктурни ограничения. Моделът съчетава централизирана SIP сигнализация с директен пренос на медийния трафик, което минимизира латентността и елиминира негативното влияние на техническите ограничения при регионалните доставчици. Това помага за заобикаляне на проблеми с NAT траверс или ограничаване на честотната лента от страна на доставчиците.
6. **Предложена е архитектура на федеративен AIS облак** за предоставяне на навигационна телеметрия като услуга. Тя се базира на стриктно разделение между управляващите и информационните функции и въвежда специализирани роли за обработка на потоци от данни. Интегрирани са механизми за дедупликация, пречистване и нормализация, които гарантират координираното предоставяне на надеждни телеметрични услуги. Федеративният облак може да обединява данни от различни източници, без да ги централизира принудително. Модулът за нормализация и дедупликация ефективно филтрира „шума“, породен от дублирането на телеметрични пакети в гъсти сензорни мрежи. Това позволява изграждането на единна, консистентна картина на трафика в реално време.

По този начин формулираните приноси очертават цялостен модел за оптимизиране на прехода от управление на асети към управление на услуги в сложни федерирани системи в публичния сектор.

Бъдещи изследвания

Получените резултати в дисертационния труд очертават редица възможности за бъдещо развитие и разширяване на предложените модели и архитектурни решения.

На първо място, логично продължение представлява развитието на федеративния AIS облак чрез усъвършенстване на механизмите за агрегиране, обработка и защитен транспорт на телеметрични потоци. В тази посока могат да бъдат изследвани подходи за следване на маршрутизиращи политики според NMEA v4 Tag Blocks, както и схеми за криптиране на транспорта през несигурни мрежи. Практическа основа за такова развитие е платформата AISMixer, предназначена за смесване на сигнали от един район в общ поток.

На второ място, перспективна посока е разширяването на модела към периферна обработка на данни чрез интегриране на леки алгоритми за локален анализ в общински и регионални възли. Подобен подход би позволил част от обработката да се извършва по-близо до източника на данни, което може да намали латентността, да ограничи натоварването на централната инфраструктура и да създаде предпоставки за по-проактивни цифрови услуги.

Трета посока за бъдещо развитие е изследването на федеративно обучение в публичния сектор. Такъв подход би позволил на различни институции да участват в изграждането на общи модели, без да се налага пряк обмен на сурови данни, което е особено важно в среди с високи изисквания за сигурност, поверителност и регулаторно съответствие.

Четвърта възможност е свързана с усъвършенстване на механизмите за доверие, проследимост и междуорганизационно взаимодействие в среди с множество автономни участници. В този контекст могат да се изследват средства за регистриране на събития, проследяване на жизнения цикъл на данните и автоматизирано отчитане на качеството на предоставяните услуги, включително при договорени параметри на обслужване.

Пета посока е адаптирането на предложените архитектурни решения към бъдещи комуникационни среди, включително 5G и 6G мрежи. Особен интерес представлява изследването на възможности за комбиниране на хибридни service-centric архитектури с

механизми за динамично разпределяне и изолиране на мрежови ресурси според потребностите на различни услуги.

Шеста важна посока е свързана с по-нататъшно развитие на киберустойчивостта чрез интегриране на post-quantum и quantum-safe криптографски подходи. С оглед на нарастващата зависимост на публичния сектор от цифрови услуги, подобни изследвания са необходими за осигуряване на дългосрочна устойчивост на системите срещу бъдещи криптографски рискове.

Перспективна насока за бъдещи изследвания е въвеждането на edge AI във федеративния AIS облак. Това би позволило част от анализа да се извършва още в периферните възли чрез ранно откриване на аномалии, предварителна оценка на риск и отделяне на значими събития. Подобен подход е в синхрон и с актуални инициативи по Дунав, включително DANRISS 2, където вече се търси съчетаване на изкуствен интелект, сензори и интеграция на данни.

Посочените направления не променят основната рамка на дисертационния труд, а представляват нейно естествено разширяване към по-висока степен на автономност, сигурност, мащабируемост и интелигентност на услугите в сложни федерирани системи.

Публикации по темата на дисертацията

1. **I. Iliev,** I. Blagoev and Y. Terziev, "Hybrid VoIP Solution to Address Regional ISP Challenges," 2025 6th International Conference on Communications, Information, Electronic and Energy Systems (CIEES), Ruse, Bulgaria, 2025, pp. 1-6, doi: 10.1109/CIEES66347.2025.11300241.
2. **Iliev, Il.,** Blagoev I., Centralized Parallel Computing as a Cloud Service for Solving Digital Transformation Problems in Smart Cities. 2023 4th International Conference on Communications, Information, Electronic and Energy Systems (CIEES), IEEE, 2023, DOI:10.1109/CIEES58940.2023.10378756, 1-1-4-4
3. **Iliev, I.**, **Blagoev, I.**, An Approach to Improve Web Video Streaming Security and Prevent Personal Data Leakage. Information & Security: An International Journal, 53, 1, Procon, 2022, ISSN:1314-2119, DOI:10.11610/isij.5306, 78-88
4. Blagoev, I., Balabanov, T., **Iliev,** I. RSA Weaknesses Caused by the Specifics of Random Number Generation. Information & Security: An International Journal, 50, 2, Procon Ltd., 2021, ISSN:0861-5160, DOI:10.11610/isij.5028, 171-179, 2021
5. Blagoev, I., Balabanov, T**., Iliev,** I. The Randomness in Shared Web Hostings. Extended Abstracts of 16th Annual Meeting of the Bulgarian Section of SIAM, Fastumprint, 2021, ISSN:1313-3357, 9-10
6. Iliev, I., Blagoev, I. Security Considerations and Techniques for Video Streaming Distribution in Home ISPs (International Conference on Electronics, Engineering Physics and Earth Science (EEPES 2026) which will be held on 24th-27th June, 2026 in Bandirma, Turkey).

Участие в проекти

Националната научна програма **(ННП) „Сигурност и Отбрана” (ННП СО)**

Забелязани цитирания

Iliev, I., Blagoev, I.. An Approach to Improve Web Video Streaming Security and Prevent Personal Data Leakage. Information & Security: An International Journal, 53, 1, Procon, 2022, ISSN:1314-2119, DOI:https://doi.org/10.11610/isij.5306, 78-88

Цитира се в:

1. Daniela Borissova, Milena Bankovska, Katia Rasheva-Yordanova, Zornitsa Dimitrova, Multicriteria Model for Evaluation of Learning Management Systems, WSEAS TRANSACTIONS on BUSINESS and ECONOMICS, Volume 22, 2025, E-ISSN: 2224-2899, DOI: 10.37394/23207.2025.22.101, @2025
2. Yinka Akintunde Fagbile. Nollywood, Film Streaming, and Ethical Practices. Integral Research (Peer-reviewed, Open Access & Indexed Multidisciplinary Journal) ISSN: 3048-599, https://integralresearch.in/, Vol. 02, No. 03, March. 2025. 177

Декларация за оригиналност на резултатите

Декларирам, че дисертацията съдържа оригинални резултати, получени, при проведени от мен, научни изследвания с подкрепата и съдействието на научния ми ръководител.

Резултатите, които са получени, описани и/или публикувани от други учени, са коректно и подробно цитирани в библиографията.

Настоящият дисертационен труд не е прилаган за придобиване на научна степен в друго висше училище, университет или научен институт.

Подпис: ……..

/ ……. /

Библиография

1. Център за изследване на демокрацията, Телекомуникационната политика на България юни 1995 г. Достъпно на: https://csd.eu/fileadmin/user_upload/publications_library/files/1995/1995_20_Telekomunikacionnata_politika_na_Blgarija.pdf
2. Световна банка (World Bank), Memorandum And Recommendation Of The President Of The International Bank For Reconstruction And Development To The Executive Directors On A Proposed Loan In An Amount Equivalent To Us$30 Mllion To The Bulgarian Telecommunications Company With The Guarantee Of The Republic Of Bulgaria For A Telecommunications Project March 8, 1993. Достъпно на: https://documents1.worldbank.org/curated/en/463031468006036194/pdf/multi-page.pdf
3. БТК АД, Consolidated And Separate Financial Statements Annual Directors's Report Independent Auditor's Report 31 December 2008. Достъпно на: https://www.vivacom.bg/web/files/financial_reports/27/document/%2831.12.08%29%20Consolidated%20and%20Separate%20Financial%20Statements%20of%20BTC%20for%202008%20%28published%20on%20June%2030%2C%202009%29.pdf
4. Комисия за регулиране на съобщенията, Определяне, анализ и оценка на пазара на Предоставяне на (физически) достъп на едро до мрежова инфраструктура (включително самостоятелен и съвместен необвързан достъп) в определено местоположение и на пазара на Предоставяне на широколентов достъп на едро Приложение към Решение № 246/22.02.2011 г. Достъпно на: https://crc.bg/files/_bg/M4_5_BG_Final_nonconfidential.pdf
5. Комисия за регулиране на съобщенията, Определяне, анализ и оценка на ПАЗАРА НА ЕДРО НА ЛОКАЛЕН ДОСТЪП В ОПРЕДЕЛЕНО МЕСТОПОЛОЖЕНИЕ, Проект. Достъпно на: https://crc.bg/files/m_3a-public-pc-19.pdf
6. Министерство на транспорта и съобщенията, National Broadband Infrastructure Plan for Next Generation Access Decree № 435/ 26.06. 2014. Достъпно на: https://www.mtc.government.bg/sites/default/files/bg_nga_plan_eng.pdf
7. Valentina Petrova (Aalborg University), Master thesis – "Analysis of broadband development in Bulgaria". Достъпно на: https://projekter.aau.dk/projekter/files/260118504/Master_Thesis_Valentina.pdf

8. NATO. Resilience, civil preparedness and Article 3. NATO Topic, updated 13 November 2024. Достъпно на: https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3

9. Съвет на Европейския съюз. Maritime security, 2025. Достъпно на https://www.consilium.europa.eu/en/policies/maritime-security/

10. European External Action Service (EEAS). EU strategic approach to the Black Sea region, 20.10.2025. Достъпно на https://www.eeas.europa.eu/eeas/eu-strategic-approach-black-sea-region_en

11. Submarine Networks. Novatel to Build and Operate the Kardesa Digital Infrastructure in Bulgaria, 04.02.2026. Достъпно на https://www.submarinenetworks.com/en/systems/asia-europe-africa/kardesa/novatel-to-build-and-operate-the-kardesa-digital-infrastructure-in-bulgaria

12. Vodafone Group. Vodafone Group and Vodafone Ukraine to build new submarine cable system across Black Sea, 20.10.2025. Достъпно на https://www.vodafone.com/news/newsroom/technology/vodafone-group-and-vodafone-ukraine-to-build-new-submarine-cable-system-across-the-black-sea

13. Vivacom. "Vivacom изгражда високоскоростна свързаност в над 150 малки населени места с финансиране от ЕС". 11.07.2025. Достъпно на: https://www.vivacom.bg/za-nas/novini/vivacom-izgrazhda-visokoskorostna-svarzanost-v-nad-150-malki-naseleni-mesta-s-finansirane-ot-es?_gl

14. Министерство на транспорта и съобщенията, DIGITAL TRANSFORMATION OF BULGARIA FOR THE PERIOD 2020-2030. Достъпно на: https://www.mtc.government.bg/sites/default/files/digital_transformation_of_bulgaria_for_the_period_2020-2030_f.pdf

15. Burmambet, A. Romanian Maritime Ports in the Digital Transformation Era: The Shift from Fourth-Generation to Smart Ports and the Impact on the Global Logistics Ecosystem. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, vol. 19, no. 1, pp. 125–133, 2025. doi:10.12716/1001.19.01.15.

16. Gasparotti, C., Ungureanu, C., Popescu, G., and Domnisoru, L. Strategies for Developing Romanian Seaports as Smart Ports. Sustainability, vol. 18, no. 3, article 1658, 2026. doi:10.3390/su18031658.

17. Gu Z, Corcoglioniti F, Lanti D, et al. A systematic overview of data federation systems. Semantic Web: – Interoperability, Usability, Applicability. 2022;15(1):107-165. doi:10.3233/SW-223201

18. R. Buyya, R. Ranjan, and R. N. Calheiros, "InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services," in Proceedings of the 10th International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP), 2010, pp. 13–31. doi: 10.1007/978-3-642-13119-6_2.

19. K. Bernsmed, M. G. Jaatun, P. H. Meland и A. Undheim, „Thunder in the clouds: Security challenges and solutions for federated clouds", в Proc. 4th IEEE Int. Conf. Cloud Comput. Technol. Sci. (CloudCom), 2012, с. 113–120. https://jaatun.no/papers/2012/thunder-post.pdf

20. ITU-R Recommendation M.1371 (AIS TDMA in VHF maritime mobile band). ITU. https://www.itu.int/rec/R-REC-M.1371

21. NMEA 0183 Interface Standard – National Marine Electronics Association (NMEA). https://www.nmea.org/nmea-0183.html

22. Wu, Daniel & Aarsnes, Marion. (2017). An Introduction to Assessing Bunkering Operations Through AIS Data. 10.13140/RG.2.2.21415.04009.

23. D. Memos, "Shaking up the Maritime Industry through Open Data and Crowdsourcing," Journal of Continuous and Disruptive Innovation, pp. 1–16, Feb. 2017.

24. European Commission,Technical specifications for vessel tracking and tracing systems and repealing Regulation (EC) No 415/2007 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=PI_COM:C(2019)1114

25. Plass, Simon & Poehlmann, Robert & Hermenier, Romain & Dammann, Armin. (2015). Global Maritime Surveillance by Airliner-Based AIS Detection: Preliminary Analysis. Journal of Navigation. 68. 1-15. 10.1017/S0373463315000314.

26. Troupiotis-Kapeliaris, A.; Zissis, D.; Bereta, K.; Vodas, M.; Spiliopoulos, G.; Karantaidis, G. The Big Picture: An Improved Method for Mapping Shipping Activities. Remote Sens. 2023, 15, 5080. https://doi.org/10.3390/rs15215080

27. Šakan, Davor & Rudan, Igor & Žuškin, Srđan & Brčić, David. (2018). Near Real-time S-AIS: Recent Developments and Implementation Possibilities for Global Maritime Stakeholders. Pomorstvo. 32. 211-218. 10.31217/p.32.2.6.

28. IALA Recommendation A-124, Appendix 19: Satellite AIS Considerations (2011). https://www.e-navigation.nl/sites/default/files/A-124_19%20ed%201.00%20Satellite%20AIS%20Considerations.pdf

29. Fette I. and A. Melnikov, "The WebSocket Protocol," RFC 6455, Dec. 2011.

30. ButlerH., M. Daly, A. Doyle, S. Gillies, T. Schaub, and C. Schmidt, "The GeoJSON Format," RFC 7946, Aug. 2016.

31. Kent S. and K. Seo, "Security Architecture for the Internet Protocol," RFC 4301, Dec. 2005.

32. KaufmanC., P. Hoffman, Y. Nir, and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)," RFC 7296, Oct. 2014.

33. RescorlaE., "WebRTC Security Architecture," RFC 8827, Jan. 2021.

34. Baugher M. et al., "The Secure Real-time Transport Protocol (SRTP)," RFC 3711, Mar. 2004.

35. McGrew D. and E. Rescorla, "DTLS Extension to Establish Keys for SRTP," RFC 5764, May 2010.

36. Valin J.-M. and K. Vos, "Definition of the Opus Audio Codec," RFC 6716, Sep. 2012.

37. LeeC. A., R. B. Bohn, and M. Michel, "The NIST Cloud Federation Reference Architecture," NIST SP 500-332, 2020.

38. L. Bao, H. Luo, X. Gao, B. Ning, F. Zhao and Y. Zhu, "MT-e&R: NMEA Protocol-Assisted High-Accuracy Navigation Algorithm Based on GNSS Error Estimation Using Multitask Learning," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 11, pp. 20464-20475, Nov. 2022, doi: 10.1109/TITS.2022.3179237

39. Shi W. et al., "Edge Computing: Vision and Challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637-646, Oct. 2016.

40. SatyanarayananM., "The Emergence of Edge Computing," IEEE Computer, vol. 50, no. 1, pp. 30-39, Jan. 2017.

41. Akidau T. et al., "The Dataflow Model: A Practical Approach to Balancing Correctness, Latency, and Cost in Massive-Scale, Unbounded, Out-of-Order Data Processing," Proc. VLDB Endow., vol. 8, no. 12, pp. 1792-1803, Aug. 2015.

42. J. Nickolls, I. Buck, M. Garland, and K. Skadron, "Scalable Parallel Programming with CUDA," ACM Queue, Mar./Apr. 2008.

43. Mell P. and T. Grance, "The NIST Definition of Cloud Computing," NIST SP 800-145, 2011.

44. Julian Jang-Jaccard and SuryaNepal, “A survey of emerging threats in cybersecurity,” Journal of Computer and System Sciences 80, no. 5 (2014): 973-993.

45. Georgi Kostadinov and Tatiana Atanasova, “Security Policies for Wireless and Network Infrastructure,” Problems of Engineering Cybernetics and Robotics 71 (2019): 14-19.

46. Kristina Dineva and Tatiana Atanasova, “Regression Analysis on Data Received from Modular IoT System,” 33rd annual European and Modelling Conference ESM'2019, Palma de Mallorca, Spain, December 2019.

47. Velizar Shalamanov, Vladimir Monov, Ivaylo Blagoev, Silvia Matern, Gergana Vassileva, and Ivan Blagoev, “A Model of ICT Competence Development for Digital Transformation,” Information & Security: An International Journal 46 (2020): 269-284, https://doi.org/10.11610/isij.4619.

48. David F. DiCarlo, “Random Number Generation: Types and Techniques,” Theses (Liberty University, Center for Computer and Information Technology, 2012).

49. James Carr, “Simple Random Number Generation,” Computers & Geosciences 29, no. 10 (2003): 1269-1275, https://doi.org/10.1016/j.cageo.2003.07.002.

50. Pierre L’Ecuyer, “Random Number Generation,” in Handbook of Simulation: Princi-ples, Methodology, Advances, Applications, and Practice, edited by James E. Gentle, Wolfgang Karl Härdle, and Yuichi Mori (Berlin, Heidelberg: Springer, 2007), https://doi.org/10.1007/978-3-642-21551-3_3.

51. Andrew Jin, David Ling, and Alwyn Goh, “Biohashing: Two factor authentication featuring fingerprint data and tokenised random number,” Pattern Recognition 37 (2004): 2245- 2255.

52. Carmen Camara, Honorio Martín, Pedro Peris-Lopez, and Muawya Aldalaien, “Design and Analysis of a True Random Number Generator Based on GSR Signals for Body Sensor Networks,” Sensors 19, no. 9 (2019), 2033; https://doi.org/10.3390/ s19092033.

53. Salih Ergün, “Security analysis of a chaos-based random number generator for appli-cations in cryptography,” 15th International Symposium on Communications and In-formation Technologies (ISCIT), Nara, Japan, 2015, 319-322, https://doi.org/10.1109/ ISCIT.2015.7458371.

54. Boris Ryabko, JaakkoAstola, and Mikhail Malyutov, Compression-Based Methods of Statistical Analysis and Prediction of Time Series (Cham, Switzerland: Springer Inter-national Publishing, 2016).

55. Wade Trappe and Lawrence Washington, Introduction to cryptography with coding theory, 2nd ed. (Upper Saddle River, NJ: Pearson, 2006).

56. Markus Dichtl, “How to Predict the Output of a Hardware Random Number Genera-tor,” in Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems CHES 2003 (Berlin, Heidelberg: Springer, 2003), 181-188, https://doi.org/10.1007/978-3-540-45238-6_15.

57. Ahmad Lavasani and Taraneh Eghlidos, “Practical next bit test for evaluating pseu-dorandom sequences,” Scientia Iranica 16, no. 1 (2009): 19-33.

58. Joseph Hart, Rajarshi Roy, and Thomas Murphy, “Optical random number generation – harvesting entropy from noise and chaos,” 51st Annual Conference on Information Sciences and Systems (CISS), Baltimore, MD, USA, March 2017, https://doi.org/10.1109/CISS.2017.7926165.

59. D. J. Bernstein, Y.-A. Chang, C.-M. Cheng, L.-P. Chou, N. Heninger, T. Lange, and N. van Someren, “Factoring RSA Keys from Certified Smart Cards: Coppersmith in the Wild,” in Advances in Cryptology – ASIACRYPT 2013 (Proceedings, Part II), K. Sako and P. Sarkar, Eds., Lecture Notes in Computer Science, vol. 8270, Bengaluru, India, Dec. 1–5, 2013, pp. 341–360. Springer, Berlin, Heidelberg, 2013, doi: 10.1007/978-3-642-42045-0_18.

60. Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman, “Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices,” 21 st Security Symposium Security’12, Bellevue, WA, Aug. 8-10, 2012, pp. 205-220.

61. Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, and Christophe Wachter, “Ron was wrong, Whit is right,” 2012, https://eprint.iacr.org/2012/064.pdf.

62. Kerry Scharfglass, Darrin Weng, Joseph White, and Christopher Lupo, “Breaking weak 1024-bit RSA keys with CUDA,” 13th International Conference on Parallel and Distributed Computing, Applications and Technologies, Beijing, China, 14-16 December 2012, https://doi.org/10.1109/PDCAT.2012.58.

63. Bouke Cloostermans, “Quasi-linear GCD computation and factoring RSA moduli,” Thesis (Eindhoven University of Technology, Department of Mathematics and Computer Science, 2012).

64. R. Afreen and S. C. Mehrotra, “A Review on Elliptic Curve Cryptography for Embedded Systems,” arXiv:1107.3631 [cs.CR], Jul. 2011, doi: 10.48550/arXiv.1107.3631.

65. Sarkar, A., Singh, B.K. A multi-instance cancelable fingerprint biometric based secure session key agreement protocol employing elliptic curve cryptography and a double hash function. Multimed Tools Appl 80, 799–829 (2021). https://doi.org/10.1007/s11042-020-09375-7

66. N. Koblitz, “Elliptic curve cryptosystems,” Mathematics of Computation, vol. 48, no. 177, pp. 203–209, Jan. 1987, doi: 10.1090/S0025-5718-1987-0866109-5.

67. V. Shoup, “Lower Bounds for Discrete Logarithms and Related Problems,” in Advances in Cryptology — EUROCRYPT ’97, W. Fumy, Ed., Lecture Notes in Computer Science, vol. 1233, pp. 256–266, Springer, 1997, doi: 10.1007/3-540-69053-0_18.

68. Kessler, Gary C.. “Protected AIS: A Demonstration of Capability Scheme to Provide Authentication and Message Integrity.” TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation (2020): n. pag.

69. P. W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” in Proceedings 35th Annual Symposium on Foundations of Computer Science (FOCS), Santa Fe, NM, USA, Nov. 1994, pp. 124–134, doi: 10.1109/SFCS.1994.365700.

70. J. Proos and C. Zalka, “Shor’s discrete logarithm quantum algorithm for elliptic curves,” Quantum Information and Computation, vol. 3, no. 4, pp. 317–344, 2003.

71. Documentation Team, “Amazon Kinesis Video Streams Developer Guide,” 2018, ISBN-10:9888407848, ISBN-13:978-9888407842.

72. Tasho D. Tashev, Vladimir V. Monov, and Radostina P. Tasheva, “High Performance Computations for Study the Stability of a Numerical Procedure for Crossbar Switch Node,” In: Dimov I., Faragó I., Vulkov L. (eds) Numerical Analysis and Its Applications, 6th International Conference, NAA 2016, Lozenetz, 2016, LNCS, volume 10187, Springer, Cham, 2017, ISBN:978-3-319-57098-3, DOI:10.1007/978-3-319-57099-0_76, 665-673.

73. Ivan Blagoev, “Neglected Cybersecurity Risks in the Public Internet Hosting Service Providers,” Information & Security: An International Journal 47, no. 1 (2020): 62-76, https://doi.org/10.11610/isij.4704, https://bpos.bg/publication/18454.

74. Paul Baka, Jeremy Schatten, Hollie Acres, SSL/TLS Under Lock and Key: A Guide to Understanding SSL/TLS Cryptography Paperback (2021), ISBN-10:0648931633, ISBN-13:978-0648931638.

75. Benoit Badrignans, Jean Luc Danger, Viktor Fischer, Guy Gogniat, and Lionel Torres (Eds.), Security Trends for FPGAS - From Secured to Secure Reconfigurable Systems (Netherlands: Springer, 2011).

76. Philip Goldie, Matthew Syme, Optimizing Network Performance with Content Switching: Server, Firewall and Cache Load Balancing (2003), ISBN: 0131014684.

77. John Paul Mueller, Security for Web Developers: Using JavaScript, HTML, and CSS, 2015, ISBN-13:978-1491928646.

78. Alec Tefertiller & Kim Sheehan (2019) TV in the Streaming Age: Motivations, Behaviors, and Satisfaction of Post-Network Television, Journal of Broadcasting & Electronic Media, 63:4, 595-616, DOI: 10.1080/08838151.2019.1698233

79. A. Mackin, F. Zhang and D. R. Bull, "A Study of High Frame Rate Video Formats," in IEEE Transactions on Multimedia, vol. 21, no. 6, pp. 1499-1512, June 2019, doi: 10.1109/TMM.2018.2880603

80. Mutlu Arpaci, Elton Ho, and Wei Yen "Providing integrated services with broadband PON", Proc. SPIE 4583, Metro and Access Networks, (16 October 2001); https://doi.org/10.1117/12.445133

81. Protocols and Design Guide, https://www.amx.com/en/site_elements/multicast-for-enterprise-video-streaming, white paper v.01.2015

82. Wenyang Yang, Liumei Zhang, An Application Research on IPv6 Multicasting Testing Method, Procedia Engineering, Volume 24, 2011, Pages 143-151, ISSN 1877-7058, https://doi.org/10.1016/j.proeng.2011.11.2617

83. Multicast GPON transmission and GEM frame processing method, EP1499155A1, Date of publication 19.01.2005 Bulletin 2005/03, Application number: 04016435.2, Applicant: Samsung Electronics Co., Ltd. Suwon-si, Gyeonggi-do (KR), Inventors: Lim, Se-Youn, Samsung Electronics Co., Ltd. Suwon-si, Gyeonggi-do (KR)

84. HTTP Live Streaming, https://datatracker.ietf.org/doc/html/rfc8216, ISSN: 2070-1721, August 2017

85. Conditional-access systems for digital broadcasting, https://www.itu.int/dms_pubrec/itu-r/rec/bt/R-REC-BT.1852-1-201701-I!!PDF-E.pdf, ITU-R BT.1852-1, 10/2016

86. Ralf-Philipp Weinmann, Kai Wirt, ANALYSIS OF THE DVB COMMON SCRAMBLING ALGORITHM, Communications and Multimedia Security (pp.195-207), January 2005, DOI:10.1007/11382324_15

87. Iliyan Iliev, Ivan Blagoev" An Approach to Improve Web Video Streaming Security and Prevent Personal Data Leakage" Information & Security: An International Journal,53 no. 1(2022):78-88 .https://doi.org/10.11610/isij.5306

88. B. H. Turnbull, "Important legal developments regarding protection of copyrighted content against unauthorized copying," in IEEE Communications Magazine, vol. 39, no. 8, pp. 92-100, Aug. 2001, doi: 10.1109/35.940045

89. S. Lian and Z. Liu, "Secure media content distribution based on the improved set-top box in IPTV," in IEEE Transactions on Consumer Electronics, vol. 54, no. 2, pp. 560-566, May 2008, doi: 10.1109/TCE.2008.4560130

90. B. Lomb and T. Guneysu, "Decrypting HDCP-protected Video Streams Using Reconfigurable Hardware," 2011 International Conference on Reconfigurable Computing and FPGAs, Cancun, Mexico, 2011, pp. 249-254, doi: 10.1109/ReConFig.2011.24

91. M.A. Erskine, D.G. Gregg, J. Karimi, J.E. Scott, Business Decision-Making Using Geospatial Data: A Research Framework and Literature Review. Axioms 2014, 3, 10-30. https://doi.org/10.3390/axioms3010010

92. R. Wickramasuriya, J. Ma, M. Berryman, P. Perez, Using geospatial business intelligence to support regional infrastructure governance, Knowledge-Based Systems Volume 53, November 2013, Pages 80-89, Springer, https://doi.org/10.1016/j.knosys.2013.08.024

93. S. Rivest, Y. Bédard, M.-J. Proulx, M. Nadeau, F. Hubert, J. Pastor, SOLAP technology: Merging business intelligence with geospatial technology for interactive spatio-temporal exploration and analysis of data, ISPRS Journal of Photogrammetry and Remote Sensing, Vol. 60, Issue 1, December 2005, Pages 17-33, https://doi.org/10.1016/j.isprsjprs.2005.10.002

94. V. Shalamanov, S. Matern, G. Penchev. Digitalization and Cyber Resilience Model for the Bulgarian Academy of Sciences. In: Tagarev, T., Atanassov, K.T., Kharchenko, V., Kacprzyk, J. (eds) Digital Transformation, Cyber Security and Resilience of Modern Societies. Studies in Big Data, 2021, vol 84. Springer, Cham. https://doi.org/10.1007/978-3-030-65722-2_6

95. K. Dineva, T. Atanasova, T. Balabanov. Cloud Dataflow for Machine Learning Modeling on IoT Data in Smart Livestock Farming, 22nd International Multidisciplinary Scientific GeoConference SGEM 2022, 2 - 11 July, 2022, Albena, Bulgaria doi:10.5593/sgem2022/6.1/s25.09

96. J. de Castro Lima, Computing Data Cubes Over GPU Clusters, Monografia, December 2018, Federal University of Ouro Preto Institute of Exact Sciences and Biology Undergraduate Program in Computer Science, https://www.monografias.ufop.br/bitstream/35400000/1527/6/MONOGRAFIA_ComputingDataCubes.pdf

97. I. Blagoev, Using R Programming Language for Processing of Large Data Sets, Proc. Int. Conf. Big Data, Knowledge and Control Systems Engineering – BdKCSE'2018, 21-22 November 2018, Sofia, Bulgaria, ISSN 2367-6450, pp. 91-98.

98. D. Luebke, "CUDA: Scalable parallel programming for highperformance scientific computing," 2008 5th IEEE International Symposium on Biomedical Imaging: From Nano to Macro, Paris, France, 2008, pp. 836-838, https://doi.org/10.1109/ISBI.2008.4541126

99. G. Giunta, R. Montella, G. Agrillo, G. Coviello. A GPGPU Transparent Virtualization Component for High Performance Computing Clouds. In: D'Ambra, P., Guarracino, M., Talia, D. (eds) Euro-Par 2010 - Parallel Processing. Euro-Par 2010. Lecture Notes in Computer Science, 2010, vol 6271. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-15277-1_37

100. GPU Accelerated Data Science, https://rapids.ai/

101. Petar Maymounkov and David Mazières. 2002. Kademlia: A Peer-to-Peer Information System Based on the XOR Metric. In Revised Papers from the First International Workshop on Peer-to-Peer Systems (IPTPS '01). Springer-Verlag, Berlin, Heidelberg, 53–65.

102. Borissova, D., Z. Dimitrova, V. Dimitrov. How to support teams to be remote and productive: Group decision-making for distance collaboration software tools. Information and Security. ISSN 0861-5160, e-ISSN 1314-2119, Digital Transformation, Cyber Security and Resilience, vol. 46, pp. 36-52, 2020, https://doi.org/10.11610/isij.4603

103. Borissova D., I. Mustakerov. A concept of intelligent e-maintenance decision making system. Innovations in Intelligent Systems and Applications (INISTA), 2013 IEEE International Symposium on. 19-21 June 2013, Print ISBN: 978-1-4799-0659-8, DOI: 10.1109/INISTA.2013.6577668.

104. Mustakerov, Ivan & Borissova, Daniela. (2013). An Intelligent Approach to Optimal Predictive Maintenance Strategy Defining. 2013 IEEE International Symposium on Innovations in Intelligent Systems and Applications, IEEE INISTA 2013. 10.1109/INISTA.2013.6577666.

105. Jens Saenger, Wojciech Mazurczyk, Jörg Keller, Luca Caviglione, VoIP network covert channels to enhance privacy and information sharing, Future Generation Computer Systems, Volume 111, 2020, Pages 96-106, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.04.032. (https://www.sciencedirect.com/science/article/pii/S0167739X19333965)

106. Rao, Anwesh & Gurucharan, B & V, Kiran. (2024). Comparative Study of RIP, OSPF, and EIGRP in VoIP Networks Across Different Ethernet Topologies. 1-5. 10.1109/AICECS63354.2024.10957443.

107. Y. Dabone, T. F. Ouedraogo and P. J. Kouraogo, "Impact Of Internet Exchange Points On ISPs Speeds And Latency," 2022 International Symposium on Networks, Computers and Communications (ISNCC), Shenzhen, China, 2022, pp. 1-6, doi: 10.1109/ISNCC55209.2022.9851789.

108. Siope Vakataki ‘Ofa, 2021. "Estimating the effects of Internet exchange points on fixed-broadband speed and latency," Asia-Pacific Sustainable Development Journal, United Nations Economic and Social Commission for Asia and the Pacific (ESCAP), vol. 28(2), pages 39-68, December.

109. Chatzis, N., Smaragdakis, G., Feldmann, A., & Willinger, W. “There is More to IXPs than Meets the Eye.” ACM SIGCOMM Computer Communication Review, 43(5), 19–28, 2013. doi:10.1145/2541468.2541473

110. A. Ahmed, Z. Shafiq, H. Bedi and A. Khakpour, "Peering vs. transit: Performance comparison of peering and transit interconnections," 2017 IEEE 25th International Conference on Network Protocols (ICNP), Toronto, ON, Canada, 2017, pp. 1-10, doi: 10.1109/ICNP.2017.8117549.

111. Ahmed, M., & Mansor, A. M. “CPU Dimensioning on Performance of Asterisk VoIP PBX.” Proceedings of the 11th Communications and Networking Simulation Symposium (CNS’08), 139–146, 2008. doi:10.1145/1400713.1400737

112. ZeroTier. The Protocol. ZeroTier Documentation. Достъпно на: https://docs.zerotier.com/protocol/

113. Gentile, A.F.; Macrì, D.; Greco, E.; Fazio, P. Overlay and Virtual Private Networks Security Performances Analysis with Open Source Infrastructure Deployment. Future Internet 2024, 16, 283. https://doi.org/10.3390/fi16080283

114. S. A. Baset and H. G. Schulzrinne, "An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol," Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications, Barcelona, Spain, 2006, pp. 1-11, doi: 10.1109/INFOCOM.2006.312.

115. D. -F. Hriţcan, A. Graur and D. Balan, "Securing IoT Environments Using ZeroTier and OPNsense," 2024 23rd RoEduNet Conference: Networking in Education and Research (RoEduNet), Bucharest, Romania, 2024, pp. 1-4, doi: 10.1109/RoEduNet64292.2024.10722755.

116. Michael, Thilo; Möller, Sebastian. “Effects of Delay and Packet-Loss on the Conversational Quality.” DAGA 2020.

117. Diao, Chenyao & Arévalo Arboleda, Stephanie & Raake, Alexander. (2024). Effects of Delay on Nonverbal Behavior and Interpersonal Coordination in Video Conferencing. 10.1109/MMSP61759.2024.10743300.

118. BERNARD S. KU, CHAPTER 12 - Internet Telephony Technology and Standards Overview, Editor(s): JERRY D. GIBSON, In Communications, Networking and Multimedia, Multimedia Communications, Academic Press, 2001, Pages 191-219, ISBN 9780122821608, https://doi.org/10.1016/B978-012282160-8/50013-X.(https://www.sciencedirect.com/science/article/pii/B978012282160850013X)

119. A. A. Catellier and S. D. Voran, "Wideband Audio Waveform Evaluation Networks: Efficient, Accurate Estimation of Speech Qualities," in IEEE Access, vol. 11, pp. 125576-125592, 2023, doi: 10.1109/ACCESS.2023.3330640.3, doi: 10.1109/ACCESS.2023.3330640.

120. Zwicklhuber, T., and M. Kaufmann. “EURIS (European River Information Services System) – The Central European RIS Platform: Introducing a Joint RIS System Among 13 European Countries.” In: Li, Y., Hu, Y., Rigo, P., Lefler, F. E., and Zhao, G. (eds.), Proceedings of PIANC Smart Rivers 2022, Lecture Notes in Civil Engineering, vol. 264, Springer, Singapore, 2023, pp. 850–856. doi:10.1007/978-981-19-6138-0_75.

121. Министерство на транспорта и съобщенията. „Bulgaria and Romania with a common regime for ships inspections on the Danube.“ 22.02.2018. Достъпно на: https://www.mtc.government.bg/en/category/1/bulgaria-and-romania-common-regime-ships-inspections-danube

122. Министерство на регионалното развитие и благоустройството. „Модерна система ще следи за замърсяване на Дунав от кораби.“ 23.03.2026. Достъпно на: https://www.mrrb.bg/bg/moderna-sistema-ste-sledi-za-zamursyavane-na-dunav-ot-korabi/

123. Goodchild, M.F. Citizens as sensors: the world of volunteered geography. GeoJournal 69, 211–221 (2007). https://doi.org/10.1007/s10708-007-9111-y

124. Memos, D.; et al. Shaking up the Maritime Industry through Open Data and Crowdsourcing. Journal of Continuous and Disruptive Innovation, 1(2), 2017. (River Publishers).

125. MarineTraffic. “Inside MarineTraffic: New features & what’s coming next (EMEA & AMER | March 2026)” Webinar recording, YouTube, 18 Mar. 2026. Available: https://www.youtube.com/watch?v=6RnJGUrX_1g Accessed: 19 Mar. 2026.

126. Станкова, М. Алтернативен туризъм в рибарска област Шабла–Каварна–Балчик. София: [б. и.], 2016. 144 с.: с ил. Издание, реализирано с безвъзмездна финансова

помощ по Местна стратегия за развитие на МИРГ Шабла–Каварна–Балчик, чрез Оперативна програма за развитие на сектор „Рибарство“ 2007–2013, съфинансирана от Европейския фонд за рибарство.

127. Ramos, J.; Drakeford, B.; Costa, J.; Leitão, F. Boating Tourism and Fishing Interactions: A Social Network Analysis Using AIS Data. Sustainability 2025, 17, 4837. https://doi.org/10.3390/su17114837