NETHR: ПРВИ АНОНИМНИ И ДЕЦЕНТРАЛИЗОВАНИ ПРОТОКОЛ СЛЕДЕЋЕ ГЕНЕРАЦИЈЕ

NETHR: THE FIRST ANONYMOUS AND DECENTRALIZED NEXT-GENERATION PROTOCOL

ЛАЗАР АЛЕКСИЋ
IV Разред, Гимназија "Бора Станковић" Врање, Културно образовни центар Врање

ЈАСМИНА МЛАДЕНОВИЋ
Дипл. Инг. Електротехнике, Гимназија "Бора Станковић" Врање

РЕЗИМЕ: Овај рад представља дизајн, имплементацију и емпиријску евалуацију протокола Nethr, децентрализованог P2P протокола следеће генерације, конципираног за поуздану комуникацију у условима активне цензуре и потпуног колапса инфраструктуре. Предмет истраживања је заштита дигиталних комуникација од инфраструктурних противника који спроводе масовну цензуру, дубоку инспекцију пакета (DPI) и прекиде интернета. Nethr решава фундаменталну слабост постојећих приступа, зависност од централне инфраструктуре и препознатљивост на мрежи, увођењем три иновативна механизма која у комбинацији нису остварена ни у једном постојећем протоколу: симетричне пробне дешифрације, дедупликације без преноса идентификатора и урођене непрепознатљивости формата пакета. Примењена методологија обухвата C++ симулационо окружење за тестирање ограниченог епидемијског прослеђивања у условима насумичног и циљаног отказивања чворова у хибридним топологијама скалабилних мрежа, као и ригорозну статистичку анализу стварног Nethr саобраћаја помоћу Python алата. Резултати показују да Nethr одржава стопу испоруке изнад 90% чак и када 40% мреже откаже, уз прихватљиву латенцију на 90. перцентилу у свим тестираним сценаријима. Статистичка анализа путем Хи-квадрат и Колмогоров-Смирнов тестова, као и анализе Шенонове ентропије и Пирсонове аутокорелације, доказује да је Nethr саобраћај математички неразлучив од идеалног насумичног шума дуж целог пакета, укључујући заглавље, потпуно елиминишући сваки статични образац на којем DPI системи заснивају класификацију. Криптографску основу чине хибридна постквантна размена кључева (Noise_XX са sntrup761/X25519) и аутентификована симетрична енкрипција (ChaCha20-Poly1305), обезбеђујући отпорност на квантну криптоанализу и ниску латенцију на стандардном хардверу, без ослонца на икакву централну инфраструктуру.

КЉУЧНЕ РЕЧИ: криптографија, интернет, протокол, приватност, децентрализованост

ABSTRACT: This paper presents the design, implementation, and empirical evaluation of Nethr, a next-generation decentralized P2P protocol engineered for resilient communication under active censorship and complete infrastructure collapse. The research addresses the fundamental weaknesses of existing privacy-preserving systems, their reliance on central infrastructure and their detectable network presence, through three novel mechanisms that, in combination, have not been achieved by any existing protocol: symmetric trial decryption, identifierless deduplication, and native wire-format indistinguishability. The methodology comprises a C++ simulation engine evaluating

Bounded Epidemic Routing under random and targeted node failure scenarios across hybrid scale-free network topologies, and rigorous statistical analysis of live-captured Nethr traffic using Python. Results demonstrate that Nethr sustains a message delivery rate above 90% even under 40% network failure, with convergence latency remaining acceptable at the 90th percentile across all tested scenarios including sophisticated targeted attacks on the highest-degree network hubs. Statistical analysis via chi-square uniformity, Kolmogorov-Smirnov, Shannon entropy, and Pearson autocorrelation tests proves that Nethr traffic is mathematically indistinguishable from ideal random noise across the entire packet, including the header, completely eliminating every static byte pattern on which DPI classifiers depend. This is realized through hybrid post-quantum key exchange (Noise_XX with sntrup761/X25519) and authenticated symmetric encryption (ChaCha20-Poly1305), delivering quantum-resistant security and low convergence latency on commodity hardware, with zero reliance on any central infrastructure.

KEYWORDS: cryptography, internet, protocol, privacy, decentralization

УВОД

У савременом дигиталном добу, интернет престаје да буде универзално доступан и слободан простор. Према подацима организације Access Now [1], у 2025. години забележено је 313 прекида интернета у 52 земље широм света. Слобода интернета опада већ 15 година узастопно, без икаквих знакова стабилизације [2]. Мрежни ауторитети су последњих година, поред пасивних метода посматрања, почели да употребљавају и активне методе за рестрикцију дотока информација [3]. Ови напади на инфраструктурном нивоу чине традиционалне моделе повезивања (енгл. Client-Server) изузетно рањивим.

Протокол Nethr је дизајниран за успостављање сигурне и брзе размене података управо у условима деловања оваквог инфраструктурног противника (енгл. Infrastructural Adversary - IA). Фокус овог рада лежи на развоју система који не штити само садржај комуникације, већ идентитет и метаподатке корисника, као и само присуство протокола на мрежи кроз напредне методе обфускације, чинећи га ефективно невидљивим за системе надзора.

СПИСАК СИМБОЛА И СКРАЋЕНИЦА

СИМБОЛИ

- *H(X) [bit]* - Шенонова ентропија скупа бајтова X (изражена у битима)
- *k [/]* - фактор ширења (fanout) епидемијског прослеђивања
- *N [/]* - укупан број чворова у мрежи
- *TTL [/]* - време живота пакета (Time To Live)
- *Δ [bit]* - разлика ентропија заглавља и тела пакета, $H(\text{заглавље}) - H(\text{тело})$

СКРАЋЕНИЦЕ

- **HKDF** (HMAC-based Key Derivation Function) - Функција за извођење кључева заснована на HMAC алгоритму
- **PQ** (Post Quantum) - Односи се на енкрипцију која није ефикасно решива ни проналаском квантних рачунара и алгоритама

- **NUMS** (Nothing Up My Sleeves) - филозофија при дизајнирању алгоритма која елиминише сумњиве константе како би се избегла потенцијално скривена "задња врата" (backdoors)
- **KEM** (Key Encapsulation Mechanism) - Механизам за енкапсулацију кључа, криптографски процес где пошиљалац користи јавни кључ примаоца да безбедно генерише и упакује заједнички сесијски кључ.

ТЕОРИЈСКЕ ОСНОВЕ И СРОДНИ РАДОВИ

Дизајн протокола Nethr настао је анализом слабости постојећих решења против инфраструктурног противника, приказаних у Табели 1. Мреже попут Tor-a и I2P-a [4] ослањају се на централне директоријумске сервере који могу бити лако блокирани. Bitmessage [5] користи асиметричну ECIES енкрипцију за прослеђивање путем потпуног поплављивања мреже (енгл. full-flood), где сваки чвор прима сваку поруку, што није скалабилно, док се хеш за дедупликацију преноси у чистом тексту. Док Vuvuzela [6] и Loopix [7] пружају математички доказану диференцијалну приватност, оба система захтевају централне сервере и плаћају високу цену у перформансама. Vuvuzela кроз екстремну латенцију (~37c), а Loopix кроз минималан проток. Протокол EFPIX [8] унапређује Bitmessage модел заштитом од нежељених порука и порицивошћу, али је ово решење остало на нивоу теоријског дизајна.

ТАБЕЛА 1. Поређење са сродним протоколима
TABLE 1. Comparison with related protocols

Особина	I2P	Tor	Bitmessage	Vuvuzela	Nethr
Без сервера	~	-	+	-	+
Отпорност на DPI	-	-	-	-	+
PQ енкрипција	+	~	-	-	+
Ниска латенција	~	~	-	-	+
Штити метаподатке	-	-	~	+	+
Без ИД дедупликације	-	-	-	-	+

Ознаке: '+' функционалност потпуно имплементирана; '~' делимична имплементација са значајним ограничењима, '-' функционалност одсутна по дизајну.

Прелазак на криптографске примитиве следеће генерације доноси драстично веће убрзање и сигурност. Док се застарели протоколи ослањају на алгоритме рањиве на квантну криптоанализу или на методе које су постале ограничавајући фактор за модерне мреже, Nethr користи хибридни модел дизајниран према NUMS филозофији (Табела 2). Овај одабир елиминише сумњу у скривене рањивости и намерне пропусте у дизајну, али и омогућава експоненцијално бржу обраду података. Алгоритам sntrup761 (Streamlined NTRU Prime [9]) пружа постквантну непробојност уз минималан трошак ресурса и изабран је због дуготрајне примене и тестирања, док ChaCha20-Poly1305 и BLAKE3 омогућавају да се пробна декрипција и дедупликација извршавају готово тренутно. Истовремено, имплементација Noise_XX [10] протокола осигурава потпуну аутентификацију учесника уз скривање идентитета (јавних кључева) од пасивних посматрача током руковања у минималном броју пакета, спречавајући противника да уопште детектује успостављање сесије.

ТАБЕЛА 2. Генерацијски скок криптографских примитива
TABLE 2. Generational leap of cryptographic primitives

Категорија	Прошла генерација	Нова генерација	Кључна предност
PQ Размена кључева	Није постојала	sntrup761	Пост-квантна сигурност кроз NTRU решетке.
Класична размена	RSA/DH	X25519	Изузетно мали кључеви и имуност на тајминг нападе.
Оквир (Framework)	TLS/Наменски	Noise Protocol	Скривање идентитета, минимални пакети и оптрећење.
Аутентификација	HMAC-SHA256	Poly1305 (AEAD)	Једнопролазна аутентификација интегрисана у енкрипцију за бржу пробну декрипцију.
Симетрична енкрипција	AES-CBC	ChaCha20	Имуност на тајминг нападе и већа брзина без хардверског убрзања.
Извођење кључа	SHA-256	HKDF (HMAC базиран)	Криптографски јаче раздвајање сесионих кључева.
Хеширање	SHA-2/SHA-512	BLAKE3	Паралелизација за тренутну дедупликацију пакета.

МАТЕРИЈАЛ И МЕТОДИКА РАДА

Да би се омогућила потпуна репродукција истраживања, развој и тестирање протокола спроведени су кроз логички одвојене фазе, обухватајући развој архитектуре система, имплементацију заштитних криптографских механизама и израду алата за емпиријску евалуацију.

АРХИТЕКТУРА СИСТЕМА

Главна логика Nethr протокола развијена је у програмском језику C++20 у форми независног позадинског процеса (енгл. daemon). Оваква модуларна архитектура значи да сам протокол ради у позадини, док се сва контрола и размена података одвија искључиво преко TCP интерфејса за међупроцесну комуникацију (енгл. Inter-Process Communication - IPC).

Кроз IPC интерфејс реализовани су Flutter графички интерфејс за кориснике и Python скрипте за аутоматизовано прикупљање података и покретање експеримента.

За имплементацију постквантних примитива и стандардних криптографских операција коришћене су библиотеке liboqs [11] и libsodium [12].

ЗАШТИТА МЕТАПОДАТАКА И ОТПОРНОСТ НА DPI

Да би систем био отпоран на инфраструктурног противника, методика дизајна је захтевала потпуну елиминацију метаподатака о дужини, времену и природи комуникације.

ЗАШТИТА ДУЖИНЕ ПОРУКЕ

Сваки UDP пакет који Nethr генерише има фиксну величину од тачно 1472 бајта (максимум за IPv4 без фрагментације). Уколико је корисна порука краћа, остатак пакета се аутоматски допуњава криптографски насумичним шумом (енгл. random padding), чиме противник не може да закључи количину пренетих информација.

ОТПОРНОСТ НА DPI

Свако заглавље пакета маскира се XOR операцијом у односу на 48-бајтну вредност изведену BLAKE3 хеширањем самог тела пакета. Пошто је тело увек AEAD [13] шифрат или насумични шум, не постоје статични "магични бајтови". Сваки пакет изгледа као потпуно нов, насумичан низ података, чиме се онемогућава класификација од стране система за дубоку инспекцију пакета (DPI).

ЗАШТИТА ИДЕНТИТЕТА ДОПИСНИКА И ВРЕМЕНА ПОРУКЕ

Метаподаци о времену слања штите се иновативном употребом покривног саобраћаја. Традиционалне имплементације се ослањају на константно слање лажних порука високе или ниске фреквенције, што резултује превеликим трошковима протока или неприхватљивим кашњењима. Уместо тога, протокол континуирано генерише динамичке временске опсеге који се насумично мењају, бирајући из њих насумична одлагања. По истеку тог одлагања, уколико нема праве поруке, позадински процес шаље покривне пакете испуњене искључиво криптографским шумом. Пошто су покривни пакети, пакети за размену и праве поруке криптографски неразлучиви на мрежи, статистички је немогуће утврдити да ли процес активно комуницира или само одржава мрежу. Насумична природа интервала дозвољава слање правих порука са минималним одлагањем уз драстично мању потрошњу ресурса у поређењу са високофреквентним методама. Напомиње се да овај механизам штити од тајминг напада, али не спречава инфраструктурног противника који контролише мрежу да идентификује скуп учесника који користе протокол, аналогно Tor-овом ограничењу у срединама са малим скупом корисника.

ПРОТОКОЛ РАЗМЕНЕ ПОРУКА И КРИПТОГРАФСКИ ТОК

Noise_XX руковање омогућава узајамну аутентификацију без претходне размене кључева. Коришћењем хибридног механизма за енкапсулацију кључева (KEM) (X25519 и sntrup761) и HKDF функције, осигурана је постквантна тајност сесије и отпорност на компромитовање појединачних алгоритама. Свака порука се шифрује (ChaCha20-Poly1305), допуњава до 1472 бајта и маскира XOR операцијом заглавља са BLAKE3 хешом тела пакета, чиме се уклањају DPI обрасци. Чворови примењују пробну дешифрацију верификацијом Poly1305 ознаке, која служи као имплицитни идентификатор примаоца. Кључно својство анонимности је да се, без обзира на исход дешифрације, сваки нови пакет са TTL > 1 прослеђује насумично одабраним k суседима. Тако прималац поступа идентично посреднику, чиме се скрива одредиште. Пре прослеђивања, чвор врши дедупликацију поређењем BLAKE3 хеша шифрованог тела пакета са локалним кешом, чиме се дупликати елиминишу без увида у садржај или идентитет.

СИМУЛАЦИОНО ОКРУЖЕЊЕ И МРЕЖНА ТОПОЛОГИЈА

За евалуацију епидемијског ширења развијено је интерно симулационо окружење које покреће виртуелне чворове на повратној (енгл. loopback) адреси. Топологија мреже се генерише комбиновањем прстенасте структуре са Барабаши-Алберт (енгл. Barabási-Albert) моделом преференцијалног повезивања, чиме се добија скалабилна мрежа (енгл. scale-free) са карактеристикама "малог света". Овај хибридни модел је одабран јер највернији репрезентује стварне P2P системе који природно еволуирају ка топологијама са израженим локалним кластерима и јако повезаним чвориштима. Да би се изоловао учинак самог епидемијског ширења и пробне дешифрације, симулатор користи предуспостављене сесије, успостављајући симетричне кључеве између свих чворова пре почетка експеримента.

ОТПОРНОСТ НА SYBIL НАПАДЕ

У потпуно отвореним P2P системима, Sybil напад где противник контролише мноштво лажних чворова омогућава инфилтрацију у граф рутирања ради селективног испуштања саобраћаја или анализе токова. Nethr пружа отпорност на ове нападе на два нивоа. Прво, хибридна Barabási-Albert топологија користи преференцијално повезивање које фаворизује дуготрајне чворове са већим бројем веза, чиме се нови Sybil чворови природно маргинализују на периферији графа и тешко преузимају улогу кључних чворишта. Друго, епидемијски алгоритам са фактором ширења k обезбеђује редундантност путева, чак и ако малициозни чвор одбије прослеђивање, порука наставља ширење кроз преостале паралелне гране. Ипак, потпуна безбедност зависи од величине и хетерогености мреже. Будући развој протокола предвиђа увођење доказа рада (енгл. proof-of-work) за пријем чворова и система репутације који деприоритизују суседе који систематски не учествују у прослеђивању.

ЕКСПЕРИМЕНТАЛНО ТЕСТИРАЊЕ И СТАТИСТИЧКА АНАЛИЗА

Сви експерименти спроведени су помоћу Python алата. Скрипта је преко IPC-а аутоматизовала четири експериментална сценарија (A, B, C, D) на симулираним мрежним топологијама (основна конфигурација обухватала је 50 чворова, уз могућност скалирања параметара), са по 5 понављања по сценарију ради статистичке поузданости. Тестиран је утицај фактора ширења ($k \in \{2,3,5\}$) и насумичног или циљаног искључивања чворова (0%−40%) на стопу успешне испоруке порука, као и на медијалну (p50) и 90. перцентилну (p90) латенцију конвергенције мреже.

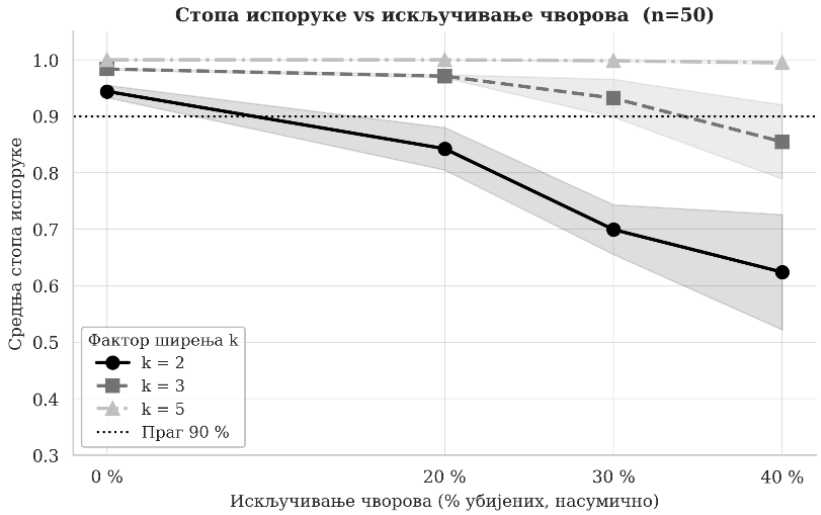
У експерименту E за доказивање отпорности на DPI, скрипта је ухватила 1000 стварних Nethr пакета у транспорту, односно са жице, између два покренута чвора. Ови пакети су упоређени са синтетички генерисаним узорцима стандардног саобраћаја (QUIC v1 и RTP/H.264) и идеалним насумичним шумом. Примењени су ригорозни статистички тестови, укључујући прорачун Шенонове ентропије, Пирсонову аутокорелацију, Колмогоров-Смирнов тест и Хи-квадрат тест униформности.

Тестирана хипотеза је да Nethr одржава стопу испоруке изнад 90% при губитку 40% чворова уз фактор ширења $k \geq 3$, и да је мрежни саобраћај статистички неразлучив од насумичног шума под свим примењеним тестовима.

РЕЗУЛТАТИ ИСТРАЖИВАЊА И ДИСКУСИЈА

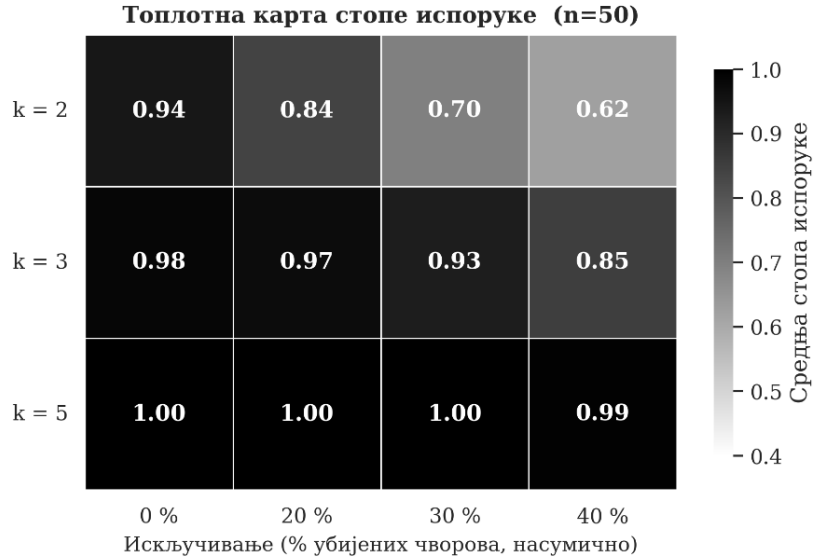
ОТПОРНОСТ МРЕЖЕ И ЛАТЕНЦИЈА ИСПОРУКЕ (ЕКСПЕРИМЕНТИ A, B, C И D)

Експерименти потврђују постављену хипотезу о поузданости протокола. Када је фактор ширења $k = 5$, резултати показују да је стопа испоруке 99% у мрежи од $N = 50$ чворова, чак и када 40% чворова нестане са мреже. Експеримент А (Слика 1) јасно илуструје ову динамику.



СЛИКА 1. Утицај насумичног отказивања чворова на стопу испоруке порука при различитим вредностима фактора ширења.

FIGURE 1. Impact of random node failure on message delivery rate at different spreading factor values.

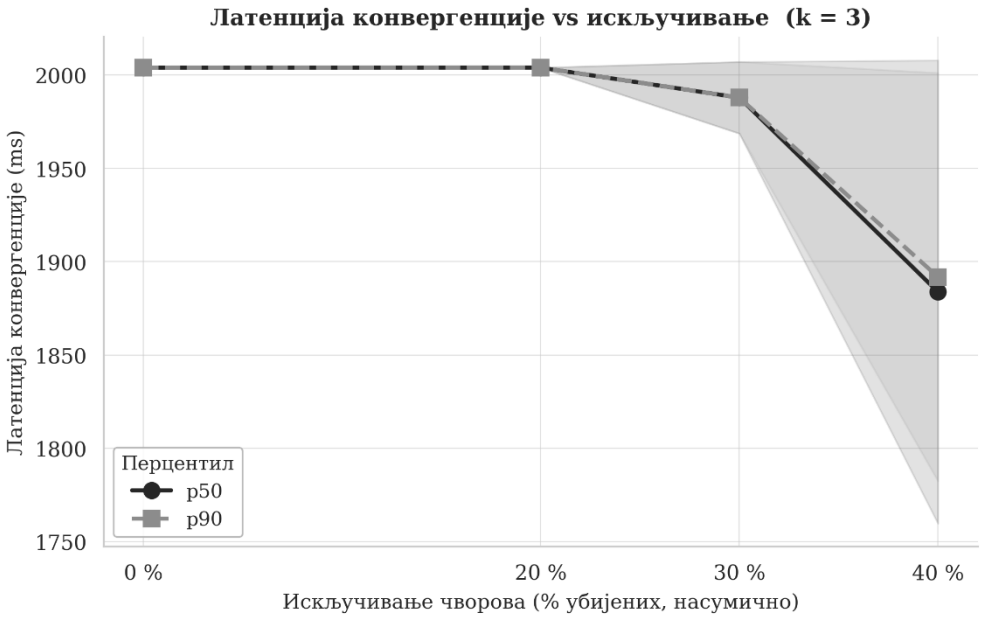


СЛИКА 2. Топлотна карта просечне стопе испоруке у функцији фактора ширења и насумичног отказивања чворова.

FIGURE 2. Heatmap of average delivery rate as a function of spreading factor and random node failure.

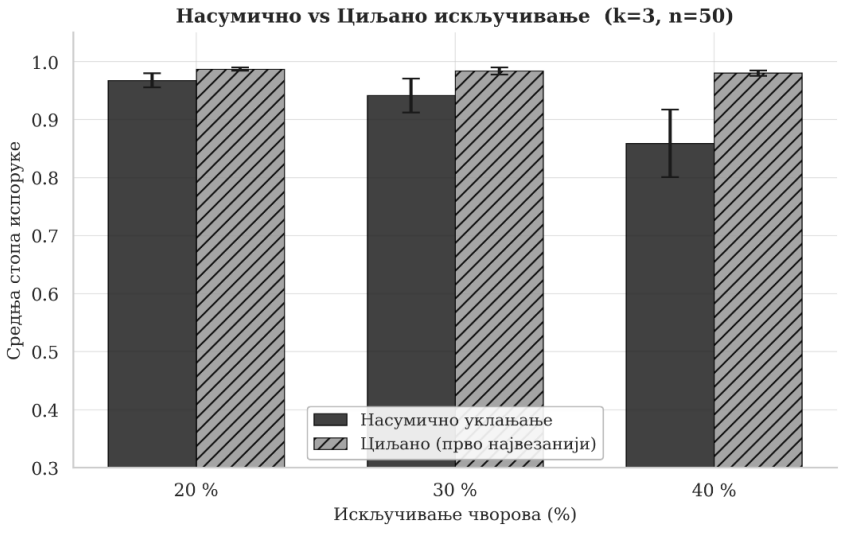
За фактор ширења k = 3, просечна стопа испоруке износи преко 90% чак и при губитку 30% мреже. Пад перформанси испод жељеног прага дешава се тек при k = 2 и губитку 30% чворова, што указује да k = 3 представља оптималан баланс између поузданости и избегавања загушења мреже (што додатно потврђује Експеримент D у идеалним условима, односно када мрежа има 0% искључивања), а k = 5 практично осигурава да ће пакет стићи.

У Експерименту B анализирана је брзина мреже. Резултати показују изузетну ефикасност симетричне пробне дешифрације.



СЛИКА 3. Латенција конвергенције мреже (p50 и p90 перцентил) у функцији отказивања чворова за k=3.
FIGURE 3. Network convergence latency (p50 and p90 percentiles) as a function of node failure for k=3.

Као што се види на Слици 3, чак и при отказу 40% чворова, медијално време конвергенције (p50) остаје изузетно ниско, док 90. перцентил (p90) бележи прихватљиве скокове. Експеримент C испитује најригорознији сценарио, разлику између насумичног испадања чворова и циљаног напада на кључна мрежна чворишта.



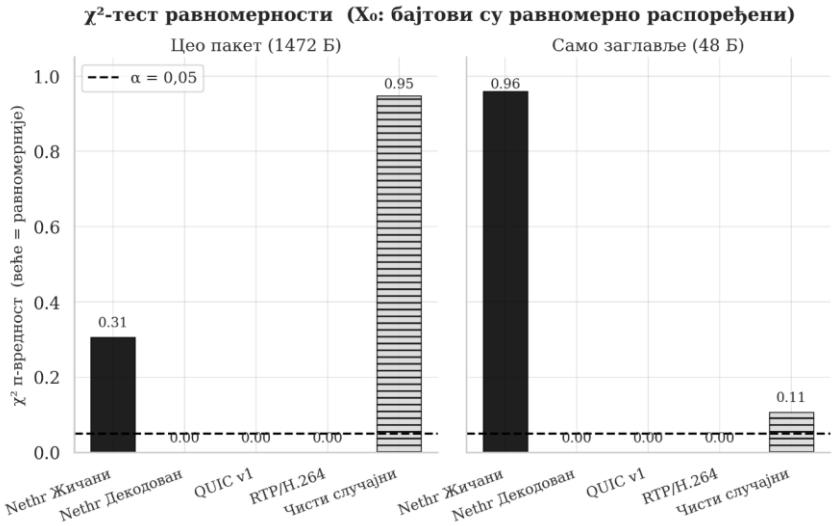
СЛИКА 4. Поређење успешности испоруке између насумичног и циљаног отказивања чворова (k = 3).
FIGURE 4. Comparison of delivery success between random and targeted node failure (k = 3).

Насумично искључивање чворова има већи негативан утицај на стопу испоруке од циљаног уклањања чворова са највећим бројем веза. Овај налаз наизглед противречи класичном перколационом моделу Barabási-Albert мрежа, које су теоријски критично рањиве на циљане нападе на чворишта.

Кључ за разумевање ове инверзије лежи у интеракцији топологије и епидемијског алгоритма са фиксним фактором ширења *k.* У стандардној мрежи, високо повезана чворишта (енгл. hubs) примају велики број порука, али због фиксног фактора прослеђују их само малом подскупу својих суседа. Чворишта тиме ефективно постају „уска грла“ (енгл. bottlenecks) која гуше епидемијско ширење на периферију мреже.

Када противник изврши циљани напад и елиминише ова чворишта, преостала мрежа постаје хомогенија и своди се на базичну прстенасту структуру где је просечан степен чвора близак фактору *k.* У оваквој хомогенизованој средини, епидемијско ширење ради готово оптимално, омогућавајући порукама да лако премосте мање празнине у графу. Насупрот томе, насумично искључивање чворова фрагментише прстен, али оставља део чворишта активним. Ова преостала чворишта настављају да неефикасно рутирају поруке преко фрагментисаног графа, што резултује већим падом испоруке. Овим је образложено да Nethr протокол, комбинујући хибридну топологију и ограничено ширење, успешно инвертује класичну рањивост скалабилних мрежа, чинећи систем најотпорнијим управо на најсофистицираније инфраструктурне нападе.

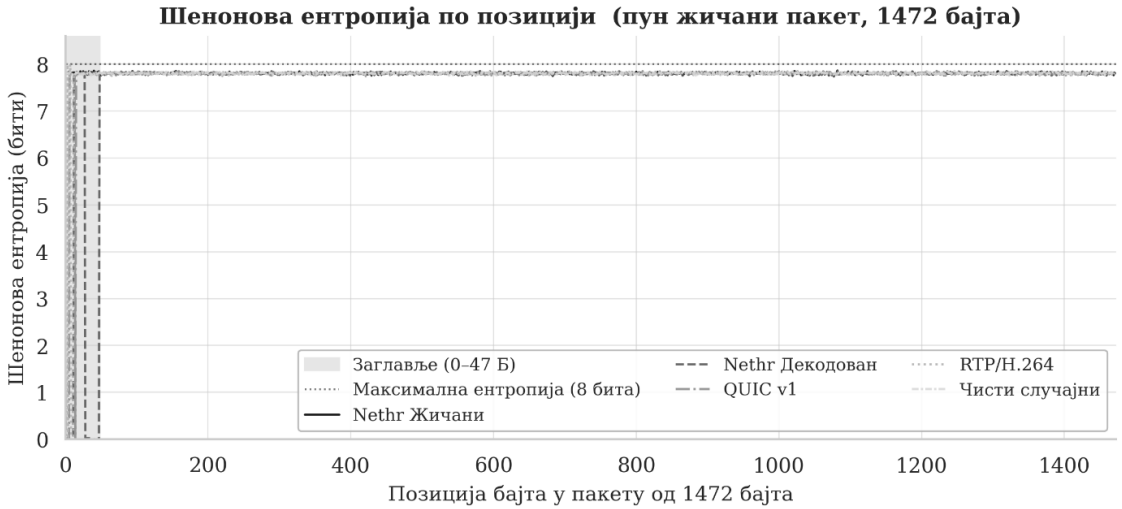
СТАТИСТИЧКА НЕВИДЉИВОСТ ПРОТОКОЛА И DPI ОТПОРНОСТ (ЕКСПЕРИМЕНТ Е)



СЛИКА 5. Хи-квадрат тест униформности комплетног пакета и заглавља у поређењу са другим протоколима.
FIGURE 5. Chi-square uniformity test of the full packet and header in comparison with other protocols.

Анализа Хи-квадрат теста (Слика 5) показује да је заглавље Nethr пакета на мрежи статистички идентично идеалном насумичном шуму (p-вредност ≈ 1,0). Са друге стране, индустријски стандарди попут QUIC и RTP протокола имају p-вредности блиске нули,

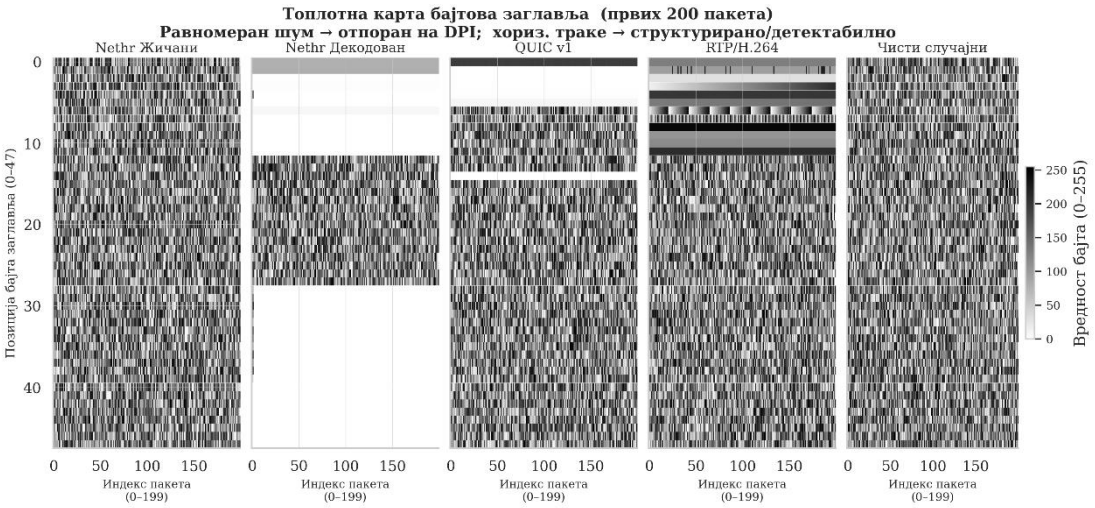
што их чини лаким метама за блокирање. Уколико бисмо анализирали "декодирани" Nethr пакет (пре примене заштитне XOR маске изведене из BLAKE3 хеша тела), његова дистрибуција би такође била лако препознатљива.



СЛИКА 6. Шенонова ентропија по позицији бајта у пакету (1472 бајта).
FIGURE 6. Shannon entropy per byte position in the packet (1472 bytes).

Коначна потврда добијена је мерењем Шенонове ентропије по позицији сваког бајта (Слика 6). Као што се очекује од модерне криптографије, сви шифровани протоколи (QUIC, RTP) постижу максималну ентропију од ~8 бита у телу пакета (након 48. бајта). Међутим, системи за дубоку инспекцију пакета (DPI) не анализирају тело, већ препознају протоколе тражећи статичне бајтове у заглављу. Док QUIC и RTP показују јасне, оштре падове ентропије у сивој зони заглавља (стварајући велику разлику ентропија заглавља и тела пакета, $\boldsymbol{\Delta} \gg 0$), Nethr на мрежи задржава савршену ентропију од ~8 бита дуж целог пакета, укључујући и заглавље ($\boldsymbol{\Delta} \approx 0$). Ови резултати недвосмислено доказују да иновативна метода маскирања заглавља потпуно елиминише све препознатљиве мрежне метаподатке, не остављајући DPI системима ниједан статичан бајт на основу којег би могли да класификују и блокирају саобраћај.

Коначни, и визуелно најупечатљивији доказ отпорности на системе за дубоку инспекцију пакета (DPI) приказан је помоћу топлотне карте вредности бајтова у заглављу (Слика 7). Анализирано је првих 48 бајтова (Y оса) кроз 200 узастопних пакета (X оса) за различите протоколе.



СЛИКА 7. Визуелна репрезентација вредности бајтова заглавља кроз 200 узастопних пакета.
FIGURE 7. Visual representation of header byte values across 200 consecutive packets.

ЗАКЉУЧАК

Протокол Nethr успешно решава проблем рањивости мрежа на инфраструктурне противнике пружајући свеобухватну заштиту садржаја и метаподатака. Комбинацијом ограниченог епидемијског рутирања у хибридним скалабилним топологијама са особинама "малог света" и брзе симетричне пробне дешифрације, постигнута је поуздана децентрализована комуникација. Главни допринос рада је вишеслојна статистичка невидљивост протокола: маскирањем заглавља хешом тела пакета и дедупликацијом без идентификатора, саобраћај постаје неразлучив од ентропије, чиме се елиминише могућност DPI филтрирања. Поред тога, увођењем механизма покривног саобраћаја базираног на насумичним динамичким интервалима, успешно су заштићени метаподаци о времену комуникације.

Значајан налаз експеримента C је да хибридна топологија инвертује класичну рањивост скалабилних мрежа: циљани напади на чворишта, уклањајући уска грла епидемијског ширења, имају мањи негативан учинак на испоруку порука од насумичног отказивања чворова.

Рад такође потврђује инхерентну отпорност ове врсте хибридне Barabási-Albert топологије на Sybil нападе, чиме се значајно сужава простор за инфилтрацију и анализу токова од стране малициозних актера. Све ово остварено је уз задржавање постквантне заштите и прихватљиве латенције на стандардном хардверу. Будућа истраживања биће усмерена на даље унапређење Sybil отпорности кроз увођење доказа рада (енгл. proof-of-work) и система репутације, као и на формалну анализу диференцијалне приватности, алтернативне методе рутирања и активна безбедносна тестирања.

ЛИТЕРАТУРА

1. Web документ: Access Now: Rising repression meets global resistance: Internet shutdowns in 2025, Access Now, #KeepItOn coalition, 2026. Скинуто 1. априла 2026. са сајта https://www.accessnow.org/wp-content/uploads/2026/03/KeepItOn-Internet-Shutdowns-2025-Annual-Report.pdf

2. Web документ: Freedom House: Freedom on the Net 2025: An Uncertain Future for the Global Internet, Freedom House, Washington D.C., 2025. Скинуто 1. априла 2026. са сајта https://freedomhouse.org/report/freedom-net/2025/uncertain-future-global-internet

3. Web документ: Zona Media: The 16-kilobyte curtain, Zona Media, 2025. Скинуто 1. априла 2026. са сајта https://en.zona.media/article/2025/06/19/cloudflare

4. R. Dingledine, N. Mathewson, P. Syverson, Tor: The Second-Generation Onion Router, Proc. 13th USENIX Security Symposium, San Diego, 2004.

5. Web документ: J. Warren: Bitmessage: A Peer-to-Peer Message Authentication and Delivery System, 2012. Скинуто 1. априла 2026. са сајта https://bitmessage.org/bitmessage.pdf

6. J. van den Hooff, D. Lazar, M. Zaharia, N. Zeldovich, Vuvuzela: Scalable Private Messaging Resistant to Traffic Analysis, Proc. 25th ACM SOSP, Monterey, 2015.

7. A. M. Piotrowska, J. Hayes, T. Elahi, S. Meiser, G. Danezis, The Loopix Anonymity System, Proc. 26th USENIX Security Symposium, Vancouver, 2017.

8. Web документ: A. Upadhyay: EFPIX: A zero-trust encrypted flood protocol for infrastructure-independent communication, arXiv, 2025. Скинуто 1. априла 2026. са сајта https://arxiv.org/abs/2509.08248

9. D. J. Bernstein, C. Chuengsatiansup, T. Lange, C. van Vredendaal, NTRU Prime: Reducing Attack Surface at Low Cost, Proc. Selected Areas in Cryptography (SAC), 2017.

10. Web документ: T. Perrin: The Noise Protocol Framework, noiseprotocol.org, 2018. Скинуто 1. априла 2026. са сајта https://noiseprotocol.org/noise.html

11. Web документ: The Open Quantum Safe Project: liboqs 0.15.0, Open Quantum Safe, 2025. Скинуто 1. априла 2026. са сајта https://github.com/open-quantum-safe/liboqs/releases/tag/0.15.0

12. Web документ: F. Denis: libsodium Documentation, version 1.0.21, libsodium, 2026. Скинуто 1. априла 2026. са сајта https://doc.libsodium.org

13. P. Rogaway, Authenticated-Encryption with Associated-Data, Proc. ACM CCS, 2002.