УНИВЕРЗИТЕТ „СВ. КИРИЛ И МЕТОДИЈ“ - СКОПЈЕ

Факултет за електротехника и информациски технологии

Институт за телекомуникации

м-р Гоце Стеваноски

РАМКА БАЗИРАНА НА ДЛАБОКО УЧЕЊЕ ЗА АДАПТИВНА ОПТИМИЗАЦИЈА НА РЕСУРСИ И ОТКРИВАЊЕ НАПАДИ КАЈ СИСТЕМИ ЗА ДЕТЕКЦИЈА НА УПАДИ

ДОКТОРСКА ДИСЕРТАЦИЈА

Скопје, 2026 година

Докторанд

ГОЦЕ СТЕВАНОСКИ

Тема

РАМКА БАЗИРАНА НА ДЛАБОКО УЧЕЊЕ ЗА АДАПТИВНА ОПТИМИЗАЦИЈА НА РЕСУРСИ И ОТКРИВАЊЕ НАПАДИ КАЈ СИСТЕМИ ЗА ДЕТЕКЦИЈА НА УПАДИ

Ментор

проф. д-р АЛЕКСАНДАР РИСТЕСКИ
Универзитет „Св. Кирил и Методиј“ во Скопје
Факултет за електротехника и информациски технологии

Комисија за одбрана

проф. д-р МАРКО ПОРЈАЗОСКИ, претседател
Универзитет „Св. Кирил и Методиј“ во Скопје
Факултет за електротехника и информациски технологии

проф. д-р АЛЕКСАНДАР РИСТЕСКИ, ментор
Универзитет „Св. Кирил и Методиј“ во Скопје
Факултет за електротехника и информациски технологии

проф. д-р ВАЛЕНТИН РАКОВИЌ, член
Универзитет „Св. Кирил и Методиј“ во Скопје
Факултет за електротехника и информациски технологии

проф. д-р ТОМИСЛАВ ШУМИНОСКИ, член
Универзитет „Св. Кирил и Методиј“ во Скопје
Факултет за електротехника и информациски технологии

проф. д-р Ќ̀ИРЕ ЈАЌИМОСКИ, член
Универзитет „Гоце Делчев“ во Штип
Воена Академија „Генерал Михаило Апостолски“ Скопје – придружна членка

Лектор

ВАЛЕНТИНА ВЕЛИКОВА (Уверение бр.27-123/6)

Научна област

Електротехника и информациски технологии

Датум на одбрана

3.7.2026 година

м-р Гоце Стеваноски

РАМКА БАЗИРАНА НА ДЛАБОКО УЧЕЊЕ ЗА АДАПТИВНА ОПТИМИЗАЦИЈА НА РЕСУРСИ И ОТКРИВАЊЕ НАПАДИ КАЈ СИСТЕМИ ЗА ДЕТЕКЦИЈА НА УПАДИ

– А п с т р а к т –

Оваа докторска дисертација обработува интегриран пристап за детекција на малициозен мрежен сообраќај и адаптивна оптимизација на ресурсите кај системите за детекција на упади во современи, динамични и ресурсно ограничени информациски околини. Истражувањето поаѓа од предизвикот дека класичните системи за детекција на упади, базирани на потписи и статички правила, имаат ограничена способност за препознавање нови и еволутивни закани, додека напредните модели, базирани на длабоко учење, често бараат значајни пресметковни ресурси. Поради тоа, во дисертацијата се разгледува потребата од интелигентни, адаптивни и ресурсно свесни механизми кои можат да го одржат квалитетот на детекција при променливи услови на мрежниот сообраќај и ограничена достапност на ресурси.

Истражувањето е поставено како повеќеслојна рамка која ги поврзува организациските, експерименталните и техничките аспекти на сајбер-безбедноста. Најнапред се анализира сајбер-безбедносната подготвеност на малите организации преку таксономија за проценка на сајбер-безбедносна подготвеност и ризик, со цел да се утврди односот помеѓу перцепцијата на ризик и реалното ниво на имплементирани безбедносни мерки. Потоа се дизајнира и имплементира тестна информациско-технолошка околина базирана на интегриран центар за мрежни операции и центар за безбедносни операции, со примена на алатки со отворен код, која овозможува прибирање, мониторинг и анализа на мрежен сообраќај, логови и безбедносни настани во контролирани услови.

Во техничкиот дел од дисертацијата се евалуира автоенкодерски модел чувствителен на реконструкциска загуба за детекција на аномалии во мрежниот сообраќај. Моделот се обучува врз легитимен сообраќај, а реконструкциската загуба се користи како индикатор за разграничување помеѓу нормалното и малициозното однесување. Во рамките на предложениот повеќеслоен пристап, овој модел се третира како применлив сегмент на безбедносната инфраструктура во ресурсно ограничени средини, каде што може да има улога на ран аналитички слој за груба селекција на нормален и нестандарден, односно потенцијално малициозен сообраќај. На тој начин, автоенкодерскиот пристап може да придонесе кон намалување на товарот врз подоцнежните нивоа на безбедносната инфраструктура, преку насочување на посложената анализа кон сообраќајот што покажува отстапување од научениот образец на нормално однесување.

Главниот научен придонес на дисертацијата е предложената двостепена Парето-водена рамка за адаптивна оптимизација на ресурси кај лесни системи за детекција на упади, именувана како A2DAPT. Рамката претставува нов интегриран пристап кој комбинира офлајн повеќекритериумска оптимизација и онлајн адаптација базирана на длабоко засилено учење. Во првата фаза, конфигурацијата на системот за детекција на упади се формализира како повеќекритериумски оптимизациски проблем, при што се генерира множество Парето-ефикасни конфигурации кои го претставуваат компромисот помеѓу

квалитетот на детекција и потрошувачката на процесорските, мемориските и мрежните ресурси. Во втората фаза, адаптивниот контролер, базиран на длабоко засилено учење, врши динамички избор на соодветна конфигурација во зависност од тековната состојба на мрежниот сообраќај и достапните ресурсни ограничувања.

Резултатите од истражувањето покажуваат дека предложениот пристап овозможува систематско моделирање на компромисот помеѓу безбедносните перформанси и ресурсната ефикасност, како и адаптивно управување со конфигурациите на системите за детекција на упади во нестационарни услови. Експерименталната евалуација на A2DAPT потврдува дека комбинацијата од Парето-ефикасниот простор на конфигурации и онлајн адаптацијата базирана на длабоко засилено учење овозможува поефикасно користење на ресурсите во споредба со статичката конфигурација. Целосната A2DAPT-рамка постигнува најниска кумулативна потрошувачка на процесорски ресурси, меморија и мрежен пропусен опсег, при што бројот на прекршувања на ресурсниот буџет се намалува од 100 на 69 во споредба со статичката конфигурација. Иако одредени алтернативни варијанти постигнуваат повисока просечна детекциска вредност, тие го прават тоа по цена на поголема потрошувачка на ресурси и почести прекршувања на ограничувањата, што ја потврдува предноста на A2DAPT како стабилен и ресурсно свесен пристап за адаптивна конфигурација на системи за детекција на упади. Со интегрирање на организациската анализа, контролираната тестна околина, ненадгледуваното длабоко учење, повеќекритериумската оптимизација и длабокото засилено учење, дисертацијата придонесува кон развој на интелигентни, применливи и ресурсно свесни сајбер-безбедносни решенија за современите информациски и комуникациски инфраструктури.

Клучни зборови: системи за детекција на упади; длабоко учење; автоенкодер; детекција на аномалии; повеќекритериумска оптимизација; Парето-ефикасност; длабоко засилено учење; адаптивна оптимизација на ресурси; A2DAPT; сајбер-безбедносна подготвеност; CyPRisT; тестна околина; интегриран центар за мрежни операции и центар за безбедносни операции.

Goce Stevanoski, M.Sc.

A DEEP LEARNING-BASED FRAMEWORK FOR ADAPTIVE RESOURCE OPTIMIZATION AND ATTACK DISCOVERY IN INTRUSION DETECTION SYSTEMS

– A b s t r a c t –

This doctoral dissertation addresses an integrated approach to malicious network traffic detection and adaptive resource optimization in intrusion detection systems within contemporary, dynamic, and resource-constrained information environments. The research is motivated by the challenge that conventional intrusion detection systems, based on signatures and static rules, have limited capability to recognize new and evolving threats, while advanced deep-learning-based models often require substantial computational resources. Accordingly, the dissertation examines the need for intelligent, adaptive, and resource-aware mechanisms capable of maintaining detection quality under changing network traffic conditions and limited resource availability.

The research is structured as a multilayered framework that connects the organizational, experimental, and technical aspects of cybersecurity. First, the cybersecurity preparedness of small organizations is analyzed by applying a taxonomy for cybersecurity preparedness and risk assessment, with the aim of examining the relationship between risk perception and the actual level of implemented security measures. Then, an information technology testbed is designed and implemented, based on an integrated network operations center and security operations center using open-source tools. This testbed enables the collection, monitoring, and analysis of network traffic, logs, and security events under controlled conditions.

In the technical part of the dissertation, a reconstruction-loss-sensitive autoencoder model is evaluated for anomaly detection in network traffic. The model is trained on legitimate traffic, while reconstruction loss is used as an indicator for distinguishing between normal and malicious behavior. Within the proposed multilayered approach, this model is treated as an applicable segment of the security infrastructure in resource-constrained environments, where it can serve as an early analytical layer for coarse filtering of normal and non-standard, that is, potentially anomalous traffic. In this way, the autoencoder-based approach may contribute to reducing the load on later layers of the security infrastructure by directing more complex analysis toward traffic that deviates from the learned pattern of normal behavior.

The main scientific contribution of the dissertation is the proposed two-stage Pareto-driven framework for adaptive resource optimization in lightweight intrusion detection systems, named A2DAPT. The framework represents a novel integrated approach that combines offline multi-objective optimization with online adaptation based on deep reinforcement learning. In the first stage, the configuration of the intrusion detection system is formalized as a multi-objective optimization problem, generating a set of Pareto-efficient configurations that represent the trade-off between detection quality and the consumption of processing, memory, and network resources. In the second stage, an adaptive controller based on deep reinforcement learning dynamically selects an appropriate configuration according to the current state of network traffic and the available resource constraints.

The research results show that the proposed approach enables systematic modeling of the trade-off between security performance and resource efficiency, as well as adaptive management of intrusion detection system configurations under non-stationary conditions. The experimental evaluation of A2DAPT confirms that the combination of a Pareto-efficient configuration space and online adaptation based on deep reinforcement learning enables more efficient resource utilization compared with a static configuration. The complete A2DAPT framework achieves the lowest cumulative consumption of processing resources, memory, and network bandwidth, while reducing the number of resource budget violations from 100 to 69 compared with the static configuration. Although certain alternative variants achieve a higher average detection score, they do so at the cost of greater resource consumption and more frequent constraint violations, confirming the advantage of A2DAPT as a stable and resource-aware approach for adaptive configuration of intrusion detection systems. By integrating organizational analysis, a controlled testbed, unsupervised deep learning, multi-objective optimization, and deep reinforcement learning, the dissertation contributes to the development of intelligent, applicable, and resource-aware cybersecurity solutions for contemporary information and communication infrastructures.

Keywords: intrusion detection systems; deep learning; autoencoder; anomaly detection; multi-objective optimization; Pareto efficiency; deep reinforcement learning; adaptive resource optimization; A2DAPT; cybersecurity preparedness; CyPRisT; testbed; integrated network operations center and security operations center.

Изразувам искрена благодарност до мојот ментор за стручната поддршка и насоките во текот на изработката на оваа докторска дисертација.
Посебна благодарност до моето семејство за разбирањето и постојаната безрезервна поддршка, без кои ова достигнување немаше да биде возможно.

Изјавувам дека оваа докторска дисертација ја изработив самостојно, дека уредно ги цитирам сите користени извори и литература и дека дисертацијата не е користена во рамките на други универзитетски студии или за стекнување на друго звање.

Потпис на авторот, с.р.

Изјавувам дека електронската верзија на оваа докторска дисертација е идентична со отпечатената верзија на докторската дисертација.

Потпис на авторот, с.р.

СОДРЖИНА

ЛИСТА НА СЛИКИ

ЛИСТА НА ТАБЕЛИ

ЛИСТА НА СКРАТЕНИЦИ

A2DAPT (A Two-Stage Pareto-Driven Framework for Adaptive Resource Optimization in Lightweight Intrusion Detection Systems)

AD (Active Directory)

AD DS (Active Directory Domain Services)

AI (Artificial Intelligence)

ANN (Artificial Neural Networks)

BP (Backpropagation)

BW (Bandwidth)

CICFlowMeter (CIC Flow Meter)

CICIDS2017 (Canadian Institute for Cybersecurity Intrusion Detection System 2017)

CPS (Cybersecurity Preparedness Score)

CPU (Central Processing Unit)

CyPRisT (Cybersecurity Preparedness-Risk Taxonomy)

D3QN (Dueling Double Deep Q-Network)

DC (Domain Controller)

DDoS (Distributed Denial of Service)

DDQN (Double Deep Q-Network)

DHCP (Dynamic Host Configuration Protocol)

DL (Deep Learning)

DMPRCA (Decision Makers' Perceived Risk of Cyber-Attack Score)

DNN (Deep Neural Network)

DoS (Denial of Service)

DQN (Deep Q-Network)

DRL (Deep Reinforcement Learning)

DSRM (Design Science Research Methodology)

DSL (Data Source Layer)

EDR (Endpoint Detection and Response)

ENISA (European Union Agency for Cybersecurity)

EU (European Union)

FCAPS (Fault, Configuration, Accounting, Performance and Security)

H0 (Null Hypothesis)

HIL (Hardware-in-the-Loop)

HTTP (Hypertext Transfer Protocol)

ICS (Industrial Control System)

IDS (Intrusion Detection System)

IGA-BP (Improved Genetic Algorithm Backpropagation)

IoT (Internet of Things)

IP (Internet Protocol)

IPS (Intrusion Prevention System)

IT (Information Technology)

JSON (JavaScript Object Notation)

KDD Cup 99 (Knowledge Discovery in Databases Cup 1999)

LMS (Log Management System)

LSTM (Long Short-Term Memory)

MAE (Mean Absolute Error)

MDP (Markov Decision Process)

MEM (Memory)

MK (Republic of Macedonia)

ML (Machine Learning)

MLP (Multi-Layer Perceptron)

MOO (Multi-Objective Optimization)

MSE (Mean Squared Error)

NAT (Network Address Translation)

NIST (National Institute of Standards and Technology)

NOC (Network Operations Center)

NoSQL (Not Only SQL)

NPAS (Network Policy and Access Services)

NS-2 (Network Simulator 2)

NSGA (Non-dominated Sorting Genetic Algorithm)

NSGA-II (Non-dominated Sorting Genetic Algorithm II)

NSL-KDD (Network Security Laboratory Knowledge Discovery in Databases)

NSM (Network Security Monitor)

OPNET (Optimized Network Engineering Tool)

PCA (Principal Component Analysis)

PER (Prioritized Experience Replay)

Q1 (Quadrant 1)

Q2 (Quadrant 2)

Q3 (Quadrant 3)

Q4 (Quadrant 4)

R2 (Coefficient of Determination)

ReLU (Rectified Linear Unit)

RL (Reinforcement Learning)

RMSE (Root Mean Squared Error)

SA (Situational Awareness)

SCAE (Stacked Contractive Autoencoder)

SIEM (Security Information and Event Management)

SL (Shallow Learning)

SML (Service Management Layer)

SMEs (Small and Medium-sized Enterprises)

SMTP (Simple Mail Transfer Protocol)

SOC (Security Operations Center)

SQL (Structured Query Language)

SSL (Secure Sockets Layer)

SVM (Support Vector Machine)

SWISH (Sigmoid-Weighted Linear Unit)

SyML (System Management Layer)

SYN (Synchronize)

TD (Temporal Difference)

TLS (Transport Layer Security)

UID (Unique Identifier)

US (United States)

VM (Virtual Machine)

WinSRV2022 (Windows Server 2022)

XDR (Extended Detection and Response)

1. Вовед

Современите информациски системи доживуваат интензивна трансформација поттикната од развојот на Интернет на нештата (анг. Internet of Things – IoT), рабната инфраструктура (анг. edge infrastructure) и облак-сервиси (анг. cloud services)[1][2]. Овие технологии овозможуваат висока скалабилност, динамичка распределба на ресурси и поддршка на голем број хетерогени уреди, но истовремено ја зголемуваат комплексноста на системите и нивната изложеност на сајбер-закани[3]. Со растот на мрежниот сообраќај и бројот на поврзани уреди, класичните безбедносни механизми стануваат сè помалку доволни за справување со современите закани, што ја нагласува потребата од напредни, интелигентни и адаптивни решенија.

Покрај техничките аспекти, современите пристапи во сајбер-безбедноста сè повеќе го нагласуваат значењето на социотехничките фактори, особено организациската подготвеност и перцепцијата на ризик [4][5]. Во оваа дисертација, таксономијата за проценка на сајбер-безбедносната подготвеност и ризик (анг. Cybersecurity Preparedness-Risk Taxonomy – CyPRisT) се користи како концептуална рамка за анализа на сајбер безбедносната поставеност кај малите организации [6]. Преку класификација според перципираниот ризик и реалното ниво на безбедносна подготвеност, CyPRisT овозможува согледување на јазот помеѓу техничките можности и практичната примена на безбедносните механизми, како и поставување на системите за откривање (детекција) на упади (анг. Intrusion Detection Systems – IDS) во соодветен организациски и ресурсен контекст.

Системите за детекција на упади претставуваат основен механизам за идентификација на малициозен сообраќај и заштита на мрежната инфраструктура [7]. Традиционалните IDS-решенија, базирани на потписи (анг. signature-based) и правила (анг. rule-based), се ефикасни при детекција на познати напади, но имаат ограничена способност за идентификација на нови, непознати и еволутивни закани [8]. Дополнително, овие системи се тешко приспособливи на динамични и дистрибуирани околини, во кои карактеристиките на мрежниот сообраќај се менуваат во реално време.

Во овој контекст, техниките од машинско учење (анг. Machine Learning – ML) се наметнуваат како значаен пристап за анализа на мрежниот сообраќај. Преку ML се овозможува учење обрасци од историски податоци и нивна примена врз нови податоци. Надгледуваните методи може да постигнат висока точност, но нивната зависност од означени податоци ја ограничува применливоста во реални сценарија, каде што новите напади не се секогаш однапред познати [9][10]. Како надградба на класичните ML-техники, длабокото учење (анг. Deep Learning – DL) овозможува учење сложени нелинеарни репрезентации преку повеќеслојни невронски мрежи [11]. Особено значајни во овој контекст се автоенкодерите, кои како ненадгледувани модели може да се користат за детекција на аномалии преку учење на репрезентацијата на нормалниот сообраќај [12]. Аномалиите се идентификуваат врз основа на реконструкциската загуба, односно разликата помеѓу влезните и реконструираните податоци, што овозможува примена за детекција на непознати и *zero-day* напади [13].

Во оваа дисертација се евалуира автоенкодерскиот модел чувствителен на загуба, при што реконструкциската загуба се користи како индикатор за разграничување помеѓу нормален и невообичаен мрежен сообраќај, што би ги потенцирало аномалиите во

структурата на мрежниот сообраќај. Со ваквиот пристап се овозможува препознавање и анализа на сообраќај кој може да биде малициозен без директна зависност од целосно означени податоци и се поставува основа за понатамошна интеграција со IDS-механизми базирани на машинско и длабоко учење.

Сепак, примената на DL-моделите во IDS воведува нови предизвици. Високата пресметковна сложеност и потребата од значајни ресурси ја ограничуваат нивната применливост во ресурсно ограничени средини, како IoT и edge системите [14][15][16]. Дополнително, перформансите на IDS зависат од нивната конфигурација, која може да вклучува избор на параметри, праг за детекција, стапка на семплирање, длабочина на инспекција и други оперативни поставки [17]. Овој проблем природно може да се формулира како повеќекритериумски оптимизациски проблем (анг. Multi-Objective Optimization – MOO) [18], каде што треба да се постигне рамнотежа помеѓу квалитетот на детекција и потрошувачката на ресурси.

Повеќекритериумската оптимизација овозможува истовремено разгледување на повеќе конфликтни цели. Во оваа дисертација се обработува генетскиот алгоритам со недоминирачко сортирање II (анг. Non-dominated Sorting Genetic Algorithm II – NSGA-II)[19], кој овозможува генерирање Парето-ефикасни решенија што го претставуваат компромисот помеѓу различни конфликтни цели. Во контекст на IDS, ова значи избор на конфигурации кои обезбедуваат прифатлив однос помеѓу квалитетот на детекција и ресурсната ефикасност.

Во рамките на ова истражување, повеќекритериумската оптимизација базирана на NSGA-II се користи за офлајн генерирање на Парето-ефикасни IDS-конфигурации, при што се разгледува компромисот помеѓу квалитетот на детекција и потрошувачката на ресурси, како процесорско време, меморија и мрежен пропусен опсег. Овие конфигурации претставуваат основа за понатамошна адаптација на системот преку нивен избор во нестационарни услови на мрежен сообраќај.

Во реалните системи, условите се менуваат континуирано, што бара адаптивни механизми за донесување одлуки. Во таа насока, засиленото учење (анг. Reinforcement Learning – RL) се користи за моделирање проблеми во кои агентот учи стратегија преку интеракција со околината [20]. Кај сложените мрежни околини, каде што просторот на состојби и акции може да биде голем, особено значајно е длабокото засилено учење (анг. Deep Reinforcement Learning – DRL), кое комбинира засилено учење со длабоки невронски мрежи [21]. Во оваа дисертација се разгледуваат механизми базирани на длабоки Q-мрежи (анг. Deep Q-Network), вклучувајќи двојни дупли длабоки Q-мрежи (анг. Dueling Double Deep Q-Network - D3QN) [22][23] со приоритизирано повторување на искуства (анг. Prioritized Experience Replay – PER) [24], кои овозможуваат поефикасно учење политики за избор на конфигурации во услови на динамичен мрежен сообраќај.

Во рамките на ова истражување, D3QN со PER се користи за динамичко избирање и адаптација на IDS-конфигурации во реално време, врз основа на тековната состојба на системот, карактеристиките на мрежниот сообраќај и достапните ресурси. На овој начин се овозможува континуирана оптимизација на IDS, со цел одржување висок квалитет на детекција при контролираната потрошувачка на ресурси.

Иако постојат бројни истражувања кои ја разгледуваат примената на DL за детекција на упади, употребата на оптимизациски техники за подобрување на конфигурациите и примената на RL за адаптивно управување, најголемиот дел од овие пристапи ги третираат овие аспекти изолирано [8][9]. Поради тоа, постои потреба од интегриран пристап кој истовремено овозможува: ненадгледувана детекција на аномалии, повеќекритериумска оптимизација на IDS-конфигурации и адаптација во реално време преку длабоко засилено учење. Оваа празнина е особено изразена во ресурсно ограничените и нестационарни околини, каде што е неопходно да се постигне баланс помеѓу безбедноста и ефикасноста.

Поради наведеното, во оваа докторска дисертација се предлага интегриран пристап кој комбинира техники од ненадгледувано длабоко учење, повеќекритериумска оптимизација и длабоко засилено учење, со цел развој на адаптивни и ресурсно свесни IDS-механизми. Предложениот пристап овозможува поврзување на организацискиот контекст на сајбер-безбедносната подготвеност со технички решенија за детекција на аномалии и динамичка адаптација на IDS-конфигурации. Со тоа, дисертацијата придонесува кон развој на интелигентни, адаптивни и ресурсно ефикасни решенија применливи во современите информациски и комуникациски околини.

1.1. Цели и мотив на истражувањето

Мотивот за ова истражување произлегува од повеќе значајни предизвици поврзани со сајбер-безбедноста на современите организации и мрежни инфраструктури. Класичните IDS имаат ограничена способност за препознавање нови и претходно непознати типови напади, особено во услови на нестационарен и хетероген мрежен сообраќај. Од друга страна, напредните модели базирани на длабоко учење овозможуваат подлабинска анализа на комплексни податоци, но нивната примена е често ограничена поради високата пресметковна сложеност и потребата од значајни ресурси. Овој проблем е особено изразен во IoT, edge и други ресурсно ограничени околини.

Дополнителен предизвик претставува фактот што голем дел од постојните пристапи за конфигурација и оптимизација на IDS се статички и не ја земаат предвид динамиката на мрежниот сообраќај. Како резултат на тоа, една фиксна конфигурација може да биде неефикасна при ниско оптоварување или недоволно ефективна при нагли промени во сообраќајот и појава на малициозни активности. Поради тоа, постои потреба од адаптивни и ресурсно свесни IDS-механизми кои можат динамички да го балансираат квалитетот на детекција и потрошувачката на ресурси.

Покрај техничките предизвици, значаен мотив за ова истражување е и потребата од подобро разбирање на организациските и социотехничките фактори кои влијаат врз сајбер безбедносната подготвеност. Особено кај малите организации, перцепцијата на ризик, достапните ресурси, организацискаата зрелост и практичната примена на безбедносните мерки можат значајно да влијаат врз ефективноста на техничките решенија. Затоа, оваа дисертација не се ограничува само на развој на техничките механизми за детекција и адаптација, туку ги разгледува и организациските предуслови за нивна примена.

Главната цел на ова истражување е развој и евалуација на адаптивна и ресурсно свесна рамка за оптимизација на IDS-конфигурации во услови на нестационарен мрежен сообраќај и ограничени ресурси. Во таа насока, дисертацијата ја формализира конфигурацијата на IDS како повеќекритериумски оптимизациски проблем, при што се

разгледува компромисот помеѓу квалитетот на детекција и потрошувачката на ресурси. За офлајн генерирање на Парето-ефикасни IDS-конфигурации се применува NSGA-II, додека за нивен динамички избор во реално време се развива адаптивен контролер базиран на длабоко засилено учење, односно D3QN со PER. Со ова се овозможува ресурсно свесна адаптација на IDS врз основа на тековната состојба на системот, карактеристиките на мрежниот сообраќај и достапните ресурси.

Втората цел е евалуација на модел базиран на ненадгледувано длабоко учење, односно автоенкодер, за детекција на аномалии во мрежниот сообраќај. Во оваа поставеност, автоенкодерот учи репрезентација на легитимен мрежен сообраќај, а реконструкциската загуба се користи како индикатор за отстапување од нормалното однесување. На тој начин се овозможува разграничување помеѓу легитимниот и малициозниот сообраќај, без директна зависност од целосно означени податоци.

Третата цел е дизајн и имплементација на тестна ИТ-околина (анг. testbed), која овозможува прибирање, следење и анализа на мрежен сообраќај во контролирани услови. Предложената тестна околина обезбедува основа за практична евалуација на адаптивната рамка за оптимизација и автоенкодерскиот модел за детекција на аномалии. Дополнително, таа овозможува прибирање логови, мрежни податоци и системски настани, како и анализа на ограничувањата и применливоста на испитуваните модели во реалистични сценарија.

Четвртата цел е квантитативна анализа на сајбер безбедносната поставеност кај малите организации преку примена на CyPRisT. Во овој контекст, CyPRisT се користи како структуриран модел за проценка на различни аспекти на сајбер-безбедноста, вклучувајќи технички, организациски и човечки фактори. Истражувањето се фокусира на утврдување на релацијата помеѓу перцепцијата на ризик кај носителите на одлуки и реалното ниво на сајбер безбедносната подготвеност, со цел да се идентификуваат потенцијалните јазови кои можат да влијаат врз ефективноста на применетите безбедносни мерки.

Очекуваниот резултат од истражувањето е развој на методолошка и техничка рамка која овозможува поефективно користење на ограничените ресурси, при истовремено задржување на соодветен квалитет на детекција. Со вака дефинираниот пристап, дисертацијата дава мултидисциплинарен придонес во областа на сајбер-безбедноста, преку поврзување на ресурсно свесна оптимизација на IDS, ненадгледувано длабоко учење, тестни околини и социотехничка анализа. Ваквиот пристап е особено релевантен за организации и мрежни средини со ограничени ресурси, каде што е неопходно да се постигне баланс помеѓу безбедноста, ефикасноста и практичната применливост.

1.2. Образложување на работните хипотези

Во оваа дисертација, како главна истражувачка хипотеза се поставува следното:

Интегрирањето на организациската анализа на сајбер-безбедносната подготвеност, контролираната тестна информациско-технолошка околина, ненадгледуваната детекција на аномалии и двостепената Парето-водена адаптивна оптимизација на ресурси овозможува развој на сеопфатен, применлив и ресурсно свесен пристап за унапредување на системите за детекција на упади во динамички и ресурсно ограничени мрежни средини.

Од главната хипотеза произлегуваат следните посебни хипотези:

Прва посебна теза

Систематската анализа на сајбер-безбедносната подготвеност на малите организации преку таксономијата за проценка на сајбер-безбедносната подготвеност и ризик овозможува идентификација на односот помеѓу перцепцијата на ризик, реалното ниво на имплементираните безбедносни мерки и организациските предуслови за примена на технички безбедносни решенија. На овој начин се обезбедува социотехнички контекст за понатамошното разгледување на применливоста на адаптивни и ресурсно свесни механизми за заштита.

Втора посебна теза

Дизајнот и имплементацијата на контролирана тестна информациско-технолошка околина, базирана на интегриран центар за мрежни операции и центар за безбедносни операции со примена на алатки со отворен код, овозможува прибирање, следење и анализа на мрежен сообраќај, системски логови и безбедносни настани потребни за експериментална евалуација на предложените безбедносни механизми. Ваквата околина претставува експериментална основа која го поврзува организацискиот контекст со техничката проверка на моделите за детекција, анализа и адаптивна оптимизација.

Трета посебна теза

Ненадгледуваните модели базирани на автоенкодери овозможуваат детекција на аномалии во мрежниот сообраќај преку анализа на реконструкциската загуба, без директна зависност од целосно означени податоци. Во рамките на повеќеслојната безбедносна инфраструктура, ваквиот пристап може да се користи како ран аналитички сегмент за груба селекција на нормален и нестандарден сообраќај, со што може да се поддржи поефикасното насочување на подоцнежните и посложени безбедносни механизми во ресурсно ограничените средини.

Четврта посебна теза

Формулирањето на конфигурацијата на системите за детекција на упади како повеќекритериумски оптимизациски проблем овозможува добивање Парето-ефикасни конфигурации преку кои се моделира компромисот помеѓу квалитетот на детекција и потрошувачката на ресурси. Комбинирањето на овие конфигурации со онлајн адаптацијата базирана на длабоко засилено учење, како што е предложено во A2DAPT-рамката, овозможува динамички избор на соодветна конфигурација во зависност од тековната состојба на мрежниот сообраќај и достапните ресурсни ограничувања.

Вака поставените хипотези ја следат логиката на истражувањето како повеќеслоен процес. Првата хипотеза го дефинира организацискиот и социотехничкиот контекст, втората ја воспоставува експерименталната основа за прибирање и анализа на податоци, третата ја разгледува примената на ненадгледуваното длабоко учење како сегмент за рана детекција на аномалии, додека четвртата ја формализира и евалуира главната техничка новина на дисертацијата преку A2DAPT-рамката. Заедно, овие хипотези ја поддржуваат главната хипотеза дека интегрираниот пристап може да придонесе кон развој на адаптивни,

применливи и ресурсно свесни системи за детекција на упади во динамички и ресурсно ограничени мрежни средини.

1.3. Користени научни методи

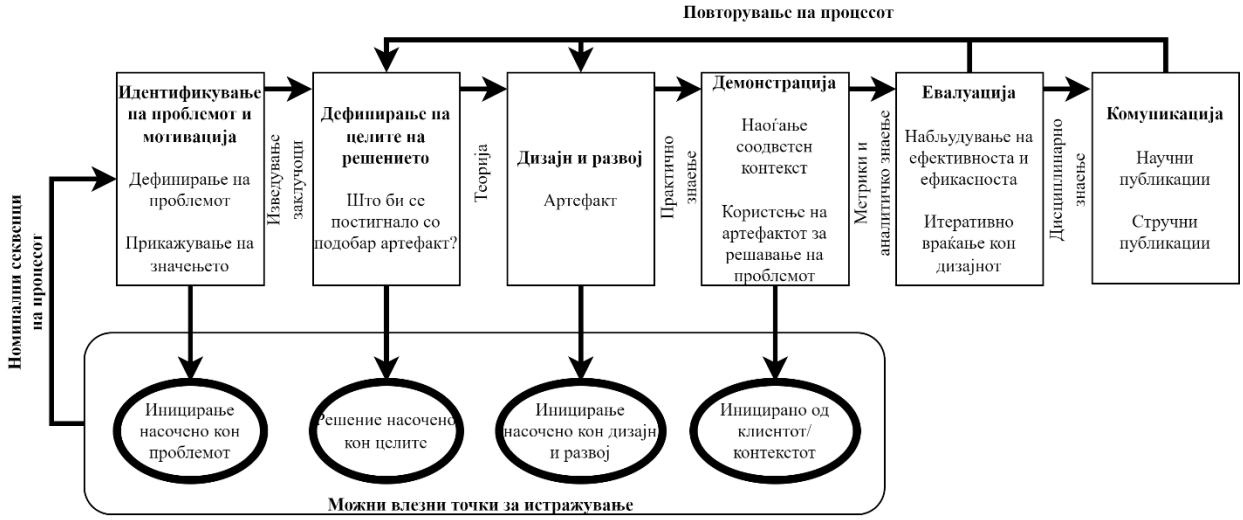
Во првиот дел од докторската дисертација се врши емпириска анализа на сајбер-безбедносната поставеност кај малите организации, со посебен акцент на нивната перцепција на ризик и реалното ниво на безбедносна подготвеност. За таа цел се користи CyPRisT,таксономија која овозможува структурирана класификација на организациите според релевантни параметри поврзани со сајбер-безбедноста. Податоците се прибираат преку структурирани прашалници, а нивната обработка се врши со примена на статистички методи, компаративна анализа и интерпретација на добиените резултати. Врз основа на добиените резултати се идентификуваат организациските и човечките фактори кои влијаат врз сајбер-безбедносната подготвеност, при што овие сознанија обезбедуваат поширок организациски контекст за применливоста на техничките решенија предложени во понатамошниот тек на истражувањето.

Во вториот дел од дисертацијата се врши развој и евалуација на моделот за детекција на аномалии базиран на ненадгледувано длабоко учење, односно автоенкодер. Во овој дел се применуваат методите на анализа, синтеза и експериментално тестирање. Моделот се обучува врз легитимен мрежен сообраќај со цел да научи репрезентација на нормалното однесување, додека реконструкциската загуба се користи како индикатор за отстапување од нормалниот образец. За проверка на поставените хипотези се користи експериментална тестна околина, во која се прибираат и анализираат податоците за легитимен и малициозен мрежен сообраќај. Добиените резултати се анализираат со примена на релевантни метрики за евалуација, врз чија основа се изведуваат заклучоци за ефективноста и применливоста на предложениот автоенкодерски пристап.

Во третиот дел од дисертацијата, истражувањето е структурирано согласно со методологијата на истражување базирана на дизајн (анг. Design Science Research Methodology – DSRM). Оваа методологија е соодветна бидејќи во рамките на истражувањето се развива технолошки артефакт, односно адаптивна и ресурсно свесна рамка за оптимизација на IDS-конфигурации. DSRM се реализира низ следните фази: идентификација на проблемот, дефинирање на целите на решението, дизајн и развој, демонстрација, евалуација и комуникација. Процесниот модел на DSRM е прикажан на слика 1.

Во фазата на идентификација на проблемот се анализира потребата од IDS-конфигурации кои можат да обезбедат компромис помеѓу квалитетот на детекција и потрошувачката на ресурси во нестационарни мрежни услови. Во фазата на дефинирање на целите се поставуваат барањата за ресурсно свесна адаптација, интерпретабилност на одлуките и применливост во ограничени околини. Во фазата на дизајн и развој се формализира конфигурацијата на IDS како повеќекритериумски оптимизациски проблем, при што се применува NSGA-II за генерирање Парето-ефикасни конфигурации. Потоа се развива онлајн контролер базиран на D3QN со PER, кој врши динамички избор на конфигурации од добиеното Парето-ефикасно множество. Во фазата на демонстрација се користи контролираната тестна околина, додека во фазата на евалуација се врши анализа на перформансите преку споредба со статичка базна линија, анализа на потрошувачката на ресурси и анализа на стабилноста на научената политика.

На крајот, се врши интеграција и синтеза на резултатите добиени од сите истражувачки целини. Притоа се применуваат методите на компарација, синтеза и дискусија, со цел да се изведат заклучоци во однос на поставените хипотези и да се оцени научната и практичната вредност на предложениот пристап. Ваквата методолошка поставеност овозможува поврзување на организациските аспекти на сајбер-безбедносната подготвеност со техничките аспекти на детекција на аномалии и адаптивна оптимизација на IDS-конфигурации.



Слика 1: Процесен модел на методологијата на истражување базирана на дизајн, адаптирано според [25]

1.4. Научен придонес

Главниот научен придонес на оваа дисертација е развојот на нов интегриран модел за адаптивна и ресурсно свесна оптимизација на системи за детекција на упади во ресурсно ограничени околини. Предложената рамка, именувана како двостепена Парето-водена рамка за адаптивна оптимизација на ресурси кај лесни системи за детекција на упади (анг. A Two-Stage Pareto-Driven Framework for Adaptive Resource Optimization in Lightweight Intrusion Detection Systems – A2DAPT), комбинира повеќекритериумска оптимизација, Парето-ефикасни конфигурации и длабоко засилено учење. На овој начин се овозможува развој на адаптивен IDS-механизам кој динамички се приспособува на нестационарните услови во мрежата, при што се настојува да се задржи соодветен квалитет на детекција и ефикасно користење на ограничените ресурси.

Дополнителен придонес на дисертацијата е примената и евалуацијата на модели базирани на ненадгледувано длабоко учење, односно автоенкодери, за детекција на аномалии во мрежниот сообраќај. Со користење на реконструкциската загуба како индикатор за отстапување од нормалното однесување, се овозможува разграничување помеѓу легитимнниот и малициозниот мрежен сообраќај, без директна зависност од целосно означени податоци. Овој пристап е особено значаен во услови на појава на нови, непознати или слабо застапени типови напади.

Дисертацијата придонесува и преку дизајн и имплементација на тестна ИТ-околина, базирана на алатки со отворен код, која овозможува прибирање, следење и анализа на мрежен сообраќај, логови и безбедносни настани во контролирани услови. Ваквата околина претставува практична основа за експериментална проверка на предложените технички решенија и за анализа на нивната применливост во реалистични сценарија.

Воедно, истражувањето придонесува кон интеграција на социотехничкиот аспект на сајбер-безбедноста преку примена на таксономијата за проценка на сајбер-безбедносната состојба (CyPRisT). Со ова се овозможува систематска анализа на сајбер-безбедносната подготвеност кај малите организации, вклучувајќи ја перцепцијата на ризик, организациските услови, човечките фактори и достапните ресурси. Овие сознанија го дополнуваат техничкиот дел од дисертацијата и овозможуваат подобро разбирање на организацискиот контекст во кој се применуваат предложените безбедносни механизми.

Главните придонеси од истражувањето може да се сумираат на следниот начин:

А. Воведување на интегрирана A2DAPT-рамка за адаптивна и ресурсно свесна оптимизација на IDS-конфигурации, која комбинира офлајн повеќекритериумска оптимизација и онлајн адаптација базирана на длабоко засилено учење.

Б. Формализација на IDS-конфигурацијата како повеќекритериумски оптимизациски проблем и примена на NSGA-II алгоритмот за генерирање Парето-ефикасни конфигурации, кои овозможуваат моделирање на компромисот помеѓу квалитетот на детекција и потрошувачката на ресурси.

В. Имплементација на адаптивен контролер базиран на D3QN со PER, кој овозможува динамички избор на IDS-конфигурации во зависност од тековната состојба на системот, карактеристиките на мрежниот сообраќај и достапните ресурси.

Г. Развој и експериментална евалуација на автоенкодерски модел за детекција на аномалии во мрежниот сообраќај, при што реконструкциската загуба се користи како индикатор за разграничување помеѓу легитимниот и малициозниот сообраќај.

Д. Дизајн и имплементација на тестна ИТ-околина за прибирање и анализа на мрежен сообраќај, логови и безбедносни настани, која обезбедува експериментална основа за проверка на предложените технички решенија.

Ѓ. Примена на CyPRisT за квантитативна анализа на сајбер-безбедносната подготвеност кај малите организации, со цел идентификација на организациски и човечки фактори кои влијаат врз ефективноста на безбедносните мерки.

Со тоа, дисертацијата дава мултидисциплинарен придонес во развојот на интелигентни, адаптивни и ресурсно ефикасни системи за сајбер безбедност. Придонесот се состои не само во развојот на технички механизми за детекција, оптимизација и адаптација, туку и во нивно поставување во поширок организациски контекст, што е од особено значење за нивната практична применливост во реални услови.

1.5. Примена на резултатите од истражувањето

Резултатите од оваа докторска дисертација имаат применлива вредност во технички и организациски контекст, обезбедувајќи интегриран пристап за унапредување на сајбер-безбедноста во современи дистрибуирани и ресурсно ограничени околини. Применливоста на предложените решенија произлегува од нивната модуларност, приспособливост и можност за интеграција во реалните системи.

Во техничка смисла, развиената A2DAPT-рамка овозможува имплементација на адаптивни IDS-механизми кои комбинираат повеќекритериумска оптимизација и динамичко управување со ресурсите. Предложениот оптимизациски пристап овозможува систематско конфигурирање на IDS во зависност од конкретните ресурсни ограничувања и оперативни приоритети. Генерирањето Парето-ефикасни конфигурации обезбедува основа за донесување информирани одлуки при дизајн и управување со безбедносни механизми, што е особено значајно во средини каде што ресурсите се ограничени и е потребно да се постигне компромис помеѓу квалитетот на детекција и потрошувачката на ресурси.

Примената на длабоко засилено учење за адаптивно управување со конфигурациите овозможува динамичка реакција на промените во мрежниот сообраќај. На овој начин, IDS може да го приспособува своето однесување според тековната состојба на мрежата, достапните ресурси и барањата за детекција. Ова е особено релевантно во реални оперативни околини, каде што статичките конфигурации не се секогаш доволни за одржување стабилен однос помеѓу безбедносните перформанси и ресурсната ефикасност.

Дополнително, моделот базиран на автоенкодер може да се примени за анализа на мрежен сообраќај во реални инфраструктури, особено во сценарија каде што достапноста на целосно означени податоци е ограничена. Преку користење на реконструкциската загуба како индикатор за отстапување од нормалното однесување, автоенкодерскиот пристап овозможува идентификација на аномални обрасци во мрежниот сообраќај. Ваквиот модел може да се користи како дополнителен механизам за рана детекција на сомнителни активности и како поддршка на постојните IDS-решенија, особено во IoT и edge околини.

Развиената тестна ИТ-околина претставува значаен практичен резултат од истражувањето. Таа овозможува контролирано тестирање и валидација на предложените безбедносни решенија, прибирање и анализа на мрежен сообраќај, логови и безбедносни настани, како и репродукција на експерименти и споредба на различни пристапи. Дополнително, ваквата околина може да се користи за едукативни и истражувачки цели во областа на сајбер-безбедноста, особено за развој и тестирање на IDS-механизми базирани на машинско учење и оптимизација.

Од организациски аспект, резултатите добиени преку примена на CyPRisT овозможуваат систематско согледување на сајбер-безбедносната подготвеност кај малите организации. Овие сознанија претставуваат основа за дефинирање соодветни политики и стратегии, поефикасно насочување на ресурсите и унапредување на свесноста за сајбер-ризиците кај носителите на одлуки. На овој начин, резултатите од организациската анализа може да придонесат кон подобро усогласување на техничките мерки со реалните потреби, ограничувања и капацитети на организациите.

Интеграцијата на техничките и организациските резултати овозможува развој на сеопфатен пристап кон сајбер-безбедноста, кој не се ограничува само на детекција на напади, туку ги зема предвид и факторите кои влијаат врз применливоста, ефективноста и одржливоста на безбедносните решенија. Со тоа, резултатите од дисертацијата може да се применат како основа за развој на интелигентни, адаптивни и ресурсно свесни сајбер-безбедносни механизми во реални организациски и технички средини.

1.6. Нацрт на содржината

Во воведната глава се дадени основните информации за докторската дисертација, со осврт на предметот на истражување, мотивот и поставените цели. Накратко се образложуваат користените научни методи, поставените хипотези, очекуваните научни и практични придонеси, како и можната примена на добиените резултати.

Во втората и третата глава е даден теоретски осврт на техниките од длабокото учење, засиленото учење и повеќекритериумската оптимизација. Се разгледуваат основните концепти на невронските мрежи, со посебен акцент на архитектурата за ненадгледуваното учење, како и принципите на повеќекритериумската оптимизација и Парето-ефикасноста. Посебно внимание е посветено на алгоритмот NSGA-II и неговата примена за решавање проблеми со повеќе конфликтни цели.

Во четвртата глава се спроведува емпириска анализа на сајбер-безбедносната подготвеност кај малите организации во Република Македонија преку примена на CyPRisT. Се анализираат организациските и човечките фактори, како и нивното влијание врз сајбер-безбедносната поставеност на организациите. Врз основа на добиените резултати се изведуваат заклучоци релевантни за практична примена и за подобро разбирање на организацискиот контекст во кој се применуваат техничките безбедносни решенија.

Во петтата глава се опишува дизајнот и имплементацијата на експерименталната тестна ИТ-околина, која служи како основа за прибирање, анализа и евалуација на мрежен сообраќај. Се разгледуваат компонентите на системот, начинот на генерирање легитимен и малициозен сообраќај, како и механизмите за прибирање, обработка и складирање на податоците. Оваа околина овозможува контролирано тестирање на предложените безбедносни механизми и практична проверка на нивната применливост.

Во шестата глава се обработува примената на техники од ненадгледувано длабоко учење за детекција на аномалии во мрежниот сообраќај. Се образложува концептот на автоенкодери, нивната архитектура и начинот на обучување, како и методологијата за детекција базирана на реконструкциска загуба. Во рамките на оваа глава се опишува експерименталната поставка и се анализираат добиените резултати преку соодветни метрики за евалуација.

Во седмата глава се разработува интегриран пристап за оптимизација и адаптивно управување со IDS, преку формализација на проблемот како повеќекритериумски оптимизациски модел и негова надградба со длабоко засилено учење. Во оваа глава се презентира предложената A2DAPT-рамка, која комбинира офлајн генерирање на Парето-ефикасни IDS-конфигурации и онлајн адаптација преку DRL-контролер. Рамката се евалуира експериментално во контролираната тестна околина, со цел анализа на компромисот помеѓу квалитетот на детекција и потрошувачката на ресурси.

Во последната глава се изведуваат заклучоците од спроведеното истражување, се сумираат главните научни и практични придонеси и се разгледуваат ограничувањата на предложениот пристап. Дополнително, се даваат насоки за идни истражувања во областа на адаптивни, интелигентни и ресурсно свесни системи за сајбер-безбедност.

2. Длабоко учење

Учењето може општо да се дефинира како процес преку кој системот го приспособува своето однесување врз основа на нови искуства и информации. Во поширок контекст, овој процес опфаќа моделирање на начинот на кој новите информации влијаат врз формирањето на претпоставки, одлуки и идно однесување. Ваквата дефиниција е доволно широка за да го опфати и контекстот во кој се развива и применува машинското учење.

Машинското учење претставува област на вештачката интелигенција во која алгоритмите учат модели од податоци и ги подобруваат своите перформанси врз основа на искуство, без потребата секое правило експлицитно да биде програмирано. Машинското учење опфаќа широка класа алгоритми кои се извршуваат на дигитални системи и постигнуваат зададена цел преку адаптација врз основа на достапните податоци. Оваа адаптација најчесто се реализира преку приспособување на параметри кои влијаат врз излезите или одлуките на моделот. Слично како што научните модели се користат за опишување и предвидување одредени аспекти на реалноста, така и моделите на машинското учење овозможуваат предвидување карактеристики на податоците и извлекување релевантни информации.

Длабокото учење претставува поткласа на машинското учење која се заснова на употребата на вештачки невронски мрежи (анг. Artificial Neural Networks – ANN) со повеќе слоеви. Овие модели овозможуваат учење хиерархиски репрезентации на податоците, при што пониските слоеви најчесто учат поедноставни карактеристики, а подлабоките слоеви учат посложени и апстрактни репрезентации. Наместо рачно дефинирање на сите карактеристики, DL-моделите можат автоматски да извлекуваат релевантни обрасци од високодимензионални податоци, како што се мрежните текови, статистичките карактеристики на пакети или временските прозорци на мрежниот сообраќај.

Во последните години, различните имплементации на вештачките невронски мрежи се наметнуваат како значаен пристап за развој на модели способни за обработка на сложени податоци и за постигнување високи перформанси во задачи како класификација, регресија, детекција на аномалии и предвидување. Во споредба со традиционалните модели на машинското учење, длабоките модели често овозможуваат поефективно учење на сложени нелинеарни односи, особено кога се достапни доволно податоци и соодветни пресметковни ресурси.

Подетален преглед на машинското и длабокото учење е даден во трудовите на Бишоп и Насрабади [26] и Годфелоу и сор. [11]. Во продолжение на ова поглавје се презентираат аспектите од длабокото учење кои се релевантни за оваа дисертација.

2.1. Длабоки невронски мрежи

Вештачките невронски мрежи претставуваат една од најзначајните парадигми во современото машинско учење, особено при обработка на комплексни податоци од реалниот свет, како што се слики [27], видеа [28], аудиосигнали [29] и природен јазик [30]. Покрај примената во задачи како класификација, регресија и предвидување, овие модели имаат значајна улога и во компресијата на податоци, преку учење компактни и информативни репрезентации со минимална загуба на релевантната информација. Нивната широка применливост произлегува од способноста за моделирање сложени нелинеарни зависности

и автоматско извлекување релевантни карактеристики од високодимензионални податоци. Во областа на сајбер-безбедноста, ова е особено важно бидејќи мрежниот сообраќај често содржи комплексни, нелинеарни и временски зависни обрасци кои тешко се опишуваат со статички правила.

Формално, вештачката невронска мрежа може да се претстави како композиција од параметризирани трансформации. Кај повеќеслојниот перцептрон (анг. Multi-Layer Perceptron – MLP), секој слој врши линеарна трансформација на влезот, по што се применува нелинеарна активациска функција. Еден скриен слој може да се запише како:

$$h = \sigma(Wx + b), \qquad (1)$$

каде што x е влезниот вектор, W е матрица на тежини, b е вектор на пристрасност, а σ е нелинеарна активациска функција. Најчесто користени активациски функции се $tanh$, сигмоидната функција и Rectified Linear Unit (ReLU), која се дефинира како:

$$ReLU(x) = \max(0, x). \qquad (2)$$

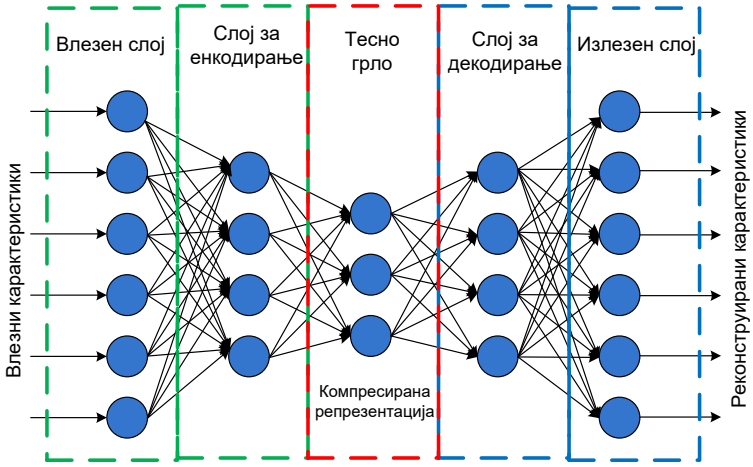
Со поврзување повеќе скриени слоеви се добива длабока невронска мрежа (анг. Deep Neural Network – DNN). Овие мрежи се способни да апроксимираат комплексните функции [31], да решаваат задачи со висока сложеност [27] [32], како и да постигнуваат добра генерализација и поволни скалабилни својства во одредени услови [33] [34]. Изборот на ширина и длабочина претставува важна одлука при дизајнот на моделот. Поголемите модели вообичаено имаат поголема репрезентациска моќ, но тоа доаѓа по цена на зголемени мемориски и пресметковни барања, како и потенцијално посложен процес на обучување.

Покрај основните MLP-структури, развиени се и специјализирани архитектури кои ја прошируваат применливоста на вештачките невронски мрежи. Конволуциските невронски мрежи [35] користат конволуциски оператори за искористување на локални просторни корелации. Рекурентните невронски мрежи [36] [37] [38] овозможуваат моделирање на секвенцијални податоци преку итеративна обработка на влезовите. Трансформер архитектурата [39], базирана на механизми на внимание (анг. attention) [40], овозможува ефикасно моделирање на долгорочни зависности во секвенцијалните податоци. Автоенкодерските архитектури, пак, се насочени кон учење компактни латентни репрезентации преку процесот на реконструкција на влезните податоци.

И покрај архитектонските разлики, овие модели се базираат на композиција од линеарни и нелинеарни трансформации и претставуваат основа за современите решенија од областа на длабокото учење. Во рамките на оваа дисертација, нивната примена се разгледува во два главни контексти: прво, преку автоенкодери за учење компактни латентни репрезентации и детекција на аномалии во мрежниот сообраќај и второ, преку длабоко засилено учење како пристап за донесување одлуки во динамички и интерактивни околини. Во таа смисла, фокусот е ставен на нивната применливост, ограничувања и можности за унапредување во рамките на интелигентни сајбер-безбедносни системи.

2.2. Автоенкодер за детекција на аномалии

Автоенкодерот претставува техника од областа на ненадгледуваното длабоко учење, која се користи за изградба на вештачки невронски мрежи способни да научат компактна репрезентација на влезните податоци и да извршат нивна реконструкција на излезот.



Слика 2: Архитектура на автоенкодерска невронска мрежа

Автоенкодерската мрежа најчесто има приближно симетрична структура, составена од енкодер, латентен простор и декодер. Енкодерот го пресликува влезниот вектор во компактна латентна репрезентација, додека декодерот ја користи оваа репрезентација за реконструкција на оригиналниот влез. Во централниот дел на мрежата прикажана на слика 2, се наоѓа т.н. тесно грло (анг. bottleneck), кое претставува слој или репрезентациски простор со намалена димензионалност. Неговата улога е да ја ограничи количината на информацијата што се пренесува низ мрежата, со што моделот се поттикнува да ги задржи најрелевантните карактеристики на влезните податоци.

Процесот на реконструкција е поврзан со одредено ниво на загуба, бидејќи реконструираниот излез најчесто не е целосно идентичен со оригиналниот влез. Доколку автоенкодерот е соодветно обучен, оваа реконструкциска загуба се минимизира за податоците кои припаѓаат на распределбата врз која моделот е обучен. Функцијата на загуба $L(x)$може да се дефинира како:

$$L(x) = \| x - D(E(x)) \|, \qquad (3)$$

каде што x ги претставува влезните податоци, $E(\cdot)$ го означува енкодерот, $D(\cdot)$ го означува декодерот, а $\|\cdot\|$ претставува избраната функција за мерење на растојание или грешка. За даден влезен вектор x, енкодерот генерира латентна репрезентација $z = E(x)$, додека декодерот ја реконструира вредноста $\hat{x} = D(z)$. Реконструкциската загуба ја изразува разликата помеѓу оригиналниот и реконструираниот влез, а параметрите на енкодерот и декодерот се оптимизираат преку нејзино минимизирање.

Автоенкодерите имаат широка примена во обработката на податоци. Добро обучениот автоенкодер може да се користи за намалување на шумот, екстракција на релевантните карактеристики, редукција на димензионалноста и учење компактни латентни репрезентации. Дополнително, варијациските автоенкодери можат да се користат за

генерирање нови податоци, додека во задачи за препознавање обрасци, автоенкодерите често се применуваат за детекција на аномалии.

Во системите за детекција на упади, автоенкодерите се користат за детекција на аномалии во мрежниот сообраќај преку учење на репрезентација на легитимниот сообраќај и идентификација на отстапувања од тоа однесување. Основната претпоставка е дека автоенкодерот обучен врз легитимен сообраќај ќе го реконструира таквиот сообраќај со мала реконструкциска загуба, додека невообичаениот или малициозниот сообраќај ќе генерира повисока загуба поради отстапување од научената распределба.

Оваа примена на автоенкодерите континуирано се развива во областа на IDS. Во [41], авторите предлагаат метод за класификација базиран на длабоко учење во фазата на претпроцесирање на податоците, со цел екстракција на карактеристики. Овој пристап доведува до подобрување на класификациските перформанси и брзината на детекција. Авторите во [42] предлагаат сличен пристап преку комбинирање на техники од длабоко учење и класично машинско учење. Притоа се користи стекнат контрактилен автоенкодер (анг. Stacked Contractive Autoencoder – SCAE) за екстракција на карактеристики од мрежниот сообраќај, по што се применува SVM-алгоритам за класификација со цел подобрување на детекциските перформанси врз двете евалуациски множества: KDD Cup 99 и NSL-KDD.

Во трудот [43], авторите комбинираат автоенкодер со подобрен генетски алгоритам базиран на *backpropagation* (IGA-BP). Во овој пристап, автоенкодерот се користи за елиминација на редундантните информации и за намалување на димензионалноста на податоците, додека IGA-BP моделот ги адресира проблемите поврзани со бавната стапка на детекција и заглавување во локалните оптимуми кај класичните BP-мрежи. Експерименталните резултати покажуваат дека предложениот метод влијае врз точноста на класификацијата, стапката на лажно позитивните резултати и стапката на детекција.

Општо земено, современите истражувања со автоенкодери во IDS се фокусираат на подобрување на екстракцијата на карактеристики, намалување на димензионалноста и комбинирање на добиените репрезентации со различни техники на машинско учење. Во оваа дисертација, автоенкодерот се користи првенствено како механизам за ненадгледувана детекција на аномалии, при што реконструкциската загуба се користи како индикатор за разграничување помеѓу легитимен и малициозен мрежен сообраќај.

2.3. Основи на засилено учење и интеракција агент – околина

Покрај тоа што моделите на машинско и длабоко учење може да се користат за класификација, предвидување и трансформација на податоците во покорисни репрезентации, во одредени сценарија тие можат да бидат дел од системите што донесуваат одлуки и преземаат акции врз основа на набљудуваните информации. Таквите системи се нарекуваат агенти. Агентот може да се разгледува како ентитет што ја набљудува состојбата на околината, избира акција и врз основа на последиците од таа акција го прилагодува своето понатамошно однесување.

Засиленото учење претставува парадигма во машинското учење во која агентот учи како да дејствува во дадена околина преку последователно преземање акции и добивање повратна информација во форма на награда. За разлика од надгледуваното учење, каде

моделот учи од однапред означени примери, кај засиленото учење агентот учи од последиците на сопствените одлуки. Основната цел е агентот да научи политика на однесување која ја максимизира очекуваната акумулирана награда во одреден временски хоризонт, односно да избира акции кои водат кон поволни долгорочни резултати.

Во контекст на оваа дисертација, агентот може да се толкува како адаптивен контролер на IDS. Тој ја набљудува тековната состојба на мрежниот сообраќај и ресурсната состојба на системот, избира соодветна IDS-конфигурација и добива награда врз основа на квалитетот на детекција и усогласеноста со дефинираниот ресурсен буџет. Околината ја претставуваат тековните мрежни услови, ограничувањата на ресурсите и ефектите од избраната конфигурација. Состојбата може да содржи карактеристики на мрежниот сообраќај, претходно применета IDS-конфигурација и ресурсниот буџет. Акцијата претставува избор на една IDS-конфигурација, додека наградата го изразува компромисот помеѓу квалитетот на детекција и потрошувачката на ресурси.

Ваквата поставеност овозможува проблемот на адаптивно управување со IDS-конфигурации да се разгледува како процес на секвенцијално донесување одлуки. Во продолжение се презентира формалниот пристап кој најчесто се користи за моделирање на засиленото учење, како и основните методи релевантни за предложената адаптивна рамка во оваа дисертација.

2.3.1. Маркови процеси на одлучување

Марково својство претставува принцип според кој следната состојба на системот зависи исклучиво од неговата тековна состојба, а не од претходните состојби [20]. Повеќестепен проблем на донесување одлуки, кај кој транзициите помеѓу состојбите го задоволуваат Марковото својство, се нарекува Марков процес на одлучување (анг. Markov Decision Process – MDP). MDP претставува стандардна формална рамка за моделирање на интеракцијата помеѓу агентот и околината во засиленото учење. Формално, MDP може да се претстави како петорка:

$$\varepsilon = \{Z^+, S, A(s), P, R\} \qquad (4)$$

каде што:

ε ја претставува околината во која дејствува агентот,

$Z^+ = \{0,1,2, \dots\}$ е множеството на временски чекори, односно фази на одлучување,

$s \in S$е состојба од просторот на состојби S,

$\mathcal{A}(s)$е множеството на можни акции во состојбата s,

$P(s, a, s')$ е веројатноста за премин од состојба s во состојба s'по преземањето акција a,

$R(s, a, s')$ е непосредната награда добиена при транзицијата од sво s'под акција a.

Во стандардното засилено учење, агентот интерактивно дејствува со околината ε во дискретни временски чекори. Во секој чекор t, агентот ја набљудува тековната состојба s_t, избира акција a_t според својата политика π, добива скаларна награда r_t, како и следната

состојба s_{t+1}. Овој процес продолжува сè до достигнување на терминална состојба или до завршување на дефинираниот временски хоризонт.

Вкупната акумулирана награда од моментот t е дефинирана како:

$$R_t = \sum_{k=0}^{\infty} \gamma^k r_{t+k}, (5)$$

каде што $\gamma \in (0,1)$ е фактор на дисконтирање. Целта на агентот е да ја максимизира очекуваната вредност на оваа акумулирана награда за секоја состојба s_t, односно да научи политика која води кон поволни долгорочни резултати.

Вредносната функција на акцијата под политика π е дефинирана како:

$$Q^{\pi}(s,a) = E[R_t \mid s_t = s, a_t = a], (6)$$

што ја претставува очекуваната акумулирана награда доколку агентот започне од состојба s, преземе акција a, и понатаму ја следи политиката π. Оваа функција ја задоволува Белмановата равенка:

$$Q^{\pi}(s,a) = E_{s',a'}[r + \gamma Q^{\pi}(s',a') \mid s,a]. \quad (7)$$

Оптималната вредносна функција на акцијата се дефинира како:

$$Q^{*}(s,a) = \max_{\pi} Q^{\pi}(s,a), \quad (8)$$

и ја претставува максималната вредност на акцијата aво состојбата sпод која било политика. Оптималната вредносна функција ја задоволува следната Белманова равенка на оптималност:

$$Q^{*}(s,a) = E_{s'}[r + \gamma \max_{a'} Q^{*}(s',a') \mid s,a]. \quad (9)$$

Откако ќе се определи Q^{*}, оптималната политика може да се изведе како:

$$\pi^{*}(s) = \arg\max_{a} Q^{*}(s,a). \quad (10)$$

Со ваквата формализација се добива јасна математичка рамка за моделирање на процесот на донесување одлуки, во која односот помеѓу состојбите, акциите, транзициите и наградите е експлицитно дефиниран.

Во контекст на оваа дисертација, MDP овозможува адаптивното управување со IDS-конфигурациите да се претстави како секвенцијален проблем на одлучување, каде што агентот учи која конфигурација е најсоодветна за дадената состојба на мрежниот сообраќај и ресурсните ограничувања. На тој начин се поставува теоретската основа за примена на DQN-базирани методи, преку кои се апроксимира оптималната вредносна функција и се избира политика што го балансира квалитетот на детекција со потрошувачката на ресурси.

2.3.2. Апроксимација на вредносни функции и временска разлика

Како и секоја друга функција, вредносните функции може апроксимативно да се претстават со модел. Во случај кога бројот на состојби и акции е конечен, вредностите може да се зачуваат во табела за пребарување, што претставува т.н. табеларен пристап. Во зависност од формулацијата на проблемот, може да се користи вредносна функција на состојба $V(s)$, која ја проценува вредноста на дадена состојба, или вредносна функција на акција $Q(s,a)$, која ја проценува вредноста на преземање акција a во состојба s. Овие функции вообичаено не се познати однапред, туку се проценуваат во текот на процесот на учење.

Кога агентот нема директен пристап до транзиционата функција P, туку располага само со примероци од интеракции со околината, вредносните функции се ажурираат врз основа на набљудувани транзиции. Методите на временска разлика (анг. Temporal Difference – TD) комбинираат идеи од динамичко програмирање и пристапите на Монте Карло бидејќи учат од искуство без потреба од целосен модел на околината и без да се чека завршување на целата епизода.

Основната TD-грешка може да се запише како:

$$\delta_t = r_t + \gamma V(s_{t+1}) - V(s_t). \quad (11)$$

Оваа грешка ја изразува разликата помеѓу тековната проценка $V(s_t)$ и новата целна проценка добиена врз основа на непосредната награда r_t и проценетата вредност на следната состојба $V(s_{t+1})$. Врз основа на оваа TD-грешка, вредноста на состојбата се ажурира според следното правило:

$$V(s_t) \leftarrow V(s_t) + \alpha\delta_t, \quad (12)$$

односно:

$$V(s_t) \leftarrow V(s_t) + \alpha[r_t + \gamma V(s_{t+1}) - V(s_t)], \quad (13)$$

каде што α е стапка на учење, а γ е фактор на дисконтирање.

Со овој метод, проценката на вредноста на тековната состојба $V(s_t)$ се подобрува со користење на непосредната награда и проценката на вредноста на следната состојба. Овој процес се нарекува *bootstrapping*, бидејќи новата проценка се гради врз основа на веќе постоечка проценка. TD-методите се значајни бидејќи овозможуваат ефикасно искористување на искуството и учење во текот на самата интеракција со околината.

Овие методи претставуваат основа за современите пристапи во длабокото засилено учење. Конкретно, алгоритмот Deep Q-Network (DQN) ја проширува TD-рамката преку апроксимација на Q-функцијата со длабока невронска мрежа, наместо нејзино чување во табела. На овој начин се овозможува примена на Q-учење во проблеми со високодимензионални состојби и дискретен простор на акции, каков што е изборот на IDS-конфигурација од ограничено множество можни конфигурации. Дополнително, TD-

грешката има значајна улога и кај методите со PER, каде што примероците со поголема грешка може да добијат поголем приоритет при обучувањето.

2.4. Длабоко засилено учење

Во секцијата 2.1. беа презентирани длабоките невронски мрежи, кои претставуваат моќна класа модели за апроксимација на функции. Во секцијата 2.3. беше претставена рамката на RL, како општ пристап за моделирање интерактивни агенти кои учат преку интеракција со околината.

Длабокото засилено учење се однесува на категоријата методи кои користат DNN за апроксимација на функциите потребни за моделирање и управување со интерактивни агенти. Со оваа комбинација, RL-методите може да се применат во посложени околини, каде што просторот на состојби е голем, високодимензионален или континуиран, а табеларното претставување на вредносните функции е непрактично.

Табеларните методи најчесто претпоставуваат дека секоја состојба и секоја акција може експлицитно да се зачуваат во табела. Таквиот пристап ја ограничува генерализацијата, бидејќи доколку не постојат претходно научени вредности за одредена состојба или акција, моделот не може соодветно да процени како треба да постапи во нова ситуација.

Поради тоа што MDP не поставува специфични претпоставки за природата на просторот на состојби S, состојбата може да биде претставена како структуриран вектор на карактеристики, на пример $S \subset \mathbb{R}^d$, каде што секоја компонента опишува одреден аспект на околината. Ваквата поставеност овозможува примена на функциска апроксимација со помош на DNN, при што агентот може да генерализира од претходно видени кон нови, претходно невидени состојби.

Во контекст на оваа дисертација, ваквата можност е особено значајна бидејќи состојбата на IDS може да вклучува повеќе променливи, како што се карактеристики на мрежниот сообраќај, претходно применета IDS-конфигурација и ресурсни ограничувања. Затоа, DRL обезбедува соодветна основа за развој на адаптивен контролер кој може да избира IDS-конфигурации во нестационарни мрежни услови.

Во следните секции се презентираат неколку значајни методи од DRL, со посебен акцент на DQN и неговите подобрени варијанти, кои се релевантни за предложената рамка за адаптивна оптимизација на ресурси кај IDS.

2.4.1. Длабоки Q-мрежи

Кај табеларниот Q-learning, под соодветни услови, проценката на вредносната функција на акцијата може да конвергира кон оптималната вредносна функција Q^*[44]. Меѓутоа, при решавање проблеми со голем или високодимензионален простор на состојби, предизвик не претставува само меморијата потребна за складирање големи табели, туку и времето и количината на податоци потребни за нивно соодветно пополнување.

Кај вредносно-базираните (анг. value-based) и модел-независните (анг. model-free) методи на засилено учење, вредносната функција на акцијата може да се апроксимира со функциски апроксиматор, како што е невронска мрежа. DQN ја апроксимира Q-функцијата преку длабока невронска мрежа, која се ажурира преку минимизирање на TD-грешката.

Нека $Q(s,a;\theta)$ е апроксимација на вредносната функција на акцијата со параметри θ. Целта на Q-learning е директно да ја апроксимира оптималната функција:

$$Q^*(s,a) \approx Q(s,a;\theta). \qquad (14)$$

Во DQN, параметрите θ се ажурираат преку минимизирање на функцијата на загуба дефинирана како квадратна разлика помеѓу целната-вредност и тековната проценка на Q-вредноста:

$$L_i(\theta_i) = E[(y_i^{DQN} - Q(s,a;\theta_i))^2], \qquad (15)$$

каде што целната вредност е:

$$y_i^{DQN} = r + \gamma \max_{a'} Q(s',a';\theta_i^-). \qquad (16)$$

Тука s' ја претставува следната состојба по состојбата s, r е непосредната награда, γ е факторот на дисконтирање, а θ_i^- ги претставува параметрите на целната мрежа.

Кога невронска мрежа се користи како апроксиматор на Q-функцијата, процесот на учење може да стане нестабилен или да дивергира [45]. Оваа нестабилност произлегува од повеќе фактори, меѓу кои се корелацијата помеѓу последователните примероци, промената на распределбата на податоците како резултат на промената на политиката, како и меѓузависноста помеѓу тековните Q-проценки и целните вредности што се користат за нивно ажурирање.

Со цел да се надминат овие проблеми, DQN воведува два клучни механизми. Првиот е *experience replay*, при што искуствата на агентот се зачувуваат во мемориски бафер и подоцна случајно се семплираат за обучување, со што се намалува корелацијата помеѓу примероците. Вториот е посебна целна мрежа (анг. target network), која се користи за пресметка на целните вредности и чии параметри периодично се ажурираат со параметрите на главната, односно онлајн мрежа.

Целната вредност во DQN може да се запише како:

$$Y_t^{DQN} = r_{t+1} + \gamma \max_a \hat{Q}(s_{t+1},a;\theta_t^-), \qquad (17)$$

каде што θ_t^- ги претставува параметрите на целната мрежа, кои периодично се ажурираат со параметрите на главната мрежа. Овој пристап ја подобрува стабилноста на процесот на учење и овозможува примена на Q-learning во проблеми со високодимензионален простор на состојби.

Во контекст на оваа дисертација, DQN е релевантен бидејќи овозможува агентот да избира акција од дискретното множество можни IDS-конфигурации. Ова претставува основа за понатамошната примена на подобрени варијанти на DQN, како Double DQN, Dueling DQN и D3QN со PER, кои се користат за адаптивен избор на IDS- конфигурации во предложената A2DAPT-рамка.

2.4.2. Дупла длабока Q-мрежа

Кај класичниот DQN, целната вредност се пресметува со користење на операторот max, кој ја избира акцијата со најголема проценета Q-вредност во следната состојба. Меѓутоа, бидејќи истите проценки се користат и за избор и за евалуација на акцијата, може да се појави систематско преценување на Q-вредностите. Овој проблем е особено изразен во услови на шумни проценки и голем простор на состојби.

Со цел да се намали ова преценување, дуплата длабока Q-мрежа (анг. Double DQN - DDQN) го раздвојува процесот на избор на акцијата од процесот на нејзина евалуација [23]. Притоа, онлајн мрежата се користи за избор на акцијата според *greedy* политика, додека целната мрежат се користи за евалуација на вредноста на избраната акција. На овој начин се искористува постоечката целна мрежа од архитектурата на DQN, без потреба од воведување дополнителна невронска мрежа.

Целната вредност кај DDQN се дефинира како:

$$Y_t^{DDQN} = r_{t+1} + \gamma \hat{Q}(s_{t+1}, \arg\max_a Q(s_{t+1}, a; \theta_t); \theta_t^-), \qquad (18)$$

каде што θ_t се параметрите на онлајн мрежата, а θ_t^- се параметрите на целната мрежа. Акцијата се избира со онлајн мрежата преку изразот $\arg\max_a Q(s_{t+1}, a; \theta_t)$, додека нејзината вредност се пресметува со целната мрежа $\hat{Q}(\cdot; \theta_t^-)$.

Со ваквото раздвојување се добиваат попрецизни проценки на Q-вредностите и се подобрува стабилноста на процесот на учење. Во контекст на оваа дисертација, ова е значајно бидејќи агентот треба стабилно да споредува повеќе можни IDS-конфигурации и да избегне систематско фаворизирање на конфигурации чии вредности се преценети поради шум во проценките.

2.4.3. Приоритизирано повторување на искуства

И DQN и DDQN користат повторување на искуства, при што искуствата на агентот се зачувуваат во мемориски бафер и потоа се избираат за обучување. Кај класичното повторување на искуства, примероците најчесто се избираат униформно, односно секое зачувано искуство има еднаква веројатност да биде избрано. Сепак, сите примероци не се подеднакво информативни за процесот на учење.

Кај Q-мрежите, TD-грешката ја претставува разликата помеѓу целната Q-вредност и тековно проценетата Q-вредност од онлајн мрежата. Примероците со поголема TD-грешка укажуваат дека тековниот модел има поголемо отстапување во проценката за тие транзиции, па затоа тие може да бидат покорисни за ажурирање на параметрите на мрежата.

Приоритизирано повторување на искуства (PER) ја користи оваа идеја така што на секој примерок му доделува приоритет врз основа на неговата TD-грешка. Наместо униформно семплирање, примероците со поголем приоритет имаат поголема веројатност да бидат избрани при обучувањето. На овој начин, агентот почесто учи од транзиции кои во дадениот момент се потешки или поинформативни за моделот.

Бидејќи неуниформното семплирање воведува пристрасност во процесот на учење, PER користи *importance-sampling* тежини за нејзино намалување. Функцијата на загуба што ја зема предвид приоритетноста може да се запише како:

$$L_i(\theta_i) = E[\omega_i(Y_t^{DDQN} - Q(s,a;\theta_i))^2], \qquad (19)$$

каде што ω_i претставува *importance-sampling* тежина на примерокот, Y_t^{DDQN} е целната вредност пресметана според Double DQN, а $Q(s,a;\theta_i)$ е тековната проценка на онлајн мрежата.

Во контекст на оваа дисертација, PER е значаен затоа што овозможува агентот почесто да учи од транзиции во кои изборот на IDS-конфигурација довел до поголема грешка во проценките, на пример при нагли промени во мрежниот сообраќај или при прекршување на ресурсните ограничувања. На тој начин се подобрува ефикасноста на обучувањето и адаптивноста на контролерот.

2.4.4. Двојни длабоки Q-мрежи

Додека PER го подобрува процесот на обучување преку приоритетно избирање поинформативни примероци, двојната длабока Q-мрежа (анг. Dueling DQN) се фокусира на подобрување на архитектурата на невронската мрежа. Основната идеја на оваа архитектура е да се раздвојат проценката на вредноста на состојбата и проценката на релативната предност на секоја акција во таа состојба.

Во класичниот DQN, мрежата директно ја апроксимира вредноста $Q(s,a)$за секоја можна акција. Наспроти тоа, кај Dueling DQN, по заедничките скриени слоеви, мрежата се раздвојува во две гранки, односно два *streams*. Првата гранка ја проценува вредносната функција на состојбата $V(s)$, која покажува колку е поволна дадената состојба независно од конкретната акција. Втората гранка ја проценува функцијата на предност на акцијата $A(s,a)$, која покажува колку одредена акција е подобра или полоша во однос на другите можни акции во истата состојба.

Излезот на моделот ги комбинира овие две компоненти за да ја формира вредноста на состојба-акција $Q(s,a)$:

$$Q(s,a;\theta,\alpha,\beta) = V(s;\theta,\beta) + \left(A(s,a;\theta,\alpha) - \frac{1}{|A|}\sum_{a'\in A} A(s,a';\theta,\alpha)\right), \qquad (20)$$

каде што θ ги претставува параметрите на заедничките слоеви пред раздвојувањето на мрежата, додека α и β се параметрите на двете гранки: гранката за предност на акцијата и гранката за вредност на состојбата. Членот со просечната вредност на $A(s,a)$ се користи за нормализација, со цел да се избегне неодреденост при комбинирањето на $V(s)$ и $A(s,a)$.

Овој пристап овозможува поефикасно учење, особено во ситуации кога изборот на конкретна акција има помало влијание од самата состојба или кога повеќе акции имаат слични вредности. Во такви случаи, мрежата може подобро да научи кои состојби се

генерално поволни, без потреба веднаш прецизно да ја процени вредноста на секоја поединечна акција.

Во контекст на оваа дисертација, Dueling DQN е значаен бидејќи повеќе IDS-конфигурации од Парето-ефикасното множество може да имаат слични перформанси во дадени мрежни услови. Раздвојувањето на вредноста на состојбата од предноста на конкретната конфигурација му овозможува на агентот постабилно да ги проценува состојбите и да избира конфигурација која обезбедува соодветен компромис помеѓу квалитетот на детекција и потрошувачката на ресурси.

2.4.5. Двојна дупла длабока Q-мрежа со приоритизирано повторување на искуства

D3QN со PER претставува проширена варијанта на DQN која комбинира повеќе подобрувања со цел зголемување на стабилноста и ефикасноста на процесот на учење. Овој пристап ги интегрира предностите на Double DQN, Dueling DQN и PER во единствена архитектура за апроксимација и ажурирање на Q-вредностите.

Double DQN правилото за ажурирање, дадено со равенка (18), ја намалува пристрасноста поврзана со преценување на Q-вредностите преку раздвојување на изборот и евалуацијата на акциите. Од друга страна, dueling архитектурата, дадена со равенка (20), ја подобрува репрезентацијата на вредносната функција преку раздвојување на вредноста на состојбата од релативната предност на поединечните акции. Дополнително, PER, даден со равенка (19), го подобрува искористувањето на претходно стекнатите искуства преку почесто избирање транзиции со поголема TD-грешка, односно транзиции што се поинформативни за процесот на учење.

Комбинацијата на овие три компоненти овозможува поефикасно и постабилно учење во околини со голем простор на состојби и нееднаква информативност на примероците. Затоа, D3QN со PER често се користи како надградба на класичниот DQN во проблеми каде што е потребно стабилно донесување одлуки врз основа на дискретен простор на акции. Во контекст на оваа дисертација, оваа архитектура е соодветна за реалновременска адаптација на IDS во услови на ограничени ресурси [46].

Архитектурата на D3QN со PER е прикажана на слика 3. Процесот на обучување се одвива преку следниот итеративен циклус:

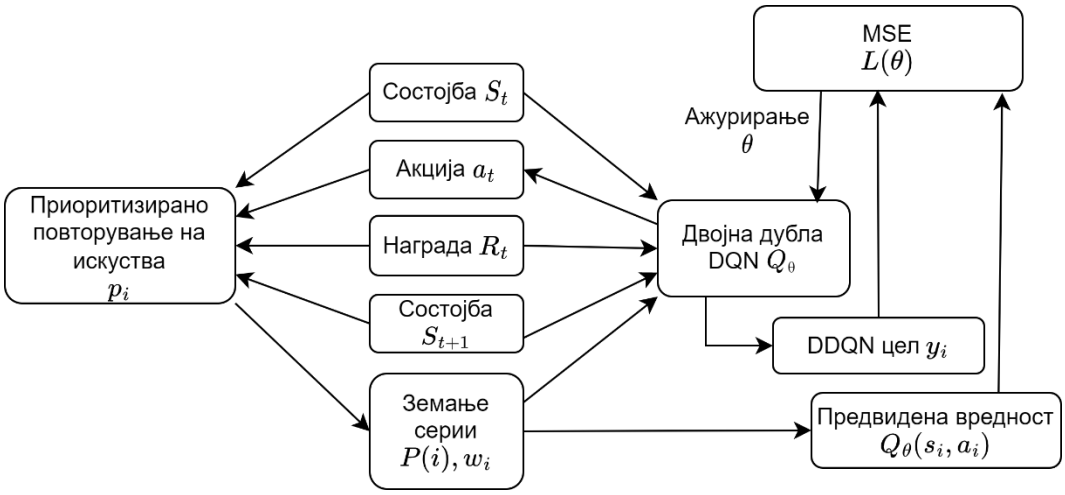
1. се земаат минисерии од транзиции од replay buffer според веројатностите $P(i)$;
2. се пресметуваат importance-sampling тежините w_i;
3. се пресметуваат Double DQN целните вредности y_i;
4. се пресметуваат dueling Q-вредностите $Q_\theta(s_i, a_i)$ преку вредносната компонента и компонентата на предност;
5. се пресметува функцијата на загуба како средноквадратна грешка пондерирана со importance-sampling тежините:

$$L(\theta) = \frac{1}{B}\sum_i w_i \left(Q_\theta(s_i, a_i) - y_i\right)^2; \qquad (21)$$

6. се извршува повратно распределување на грешката (анг. backpropagation) и ажурирање на параметрите θ;

7. се ажурираат приоритетите во replay buffer врз основа на новите TD-грешки.

Овој итеративен процес овозможува континуирано подобрување на политиката на агентот и стабилна адаптација на IDS-конфигурациите во нестационарни и ресурсно-ограничени околини. Во предложената рамка, агентот избира конфигурации од дефинирано множество врз основа на тековната состојба на мрежниот сообраќај, ресурсниот буџет и очекуваниот компромис помеѓу квалитетот на детекција и потрошувачката на ресурси.



Слика 3: Архитектура на D3QN + PER, адаптирано според [46]

3. Повеќекритериумска оптимизација

Во голем број реални оптимизациски проблеми, квалитетот на едно решение не може да се оцени преку единствен критериум. Наместо тоа, потребно е истовремено да се разгледуваат повеќе цели, кои често се меѓусебно конфликтни. Подобрувањето на една цел може да доведе до влошување на друга, што го оневозможува постоењето на едно апсолутно најдобро решение. Во такви случаи, задачата на оптимизацијата не е да пронајде единствен оптимум, туку множество решенија кои претставуваат различни компромиси помеѓу разгледуваните цели.

Повеќекритериумската оптимизација овозможува формално моделирање и решавање на вакви проблеми. Таа е особено значајна во инженерските и информациските системи, каде што перформансите, точноста, трошокот, времето на извршување и потрошувачката на ресурси често треба да се разгледуваат истовремено. Наместо директно сведување на сите цели во една скаларна функција, повеќекритериумскиот пристап овозможува анализа на компромисите и избор на решение според конкретните ограничувања и приоритети.

Во контекст на оваа дисертација, овие концепти се значајни бидејќи се применуваат за моделирање на компромисот помеѓу квалитетот на детекција и потрошувачката на ресурси кај IDS-конфигурациите. Во оваа секција се опишуваат основните концепти на повеќекритериумската оптимизација и Парето-доминацијата, по што се дава преглед на структурата и постапката на алгоритмот NSGA-II.

3.1. Формална дефиниција на повеќекритериумски оптимизациски проблем

Повеќекритериумскиот оптимизациски проблем опфаќа множество од n одлучувачки променливи, k целни функции и множество ограничувања, кои може да бидат зададени како m нееднакви и p еднакви ограничувања. Во општ случај, проблемот може да се запише како минимизација на вектор од целни функции:

$$(\min)_{x \in X_f}\, y \equiv f(x) = (f_1(x), f_2(x), \dots, f_k(x)), k \geq 2, \qquad (22)$$

при следните ограничувања:

$$g_i(x) \leq 0, i = 1,2, \dots, m, \qquad (23)$$
$$h_j(x) = 0, j = 1,2, \dots, p. \qquad (24)$$

Тука $x = (x_1, x_2, \dots, x_n)$ е n-димензионален вектор на одлучувачки променливи, при што $X \subseteq \mathbb{R}^n$го претставува просторот на пребарување. Векторот $y \in \mathbb{R}^k$ги содржи вредностите на k целни функции, а $f: X \to \mathbb{R}^k$ја дефинира мапирачката функција од просторот на одлучувачки променливи кон просторот на цели. Функциите $g_i(x)$ ги претставуваат нееднаквите ограничувања, додека функциите $h_j(x)$ ги претставуваат еднаквите ограничувања.

Ограничувањата го дефинираат множеството на изводливи решенија:

$$X_f = \{x \in X \mid g_i(x) \leq 0,\ i = 1, \dots, m,\ h_j(x) = 0,\ j = 1, \dots, p\}. \quad (25)$$

Секое решение $x \in X_f$ се нарекува изводливо решение, а неговата слика $f(x)$ во просторот на целните функции го претставува соодветниот вектор на перформанси. Бидејќи кај повеќекритериумските проблеми целните функции често се конфликтни, вообичаено не постои едно решение кое истовремено ги оптимизира сите цели. Наместо тоа, се добива множество компромисни решенија, кои овозможуваат избор во зависност од зададените ограничувања и приоритети.

3.2. Концепт на Парето-доминација

Нека x^1и x^2 се две изводливи решенија на повеќекритериумскиот оптимизациски проблем дефиниран со (1). Во случај на минимизација, решението x^1 доминира над решението x^2 доколку се исполнети следните услови:

$$f_j(x^1) \leq f_j(x^2), \forall j = 1,2, \dots, k, \quad (26)$$

$$f_j(x^1) < f_j(x^2), \text{ за најмалку едно } j = 1,2, \dots, k. \quad (27)$$

Тука k е бројот на целни функции, а $f_j(x^i)$ја претставува вредноста на j-тата целна функција за решението x^i, $i = 1,2$. Првиот услов означува дека x^1 не е полошо од x^2 во ниту една целна функција, додека вториот услов бара x^1 да биде строго подобро од x^2 барем во една целна функција.

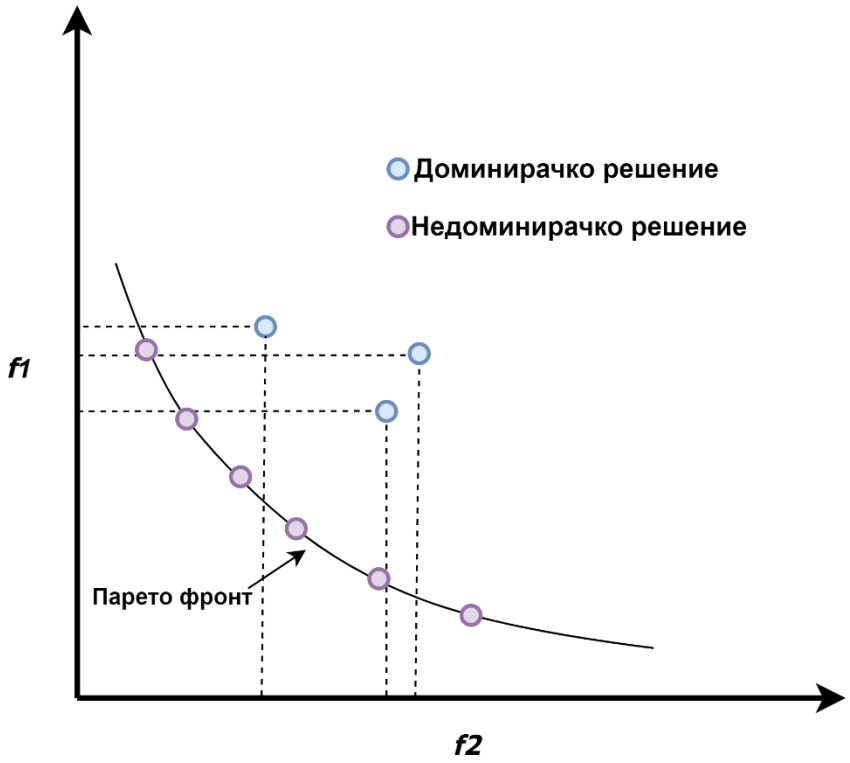
Во таков случај се вели дека x^1 Парето доминира над x^2, односно дека x^2 е доминирано решение. Записот

$$x^1 \prec x^2 \quad (28)$$

означува дека x^1 доминира над x^2.

Доколку едно изводливо решение x не е доминирано од ниту едно друго изводливо решение, тоа се нарекува Парето-ефикасно, односно недоминирано решение. Множеството од сите Парето-ефикасни решенија во просторот на одлучувачки променливи се нарекува Парето множество (анг. Pareto set). Соодветните вектори на целните функции, односно сликите на овие решенија во просторот на цели, ја формираат Парето-фронтата (анг. Pareto front), како што е прикажано на слика 4.

Концептот на Парето-доминација во оваа секција е претставен за проблем на минимизација. Кај повеќекритериумските проблеми на максимизација, насоката на споредба се менува, односно условите за доминација се дефинираат со спротивни нееднаквости.



Слика 4: Илустрација на Парето-доминација и Парето-фронта, адаптирано според [19]

3.3. Генетскиот алгоритам со недоминирачко сортирање

Генетскиот алгоритам со недоминирачко сортирање (NSGA-II) [47] претставува еден од најчесто користените еволутивни алгоритми за решавање повеќекритериумски оптимизациски проблеми. Алгоритмот е предложен од Деб и сор. [19] како подобрена верзија на оригиналниот генетски алгоритам со недоминирачко сортирање (NSGA), кој бил ограничен поради отсуство на елитизам, потреба од дефинирање параметар за споделување за зачувување на разновидноста и релативно висока пресметковна сложеност.

NSGA-II ги надминува овие ограничувања преку воведување елитизам, ефикасно недоминирачко сортирање и механизам за одржување на разновидноста базиран на растојание на згуснување (анг. crowding distance). Елитизмот овозможува најдобрите решенија, односно недомининираните решенија со повисок ранг, да се задржат и да се пренесат во следната генерација. Од друга страна, растојанието на згуснување овозможува зачувување на разновидноста на решенијата долж Парето-фронтата, без потреба од дополнително подесување на параметар за споделување.

Пресметковната сложеност на NSGA-II изнесува $O(MN^2)$, каде што M е бројот на целни функции, а N е големината на популацијата. Оваа сложеност, главно, произлегува од операциите на недоминирачко сортирање и пресметка на растојанието на згуснување. Поради комбинацијата од елитизам, одржување на разновидноста и релативно ефикасна пресметка, NSGA-II е широко применуван за добивање апроксимации на Парето-фронтата кај проблеми со повеќе конфликтни цели.

3.4. Структура на NSGA-II

Структурата на NSGA-II се заснова на неколку клучни механизми кои овозможуваат истовремено приближување кон Парето-фронтата и зачувување на разновидноста на решенијата. Најзначајни компоненти на алгоритмот се:

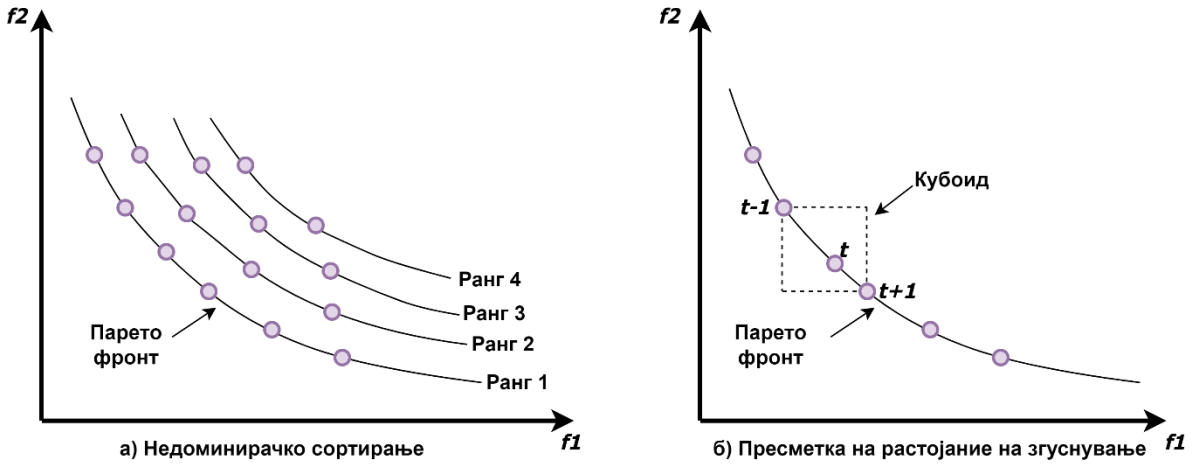
- недоминирачко сортирање (анг. non-dominated sorting);
- оператор за зачувување елитни решенија (анг. elite-preserving operator);
- растојание на згуснување (анг. crowding distance);
- оператор за селекција (анг. selection operator).

Овие компоненти накратко се опишани во продолжение.

а) Недоминирачко сортирање

Недоминирачкото сортирање претставува постапка со која членовите на популацијата се класифицираат според релацијата на Парето-доминација. Процесот започнува со идентификација на сите решенија кои не се доминирани од ниту едно друго решение во тековната популација. Овие решенија добиваат прв ранг и го формираат првиот Парето-фронт.

Потоа, решенијата од првиот фронт привремено се отстрануваат од разгледување, а истата постапка се применува врз преостанатата популација. Недоминираните решенија во оваа редуцирана популација добиваат втор ранг и го формираат вториот фронт. Процесот продолжува итеративно сè додека сите членови на популацијата не бидат распределени во соодветни фронтови според нивото на недоминација, како што е прикажано на слика 5 (а).



Слика 5: Постапка на недоминирачко сортирање и пресметка на растојание на згуснување, адаптирано според [19]

б) Оператор за зачувување елитни решенија

Операторот за зачувување елитни решенија овозможува најдобрите решенија од тековната генерација да се задржат и да се пренесат во следната генерација. На овој начин

се намалува можноста квалитетните недоминирани решенија да бидат изгубени при примената на генетските оператори, како што се вкрстување и мутација.

Во NSGA-II, елитизмот се реализира преку обединување на родителската и потомската популација, по што се избираат најдобрите N индивидуи според рангот на недоминација и вредноста на растојанието на згуснување.

в) Растојание на згуснување

Растојанието на згуснување (анг. crowding distance) претставува мерка за локалната густина на решенијата околу дадено решение во рамките на ист фронт. Решенијата со поголема вредност на растојанието на згуснување се наоѓаат во поретко населени области од просторот на целните функции и затоа се преферираат при селекцијата, со цел да се зачува разновидноста долж Парето-фронтата. Растојанието на згуснување за i-тото решение се дефинира како просечна должина на страните на хиперправоаголник, односно кубоид, како што е прикажано на слика 5 (б).

За секој фронт, решенијата најпрво се сортираат посебно според секоја целна функција. Граничните решенија, односно решенијата со најмала и најголема вредност за дадена целна функција, добиваат бесконечно голема вредност на растојанието на згуснување, со цел да се зачуваат екстремните делови од фронтата. За останатите решенија, растојанието на згуснување се пресметува како сума од нормализираните растојанија помеѓу соседните решенија:

$$cd(i) = \sum_{j=1}^{k} \frac{f_j^{(i+1)} - f_j^{(i-1)}}{f_j^{max} - f_j^{min}}, \qquad (29)$$

каде што k е бројот на целни функции, $f_j^{(i+1)}$ и $f_j^{(i-1)}$ се вредностите на j-тата целна функција за соседните решенија на решението i, по сортирање според таа целна функција, а f_j^{max} и f_j^{min} се максималната и минималната вредност на j-тата целна функција во разгледуваниот фронт. Нормализацијата овозможува целните функции со различни размери да имаат споредливо влијание врз пресметката.

г) Оператор за селекција

Популацијата за следната генерација се формира со користење на операторот за турнирска селекција со згуснување (анг. crowded tournament selection). Овој оператор ги зема предвид и рангот на решението и неговата вредност на растојанието на згуснување. При споредба на две решенија важат следните правила:

- Ако решенијата имаат различни рангови, се избира решението со подобар, односно понизок ранг.
- Ако решенијата имаат ист ранг, се избира решението со поголема вредност на растојанието на згуснување.

На овој начин, алгоритмот истовремено фаворизира решенија поблиску до Парето-фронтата и решенија кои придонесуваат за поголема разновидност на популацијата.

3.5. Постапка на NSGA-II

Постапката на NSGA-II започнува со генерирање иницијална родителска популација P_t со големина N. Врз оваа популација се применуваат генетски оператори, како што се вкрстување (анг. crossover) и мутација (анг. mutation), со што се создава потомска популација Q_t, исто така со големина N.

Потоа, родителската и потомската популација се обединуваат во заедничка популација:

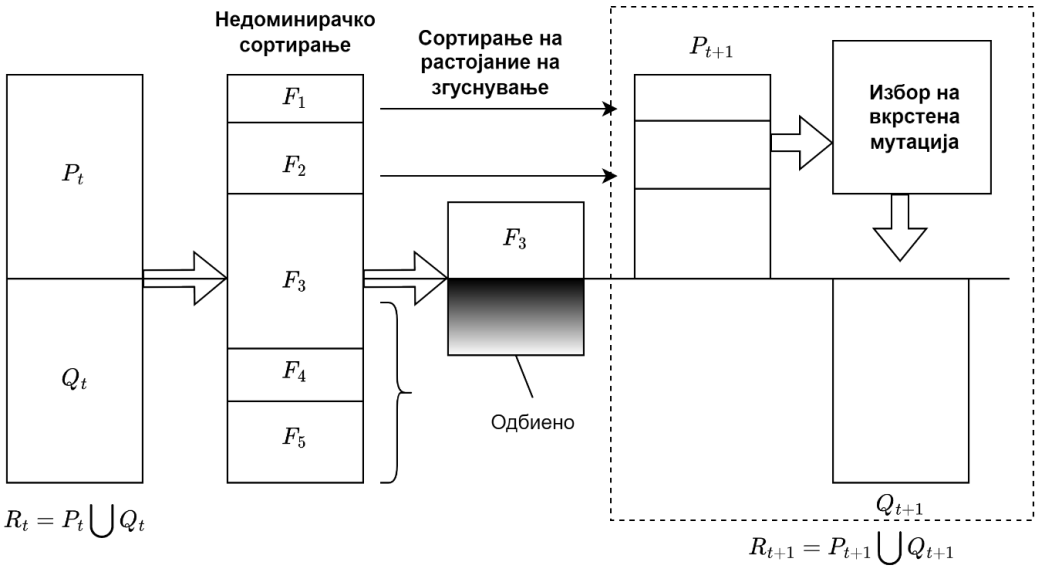
$$R_t = P_t \cup Q_t, \qquad (30)$$

со големина $2N$. Врз популацијата R_t се применува недоминирачко сортирање, при што индивидуите се распределуваат во повеќе фронтови $F_1, F_2, ...$, според нивниот ранг на недоминација.

Следната генерација P_{t+1} се формира со последователно додавање на фронтовите, започнувајќи од најдобриот фронт F_1. Сите индивидуи од даден фронт се додаваат во P_{t+1} доколку со нивното додавање не се надмине големината N. Доколку следниот фронт не може целосно да се вклучи, индивидуите од тој фронт се сортираат според растојанието на згуснување, а се избираат оние со најголема вредност на растојанието на згуснување сè додека популацијата P_{t+1} не достигне големина N.

По формирањето на P_{t+1}, повторно се применуваат генетските оператори за создавање нова потомска популација, а процесот се повторува за наредните генерации $P_{t+2}, P_{t+3}, ...$ Алгоритмот продолжува сè до исполнување на претходно дефиниран критериум за запирање, како што е максимален број генерации, стабилизирање на Парето-фронтата или достигнување зададено ниво на квалитет.

Постапката на NSGA-II е прикажана на слика 6.



Слика 6: Постапка на NSGA-II, адаптирано според [19]

4. Поставеност на мерки за сајбер-безбедноста во мали организации

Сајбер-безбедноста претставува сè поизразен предизвик и фактор од суштинско значење за малите претпријатија и организации, особено во услови на нивна зголемена зависност од информацискатa технологија. Истовремено, информацискатa технологија претставува еден од клучните двигатели на нивниот организациски и економски развој. Ваквата зависност, во комбинација со изложеноста на различни ранливости и закани, создава потреба од воспоставување соодветни механизми за заштита.

Недоволната или несоодветната примена на мерки за сајбер-безбедност може да резултира со значителни финансиски и оперативни последици, како и со нарушување на репутацијата на организацијата. Според [48], во Обединетото Кралство речиси половина од деловните субјекти, односно 46 %, пријавиле сајбер-безбедносни пробиви или напади во период од 12 месеци. Малите претпријатија се сметаат за еден од основните столбови на економијата на Европската Унија и учествуваат со значаен удел во вкупниот бруто-домашен производ на Европа. Имајќи го предвид нивното економско значење, проценката на нивната сајбер-безбедносна состојба, како и идентификацијата на мерки за нејзино унапредување, претставуваат прашања од особено значење.

4.1. Поврзана работа и дискусија

Во научната и стручната литература не постои универзално прифатена дефиниција за поимот „мала организација“. Во ова истражување се зема предвид дефиницијата на ЕУ [49], според која малите и средни претпријатија (анг. Small and Medium-sized Enterprises – SMEs) се организации кај кои бројот на вработени е помал од 50, а годишниот обрт е помал од 10 милиони евра. Сепак, предметот на ова истражување не е ограничен исклучиво на деловни претпријатија, туку ги опфаќа и институциите од јавната администрација, невладините организации, давателите на комунални услуги, како и други сродни субјекти.

Поради тоа, во рамките на ова истражување терминот „мала организација“ се користи за означување на организација која обезбедува услуги, независно од секторот во кој функционира, и која располага со основна ИТ-инфраструктура составена најмалку од веб-страница и локална мрежа со помалку од 50 кориснички работни станици во секторот што е предмет на истражувањето или во рамките на целата организација.

Истражувањето користи таксономија за проценка на сајбер-безбедносната состојба (CyPRisT)[6], како социотехничка рамка за анализа на сајбер-безбедносната поставеност кај малите организации. CyPRisT се заснова на релацијата помеѓу два клучни параметри кои ја определуваат сајбер-безбедносната состојба на една организација:

- ниво на сајбер-безбедносна подготвеност (анг. Cybersecurity Preparedness Score – CPS),
- перципиран ризик од сајбер-напад кај носителите на одлуки (анг. Decision Makers' Perceived Risk of Cyber-Attack score – DMPRCA).

Овие два параметри овозможуваат организацијата да се разгледува не само преку објективното ниво на имплементирани безбедносни мерки, туку и преку субјективната перцепција на ризик кај носителите на одлуки. На тој начин, CyPRisT обезбедува рамка за поврзување на техничките, организациските и бихевиоралните аспекти на сајбер-безбедноста.

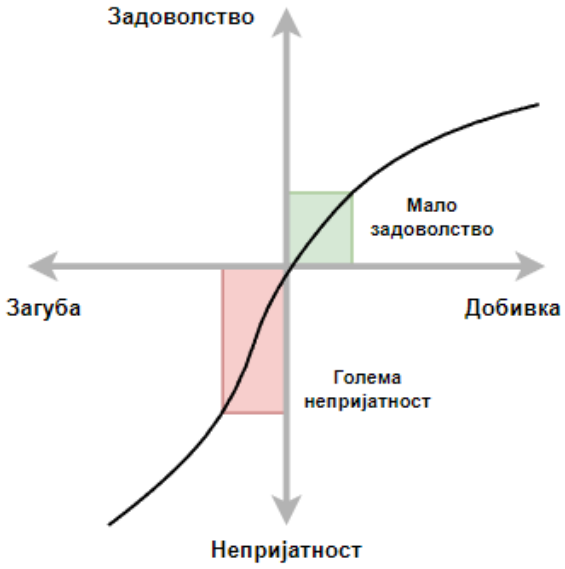
4.2. Теоретска основа на CyPRisT

Основата на CyPRisT се темели на социјални и бихевиорални теории за управување со ризик. Ваквиот пристап е поддржан со наоди од претходни истражувања, меѓу кои и истражувањата на Гупата и сор. [50] каде што се укажува дека организациите често се соочуваат со рамнодушност на носителите на одлуки кон заканите поврзани со сајбер-безбедноста, додека нивното внимание примарно е насочено кон извршување на основните деловни активности.

Меѓу релевантните теоретски рамки особено се издвојуваат теоријата на перспективи (анг. Prospect Theory) и пристрасноста кон статус кво (анг. Status Quo Bias) [51]. Овие концепти ја објаснуваат субјективната димензија во CyPRisT. Теоријата на перспективи ја објаснува перцепцијата на ризик кај носителите на одлуки, односно DMPRCA, додека пристрасноста кон статус кво ја објаснува нивната склоност кон задржување на постојната состојба, што може директно да влијае врз нивото на сајбер-безбедносната подготвеност, односно CPS.

Теоријата на перспективи, обезбедува увид во причините поради кои носителите на одлуки може да донесуваат нецелосно рационални одлуки кога исходите се претставени во различни рамки на добивки и загуби. Базерман [52] го анализира ефектот од ваквото претставување и утврдува дека носителите на одлуки имаат тенденција да избегнуваат ризик кога состојбите се позитивно претставени, додека при негативно претставени состојби покажуваат поголема склоност кон преземање ризик.

Дополнително, авторите на [51] покажуваат дека задржувањето на статус кво често претставува една од можните опции при донесувањето одлуки, што се поврзува со пристрасноста кон статус кво и со феноменот на избегнување загуба. Според нив, вредносната функција прикажана на сликата 7 ја илустрира примената на теоријата на перспективи во процесот на донесување одлуки. Референтната точка го претставува пресекот помеѓу субјективната вредност на перципираната добивка или загуба и состојбата што се смета за нормална, очекувана или почетна.



Слика 7: Илустрација на вредносна функција според Тверски и Кахнеман, адаптирано од [51]

На хоризонталната оска се прикажани загубите и добивките, додека вертикалната оска ја прикажува субјективната вредност што носителот на одлука им ја припишува на тие исходи. Клучната идеја е дека исходите не се оценуваат според нивната апсолутна вредност, туку според тоа дали се перципираат како добивка или загуба во однос на референтната точка.

Кривата има три значајни карактеристики. Прво, загубите имаат поголема психолошка тежина од добивките, што се гледа преку пострмната лева страна на кривата. Овој ефект се означува како аверзија кон загуба (анг. Loss Aversion). Второ, вредноста не се менува линеарно, односно секоја дополнителна добивка или загуба има различен маргинален ефект врз субјективната вредност. Трето, референтната точка има клучна улога, бидејќи ист исход може да се доживее како добивка или како загуба, во зависност од почетната состојба од која се оценува.

Во контекст на оваа дисертација, овие концепти се поврзуваат со однесувањето на организациите кон сајбер-безбедноста. На пример, носителите на одлуки може да ја третираат инвестицијата во сајбер-безбедноста како трошок или загуба во однос на тековната состојба, наместо како механизам за заштита од поголема идна загуба. Поради тоа, организациите може да го задржат статус квото, иако реалниот сајбер-ризик е значаен. Ова ја објаснува врската помеѓу пристрасноста кон статус кво и рамката CyPRisT: организациите не реагираат само според објективното ниво на ризик, туку и според начинот на кој го перципираат ризикот, загубата и потребата за промена.

Сајбер-безбедносна подготвеност

Нивото на сајбер-безбедносна подготвеност (CPS) претставува композитна мерка за управување со ризик, која ги опфаќа аспектите на подготвеност и отпорност на

организацијата. Проценката на оваа величина се базира на активностите дефинирани во NIST Cybersecurity Framework [53], каде што тие се групирани во пет основни функции: идентификувај (анг. Identify), заштити (анг. Protect), детектирај (анг. Detect), одговори (анг. Respond) и обнови (анг. Recover).

Активностите од рамката се трансформирани во прашања преку итеративен процес базиран на Делфи (Delphi) методот, во кој учествувале експерти од областа. Во текот на овој процес, прашањата биле валидирани и дополнително тежински вреднувани [6]. Како резултат на тоа, дефинирани се 70 прашања со бинарни одговори (Yes = 1 / No = 0), распределени во рамките на петте функции на NIST.

Секое прашање е придружено со тежински фактор кој ја одразува неговата релативна важност, определена од страна на експертите со користење на Ликертовата скала со седум степени. Крајниот резултат се изразува преку величината CPS, која има вредност во интервалот [0, 5]. CPS се пресметува како нормализиран збир по функциите на NIST, при што се сумираат производите помеѓу бинарните одговори на прашањата и нивните соодветни тежински фактори.

Перципиран ризик од сајбер-напад кај носителите на одлуки

Параметарот DMPRCA ја претставува субјективната проценка на ризикот од сајбер-закани од страна на лицата што носат одлуки во организацијата.

Во рамките на студијата [6], чиј истражувачки инструмент е избран за мерење и компаративна анализа во оваа дисертација, ризикот се проценува преку комбинација од перципираното влијание и перципираната веројатност за појава на сајбер-закани.

Во таа насока, дефинирани се 10 категории на сајбер-напади, базирани на класификацијата предложена од [54]: General malware, Advanced malware/zero-day attack, Compromised/stolen devices, Cross-site scripting, Denial of service, Malicious insider, Phishing/social engineering, SQL injection, Web-based attack и Other.

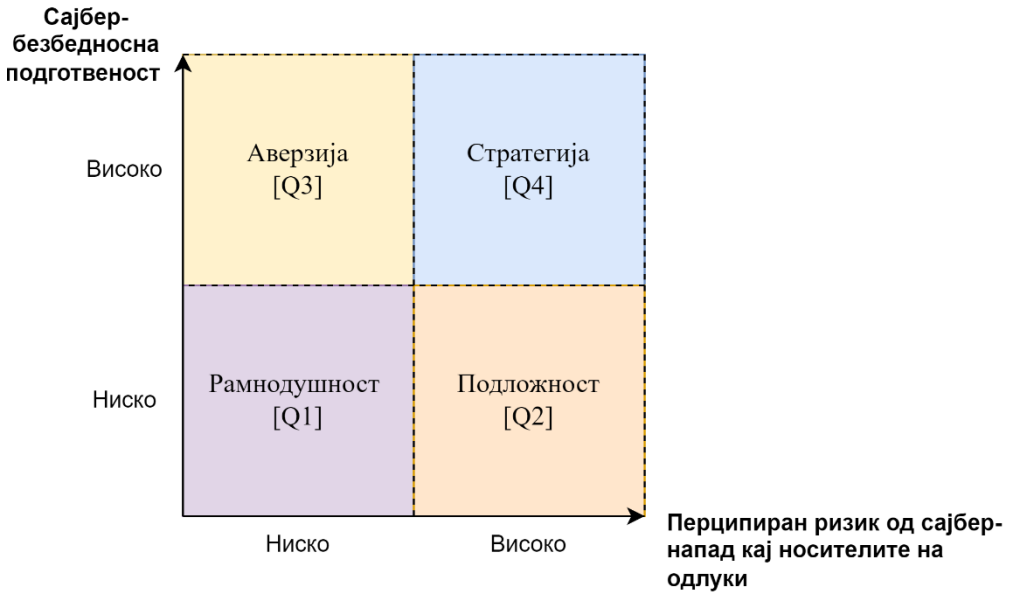
За секоја од наведените категории, формулирани во вид на прашања, се мери перципираната веројатност и перципираното влијание со користење на Ликертовата скала со седум степени. Потоа, за секоја категорија се пресметува производот помеѓу веројатноста и влијанието (likelihood × impact), при што конечната вредност се добива како просек од сите категории.

Добиената вредност се нормализира и се изразува во проценти, при што се дефинира како DMPRCA. За разлика од CPS, кој го одразува нивото на имплементирани активности и мерки за сајбер-безбедносна подготвеност, DMPRCA ја одразува субјективната перцепција на ризик кај носителите на одлуки.

4.3. CyPRisT (таксономија за проценка на сајбер-безбедносната состојба)

Комбинацијата на CPS како мерка за сајбер-безбедносна подготвеност и DMPRCA како мерка за перципиран ризик овозможува формирање дводимензионална социотехничка рамка за анализа на сајбер-безбедносната состојба на организациите. Со позиционирање на организациите според овие две величини, CyPRisT овозможува нивна класификација во четири квадранти, како што е прикажано на слика 8. На овој начин се добива

репрезентативен приказ на односот помеѓу реалното ниво на сајбер-безбедносната подготвеност и субјективната перцепција на ризик кај носителите на одлуки.



Слика 8: Cybersecurity Preparedness-Risk Taxonomy – CyPRisT, според Eilts (2020)

Првиот квадрант (Q1), рамнодушност (анг. Indifference), се карактеризира со ниско ниво на сајбер-безбедносна подготвеност и низок перципиран ризик. Во оваа состојба, носителите на одлуки покажуваат склоност кон задржување на статус квото и не преземаат доволно активности за подобрување на безбедноста, што ја изложува организацијата на зголемен ризик од сајбер-инциденти.

Вториот квадрант (Q2), подложност (анг. Susceptible), се карактеризира со висок перципиран ризик, но ниско ниво на сајбер-безбедносна подготвеност. Иако постои свесност за потенцијалните закани и последици, организацијата не имплементира соодветни мерки за нивно ублажување, што укажува на недоволно ефикасно управување со ризик.

Третиот квадрант (Q3), аверзија кон загуба (анг. Aversive), се карактеризира со високо ниво на сајбер-безбедносна подготвеност, но релативно низок перципиран ризик. Во овој случај, организацијата има имплементирано безбедносни мерки, но понатамошното подобрување може да биде ограничено поради намалената перцепција на ризик, што може да доведе до стагнација во управувањето со безбедноста.

Четвртиот квадрант (Q4), стратешки пристап (анг. Strategic), претставува состојба со високо ниво на сајбер-безбедносна подготвеност и висок перципиран ризик. Во оваа состојба постои усогласеност помеѓу разбирањето на ризикот и имплементацијата на соодветни безбедносни мерки, што резултира со проактивно и ефективно управување со сајбер-безбедноста.

Примена на CyPRisT во ова истражување

Следејќи ја оваа методолошка рамка, во ова истражување се реализира систематска квантитативна проценка на сајбер-безбедносната состојба на малите организации во Република Македонија, како и компаративна анализа со резултатите добиени во Европската Унија и Соединетите Американски Држави.

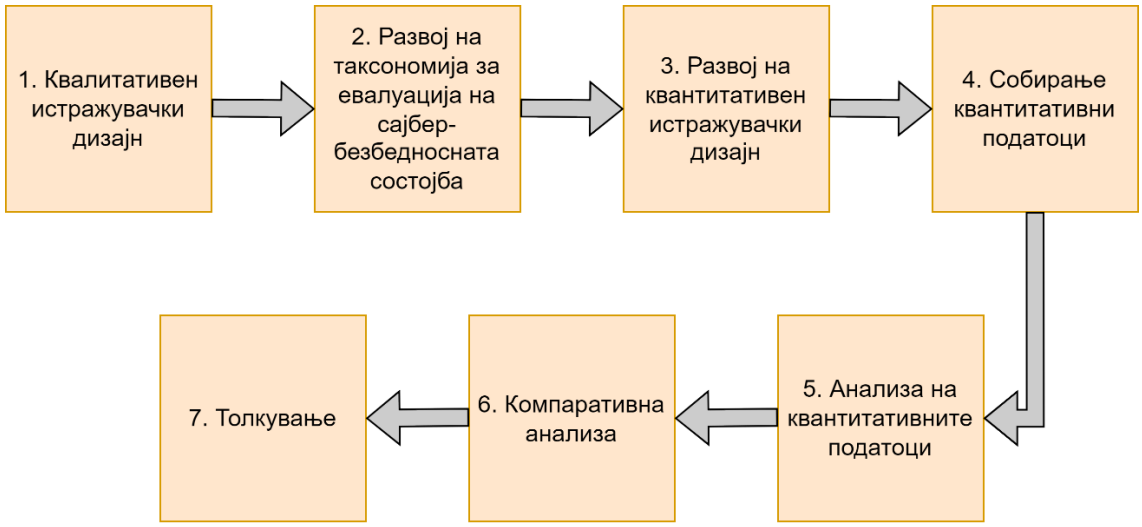
Како референтни извори за компарација се користат резултатите од Агенцијата за сајбер безбедност на Европската Унија (анг. The European Union Agency for Cybersecurity - ENISA) презентирани во [55] и [6]. Со цел да се обезбеди споредливост на резултатите, во ова истражување е применет истражувачкиот инструмент развиен во [6].

4.4. Методологија на истражувањето

Ова истражување е реализирано низ седум последователни фази, со цел да се даде одговор на следните истражувачки прашања:

1. Каква е сајбер-безбедносната состојба на малите организации во Република Македонија?
2. Дали постои значајна разлика во споредба со состојбата во Европската Унија и Соединетите Американски Држави?

Прегледот на фазите на истражувањето е прикажан на слика 9.



Слика 9: Фази на истражувачката постапка

Во првата фаза е дефиниран квалитативниот истражувачки пристап и формулирани се истражувачките прашања врз основа на релевантна научна литература. Притоа е утврдено дека истражувањето треба да биде усогласено со современите научни сознанија и практика во оваа област во Европската Унија и Соединетите Американски Држави.

Во втората фаза е избрана и адаптирана соодветната таксономија за евалуација на сајбер-безбедносната состојба, додека во третата фаза е дефиниран квантитативниот истражувачки дизајн. Во таа насока, применет е истражувачкиот инструмент предложен во

[6], со цел да се овозможи релевантна компарација со резултатите добиени во Европската Унија и Соединетите Американски Држави.

Во четвртата фаза е спроведено прибирање квантитативни податоци, по што во петтата фаза е извршена нивна статистичка анализа. Истражувањето е реализирано врз примерок од 20 мали организации во Република Македонија.

Во шестата фаза е извршена компаративна анализа со резултатите од сродни истражувања спроведени во Европската Унија и Соединетите Американски Држави, додека во седмата фаза се изведени заклучоците и дефинирани се насоките за понатамошно унапредување на сајбер-безбедносната состојба, како и препораки за идни истражувања.

Во продолжение е даден опис на најзначајните елементи на применетата таксономија и истражувачкиот инструмент.

Применетата методологија е реализирана преку онлајн анкетен инструмент, со цел да се изврши квантитативна проценка на сајбер-безбедносната состојба на малите организации во Република Македонија. Во истражувањето се вклучени организации од различни индустриски сектори. Прибирањето на податоците е спроведено во периодот од ноември 2022 до март 2023 година, при што организациите се контактирани по телефон, електронска пошта и преку директни посети.

Пред спроведувањето на анкетата, носителите на одлуки се информирани дека учеството е анонимно и дека резултатите ќе бидат презентирани исклучиво во сумирана и статистичка форма. Со цел да се обезбеди валидност на податоците, анкетата е спроведувана само во случаи кога е утврдена соодветна мотивираност за учество.

Во литературата постојат различни препораки за големината на примерокот во квантитативни истражувања, при што предложените вредности варираат од 20 до 40 или повеќе испитаници [56], [57], [58]. Во рамките на ова истражување е избран примерок од 20 организации, што се смета за соодветно со оглед на природата на истражувањето, сложеноста на процесот на прибирање податоци и ресурсните ограничувања.

Големината на примерокот е дополнително валидирана преку статистички пристап базиран на степенот на прецизност и нивото на доверба, со примена на релацијата:

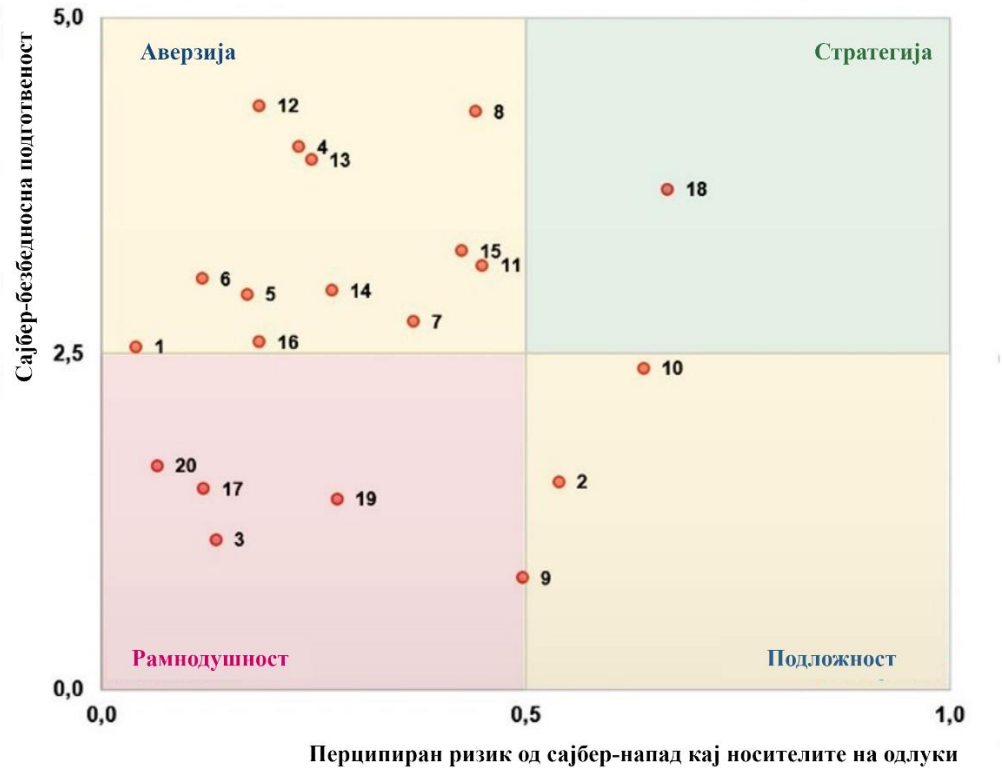
$$n = \left(\frac{z \cdot \sigma}{e}\right)^2 \qquad (31)$$

каде што n ја претставува големината на примерокот, $z = 1{,}96$ за ниво на доверба од 95 %, σ е стандардната девијација, а e е стандардната грешка. За величината CPS е добиена вредност $n = 20$, при што $\sigma = 1{,}08$, а $e = 0{,}46$. За величината DMPRCA, исто така, е добиена вредност $n = 20$, при што $\sigma = 0{,}188$, а $e = 0{,}0824$.

4.5. Анализа на експерименталните резултати

Податоците прибрани преку претходно опишаниот истражувачки инструмент се квантитативно анализирани, при што се пресметани вредностите на CPS и DMPRCA за секоја од анализираните организации. Добиените вредности се позиционирани во рамките

на CyPRisT, при што DMPRCA е прикажан на хоризонталната оска, а CPS на вертикалната оска, како што е прикажано на слика 10.



Слика 10: Позиционирање на анализираните организации во рамките на CyPRisT

Од слика 10 може да се забележи дека анализираните организации не се рамномерно распределени низ сите квадранти. Поголем дел од организациите се позиционирани во квадрантот на аверзија кон загуба, што укажува на релативно повисоко ниво на сајбер-безбедносна подготвеност при пониско ниво на перципиран ризик. Истовремено, дел од организациите се наоѓаат во квадрантот на рамнодушност, што укажува на ниска подготвеност и ниска перцепција на ризик. Само мал број организации се позиционирани во квадрантите на подложност и стратешки пристап.

Сумираните вредности за сајбер-безбедносната состојба, претставени преку величините DMPRCA и CPS за примерокот од 20 организации, се прикажани преку дескриптивна статистика во табела 1. Во табелата се прикажани минималната и максималната вредност, средната вредност и стандардната девијација за двете анализирани величини.

Количина	N	Min	Max	Средна вредност	Стандардна девијација
DMPRCA	20	0,04	0,67	0,30	0,19
CPS	20	0,84	4,35	2,71	1,08

Табела 1: Дескриптивна статистика за DMPRCA и CPS во Република Македонија

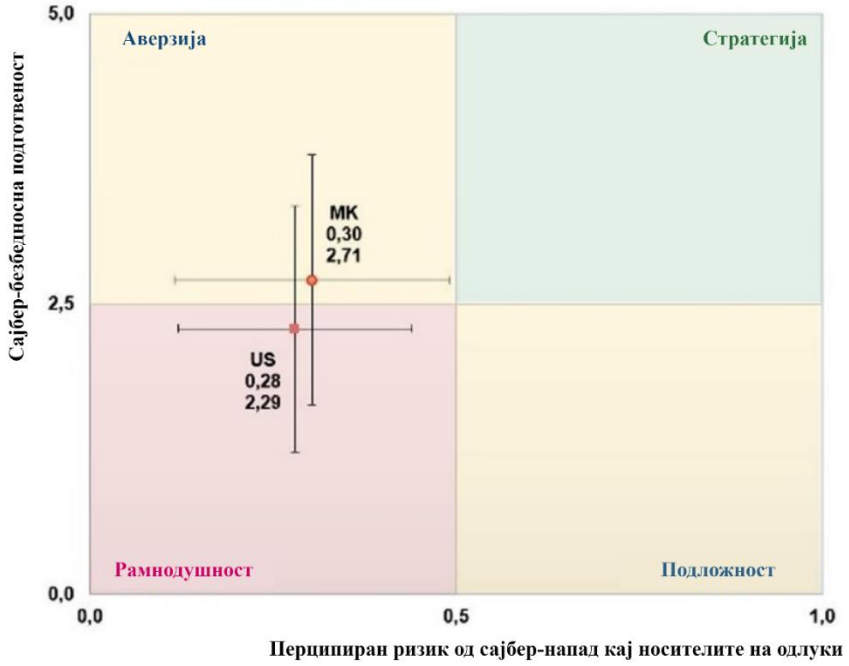
Средната вредност на DMPRCA изнесува 0,30, што укажува на ниско ниво на перципиран ризик од сајбер-напад кај носителите на одлуки. Средната вредност на CPS изнесува 2,71, што укажува на средно ниво на сајбер-безбедносна подготвеност кај анализираниот примерок.

Потоа, добиените резултати од табела 1 се споредени со резултатите презентирани во [6], прикажани во табела 2. Ова овозможува споредбена анализа на сајбер-безбедносната состојба на малите организации во Република Македонија со соодветен примерок од Соединетите Американски Држави.

Количина	N	Min	Max	Средна вредност	Стандардна девијација
DMPRCA	216	0,02	0,85	0,28	0,16
CPS	216	0,14	4,47	2,29	1,06

Табела 2: Дескриптивна статистика за DMPRCA и CPS во Соединетите Американски Држави, според [6]

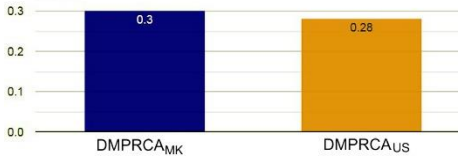
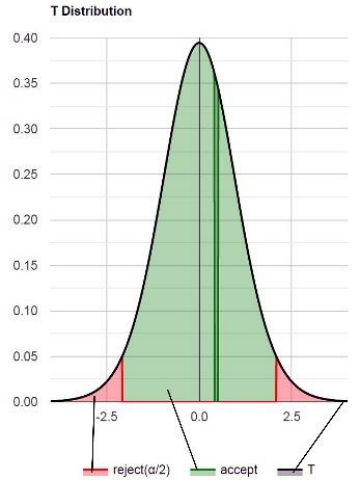
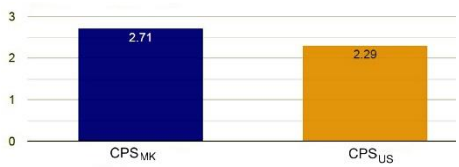
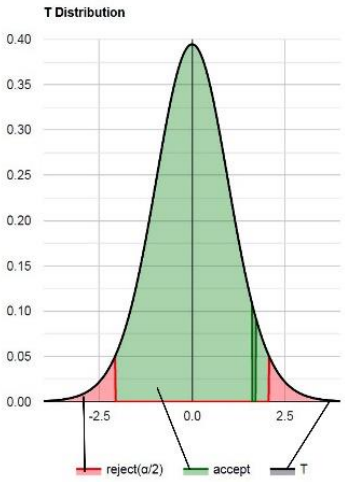
На слика 11 е прикажана компаративната позиција на средните вредности на DMPRCA и CPS во рамките на CyPRisT за примерокот од Република Македонија и споредбениот примерок од Соединетите Американски Држави. Ознаката „MK“ се однесува на резултатите добиени од емпириското истражување спроведено во Република Македонија, додека ознаката „US“ се однесува на резултатите презентирани во [6]. Хоризонталните линии ја претставуваат стандардната девијација на DMPRCA, а вертикалните линии ја претставуваат стандардната девијација на CPS.



Слика 11: Компаративен приказ на вредностите на CyPRisT за Република Македонија и САД, со прикажани стандардни девијации

Резултатите беа анализирани со примена на t-тест за нееднакви варијанси, односно Welch t-тест, за двете величини: DMPRCA и CPS. Целта на оваа анализа беше да се споредат пресметаните средни вредности и да се утврди дали постојат статистички значајни разлики помеѓу примерокот од Република Македонија и споредбениот примерок од Соединетите Американски Држави. При изборот на овој тест беше земено предвид дека станува збор за независни примероци со различна големина и потенцијално различни варијанси. Резултатите од тестот се прикажани во табела 3.

Добиените резултати не покажуваат статистички значајни разлики помеѓу средните вредности $DMPRCA_{MK}$ и $DMPRCA_{US}$, ниту помеѓу CPS_{MK} и CPS_{US}, на ниво на значајност $\alpha = 0{,}05$. Сепак, дескриптивно може да се забележи дека примерокот од Република Македонија има нешто повисоки средни вредности и кај DMPRCA и кај CPS. Ваквата распределба ја поместува просечната позиција на примерокот кон квадрантот на аверзија кон загуба во рамките на CyPRisT.

 	 
α=0.05 *df*=21.5688 (двостран тест) Бидејќи *p*-value > *α*, H_0 не може да биде одбиен *p*-value = 0.6529 *T* = 0.456 $\overline{\text{DMPRCA}_{\text{MK}}} - \overline{\text{DMPRCA}_{\text{USA}}}$=0.02 Стандардна девијација на разликата, S' = 0.0439 Набљудуваниот ефект d е мал, 0.12	α=0.05 *df*=22.5247 (двостран тест) Since *p*-value > *α*, H_0 не може да биде одбиен *p*-value = 0.1095 *T* = 1.6664 $\overline{\text{CPS}_{\text{MK}}} - \overline{\text{CPS}_{\text{USA}}}$==0.42 Стандардна девијација на разликата, S' = 0.252 Набљудуваниот ефект d е мал, 0.4

Табела 3: Резултати од t-тест за два независни примероци со нееднакви варијанси, со примена на t-дистрибуција

Дополнително, беше извршена и квалитативна споредбена анализа со резултатите презентирани во [55], каде што се прикажани наодите од студија која опфаќа 249 мали и средни претпријатија од 25 земји членки на Европската Унија. Ниската вредност на $DMPRCA_{MK}$ се совпаѓа со заклучокот во [55] дека голем дел од малите и средни претпријатија не го препознаваат целосно потенцијалниот ризик од сајбер-безбедносните закани за нивното работење. Истовремено, средното ниво на CPS_{MK} е во согласност со наодите во [55], според кои малите и средни претпријатија најчесто имплементираат дел од основните мерки за сајбер-безбедност, било како дел од нивната општа ИТ-инфраструктура било како резултат на законски и регулаторни обврски.

4.6. Заклучок

Ова истражување обработува прашања што се релевантни и значајни за областа на безбедноста на информациските системи, со посебен фокус на сајбер-безбедносната состојба кај малите организации. Во рамките на истражувањето се презентирани наоди кои вклучуваат квантитативно мерење на тековната сајбер-безбедносна состојба во Република Македонија, како и квантитативна и квалитативна споредба со резултати добиени во сродни студии спроведени во Европската Унија и Соединетите Американски Држави.

Резултатите покажуваат дека помалку од една четвртина од анализираните мали организации во Република Македонија се позиционирани во квадрантот на рамнодушност кон сајбер-безбедноста. Во споредба со резултатите од Соединетите Американски Држави, каде што повеќе од половина од малите и средни претпријатија се позиционирани во оваа група, ова претставува поповолен резултат. Дополнително, само мал број организации се класифицирани во квадрантот на подложност, односно во состојба која се карактеризира со висок перципиран ризик, но ниско ниво на сајбер-безбедносна подготвеност. Овој наод е во согласност со резултатите од сродните студии спроведени во Соединетите Американски Држави и Европската Унија.

Најголемиот дел од организациите во Република Македонија се позиционирани во квадрантот на аверзија кон загуба, што укажува на релативно повисоко ниво на сајбер-безбедносна подготвеност при пониско ниво на перципиран ризик. Овој резултат може да се толкува како показател дека постојните регулативи и практикубања, особено во банкарскиот и ИТ-секторот, имаат позитивно влијание врз имплементацијата на основни безбедносни мерки. Сепак, ниската перцепција на ризик укажува дека носителите на одлуки сè уште не се доволно насочени кон проактивно управување со сајбер-заканите. Наодите, исто така, покажуваат дека речиси и не постојат организации кај кои е постигната стратешка рамнотежа помеѓу разбирањето на сајбер-ризикот и спроведувањето соодветни безбедносни активности, што е во согласност со заклучоците од студиите спроведени во Европската Унија и Соединетите Американски Држави.

Значајна практична импликација од ова истражување е потребата од понатамошен развој на програми и иницијативи кои ќе им помогнат на малите организации да ја подобрат својата сајбер-безбедносна состојба. Особено важно е да се зголеми свесноста кај носителите на одлуки за реалните сајбер-ризици и за потребата од нивно систематско управување, паралелно со фокусот на примарните деловни активности. На овој начин може да се поттикне поактивен и постратешки пристап кон намалување на сајбер-безбедносните ризици.

4.6.1. Препораки за идни истражувања

Имајќи ги предвид обемот и ограничувањата на ова истражување, се отвора простор за понатамошна и подетална анализа на сајбер-безбедносната состојба кај малите организации. Како особено значајни насоки за идни истражувања може да се издвојат:

- зголемување на големината на примерокот, односно бројот на анализирани организации;
- подетална статистичка анализа во однос на демографските и организациските карактеристики, како што се индустрискиот сектор, бројот на вработени, годините на работење, годишниот приход и буџет за ИТ;
- анализа на CPS и DMPRCA во однос на индустрискиот сектор, бројот на вработени и буџетот за ИТ;
- анализа на DMPRCA во однос на перципираната веројатност од сајбер-напад според различни вектори на напад;
- анализа на CPS во однос на перципираното влијание од сајбер-напад според различни вектори на напад.

4.7. Употребна вредност

Спроведеното истражување за сајбер-безбедносната поставеност кај малите организации има значајна употребна вредност во средини каде што е потребно структурирано согледување на сајбер-безбедносната состојба. Преку примената на таксономијата за проценка на сајбер-безбедносната состојба (CyPRisT) се обезбедува квантитативна рамка за проценка на односот помеѓу сајбер-безбедносната подготвеност и перципираниот ризик од сајбер-напади кај носителите на одлуки.

Со класификација на организациите врз основа на CPS и DMPRCA, CyPRisT овозможува идентификација на различни профили на сајбер-безбедносна поставеност. На овој начин се добиваат сознанија за организациските и човечките фактори кои влијаат врз управувањето со ризикот и имплементацијата на безбедносни мерки. Ова е особено релевантно за малите организации, кои често функционираат со ограничени ресурси, ограничена експертиза и недоволно развиени интерни капацитети во областа на сајбер-безбедноста.

Емпириските наоди за Република Македонија укажуваат на средно ниво на сајбер-безбедносна подготвеност и ниско ниво на перципиран ризик. Овој однос укажува на постоење јаз помеѓу реалните безбедносни потреби и свесноста на носителите на одлуки за сајбер-ризиците. Ваквите сознанија можат да се применат во реални организациски средини за поддршка на донесување одлуки базирани на ризик, приоритизирање на инвестициите во сајбер-безбедноста и идентификување организации кои се потенцијално ранливи поради когнитивни пристрасности, како што се пристрасноста кон статус кво и аверзијата кон загуба.

Предложениот пристап не е применлив само за академска анализа, туку може да служи и како практична алатка за подобрување на управувањето со сајбер-безбедноста, зголемување на организациската отпорност и поддршка на континуираната евалуација на безбедносната поставеност кај малите организации.

5. Тестна околина на интегриран центар за мрежни операции и центар за безбедносни операции базиран на алатки со отворен код

Во претходната глава беа анализирани клучните аспекти на сајбер-безбедносната состојба кај малите организации во Република Македонија, со посебен фокус на однесувањето на носителите на одлуки и нивната перцепција на ризик. Преку квантитативна и квалитативна анализа, како и преку споредба со релевантни студии од ЕУ и САД, беа идентификувани значајни трендови, вклучувајќи ја доминантната склоност кон аверзија кон загуба и недоволната стратешка рамнотежа во управувањето со сајбер-ризиците. Овие наоди укажуваат на постоење одреден степен на регулаторна усогласеност, но и на потреба од понатамошно унапредување на свесноста, техничката подготвеност и практичниот пристап кон сајбер-безбедноста, особено кај малите организации.

Врз основа на овие согледувања, оваа глава се насочува кон практична имплементација на концепти кои може да придонесат за подобрување на сајбер-безбедносната состојба во организациските ИТ-околини. Поточно, се воведува пристап базиран на развој на тестна ИТ-околина (анг. testbed), која овозможува безбедно експериментирање, анализа и евалуација на мрежни закани и одбранбени механизми. Во овој контекст се разгледуваат методологии и технологии за изградба на вакви околини, како и нивната улога во поддршка на системи за детекција на упади, вклучувајќи IDS-решенија базирани на машинско учење и вештачка интелигенција, со цел поефикасно и проактивно управување со сајбер-заканите.

Сајбер-безбедносните пробиви претставуваат значајна закана за ИТ-мрежната инфраструктура, предизвикувајќи финансиски загуби, нарушување на оперативното функционирање и сериозни негативни последици врз репутацијата на организациите. Ова ја нагласува потребата секоја организација да воспостави соодветни механизми за заштита на својата инфраструктура преку континуирано следење, евалуација и унапредување на мрежните системи. Еден пристап за постигнување на оваа цел е воспоставување посебна ИТ-мрежна околина, односно тестна околина, која ги рефлектира потребите, ограничувањата и параметрите на реалната продукциска ИТ-мрежна инфраструктура.

Тестната околина треба да функционира како контролирана и изолирана средина за непречена евалуација на сајбер-безбедносната состојба на организацијата. Потребата од ваков пристап беше јасно демонстрирана во 2024 година преку инцидентот поврзан со CrowdStrike, каде што системските ажурирања кои не биле соодветно тестирани предизвикаа значително нарушување на ИТ-инфраструктурата на глобално ниво, влијаејќи врз голем број организации од различни индустриски сектори [59].

Покрај овозможувањето побезбедна дистрибуција и проверка на системски и мрежни ажурирања, постоењето на тестна мрежа обезбедува сигурна околина за тестирање различни сценарија на мрежни закани и за евалуација на стратегии за нивно ублажување. Ваквите околини може да бидат развиени во помал обем, но треба да ја рефлектираат реалната конфигурација и логика на продукциската ИТ-мрежа. Знаењата и вештините стекнати во тестни околини може директно да се применат во продукциски или поголеми мрежни системи. Овој пристап придонесува кон воспоставување концепти, методологии и

добри практикувања кои може да се имплементираат во реални ИТ-околини, обезбедувајќи практична основа за истражување, тестирање и унапредување на сајбер-безбедносните механизми. Клучни пристапи за изградба на вакви тестни околини вклучуваат виртуелизација на ресурси, симулација на околина, емулација на мрежи, изолирано извршување (анг. sandboxing), симулација со хардвер во јамка (анг. hardware-in-the-loop – HIL) и други сродни техники.

Една од главните предности на безбедна и контролирана околина за тестирање мрежни закани е можноста за анализа на мрежниот сообраќај со цел детекција на аномалии и малициозни активности. Воведувањето тестна ИТ-околина овозможува подобро разбирање на нормалниот мрежен сообраќај и идентификација на неочекувани или потенцијално опасни однесувања. Како клучна активност во сајбер-безбедноста, анализата на мрежниот сообраќај опфаќа следење и обработка на тековите на податоци со цел откривање безбедносни ранливости, сомнителни активности и неправилности во функционирањето на системот. Дополнително, ваквата анализа овозможува длабински увид во различни типови мрежни протоколи, комуникациски обрасци и трендови во рамките на ИТ-околината. Овие аспекти придонесуваат за поефикасна употреба на алатки за мониторинг, анализа на логови и идентификација на безбедносни проблеми, а стекнатите сознанија може понатаму да се применат во реални сценарија за справување со сајбер-напади во организациски мрежи.

Во рамките на ова истражување се предлага тестна ИТ-инфраструктура базирана на алатки со отворен код, која овозможува прибирање мрежен сообраќај и системски логови за понатамошна анализа во рамките на системи за детекција на упади. Притоа, собраните податоци може да се користат како основа за примена на алгоритми од машинско учење и вештачка интелигенција (анг. Artificial Intelligence – AI) за препознавање на аномалии и малициозни активности. Предложената тестна околина овозможува мониторинг, управување и конфигурирање на мрежни уреди и системи, при што пристапот се базира на современи насоки за развој на интегрирани центри за мрежни операции (анг. Network Operations Center – NOC) и безбедносни оперативни центри (анг. Security Operations Center – SOC) [60].

5.1. Поврзана работа и дискусија

Основите за изградба на тестни околини за ИТ-мрежи се поставени во 1980-тите и 1990-тите години, кога започнуваат првите истражувања поврзани со компјутерски базирани мрежни симулации. Авторите во [61] и [62] предложиле развој на мрежни симулатори за истражувачки цели. Подоцна, авторите во [63], [64] и [65] ја идентификувале потребата од дополнителни алатки и техники за едукација, тестирање и истражување во областа на мрежната безбедност. До крајот на 1990-тите години, овие истражувања придонеле за развој на мрежни симулатори како NS-2 и OPNET Modeler, денес познат како Riverbed Modeler.

Со појавата и развојот на технологиите за виртуелизација, значително се проширили можностите за креирање тестни околини, овозможувајќи интеграција на реалните системи и сервиси во рамките на контролираните тестни инфраструктури, со пониски трошоци за имплементација. Голем број истражувачи ги препознале предностите на тестните околини за мрежна безбедност, особено за тестирање, анализа и валидација на новите концепти. Во 2007 година, авторите во [66] предложиле употреба на софтверска виртуелизација за дизајн

на виртуелна мрежна тестна околина, која овозможува изолирано извршување на потенцијално опасен код во рамките на истражувачките и развојни експерименти. Слични пристапи подоцна се предложени и во [67], [68] и [69].

Овие можности, во комбинација со реалните уреди и сервиси, довеле до поширока примена на тестните околини во истражувањата поврзани со детекција на аномалии во ИТ-мрежите и справување со сајбер-закани. Развиени се различни тестни околини наменети за генерирање логови и прибирање мрежен сообраќај, со цел развој и евалуација на системи за детекција на упади (IDS). На пример, Шарафалдин и сор. [70] развиле мрежна околина со реални уреди, во која биле имплементирани различни сервиси, како заштитни ѕидови, сервери, кориснички уреди и мрежни прекинувачи. Оваа конфигурација овозможила изведување на различни типови напади и класификација на прибраниот мрежен сообраќај. За разлика од претходните пристапи, нивното решение користи реална инфраструктура, но истовремено вклучува и виртуелна околина.

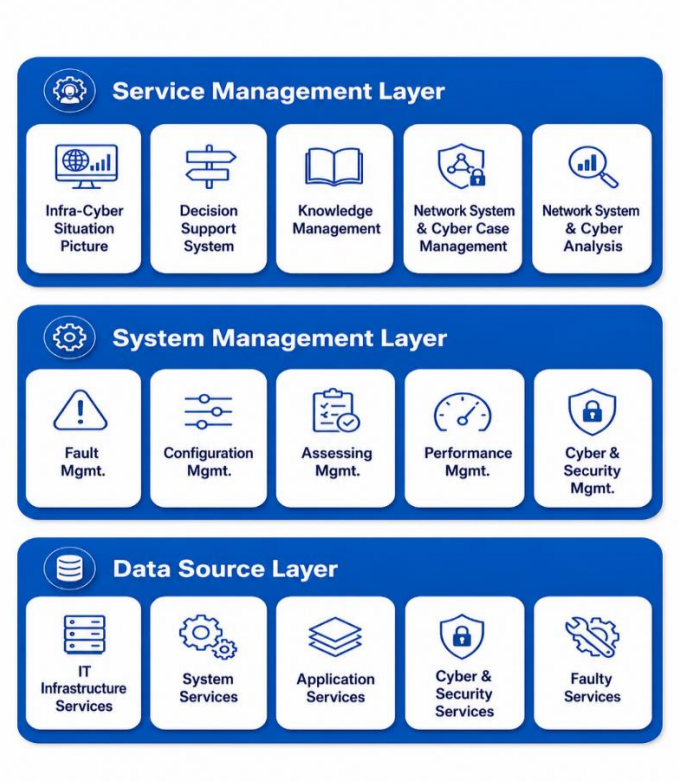
Ринг и сор. [71] предложиле инфраструктура која ја претставува мрежата на мала организација, вклучувајќи веб-сервери, сервери за електронска пошта, датотечни сервери и сервери за резервни копии. Во нивниот пристап, нормалното однесување на корисниците е симулирано преку скрипти, а дополнително се изведени и различни типови напади. Иако нивната мрежа е поврзана со интернет, репродуцибилноста на тестовите е ограничена. Во предложениот пристап во оваа дисертација, тестната околина е исто така поврзана со интернет, но мрежниот сообраќај се филтрира преку заштитен ѕид, со што се обезбедува контролирана и безбедна тестна средина.

Во 2022 година, авторите во [72] предложиле систематски пристап за интеграција на SOC во сајбер-безбедносни експерименти, вклучувајќи процеси на евалуација и тестирање. Притоа, бил предложен референтен SOC-модел, како и различни софтверски дистрибуции соодветни за имплементација во *cyber range* околини, заедно со насоки и методологија за спроведување ригорозни експерименти, вклучувајќи и експерименти со човечки оператори. Ова истражување го проширува тој опфат преку имплементација на интегриран NOC и SOC, со посебен фокус на дефинирање и примена на алатки со отворен код во рамките на тестна ИТ-околина.

5.2. Интегриран NOC и SOC базиран на отворен код

Воведувањето на елементи на NOC и SOC во организациските ИТ-мрежи овозможува централизирано следење на перформансите, безбедноста и оперативната состојба на имплементираните ресурси. Интеграцијата на овие два концепта ги комбинира нивните придобивки, при што се овозможува поефикасно управување со мрежната инфраструктура, подобра видливост на безбедносните настани и потенцијално намалување на трошоците за имплементација и одржување. Во рамките на ова истражување се предлага тестна ИТ-архитектура која ги следи современите насоки презентирани во [60], како што е прикажано на слика 12.

Предложената архитектура се состои од три слоја: слој на извори на податоци (анг. Data Source Layer – DSL), слој за управување со системи (анг. System Management Layer – SyML) и слој за управување со сервиси (анг. Service Management Layer – SML). Секој од овие слоеви има специфична улога во процесот на прибирање, обработка, анализа и користење на податоците за управување со перформансите и безбедноста на мрежата.



Слика 12: Архитектура на интегриран NOC и SOC [60]

Слојот на извори на податоци, DSL, ги опфаќа мрежните елементи, системските сервиси, апликациските сервиси, безбедносните компоненти и крајните точки во рамките на инфраструктурата. Овој слој генерира податочни точки од различни извори и ги проследува кон слојот за управување со системи во форма на логови, настани, мерења и други релевантни телеметриски податоци.

Во рамките на слојот за управување со системи, SyML, се спроведува мониторинг во реалното време согласно со моделот FCAPS [73], кој опфаќа управување со дефекти (анг. Fault Management), конфигурација (анг. Configuration Management), администрација или сметководствено следење на ресурси (анг. Accounting Management), перформанси (анг. Performance Management) и безбедност (анг. Security Management). Овој слој овозможува прибирање, обработка и иницијална анализа на логови и настани со цел идентификација на проблемите поврзани со достапноста, конфигурацијата, перформансите и безбедноста на мрежата. Дополнително, SyML генерира алармни и безбедносни настани кои понатаму се проследуваат кон слојот за управување со сервиси.

Слојот за управување со сервиси, SML, претставува највисок слој во архитектурата и е одговорен за поддршка на процесите на донесување одлуки. Овој слој ги прима обработените податоци од SyML и овозможува сеопфатен преглед на состојбата на мрежата и безбедносната поставеност на инфраструктурата. Во рамките на SML се врши собирање, мапирање, корелација и индексирање на логови и настани, со цел поддршка на процесите за управување со инциденти, детекција на закани, ревизија, анализа на влијание, управување со знаење и предвидување на идни состојби и настани.

Овој слоевит пристап кон дизајнот на интегриран NOC и SOC обезбедува јасна основа за избор и имплементација на соодветни алатки во рамките на секој архитектонски слој. Во предложената тестна околина се предвидува употреба на алатки со отворен код, имајќи предвид дека ИТ-заедницата во текот на изминатите години разви стабилни, доверливи и функционално зрели решенија кои можат да се применат во различни сегменти од ваквата архитектура.

Слој за управување со сервиси	OTRS (Open Ticket Request System) Zammad The Hive	MediaWiki Zammad	GLPI / iTop	iTop	GLPI	iTop	OTRS / Zammad	
	Управување со инциденти	**Управување со знаење**	**Управување со средства и конфигурации**	**Управување со ниво на услуги**	**Управување со барања за услуги**	**Управување со промени**	**Управување со проблеми**	
Слој за управување со системи		Prometheus Zabbix	Cockpit phpIPAM	Ansible / Puppet RANCID	Nagios Core / Icinga Zabbix	Shuffle OSSEC Wazuh The Hive		
		Управување со перформанси	**Администрација**	**Управување со конфигурации**	**Управување со дефекти**	**Управување со безбедност**		
Слој за извори на податоци	Elasticsearch Logstash Fluentd Graylog	nProbe ntopng Zeek Suricata	Prometheus Collectd Telegraf	PostgreSQL MySQL/MariaDB MongoDB InfluxDB	Kafka RabbitMQ NATS	Ceph MinIO GlusterFS	Beats Flume Vector	Wireshark tcpdump pcap-ng
	Алатки за собирање и управување со логови	**Алатки за собирање мрежни податоци**	**Алатки за собирање метрики**	**Алатки за собирање и управување со бази на податоци**	**Алатки за собирање настани**	**Алатки за складирање датотеки и објекти**	**Алатки за агрегација на податоци**	**Алатки за снимање мрежни пакети**
	Мрежни елементи	**Мрежни елементи**	**Мрежни елементи**	**Мрежни елементи**	**Мрежни елементи**	**Мрежни елементи**	**Мрежни елементи**	**Мрежни елементи**
	Комутатори, рутери, безбедносни крајни точки, компјутери, лаптопи, телефони, системи/уреди за мониторинг, заштитни ѕидови, мрежен и безбеднос ен хардвер							

Слика 13: Алатки со отворен код за интегриран NOC и SOC

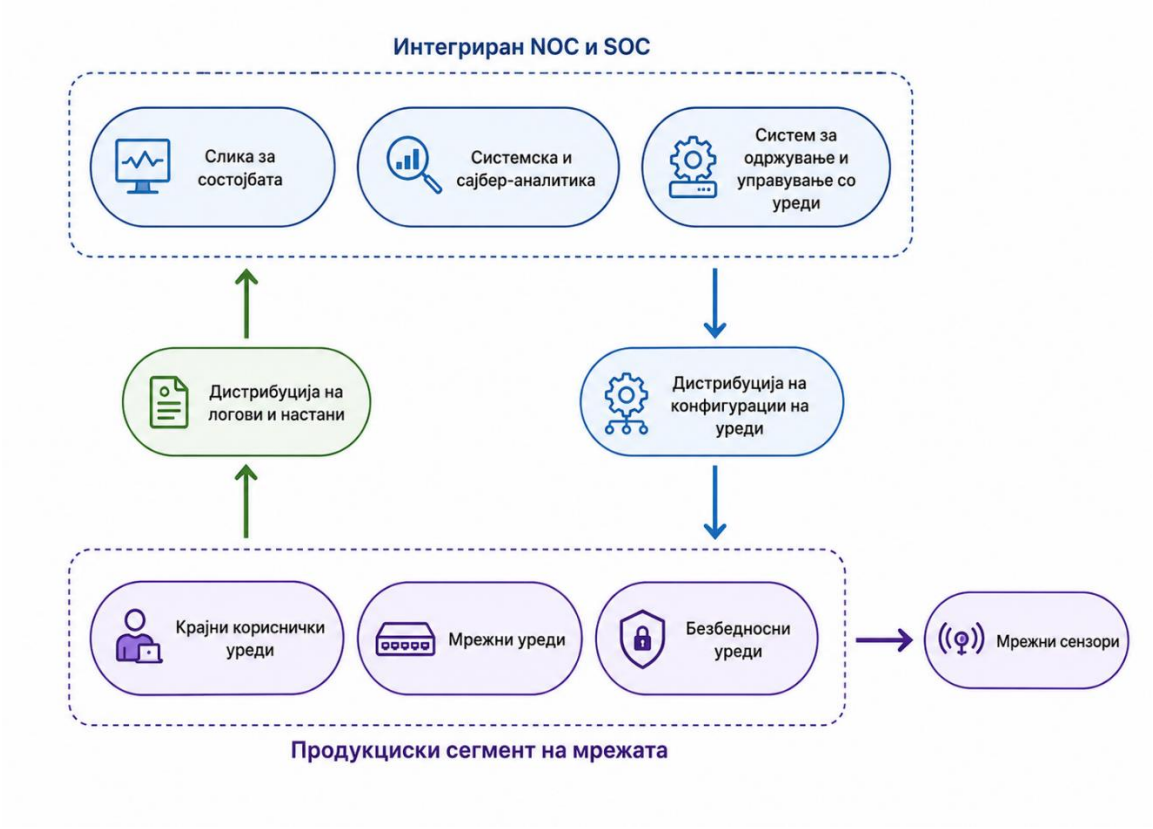
На слика 13 се прикажани алатките со отворен код распределени според слоевите на интегрираната NOC–SOC архитектура, како и нивната функционална поврзаност со соодветните управувачки и оперативни домени. Ваквата распределба овозможува појасно согледување на улогата на поединечните алатки во процесите на прибирање податоци, мониторинг, анализа, управување со настани и поддршка на донесување одлуки.

Потребно е да се нагласи дека одредени алатки, поради нивната архитектура и функционалности, можат да се применуваат во повеќе слоеви или на нивната меѓусебна граница. Сепак, во рамките на предложената архитектура тие се позиционирани во слојот во кој нивната примарна функција доаѓа до најголем израз.

5.3. Тестна околина за ИТ-инфраструктура

Предложената тестна околина е дизајнирана со цел да поддржи истражувања во областа на сајбер-безбедноста, особено во доменот на мониторинг, анализа на мрежен сообраќај и евалуација на механизми за детекција на упади. Таа е наменски конципирана да обезбеди реалистична репрезентација на организациска ИТ-околина, составена од продукциски сегмент на мрежата и интегриран NOC и SOC базиран на алатки со отворен код. Општиот архитектурен приказ на предложената тестна околина е даден на слика 14.

Во предложената архитектура, уредите во продукцискиот сегмент на мрежата се надгледуваат преку прибирање логови, настани и мрежен сообраќај, кои понатаму се проследуваат кон интегрираниот NOC и SOC. На овој начин се овозможува формирање сеопфатна слика за состојбата на системот, како и поддршка на процесите за анализа, корелација и донесување одлуки врз основа на имплементираните аналитички механизми. Донесените одлуки понатаму може да се спроведат преку дистрибуција на конфигурациски команди, правила или датотеки кон соодветните мрежни, крајни и безбедносни уреди. Дополнително, тестната околина предвидува имплементација на различни типови мрежни сензори, кои овозможуваат прибирање дополнителни податоци за потребите на безбедносен мониторинг и понатамошна анализа.



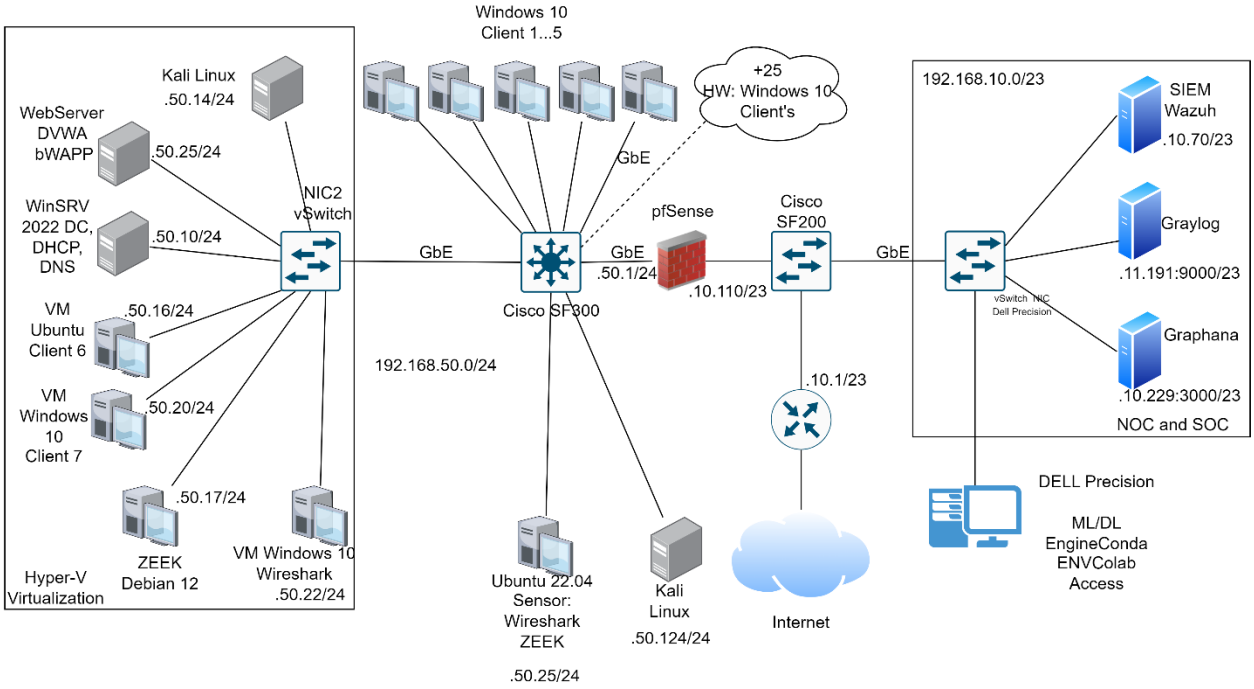
Слика 14: Општ архитектурен приказ на предложената тестна мрежна околина

Со цел да се демонстрира доказ на концепт за предложената ИТ мрежна инфраструктура, во рамките на истражувањето беше имплементирана тестна околина согласно со архитектурата прикажана на слика 15. Имајќи предвид дека Windows Active Directory е широко застапен во организациските ИТ-инфраструктури [74], предложената архитектура е базирана на доменските сервиси на Windows. Ваквата доменска мрежа претставува основа на продукцискиот сегмент на тестната околина и е поврзана со интегрираниот NOC и SOC со цел следење на перформансите, безбедносен мониторинг и управување со мрежните ресурси.

Тестната околина е изградена како комбинација од физички уреди и виртуелни машини (анг. Virtual Machines – VM), при што виртуелните машини се распределени на два наменски физички сервери со користење софтверски решенија со отворен код. За да се овозможи подлабинско истражување и анализа, низ мрежата се распоредени дополнителни сензори. Овие сензори имаат клучна улога во мониторингот и прибирањето детални податочни точки поврзани со мрежните активности, со што се обезбедуваат релевантни податоци за понатамошни сајбер-безбедносни истражувања.

5.3.1. Доменска мрежа

Доменската мрежа во рамките на тестната околина е организирана околу Windows доменот управуван од Windows Server 2022 (WinSRV2022), кој ја извршува функцијата на доменски контролер (анг. Domain Controller – DC). Доменскиот контролер претставува централна компонента одговорна за управување со корисници, уреди, политики за пристап и клучни мрежни сервиси во рамките на доменот. Во доменската мрежа се интегрирани повеќе физички и виртуелни клиентски уреди, со што се овозможува реалистична репрезентација на организациската ИТ-околина.



Слика 15: Архитектура на имплементираната тестна ИТ-инфраструктура

Во рамките на доменот, корисниците се креираат и управуваат преку активниот директориум (анг. Active Directory – AD), при што на секој корисник му се доделуваат соодветни улоги и привилегии кои го дефинираат нивото на пристап до мрежната инфраструктура. Овој модел на контрола на пристап базиран на улоги претставува клучна карактеристика на современите организациски мрежи, бидејќи овозможува доделување права во согласност со работните функции и безбедносните политики на организацијата. Централизираното управување со корисници, уреди и сервиси во рамките на Windows доменската мрежа ја реплицира комплексноста на реалната организациска инфраструктура

и обезбедува соодветна основа за тестирање, мониторинг и истражување во областа на сајбер-безбедноста.

Ваквата поставеност овозможува анализа и експериментирање со различни сајбер-безбедносни сценарија, преку симулирање реални услови, корисничко однесување и потенцијални закани во контролирана и безбедна средина.

5.3.2. Сервиси

Тестната мрежна околина е поддржана од повеќе системски и апликациски сервиси кои овозможуваат реалистична репрезентација на организациска ИТ-инфраструктура. Во рамките на доменската мрежа се имплементирани Active Directory Domain Services (AD DS), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Group Policy, Hyper-V, Network Policy and Access Services (NPAS), веб-сервиси и други придружни сервиси. Ваквата поставеност овозможува симулација на типични организациски функционалности, како централизирано управување со корисници и уреди, доделување мрежни параметри, примена на политики, виртуелизација и обезбедување апликациски услуги.

Архитектурата на тестната околина е модуларна, што овозможува одредени сервиси да бидат отстранети, заменети или дополнително проширени во зависност од целите на експериментот и типот на мрежни активности или напади кои се планира да се генерираат. На тој начин, тестната околина може да се приспособува за различни сценарија на сајбер-безбедносното тестирање, без нарушување на основната архитектонска поставеност.

5.3.3. Безбедност

Мониторингот, известувањето и безбедносната анализа на продукцискиот сегмент на мрежата имаат значајна улога во предложената архитектура. Овие функции се реализираат преку интегрираниот NOC и SOC, кој користи повеќе алатки со отворен код, меѓу кои Wazuh како Security Information and Event Management (SIEM) решение [75], Wazuh XDR за проширена детекција и анализа, Graylog Open 5.0 [76] како систем за управување со логови, OpenSearch [77] како дистрибуиран систем за пребарување и анализа, Grafana [78] за визуализација, како и pfSense [79] како заштитен sид и рутер.

Wazuh претставува SIEM-решение со отворен код кое овозможува централизирано прибирање, корелација и анализа на телеметриски податоци во реално време, со цел детекција на закани и проценка на безбедносната усогласеност. Системот користи Endpoint Detection and Response (EDR) агенти, преку кои се прибираат логови и настани од различни извори во мрежата, вклучувајќи крајни уреди, сервери, мрежни уреди, апликации и други инфраструктурни компоненти. Неговите функционалности опфаќаат анализа на безбедносни логови, детекција на ранливости, проценка на безбедносни конфигурации, следење на усогласеност, генерирање извештаи, алармирање и известување. Во предложената архитектура, Wazuh е поврзан и со Wazuh XDR, кој овозможува проширена детекција и одговор преку анализа на телеметриски податоци од повеќе извори.

OpenSearch се користи како дистрибуиран систем за пребарување, индексирање и анализа на податоци. Во рамките на предложената архитектура, тој овозможува складирање и пребарување на големи количини логови и настани, што е особено значајно за безбедносен мониторинг, анализа на инциденти и визаелизација на состојбата на системот.

Дистрибуираната природа на OpenSearch овозможува поголема скалабилност и поефикасна обработка на податоците во споредба со централизирани решенија со ограничен капацитет.

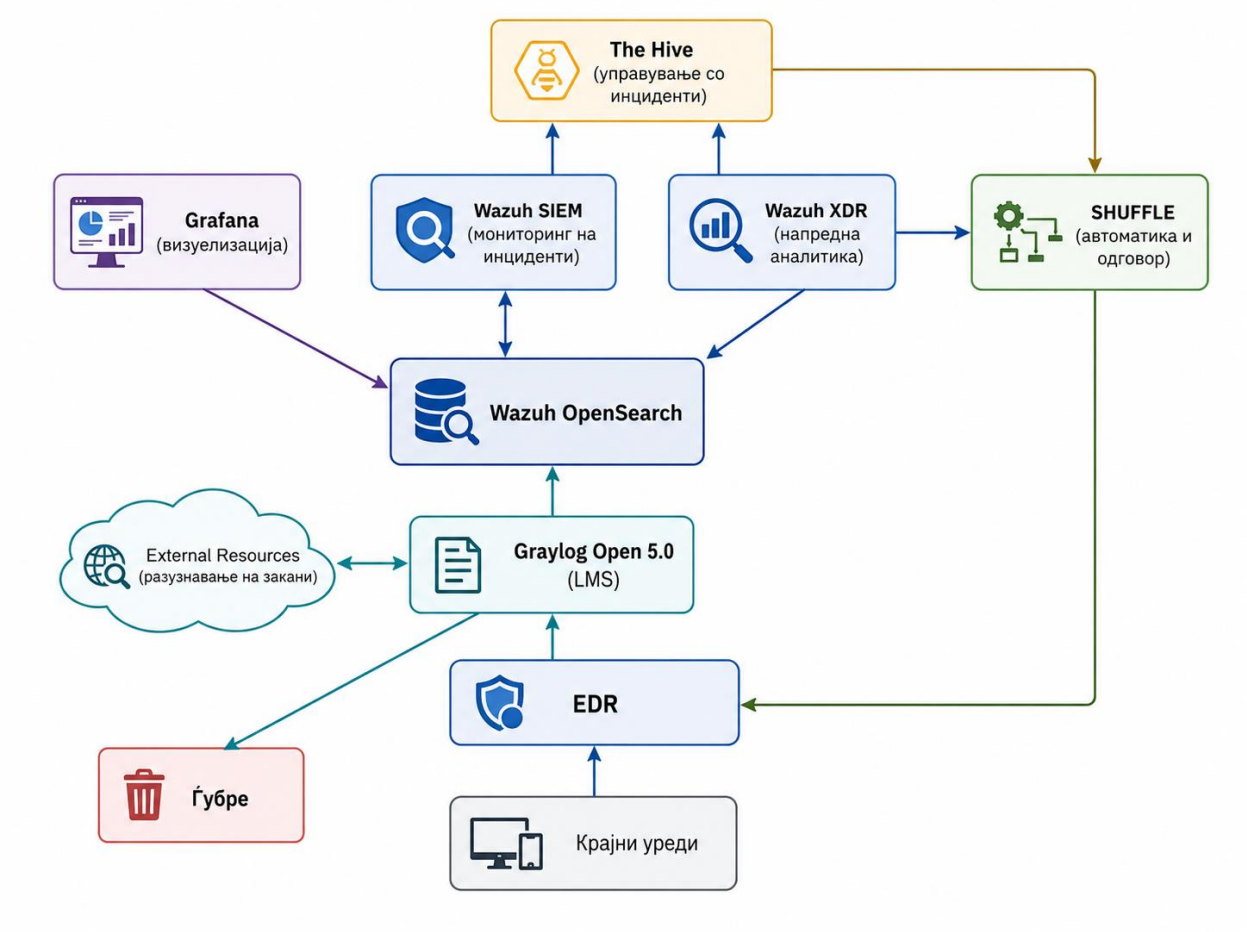
Graylog Open 5.0 претставува централизирана платформа за управување со логови (анг. Log Management System – LMS) со отворен код, која овозможува прибирање, сумирање, парсирање и обработка на податоци од различни уреди, апликации и оперативни системи. Во предложената тестна околина, Graylog има улога на посреднички слој за обработка на логови, при што се отстрануваат непотребните информации, се додаваат релевантни метаподатоци и се подготвуваат податоците за понатамошно внесување, пребарување и анализа. Ваквиот пристап е применлив за форензичка анализа, откривање закани, оперативен мониторинг и поддршка на безбедносни истражувања.

Grafana претставува алатка со отворен код за визуализација и анализа на податоци. Таа овозможува креирање контролни табли, пребарување и визуализација на метрики, логови и временски серии, како и дефинирање аларми врз основа на специфични услови или прагови. Во предложената архитектура, Grafana се користи за визуелно претставување на состојбата на системот и за поддршка на оперативното следење на перформансите и безбедносните настани. Дополнително, нејзиниот систем на додатоци (анг. plugins) овозможува интеграција со различни извори на податоци, вклучувајќи OpenSearch, SQL/NoSQL бази и други мониторинг платформи.

pfSense претставува дистрибуција базирана на FreeBSD со отворен код, која може да функционира како заштитен sид и рутер во рамките на тестната мрежна околина. Решението обезбедува веб-интерфејс за управување и поддржува проширување на функционалностите преку дополнителни софтверски пакети. Неговите функционалности вклучуваат Stateful Packet Inspection, IP/DNS-базирано филтрирање, anti-spoofing механизми, NAT-мапирање, правила базирани на време, ограничување на конекции, IDS/IPS механизми, анализа на пакети и можност за блокирање познати малициозни IP-адреси. Во предложената архитектура, pfSense е позициониран помеѓу мрежните сегменти и овозможува контрола на мрежниот сообраќај, филтрирање на сомнителни комуникации и спречување на ширење малициозен сообраќај кон останатите делови од мрежата.

Протокот на безбедносно релевантни податоци во имплементираната тестна архитектура е прикажан на слика 16. EDR-агентите се имплементирани на крајните уреди и се управуваат преку Wazuh SIEM, од каде што добиваат конфигурациски ажурирања и правила за мониторинг. Логовите и настаните прибрани од крајните уреди се проследуваат кон Graylog Open 5.0, каде што се врши нивно парсирање, филтрирање и збогатување со дополнителни метаподатоци, како на пример информации поврзани со IP-адреси или други индикатори од надворешни извори.

По обработката во Graylog, филтрираните и збогатени податоци се испраќаат кон Wazuh OpenSearch за внесување (анг. ingestion), индексирање и понатамошна анализа. Од овој момент, релевантните податоци стануваат достапни за пребарување, корелација, визуализација и генерирање аларми преку Wazuh SIEM, Wazuh XDR и Grafana. На овој начин се овозможува подобро разбирање на состојбата на системот, детекција на сомнителни активности и поддршка на процесите за управување со безбедносни инциденти.



Слика 16: Проток на безбедносно релевантни податоци во имплементираната тестна архитектура

5.3.4. Сензори

Покрај мониторингот и известувањето реализирани преку SIEM и XDR решенијата, во тестната мрежна околина се интегрирани сензорски уреди на различни локации во мрежата. Нивната улога е да регистрираат мрежни активности и да прибираат податоци за сообраќајот, кои понатаму може да се користат за безбедносна анализа, детекција на аномалии и евалуација на IDS-механизми. За оваа намена, на сензорските уреди се користат алатките Wireshark [80] и Zeek [81].

Wireshark претставува алатка со отворен код за анализа на мрежни пакети, која овозможува детална инспекција на прибраниот мрежен сообраќај. Таа поддржува снимање пакети во реално време од мрежни интерфејси, отворање и анализа на претходно зачувани датотеки со пакети, детална анализа на протоколи, филтрирање и пребарување според различни критериуми, како и извоз на податоци во различни формати. Поради ваквите функционалности, Wireshark е особено погоден за длабинска анализа на поединечни комуникациски сесии, проверка на протоколско однесување и форензичка анализа на мрежни настани.

Zeek претставува пасивен анализатор на мрежен сообраќај со отворен код, кој се користи како систем за мониторинг на мрежна безбедност (анг. Network Security Monitor – NSM). За разлика од алатките што се фокусираат на детална анализа на поединечни пакети, Zeek го интерпретира мрежниот сообраќај и генерира структурирани логови за конекции, протоколи и апликациски активности. Овие логови може да опфаќаат податоци за HTTP-сесии, DNS-барања и одговори, TLS/SSL-сертификати, SMTP-комуникација и други релевантни мрежни активности. Податоците се зачувуваат во структурирани лог-датотеки, како *tab-separated* или *JSON формат*, што ги прави погодни за понатамошна автоматизирана обработка, корелација и анализа.

Во предложената тестна околина, Wireshark и Zeek имаат комплементарна улога. Wireshark овозможува детална анализа на пакети на ниво на рамка и протокол, додека Zeek обезбедува покомпактна и структурирана репрезентација на мрежната активност преку логови. Оваа комбинација овозможува истовремено прибирање детални податоци за конкретни мрежни настани и сумирани информации погодни за понатамошна анализа со алатки за мониторинг, IDS и модели базирани на машинско учење.

5.4. Демонстрација на потенцијалот за мониторинг во тестната околина

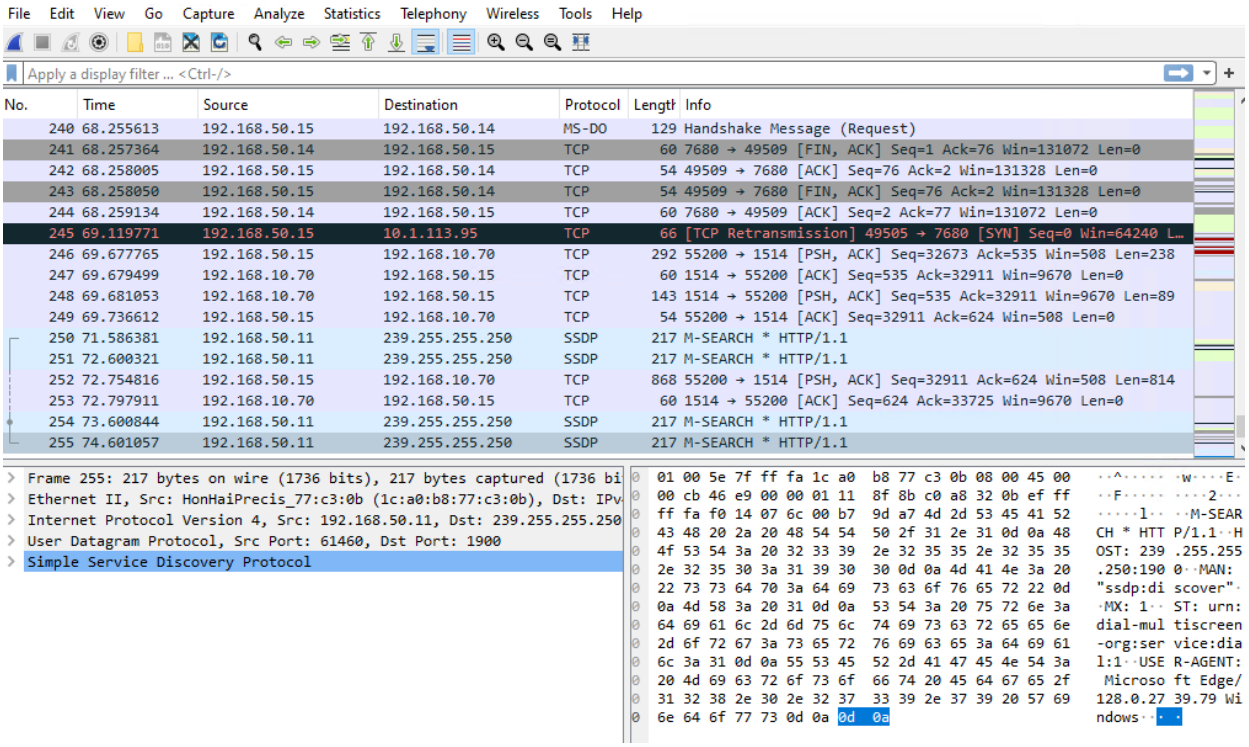
Со цел да се демонстрира потенцијалот на имплементираната тестна околина во контекст на сајбер-безбедносниот мониторинг, беше спроведен тест за следење на мрежниот сообраќај при напад со вметнување команди преку командна линија (анг. Command Line Injection Attack) врз тест веб-сервер. Целта на овој тест е да се прикажат можностите на предложената тестна околина за прибирање и корелација на податоци од повеќе извори, без навлегување во детална анализа на процесите за детекција на упади, што не претставува примарен фокус на оваа демонстрација.

Во рамките на сценариото, напаѓачката машина изведува напад со вметнување команди врз тест веб-страница. Имплементираните сензори и мониторинг компоненти ги следат мрежните активности и прибираат релевантни податочни точки. Во овој пример, податоците се прибираат од три различни извори: Zeek, кој генерира трансакциски логови за мрежните конекции, Wireshark, кој овозможува детално прибирање и анализа на мрежни пакети, и Wazuh SIEM, кој обезбедува логирање и мониторинг на безбедносни настани.

Слика 17 ги прикажува трансакциските логови генерирани од Zeek за време на спроведеното тест-сценарио. Овие логови содржат информации за мрежните конекции, како што се изворна и одредишна IP-адреса, порти, протокол, сервис и времетраење на комуникацијата. Способноста на Zeek да доделува уникатни идентификатори на тековите, односно UID-вредности, овозможува поврзување и анализа на настани што се однесуваат на иста комуникациска сесија или на поврзани активности во рамките на истото сценарио.

Слика 17: Zeek-логови прибрани при напад со вметнување команди преку командна линија

Слика 18 ги прикажува можностите на Wireshark за снимање и детална анализа на мрежни пакети во рамките на спроведеното тест-сценарио. Преку ваквиот приказ може да се анализираат повеќе карактеристики на мрежниот сообраќај, како што се изворна и одредишна IP-адреса, користени протоколи, порти, должина на пакетите, временски редослед на комуникацијата и содржина на поединечни пакети. Овие податоци обезбедуваат основа за подлабинска анализа на мрежните активности, како и за екстракција на карактеристики што може да се користат во понатамошните процеси на детекција на аномалии и евалуација на IDS-механизми. При употребата на дополнителни алатки, како CICFlowMeter, снимените пакети може да се трансформираат во сумирани тековни карактеристики погодни за обработка со алгоритми од машинско учење.



Слика 18: Wireshark-снимка од мрежен сообраќај при напад со вметнување команди преку командна линија

Слика 19 прикажува пример за генериран безбедносен настан во Wazuh SIEM, прибран од тест веб-серверот за време на спроведеното сценарио. Настанот содржи повеќе релевантни атрибути, како идентификатор и име на агентот, процес, патека до извршна датотека, корисник, временска ознака, дигитален потпис и правило поврзано со детектираната активност. Во конкретниот пример, настанот е поврзан со правило кое се однесува на техниката за вметнување процес (анг. Process Injection), што покажува дека мониторингот на крајните уреди може да обезбеди дополнителен контекст кој не е секогаш видлив само преку анализа на мрежниот сообраќај.

Мониторингот на настани, во овој случај реализиран преку Sysmon и интегриран во Wazuh SIEM, ги проширува можностите за следење на активностите на крајните уреди. На овој начин се обезбедува дополнителна видливост во процесите, извршните датотеки, корисничките активности и безбедносно релевантните промени во системот. Ваквите податоци значајно придонесуваат за безбедносен мониторинг, анализа на инциденти и корелација со податоците добиени од други извори, како што се Zeek-логови и Wireshark-снимки.

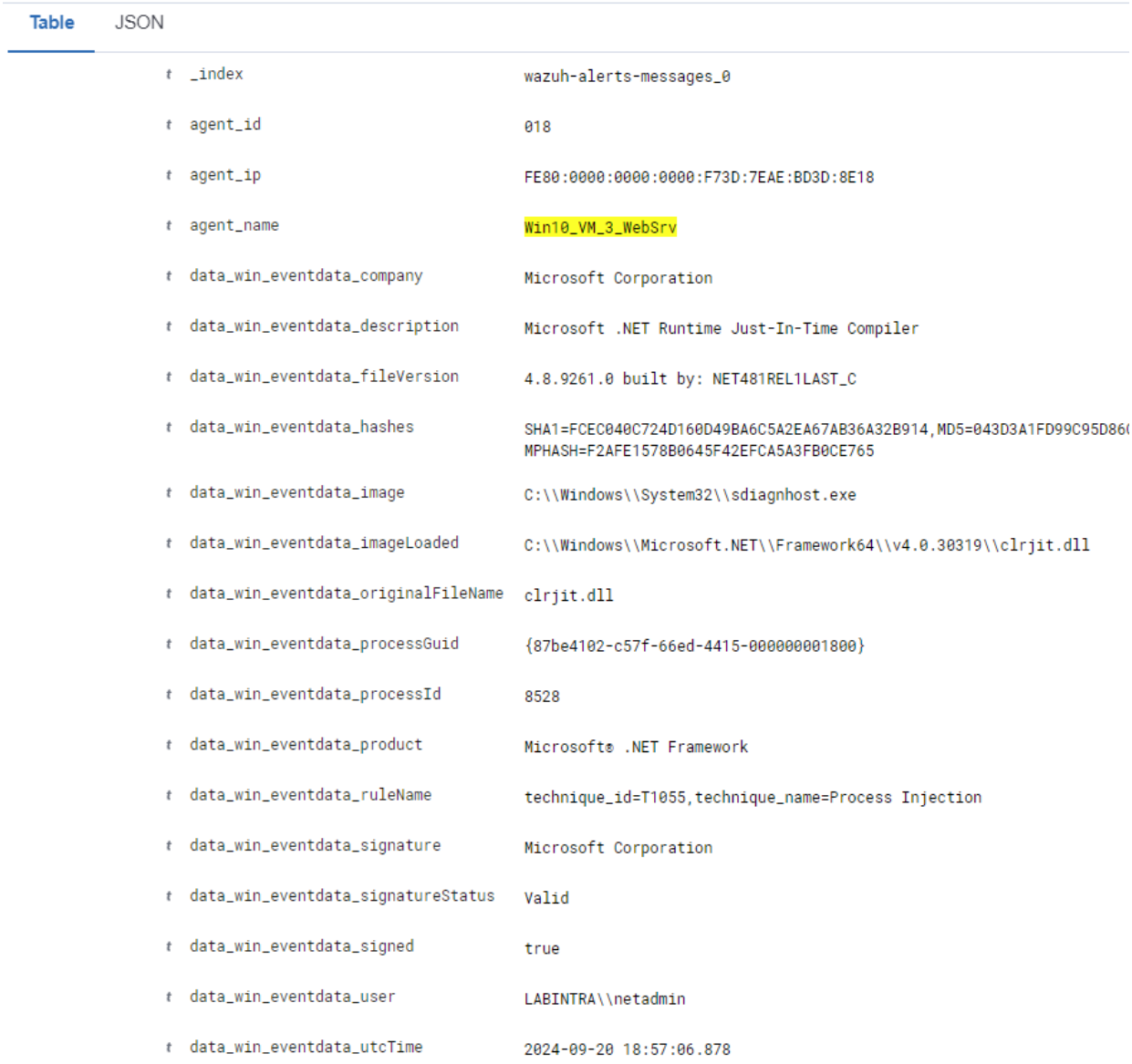


Table JSON

t _index	wazuh-alerts-messages_0
t agent_id	018
t agent_ip	FE80:0000:0000:0000:F73D:7EAE:BD3D:8E18
t agent_name	Win10_VM_3_WebSrv
t data_win_eventdata_company	Microsoft Corporation
t data_win_eventdata_description	Microsoft .NET Runtime Just-In-Time Compiler
t data_win_eventdata_fileVersion	4.8.9261.0 built by: NET481REL1LAST_C
t data_win_eventdata_hashes	SHA1=FCEC040C724D160D49BA6C5A2EA67AB36A32B914,MD5=043D3A1FD99C95D86(MPHASH=F2AFE1578B0645F42EFCA5A3FB0CE765
t data_win_eventdata_image	C:\\Windows\\System32\\sdiagnhost.exe
t data_win_eventdata_imageLoaded	C:\\Windows\\Microsoft.NET\\Framework64\\v4.0.30319\\clrjit.dll
t data_win_eventdata_originalFileName	clrjit.dll
t data_win_eventdata_processGuid	{87be4102-c57f-66ed-4415-000000001800}
t data_win_eventdata_processId	8528
t data_win_eventdata_product	Microsoft® .NET Framework
t data_win_eventdata_ruleName	technique_id=T1055,technique_name=Process Injection
t data_win_eventdata_signature	Microsoft Corporation
t data_win_eventdata_signatureStatus	Valid
t data_win_eventdata_signed	true
t data_win_eventdata_user	LABINTRA\\netadmin
t data_win_eventdata_utcTime	2024-09-20 18:57:06.878

Слика 19: Генериран безбедносен настан во Wazuh SIEM

Собраните податоци од имплементираната тестна околина покажуваат дека предложената архитектура овозможува прибирање разновидни и безбедносно релевантни информации од повеќе нивоа на инфраструктурата: мрежен сообраќај, трансакциски логови и настани од крајни уреди. Овие податоци може да претставуваат основа за понатамошни истражувања и развој на механизми за детекција на аномалии, вклучувајќи пристапи базирани на машинско учење, длабоко учење и вештачка интелигенција.

5.5. Заклучок

Во оваа глава беше дефинирана и имплементирана инфраструктура на тестна околина за организациска доменска мрежа базирана на Windows, управувана преку интегриран NOC и SOC со примена на алатки со отворен код. Предложената архитектура овозможува реалистична репрезентација на организациска ИТ-околина, во која продукцискиот сегмент на мрежата е поврзан со централизирани механизми за мониторинг, прибирање логови, анализа на настани и визуализација на состојбата.

Спроведената демонстрација покажа дека тестната околина може да поддржи прибирање различни типови податоци од повеќе извори, вклучувајќи мрежен сообраќај, трансакциски логови и системски настани од крајни уреди. Со имплементација на сензори и мониторинг компоненти на повеќе точки во мрежата, се овозможува сигурно и структурирано прибирање податоци кои се неопходни за анализа на мрежните активности, детекција на аномалии и евалуација на системи за детекција на упади.

Дополнително, резултатите ја потврдуваат применливоста на алатките со отворен код како доверлива, флексибилна и економична основа за развој, тестирање и валидација на современи сајбер-безбедносни решенија. Ваквата тестна околина претставува значајна основа за понатамошни истражувања, особено за примена на модели базирани на машинско учење, длабоко учење и вештачка интелигенција во процесите на детекција на аномалии и анализа на мрежен сообраќај.

5.6. Употребна вредност

Предложената интегрирана NOC–SOC архитектура покажува висока применливост во реални средини благодарение на нејзината усогласеност со: современите архитектури на организациите, потпирање на проверени алатки со отворен код и капацитетите за централизирано следење, собирање, анализа и донесување одлуки. Нејзиниот слоевит дизајн, кој се состои од слој за прибирање на податоци, слој за управување со системот и слој за управување со услуги, ги рефлектира воспоставените оперативни модели што се користат во современите ИТ-инфраструктури, овозможувајќи лесна интеграција со постојните организациски процеси. Со обединување на мониторингот на перформанси и безбедносните операции во единствена рамка, архитектурата го подобрува прегледот на ситуацијата во организацијата, овозможувајќи поефикасна детекција, корелација и реакција на мрежни настани. Дополнително, користењето на широко прифатени технологии со отворен код обезбедуваат економичност и флексибилност, што го прави решението достапно за широк спектар на организации, вклучително и оние со ограничени ресурси.

Како резултат, предложената рамка е високо соодветна за примена не само во истражувачки и едукативни средини, како што се сајбер-опсези, туку и во оперативни SOC-инфраструктури, каде што може да поддржи континуиран мониторинг, управување со инциденти и проактивни стратегии за одбрана во динамични и комплексни мрежни средини.

6. Евалуација на автоенкодер чувствителен на загуба

Во претходната глава беше дефинирана и имплементирана тестна ИТ-инфраструктура за организациска доменска мрежа базирана на Windows, управувана преку интегриран NOC и SOC со примена на алатки со отворен код. Преку спроведената демонстрација беше потврдено дека ваквата околина овозможува сигурно и континуирано прибирање мрежен сообраќај, трансакциски логови и системски настани од повеќе точки во мрежата, што претставува клучна основа за понатамошна безбедносна анализа. Дополнително, предложената архитектура ја истакнува применливоста на решенијата со отворен код како ефективна, доверлива и флексибилна платформа за развој и тестирање современи пристапи за сајбер-безбедност, со што се поставува основа за истражувања во областа на детекција на аномалии.

Надоврзувајќи се на оваа инфраструктура, оваа глава се фокусира на имплементација и евалуација на пристап за детекција на малициозен мрежен сообраќај со примена на техники од машинско учење. Во овој контекст се разгледува улогата на системите за детекција на упади и можностите на ML-алгоритмите за подобрување на детекцијата на малициозните активности. Посебен акцент е ставен на употребата на ненадгледувани модели од длабокото учење, конкретно автоенкодери, кои преку анализа на реконструкциската загуба овозможуваат идентификација на аномалии во мрежниот сообраќај.

Системот за детекција на упади претставува критична компонента на современата организациска безбедносна архитектура. Во контекст на безбедноста на ИТ-мрежите, упадот може да се дефинира како активност насочена кон компромитирање на доверливоста, интегритетот или достапноста на мрежните ресурси, серверската инфраструктура или сервисите кои се извршуваат во рамките на системот. Имплементацијата на IDS овозможува мониторинг, детекција и реакција на малициозни активности во мрежата, со цел заштита на критичните ресурси и намалување на ризикот од безбедносни инциденти [82]. Повеќе студии покажуваат дека примената на машинско учење во IDS може да придонесе за намалување на бројот на лажни аларми и зголемување на стапката на детекција [83].

IDS решенијата базирани на машинско учење се потпираат на учење обрасци од претходно прибрани податоци и нивна примена врз нови, претходно невидени податоци. На овој начин, моделите може да идентификуваат карактеристики на нормален и малициозен мрежен сообраќај и да поддржат донесување одлуки во процесот на детекција. Според пристапот на учење, машинското учење најчесто се класифицира во три основни категории: надгледувано учење (анг. Supervised Learning), ненадгледувано учење (анг. Unsupervised Learning) и полунадгледувано учење (анг. Semi-supervised Learning) [84].

Во рамките на ова истражување се евалуира пристапот за детекција на малициозен мрежен сообраќај преку користење на реконструкциската загуба добиена од ненадгледуван модел од длабоко учење, односно автоенкодер. Основната претпоставка е дека автоенкодерот, обучен врз нормален мрежен сообраќај, ќе генерира пониска реконструкциска загуба за легитимни примероци, додека малициозниот или невообичаен сообраќај ќе резултира со повисоки вредности на загуба. На тој начин, нивото на загуба се користи како индикатор за разграничување помеѓу нормално и невообичаено однесување во мрежниот сообраќај.

6.1. Поврзана работа и дискусија

Во литературата се среќаваат бројни релевантни истражувања во кои автоенкодерите се разгледуваат како ефикасен пристап за детекција на аномалии во мрежниот сообраќај. Во рамките на системите за детекција на упади, автоенкодерите најчесто се користат за учење на компактна репрезентација на нормалниот сообраќај и за идентификација на отстапувања преку анализа на реконструкцискатa грешка. Ваквиот пристап овозможува разликување помеѓу нормален и невообичаен мрежен сообраќај, особено во услови кога означените податоци се ограничени или недостапни.

Примената на автоенкодери во оваа област континуирано се развива, при што се забележуваат подобрувања во точноста на детекција,та обработката на високодимензионалните податоци и намалувањето на бројот на лажно позитивните резултати. Во [41], авторите предлагаат метод базиран на длабоко учење за предобработка на податоци и екстракција на карактеристики, што резултира со подобрени перформанси на класификација и зголемена брзина на детекција. Авторите во [42] предлагаат сличен пристап преку комбинирање техники од длабоко учење и плитко учење (анг. Shallow Learning – SL), при што презентираат SCAE за екстракција на карактеристики од суров мрежен сообраќај. Дополнително, тие применуваат Support Vector Machine – SVM класификациски алгоритам за подобрување на детекциските перформанси, користејќи две евалуациски бази на податоци: KDD Cup 99 и NSL-KDD.

Во трудот [43], авторите комбинираат автоенкодер со Improved Genetic Algorithm Backpropagation (IGA-BP) во единствен пристап. Во оваа поставеност, автоенкодерот се користи за елиминација на редундантни информации и намалување на димензионалноста на податоците, додека моделот IGA-BP ги адресира проблемите поврзани со бавна стапка на детекција и појава на локални оптимуми кај BP-мрежите. Експерименталните резултати покажуваат дека предложениот метод придонесува за подобрување на точноста на класификацијата, стапката на лажно позитивните резултати и на стапката на детекција.

Пристапот разгледан во оваа дисертација концепциски се разликува од претходно наведените истражувања по тоа што не се користат дополнителни техники од плитко учење ниту посебен класификациски модел врз излезот од автоенкодерот. Наместо тоа, фокусот е ставен на директната анализа на реконструкцискатa загуба добиена од автоенкодерот како индикатор за разграничување помеѓу легитимниот и малициозниот мрежен сообраќај. Експерименталниот дел опфаќа споредба на различни активациски функции, со цел да се утврди која конфигурација овозможува најизразена дистинкција помеѓу нормалните и аномалните примероци во рамките на анализираното податочно множество.

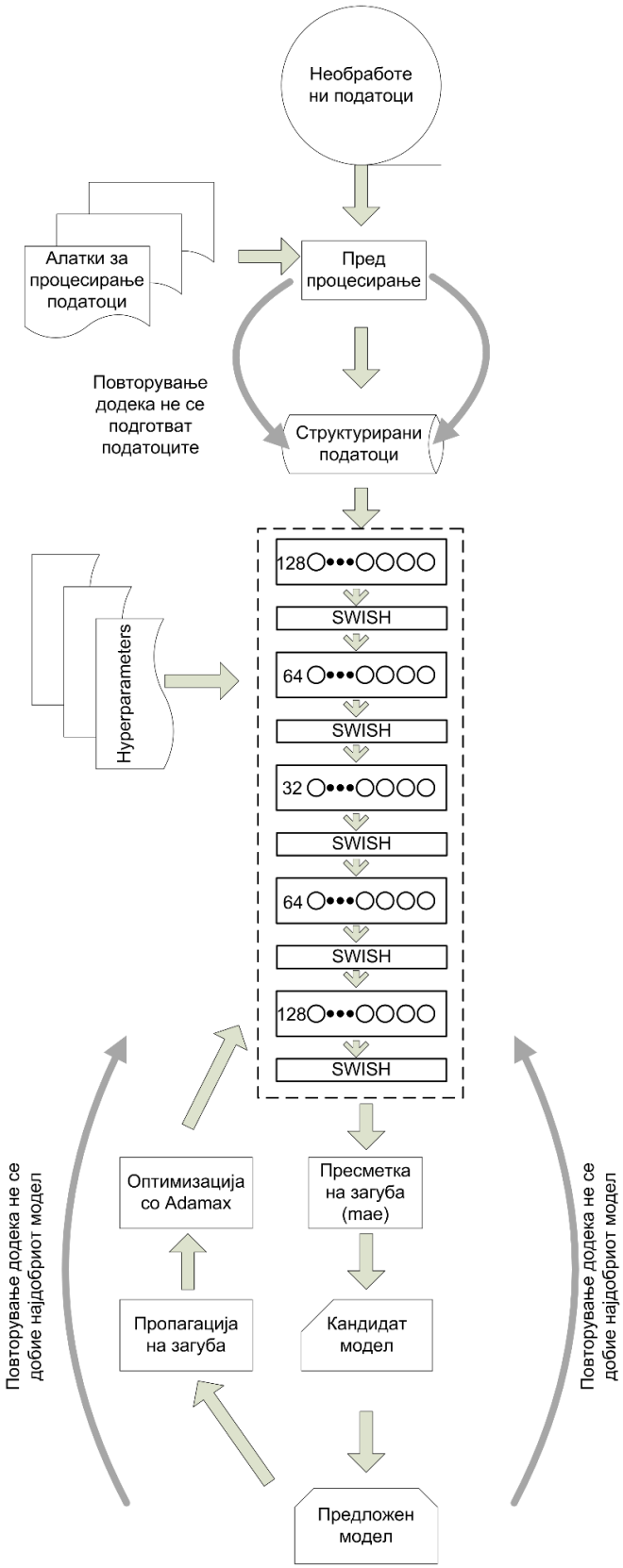
6.2. Експериментална околина на автоенкодер чувствителен на загуба за детекција на малициозен сообраќај

Карактеристиките на автоенкодерите овозможуваат нивна примена во различни сценарија за детекција на невообичаен мрежен сообраќај. Во рамките на ова истражување се евалуира автоенкодерскиот модел наменет за детекција на малициозен мрежен сообраќај преку користење на реконструкцискатa загуба како индикатор за отстапување од нормалното однесување. Основната претпоставка е дека моделот, обучен врз легитимен мрежен сообраќај, ќе постигне помала реконструкциска загуба за примероци со слични

карактеристики, додека малициозниот или невообичаен сообраќај ќе резултира со повисоки вредности на загуба.

Моделот е изграден врз автоенкодерска архитектура која вклучува повеќе хиперпараметри релевантни за процесот на учење, реконструкција и разграничување на мрежниот сообраќај. Архитектурата користи динамичка форма на влез (анг. Dynamic Input Shape), што овозможува флексибилност при експериментирањето со податочните множества со различни димензии на влезните податоци. Енкодерскиот дел започнува со слој од 128 неврони, по што следува слој од 64 неврони, додека централниот *bottleneck* слој содржи 32 неврони. Преку овој слој се формира компактна латентна репрезентација на влезните податоци, која потоа се користи од декодерскиот дел за реконструкција на оригиналниот влез. Финалниот број на слоеви и неврони е определен преку серија експерименти врз анализираните податочни множества и евалуација на добиените резултати. Експерименталната поставка за евалуација на автоенкодерот е прикажана на слика 20.

Дополнително, во рамките на истражувањето беа спроведени тестирања со различни активациски функции, функции на загуба и оптимизатори. Врз основа на анализата на добиените резултати, најдобри перформанси беа постигнати со примена на SWISH активациската функција, во комбинација со Mean Absolute Error (MAE) како функција на загуба и Adamax како оптимизатор. Оваа комбинација е избрана како основна конфигурација за понатамошната експериментална евалуација на моделот.



Слика 20: Експериментална поставка на модел со автоенкодер

6.3. Активациска функција

Изборот на активацискатa функција во моделите од длабоко учење има значајно влијание врз динамиката на обучување, стабилноста на оптимизацијата и перформансите на моделот во крајната задача. SWISH претставува активациска функција предложена од истражувачкиот тим на Google Brain [85], која во повеќе експериментални поставки покажува подобри резултати во споредба со ReLU, особено при изградба на длабоки модели врз комплексни податочни множества. Во нивните експерименти, замената на ReLU со SWISH довела до подобрување на точноста за 0,9 % на ImageNet и 0,6 % кај Inception-ResNet-v2. Поради едноставноста на имплементацијата и сличноста со ReLU, SWISH претставува соодветна алтернатива за примена во длабоки невронски мрежи.

Главната карактеристика на SWISH е тоа што претставува мазна и немонотонска активациска функција. Таа се дефинира со следната релација:

$$f(x) = x \cdot \sigma(\beta x) \qquad (32)$$

каде што $\sigma(z)$ е сигмоидна функција дефинирана како:

$$\sigma(z) = \frac{1}{1+e^{-z}} \quad (33)$$

а β претставува константа или параметар кој може да се обучува. Преку вредноста на β се контролира обликот на функцијата и степенот на нелинеарност, со што може да се приспособи нејзиното однесување во процесот на обучување.

Активацискатa функција SWISH е неограничена во позитивниот дел, додека во негативниот дел овозможува мазно и немонотонско однесување. Ова ја разликува од ReLU, која ги нулира негативните вредности и може да доведе до губење на дел од информацијата во одредени слоеви на мрежата. Ваквите својства ја прават SWISH погодна за длабоки невронски мрежи, особено во случаи каде што е потребна постабилна оптимизација и подобра репрезентациска способност.

Во рамките на ова истражување беше извршена споредба помеѓу резултатите добиени со примена на активациските функции SWISH и ReLU. Добиените резултати покажаа дека SWISH обезбедува подобри перформанси во анализираната експериментална поставка, поради што понатамошната евалуација на автоенкодерскиот модел е базирана на нејзина примена.

6.4. Методологија

Имајќи предвид дека автоенкодерот ја реконструира влезната репрезентација на својот излез преку минимизирање на реконструкциската загуба, целта на оваа експериментална поставка е да се евалуира моделот кој учи карактеристична репрезентација на легитимен мрежен сообраќај и овозможува разграничување во однос на малициозниот или невообичаениот сообраќај. Во рамките на експериментот е развиен автоенкодерски модел кој се обучува врз легитимен (анг. benign) мрежен сообраќај, при што реконструкциската загуба се користи како индикатор за отстапување од нормалното однесување.

Во текот на експерименталната работа беа разгледани и пристапи кои користат екстракција на карактеристики преку Principal Component Analysis (PCA) или автоенкодерски репрезентации. Сепак, овие пристапи не дадоа значајни резултати врз анализираните податочни множества. Поради тоа, за разлика од дел од претходно разгледаните трудови, во ова истражување не се применуваат дополнителни техники за екстракција на карактеристики ниту методи од плитко учење. Наместо тоа, фокусот е ставен на директната анализа на реконструкцискатa загуба добиена од автоенкодерскиот модел.

6.4.1. Процесирање на податоци

Мрежниот сообраќај користен во експериментите е преземен од податочното множество CICIDS2017 [86], кој содржи различни типови легитимен и малициозен мрежен сообраќај. Во рамките на ова истражување се анализирани четири типови малициозен сообраќај: Distributed Denial of Service (DDoS) напад, Infiltration, Web Application Attack и Port Scan.

Во почетната фаза, податочното множество беше пред обработено, при што беа извршени чистење, стандардизација и нормализација на податоците. Потоа, податоците беа поделени во две главни групи: податоци што претставуваат легитимен мрежен сообраќај и податоци што претставуваат малициозен мрежен сообраќај.

Легитимниот мрежен сообраќај беше дополнително поделен на податочно множество за тренинг или обука и податочно множество за тестирање, во сооднос 80 % : 20 %. Двете подмножества беа формирани преку случаен избор (анг. random sampling) од основниот множество со легитимен сообраќај. Со цел да се обезбеди репродуцибилност на резултатите, беше користено фиксно семе за случаен избор (анг. random seed).

Множеството со малициозен мрежен сообраќај беше искористен во фазата на евалуација, со цел споредба на реконструкцискатa загуба добиена за невидените легитимни примероци од множеството за тестирање и примероците што припаѓаат на различни категории малициозен сообраќај.

6.4.2. Обучување на моделот

Во следната фаза, автоенкодерскиот модел беше обучен со користење на SWISH активацискатa функција, во комбинација со MAE како функција на загуба и Adamax како оптимизатор. Изборот на оваа комбинација произлегува од претходно спроведените експерименти со различни активациски функции, функции на загуба и оптимизатори, при што беа добиени најповолни резултати за разграничување помеѓу легитимниот и малициозниот мрежен сообраќај.

Во процесот на обучување беа применети соодветни хиперпараметри со цел подобрување на стабилноста на моделот и постигнување конвергенција на функцијата на загуба. Постигнатата конвергенција укажува дека моделот успешно ја научил репрезентацијата на легитимниот мрежен сообраќај, што претставува основа за понатамошна евалуација врз невидени легитимни и малициозни примероци.

6.4.3. Предвидување и споредба на сообраќај

Во последната фаза од експериментот беше извршена проценка и графичко прикажување на реконструкцискатa загуба на множеството за тестирање со легитимен

сообраќај и за множествата со малициозен сообраќај. За секоја анализирана малициозна активност беше извршена споредба помеѓу вредностите на реконструкциската загуба добиени за легитимниот и малициозниот мрежен сообраќај.

Со користење на множеството за тестирање се обезбедуваат претходно невидени легитимни податоци за моделот, што овозможува валидна споредба со вредностите добиени од малициозниот сообраќај. На овој начин се оценува способноста на автоенкодерот да генерира различни нивоа на реконструкциска загуба за нормални и невообичаени примероци.

6.4.4. Детали за имплементацијата

Моделот беше изграден со користење на повеќе софтверски пакети што го поддржуваат процесот на обработка, моделирање и анализа на податоците. За стандардизација и нормализација на податоците беше користен Scikit-learn [87], за манипулација и управување со податочните множества беше применет Pandas [88] [89], додека за визуализација на резултатите беше користен Matplotlib [90]. За изградба, обучување и евалуација на автоенкодерскиот модел беше користен [91].

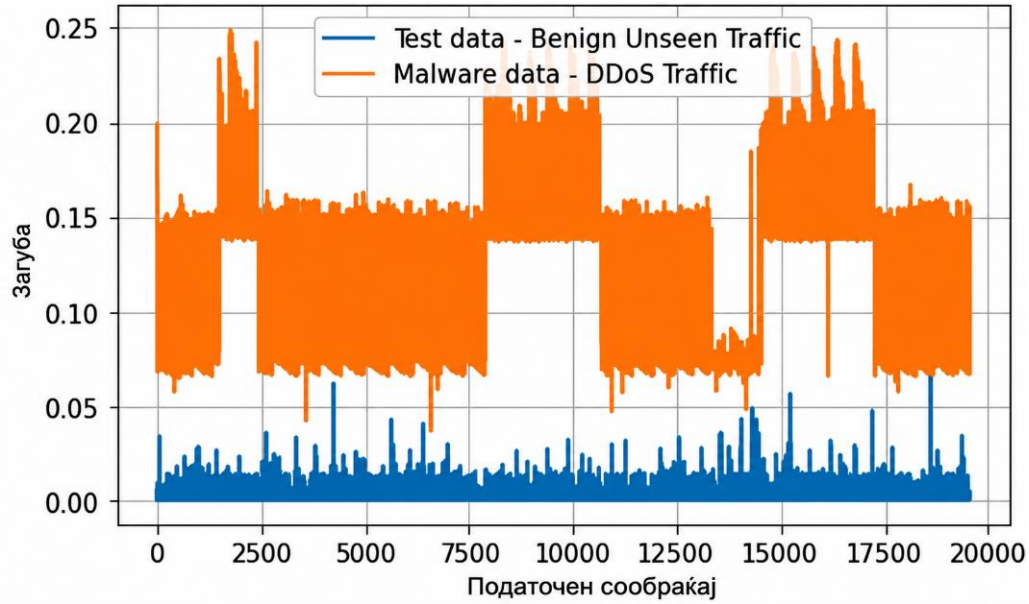
На почетокот на секој експеримент, податочните примероци беа нормализирани во интервалот (0, 1). Со ова се ограничува опсегот на вредностите на влезните карактеристики, што придонесува за постабилно обучување, поефикасна обработка и појасна споредба на добиените вредности на реконструкциската загуба.

Обучувањето на моделот беше спроведено во текот од 200 епохи. Добиените резултати покажуваат дека во текот на обучувањето е постигната стабилна конвергенција на функцијата на загуба, што овозможува понатамошна примена на моделот за споредба помеѓу легитимниот и малициозниот мрежен сообраќај.

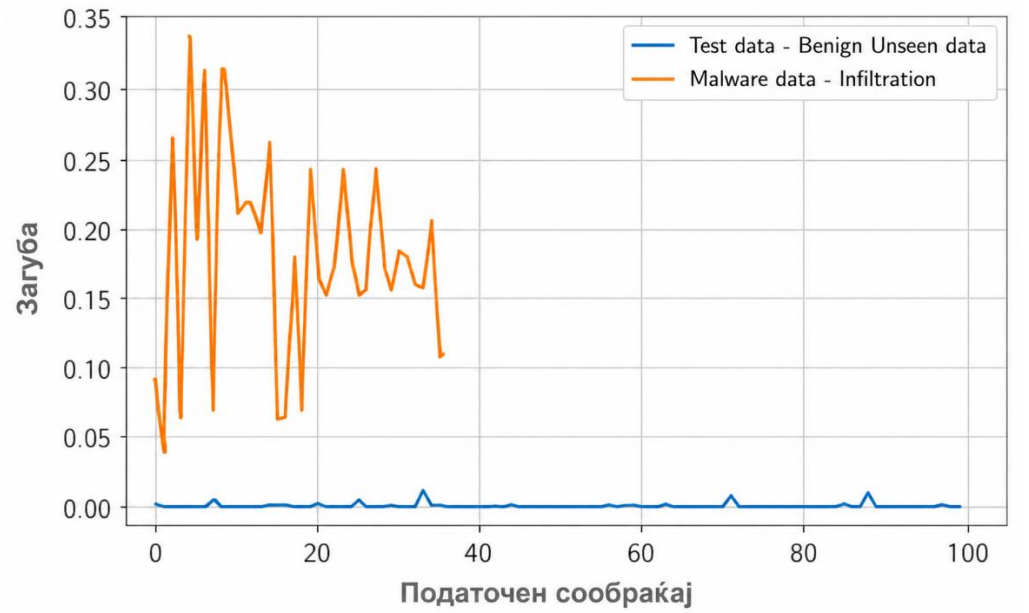
6.5. Анализа на експерименталните резултати

Во секој експеримент беше користен различен тип малициозен мрежен сообраќај, при што беа спроведени повеќе тестирања со различни комбинации на активациски функции, број на неврони, функции на загуба и оптимизатори. Најдобри резултати беа постигнати со примена на SWISH како активациска функција, MAE како функција на загуба и Adamax како оптимизатор. Архитектурата на моделот започнува со влезен слој од 128 неврони, по што следува слој од 64 неврони, а репрезентацијата се редуцира до 32 неврони во слојот *bottleneck*.

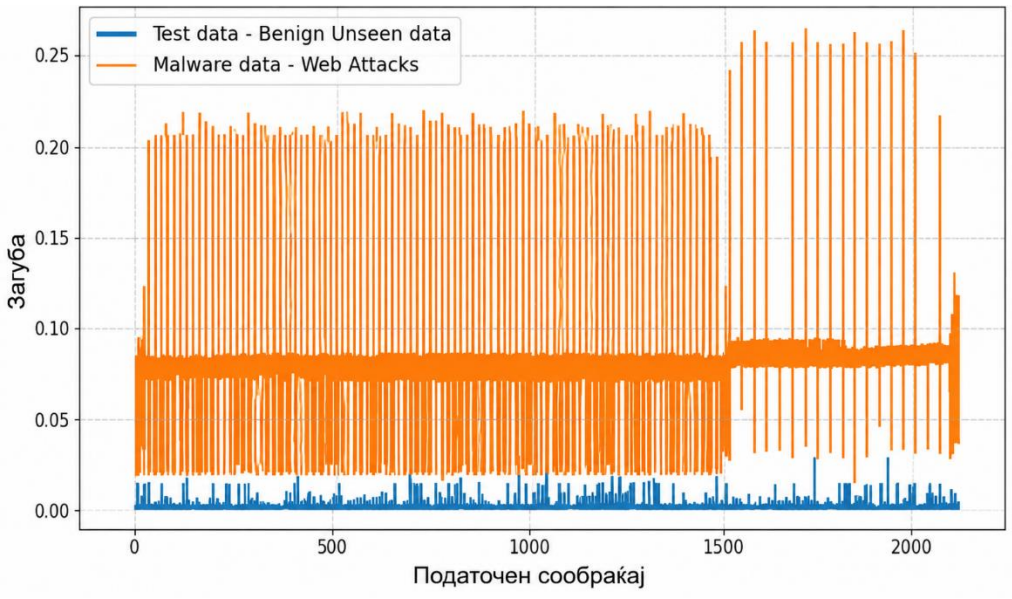
Резултатите од четирите експерименти се прикажани на сликите 21 – 24. Секоја слика ја прикажува реконструкциската загуба добиена при обработка на невиден легитимен мрежен сообраќај и соодветниот тип малициозен мрежен сообраќај. На овој начин се овозможува визуелна споредба на однесувањето на автоенкодерскиот модел при обработка на нормални и невообичаени примероци.



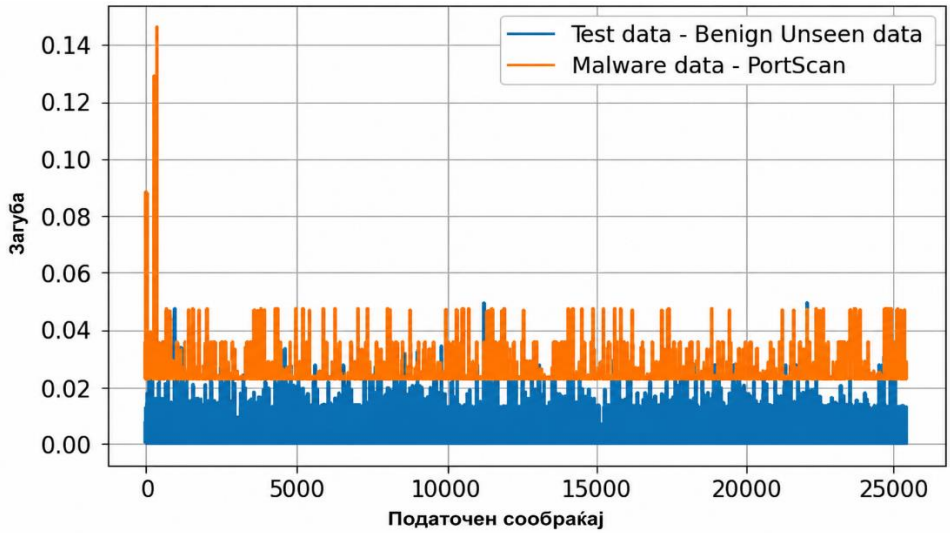
Слика 21: Резултати од тестирање со DDoS малициозен сообраќај каде што се забележува изразена разлика помеѓу вредностите на реконструкциската загуба добиени за DdoS-сообраќајот и вредностите добиени при обработка на легитимниот мрежен сообраќај



Слика 22: Резултати од тестирање со Infiltration малициозен сообраќај. На дијаграмот се забележува јасно разграничување помеѓу реконструкциската загуба за легитимниот и малициозниот сообраќај, што потврдува дека моделот може да разликува легитимен од малициозен сообраќај



Слика 23: Резултати од тестирање со Web Application Attack малициозен сообраќај. Видливо е јасно разграничување на вредностите на реконструкцискатa загуба кај малициозниот сообраќај кои се значително повисоки во однос на легитимниот сообраќај



Слика 24: Резултати од тестирање со Port Scan малициозен сообраќај. Се забележува преклопување помеѓу вредностите на реконструкцискатa загуба за легитимниот и малициозниот сообраќај. Но и покрај тоа, дел од малициозните примероци генерираат повисоки вредности на загуба

Првиот експеримент беше спроведен со DDoS малициозен мрежен сообраќај. Во податочното множество CICIDS2017, овој тип сообраќај учествува со 36,47 % од вкупното податочно множество. Како што е прикажано на слика 21, се забележува изразена разлика помеѓу вредностите на реконструкцискатa загуба добиени за DdoS-сообраќајот и вредностите добиени при обработка на невидениот легитимен мрежен сообраќај. Овој

резултат укажува дека автоенкодерскиот модел успешно го разликува овој тип малициозен сообраќај од нормалниот сообраќај врз основа на реконструкциската загуба.

Во вториот експеримент, за евалуација на перформансите на моделот беше користен *Infiltration* типот на мрежен сообраќај. Овој тип сообраќај учествува со 0,012 % од вкупниот мрежен сообраќај во CICIDS2017, што претставува релативно мал удел за поширока статистичка евалуација. И покрај тоа, резултатите прикажани на слика 22 покажуваат јасна сепарација помеѓу реконструкциската загуба за легитимниот и малициозниот сообраќај. Ова укажува дека моделот може да идентификува отстапувања и кај типовите напади кои се слабо застапени во податочното множество, иако за поцврста генерализација би бил потребен поголем број примероци.

Третиот експеримент беше насочен кон Web Application Attack типот на малициозен мрежен сообраќај, кој учествува со 1,27 % од вкупниот сообраќај во CICIDS2017. На слика 23 е прикажана споредбата помеѓу реконструкциската загуба добиена за веб-апликациските напади и легитимниот мрежен сообраќај. Може да се забележи дека вредностите на реконструкциската загуба кај малициозниот сообраќај се значително повисоки во однос на легитимниот сообраќај, што овозможува јасно разграничување помеѓу двете групи примероци.

Последниот експеримент беше спроведен со Port Scan малициозен мрежен сообраќај, исто така од CICIDS2017. Овој тип сообраќај учествува со 55,47 % од вкупното податочно множество, а резултатите се прикажани на слика 24. Во споредба со претходните експерименти, кај Port Scan сообраќајот се забележува поголемо преклопување помеѓу вредностите на реконструкциската загуба за легитимниот и малициозниот сообраќај. Сепак, и покрај изразеното преклопување, дел од малициозните примероци генерираат повисоки вредности на загуба, што укажува на можност за нивно разграничување. Овој резултат покажува дека Port Scan активностите претставуваат посложен случај за детекција со предложениот автоенкодерски модел и отвораат простор за дополнителна оптимизација на архитектурата, прагот за одлучување или изборот на карактеристики.

6.6. Заклучок од експериментите

Во рамките на ова истражување беше презентиран и евалуиран автоенкодер чувствителен на загуба за детекција на малициозен мрежен сообраќај. Евалуацијата покажа дека реконструкциската загуба може да се користи како релевантен индикатор за разграничување помеѓу легитимен и малициозен мрежен сообраќај. Во сите анализирани експерименти беше забележана разлика помеѓу вредностите на реконструкциската загуба кај легитимниот и малициозниот сообраќај, при што најизразено разграничување беше постигнато кај DDoS, Infiltration и Web Application Attack сценаријата.

Резултатите покажуваат дека предложениот автоенкодерски пристап има потенцијал за примена во системи за детекција на аномалии, особено во ситуации каде што е потребна идентификација на невообичаени обрасци во мрежниот сообраќај без примена на дополнителен класификациски модел. Кај Port Scan активностите беше забележано поголемо преклопување помеѓу легитимниот и малициозниот сообраќај, што укажува дека овој тип напад претставува посложен случај за детекција и отвора простор за понатамошна оптимизација на архитектурата, изборот на карактеристики и прагот за одлучување.

Значајна придобивка од спроведеното истражување е потврдувањето дека соодветно дизајнираниот автоенкодер може да се користи не само за детекција на малициозен мрежен сообраќај, туку и како основа за поширока анализа на мрежни обрасци. Ваквиот пристап може да биде интегриран во системи за мониторинг и анализа на мрежниот сообраќај, како дополнителен механизам за препознавање на аномалии и поддршка на процесите за сајбер-безбедносна евалуација.

6.7. Употребна вредност

Предложениот автоенкодер чувствителен на загуба има висока употребна вредност во реалните имплементации за безбедност на мрежи, особено за детекција на упади базирана на аномалии во динамични и хетерогени услови на мрежен сообраќај. Преку учењето на репрезентативниот модел на нормалното (бенигно) однесување на мрежата и користење на реконструкциската загуба како дискриминативна карактеристика, пристапот овозможува ефикасна диференцијација помеѓу нормален и малициозен сообраќај без потреба од експлицитно извлекување на карактеристики или класификација со ненадгледувано учење. Ова е особено значајно во оперативни средини каде означените податочни множества се ограничени или застарени и каде што новите или еволуирачки модели на напади, како што се DDoS, инфилтрација, веб-апликациските напади и Port Scan, треба да се детектираат во реално време. Експерименталните резултати добиени со користење на податочното множество CICIDS2017 потврдуваат дека моделот конзистентно генерира поголема реконструкциска загуба за малициозниот сообраќај, обезбедувајќи сигурна основа за детекција на аномалии. Ова однесување го прави пристапот соодветен за интеграција во постојните инфраструктури за мрежен мониторинг, вклучувајќи системи за детекција на упади и платформи за анализа на сообраќај, како дополнителен слој за идентификација на сомнителни активности. Понатаму, едноставноста и ефикасноста на архитектурата на автоенкодерот овозможуваат практична имплементација и во централизирани и во дистрибуирани средини, вклучувајќи мрежни сензори, IoT и edge-базирани системи за мониторинг.

Предложениот модел може да биде имплементиран како прв филтер на малициозните закани по системот пред да се премине на пософистицирани модели, со што значајно ќе ја намали работата на следните системи за безбедност. Како резултат, овој пристап не е применлив само во истражувачки и експериментални тестни околини, туку претставува и одржливо решение за реални имплементации во сајбер-безбедноста, поддржувајќи континуиран мониторинг, детекција на аномалии и анализа на мрежниот сообраќај која е базирана на податоците во современите мрежни средини.

7. Парето-водена рамка во две фази за адаптивна оптимизација на ресурси кај лесни системи за детекција на упади

Во претходната глава беше развиен и евалуиран автоенкодер чувствителен на загуба за детекција на малициозен мрежен сообраќај. Преку експерименталната анализа беше потврдено дека реконструкциската загуба може да се користи како релевантен индикатор за разграничување помеѓу легитимниот и малициозниот мрежен сообраќај. Добиените резултати покажаа дека автоенкодерскиот пристап има потенцијал за примена во системите за детекција на аномалии, особено во услови кога е потребно препознавање на невообичаени обрасци без примена на дополнителен класификациски модел. Истовремено, резултатите укажаа дека одредени типови активности, како Port Scan, претставуваат посложен случај за детекција и бараат понатамошна оптимизација на моделот, изборот на карактеристики или прагот за одлучување.

Надоврзувајќи се на овие резултати, оваа глава ја проширува перспективата од изолирана детекција на аномалии кон системско и динамичко управување со IDS-конфигурации во ресурсно ограничени средини. Современите дистрибуирани околини, како IoT, Edge и Fog инфраструктурите, се карактеризираат со ограничени пресметковни, меморискиот и комуникациски ресурси, што ја отежнува директната примена на комплексни IDS-решенија. Во овој контекст се предлага A2DAPT-рамката, која комбинира повеќекритериумска оптимизација и длабоко засилено учење со цел адаптивно управување со IDS-конфигурации во услови на динамичен и нестационарен мрежен сообраќај.

Интеграцијата на IoT, Edge и Fog технологиите во индустриските процеси и секојдневните апликации овозможува висока меѓусебна поврзаност, ефикасност и практична применливост [92]. Сепак, оваа технолошка еволуција воведува и значајни сајбер-безбедносни предизвици, особено поради ограничувањата на уредите во однос на пресметковна моќ, меморија, енергија и пропусен опсег [93], [94], [95]. Овие ограничувања директно влијаат врз можноста за имплементација на безбедносни механизми кои истовремено треба да обезбедат висок квалитет на детекција и прифатлива потрошувачка на ресурси.

Системите за детекција на упади имаат специфични ресурсни барања во зависност од средината во која се имплементираат. Додека корпоративните и облак (cloud) околините вообичаено располагаат со моќни серверски ресурси, IoT, Edge и Fog околините најчесто се базираат на хардвер со ограничени можности, како вградени уреди, безжични сензори и *gateway* јазли. Овие разлики ја наметнуваат потребата од лесни IDS-решенија, приспособени за работа во средини со ограничени ресурси [96].

Ваквата промена на оперативната средина бара адаптација на IDS-решенијата со цел да се задоволат барањата за ефикасност, стабилност и одржливост. Поради ограничените ресурси во овие средини, употребата на лесни IDS-решенија не е само прашање на намалување на пресметковната сложеност, туку и прашање на динамичко балансирање помеѓу квалитетот на детекција и потрошувачката на ресурси. Затоа е потребен оптимизациски пристап кој ќе овозможи избор на соодветна IDS-конфигурација во зависност од тековната состојба на мрежниот сообраќај и достапните ресурси.

Целта на ова истражување е развој на ресурсно свесна адаптивна контролна рамка за лесни IDS, која динамички го балансира квалитетот на детекција и потрошувачката на ресурси во услови на нестационарен мрежен сообраќај. Поконкретно, предложениот пристап комбинира офлајн Парето-оптимизација со онлајн DRL, со што се овозможува ефикасно и стабилно донесување одлуки за избор на соодветна конфигурација на IDS.

Клучните придонеси на оваа глава може да се сумираат на следниот начин:

1. Се предлага двостепена оптимизациска рамка за IDS, наречена A2DAPT, која комбинира повеќекритериумска оптимизација и длабоко засилено учење. Ресурсно свесната конфигурација на IDS се формализира како проблем на две нивоа:
   (i) офлајн повеќекритериумско пребарување со користење на NSGA-II [19], преку кое се идентификуваат Парето-ефикасни IDS-конфигурации; и
   (ii) онлајн адаптација со користење на D3QN со PER [23], [24], [22], [46], ограничена на дискретното Парето множество, со што се овозможува адаптивен избор на IDS-конфигурација за секој временски прозорец.

2. Се воведуваат детекциска мерка зависна од ознаките и наградна функција зависна од ресурсниот буџет, со кои директно се моделираат оперативните ограничувања и компромисите при извршување. Ваквата формулација го насочува процесот на учење кон одлуки усогласени со достапните ресурси, овозможувајќи балансирање помеѓу квалитетот на детекција и системските ограничувања на контролиран и формализиран начин.

3. Се воведува интерпретабилен конфигурациски простор преку ограничување на просторот на акции на Парето ефикасни IDS-конфигурации. Ова ограничување ја подобрува стабилноста на адаптивниот контролер преку елиминирање на небезбедно истражување во неефикасни конфигурациски региони и намалување на варијабилноста на одлуките, што резултира со доверлива и ресурсно усогласена адаптација во услови на нестационарен мрежен сообраќај.

Работата на IDS се моделира преку повеќедимензионална конфигурациска состојба, при што рачното подесување на системот се трансформира во формален оптимизациски проблем. Во рамките на предложената рамка се користи метрика за детекција зависна од ознаки (анг. label-aware detection score) и наградна функција зависна од ресурсен буџет (анг. budget-aware reward), со што експлицитно се моделираат оперативните ограничувања и компромисите при извршување. Со цел зголемување на робусноста, *fitness* функцијата на NSGA-II се пресметува врз стратифицирани минисерии (анг. mini-batches), што овозможува генерирање на Парето множества применливи во различни режими на мрежниот сообраќај. Дополнително, се користат сурогат модели за потрошувачка на процесор, меморија и пропусен опсег, со што се овозможува поефикасна оптимизација и учење на политики, при истовремено приближување кон реалното однесување на IDS .

7.1. Поврзана работа и дискусија

7.1.1. Конфигурација на IDS како оптимизациски проблем

IDS имплементирани во IoT, Edge и Fog околини мора да функционираат под строги ограничувања во однос на пресметковните ресурси, меморијата, енергијата и пропусниот опсег [97], [98], [99]. За адресирање на овој предизвик, повеќе истражувања ја формулираат конфигурацијата на IDS како конечно димензионален вектор на параметри, со што процесот на детекција и потрошувачката на ресурси може да се оптимизираат алгоритамски, наместо преку рачно подесување [100], [101], [102], [103], [104]. Ваквата формулација природно ја поддржува примената на метахеуристичките и еволутивните оптимизациски техники, кои овозможуваат пребарување во сложен конфигурациски простор и идентификација на компромисни решенија меѓу детекциските перформанси и ресурсните трошоци.

Сепак, најголем дел од постојните пристапи се базираат на офлајн оптимизација и резултираат со избор на една фиксна конфигурација, што имплицитно претпоставува стационарен карактер на мрежниот сообраќај. Иако ваквите пристапи може да обезбедат задоволителни перформанси при просечни оптоварувања, тие не ја опфаќаат краткорочната варијабилност на сообраќајот и динамичките обрасци на оптоварување карактеристични за IoT, Edge и Fog околините. Како резултат, статичките конфигурации може да доведат до неефикасно искористување на ресурсите во периоди на ниско оптоварување или до намалени детекциски перформанси при нагли зголемувања на сообраќајот, со што се ограничува нивната применливост во реални оперативни услови.

7.1.2. Ограничувања на ресурси и повеќекритериумска оптимизација на IDS

Ограничувањата на ресурсите поттикнале развој на аналитички и оптимизациски пристапи за имплементација на IDS во ограничени околини. Даи и Улудаг [105] ги истакнуваат компромисите помеѓу точноста на детекција и трошокот на инференција, додека Хосеинпур и сор. [106] се фокусираат на искористувањето на ресурсите во *fog computing*, со посебен акцент на комуникациската ефикасност. Одредени истражувања ги комбинираат детекциските и ресурсните трошоци во единствена скаларизирана целна функција [107], [108]. Сепак, ваквите формулации ги прикриваат компромисите помеѓу конфликтните цели и резултираат со една оперативна точка, со што се ограничува флексибилноста при имплементација и се намалува можноста за избор на конфигурации усогласени со конкретните ресурсни ограничувања.

За надминување на ова ограничување, предложени се еволутивни и сурогатско поддржани оптимизациски методи. Алшахрани и сор. [109], [110] ја анализираат конфигурацијата на IDS во ресурсно ограничени IoT-мрежи со користење генетски алгоритми и сурогатско базирани апроксимации на функцијата *fitness*. Нивните резултати ја демонстрираат важноста на балансирањето на детекциските перформанси во однос на пресметковниот и енергетскиот буџет, како и применливоста на NSGA-II како метод за повеќекритериумска оптимизација. Иако овие пристапи ефикасно идентификуваат компромисни решенија, тие најчесто се ограничени на офлајн оптимизација и претпоставуваат статички услови на сообраќајот. Таквата претпоставка ја ограничува нивната способност за адаптација кон динамички оптоварувања, кои се чести во реални IoT

и Edge околини. Како резултат, конфигурациите добиени во офлајн фазата може да станат субоптимални или неефикасни кога се применуваат во услови на нестационарен сообраќај.

Понатаму, претходните истражувања покажуваат дека стабилноста и генерализацијата на Парето-фронтовите се чувствителни на начинот на кој се проценуваат целните функции. Евалуациите врз ограничени или небалансирани примероци може да доведат до прекумерно приспособување кон специфични оперативни режими, што ја намалува робусноста на добиените конфигурации. Иако се предложени стратегии за евалуација базирани на серии и стратификација со цел да се ублажи овој проблем [111], нивната примена во контекст на IDS-конфигурацијата останува ограничена. Дополнително, постојните примени на NSGA-II во сродни IoT домени, како композиција на сервиси и енергетски ефикасно распоредување [112], [18], не ја адресираат експлицитно интеракцијата помеѓу детекциските перформанси и ресурсните ограничувања кај IDS.

На крајот, неколку прегледни трудови за оптимизациски техники укажуваат дека ресурсно свесната оптимизација на IDS останува недоволно истражена. На пример, Хоусеин и сор. [113] ги анализираат метахеуристичките алгоритми во безжични сензорски мрежи, но не ја разгледуваат нивната примена за ефикасна и ресурсно свесна имплементација на IDS. Следствено, и покрај препознаената важност на оптимизацијата на ресурсите, постојните методи не обезбедуваат унифициран пристап кој комбинира робусна повеќекритериумска оптимизација со адаптивно донесување одлуки за време на извршување во услови на нестационарен мрежен сообраќај. Предложената A2DAPT-рамка ја адресира оваа празнина преку интеграција на стратифицирана повеќекритериумска оптимизација со контролирана онлајн адаптација, овозможувајќи робусна идентификација на конфигурации и ресурсно свесно работење во реално време.

7.1.3. Длабоко засилено учење за адаптивно однесување на IDS

Основните концепти на длабокото засилено учење, како и DQN-базираните архитектури релевантни за оваа дисертација, се обработени во поглавјето 2.4. Во оваа секција, DRL се разгледува од аспект на неговата примена во сродни истражувања за адаптивното однесување на IDS и неговите ограничувања во ресурсно ограничени околини.

Во последните години, DRL сè почесто се применува кај IDS, најчесто со цел подобрување на ефективноста на детекција, адаптација на политиките за инспекција или моделирање на процесот на детекција како секвенцијален проблем на донесување одлуки. Дел од поновите истражувања ја нагласуваат важноста од експлицитно моделирање на временските зависности во IoT и Industrial Control System (ICS) околини, преку архитектури чувствителни на секвенци, како што се енкодерите базирани на Long Short-Term Memory (LSTM), интегрирани со генеративни модели [114]. Ким и сор. [103] применуваат DRL за приспособување на стапките на инспекција на сообраќајот без директна промена на IDS-конфигурациите, додека други истражувања ја моделираат детекцијата на упади како секвенцијален процес на донесување одлуки со цел подобрување на класификациските перформанси [115], [116],[117].

Иако овие пристапи ја потврдуваат применливоста на DRL во IDS околините, најголем дел од нив се фокусираат првенствено на точноста на детекцијата, додека оперативните ограничувања поврзани со потрошувачката на ресурси се третираат ограничено или имплицитно. Ова е особено значајно кај имплементации во IoT, Edge и Fog

околини, каде што ограничувањата во однос на процесорското време, меморија и пропусен опсег претставуваат клучни фактори за практична применливост [118]. Дополнително, дел од DRL-базираните решенија користат континуирани или широко дефинирани простори на акции, што може да воведе ризик од неефикасно или небезбедно истражување за време на процесот на учење [115], [116], [117]].

Следствено, постојните DRL-пристапи најчесто не обезбедуваат експлицитна гаранција дека избраните акции или конфигурации ќе бидат усогласени со дефинираниот ресурсен буџет. Во практичните имплементации, ова може да резултира со избор на конфигурации кои се пресметковно скапи, нестабилни или неизводливи за ресурсно-ограничени уреди. Овој проблем е особено критичен во IoT, Edge и Fog околини, каде што неефикасното користење на ресурсите може да доведе до деградација на перформансите, нарушување на достапноста или прекин на услугите.

За разлика од претходно наведените пристапи, рамката предложена во оваа дисертација ја интегрира состојбата со ресурсите директно во процесот на донесување одлуки. Притоа, просторот на акции не се дефинира како произволно множество на можни IDS-конфигурации, туку се ограничува на претходно идентификувани Парето-ефикасни конфигурации добиени преку офлајн повеќекритериумска оптимизација. На овој начин, DRL-агентот не истражува небезбедни или очигледно неефикасни конфигурации, туку учи политика за избор меѓу конфигурации кои веќе претставуваат компромис помеѓу квалитетот на детекција и потрошувачката на ресурси. Ваквата поставеност овозможува побезбедна, поинтерпретабилна и оперативно изводлива адаптација во услови на нестационарен мрежен сообраќај.

7.2. Дефиниција на проблемот

Современите IDS кои се имплементираат во IoT, Edge и Fog околини треба да обезбедат висок квалитет на детекција, но истовремено да функционираат во рамките на ограничените пресметковни, мемориски и комуникациски ресурси. Во практични услови, мрежниот сообраќај има нестационарен карактер, при што неговите статистички својства и интензитет може значително да се менуваат во кратки временски интервали. Во такви услови, фиксните IDS-конфигурации може да доведат до неефикасно користење на ресурсите во периоди на ниско оптоварување или до намалени детекциски перформанси при нагли зголемувања на сообраќајот. Дополнително, динамиката на современите мрежни околини го прави рачното подесување на IDS -онфигурациите практично неизводливо.

Целта на ова истражување е да се дизајнира контролер во реално време кој, за даден временски прозорец на мрежен сообраќај, избира соодветна IDS-конфигурација со цел одржување висок квалитет на детекција, намалување на потрошувачката на ресурси и избегнување прекршување на зададениот ресурсен буџет. За да биде применлив во реални оперативни услови, контролерот треба да обезбеди стабилни и интерпретабилни одлуки, како и да избегнува небезбедно или неефикасно однесување при промена на конфигурациите.

Постојните пристапи за конфигурирање на IDS имаат неколку значајни ограничувања. Статичките или ретко ажурираните конфигурации не можат соодветно да се адаптираат на краткорочни варијации во мрежниот сообраќај, што може да резултира со неефикасно користење на ресурсите или намалено ниво на заштита. Пристапите кои го

сведуваат повеќекритериумскиот проблем на единствена скаларна целна функција ги прикриваат компромисите помеѓу квалитетот на детекција и потрошувачката на ресурси, при што се добива само една оперативна точка наместо множество применливи компромисни решенија. Дополнително, пристапите базирани на директна или континуирана оптимизација преку длабоко засилено учење може да претставуваат оперативен ризик, бидејќи бараат значителни количини податоци за обучување и може да истражуваат неефикасни или небезбедни делови од конфигурацискиот простор. Ова ја ограничува нивната применливост во продукциски и ресурсно ограничени околини.

Врз основа на наведеното, проблемот што се разгледува во оваа глава може да се формулира преку две поврзани истражувачки прашања. Прво, како врз основа на историски податоци за мрежниот сообраќај и познати ресурсни ограничувања да се идентификува множество од Парето-ефикасни IDS-конфигурации кои го одразуваат компромисот помеѓу квалитетот на детекција и потрошувачката на ресурси. Второ, како да се научи брза, стабилна и ресурсно свесна политика за динамички избор на соодветна конфигурација во зависност од тековните услови на сообраќајот, без нарушување на дефинираниот ресурсен буџет.

Предложената рамка се базира на двостепен пристап. Во првата фаза се применува офлајн повеќекритериумска оптимизација, при што се генерира множество од Парето-ефикасни IDS-конфигурации. Секоја конфигурација во ова множество претставува јасно дефиниран и практично применлив компромис помеѓу квалитетот на детекција и потрошувачката на ресурси. Во втората фаза се применува онлајн учење на политика, при што контролер во реално време избира конфигурација од добиеното Парето множество врз основа на тековната состојба на мрежниот сообраќај и системските ресурси.

Ваквата поставеност овозможува раздвојување на процесот на идентификација на безбедни и ефикасни конфигурации од процесот на нивен динамички избор за време на извршување. На тој начин, предложената рамка овозможува намалување на потрошувачката на ресурси, ограничување на прекршувањата на ресурсниот буџет и задржување на интерпретабилноста на одлуките, што ја прави соодветна за примена кај IDS во ресурсно ограничени и нестационарни мрежни околини.

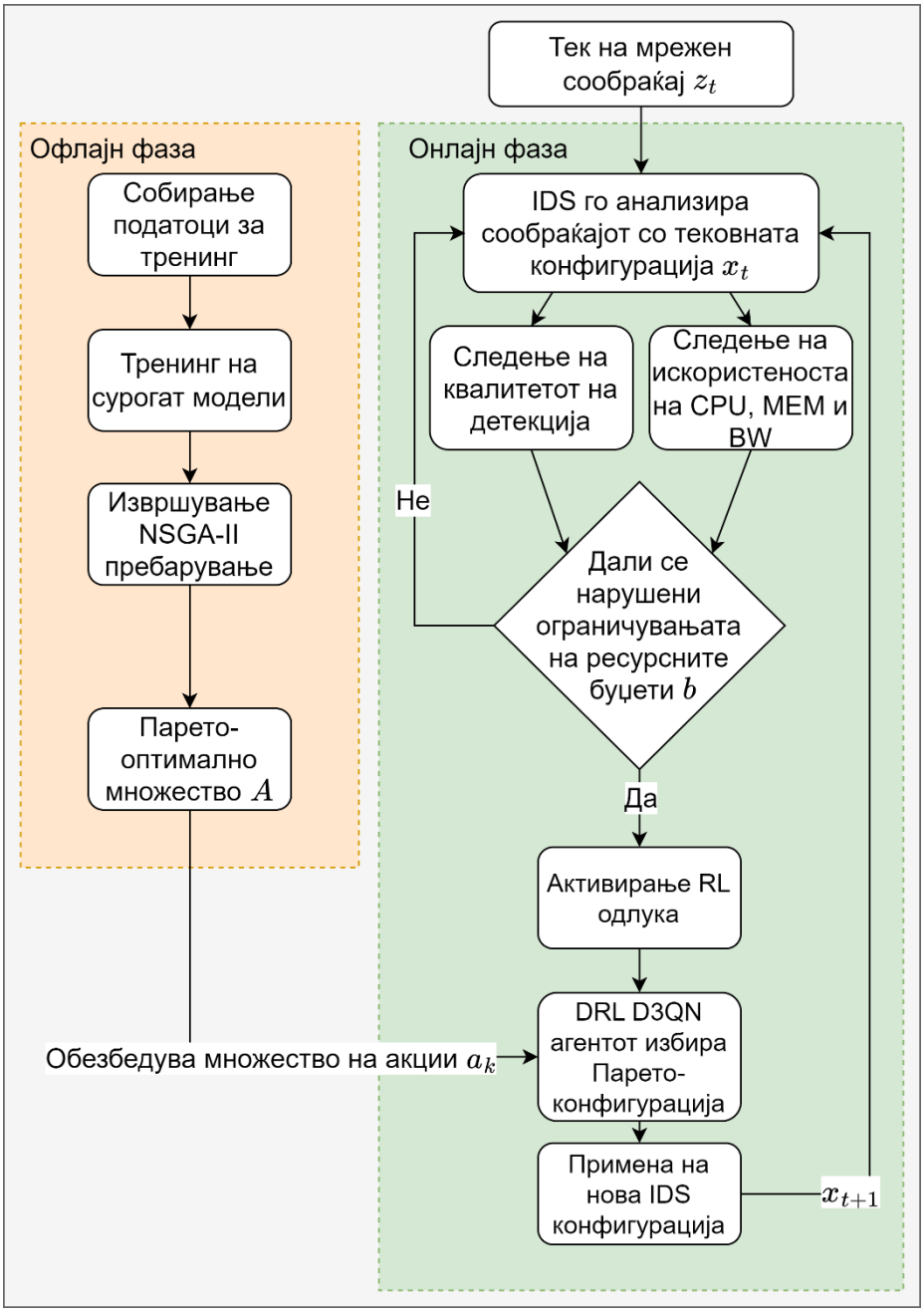
7.3. Математичка формулација на предложената рамка

7.3.1. Поставување на проблемот и нотација

Ова истражување ја разгледува динамичката конфигурација на лесен IDS кој функционира во услови на ресурсни ограничувања. Во секој дискретен временски момент t, системот ги набљудува карактеристиките на мрежниот сообраќај z_t и треба да избере IDS-конфигурација $x_t \in [0,1]^C$, каде што C го претставува бројот на разгледувани конфигурациски параметри. Целта е да се постигне компромис помеѓу квалитетот на детекција и потрошувачката на ресурси, при што во ова истражување се разгледуваат процесорската потрошувачка (CPU), работната меморија (MEM) и искористениот мрежен сообраќај (BW).

Потрошувачката на ресурси и детекциските перформанси се моделираат преку Борелово мерливи сурогат функции, нормализирани во интервалот $[0,1]$. Вредностите

добиени од овие функции се споредуваат со нормализираниот вектор на ресурсни буџети $b \in [0,1]^3$, кој ги дефинира дозволените граници за CPU, MEM и BW.



Слика 25: Архитектонска декомпозиција на A2DAPT-рамката преку поврзување на офлајн повеќекритериумското пребарување со NSGA-II и онлајн контролата со длабоко засилено учење

Со цел адресирање на поставениот проблем, предложената рамка е структурирана во две фази:

- офлајн фаза, каде што се применува надгледувано учење за изградба на сурогат модели за ресурсна потрошувачка и детекциски метрики, по што се користи NSGA-II за добивање дискретно множество од Парето-ефикасни конфигурации;
- онлајн фаза, каде што агент, базиран на D3QN со PER, избира конфигурација од ова множество, со цел адаптација кон тековната динамика на мрежниот сообраќај.

Декомпозицијата на предложената рамка е прикажана на слика 25.

Предложената рамка функционира врз податочен прозорец:

$$D = \{(x_i, z_i, r_i, y_i)\}_{i=1}^{N}. \qquad (34)$$

Во ова податочно множество, секој примерок i претставува еден временски прозорец на мрежен сообраќај. Векторот $x_i \in [0,1]^C$ ја кодира IDS-конфигурацијата, на пример праг, стапка на семплирање или длабочина на инспекција, додека $z_i \in [0,1]^M$ ги опфаќа нормализираните карактеристики на сообраќајот екстрахирани од соодветниот прозорец. Потрошувачката на ресурси е дефинирана како:

$$r_i = (r_i^{CPU}, r_i^{MEM}, r_i^{BW}) \in \mathbb{R}_+^3, \qquad (35)$$

а вистинската ознака е $y_i \in \{0,1\}$, каде што вредноста 1 означува малициозен (анг. malicious) сообраќај, а вредноста 0 означува легитимен (анг. *benign*) сообраќај.

Со цел да се обезбеди споредливост на влезните податоци, се применува min-max нормализација преку пресликувањата ϕ_x и ϕ_z, кои се обучуваат врз тренинг подмножеството, а потоа се применуваат врз валидациските и тест-податоците. Дополнително, ресурсните ограничувања се изразуваат преку нормализиран вектор на буџет:

$$b = (b^{CPU}, b^{MEM}, b^{BW}) \in [0,1]^3, \qquad (36)$$

кој ги дефинира дозволените граници според ресурсната метрика, користени при оптимизација и евалуација на политиката.

Со цел да се овозможи класификациски свесно земање на примероци и евалуација, се дефинираат следните индексни множества:

$$I_0 = \{i : y_i = 0\}, I_1 = \{i : y_i = 1\}. \qquad (37)$$

За дадена фракција на минисерија $f \in (0,1)$, се формира стратифицирана минисерија B преку земање легитимни примероци од I_0 и малициозни примероци од I_1, при што се задржува истиот однос помеѓу класите како во целокупното податочно множество. Ваквите минисерии се користат за проценка на целните функции во NSGA-II алгоритмот во офлајн

фазата, како и за генерирање на сигнали за награда при учење на политиката во онлајн фазата на предложената рамка.

7.3.2. Моделирање на детекција и ресурси

Со цел да се обезбедат брзи приближни проценки на потрошувачката на ресурси при извршување, во оваа фаза се обучуваат три сурогат регресиски модели. Овие модели како влез ја користат нормализираната IDS-конфигурација и карактеристиките на мрежниот сообраќај, односно $(x, z) \in [0,1]^{C+M}$, а како излез ја проценуваат соодветната ресурсна метрика: CPU, MEM или BW. За секоја ресурсна метрика $j \in \{CPU, MEM, BW\}$се дефинира сурогат функција:

$$f^j : [0,1]^{C+M} \to \mathbb{R}_+. \qquad (38)$$

Функцијата f^j се обучува врз основа на конкатенираниот влез (x_i, z_i) и набљудуваната целна вредност r_i^j. Секој сурогат модел се обучува преку минимизирање на средната квадратна грешка (анг. Mean Squared Error – MSE) над множеството за тестирање:

$$\min_{f^j} \frac{1}{N} \sum_{i=1}^{N} \left(f^j(x_i, z_i) - r_i^j \right)^2 . \qquad (39)$$

По обучувањето, трите модели се користат заеднички за да се добие векторска проценка на потрошувачката на ресурси за произволен пар (x, z):

$$\hat{r}(x, z) = (f^{CPU}(x, z), f^{MEM}(x, z), f^{BW}(x, z)). \qquad (40)$$

Овие сурогат модели имаат двојна улога во предложената рамка. Прво, тие ја дефинираат ресурсната компонента во повеќекритериумската оптимизациска функција што се оптимизира со NSGA-II, преку просечни вредности пресметани врз стратифицирани минисерии. Второ, тие обезбедуваат проценка на потрошувачката на ресурси во секој чекор од онлајн фазата, која се користи при пресметка на наградната функција и при пенализација на прекршувањата на ресурсниот буџет во процесот на учење и евалуација на политиката.

Со цел да се квантифицира квалитетот на детекцијата на стабилен и интерпретабилен начин, се обучува веројатносен класификатор. Неговиот влез е нормализираниот пар (x, z), каде што x ја претставува IDS-конфигурацијата, а z ги опфаќа тековните карактеристики на мрежниот сообраќај. Класификаторот ја проценува веројатноста дека даденият временски прозорец на сообраќај е малициозен:

$$g : [0,1]^{C+M} \to [0,1], \qquad (41)$$

при што:

$$g(x, z) \approx p(y = 1 \mid x, z).$$

Моделот се обучува преку минимизирање на стандардната бинарна крос-ентрописка загуба:

$$\min_{g} -\frac{1}{N}\sum_{i=1}^{N}[y_i \log g(x_i, z_i) + (1-y_i)\log(1-g(x_i, z_i))]\,. \qquad (42)$$

Со ова се обезбедува класификаторот да доделува висока веројатност на малициозни примероци и ниска веројатност на легитимни примероци. Поврзувањето на оваа проценка со Бернулиевиот модел овозможува дефинирање квантитативна мерка за квалитетот на детекцијата, зависна од вистинската ознака на примерокот. Оваа мерка, односно детекциска мерка зависна од ознаката (анг. label-aware detection score), директно се интегрира во офлајн и онлајн фазите на предложената рамка:

$$d(x, z; y) = \begin{cases} g(x, z), & y = 1 (\text{малициозен прозорец}), \\ 1 - g(x, z), & y = 0\ (\text{легитимен прозорец}). \end{cases} \qquad (43)$$

7.3.3. Офлајн повеќекритериумска оптимизација

Една од клучните предности на NSGA-II при оптимизација на IDS-конфигурации е неговата способност да генерира стабилни и разновидни Парето-фронтови, кои овозможуваат идентификација на повеќе компромисни решенија помеѓу квалитетот на детекција и потрошувачката на ресурси. Во предложената рамка, вредностите на целните функции се проценуваат преку стратифицирани минисерии, наместо преку целото податочно множество или преку поединечни временски прозорци. Ваквиот пристап има за цел да ја намали чувствителноста на оптимизацијата кон поединечни примероци и да придонесе за поголема робусност на добиените Парето-ефикасни конфигурации.

За дадена фиксна конфигурација x, целите на оптимизацијата се дефинираат како очекувани вредности врз непознатата распределба на карактеристиките на сообраќајот и ознаките:

$$(\mathbb{E}[\hat{r}^{CPU}(x, Z)], \mathbb{E}[\hat{r}^{MEM}(x, Z)], \mathbb{E}[\hat{r}^{BW}(x, Z)], 1 - \mathbb{E}[d(x, Z; Y)]), \qquad (44)$$

каде што Z и Y се случајни променливи кои ги претставуваат карактеристиките на сообраќајот и ознаките, $\hat{r}$ ги означува сурогат проценките за потрошувачката на ресурси, а d е детекциската мерка зависна од ознаката.

Бидејќи вистинската распределба не е позната, очекуваните вредности се апроксимираат со Монте Карло проценки пресметани врз стратифициран мини-серии B:

$$\bar{r}(x; B) = \frac{1}{|B|}\sum_{i \in B} \hat{r}(x, z_i), \bar{d}(x; B) = \frac{1}{|B|}\sum_{i \in B} d(x, z_i; y_i). \qquad (45)$$

Овие проценки го дефинираат векторот на цели:

$$\left(\bar{CPU}, \bar{MEM}, \bar{BW}, 1 - \bar{d}\right),$$

кој се користи во NSGA-II алгоритмот.

Алгоритмот NSGA-II се применува со цел да се пронајдат недоминирани, односно Парето-ефикасни конфигурации $x \in [0,1]^C$, кои ги минимизираат просечните ресурсни трошоци и детекциската грешка, изразена како $1 - \bar{d}(x; B)$. За даден стратифициран мини-серии B, оптимизацискиот проблем се дефинира како:

$$\min_{x \in [0,1]^C} \left(\bar{r}^{CPU}(x; B), \bar{r}^{MEM}(x; B), \bar{r}^{BW}(x; B), 1 - \bar{d}(x; B) \right). \qquad (45)$$

Согласно со принципите на NSGA-II, алгоритмот се извршува врз нормализираниот конфигурациски простор $[0,1]^C$, при што се добива множество од Парето-ефикасни IDS-конфигурации. Секоја од овие конфигурации претставува различен компромис помеѓу квалитетот на детекција и потрошувачката на ресурси. Добиеното множество решенија се зачувува и се користи како дискретен акциски простор во онлајн фазата:

$$\mathcal{A} = \{a_1, \dots, a_K\} \subset [0,1]^C.$$

7.3.4. Онлајн адаптација како Марков процес на одлучување

Во онлајн фазата, адаптивната конфигурација на IDS се моделира како Марков процес на одлучување. Во оваа формулација, агентот избира IDS-конфигурација од множество на Парето-ефикасни конфигурации, во зависност од тековната состојба на мрежниот сообраќај и зададените ресурсни буџети. На тој начин, процесот на адаптација се сведува на секвенцијално донесување одлуки, при што секоја одлука претставува избор на IDS-конфигурација за конкретен временски прозорец.

Состојба. Во секој временски чекор t, кој одговара на еден анализиран сообраќаен прозорец, состојбата се дефинира како:

$$s_t = (x_{t-1}, z_t; b), \qquad (46)$$

каде што x_{t-1} ја претставува IDS-конфигурацијата применета во претходниот временски прозорец, z_t ги претставува нормализираните карактеристики на сообраќајот во моментот t, а

$$b = (b^{CPU}, b^{MEM}, b^{BW}) \in [0,1]^3$$

е фиксен вектор на нормализирани ресурсни буџети. Ваквата репрезентација на состојбата ги комбинира претходната конфигурациска одлука, тековните карактеристики на мрежниот сообраќај и ресурсните ограничувања, со што агентот добива доволно информации за ресурсно свесен избор на следната конфигурација.

Акција. Акцискиот простор е ограничен на конечно множество $\mathcal{A}$ од Парето-ефикасни IDS-конфигурации добиени во офлајн фазата:

$$\mathcal{A} = \{a_1, \dots, a_K\}.$$

Во секој временски чекор t, агентот избира една акција $a_t \in \mathcal{A}$, која директно одговара на конкретна IDS конфигурација. Затоа применетата конфигурација во тековниот чекор се дефинира како:

$$x_t = a_{a_t}. \qquad (47)$$

Ова ограничување обезбедува системот да избира само конфигурации кои претходно се идентификувани како ефикасни компромиси помеѓу квалитетот на детекција и потрошувачката на ресурси. На овој начин се избегнува неконтролираното пребарување низ целиот конфигурациски простор и се намалува ризикот од избор на нестабилни или ресурсно неефикасни конфигурации.

Транзиција. По примената на избраната акција a_t, системот преминува во следната состојба преку набљудување нов сообраќаен прозорец, при што векторот на ресурсни буџети b останува непроменет. Следната состојба се дефинира како:

$$s_{t+1} = (x_t, z_{t+1}; b), \qquad (48)$$

каде што z_{t+1} ги претставува нормализираните карактеристики на новонабљудуваниот сообраќаен прозорец, добиен од реалната секвенца на податоци.

Казна за ресурси. Со цел да се земат предвид прекршувањата на ресурсниот буџет, потрошувачката на ресурси се проценува со користење на претходно обучените сурогат модели. За секоја ресурсна димензија $i \in \{CPU, MEM, BW\}$, прекршувањето се дефинира како:

$$pen_{t,i} = \max(0, \hat{r}_{t,i} - b^i),$$

каде што $\hat{r}_{t,i}$ ја претставува предвидената нормализирана потрошувачка на ресурсот i, а b^iе соодветниот нормализиран ресурсен буџет. Оваа формулација казнува само случаи во кои предвидената потрошувачка го надминува дозволениот буџет, додека конфигурациите кои остануваат во рамки на зададените ограничувања не се нагативно засегнати.

Вкупната казна за прекршување на ресурсниот буџет P_t се пресметува преку тежинска сума на прекршувањата по поединечни ресурси $pen_{t,i}$:

$$P_t = \sum_i w_i \cdot pen_{t,i}, \qquad (49)$$

каде што w_i се тежински коефициенти кои ја изразуваат релативната важност на секоја ресурсна димензија. Следејќи ги вообичаените пристапи кај повеќекритериумската оптимизација [119], прекршувањата на ресурсните ограничувања се претставуваат преку казнени членови $pen_{t,i}$, кои потоа се вклучуваат во наградната функција на RL агентот. На овој начин се насочува ресурсно-свесното однесување на агентот за време на извршувањето.

Награда. Наградата R_t ги комбинира детекциските перформанси $\tilde{S}_t$, казната за прекршување на ресурсниот буџет P_t и дополнителниот бонус за целосна усогласеност со ресурсните ограничувања B_t:

$$R_t = \lambda_d \tilde{S}_t - \lambda_c P_t + \lambda_b B_t. \qquad (50)$$

Членот $\tilde{S}_t$ја означува нормализираната детекциска мерка зависна од ознаката, изведена од веројатносниот класификатор дефиниран во равенка (43). Поконкретно:

$$S_t = d(x_t, z_t; y_t), \tilde{S}_t = S_t,$$

каде што $d(\cdot)$е детекциската функција, а x_t, z_tи y_t ги означуваат применетата IDS-конфигурација, карактеристиките на сообраќајот и вистинската ознака во временскиот чекор t, соодветно. Бидејќи класификаторот генерира веројатности во интервалот $[0,1]$, оваа мерка е природно нормализирана и директно споредлива меѓу различни конфигурации.

Бинарниот индикатор за усогласеност со ресурсниот буџет B_t се дефинира како:

$$B_t = \begin{cases} 1, & \text{ако } \hat{r}_{t,i} \le b^i, \ \forall i, \\ 0, & \text{инаку.} \end{cases}$$

Овој индикатор обезбедува дополнителен бонус за избор на конфигурации кои целосно ги задоволуваат сите ресурсни ограничувања.

Сите компоненти на наградната функција се дефинирани на споредливи нормализирани скали, со што се обезбедува стабилно учење и се спречува доминација на кој било поединечен член поради разлики во големината. Тежинските коефициенти λ_d, λ_cи λ_bго регулираат компромисот помеѓу квалитетот на детекција, ресурсната ефикасност и усогласеноста со буџетот. Бидејќи акцискиот простор е ограничен на Парето-ефикасни конфигурации, екстремните и неефикасни компромиси се природно ограничени, што придонесува за постабилно учење.

Дополнително, во наградната функција може да се вклучи и казнен член за промена на конфигурацијата, со цел да се обесхрабрат прекумерните промени на IDS конфигурацијата и да се поттикне оперативна стабилност.

Цел. Целта на агентот е да научи политика π, која ја максимизира очекуваната дисконтирана награда:

$$J(\pi) = \mathbb{E}_\pi \left[\sum_{t=1}^{\infty} \gamma^{t-1} R(s_t, a_t) \right], \qquad (51)$$

каде што $\gamma \in (0,1)$е фактор на дисконтирање.

Со вградување на Парето-ефикасниот акциски простор во MDP-формулацијата, научената политика овозможува адаптација на IDS-конфигурациите во текот на времето,

притоа почитувајќи ги ресурсните ограничувања. На овој начин, онлајн фазата овозможува динамично, ресурсно свесно и интерпретабилно управување со IDS-конфигурациите во услови на нестационарен мрежен сообраќај.

7.3.5. Алгоритам за учење: D3QN со PER

Со цел да се научи политика за избор од дискретното множество на Парето-ефикасни акции $\mathcal{A}$, предложената рамка користи D3QN со PER. Овој избор овозможува постабилно и поефикасно учење во услови кога повеќе акции може да имаат слична долгорочна вредност, што е карактеристично за конфигурации кои припаѓаат на ист Парето-фронт.

Апроксимација на вредносната функција

Акциско-вредносната функција $Q(s,a)$се апроксимира со користење на dueling архитектура, која ја разложува Q-функцијата на две компоненти: вредност на состојбата и предност на акцијата. Согласно со равенката на Белмановата оптималност [118] во оваа архитектура, Q-вредноста се дефинира како:

$$Q(s,a;\theta) = V(s;\theta) + A(s,a;\theta) - \frac{1}{|\ A\ |}\sum_{a'\in A} A(s,a';\theta), \qquad (52)$$

каде што θ ги претставува параметрите на онлајн мрежата. Во оваа формулација, $V(s;\theta)$ ја проценува вредноста на состојбата s, додека $A(s,a;\theta)$ја проценува релативната предност на изборот на акцијата aво таа состојба. Ваквата декомпозиција ја подобрува ефикасноста на учењето, особено во ситуации кога разликите помеѓу можните акции се мали.

Double DQN целни вредности

Со цел да се намали пристрасноста при проценување на Q-вредностите, изборот и евалуацијата на акциите се раздвојуваат преку Double DQN формулацијата. За дадена транзиција (s_t, a_t, r_t, s_{t+1}), целната вредност се пресметува како:

$$y_t = r_t + \gamma Q\left(s_{t+1}, \arg\max_{a'\in A} Q(s_{t+1},a';\theta);\theta^{-}\right), \qquad (53)$$

каде што θ^{-}ги означува параметрите на целната мрежа, кои периодично се синхронизираат со параметрите θ на онлајн мрежата. На овој начин, онлајн мрежата се користи за избор на најдобрата наредна акција, додека целната мрежа се користи за евалуација на нејзината вредност.

Приоритетно повторување на искуства

Транзициите се избираат од меморијата за повторување на искуства (анг. replay buffer) според нивниот приоритет. Приоритетот се дефинира врз основа на големината на грешката на временската разлика (анг. temporal-difference error – TD error):

$$p_i = (\mid \delta_i \mid + \varepsilon)^{\alpha}, P(i) = \frac{p_i}{\sum_j p_j}, \qquad (54)$$

каде што p_iе приоритетот на транзицијата i, $P(i)$е веројатноста таа транзиција да биде избрана од меморијата, δ_iе TD-грешката, $\varepsilon > 0$обезбедува ненулта веројатност за избор, а $\alpha \in [0,1]$го контролира степенот на приоритизација. Поголеми вредности на $\mid \delta_i \mid$укажуваат дека транзицијата носи поголема информациска вредност за процесот на учење, па затоа таквите транзиции имаат поголема веројатност да бидат избрани.

Со цел да се коригира пристрасноста воведена со неуниформното избирање транзиции, се применуваат тежини за земање примероци според важност:

$$w_i = \left(\frac{1}{N \cdot P(i)}\right)^{\beta}, \qquad (55)$$

каде што βпостепено се приближува кон 1 во текот на обучувањето, а Nја претставува големината на меморијата. Овие тежини ја намалуваат пристрасноста која произлегува од фактот дека транзициите не се избираат со еднаква веројатност.

Оптимизација

Параметрите на онлајн мрежата се ажурираат преку минимизирање на тежинска средноквадратна грешка помеѓу предвидените Q-вредности и D3QN целните вредности. За минисерии B, функцијата на загуба се дефинира како:

$$L(\theta) = \frac{1}{\mid B \mid} \sum_{i \in B} w_i \, (Q(s_i, a_i; \theta) - y_i)^2. \qquad (56)$$

За време на обучувањето се користи ε-*greed*y стратегија за истражување, при што εпостепено се намалува. Во почетните фази агентот почесто истражува различни конфигурации од Парето множеството, додека во подоцнежните фази сè повеќе ги избира конфигурациите со повисока очекувана вредност.

Со комбинирање на *dueling* архитектурата, Double DQN целните вредности и PER, процесот на учење станува постабилен и се насочува кон информативни транзиции, особено оние поврзани со прекршување на ресурсниот буџет или со нагли промени во квалитетот на детекција. Дополнително, ограничувањето на акцискиот простор на Парето-ефикасни конфигурации обезбедува научената политика да истражува само безбедни, интерпретабилни и оперативно релевантни IDS-поставки.

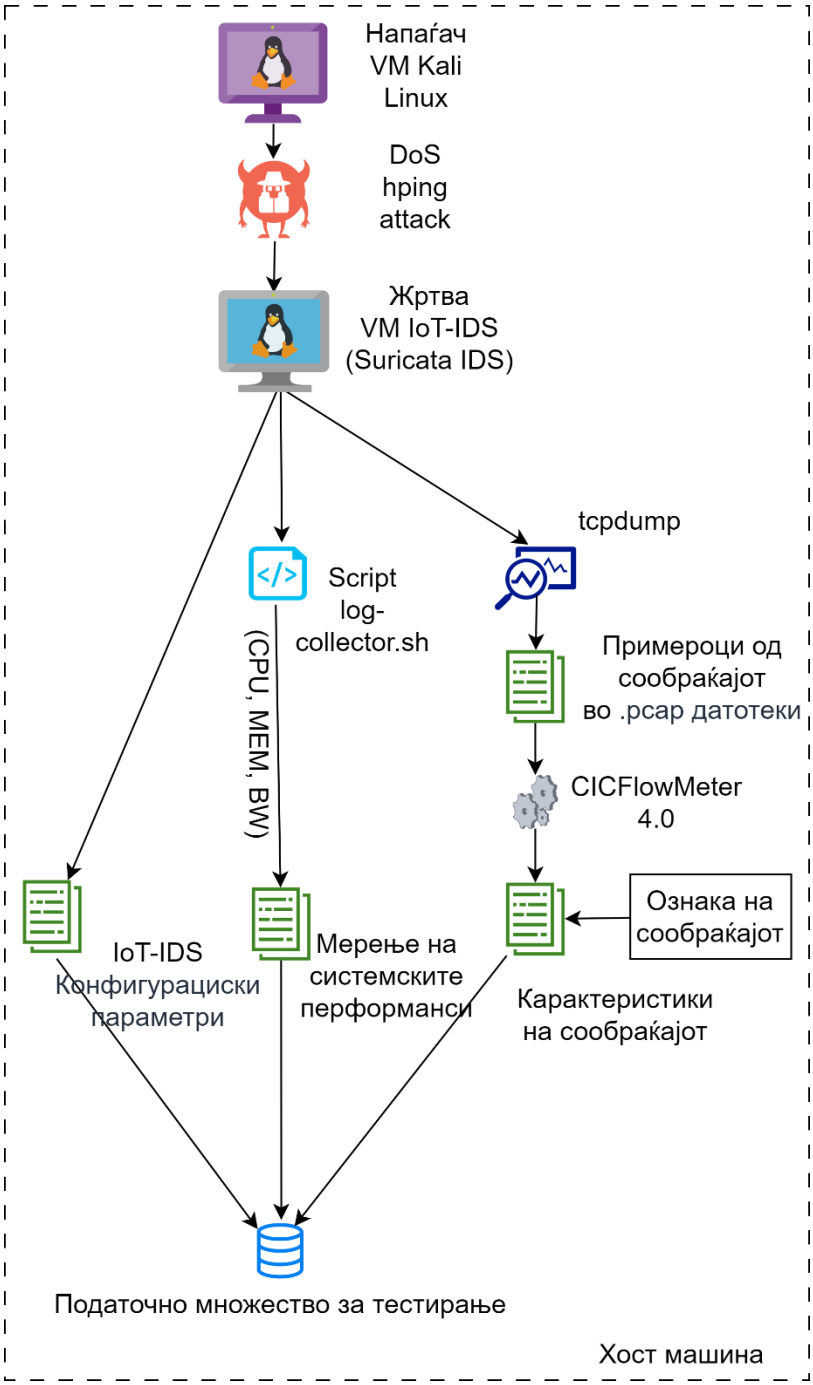
7.4. Експериментална евалуација

7.4.1. Експериментална поставка

Целта на експерименталната евалуација е да се утврди дали предложената A2DAPT-рамка може да ја намали потрошувачката на ресурси, притоа задржувајќи соодветен квалитет на детекција во услови на нестационарен мрежен сообраќај. За таа цел беше конструирано податочно множество кое ги комбинира карактеристики на мрежниот сообраќај, емпириски измерена потрошувачка на ресурси од IDS имплементиран во ресурсно ограничена околина, како и синтетички генерирани параметри на IDS-конфигурации усогласени со соодветните временски прозорци на сообраќајот.

Евалуацијата се спроведува преку двофазна експериментална постапка, која комбинира емпириско профилирање и анализа базирана на траги (анг. trace-driven analysis), како што е прикажано на слика 26. Во првата експериментална фаза беа извршени контролирани сценарија со легитимен и малициозен сообраќај врз IoT-базиран IDS-уред (IoT-IDS). За време на овие сценарија континуирано беа следени искористеноста на процесорот, работната меморија и мрежниот пропусен опсег. На овој начин беа добиени референтни профили на потрошувачка на ресурси, кои ја претставуваат емпириската основа за понатамошно моделирање и евалуација.

Мрежниот сообраќај беше сегментиран во фиксни временски прозорци, при што за секој прозорец беа евидентирани карактеристиките на сообраќајот, резултатите од детекцијата на IDS и активните параметри на IDS-конфигурацијата. Ваквата организација овозможува секој временски прозорец да се третира како посебен примерок во експерименталното податочно множество, усогласен со математичката формулација на предложената рамка.



Слика 26: Работен тек на првата експериментална фаза за прибирање емпириски хардверски профили и траги од мрежен сообраќај за конструирање на тренинг и тест податочни множества

Во втората експериментална фаза, прибраните временски прозорци од мрежниот сообраќај беа репродуцирани преку *trace-driven* симулација на посебен хост, со цел евалуација на A2DAPT-рамката во изолирана софтверска околина [20], согласно со математичката формулација дефинирана во претходната секција. Поради комбинираната

комплексност на конфигурацискиот простор на IDS и високата динамика на мрежниот сообраќај, директното профилирање на сите можни конфигурации во реално време е практично неизводливо. Затоа беше применето синтетичко скалирање на конфигурациските параметри, со цел апроксимација на потрошувачката на ресурси низ поширок дел од конфигурацискиот простор.

7.4.2. Протокол за евалуација и метрики

Рамката A2DAPT беше евалуирана преку споредба со статичка базна линија, конфигурирана да го максимизира квалитетот на детекција под фиксни ресурсни ограничувања. Двата пристапа беа применети врз иста тест-секвенца на мрежен сообраќај, со цел да се обезбеди директна споредливост на резултатите. За секој временски прозорец t, беа евидентирани проценетата потрошувачка на ресурси и квалитетот на детекција.

Кумулативната потрошувачка на ресурсот j во текот на временски хоризонт T се дефинира како:

$$R_j^{cum} = \sum_{t=1}^{T} f^j\,(x_t, z_t), \qquad (57)$$

каде што $f^j(\cdot)$ го претставува сурогат моделот за ресурсот $j \in \{CPU, MEM, BW\}$. Кај статичката базна линија, конфигурацијата е фиксна, односно $x_t = x^{static}$ за секое t, додека кај A2DAPT-конфигурацијата се одредува преку научената политика, односно $x_t = \pi(s_t)$.

Релативната заштеда во однос на статичката базна линија се дефинира како:

$$S_j = \frac{R_{j,base}^{cum} - R_{j,A2DAPT}^{cum}}{R_{j,base}^{cum}}. \qquad (58)$$

И статичката базна линија и адаптивната политика се евалуираат врз иста задржана тест-секвенца (анг. held-out test sequence), составена од нормализирани временски прозорци со познати референтни ознаки (анг. ground-truth labels).

Перформансите на детекција се споредуваат преку детекциската мерка зависна од ознаката, дефинирана во претходната математичка формулација, сумирана низ целиот временски хоризонт на евалуација. Дополнително, се евидентираат временските траги од избраните конфигурации, потрошувачката на ресурси и вредностите на наградата, со цел анализа на адаптивното однесување на системот.

7.5. Резултати и дискусија

Валидација на сурогат моделите

Бидејќи предложената A2DAPT-рамка се потпира на сурогат модели за проценка на потрошувачката на ресурси, во оваа фаза се евалуира нивната предиктивна точност и способност за генерализација. Секој сурогат модел, односно моделите за CPU, MEM и BW, беше обучен согласно со постапката опишана во претходната секција и евалуиран врз издвоено податочно множество за тестирање. За евалуација беа користени стандардни

регресиски метрики, вклучувајќи корен од средната квадратна грешка (анг. Root Mean Squared Error – RMSE), средна апсолутна грешка MAE, коефициент на детерминација R^2 и корелација.

Резултатите се сумирани во табела 4. Добиените вредности укажуваат на добри предиктивни перформанси кај сите ресурсни димензии, со високи вредности на R^2 и силна корелација помеѓу проценетите и измерените вредности.

Ресурс	RMSE	MAE	R^2	Корелација
CPU	0,121	0,072	0,885	0,971
MEM	0,070	0,087	0,855	0,973
BW	0,065	0,073	0,848	0,972

Табела 4: Регресиски метрики за перформансите на ресурсните сурогат модели за CPU, MEM и BW

Овие резултати покажуваат дека сурогат моделите соодветно го апроксимираат однесувањето на ресурсната потрошувачка и генерализираат кон претходно невидени конфигурации. Ваквата точност е доволна за потребите на повеќекритериумската оптимизација и онлајн адаптацијата, каде што конзистентното рангирање на конфигурациите е од особено значење. Во тој контекст, сурогат моделите обезбедуваат доверлива и ефикасна апроксимација за насочување на офлајн оптимизацискиот процес, како и за поддршка на донесувањето одлуки за време на извршувањето.

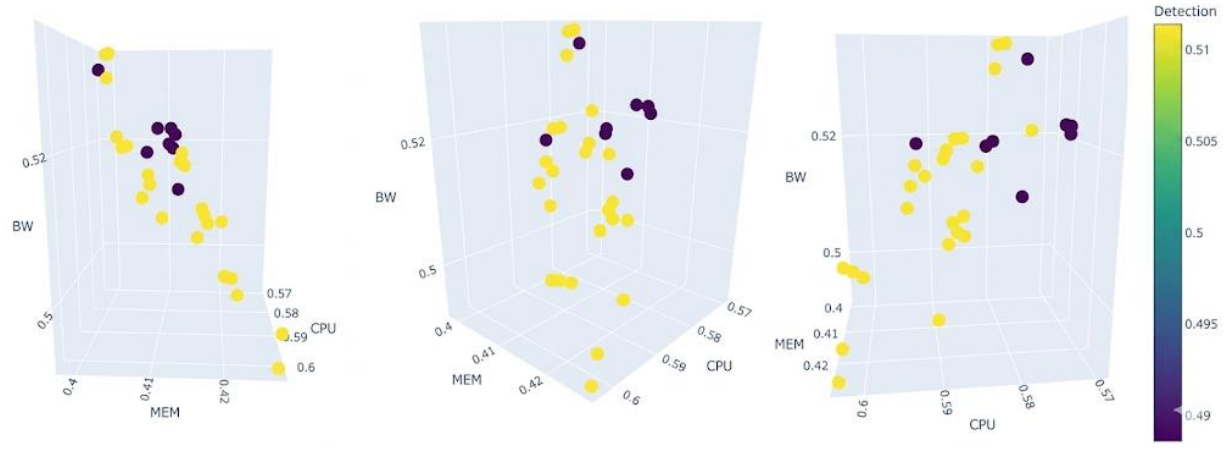
Парето-ефикасен конфигурациски простор

Офлајн оптимизацијата со NSGA-II резултираше со дискретно множество од Парето-ефикасни IDS-конфигурации, кои експлицитно ги опишуваат компромисите помеѓу квалитетот на детекција и потрошувачката на ресурси. Добиената Парето-фронта, прикажана на алика 27, опфаќа ограничен и структуриран регион од конфигурацискиот простор, при што вредностите на процесорската потрошувачка се движат приближно во интервалот $[0.56, 0.61]$, потрошувачката на меморија во интервалот $[0.39, 0.43]$, а пропусниот опсег во интервалот $[0.49, 0.53]$. Оваа распределба упатува на постоење на јасно изразена површина на компромисни решенија, а не на случајна дисперзија на конфигурации.

Во рамките на студијата за доказ на концептот, беше покажано дека предложената рамка ефективно функционира во услови на ресурсни ограничувања, при што во експериментите беше применет праг на ресурсен буџет од 0,6. Добиените Парето-ефикасни конфигурации експлицитно ги карактеризираат односите помеѓу детекцискатa мерка и користењето на системските ресурси, обезбедувајќи дискретен и интерпретабилен простор на акции за онлајн фазата на A2DAPT.

Анализата на Парето-фронтот покажува дека повисоки вредности на детекцискатa мерка најчесто се постигнуваат при умерени нивоа на ресурсна потрошувачка, додека екстремно ниските и екстремно високите вредности на ресурсите не водат нужно до подобри резултати. Поточно, конфигурациите со ниска потрошувачка на ресурси обично се поврзани со ослабен квалитет на детекција, додека зголеменото користење на ресурси не гарантира пропорционално подобрување на детекциските перформанси.

Дополнително, Парето-фронтот покажува релативно мазно и стабилно однесување, при што процесорската потрошувачка има најизразено влијание врз варијациите во детекциската мерка, додека потрошувачката на меморија останува релативно поконзистентна. Генерално, овие резултати потврдуваат дека офлајн оптимизацијата успешно идентификува значајни и оперативно релевантни компромиси, со што се обезбедува ефикасна основа за избор на конфигурации во услови на ресурсни ограничувања.



Слика 27: Тридимензионална визуализација на Парето-ефикасното множество конфигурации добиено со NSGA-II, при што се прикажани потрошувачката на ресурси (CPU, меморија и пропусен опсег), додека бојата ја претставува детекциската мерка

Однесување при онлајн адаптација

За време на онлајн работењето, научената политика динамички избира конфигурации од Парето-ефикасното множество како одговор на промените во мрежниот сообраќај. Трагата од извршувањето, прикажана на слика 28, покажува дека агентот врши префрлување помеѓу повеќе конфигурации, при што акциите како 7, 16 и 19 се избираат повеќепати. Ова укажува на фокусирање кон високовредни конфигурации поврзани со конзистентно високи награди ($a \approx b + 1.0$).

Во $t = 0$, изборот на акцијата 21 резултира со проценета потрошувачка на CPU од 0.697, што го надминува дефинираниот ресурсен буџет од 0,6 и доведува до негативна награда од $-0{,}063$. Во следните чекори, агентот преминува кон конфигурации со понизок ресурсен трошок, како акција 7, при што потрошувачката на CPU се намалува на 0,515 во $t = 1$ и на 0,256 во $t = 2$. Во двата случаи се постигнува награда од $+1{,}0$, што укажува на целосна усогласеност со ресурсните ограничувања и задржан квалитет на детекција според дефинираната наградна функција. Слично корективно однесување се забележува и во понатамошниот тек на извршувањето, каде што прекршувањата на буџетот најчесто се разрешуваат во рок од еден до два временски чекори.

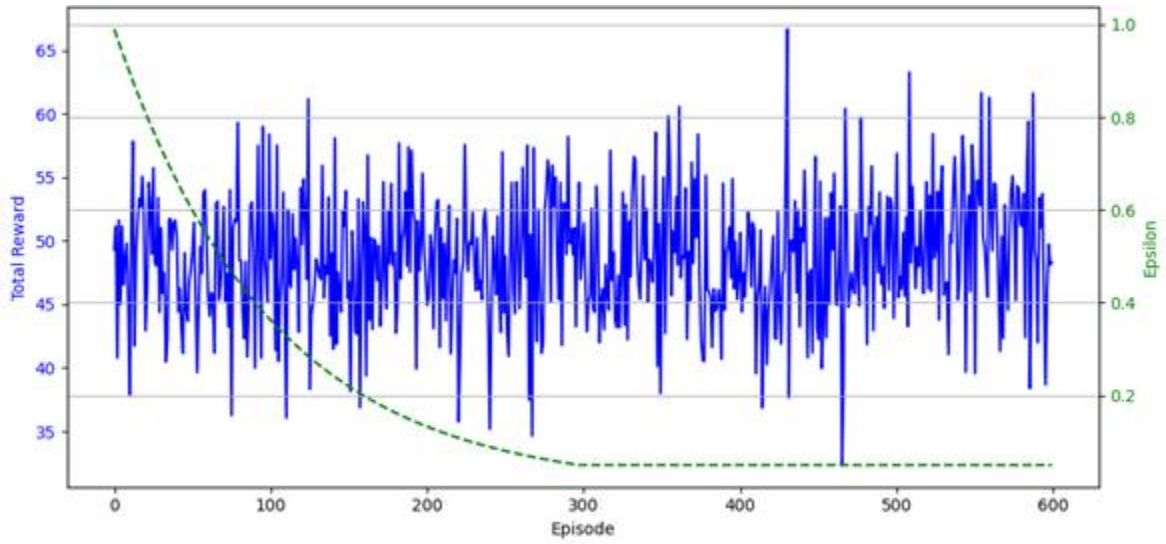
```
Runtime adaptation demo (following Regular vs Adaptive eval sequence):
 t= 0    action=21    cpu=0.697    mem=0.527    bw=0.608    reward=-0.063
 t= 1    action= 7    cpu=0.515    mem=0.381    bw=0.473    reward=+1.000
 t= 2    action= 7    cpu=0.256    mem=0.332    bw=0.581    reward=+1.000
 t= 3    action=19    cpu=0.541    mem=0.488    bw=0.452    reward=+1.000
 t= 4    action=19    cpu=0.677    mem=0.533    bw=0.444    reward=-0.034
 t= 5    action=19    cpu=0.492    mem=0.402    bw=0.597    reward=+1.000
 t= 6    action=19    cpu=0.582    mem=0.401    bw=0.585    reward=+0.000
 t= 7    action=12    cpu=0.662    mem=0.431    bw=0.419    reward=-0.020
 t= 8    action=19    cpu=0.608    mem=0.434    bw=0.561    reward=+1.034
 t= 9    action=19    cpu=0.656    mem=0.388    bw=0.518    reward=-0.014
 t=10    action=19    cpu=0.516    mem=0.441    bw=0.465    reward=+1.000
 t=11    action=16    cpu=0.645    mem=0.415    bw=0.477    reward=+0.997
 t=12    action=19    cpu=0.689    mem=0.428    bw=0.528    reward=-0.047
 t=13    action=19    cpu=0.385    mem=0.349    bw=0.468    reward=+0.000
 t=14    action=19    cpu=0.554    mem=0.414    bw=0.621    reward=+1.021
 t=15    action=19    cpu=0.394    mem=0.343    bw=0.391    reward=+1.000
 t=16    action=19    cpu=0.504    mem=0.420    bw=0.503    reward=+0.000
 t=17    action=19    cpu=0.531    mem=0.458    bw=0.505    reward=+0.000
 t=18    action=19    cpu=0.709    mem=0.466    bw=0.549    reward=+0.933
```

Слика 28: Трага од адаптација за време на извршување, која го прикажува динамичкото менување на конфигурациите од страна на DRL-агентот како одговор на мешан легитимен и DoS-сообраќај, со цел одржување усогласеност со ресурсниот буџет

Најголемиот дел од избраните конфигурации остануваат во рамките на ограничувањата за CPU, меморија и пропусен опсег, што укажува на ефективна адаптација свесна за ресурсните ограничувања. Повторливиот избор на ограничено подмножество акции и одржувањето високи вредности на наградата укажуваат дека агентот се стабилизира кон оперативно поволни режими. Ова однесување покажува дека предложената онлајн фаза може да обезбеди стабилно и интерпретабилно управување со IDS-конфигурациите во услови на нестационарен мрежен сообраќај.

Еволуцијата на епизодната награда и стапката на истражување ε за време на обучувањето е прикажана на слика 29. Параметарот за истражување се намалува експоненцијално и постепено се стабилизира околу $\varepsilon \approx 0{,}05$, што укажува на премин од почетна фаза со поизразено истражување кон фаза во која доминира експлоатација на веќе научените конфигурациски избори. И покрај присутните флуктуации, епизодните награди остануваат во релативно стабилен опсег, приближно помеѓу 40 и 60, со вредности најчесто концентрирани околу 50. Ова однесување укажува дека процесот на учење останува стабилен и по намалувањето на стапката на истражување.

Повремените пикови и падови во наградата може да се поврзат со стохастичката природа на мрежниот сообраќај, промените во временските прозорци и преостанатото ограничено истражување во текот на обучувањето. Сепак, не се забележува систематско влошување на наградата со намалувањето на ε, што укажува дека политиката не колабира кон неефикасно однесување. За разлика од поставките каде што главната цел е монотоно зголемување на вкупната награда, во оваа рамка поважно е одржувањето стабилни перформанси при истовремено почитување на ресурсните ограничувања и задржување на квалитетот на детекција. Набљудуваното однесување на наградата укажува дека агентот конвергира кон робусна политика која се адаптира на променлив сообраќај, истовремено одржувајќи ги ресурсните ограничувања и детекциските перформанси.



Слика 29: Еволуција на епизодната награда и стапката на истражување ε за време на обучувањето на DQN-агентот

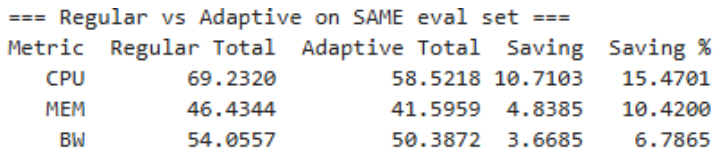
Заштеда на ресурси и перформанси на детекција

Во споредба со статичката базна линија, A2DAPT постигнува намалување на кумулативната потрошувачка на ресурси во текот на евалуацискиот период, како што е прикажано на слика 30. Потрошувачката на CPU се намалува од 69,23 на 58,52, што претставува заштеда од 10,71, односно 15,47 %. Искористеноста на меморијата се намалува од 46,43 на 41,60, што одговара на заштеда од 4,84, односно 10,42 %. Потрошувачката на пропусен опсег се намалува од 54,06 на 50,39, што претставува заштеда од 3,67, односно 6,79 %.

Бидејќи мрежниот сообраќај има стохастичка и нестационарна природа, апсолутните вредности на заштедите може да варираат помеѓу различни евалуациски извршувања. Сепак, добиените резултати покажуваат дека комбинирањето на офлајн идентификација на Парето-ефикасни конфигурации со онлајн учење политика овозможува мерливо намалување на ресурсната потрошувачка кај IDS-имплементации во ресурсно ограничени околини.

И покрај намалувањето на потрошувачката на ресурси, адаптивната политика задржува стабилно однесување во однос на детекцискатa мерка, што се потврдува преку високите вредности на наградата забележани за време на извршувањето, прикажани на слика 28. Ова укажува дека заштедата на ресурси е постигната без значајно нарушување на квалитетот на детекција според дефинираната наградна функција и користената детекциска мерка.

Дополнително, адаптивниот IDS покажува подобрена ресурсна ефикасност во споредба со статичката конфигурација. Ова укажува дека DRL-агентот, кој функционира како онлајн контролер, донесува ефективни избори од Парето-ефикасниот простор на акции. Добиените резултати покажуваат дека предложената рамка претставува практичен пристап за ресурсно свесна имплементација на IDS во ограничени околини, каде што ефикасното користење на CPU, меморијата и пропусниот опсег е од критично значење.



```
=== Regular vs Adaptive on SAME eval set ===
Metric  Regular Total  Adaptive Total  Saving  Saving %
   CPU        69.2320         58.5218 10.7103   15.4701
   MEM        46.4344         41.5959  4.8385   10.4200
    BW        54.0557         50.3872  3.6685    6.7865
```

Слика 30: Споредба на перформансите која ги прикажува придобивките во ресурсната ефикасност постигнати од адаптивниот DRL-агент во однос на статичката конфигурација, за CPU, меморија и пропусен опсег

Аблациска анализа

Со цел да се процени придонесот на поединечните компоненти во предложената рамка, спроведена е аблациска анализа преку споредба на целосната A2DAPT-рамка со две алтернативни варијанти. Првата варијанта претставува статичка конфигурација, кај која системот користи една фиксна IDS-конфигурација во текот на целата евалуација. Втората варијанта користи случајно избрано подмножество од конфигурации како простор на акции, наместо Парето-ефикасно множество добиено преку NSGA-II. Резултатите од анализата се прикажани во табела 5.

Варијанта	Просечна награда	Просечна детекција	CPU вкупно	MEM вкупно	BW вкупно	Прекршувања на буџет
Full A2DAPT	0,4593	0,4900	60,6419	42,3510	52,0187	69
Static Configuration (V1)	0,4322	0,5200	69,2320	46,4344	54,0557	100
Random Action Subset (V2)	0,4740	0,5500	67,3604	45,4875	53,8090	88

Табела 5: Аблациска анализа на придонесот на Парето-ефикасниот акциски простор и онлајн адаптацијата во A2DAPT-рамката

Резултатите покажуваат дека целосната A2DAPT-рамка постигнува најниска кумулативна потрошувачка на ресурси кај сите три ресурсни димензии и најмал број прекршувања на буџетот. Во споредба со статичката конфигурација, A2DAPT ја намалува потрошувачката на CPU, MEM и BW, а бројот на прекршувања на буџетот се намалува од 100 на 69. Ова ја потврдува важноста на онлајн адаптацијата за избор на соодветна конфигурација во услови на нестационарен мрежен сообраќај.

Статичката конфигурација, иако постигнува повисока просечна детекциска вредност од целосниот A2DAPT-модел, тоа го постигнува со значително поголема потрошувачка на ресурси и поголем број прекршувања на буџетот. Ова укажува дека фиксната конфигурација не обезбедува доволна флексибилност за балансирање помеѓу квалитетот на детекција и ресурсните ограничувања.

Варијантата со случајно избрано подмножество акции постигнува највисока просечна награда и просечна детекциска вредност, но истовремено има поголема потрошувачка на ресурси и повеќе прекршувања на буџетот во споредба со целосниот A2DAPT-модел. Овој резултат укажува дека повисоката детекциска вредност може да се постигне по цена на намалена ресурсна усогласеност. Бидејќи просторот на акции кај оваа варијанта не е структуриран преку Парето-ефикасни компромиси, добиеното однесување е помалку контролирано и потенцијално помалку стабилно во ресурсно ограничени услови.

Од анализата може да се заклучи дека комбинацијата од Парето-ефикасен акциски простор и онлајн засилено учење овозможува ресурсно-свесна адаптација со најдобра усогласеност со ресурсниот буџет. Иако алтернативните варијанти можат да постигнат повисоки вредности на детекциската мерка, тие тоа го прават со повисока ресурсна потрошувачка и почести прекршувања на ограничувањата. Затоа целосната A2DAPT-рамка претставува стабилен пристап за IDS-конфигурација во ресурсно ограничени и нестационарни мрежни околини.

7.6. Претпоставки и ограничувања

Иако формулацијата и евалуацијата на A2DAPT ја демонстрираат изводливоста на предложениот пристап и неговите потенцијални придобивки, постојат неколку ограничувања кои треба да се земат предвид при интерпретација на резултатите.

Прво, онлајн фазата на адаптација се базира на Марковата поставеност, според која следната состојба зависи од тековната состојба и избраната акција. Со оваа формулација не се моделираат експлицитно долгорочните временски зависности, делумната набљудливост на мрежниот сообраќај и повеќефазните нападни сценарија кои бараат историски контекст. Ова ограничување може да се адресира преку проширување на состојбата со краткорочен временски контекст, на пример $\tilde{z}_t = [z_{t-k}, \dots, z_t]$, или преку примена на рекурентни варијанти на DRL-агентот. Ваквите проширувања би ја зачувале основната архитектура на рамката, а истовремено би овозможиле подобро моделирање на нападни обрасци кои еволуираат низ времето.

Второ, офлајн повеќекритериумската оптимизација се базира на стратифицирани минисерии извлечени од ограничени податочни множества. Кога доменот на сообраќај е тесен или доминиран од конкретен тип напад, добиениот Парето-фронт може да не се генерализира доволно добро кон други типови напади или мешани сценарија. Поради тоа, потребни се пообемни податочни множества кои опфаќаат различни типови оптоварувања, класи на напади и подолги временски интервали, со цел добивање Парето-ефикасни множества применливи во различни режими на мрежен сообраќај. Дополнително, иако NSGA-II е соодветен за конфигурациски простори со умерена димензионалност, неговата пресметковна сложеност може да се зголеми со раст на бројот на параметри, што упатува на потреба од редукција на конфигурацискиот простор или примена на поефикасни сурогатно поддржани методи за пребарување.

Трето, предложената рамка користи *min-max* нормализација на карактеристиките на сообраќајот, која може да биде чувствителна на вредности надвор од опсегот на податоците за обука. Екстремните вредности, како многу високите стапки на пакети или невообичаените временски интервали помеѓу пакетите, може да доведат до вредности надвор од очекуваниот нормализиран интервал и да влијаат врз стабилноста на учењето. Потенцијалното решение е примена на поцврсти техники за нормализација, како скалирање базирано на перцентили, отсекување на екстремни вредности или периодична рекалибрација на нормализациските граници.

Четврто, наградната функција се базира на рачно избрани тежински коефициенти кои го дефинираат компромисот помеѓу квалитетот на детекција, потрошувачката на ресурси и усогласеноста со ресурсниот буџет. Перформансите на агентот и стабилноста на учењето може да бидат чувствителни на изборот на овие параметри. Сепак, ограничувањето на

акцискиот простор на Парето-ефикасните конфигурации го намалува ризикот од избор на екстремно неефикасни конфигурации. Во идните истражувања треба да се разгледаат систематските механизми за избор или адаптација на тежинските коефициенти, како и воведување експлицитни казни за честите промени на конфигурацијата со цел подобрување на оперативната стабилност.

Петто, засиленото учење воведува добро познати предизвици, како неефикасност во однос на бројот на потребни примероци, нестабилност за време на обучувањето и чувствителност кон дизајнот на наградната функција [120]. Дополнително, процесот на учење на политиката зависи од изборот на хиперпараметрите, што може да влијае врз стабилноста на конвергенцијата и генерализацијата кон претходно невиден мрежен сообраќај. Во оперативни IDS-околини, неконтролираното истражување може да доведе до небезбедни конфигурации или до конфигурации кои ги нарушуваат ресурсните ограничувања. Во A2DAPT овој ризик е намален преку ограничување на просторот на акции на Парето-ефикасните конфигурации, но не е целосно елиминиран, поради што е потребно внимателно управување со процесот на обучување и валидација пред реалната имплементација.

На крај, евалуацијата е спроведена во симулирана лабораториска поставка и врз еден IoT-IDS-јазол. Иако ваквата поставеност овозможува контролирана и репродуцибилна анализа, таа не ги опфаќа сите комплексности на дистрибуирани или повеќејазолни имплементации. Во такви околини се појавуваат дополнителни предизвици, како координација помеѓу јазлите, конзистентност на адаптивните политики и комуникациски трошок, што може да влијае врз скалабилноста и системските перформанси. Сепак, рамката е модуларна и може да се прошири кон дистрибуираните околини преку комбинирање централизирана Парето-оптимизација со независни агенти по јазол или преку воведување механизми за координација. Истражувањето на дистрибуираната оптимизација и комуникациски свесните политики претставува значајна насока за понатамошна работа.

7.7. Заклучок

Во оваа глава беше претставена A2DAPT, унифицирана математичка рамка за адаптивна и ресурсно свесна конфигурација на IDS. Предложениот пристап ја формализира конфигурацијата на IDS како проблем на секвенцијално донесување одлуки под ресурсни ограничувања. Рамката комбинира сурогат модели за проценка на потрошувачката на CPU, меморија и пропусен опсег, веројатносен детектор за проценка на квалитетот на детекција, офлајн повеќекритериумска оптимизација со NSGA-II и онлајн адаптација базирана на длабоко засилено учење.

Експерименталната евалуација беше спроведена врз сопствено податочно множество, добиено од IoT-IDS тестна околина изложена на легитимен и SYN-flood сообраќај. Резултатите покажаа дека A2DAPT овозможува мерливо намалување на ресурсната потрошувачка во споредба со статичката базна линија. Во репрезентативниот евалуациски интервал, адаптивната политика постигна намалување на кумулативната потрошувачка на CPU од приближно 15,47 %, на меморија од околу 10,42 % и на пропусен опсег од околу 6,79 %, без значајно нарушување на квалитетот на детекција според користената детекциска мерка и наградна функција. Временските траги дополнително покажаа дека научената политика реагира на промени во сообраќајот, ги ограничува

долготрајните прекршувања на ресурсните буџети и се насочува кон подмножество од Парето-ефикасни конфигурации.

Дополнителна предност на предложената рамка е нејзината интерпретабилност. Секоја акција на DRL-агентот е поврзана со конкретна IDS-конфигурација добиена преку офлајн Парето-оптимизација, додека наградната функција експлицитно ги моделира ресурсните ограничувања и компромисот помеѓу детекцискиот квалитет и потрошувачката на ресурси. Ограничувањето на акцискиот простор на Парето-ефикасни конфигурации го намалува ризикот од небезбедно или неефикасно истражување, што ја прави рамката погодна за примена во IoT *gateway* уреди, *edge* инфраструктури и други средини со ограничени ресурси.

Сепак, добиените резултати треба да се интерпретираат во рамките на ограничувањата на спроведената евалуација. Студијата за доказ на концептот е реализирана врз лабораториско податочно множество со ограничен тип напад и релативно тесен домен на сообраќај. Сурогат моделите може да имаат ограничена генерализација во посложени оперативни услови, а *min-max* нормализацијата може да биде чувствителна на вредности надвор од опсегот на податоците за обука. Дополнително, перформансите на DRL-политиката зависат од изборот на тежинските коефициенти, пенализациските параметри и хиперпараметрите на обучување.

Идните истражувања може да ја прошират A2DAPT-рамката преку вклучување дополнителни цели, како латентност, загуба на пакети или обем на аларми, како и преку примена на ограничено засилено учење или Лагранжови методи за експлицитно управување со ресурсните буџети. Дополнителните насоки вклучуваат динамичко ажурирање на сурогат моделите и Парето множествата при појава на концептуален *drift,* тестирање врз поразновидни податочни множества, примена кај хетерогени IDS-јазли и координација на повеќе сензори во дистрибуираните околини.

Севкупно, резултатите покажуваат дека комбинирањето на офлајн Парето-оптимизацијата со онлајн адаптацијата базирана на DRL претставува применлив и интерпретабилен пристап за управување со компромисот помеѓу квалитетот на детекција и ресурсната потрошувачка кај IDS во нестационарни и ресурсно ограничени мрежни околини.

8. Заклучок и понатамошна работа

Современите информациски и комуникациски инфраструктури функционираат во услови на зголемена комплексност, динамичен мрежен сообраќај и сè поголема изложеност на разновидни сајбер-закани. Во такви услови, системите за детекција на упади имаат клучна улога во препознавањето на малициозни активности, но нивната ефективност сè повеќе зависи од способноста да се приспособуваат на променливи услови и ограничени ресурси. Овој предизвик е особено изразен кај ресурсно ограничените средини, како што се рабните инфраструктури, уредите од Интернет на нештата и помалите организациски мрежи, каде што примената на сложени безбедносни механизми мора да биде усогласена со достапните процесорски, мемориски и мрежни капацитети. Поради тоа, потребни се пристапи кои истовремено ја земаат предвид детекциската ефикасност, потрошувачката на ресурси и реалните организациски услови во кои безбедносните решенија се применуваат.

Во оваа дисертација е развиен интегриран и ресурсно свесен пристап за унапредување на системите за детекција на упади во динамички мрежни средини. Истражувањето ги поврзува социотехничките предуслови за примена на безбедносни решенија, експерименталната основа за нивна проверка и техничките механизми за детекција, анализа и адаптивна оптимизација. На овој начин, дисертацијата не ја разгледува сајбер-безбедноста само како изолиран технички проблем, туку како мултидисциплинарен процес во кој организациската подготвеност, квалитетот на податоците, детекцијата на аномалии и управувањето со ресурсите се меѓусебно поврзани. Централно место во оваа поставеност има A2DAPT-рамката, која претставува двостепен Парето-воден пристап за адаптивна и ресурсно-свесна оптимизација на системи за детекција на упади.

Главната истражувачка хипотеза на дисертацијата се однесуваше на можноста преку интегриран и ресурсно свесен пристап да се унапреди управувањето со системите за детекција на упади во динамички и ресурсно ограничени мрежни средини. Спроведените истражувања ја поддржуваат оваа хипотеза, бидејќи покажуваат дека ваквиот пристап овозможува поцелосно разгледување на проблемот на детекција и управување со ресурси. Во таа целина, A2DAPT има централна улога поради тоа што ја формализира и експериментално ја потврдува можноста за динамички избор на конфигурации кои го балансираат квалитетот на детекција и потрошувачката на ресурси.

Во однос на првата посебна хипотеза, резултатите од анализата на сајбер-безбедносната подготвеност на малите организации покажуваат дека примената на таксономијата за проценка на сајбер-безбедносна подготвеност и ризик овозможува идентификација на односот помеѓу перцепцијата на ризик, реалното ниво на имплементирани безбедносни мерки и организациските предуслови за примена на технички безбедносни решенија. Квантитативната анализа спроведена врз примерок од мали организации во Република Македонија покажа дека помалку од една четвртина од анализираните организации се позиционирани во квадрантот на рамнодушност, додека најголем дел се позиционирани во квадрантот на аверзија кон загуба. Овој резултат укажува дека кај значителен дел од организациите постои релативно повисоко ниво на имплементирани безбедносни мерки, но истовремено и пониска перцепција на сајбер-ризик. Ваквиот однос ја потврдува потребата техничките решенија за сајбер-безбедност да се разгледуваат во поширок организациски контекст, бидејќи нивната ефективност не

зависи само од достапноста на технологијата, туку и од свесноста, перцепцијата на ризик, ресурсите и начинот на донесување одлуки кај организациите.

Во однос на втората посебна хипотеза, во дисертацијата беше дизајнирана и имплементирана контролирана тестна информациско-технолошка околина, базирана на организациска доменска мрежа управувана преку интегриран центар за мрежни операции и центар за безбедносни операции со примена на алатки со отворен код. Спроведената демонстрација покажа дека ваквата околина овозможува прибирање различни типови податоци од повеќе извори, вклучувајќи мрежен сообраќај, трансакциски логови и системски настани од крајни уреди. Со имплементација на сензори и мониторинг компоненти на повеќе точки во мрежата беше овозможено структурирано прибирање податоци потребни за анализа на мрежни активности, детекција на аномалии и евалуација на системи за детекција на упади. Дополнително, резултатите ја потврдија применливоста на алатките со отворен код како флексибилна, економична и доверлива основа за развој, тестирање и валидација на современи сајбер-безбедносни решенија.

Во однос на третата посебна хипотеза, во дисертацијата беше презентиран и евалуиран автоенкодерски модел чувствителен на реконструкциска загуба за детекција на аномалии во мрежниот сообраќај. Експерименталните резултати покажаа дека реконструкциската загуба може да се користи како релевантен индикатор за разграничување помеѓу легитимен и малициозен мрежен сообраќај. Во сите анализирани експерименти беше забележана разлика помеѓу вредностите на реконструкциската загуба кај легитимниот и малициозниот сообраќај, при што најизразено разграничување беше постигнато кај сценаријата со DDoS, Infiltration и Web Application Attack. Кај Port Scan активностите беше забележано поголемо преклопување помеѓу легитимниот и малициозниот сообраќај, што укажува дека овој тип напад претставува посложен случај за детекција и бара дополнителна оптимизација на архитектурата, изборот на карактеристики или прагот за одлучување. Сепак, резултатите ја потврдуваат употребната вредност на автоенкодерскиот пристап како ран аналитички сегмент во повеќеслојна безбедносна инфраструктура, особено во ресурсно ограничени средини каде што е потребна груба селекција на нормален и нестандарден сообраќај пред негово проследување кон посложени безбедносни механизми.

Во однос на четвртата посебна хипотеза, во дисертацијата беше предложена A2DAPT-рамката како унифициран математички и експериментален пристап за адаптивна и ресурсно-свесна конфигурација на системи за детекција на упади. Предложениот пристап ја формализира конфигурацијата на системот за детекција на упади како повеќекритериумски оптимизациски проблем и како проблем на секвенцијално донесување одлуки под ресурсни ограничувања. Рамката комбинира сурогат модели за проценка на потрошувачката на процесорски ресурси, меморија и мрежен пропусен опсег, веројатносен детектор за проценка на квалитетот на детекција, офлајн повеќекритериумска оптимизација со генетски алгоритам со недоминирачко сортирање и онлајн адаптација базирана на длабоко засилено учење.

Експерименталната евалуација на A2DAPT, спроведена врз сопствено податочно множество добиено од тестна околина изложена на легитимен и SYN-flood сообраќај, покажа дека предложената рамка овозможува мерливо намалување на ресурсната потрошувачка во споредба со статичка базна линија. Во репрезентативниот евалуациски интервал, адаптивната политика постигна намалување на кумулативната потрошувачка на

процесорски ресурси од приближно 15,47 %, на меморија од околу 10,42 % и на мрежен пропусен опсег од околу 6,79 %, без значајно нарушување на квалитетот на детекција според користената детекциска мерка и наградна функција. Дополнително, резултатите покажаа дека целосната A2DAPT-рамка постигнува најниска кумулативна потрошувачка на ресурси, при што бројот на прекршувања на ресурсниот буџет се намалува од 100 на 69 во споредба со статичката конфигурација. Временските траги покажаа дека научената политика реагира на промени во сообраќајот, ги ограничува долготрајните прекршувања на ресурсните буџети и се насочува кон подмножество од Парето-ефикасни конфигурации.

Сумирано, резултатите од сите истражувачки сегменти ја поддржуваат главната истражувачка хипотеза, а научниот придонес на дисертацијата се состои во развој на интегриран пристап кој не ја разгледува сајбер-безбедноста исклучиво како технички проблем, туку како повеќеслоен систем.

Практичната вредност на дисертацијата произлегува од можноста предложените решенија да се применат во средини каде што ресурсите се ограничени, а мрежните услови се променливи. CyPRisT-анализата би се користела во идентификација на организациски профили и јазови во сајбер-безбедносната подготвеност. Тестната околина би дала значен придонес како основа за понатамошни истражувања, едукација, валидација на безбедносни механизми и развој на модели базирани на машинско и длабоко учење. Автоенкодерскиот пристап има употребна вредност при примена како дополнителен механизам за рана анализа и груба селекција на мрежниот сообраќај. Рамката A2DAPT може да се користи како основа за адаптивно управување со системи за детекција на упади во уреди од типот IoT *gateway, edge* инфраструктури и други мрежни средини со ограничени ресурси.

И покрај добиените резултати, потребно е да се истакнат и ограничувањата на истражувањето. Анализата на сајбер-безбедносната подготвеност е спроведена врз ограничен примерок од мали организации, што отвора простор за проширување на примерокот и подетална анализа според сектор, големина, буџет и организациска зрелост. Евалуацијата на автоенкодерскиот модел покажа различна успешност кај различни типови напади, што укажува на потреба од дополнително истражување на архитектурата, изборот на карактеристики и механизмите за поставување праг на одлучување. Рамката A2DAPT е евалуирана како доказ на концепт врз лабораториско податочно множество со ограничен домен на сообраќај и ограничен тип напад, поради што идните истражувања треба да ја прошират евалуацијата кон поразновидни сценарија, поголем број типови напади и посложени оперативни услови. Притоаидните истражувања може да се насочат кон проширување на A2DAPT-рамката со дополнителни оптимизациски цели, како латентност, загуба на пакети, обем на аларми или енергетска потрошувачка.

Референци

[1] P. Mell and T. Grance, “The NIST definition of cloud computing,” 2011.

[2] A. Al-Dulaimy *et al.*, “The computing continuum: From IoT to the cloud,” *Internet of Things*, vol. 27, p. 101272, Oct. 2024, doi: 10.1016/j.iot.2024.101272.

[3] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, “A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things,” *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4004–4022, Mar. 2021, doi: 10.1109/JIOT.2020.3015432.

[4] EU ENISA, “Cyber Security Culture in Organisations,” 2017. Accessed: May 10, 2026. [Online]. Available: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

[5] T. McEvoy and S. Kowalski, “Deriving Cyber Security Risks from Human and Organizational Factors – A Socio-technical Approach,” *Complex Systems Informatics and Modeling Quarterly*, pp. 47–64, May 2019, doi: 10.7250/csimq.2019-18.03.

[6] D. Eilts, “An empirical assessment of cybersecurity readiness and resilience in small businesses,” 2020.

[7] K. Scarfone and P. Mell, “Guide to intrusion detection and prevention systems (idps),” *NIST special publication*, vol. 800, no. 2007, p. 94, 2007.

[8] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, “Survey of intrusion detection systems: techniques, datasets and challenges,” *Cybersecurity*, vol. 2, no. 1, p. 20, Dec. 2019, doi: 10.1186/s42400-019-0038-7.

[9] A. Buczak and E. Guven, “A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection,” *IEEE Communications Surveys & Tutorials*, vol. 18, p. 1, May 2015, doi: 10.1109/COMST.2015.2494502.

[10] R. Sommer and V. Paxson, “Outside the Closed World: On Using Machine Learning for Network Intrusion Detection,” in *Proceedings - IEEE Symposium on Security and Privacy*, May 2010, pp. 305–316. doi: 10.1109/SP.2010.25.

[11] I. Goodfellow, “Deep learning,” 2016, *MIT press*.

[12] Y. Song, S. Hyun, and Y.-G. Cheong, “Analysis of Autoencoders for Network Intrusion Detection,” *Sensors*, vol. 21, no. 13, p. 4294, Jun. 2021, doi: 10.3390/s21134294.

[13] G. Pang, C. Shen, L. Cao, and A. Van Den Hengel, “Deep Learning for Anomaly Detection,” *ACM Comput. Surv.*, vol. 54, no. 2, pp. 1–38, Mar. 2022, doi: 10.1145/3439950.

[14] H.-I. Liu *et al.*, “Lightweight Deep Learning for Resource-Constrained Environments: A Survey,” *ACM Comput. Surv.*, vol. 56, no. 10, pp. 1–42, Oct. 2024, doi: 10.1145/3657282.

[15] E. C. P. Neto, S. Iqbal, S. Buffett, M. Sultana, and A. Taylor, “Deep learning for intrusion detection in emerging technologies: a comprehensive survey and new perspectives,” *Artif. Intell. Rev.*, vol. 58, no. 11, p. 340, Aug. 2025, doi: 10.1007/s10462-025-11346-z.

[16] A. Hozouri, A. Mirzaei, and M. Effatparvar, “A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges,” *Discover Artificial Intelligence*, vol. 5, no. 1, p. 314, Nov. 2025, doi: 10.1007/s44163-025-00578-1.

[17] H. Dreger, A. Feldmann, V. Paxson, and R. Sommer, “Predicting the Resource Consumption of Network Intrusion Detection Systems,” in *Recent Advances in Intrusion Detection*, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 135–154. doi: 10.1007/978-3-540-87403-4_8.

[18] N. Kashyap, A. C. Kumari, and R. Chhikara, “Multi-objective Optimization using NSGA II for service composition in IoT,” *Procedia Comput. Sci.*, vol. 167, pp. 1928–1933, 2020, doi: 10.1016/j.procs.2020.03.214.

[19] K. Deb, A. Pratap, S. Agarwal, and T. Meyarivan, “A fast and elitist multiobjective genetic algorithm: NSGA-II,” *IEEE Transactions on Evolutionary Computation*, vol. 6, no. 2, pp. 182–197, Apr. 2002, doi: 10.1109/4235.996017.

[20] R. S. , & B. A. G. Sutton, *Reinforcement learning: An introduction*, 2nd ed. The MIT Press, 2018.

[21] V. Mnih *et al.*, “Human-level control through deep reinforcement learning,” *Nature*, vol. 518, no. 7540, pp. 529–533, Feb. 2015, doi: 10.1038/nature14236.

[22] Z. Wang, T. Schaul, M. Hessel, H. van Hasselt, M. Lanctot, and N. de Freitas, “Dueling Network Architectures for Deep Reinforcement Learning,” Apr. 2016.

[23] H. Hasselt, “Double Q-learning,” *Adv. Neural Inf. Process. Syst.*, vol. 23, 2010.

[24] T. Schaul, J. Quan, I. Antonoglou, and D. Silver, “Prioritized Experience Replay,” Feb. 2016.

[25] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, “A Design Science Research Methodology for Information Systems Research,” *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, Dec. 2007, doi: 10.2753/MIS0742-1222240302.

[26] C. M. Bishop and N. M. Nasrabadi, *Pattern recognition and machine learning*, vol. 4, no. 4. Springer, 2006.

[27] A. Krizhevsky, I. Sutskever, and G. E. Hinton, “Imagenet classification with deep convolutional neural networks,” *Adv. Neural Inf. Process. Syst.*, vol. 25, 2012.

[28] M. Ranzato, A. Szlam, J. Bruna, M. Mathieu, R. Collobert, and S. Chopra, “Video (language) modeling: a baseline for generative models of natural videos,” *arXiv preprint arXiv:1412.6604*, 2014.

[29] A. Van Den Oord *et al.*, “Wavenet: A generative model for raw audio,” *arXiv preprint arXiv:1609.03499*, vol. 12, no. 1, 2016.

[30] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, “Bert: Pre-training of deep bidirectional transformers for language understanding,” in *Proceedings of the 2019 conference of the*

North American chapter of the association for computational linguistics: human language technologies, volume 1 (long and short papers), 2019, pp. 4171–4186.

[31] G. Montúfar, R. Pascanu, K. Cho, and Y. Bengio, "On the number of linear regions of deep neural networks," *Adv. Neural Inf. Process. Syst.*, vol. 27, 2014.

[32] K. He, X. Zhang, S. Ren, and J. Sun, "Delving deep into rectifiers: Surpassing human-level performance on imagenet classification," in *Proceedings of the IEEE international conference on computer vision*, 2015, pp. 1026–1034.

[33] A. Zhang, Y. Wu, and J. Pineau, "Natural environment benchmarks for reinforcement learning," *arXiv preprint arXiv:1811.06032*, 2018.

[34] J. Kaplan *et al.*, "Scaling laws for neural language models," *arXiv preprint arXiv:2001.08361*, 2020.

[35] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," *Proceedings of the IEEE*, vol. 86, no. 11, pp. 2278–2324, 2002.

[36] D. E. Rumelhart, G. E. Hinton, and R. J. Williams, "Learning representations by back-propagating errors," *Nature*, vol. 323, no. 6088, pp. 533–536, 1986.

[37] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, 1997.

[38] A. Graves, "Generating sequences with recurrent neural networks," *arXiv preprint arXiv:1308.0850*, 2013.

[39] A. Vaswani *et al.*, "Attention is all you need," *Adv. Neural Inf. Process. Syst.*, vol. 30, 2017.

[40] D. Bahdanau, K. Cho, and Y. Bengio, "Neural machine translation by jointly learning to align and translate," *arXiv preprint arXiv:1409.0473*, 2014.

[41] J. Lee, J. Pak, and M. Lee, "Network Intrusion Detection System using Feature Extraction based on Deep Sparse Autoencoder," in *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, IEEE, Oct. 2020, pp. 1282–1287. doi: 10.1109/ICTC49870.2020.9289253.

[42] W. Wang, X. Du, D. Shan, R. Qin, and N. Wang, "Cloud Intrusion Detection Method Based on Stacked Contractive Auto-Encoder and Support Vector Machine," *IEEE Transactions on Cloud Computing*, vol. 10, no. 3, pp. 1634–1646, Jul. 2022, doi: 10.1109/TCC.2020.3001017.

[43] H. Deng and T. Yang, "Network Intrusion Detection Based on Sparse Autoencoder and IGA-BP Network," *Wirel. Commun. Mob. Comput.*, vol. 2021, pp. 1–11, Jul. 2021, doi: 10.1155/2021/9510858.

[44] C. J. C. H. Watkins and P. Dayan, "Q-learning," *Mach. Learn.*, vol. 8, no. 3–4, pp. 279–292, May 1992, doi: 10.1007/BF00992698.

[45] V. Mnih *et al.*, "Human-level control through deep reinforcement learning," *Nature*, vol. 518, no. 7540, pp. 529–533, Feb. 2015, doi: 10.1038/nature14236.

[46] D. Fahrmann, N. Jorek, N. Damer, F. Kirchbuchner, and A. Kuijper, “Double Deep Q-Learning With Prioritized Experience Replay for Anomaly Detection in Smart Environments,” *IEEE Access*, vol. 10, pp. 60836–60848, 2022, doi: 10.1109/ACCESS.2022.3179720.

[47] N. Srinivas and K. Deb, “Muiltiobjective Optimization Using Nondominated Sorting in Genetic Algorithms,” *Evol. Comput.*, vol. 2, no. 3, pp. 221–248, Sep. 1994, doi: 10.1162/evco.1994.2.3.221.

[48] E. Johns and M. Ell, “Cyber security breaches survey 2020,” *London: Department for Digital, Culture, Media & Sport*, vol. 4, no. 1, pp. 1–4, 2020.

[49] EU Commission, “User Guide to the SME Definition,” 2020.

[50] A. Gupta and R. Hammond, “Information systems security issues and decisions for small businesses: An empirical examination,” *Information management & computer security*, vol. 13, no. 4, pp. 297–310, 2005.

[51] A. Tversky and D. Kahneman, “Loss aversion in riskless choice: A reference-dependent model,” *Q. J. Econ.*, vol. 106, no. 4, pp. 1039–1061, 1991.

[52] M. H. Bazerman, “The relevance of Kahneman and Tversky’s concept of framing to organizational behavior,” *J. Manage.*, vol. 10, no. 3, pp. 333–343, 1984.

[53] NIST - National Institute of Standards and Technology, “NIST Cybersecurity framework,” 2018. Accessed: May 09, 2026. [Online]. Available: https://www.nist.gov/cyberframework

[54] Ponemon Institute, “2018 State of Cybersecurity in Small & Medium Size Businesses,” Nov. 2018. Accessed: May 09, 2026. [Online]. Available: https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf

[55] EU ENISA, “CYBERSECURITY FOR SMES Challenges and Recommendations,” Jun. 2021. Accessed: May 09, 2026. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

[56] C. R. Kothari, *Research methodology: Methods and techniques*. New Age International, 2004.

[57] J. Sauro and J. R. Lewis, *Quantifying the user experience: Practical statistics for user research*. Morgan Kaufmann, 2016.

[58] D. Lakens, “Sample size justification,” *Collabra Psychol.*, vol. 8, no. 1, p. 33267, 2022.

[59] A. S. George, “When Trust Fails: Examining Systemic Risk in the Digital Economy from the 2024 CrowdStrike Outage,” vol. 01, pp. 134–152, Jul. 2024, doi: 10.5281/zenodo.12828222.

[60] D. Shahjee and N. Ware, “Integrated Network and Security Operation Center: A Systematic Analysis,” *IEEE Access*, vol. 10, pp. 27881–27898, 2022, doi: 10.1109/ACCESS.2022.3157738.

[61] S. Keshav, *REAL: A network simulator*. University of California Berkeley, Calif, USA, 1988.

[62] J. R. Doner, “GENESIM (generic network simulator),” *IEEE Journal on Selected Areas in Communications*, vol. 6, no. 1, pp. 172–179, 1988, doi: 10.1109/49.192740.

[63] M. Bishop, “The state of infosec education in academia: Present and future directions,” in *Proceedings of the National Colloquium on Information System Security Education*, 1997, pp. 19–33.

[64] J. M. D. Hill, C. A. Carver Jr, J. W. Humphries, and U. W. Pooch, “Using an isolated network laboratory to teach advanced networks and security,” *ACM SIGcSe Bulletin*, vol. 33, no. 1, pp. 36–40, 2001.

[65] P. Mullins *et al.*, “Panel on integrating security concepts into existing computer courses,” *ACM SIGCSE Bulletin*, vol. 34, no. 1, pp. 365–366, 2002.

[66] A. Volynkin and V. Skormin, “Large-scale Reconfigurable Virtual Testbed for Information Security Experiments,” in *2007 3rd International Conference on Testbeds and Research Infrastructure for the Development of Networks and Communities*, IEEE, 2007, pp. 1–9. doi: 10.1109/TRIDENTCOM.2007.4444663.

[67] R. van Heerden, H. Pieterse, I. Burke, and B. Irwin, “Developing a virtualised testbed environment in preparation for testing of network based attacks,” in *2013 International Conference on Adaptive Science and Technology*, IEEE, Nov. 2013, pp. 1–8. doi: 10.1109/ICASTech.2013.6707509.

[68] J. Uramova, P. Segec, J. Papan, and I. Bridova, “Management of Cybersecurity Incidents in Virtual Lab,” in *2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, IEEE, Nov. 2020, pp. 724–729. doi: 10.1109/ICETA51985.2020.9379159.

[69] T. Bălan, D. Robu, F. Sandu, and A. Bălan, “Building a Virtualized Cybersecurity Lab: Using Industry Support, Academic Programs and Open Source Solution for Setting-Up a Virtualized Cybersecurity Lab,” in *Internet of Things, Infrastructures and Mobile Applications: Proceedings of the 13th IMCL Conference 13*, Springer, 2021, pp. 1024–1032.

[70] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward generating a new intrusion detection dataset and intrusion traffic characterization.,” *ICISSp*, vol. 1, pp. 108–116, 2018.

[71] M. Ring, S. Wunderlich, D. Grüdl, D. Landes, and A. Hotho, “Flow-based benchmark data sets for intrusion detection,” in *Proceedings of the 16th European conference on cyber warfare and security. ACPI*, 2017, pp. 361–369.

[72] M. Collins, A. Hussain, and S. Schwab, “Towards an Operations-Aware Experimentation Methodology,” in *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, IEEE, Jun. 2022, pp. 384–393. doi: 10.1109/EuroSPW55150.2022.00046.

[73] I. O. for S. E. Commission, “Information Technology—Open Systems Interconnection—Systems Management Overview,” *ISO/IEC*, vol. 10040, 1991.

[74] S. Krishnamoorthi and J. Carleton, “Active Directory Holds the Keys to your Kingdom, but is it Secure,” *Frost and Sullivan*, 2020.

[75] Wazuh Inc., “Wazuh Documentation,” 2026.

[76] Graylog Inc., “Graylog Open 5.0 Documentation,” 2023.

[77] OpenSearch Project, “OpenSearch Documentation,” 2026.

[78] Grafana Labs, “Grafana Documentation,” 2026.

[79] Netgate, “pfSense Documentation,” 2026.

[80] Wireshark Foundation, “Wireshark User’s Guide,” 2026.

[81] The Zeek Project, “Zeek Documentation,” 2026.

[82] J. McHugh, “Intrusion and intrusion detection,” *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 14–35, Aug. 2001, doi: 10.1007/s102070100001.

[83] L. Haripriya and M. A. Jabbar, “Role of Machine Learning in Intrusion Detection System: Review,” in *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, IEEE, Mar. 2018, pp. 925–929. doi: 10.1109/ICECA.2018.8474576.

[84] G. Prethija and J. Katiravan, “Machine Learning and Deep Learning Approaches for Intrusion Detection: A Comparative Study,” 2022, pp. 75–95. doi: 10.1007/978-981-16-5529-6_7.

[85] P. Ramachandran, B. Zoph, and Q. V Le, “Searching for activation functions,” *arXiv preprint arXiv:1710.05941*, 2017.

[86] Kurniabudi, D. Stiawan, Darmawijoyo, M. Y. Bin Idris, A. M. Bamhdi, and R. Budiarto, “CICIDS-2017 Dataset Feature Analysis With Information Gain for Anomaly Detection,” *IEEE Access*, vol. 8, pp. 132911–132921, 2020, doi: 10.1109/ACCESS.2020.3009843.

[87] F. Pedregosa *et al.*, “Scikit-learn: Machine learning in Python,” *the Journal of machine Learning research*, vol. 12, pp. 2825–2830, 2011.

[88] W. McKinney and others, “Data structures for statistical computing in python,” in *Proceedings of the 9th Python in Science Conference*, 2010, pp. 51–56.

[89] T. pandas development team, “pandas-dev/pandas: Pandas,” Feb. 2020, *Zenodo*. doi: 10.5281/zenodo.3509134.

[90] J. D. Hunter, “Matplotlib: A 2D graphics environment,” *Comput. Sci. Eng.*, vol. 9, no. 03, pp. 90–95, 2007.

[91] Martín~Abadi *et al.*, “ TensorFlow: Large-Scale Machine Learning on Heterogeneous Systems,” 2015. [Online]. Available: https://www.tensorflow.org/

[92] Bitdefender, “THE 2025 IOT SECURITY LANDSCAPE REPORT,” 2025.

[93] Z. Alwaisi, T. Kumar, E. Harjula, and S. Soderi, “Securing constrained IoT systems: A lightweight machine learning approach for anomaly detection and prevention,” *Internet of Things*, vol. 28, p. 101398, Dec. 2024, doi: 10.1016/j.iot.2024.101398.

[94] W. Chia Chuan, S. Ul Arfeen Laghari, S. Manickam, E. Ashraf, and S. Karuppayah, "Challenges and Opportunities in Fog Computing Scheduling: A Literature Review," *IEEE Access*, vol. 13, pp. 14702–14726, 2025, doi: 10.1109/ACCESS.2024.3525261.

[95] H. Sun, H. Yu, G. Fan, L. Chen, and Z. Liu, "Security-Aware and Time-Guaranteed Service Placement in Edge Clouds," *IEEE Transactions on Network and Service Management*, vol. 20, no. 1, pp. 711–725, Mar. 2023, doi: 10.1109/TNSM.2022.3213761.

[96] M. Fatima, O. Rehman, and I. M. H. Rehman, "Li-IDS: An Approach Towards a Lightweight IDS for Resource-Constrained IoT," in *2023 International Conference on Smart Applications, Communications and Networking (SmartNets)*, IEEE, Jul. 2023, pp. 1–6. doi: 10.1109/SmartNets58706.2023.10216096.

[97] X. He, Q. Chen, L. Tang, W. Wang, and T. Liu, "CGAN-Based Collaborative Intrusion Detection for UAV Networks: A Blockchain-Empowered Distributed Federated Learning Approach," *IEEE Internet Things J.*, vol. 10, no. 1, pp. 120–132, Jan. 2023, doi: 10.1109/JIOT.2022.3200121.

[98] M. Asad, S. Otoum, and S. Shaukat, "Clients Eligibility-Based Lightweight Protocol in Federated Learning: An IDS Use Case," *IEEE Transactions on Network and Service Management*, vol. 21, no. 4, pp. 3759–3774, Aug. 2024, doi: 10.1109/TNSM.2024.3398213.

[99] D. Hamouda, M. A. Ferrag, N. Benhamida, and H. Seridi, "Intrusion Detection Systems for Industrial Internet of Things: A Survey," in *2021 International Conference on Theoretical and Applicative Aspects of Computer Science (ICTAACS)*, IEEE, Dec. 2021, pp. 1–8. doi: 10.1109/ICTAACS53298.2021.9715177.

[100] S. Shoukat, T. Gao, D. Javeed, M. Adil, and P. Kumar, "Spatiotemporal Conditioning With Dynamic Multihead Attention for IoT Intrusion Detection," *IEEE Internet Things J.*, vol. 12, no. 19, pp. 40305–40319, Oct. 2025, doi: 10.1109/JIOT.2025.3589262.

[101] L. Yang and A. Shami, "Toward Autonomous and Efficient Cybersecurity: A Multi-Objective AutoML-Based Intrusion Detection System," *IEEE Transactions on Machine Learning in Communications and Networking*, vol. 3, pp. 1244–1264, 2025, doi: 10.1109/TMLCN.2025.3631379.

[102] S. Sharma, V. Kumar, and K. Dutta, "Multi-objective optimization algorithms for intrusion detection in IoT networks: A systematic review," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 258–267, 2024, doi: 10.1016/j.iotcps.2024.01.003.

[103] S. Kim *et al.*, "DIVERGENCE: Deep Reinforcement Learning-Based Adaptive Traffic Inspection and Moving Target Defense Countermeasure Framework," *IEEE Transactions on Network and Service Management*, vol. 19, no. 4, pp. 4834–4846, Dec. 2022, doi: 10.1109/TNSM.2021.3139928.

[104] M. Y. Shabir, "Optimizing AI for IoT: Techniques for Model Compression and Edge Deployment," 2025.

[105] N. Dai and S. Uludag, "Performance Tradeoff in ML-Based Intrusion Detection Systems: Efficacy vs. Resource Usage," in *2024 IEEE 21st Consumer Communications &*

Networking Conference (CCNC), IEEE, Jan. 2024, pp. 1030–1031. doi: 10.1109/CCNC51664.2024.10454871.

[106] F. Hoseinpur, "Towards security and resource efficiency in fog computing networks," 2022.

[107] J. A. Simioni, E. K. Viegas, A. O. Santin, and E. de Matos, "An Energy-Efficient Intrusion Detection Offloading Based on DNN for Edge Computing," *IEEE Internet Things J.*, vol. 12, no. 12, pp. 20326–20342, Jun. 2025, doi: 10.1109/JIOT.2025.3544060.

[108] N. Gunantara, "A review of multi-objective optimization: Methods and its applications," *Cogent Eng.*, vol. 5, no. 1, p. 1502242, Jan. 2018, doi: 10.1080/23311916.2018.1502242.

[109] A. Alshahrani and J. A. Clark, "On Optimal Configuration of IDS for RPL Resource-Constrained Networks Using Evolutionary Algorithm," 2023, pp. 514–535. doi: 10.1007/978-3-031-18458-1_35.

[110] A. Alshahrani and J. A. Clark Hamish Cunningham, "Optimising IDS Configurations for IoT Networks using AI Approaches," 2023.

[111] K. Li and R. Chen, "Batched Data-Driven Evolutionary Multi-Objective Optimization Based on Manifold Interpolation," Sep. 2021.

[112] S. P. Singh, G. Dhiman, W. Viriyasitavat, and S. Kautish, "A Novel Multi-Objective Optimization Based Evolutionary Algorithm for Optimize the Services of Internet of Everything," *IEEE Access*, vol. 10, pp. 106798–106811, 2022, doi: 10.1109/ACCESS.2022.3209389.

[113] E. H. Houssein, M. R. Saad, Y. Djenouri, G. Hu, A. A. Ali, and H. Shaban, "Metaheuristic algorithms and their applications in wireless sensor networks: review, open issues, and challenges," *Cluster Comput.*, vol. 27, no. 10, pp. 13643–13673, Dec. 2024, doi: 10.1007/s10586-024-04619-9.

[114] K. Patel, Shreyas. A. V, T. Aleobahaey, K. Patel, and J. Velumani, "An Enhanced Dual Autoencoder GAN with Temporal Modelling for Reliable Anomaly Detection in ICS and IoT," in *2025 International Conference on Intelligent Communication Networks and Computational Techniques (ICICNCT)*, IEEE, Sep. 2025, pp. 1–6. doi: 10.1109/ICICNCT66124.2025.11232642.

[115] A. Okutan Kara, M. Kara, and A. Boyaci, "A Comparative Analysis of Machine Learning and Deep Reinforcement Learning Approaches for Adaptive Intrusion Detection," *IEEE Access*, vol. 13, pp. 189833–189849, 2025, doi: 10.1109/ACCESS.2025.3627098.

[116] M. Alkasassbeh, E. H. Omoush, M. Almseidin, and A. Aldweesh, "A Self-Adaptive Intrusion Detection System for Zero-Day Attacks Using Deep Q-Networks," *IEEE Access*, vol. 13, pp. 174280–174296, 2025, doi: 10.1109/ACCESS.2025.3617792.

[117] Mr. M. Subhani Shaik Ch and Y. N. Rao, "Design of an Iterative Method Leveraging Deep Q-Networks for Intrusion Detection System Operations," *IEEE Access*, vol. 13, pp. 48720–48745, 2025, doi: 10.1109/ACCESS.2025.3551718.

[118] T. T. Nguyen and V. J. Reddi, “Deep Reinforcement Learning for Cyber Security,” *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 34, no. 8, pp. 3779–3795, Aug. 2023, doi: 10.1109/TNNLS.2021.3121870.

[119] JASBIR S. ARORA, *Introduction to optimum design 4th Edition*. 2017.

[120] A. M. K. Adawadkar and N. Kulkarni, “Cyber-security and reinforcement learning — A brief survey,” *Eng. Appl. Artif. Intell.*, vol. 114, p. 105116, Sep. 2022, doi: 10.1016/j.engappai.2022.105116.

Објавени трудови

1. STEVANOSKI G., RISTESKI A., SERAFIMOVA N., PORJAZOVSKI M., & BOGDANOSKI M., “A Two-Stage Pareto-Driven Framework for Adaptive Resource Optimization in Lightweight Intrusion Detection Systems”, IEEE Access, May 2026, doi: 10.1109/ACCESS.2026.3690732. **Impact Factor: 3.6, Eigenfactor: 0.3457, Article Influence Score: 0.67, CiteScore: 9. (2026)**

2. STEVANOSKI, G., KACHUROVA, M., PORJAZOSKI, M., RISTESKI, A., & JAKIMOSKI, K. “Evaluation of a loss-sensitive autoencoder-a deep learning model for malicious network traffic detection”, International Scientific Conference on Computer Science (COMSCI) (pp. 1-5). September 2023, IEEE, doi: 10.1109/COMSCI59259.2023.10315849 (2023)

3. STEVANOSKI, G., PORJAZOSKI, M., RISTESKI, A., & BOGDANOSKI, M. “Testbed of an Integrated Network Operations Center and a Security Operations Center Based on Open-Source Tools”, Information & Security, 55(1), 81-94, doi: 10.11610/isij.5550 (2024)

4. STEVANOSKI, G., PORJAZOSKI, M., RISTESKI, A., & BOGDANOSKI, M., “Overview of deep learning techniques for network intrusion detection systems”, Journal of Electrical Engineering and Information Technologies. (2023)

5. JAKIMOSKI, K., BOGDANOSKI, M., RISTESKI, A., BOGATINOV, D., & STEVANOSKI, G. “A Scalable and Adaptable Asset-Based Cyber Risk Assessment Tool for All Types of Organizations”. Information & Security, 55(1), 32-43, doi: 10.11610/isij.5539 (2024)

6. TRAJCHEVSKI, NEVEN, AND GOCE STEVANOSKI. "Cybersecurity posture research in small organizations." Contemporary Macedonian Defence Journal 23.44: 51-60. (2023)

7. STEVANOSKI, G., PORJAZOSKI, M., PAUNOVSKI, I., KACHUROVA, M., & RISTESKI, A. “A Review on Machine Learning Based Intrusion Detection System: Techniques, Public Datasets and Challenges”, ETAI Conference. (2024)

8. STEVANOSKI G., RISTESKI A., AND BOGDANOSKI M. "A review of resource optimization techniques in intrusion detection systems” UDC: 004.728. 056: 004.491." ETIMA 3.1: 311-320. doi: 10.46763/ETIMA2531311s. (2025)

9. STEVANOSKI G., RISTESKI A., PORJAZOSKI M., KACHUROVA M. AND ATANASOVSKA A. "Experimental Evaluation of the A2DAPT Framework for Adaptive Resource Optimization in Lightweight Intrusion Detection Systems”, Journal of Electrical Engineering and Information Technologies. (2026)