VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2019 Jan Strakoš

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

DETEKCE ANOMÁLIÍ POMOCÍ NEURONOVÝCH SÍTÍ
ANOMALY DETECTION BY NEURAL NETWORKS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Jan Strakoš**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Blažek**
SUPERVISOR

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Informační bezpečnost**
Ústav telekomunikací

Student: Jan Strakoš ***ID:*** 195171
Ročník: 3 ***Akademický rok:*** 2018/19

NÁZEV TÉMATU:

Detekce anomálií pomocí neuronových sítí

POKYNY PRO VYPRACOVÁNÍ:

Bakalářská práce je zaměřena na identifikaci síťových útoků pomocí neuronových sítí (NS). Cílem bakalářské práce je navrh detekčního systému založeného na NS, který bude schopen detekovat anomálie v síťové komunikaci. Dílčím cílem bakalářské práce je volba vhodných parametrů ze síťové komunikace, které budou sloužit jako vstup do NS. V teoretické části práce nastudujte detekci anomálií v síťové komunikaci pomocí NS a zvolte minimálně šest různých typů anomálii. V praktické části realizujte NS a implementujte definované parametry, které budou identifikovat zvolené anomálie v síťové komunikaci. Výstupem bakalářské práce bude systém, který bude na základě alespoň šesti vybraných parametrů spolehlivě detekovat a klasifikovat anomálie v síťové komunikaci.

DOPORUČENÁ LITERATURA:

[1] VONDRÁK, Ivo, 1998. Umělá inteligence a neuronové sítě. Ostrava: Vysoká škola báňská - Technická univerzita Ostrava. ISBN 80-707-8259-5. Dostupné z: http://vondrak.cs.vsb.cz/download/Neuronove_site.pdf

[2] ALI, Siti Hajar Aminah, Seiichi OZAWA, Tao BAN, Junji NAKAZATO a Jumpei SHIMAMURA, 2016. A neural network model for detecting DDoS attacks using darknet traffic features. 2016 International Joint Conference on Neural Networks (IJCNN) [online]. IEEE, 2979-2985 [cit. 2017-09-13]. DOI: 10.1109/IJCNN.2016.7727577.

Termín zadání: 1.2.2019 ***Termín odevzdání:*** 27.5.2019

Vedoucí práce: Ing. Petr Blažek
Konzultant:

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Bakalářská práce se zaměřuje na detekci anomálii v podobě síťových útoků, pomocí neuronových sítí. Mezi nejčastější síťové útoky patří Distributed Denial of Service (DDoS) útoky, které by měl detekční systém založený na neuronových sítích identifikovat. V teoretické části práce je rozebrán legitimní, nestandardní a útočný provoz. Součástí teoretické části práce je i popis DDoS útoků, možnosti jejich detekce a princip využití neuronových sítí. Praktická část popisuje zvolené parametry síťové komunikace, stanovení prahových intervalů, návrh a realizaci neuronové sítě s využitím těchto parametrů a jejich prahových intervalů, implementaci neuronové sítě do detekčního systému spolu s výsledkem testování realizovaného systému.

KLÍČOVÁ SLOVA

anomálie, legitimní provoz, DDoS, IDS, neuronové sítě, Python, Scikit–learn

ABSTRACT

This bachelor thesis is focused on anomaly detection represented as computer network attacks by neural network. One of the most common groups of attacks is Distributed Denial of Service (DDoS) attacks, which the system based on neural network should identificate. In the theoretical part of this thesis are described legitimate, non-standard and illegitimate traffic. Another part of this chapter described DDoS attacks, options of their detection, neural networks principle and their use. Practical part describe choosed communication parameters, specifying the threshold intervals of legitimate traffic, constructing a neural network which use of these parameters and threshold intervals, implementation of neural network into the system and presenting results.

KEYWORDS

anomaly, legitimate traffic, DDoS, IDS, neural networks, Python, Scikit–learn

STRAKOŠ, Jan. *Detekce anomálií pomocí neuronových sítí*. Brno, 2019, 53 s. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. Petr Blažek

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Detekce anomálií pomocí neuronových sítí“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu bakalářské práce panu Ing. Petru Blažkovi za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno ....

podpis autora

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic

http://www.six.feec.vutbr.cz

PODĚKOVÁNÍ

Výzkum popsaný v této bakalářské práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

Brno ....

podpis autora

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OP Výzkum a vývoj
pro inovace

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Trend komunikačních sítí a síťové komunikace, kde se nehmatatelné stává skutečným, zažívá v posledních letech nebývalého růstu. Jako druh máme zabudovanou potřebu spojovat se s ostatními. Propojování počítačových sítí a utváření obrovských informačních datových toků vytváří přirozené prostředí pro útočníky, neboli hackery. Spoluúčast těchto útočníků v komunikaci je nežádoucím prvkem a síť jako taková by měla být schopna útočníka rozpoznat a zamezit jeho nekalé činnosti.

Na základě neobvyklého nebo neočekávaného chování komunikační sítě lze predikovat tzv. anomálie v síti. Tyto anomálii je nutné prověřit a v případě detekce útoku nastolit vhodná opatření, popřípadě restrikce. Né každá anomálie v síťové komunikaci musí nutně znamenat potenciální hrozbu. Může se jednat pouze o nadměrně vysokou aktivitu legitimních uživatelů sítě nebo zvýšený objem přenášených dat způsobený aktualizací softwaru koncových stanic. I takové případy je však nutné analyzovat a zařadit. Jednou z vhodných metod pro detekci anomálií síťového provozu jsou neuronové sítě.

Neuronové sítě se používají na úlohy směřované do oblasti klasifikace, aproximace a predikce. Svůj prapůvod mají umělé neuronové sítě v biologické oblasti. Od vzniku prvních počítačů se programátorské kapacity snaží vytvořit algoritmus, který bude činnost lidského mozku napodobovat. V dnešní době jsou jedním z nezastupitelných prvků moderní kybernetické bezpečnosti. Jednou z hlavních předností neuronové sítě je schopnost učit se. V tomto smyslu neuronová síť připomíná inteligenci člověka, který získává mnohé znalosti a dovednosti ze zkušeností.

Tato bakalářská práce se věnuje studii anomálií v síťové komunikaci a výběrem vhodných parametrů identifikujících jednotlivé anomálie. Práce se dále zaměřuje na vytvoření detekčního systému založeného na neuronových sítích, kde vstupem do neuronové sítě budou vhodně zvolené parametry síťové komunikace.
Samotná práce je rozdělena do 3 hlavních kapitol. První dvě kapitoly se zabývají teoretickou části problematiky. Třetí kapitola se věnuje návrhu a realizaci neuronové sítě, testování a následnému zhodnocení dosažených výsledků.

1 Neuronové sítě

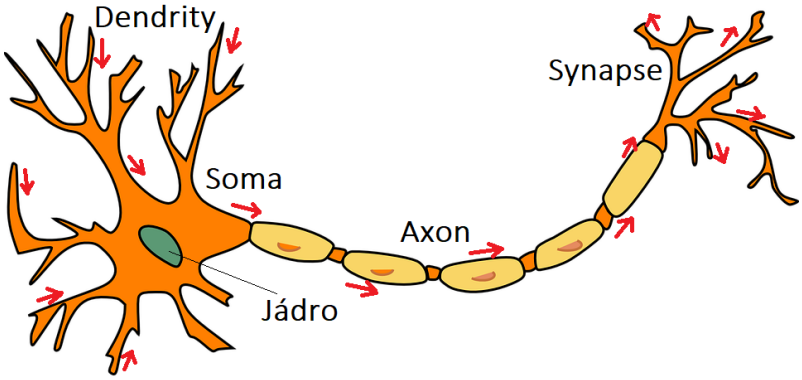
Již v dřívějších dobách bylo zjištěno, že mozek je tvořen velkým množstvím vzájemně propletených buněk. Tyto buňky nazýváme neurony. Kolem 40–50.let 20. století došlo k prvním pokusům převést tento biologický systém do světa informačních technologií a počítačů. V této kapitole je vysvětlený model umělého a biologického neuronu a zároveň popis jednotlivých typů umělých neuronových sítí.

1.1 Biologický neuron

Biologický neuron je základní buňkou nervové tkáně. Jedná se o vysoce specializované buňky, které jsou schopné přijmout, vést, zpracovat a odpovědět na speciální signály. Přenášejí informace jak z vnitřního, tak vnějšího prostředí a tím podmiňují organismus na ně reagovat.

Každý biologický neuron se skládá z těla (soma), jádra, dendritů, axonu a synapsí. Tělo neuronu společně s jádrem neuronu sčítá signály dané okolními neurony a rozhoduje o excitaci (vybuzení), nebo inhibici (utlumení) samotného neuronu. Dendrity fungují jako přijímače signálu od ostatních neuronů. Pomocí axonu neuron posílá signál daný stupněm excitace k synapsím. Synapse představují výstup neuronu a komunikují s dendrity jiných neuronů. [1]

Schématické znázornění biologického neuronu spolu s průběhem signálu od dendritů přes jádro neuronu, axon až po synapse znázorňuje obrázek 1.1.



Obr. 1.1: Schématické znázornění biologického neuronu

1.2 Umělý neuron

Autoři článku [2] popisují umělý neuron vycházející z neuronu biologického, jako základní stavební jednotku umělé neuronové sítě. Neurony jsou propojeny a navzájem si předávají signály jak již bylo zmíněno v podkapitole 1.1. Signály transformují pomocí určitých přenosových funkcí. Počet vstupů umělého neuronu je libovolný, avšak výstup je jen jeden.

Mezi proměnné vystupující v modelu umělého neuronu patří vstupní hodnoty, váhy jednotlivých vstupů, prahové hodnoty samotných neuronů a výstupní hodnota. Vstupy chápeme jako podněty z vnějšího okolí, nebo jako výstup z jiných neuronů. Každý vstup, váha i výstup je reprezentován číselnou hodnotou. Váhy reprezentují citlivost jednotlivých spojů mezi navzájem propojenými neurony. Vstup je vynásoben hodnotu váhy daného spojení. Výsledná suma součinu vstupních hodnot a vah jednotlivých spojů je porovnána s prahovou hodnotou daného umělého neuronu. Pokud hodnota přesáhne prahovou hodnotu, dojde k excitaci (vybuzení) neuronu a následné indikaci výstupu ve formě přenosové funkce (funkce přechodu, někdy též aktivační funkce). Následující podkapitoly se budou podrobněji věnovat matematickému pohledu na model umělého neuronu.

1.2.1 Činnost umělého neuronu z matematického hlediska

Níže uvedený matematický popis umělého neuronu vychází ze článku [2]. Znalost činnosti umělého neuronu z matematického hlediska je nezbytná pro pochopení celého systému neuronové sítě. Následující popis vychází z obrázku 1.2, kde

- $\mathbf{x_1}, \mathbf{x_n}$ jsou vstupní hodnoty/vstupy, které vstupují do umělého neuronu. Hodnoty jsou z množiny reálných čísel R.
- $\mathbf{w_1}, \mathbf{w_n}$ jsou hodnoty vah, které mohou být také reálným číslem a často jsou modelovány, jako vstupy. Tyto hodnoty jsou z počátku inicializovány náhodně. Hodnoty vah jsou vynásobeny s odpovídajícími vstupními hodnotami.
- $\mathbf{\Sigma}$ je funkce Suma, která představuje součet součinů jednotlivých vah s příslušnými vstupními hodnotami.
- $\mathbf{G}$ je výstup z funkce Suma, který je zároveň vstupem do Aktivační funkce. Tento výstup počítáme následujícím způsobem:

$$G = \sum_{i=1}^{n} (x_i \times w_i). \tag{1.1}$$

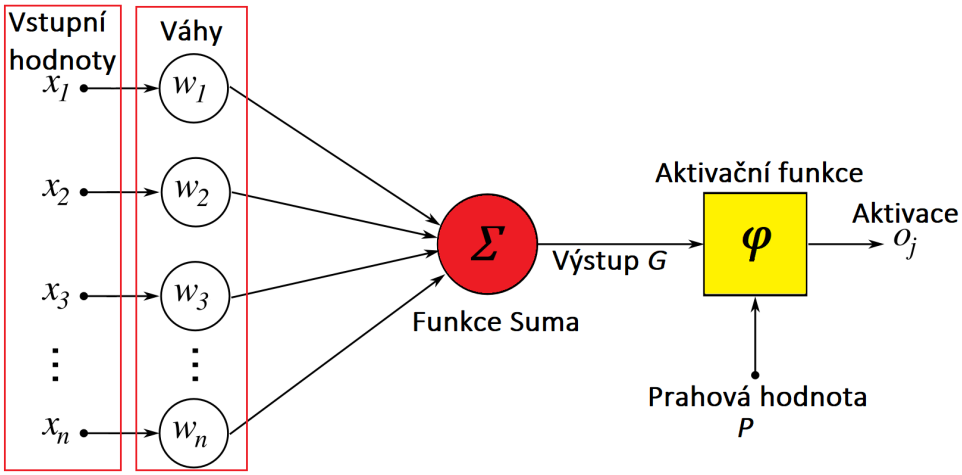
- φ je Aktivační funkce (přenosová funkce), která zpřesňuje proces excitace/inhibice umělého neuronu.

- **P** je prahová hodnota, která je porovnána s hodnotou výstupu z funkce Suma indikované ve formě Aktivační funkce. Pokud je výstup **G** větší než prahová hodnota, dojde k excitaci umělého neuronu, v opačném případě k jeho inhibici.
- $\mathbf{o_j}$ je hodnota aktivace, neboli hodnota, která představuje výstup z umělého neuronu. Tato hodnota je výsledkem výstupu z aktivační funkce.

Celou činnost neuronu pak lze zapsat jedním matematickým vztahem, kde **P** bude záporné číslo představující práh, který musí potenciál **G** překonat.

$$o_j = \varphi(P + G). \tag{1.2}$$

.



Obr. 1.2: Schématické znázornění umělého neuronu

1.2.2 Aktivační funkce

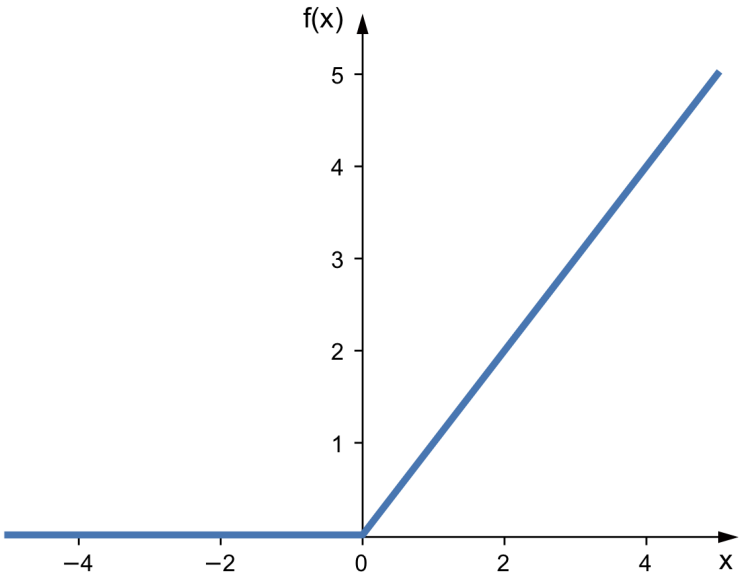
Aktivační funkce je důležitým prvkem v procesu excitace/inhibice umělého neuronu. Tato funkce upravuje výstup G na hodnoty, které se dále šíří v neuronové síti. Existuje celá řada aktivačních (přenosových funkcí).

Funkce se dle článku [3] dělí do dvou základních tříd a to lineární a nelineární. Nejvíce používané jsou právě nelineární aktivační funkce. Mezi nejznámější patří funkce jednotkového skoku(*hardlim*), funkce signum (*hardlims*), lineární aktivační funkce (*purelin*), hyperbolický tangent (*tansig*), logistická sigmoida (*sigmoid*) nebo aktivační funkce ReLU (The Rectified Lunear Unit). Volba vhodné aktivační funkce rozhoduje o kvalitě celé neuronové sítě. O volbě aktivační funkce rozhoduje úloha, kterou neuronová síť řeší. Pro klasifikační úlohy je například vhodná funkce *sigmoid* nebo *tansig*, pomocí kterých lze rozdělit pozorované vzorky do dvou tříd.

Jako příklad aktivační funkce zvolíme ReLU. ReLU (The Rectified Linear Unit) je nejčastěji používanou aktivační funkcí. Funkce vrátí 0, jestliže obdrží zápornou vstupní hodnotu. Obdrží-li hodnotu kladnou, pak je tato hodnota výstupem funkce. Lze tedy napsat

$$f(x) = max(0,x), \tag{1.3}$$

kde x je vstupem do aktivační funkce. Průběh aktivační funkce ReLU zobrazuje obrazek 1.3.



Obr. 1.3: Aktivační funkce – ReLU (The Rectified Linear Unit)

1.3 Vícevrstvé neuronové sítě

Vícevrstvá neuronová síť je taková síť, která obsahuje více než jednu vrstvu umělých neuronů nebo uzlů. Existuje jich velká řada, a proto se bude následující podkapitola věnovat pouze těm nejznámějším. Je důležité zmínit, že jednovrstvé neuronové sítě byly užitečné v počátcích evoluce umělé inteligence, avšak dnes je veliká většina neuronových sítí vícevrstvých.

Ve vícevrstvých neuronových sítích je obvykle jedna vstupní vrstva, která posílá vážené vstupy do řady vnitřních skrytých vrstev a vrstva výstupní na konci. Počet umělých neuronů ve skryté vrstvě závisí na složitosti a unikátnosti dané úlohy. Větší počet neuronů a skrytých vrstev může zvýšit schopnost učení se a zároveň vnáší do procesu učení se i nelinearitu, která je v určitých případech nezbytná. Né vždy

tomu tak je, a proto je potřeba tento počet vždy zohlednit na základě složitosti dané úlohy. Zatímco některé z těchto modelů mohou být sestaveny i fyzicky, většinou se jedná o softwarové řešení, které modeluje nervovou aktivitu. [4]

1.3.1 Druhy vícevrstvých neuronových sítí

Jak již bylo zmíněno v kapitole 1.3, existuje celá řada druhů vícevrstvých neuronových sítí. Tato kapitola se věnuje pouze těm nejznámějším a stručně popisuje principy, které se v daném druhu neuronové sítě uplatňují. Níže popsané vícevrstvé neuronové sítě vychází z [5].

MLP – Vícevrstvý perceptron

Vícevrstvý perceptron (Multilayer perceptron) má tři nebo více vrstev. Tato síť využívá nelineární aktivační funkci při procesu excitace/inhibice umělého neuronu. Každý neuron ve vrstvě je přímo spojen s každým neuronem ve vrstvě následující, čímž je síť plně propojená. Využití vícevrstvého perceptronu je vhodné v případě, kdy máme jen příklady vstupů a výstupů nějakého sledovaného procesu. Náročnost sítě je dána zejména optimalizací pomocí algoritmu backpropagation. Na základě tohoto algoritmu jsou zpětně upravovány váhové hodnoty jednotlivých spojení takovým způsobem, aby došlo k přiblížení se požadovanému výsledku. Takováto síť se využívá například při zpracování přirozeného jazyka a rozpoznávání řeči.

CNN – Konvoluční neuronové sítě

Konvoluční neuronové sítě (Convolutional neural networks) jsou velmi podobné běžným neuronovým sítím. Jsou také tvořeny jednotlivými vrstvami umělých neuronů. Důležité však je s jakými vstupními hodnotami tato síť pracuje. Implementace konvoluční neuronové sítě je totiž vhodná zejména v oblasti rozpoznávání a komprese obrazu.

V případě, kdy chceme nějakým způsobem popsat dvojrozměrnou strukturu rozpoznávaného obrazu, využijeme nástroj nazývaný konvoluční okno/konvoluční filtr. Zjednodušeně si za tímto pojmem můžeme představit matici, jejíž jednotlivé hodnoty představují váhy. Takováto matice postupně „scanuje“ na obrazu matici pixelů o stejné velikosti a pomocí roznásobení hodnoty váhy s hodnotou pixelu vytvoří výstup. Konvolučních oken/ filtrů je samozřejmě větší množství a zároveň se nacházejí ve více vrstvách. Výsledkem je potom schopnost detekce náběžných hran a jiných pozorovaných jevů.

RNN – Rekurentní neuronové sítě

Všechny doposud zmíněné druhy neuronových sítí byly nezávislé na kontextu, zjednodušeně řečeno stejná vstupní hodnota vyvolala vždy stejnou odezvu sítě. Cílem rekurentních neuronových sítí je implementace časového kontextu. To znamená, že odezva sítě nebude dána pouze aktuální vstupní hodnotou, ale bude odrážet i vstupní hodnoty, které jí předcházeli. V rekurentní neuronové síti se signál nešíří pouze od vstupní vrstvy směrem ke vrstvě výstupní, ale dochází k zpětnovazebnému šíření z vrstev vyšších k vrstvám nižším. Takováto síť se využívá například v úlohách modelování a predikce řeči nebo rozpoznávání hlasu.

MNNs – Modulární neuronové sítě

Modulární neuronové sítě (Modular neural networks) se skládají ze sady různých sítí, které pracují nezávisle a přispívají s výstupu. Každá neuronová síť má sadu vstupů, které jsou jedinečné ve srovnání s jinými sítěmi. Tyto sítě spolu vzájemně nekomunikují a neinformují se. Výhodou modulární neuronové sítě je to, že rozkládá náročný výpočetní proces na menší části, což snižuje složitost. Čas zpracovávání však bude záviset na počtu neuronů a jejích zapojení do výpočtu požadovaného výsledku. Modulární neuronové sítě jsou rychle rostoucí oblastí a podléhají ustavičnému výzkumu. Motivací vzniku těchto sítí je mnoho, jedná se zejména o oblasti hardwarové, biologické a výpočetní.

Kohonenovy samoorganizující neuronové sítě

Cílem Kohonenových map je prostorově reprezentovat složité datové struktury. Jedná se tedy o snahu vytvořit topologii neuronů takovou, aby reprezentovali třídy podobných si vektorů. Tímto způsobem je možné zobrazit mnohodimenzionální data v jednodušším prostoru. Nejčastější je využití právě v prostoru dimenzionálním. Takovéto mapy dokážou sami rozpoznávat sobě podobné, nebo naopak rozdílné prvky. Síť ke svému nastavení nepotřebují ideální vzory, místo toho hledají v datech spojitosti, společné vlastnost nebo výrazné odlišnosti. Kohenovy samoorganizující neuronové sítě jsou využívání pro rozpoznávání, rozlišení a třídění různých číslicových signálů, dat, objektů nebo značek. Velmi častou implementací je rozpoznávání řeči nebo odstranění neznámého rušení.

2 Anomálie síťového provozu

Pojem anomálie v pojetí síťového provozu označuje něco co se odchyluje od standardního, normálního a očekávaného provozu. Provoz v síti je v dnešním době vlivem technologického rozvoje čím dál více nebezpečný. Podle Ginni Rometty (ředitelka společnosti IBM) by se měla během následujících pěti let stát kyberkriminalita největší hrozbou pro každou osobu, místo i věc [6]. Tento provoz je nutné včas detekovat a nastolit vhodná opatření. Jako anomálii můžeme například označit neočekávaný nárůst objemu přenášených dat, podezřele velké množství paketů se specifickými příznaky nebo zvýšenou frekvence nestandardních dotazů.

Zmíněné projevy však nemusí nutně představovat výskyt útoku. Příčinu těchto projevů může způsobit např. update firemního softwaru. Takovýto provoz není sice zcela běžný a standardní, avšak nemusí nutně představovat hrozbu v podobě útoku, a proto jej označujeme jako nestandardní. Z výše uvedených důvodu je nutné rozlišovat mezi legitimním provozem, v rámci kterého nedochází k žádným větším odlišnostem, nestandardním provozem a útokem, kde útok zpravidla představuje sousled více anomálií. Mezi útoky projevující se již zmíněnými nebo jinými anomáliemi patří například Distrubuted Denial of Service útoky (DDoS), jejichž detekcí se zabývá tato bakalářská práce.

2.1 Distributed Denial of Service DDoS

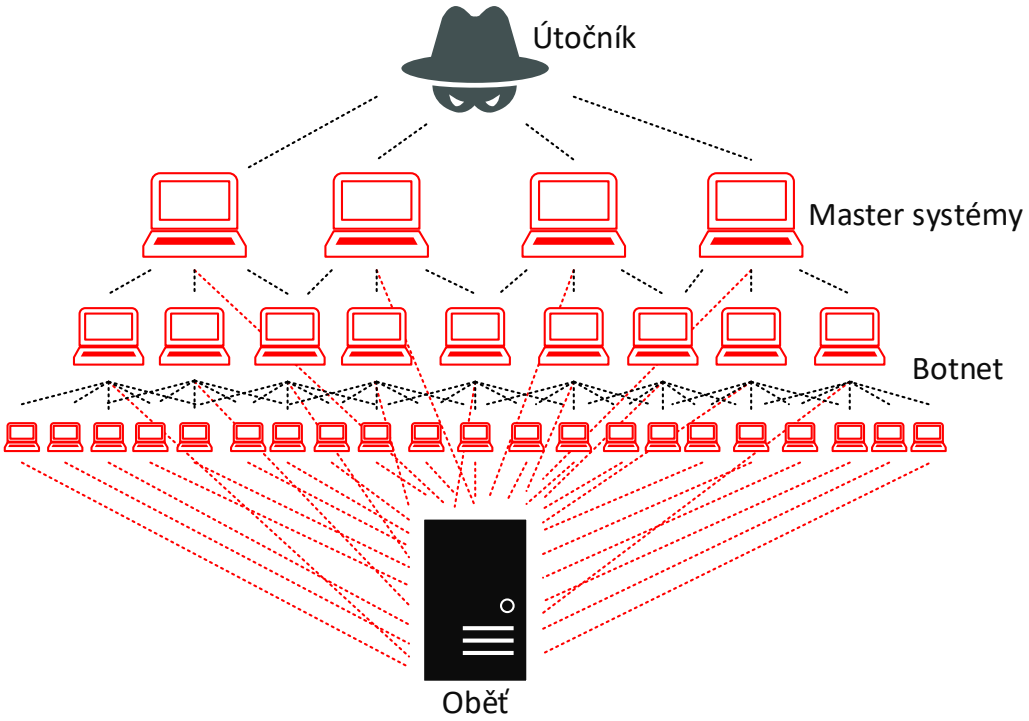
Distrubited Denial of Service (DDoS) je útok, při kterém dochází k přehlcení cílové služby požadavky a následnému znemožnění využití této služby. Zprostředkovatel služby může být server, webová aplikace nebo například síťový zdroj. Záplava přicházejících zpráv, požadavků nebo chybně formátovaných paketů do systému oběti způsobí zpomalení nebo úplný pád systému, čímž zapříčiní nedostupnost dané služby. Útoky DDoS mohou vytvářet významná obchodní rizika s trvalými účinky, proto je důležité s danými hrozbami dopředu počítat a vytvořit opatření, která budou takové situaci předcházet. [7]

2.1.1 Princip DDoS útoku

Následující popis principu DDoS útoku vychází z článku [8]. Při typickém DDoS útoku utočník začíná tím, že využívá zranitelnost jednoho počítačového systému, ze kterého dělá tkzv. DDoS master systém. Útočníkův master systém identifikuje ostatní zranitelné systémy a získá nad nimi kontrolu tím, že systémy napadá

malwarem[1] nebo skrze obejití ovládacích prvků autentizace (např. uhodnutí defaultního hesla na široce rozšířeném systému nebo zařízení.

Ovládnutý počítač nebo nebo síťový prvek je označován jako zombie nebo bot. Síť takto napadnutých zařízení se označuje jako botnet. Obvykle první „naverbovaný“ systém do botnetu je označován jako botmaster, jelikož se využívá pro kontrolu aktivity jiných systému v botnetu. Schématickou topologii útoku DDoS zobrazuje obrázek 2.1. Botnety mohou být tvořeny téměř jakýmkoliv počtem botů. Botnety s desítkami nebo stovkami tisíc uzlů se stávají stále častějšími s tím, že horní limit jejich velikosti není stanoven. Jakmile je botnet sestaven, útočník může využívat provoz generovaný kompromitovanými zařízeními k znemožnění cílové služby.



Obr. 2.1: Schematické znázornění obecného principu DDoS útoku

2.1.2 Motivace DDoS útočníků

Motivace pro útočníky může být různá. Nejčastěji se jedná o snahu poškodit nějakou společnost, firmu či instituci za účelem „vyrovnání účtů“, potřeby destrukce

[1]Software (kód, skript), jenž je tvořen a šířen s cílem získat citlivá data nebo ovládnout nějaký počítač či systém.

nebo sesazení konkurence z pomyslného vrcholu. Mezi další důvody realizace útoků patří vydírání, demonstrace síly, určitá forma protestu (např. skupina Anonymous) nebo zakrytí hlavního útoku, který s DDoS útokem probíhá paralelně. Někteří hackeři jsou označování jako „hacktivisté“ motivovaní politikou. Již zmiňovaná skupina Anonymous věří, že turecká vláda podporuje ISIS[2], a proto zahájila útoky DDoS, které poškodili stránky tureckých vládních agentur a finančních institucí. Další skupina nazývaná New World Hackers směřovali svůj DDoS útok na internetové stránky prezidenta spojených států Donalda Trumpa z důvodu nesouhlasu s jeho politickými názory [9].

Není tajemstvím, že se kyberzločinci hackují do systémů kvůli citlivým a důvěrným informacím, jako jsou e-mailové adresy, bankovní údaje a čísla kreditních karet. Předpokládá se, že hackeři mohou a také podvodně používají čísla ukradených kreditních karet nebo je prodávají jiným zločincům.

Jak již bylo zmíněno, hackeři často využívají útoku DDoS k zakrytí jiného, hlavního útoku. Útočníci využijí DDoS jako tzv. „smokescreen“, při kterém odvrátí pozornost bezpečnostních pracovníků zatímco se například nabourávají do firemní databáze. Příkladem by mohl být útok na společnost Linode z roku 2016. Podle nezávislého zpravodaje threatpost [10] hackeři směřovali DDoS útok na společnost Linode a během útoku došlo i k neoprávněnému přihlášení do třech účtu z externího zařízení. Z toho důvodu byli všichni zákazníci nuceni obnovit svá hesla, čímž došlo k zneplatnění starých pověření, jejichž zranitelnost útočníci využili.

Další zajímavostí je, že stále více kybernetických zločinců požaduje výkupné od firem ve formě bitcoinu[3]. Europol[4] oznámil, že tým evropských orgánu činných v trestním řízení se stále častěji setkává právě s takovými skupinami hackerů. V roce 2016 to byla např. skupina DD4BC (DDoS for Bitocin).

Marketwatch [11] uvádí, že podle průzkumu Cloud Alliance je téměř čtvrtina společností (24,6%) ochotna zaplatit hackerům výkupné za to, aby zabránili kybernetickému útoku. Právě toto chování motivuje hackery k dalším útokům.

2.1.3 Škody způsobené DDoS

Škody jsou velmi různorodé. Může se jednat o přesčasy zaměstnanců způsobené časem stráveným nad nápravou škod nebo nutnost přijímat zaměstnance nové. Mezi další škody patří určitě zhoršení pověsti firmy. Průměrná výše ztrát je samozřejmě odhad, jelikož výše škod je závislá na velikosti firmy, společnosti nebo instituce, nicméně podle jiných údajů společnosti Neustar [12] hodinový výpadek služeb může

[2]Islámský stát je radikální islámská teroristická organizace původem z Iráku.

[3]Kryptoměna, jejíž hlavní unikátností je plná decentralizace.

[4]Organizace patřící pod Evropskou unii zabývající se potíráním organizované trestné činnosti.

velké podniky vyjít i na 100 000−250 000 dolarů. Danou společnost často upozorní na incident někdo zvenčí, jelikož se nemusí jednat o útok na hlavní web, ale například na portál určeným zákazníkům [13]. V takovém případě rychlost reakce určuje velikost škod způsobených DDoS útokem.

2.1.4 Záplavové útoky

Záplavové útoky se zaměřují na vytížení komunikační/paměťové/výpočetní kapacity cíle. Útoky se nejčastěji vyskytují na 3. a 4. vrstvě ISO/OSI (Open System Interconnection) modelu. Jedná se o jeden z nejčastějších typů útoků. Přestože jsou záplavové útoky charakteristické obrovským množstvím provozu, nevyžadují takový provoz přímo od útočníků (hackerů). Právě tato vlastnost dělá ze záplavového útoku nejjednodušší útok DDoS. Útočníci například zasílají legitimní požadavky na DNS[5], NTP[6] server s podvrženou (spoofed) IP adresou. V takovém scénáři je potom podvržená IP adresa bombardována zesíleným datovým tokem. [14]

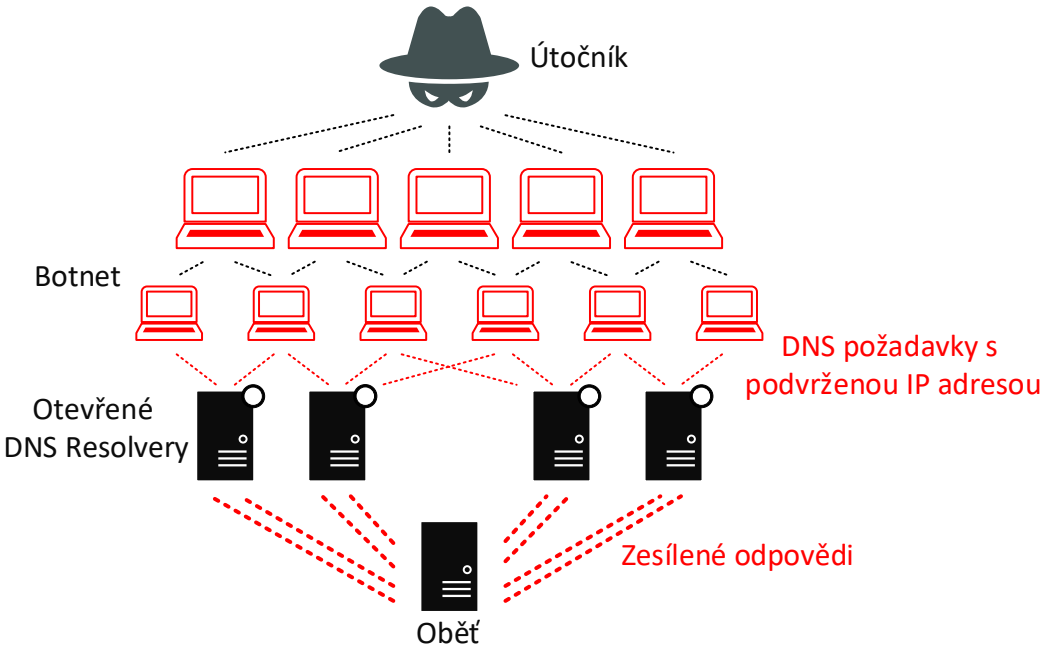
Typickými zástupci záplavových útoků jsou například NTP (Network Time Protocol) Amplification (zesílení), DNS (Domain Name System) Amplification, UDP (User Datagram Protocol) Flood (záplava), TCP (Transmission Control Protocol) Flood , TCP Reset Attack a další. V následující části budou některé zmiňované záplavové útoky podrobněji popsány.

DNS Amplification

DNS Amplification útok je jedna z populárních forem záplavových útoků, při kterém útočník využívá otevřené rekurzivní DNS nameservery k zaplavení oběti odpověďmi, které si sama nevyžádala. „Otevřené“ proto, protože poskytují své služby nejen uživatelům své místní sítě, ale i komukoliv jinému. Takovéto servery znamenají nebezpečí pro celý internet. Podle serveru cz.nic je přibližně 50 % nameserverů uvedených v domén zóně „.cz“ nebezpečných.

Útočník posílá na server DNS dotazy s podvrženou IP adresou. Čím více dotazů se zašle na otevřený DNS resolver[7], tím silněji bude oběť zasažena. Při útoku se projeví i již zmiňovaná „amplification“, kdy útočník zasílá poměrně malé DNS dotazy a na IP adresu oběti jsou pak zasílaný mnohem větší odpovědi, tak jako tomu je vidět na obrázku 2.2. Vzhledem k rozdílu velikosti mezi zasílanými a přijímanými dotazy může i útočník disponující pomalejší linkou zahltit rychlejší linku oběti. [15]

[5] Hierarchický systém doménových jmen.
[6] „časové“ servery.
[7] Vyhledávací nástroj, který řeší DNS dotazy.

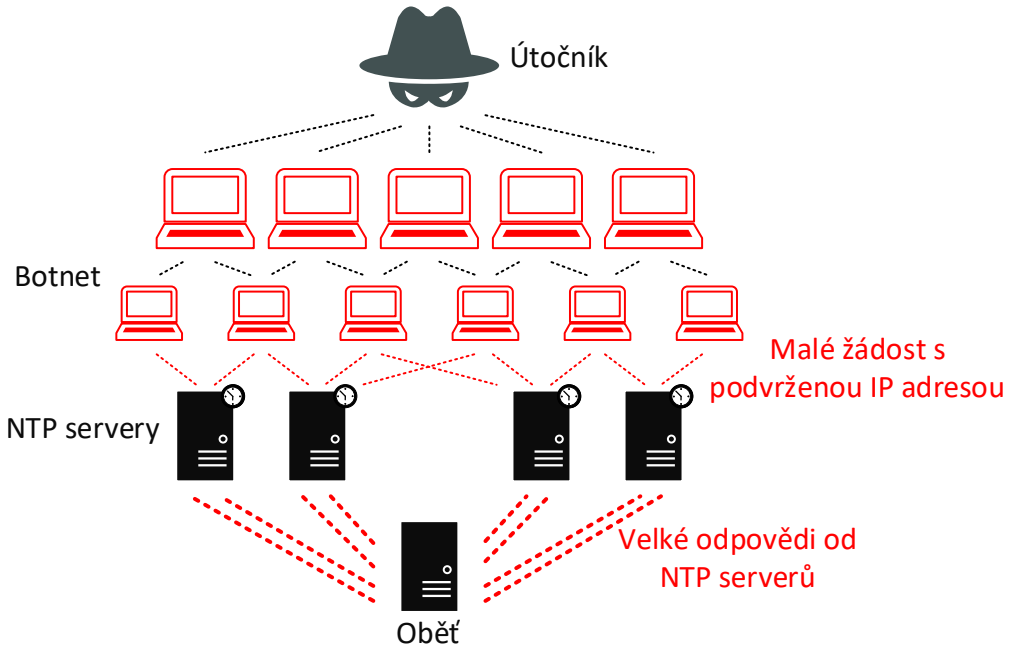


Obr. 2.2: Schématický znázornění DDoS útoku – DNS amplification

NTP Amplification

NTP je protokol z rodiny protokolů TCP/IP (Transmission Control Protocol/Internet Protocol), který slouží k synchronizaci času na počítačích a dalších zařízeních v síti. NTP využívá UDP protokol, a proto se může podobně jako DNS stát vektorem úspěšného DDoS útoku.

Následující popis vychází ze článku [16]. Princip útoku spočívá v tom, že útočník opakovaně zasílá `get monlist` požadavek s podvrženou (spoofed) IP adresou oběti na NTP server. NTP server však nedokáže rozlišit jestli se jedná o legitimního uživatele nebo o nežádoucího útočníka, a proto na něj odpoví. V odpovědi od serveru se potom projeví i „amplification“, neboli zesílení. Odpověď od serveru je totiž mnohem větší než přijatý dotaz, zhruba v poměru 70:1. Průběh útoku zobrazuje obrázek 2.3. Podstatou útoku je již zmiňovaný příkaz `get monlist`, který slouží k monitorování provozu na serveru. Pokud je server zranitelný, můžeme pomocí tohoto příkazu získat seznam posledních 600 připojených IP adres, který se posílá na podvrženou IP adresu a tím dojde k zahlcení oběti.



Obr. 2.3: Schématický znázornění DDoS útoku – NTP amplification

TCP SYN Flood

Před popsáním samotného útoku je nejdříve nutné pochopit základní princip navázání TCP spojení. Takovémuto navázání spojení se říká Three-way handshake (třícestné potřesení rukou). Během takového navazování spojení se obě strany dohodnou na číslu sekvence a potvrzovacím čísle. Uživatel žádající o spojení odesílá datagram s nastaveným příznakem SYN (synchronize), potvrzovací číslo (0) a číslo sekvence x, které je náhodně vygenerované. Druhá strana odpovídá datagramem s nastaveným příznakem SYN-ACK (synchronize–acknowledgement), náhodně vygenerované číslo sekvence y, potvrzovací číslo $(x+1)$. Žadatel příjme tuto informaci a odesílá datagram s nastaveným příznakem ACK (acknowledgement), kde je číslo sekvence $(x+1)$ a číslo odpovědi $(y+1)$. [17]

Autoři článku [18] popisují TCP SYN Flood jako běžný DDoS útok, při kterém útočník využívá část třícestné navázání TCP spojení (three-way handshake) k spotřebování prostředků oběti a vyloučení její činnosti. Útočník v podstatě odesílá žádosti o TCP spojení tak rychle, že je stanice oběti nestíhá zpracovávat, což způsobí její přehlcení. Zranitelný systém oběti alokuje prostředky ihned po obdržení paketu s příznakem SYN, ještě před tím, než obdrží paket ACK.

Existují potom dva způsoby jak se může útočník zachovat. Buď paket s příznakem ACK vůbec nepošle, nebo může již zmiňovaný paket SYN poslat s podvrženou (spoofed) IP adresou. Server potom posílá SYN-ACK na podvrženou IP adresu, od které se samozřejmě ACK paketu nedočká. Nutno však podotknout, že pokud počítač jehož IP adresu útočník použil najednou obdrží paket s příznakem SYN-ACK, i přestože předtím žádný paket s příznakem SYN neposlal, odpovídá paketem s příznakem RST (reset). Paket s takovým příznakem okamžitě polootevřené spojení ukončuje. Z tohoto důvodu si útočníci vybírají takové IP adresy stanic, které jsou momentálně nedostupné. Obět je potom nucena polootevřené spojení držet po dobu zhruba 75 sekund.

Tímto způsobem dochází k vytváření napůl otevřených spojení, které zanedlouho vyčerpají dostupné prostředky. Díky tomu může dojít k zpomalení serveru nebo zhroucení celého systému.

2.1.5 Logické útoky

Druhou skupinou DDoS útoků jsou logické útoky, které cílí na slabinu v programu, protokolu nebo operačním systému. Skupinu jako takovou lze ještě dělit na útoky protokolové a aplikační. Jak už název napovídá, protokolové útoky zneužívají zranitelnosti protokolu a aplikační aplikace.

Útoky založené na zranitelnosti protokolu se nacházejí na 3. a 4. vrstvě modelu ISO/OSI. Útoky mohou být zaměřeny na cílové prostředí zdroje, jako jsou například brány firewall[8]. Aplikační útoky, také známe jako útoky 7. vrstvy modelu ISO/OSI, zahrnují útoky zaměřené na zranitelná místa ve webových službách jako jsou Apache, IIS, NGINX a další. Tyto útoky nemusí být z pohledu objemu dat, jako je tomu u záplavových útoku, významné. Výsledkem zneužití zranitelného systému opět dochází k pádu nebo přetížení aplikačního serveru, což vede k nedostupnosti služby. Pro demonstraci si představme uživatele, který odešle požadavek do online účtu, jako je například Gmail. Množství dat a prostředků, který uživatelský počítač musí využívat je minimální a nepřiměřený množství prostředků spotřebovaných při procesu kontroly přihlašovacích údajů, načtení dat příslušného uživatele z databáze a následné vyřizování odeslaných odpovědí obsahujících požadovanou akci. I při absenci přihlašování musí server, který přijímá požadavky od klienta, provádět databázové dotazy nebo jiné volání API[9]. Když je tato nerovnost zvýšená v důsledku mnoha zařízení zaměřených na jednu webovou službu, může tento efekt přemoct cílovou službu, což má za následek nedostupnost legitimního provozu. [19].

[8]Síťové zařízení, které slouží k řízení a zabezpečování síťového provozu.

[9]Application Programming Interface. Jedná se o rozhraní pro programování aplikací.

Mezi nejznámější logické útoky patří Ping of Death, Land Attack, Slowloris, XMasTree Attack, Teardrop. Některým z těchto útoků se budou podrobněji věnovat následující podkapitoly.

Christmas Tree Attack

Christmas Tree paket (paket vánočního stromku) je takový paket, který se vyznačuje množstvím specifického nastavení, které IT (Information technology) experti nazývají jako univerzální nebo defaultní (přednastavené). Označení „paket vánočního stromku“ kvůli metaforické představě, že jednotlivé příznaky (flags) „září“ různými barvami a paket je v podstatě vyzdoben jako vánoční stromek. Paket je potom nastaven takovým způsobem, že obsahuje informace náročné na zpracování a zároveň takové, které interaktivně reagují různým způsobem s určitými protokoly.

Útočník může vhodnou manipulací s hlavičkou TCP segmentu vytvořit Christmas Tree paket, kde každý z několika příznaků nastaví na „otevřeno“. Toto nastavení současně způsobuje to, že je takový paket náročnější na zpracování a vyžaduje vyšší výpočetní výkon od příjemce. Jedná se například o příznaky FIN (finialize), URG (urgent) a PSH (push). Celý průběh útoku demonstruje obrázek 2.4. [20]

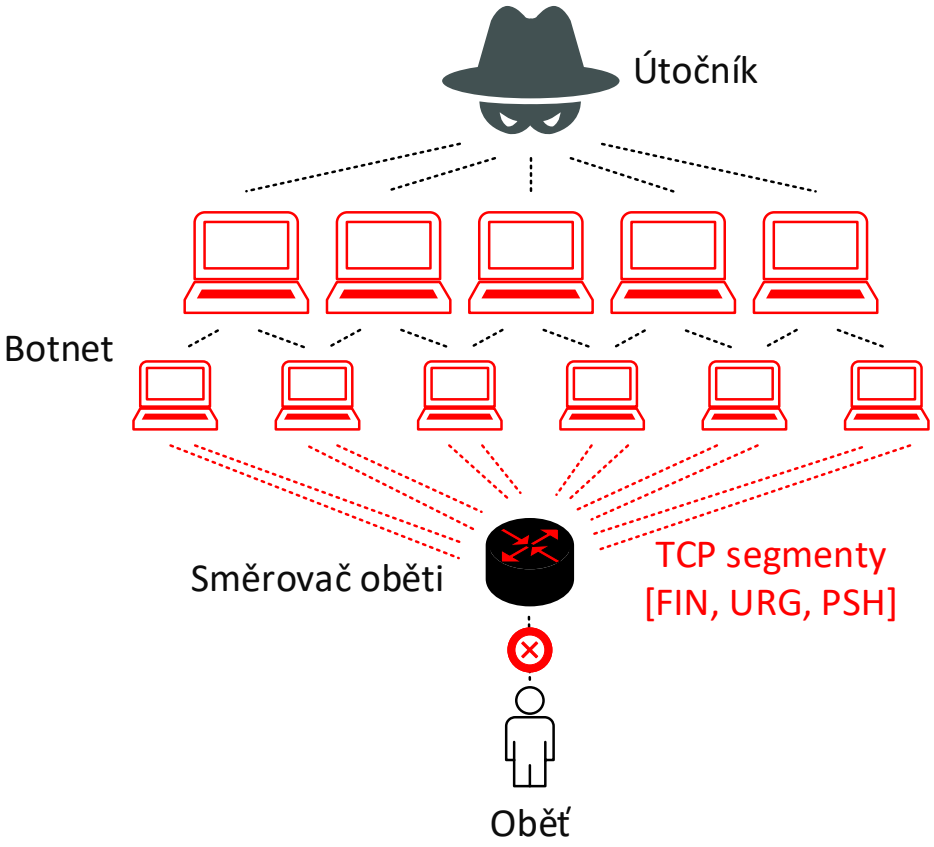
Takové pakety jsou potom využívány při útocích. Odesílání velkého množství těchto datově náročných paketů může způsobit zpomalení nebo zahlcení komunikační sítě. Christmas Tree pakety se krom DDoS útoků mohou využívat i při tzv. hackerských průzkumech, kdy útočníci odesílají tyto pakety, aby získaly lepší představu o síti, do které se snaží proniknout. Každé zařízení v síti může na takové pakety odpovídat jiným způsobem, což může útočníkovi nemálo prozradit. Pakety mohou způsobit vypnutí nebo restartování určitého hardwaru. Takové chování může odesílateli naznačit slabinu v podobě zastaralé části zařízení s menší výpočetní schopností, na které může svůj útok směřovat. [21]

Slowloris

Slowloris je DDoS útok, který umožňuje útočníkovi vyřadit z provozu HTTP (HyperText Transfer Protocol) server běžící na jiném počítači pomocí velkého množství otevřených síťových spojení mezi útočníkem a obětí po co nejdelší možnou dobu.

Jedná se o útok na 7. vrstvě ISO/OSI modelu pracující s HTTP požadavky. Nejedná se přímo o typ útoku, jako spíš o útočný nástroj, který umožňuje jedinému počítači znepřístupnit server bez použití velké šířky pásma. Na rozdíl od útoků založených na reflexích, jako jsou například NTP Amplification, používá tento útok nízkou šířku pásma a usiluje o využití serverových zdrojů pomocí požadavků, které se zdají být pomalejší než obvykle, ale jinak napodobují běžnou komunikaci.

Patří do kategorie útoků známých jako „low and slow“ (nízké a pomalé). Cílový server má k dispozici pouze omezený počet podprocesů pro zpracování souběžných připojení. Útočník tak pošle neukončený HTTP požadavek a pak postupně posílá záhlaví dílčích HTTP požadavků, aby udržel požadavek naživu. V podstatě říká „Jsem stále tady! Jsem jen pomalý, počkejte na mě!“. Každý podproces serveru se pokusí zůstat aktivní, zatímco čeká na pomalou žádost o dokončení, která nikdy nedorazí. Po překročení maximálního možného počtu připojení serveru bude každé další připojení odmítnuto a tím dojde k zamítnutí dané služby [22].



Obr. 2.4: Schématický znázornění DDoS útoku – Christmas Attack

Land Attack

Tento útok bývá také znám jako Same source attack nebo Dest Flood. Oběť útoku obdrží spoofed(podvržené) TCP–SYN pakety s vysokou četností. Podvržená IP adresa je adresa oběti. V hlavičce paketu je v poli source (zdroj) i destination (cíl)

identická IP adresa. Tím dochází k nekonečné smyčce. Přestože je zdrojová a cílová adresa identická, obsah paketu je velmi často irelevantní. Útočník se totiž snaží vyčerpat systémové prostředky oběti. Většina bran firewall by měla zachytit a zlikvidovat nežádoucí pakety tohoto druhu a tím chránit oběť před útokem. Některé operační systémy vydaly aktualizace, které opravují tuto bezpečnostní zranitelnost. Kromě toho by měli být všechny směrovače konfigurovány tak, že budou blokovat veškerý provoz paketů, který má stejnou zdrojovou a cílovou IP adresu. [23]

2.2 Legitimní provoz

Legitimní provoz je relativní pojem označující takový provoz, který má ke koncovému uživateli, zákazníkovi nebo serveru opravdu směřovat. Zároveň se jedná o provoz, v rámci kterého nedochází k žádným útokům nebo nestandardním událostem v podobě anomálií síťového provozu. Nastává zde však problém, síťový provoz který se jeví v rámci jedné síťové infrastruktury jako nestandardní (např. zvýšené množství přenášených dat nebo velké množství TCP spojení) může představovat v jiné síťové infrastruktuře zcela běžný a legitimní provoz. Z takového důvodu je nutné přistupovat k definici legitimního provozu vždy ve vztahu ke konkrétní síťové infrastruktuře.

Dalším problémem je stanovení parametrů, které budou mít dostatečnou vypovídající hodnotu. I k stanovování těchto parametrů je nutné přistupovat individuálně. Pro běžného uživatele domácí sítě není množství přenášených dat za posledních deset minut tak důležitým parametrem jako pro větší firemní síť, pro kterou může zvýšená hodnota signalizovat potenciální hrozbu a s ní spojenou možnou finanční ztrátu. S definicí legitimního provozu a stanovením dostatečně vypovídajících parametrů souvisí i určení tkzv. prahových hodnot. [24]

2.2.1 Prahové hodnoty legitimního provozu

Jak již bylo zmíněno v kapitole 2.2, nedílnou součástí definice legitimního provozu a určení dostatečně vypovídajících parametrů je i stanovení prahových hodnot. Prahová hodnota je taková hodnota, která představuje určitou mez, jejíž překročením nebo vychýlením se, dojde k nějakému jevu. Prahová hodnota nemusí být jedna konkrétní hodnota, může se jednat o interval, jehož překročením nebo vychýlením se, dojde k již zmiňovanému jevu. [25]

V pojetí síťového provozu je stanovování takovýchto hodnot otázkou dlouhodobého monitoringu a zároveň shromáždění dostatečně velké množiny dat, která bude následně zanalyzována a nad kterou budou provedeny vhodné statistické výpočty, jejichž výstupem bude již zmiňovaná prahová hodnota nebo interval.

Statistických metod, využívaných pro analýzu dat existuje celá řada a jejich volba přímo ovlivňuje vypovídající úroveň výsledných hodnot. Níže popsané statistické metody vycházejí z článku [26].

Aritmetický průměr

Aritmetický průměr představuje součet shromážděných hodnot vydělený jejich počtem. Je užitečný při určování celkového trendu datového souboru nebo pro rychlé nastínění povahy dat. Mezi další výhody patří snadná implementace a jednoduchost. Samotný aritmetický průměr je však nebezpečným nástrojem. V datech s vysokým počtem odlehlých hodnot nebo různých typů rozdělení průměr jednoduše neposkytuje dostatečnou přesnost. Udává se jako 2.1,

$$\overline{x} = \frac{1}{n}(x_1 + x_2 + \ldots + x_n) = \frac{1}{n}\sum_{i=1}^{n} x_i. \tag{2.1}$$

Směrodatná odchylka

Směrodatná odchylka představuje míru statistické variability. Určuje tedy jak moc jsou naměřené hodnoty rozptýleny nebo odchýleny od průměru. Nízká směrodatná odchylka znamená, že se větší množství naměřených hodnot blíží střední hodnotě (průměru). Stejně jako aritmetický průměr může i směrodatná odchylka být sama o sobě klamná. Pokud mají data podivný vzor, nebo vysoké množství odlehlých hodnot, pak směrodatná odchylka neposkytne všechny potřebné informace. Udává se jako 2.2,

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \overline{x})^2}. \tag{2.2}$$

Regrese

Regresní analýza je označení statistických metod, které umožňují odhadovat hodnotu jisté náhodné veličiny na základě znalosti jiných veličin. Někdy však může význam určitých hodnot ležet dostatečně odlehle od jiných hodnot. Regresní křivka se pak bude snažit takovou hodnotu ignorovat a tím i zkreslovat výsledek.

Stanovení velikosti vzorku

Při měření velkého souboru dat (např. populace) vždy není nutné sbírat informace od každého člena této populace. Trik spočívá v určení správné velikosti vzorku, jehož vypovídající síla bude dostatečně přesná. Pomocí metod již zmiňovaných lze určit správnou velikost vzorku, kterou potřebujeme k tomu, aby byl sběr dat statisticky významný.

Problém však může nastat v případě, kdy probíhá studie nové, netestované proměnné. V takovém případě musí tzv. proporční rovnice spoléhat na určité předpoklady, které však mohou být zcela nepřesné.

Testování hypotéz

Testování hypotéz, také běžně známé jako t-testování. Posuzuje, zda určitá premisa skutečně platí pro naměřeno sadu dat. Testy hypotéz se používají ve všech oblastech, od vědy a výzkumu až po obchodní a ekonomické. Aby byly testy hypotéz přesné, musí brát na vědomí běžné chyby, ke kterým během měření nebo testování dochází.

3 Praktická část bakalářské práce

V následující kapitole je popsán průběh praktické části bakalářské práce. Jsou zde rozebrány zvolené parametry síťové komunikace, sběr dat, zpracování dat a následná realizace neuronové sítě. Závěrem kapitoly jsou popsány dosažené výsledky.

3.1 Volba parametrů síťové komunikace

Síťovou komunikaci lze popsat celou řadou rozličných parametrů. Na základě těchto parametrů jsme schopni vytvářet závěry, na základě kterých lze klasifikovat, co se během komunikace děje nebo dělo, kdo s kým navazoval spojení, popřípadě jaká byla velikost přenesených dat.

Tato bakalářská práce se zaměřuje zejména na klasifikaci sledované komunikace, která je zaměřena na rozlišení legitimní komunikace od nestandardního provozu a útoků typu DDoS. Události odlišné od legitimní komunikace lze detekovat právě na základě specifických parametrů, kterými jsou tyto jevy charakteristické. Jedná se například o náhlý a neočekávaně velký objem přenesených dat, množství nápadných a nežádoucích paketů nebo velký počet polootevřených spojení. Některé z těchto parametrů byli použity v podobných pracích [27, 28], přičemž jejich vypovídající síla je pro tuto bakalářskou práci dostatečná. Jako parametry vypovídající o anomálii nebo DDoS útoku byly zvoleny:

1. *Množství přenesených dat*: Záplavové DDoS útoky jsou charakteristické nadměrných množstvím přenášených dat. Důležité je však zmínit, že toto nadměrné množství je neočekávané. Může se například jednat o plánovaný update softwaru firemní infrastruktury, který je doprovázen větším množstvím přenášených dat. Takováto událost by měla být s dostatečným předstihem dopředu hlášena. V rámci legitimního provozu k takovým jevům dochází buď z opodstatněných důvodů nebo v případě, že je daný jev pro danou povahu provozu očekávaný. Pro síť s datovými servery s velkým množstvím obsahu, bude zvýšená hodnota tohoto parametrů standardní a běžná. To znamená, že i z dlouhodobého hlediska bude tento parametr nabývat podobných a vyšších hodnot oproti klasické domácí sítí. Udává se jako 3.1,

$$s_d = \sum_{i=1}^{n} x_i, \tag{3.1}$$

kde n představuje počet paketů v celém úseku zachycené komunikace a x_i velikost každého následujícího paketu.

2. *Počet paketů*: Příliš velké množství paketů může být způsobeno právě útokem DDoS. Takovéto množství nemusí jednotlivé síťové prvky stíhat zpracovávat nebo přeposílat a dojde k zahlcení. Vysoký počet paketů může signalizovat zvýšený provoz v síti, který může být pro určitou síťovou infrastrukturu běžný a pro jinou nestandardní.
3. *Počet nestandardních paketů*: Jako nestandardní nebo nesmyslné pakety jsou označovány takové pakety, které obsahují nestandardní nebo nesmyslnou kombinaci nastavených příznaků, nevyskytujících se v běžné komunikaci. Může se jednat například o paket, který má všechny příznaky nastavené na SET. Dalším nestandardním paketem je Christmas paket, jehož popisem se zabývá kapitola 2.1.5. Takovéto pakety vyžadují větší množství výpočetní kapacity jednotlivých síťových prvků než „standardní“ pakety. V krajních případech můžou takovéto pakety vyřadit zranitelný síťový prvek z provozu a tím poškodit celou síťovou infrastrukturu.

   Řada modernějších IDS (Intrusion Detection System)[1] systémů dokáže takovéto pakety rozpoznat a automaticky zahodit.
4. *Entropie velikosti paketu*: Velké množství DDoS i DoS útoků zcela vynechávají část datového přenosu a dochází k zasílání nadměrného množství podobných, ne-li stejně velkých paketů. Proto může být hodnota tohoto parametru užitečná při detekci těchto událostí. Při takovýchto útocích se hodnota parametru blíží nule. V rámci legitimního provozu je tato hodnota naopak vyšší a velmi proměnná, jelikož během provozu dochází k posílání paketů rozličných velikostí. Udává se jako 3.2,

$$p_e = -\sum P_i \log_2 P_i, \tag{3.2}$$

   kde P_i představuje pravděpodobnost výskytu paketu určité velikosti v zachyceném úseku síťové komunikace.
5. *Počet spojení*: Počet komunikujících stran je během DDoS útoků vyšší. Jak již bylo zmíněno v podkapitole 2.1.1, takovéto útoky využívají tkzv. botnetu, jehož existence automaticky zvyšuje hodnotu tohoto parametru. Během legitimního provozu je hodnota nižší oproti provozu, ve kterém došlo k útoku.

[1] Software nebo hardware užívaný k odhalení pokusů o proniknutí do sítě nebo systému.

6. *Průměrné množství dat za sekundu*: Záplavové útoky jsou charakteristické schopností vygenerovat obrovské množství dat během velmi krátkého úseku. Proto je tento parametr více než vhodný pro detekci takovýchto událostí. Během legitimního provozu je hodnota tohoto parametru spíše nižší oproti provozu, ve kterém došlo k útoku nebo nějaké nestandardní události. Udává se jako 3.3,

$$a_{ps} = \frac{\sum_{i=1}^{n} x_i}{t_e - t_a}, \tag{3.3}$$

kde n představuje počet paketů v celém úseku zachycené komunikace, x_i velikost každého následujícího paketu, t_e čas doručení prvního paketu a t_a čas doručení posledního paketu.

3.2 Sběr dat

Sběr dat je nedílnou součásti při tvorbě detekčního systému. Samotná data nám charakterizují události, které se během síťové komunikace udály. Pomocí těchto dat je potom detekční systém schopen rozpoznat odlišnosti v síťové komunikaci. Proto, aby byl systém schopen rozlišit mezi legitimním, nestandardním a útočným provozem, je nejdříve nutné připravit data, která takové provozy demonstrují. Pro záznam dat v této práci byla použita počítačová aplikace Wireshark, která slouží jako protokolový analyzér a paketový sniffer (čmuchal). Výstupem tohoto programu je soubor ve formátu PCAP[2]. Takovýto PCAP soubor je potom nutné převést do formátu CSV[3], který je pro zpracování v navrženém systému vhodnější. Reálnost hodnot v použitých datech určuje jejich vypovídající sílu.

3.2.1 Legitimní provoz

Síťová komunikace použitá v této bakalářské práci demonstrující legitimní provoz byla převzata z výzkumné laboratoře na ČVUT (České vysoké učení technické v Praze) [29]. Jedná se o provoz během kterého uživatelé přistupují k nejvíce navštěvovaným webovým stránkám nebo vykonávají běžné úkony v síti, jako je čtení článků, chatování, poslech hudby a stahování legálního obsahu. Tyto webové stránky jsou vybírány na základě statistických výsledků, vyplývajících z průzkumů dceřiné společnosti Alexa, spadající pod společnost Amazon [30]. Komunikace byla zachycena z různých časových úseku dne v rozmezí 6:00 – 23:00. V těchto časech byli uživatelé aktivní. Tyto data budou následně použita pro stanovení prahových hodnot legitimního provozu.

[2]Souborový formát, který obsahuje zachycenou síťovou komunikaci

[3]Jednoduchý souborový formát určený pro výměnu tabulkových dat.

3.2.2 Nestandardní provoz

Síťová komunikace použitá v této bakalářské práci demonstrující nestandardní provoz, tedy takový provoz v rámci kterého může docházet k odlišnostem od námi stanoveného legitimního provozu, byla zachycena ve spolupráci se sdružením CESNET[4]. Během této komunikace docházelo ke stahování obsahu a přistupování na FTP server[5]. Součástí komunikace jsou tedy i události jako například zvýšený objem přenášených dat, nebo větší množství spojení. Během této komunikace sice nedošlo k žádnému útoku, avšak od síťové infrastruktury generující legitimní provoz popsané v podkapitole 3.2.1, je takový provoz odlišný.

3.2.3 Útočný provoz

První část síťové komunikace použitá v této bakalářské práci demonstrující útočný provoz byla simulována pomocí dvou virtuálních počítačů s operačním systémem Linux a distribucí Debian ve verzi 4.9.110. Samotné virtuální počítače byly spuštěny pomocí virtualizačního nástroje Oracle VM VirtualBox. Obě stanice představují útočníka, který se snaží oběť zaplavit množstvím nestandardních paketů. Útočná komunikace byla zachycena během provozu, v rámci kterého docházelo k přístupům na rozličné webové stránky. Útočný provoz vyskytující se v síťové komunikaci je reprezentován výskytem nestandardních Christmas paketů, které jsou popsány v kapitole 2.1.5.

Druhá část síťové komunikace byla simulována pomocí zátěžového generátoru Spirent Avalanche 3100B [31], určeného k testování síťové infrastruktury na vrstvách L4–L7 ISO modelu. Umožňuje simulovat požadavky nebo například množství uživatelů podle zvolené zátěže. Ovládání tohoto generátoru bylo zprostředkováno pomocí serveru s OS Windows 2012, na kterém byl nainstalovaný ovládací software Avalanche Commander. Pro účely této bakalářské práce byl Spirent Avalance 3100B použit jako generátor útoků (DNS Amplification, TCP SYN Flood, UDP Flood, NTP Amplification) popsaných v podkapitole 2.1.4.

Třetí část síťové komunikace představující útočný provoz byla simulována pomocí nástroje SlowHTTPTest [32]. Nástroj je vhodný pro testování aplikačních útoku typu DoS. Pro účelý této bakalářské práce byl generován provoz útoku Slowloris 2.1.5.

3.3 Zpracování dat

Data výše uvedené komunikace jsou v „surové“ podobě ve formátu CSV. Pro spolehlivou klasifikaci komunikace je nutné taková data zpracovat a analyzovat pomocí

[4]Sdružení zabývající se výzkumem a vývojem informačních a komunikačních technologií.

[5]Počítač, který napomáhá při výměně souborů přes internet

klasifikačních metod, které rozhodnou, zda-li se jedná o legitimní provoz, nestandardní provoz nebo útok. Pro zpracování těchto dat byl využit objektově orientovaný programovací jazyk Python ve verzi 3.6.7, pomocí kterého byl napsán skript, který s těmito daty pracuje. Skript byl naprogramován ve vývojovém prostředí PyCharm ve verzi 2018.3 Community Edition od společnosti JetBrains.

Samotný skript využívá pro práci s daty knihovnu Pandas [33]. Jedná se o vhodnou knihovnu pro analýzu dat, které lze reprezentovat 2D tabulkou. Tento „tvar“ dat najdeme právě v CSV souborech. Skript nejdříve pracuje s daty v „surové“ podobě a jednotlivé CSV soubory rozděluje vždy po desetiminutových úsecích. Prochází každý řádek a data jednotlivých kategorií setřiďuje a ukládá do vhodné datové struktury v podobě seznamu (list). Nad těmito seznamy pak skript počítá jednotlivé statistické výpočty.

3.3.1 Stanovení prahových hodnot

Jak již bylo nastíněno v kapitole 2.2.1, legitimní provoz je relativní pojem. Zcela běžné chování v rámci jedné síťové infrastruktury, může v jiné síťové infrastruktuře představovat potenciální nebezpečí. Proto je potřeba k definici legitimního provozu přistupovat individuálně. Jako legitimní provoz, na základě kterého budou stanoveny prahové hodnoty byl zvolen provoz popsaný v podkapitole 3.2.1.

Jako statistickou metodu, pro stanovení prahových hodnot zvolených parametrů byl použit interval spolehlivosti s konfidenční hladinou 95 % [25]. Jedná se o typ intervalového odhadu neznámého parametru. Pomocí tohoto intervalu lze získat představu o tom, v jakém rozpětí se může hodnota daného parametru pohybovat. Existují tři typy intervalu spolehlivosti: oboustranný, levostranný a pravostranný. V této bakalářské práci jsou použity všechny tři. Vzorec pro výpočet oboustranného intervalu spolehlivosti pro střední hodnotu se udává jako 3.4,

$$\overline{x} - 1,96 \times \frac{\sigma}{\sqrt{n}} \leq \mu \leq \overline{x} + 1,96 \times \frac{\sigma}{\sqrt{n}}, \tag{3.4}$$

kde $\overline{x}$ představuje střední hodnotu, σ směrodatnou odchylku, n počet naměřených hodnot. Hodnota 1,96 představuje 100 × (1 - 0,05/2) = 97,5% kvantil normovaného Gaussova normálního rozdělení $u_{0,975}$. Pravostranný interval spolehlivosti s konfidenční hladinou 95 % se udává jako 3.5,

$$-\infty \leq \mu \leq \overline{x} + 1,645 \times \frac{\sigma}{\sqrt{n}}, \tag{3.5}$$

kde hodnota 1,645 představuje 100 × (1 - 0,05) = 95% kvantil normovaného Gaussova normálního rozdělení $u_{0,950}$. Levostranný interval spolehlivosti s konfidenční hladinou 95 % se potom udává jako 3.6,

$$\overline{x} - 1,645 \times \frac{\sigma}{\sqrt{n}} \leq \mu \leq \infty. \tag{3.6}$$

Pro stanovení intervalu spolehlivosti ve vztahu k legitimnímu provozu je nutné velké množství naměřených hodnot. Obyčejně taková data představují naměřené hodnoty z několika měsíců i let. Pro účely této bakalářské práce však byla shromážděna data z jednoho týdne aktivního provozu sítě, tedy zhruba 120 hodin, což představuje 720 desetiminutových úseků (vzorků), ze kterých budou stanoveny prahové hodnoty. Tuto skutečnost je nutné brát na vědomí a zavést do celého systému určitou toleranci výsledků.

Prahové intervaly zvolených parametrů

Volba vhodného intervalu spolehlivosti pro zvolené parametry je důležitou součástí procesu stanovování prahových intervalů. Pro parametry popisující množství paketů, množství přenesených dat, průměrné množství dat za sekundu a počet nestandardních paketů je nejvhodnější použít pravostranný interval spolehlivosti. Tento interval popisuje maximální možnou tolerovanou hodnotu. Čím vyšší je naměřená hodnota těchto parametrů, tím vyšší je zatížení síťové infrastruktury. V opačném případě tomu je u parametru popisujícího entropii velikosti paketu. Čím vyšší je naměřená hodnota tohoto parametru, tím různorodější provoz je. Záplavové útoky jsou charakteristické posíláním obrovského množství stejně velikých paketů, tato skutečnost má za následek to, že se naměřené hodnoty tohoto parametru blíží nule. Z tohoto důvodu byl pro tento parametr zvolen levostranný interval spolehlivosti. Oboustranný interval spolehlivosti byl použit u parametru popisujícího počet spojení během komunikace. Příliš vysoká hodnota může signalizovat záplavové útoky a příliš nízká hodnota zase útoky DoS.

Prahové intervaly zvolených parametrů společně s použitým typem intervalu spolehlivosti zobrazuje tabulka 3.1. Všechny tyto prahové intervaly se vztahují k hodnotám naměřeným během desetiminutových úseků z celkem 720 hodin. Jak již bylo uvedeno v podkapitole 2.2, využití průměru, směrodatné odchylky apod. sebou přináší různé problémy. V datech s vysokým počtem odlehlých hodnot nemusí tyto veličiny poskytovat dostatečnou přesnost. Zároveň musí být zohledněna skutečnost, že je množství naměřených hodnot nižší, než by tomu tak bylo při dlouhodobějším měření. Pro pojmutí většího množství vzorků pro následné označkování dat byla zvolena 30% tolerance přesahu prahového intervalu, která se ukázala dle tabulky 3.2, jako nejvhodnější. V takovém případě interval pojme nejvíce vzorků a zároveň nedochází k příliš velkému vychýlení ze stanoveného prahového intervalu.
Z grafu 3.1 zobrazujícího stanovenou prahovou hodnotu pro množství paketů lze vypozorovat, že se hodnoty parametru, až na několik výjimek pohybují ve stanoveném intervalu. Stejné skutečnosti si lze všimnout u grafů 3.2, 3.3, 3.4, 3.5, které zobrazují ostatní parametry a jejich prahové intervaly. Jedinou výjimkou je

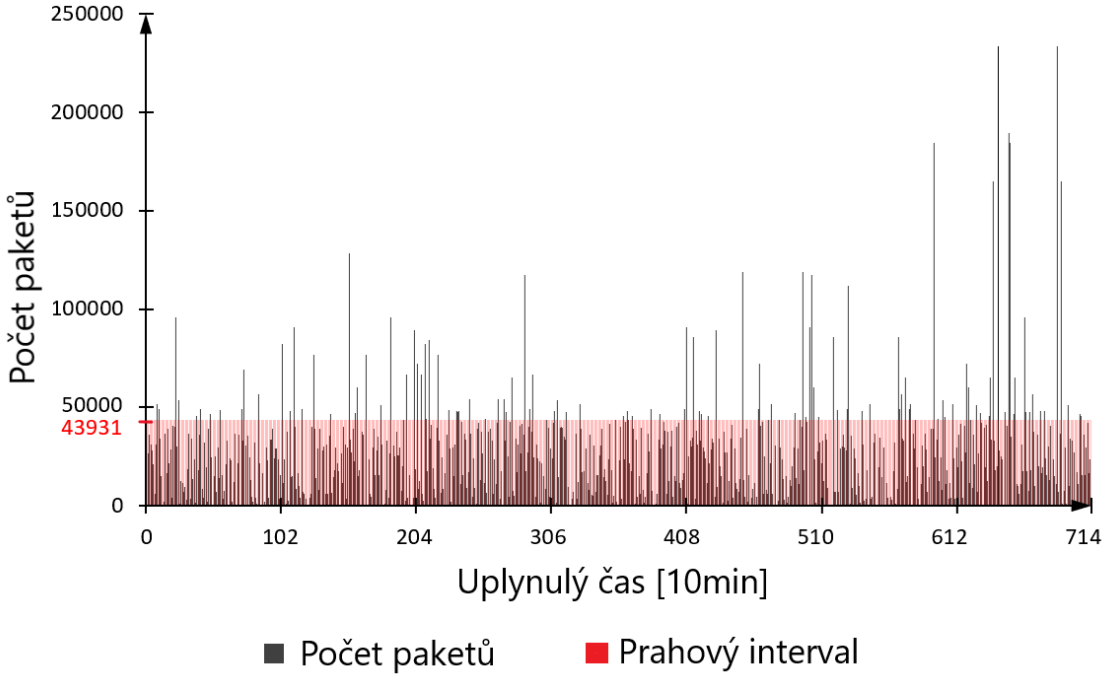
parametr popisující výskyt množství nestandardních paketů. Během legitimního provozu se totiž takový paket vůbec nevyskytl, a proto byl prahový interval stanoven jako $(0; 0\rangle$.

Tab. 3.1: Prahové intervaly jednotlivých parametrů.

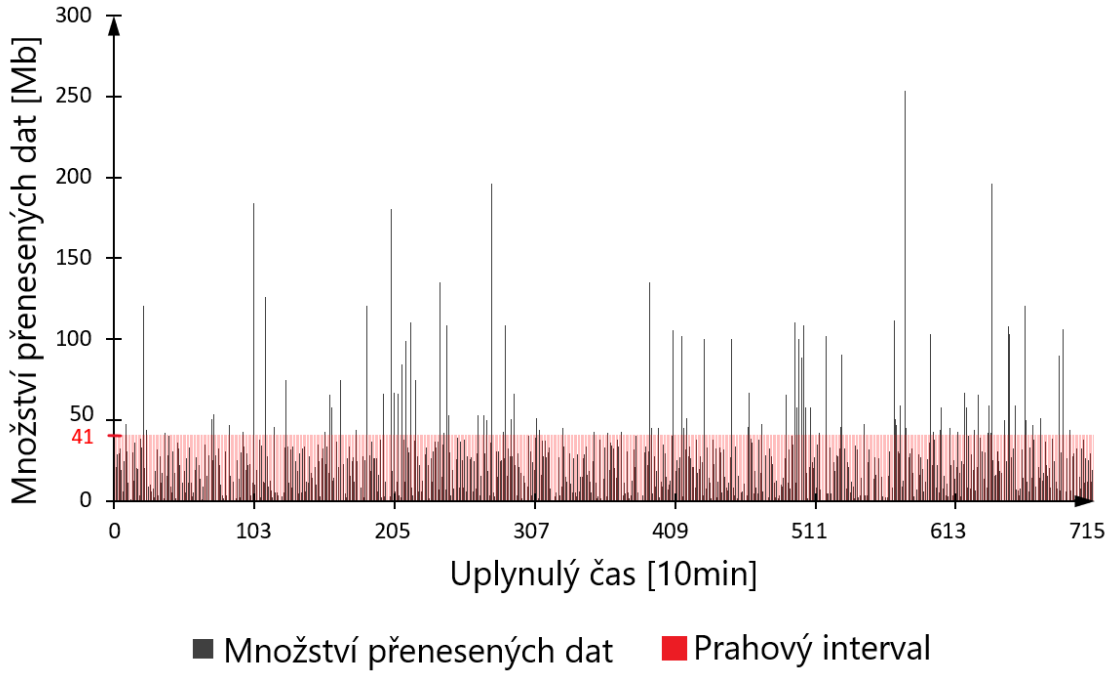
Parametr	**Prahový interval**	**Interval spolehlivosti**
Počet paketů	$(0; 43931\rangle$	pravostranný
Množství přenesených dat [Mb]	$(0; 41{,}0\rangle$	pravostranný
Počet spojení	$\langle 118; 217\rangle$	oboustranný
Průměrné množství dat za sekundu [Mb]	$(0; 0{,}15\rangle$	pravostranný
Entropie velikosti paketu	$\langle 2{,}3; \infty)$	levostranný
Počet nestandardních paketů	$(0; 0\rangle$	pravostranný

Tab. 3.2: Množství použitých vzorků s % tolerancí přesahu prahových intervalů.

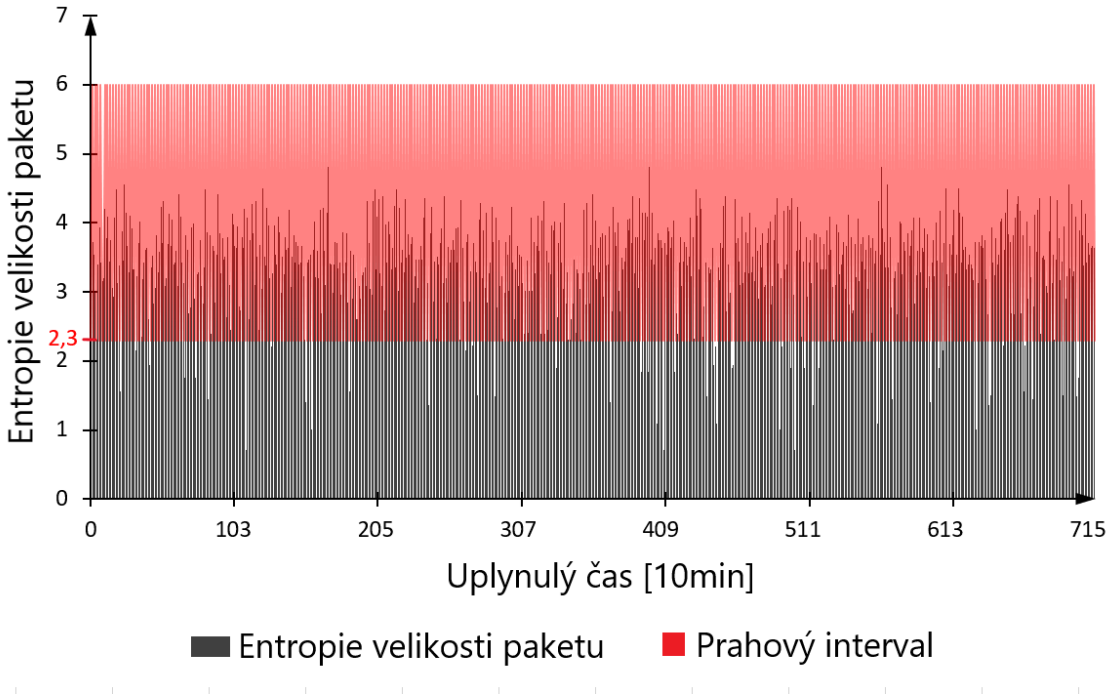
	Tolerance		
Parametr	**30 %**	**20 %**	**10 %**
Počet paketů	83,75%	79,9%	73,75%
Množství přenesených dat	85,83%	80,12%	79,5%
Počet spojení	93,42%	86,25%	81,20%
Průměrné množství dat za sekundu	93,33%	86,14%	81,25%
Entropie velikosti paketu	92,91%	87,90%	80,83%
Počet nestandardních paketů	100,00%	100%	100%



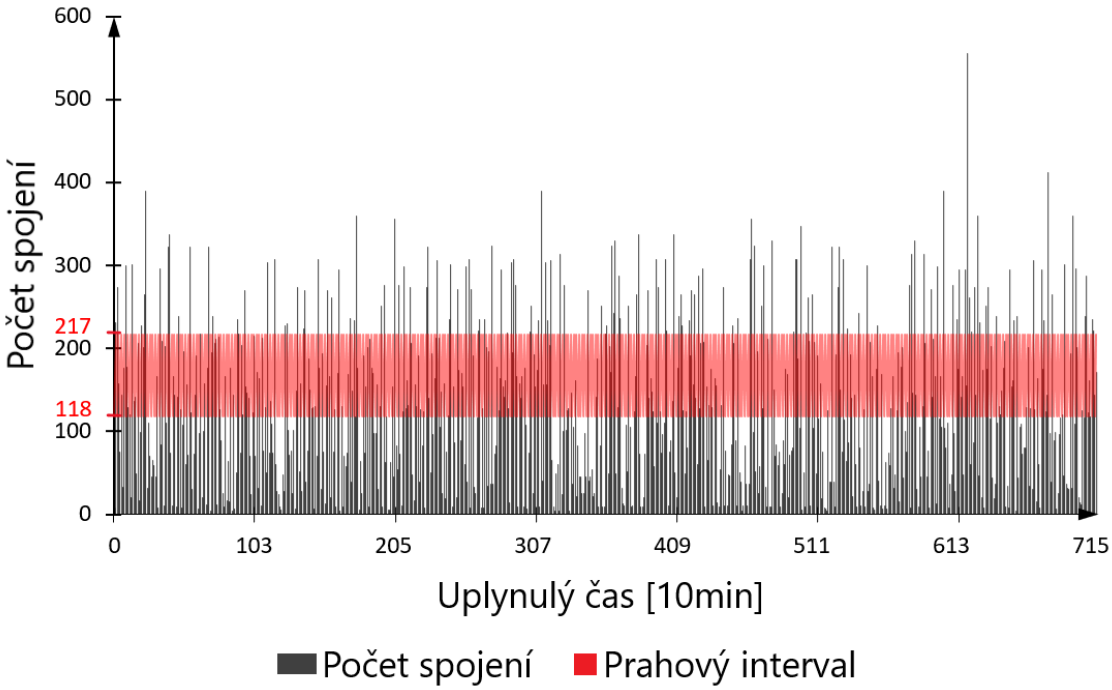
Obr. 3.1: Graf prahového intervalu pro množství paketů.



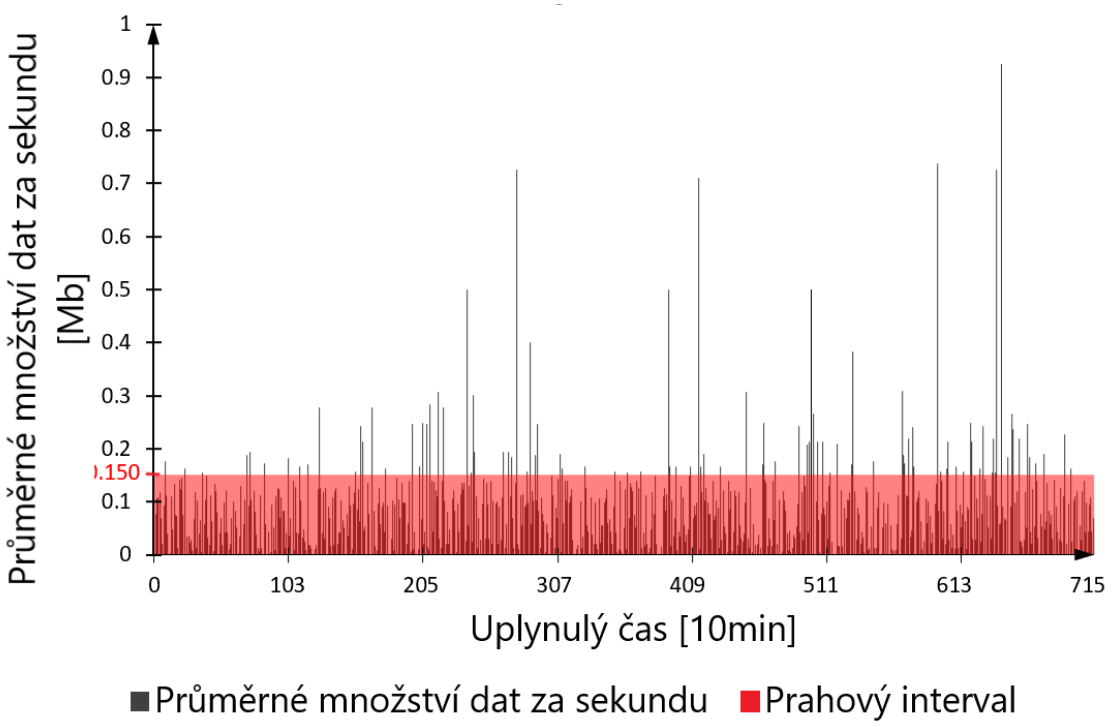
Obr. 3.2: Graf prahového intervalu pro množství přenesených dat.



Obr. 3.3: Graf prahového intervalu pro entropii velikosti paketu.



Obr. 3.4: Graf prahového intervalu pro počet spojení.



Obr. 3.5: Graf prahového intervalu pro průměrné množství dat za sekundu.

Značkování dat

Značkování dat je nedílnou součástí procesu zpracování dat. Pomocí vhodného označkování bude posílena rozlišovací schopnost neuronové sítě. Se samotným značkováním souvisí i stanovení pravidel, na základě kterých budou daná data označkována. Při tvorbě pravidel je nutné brát na vědomí fakt, že vychýlení určitých parametrů nemusí nutně znamenat výskyt anomálie nebo útoku. Během normálního provozu se běžné stává, že uživatelé stahují větší množství obsahu než je obvyklé nebo navštěvují větší množství webových stránek. Obecně však taková situace nepředstavuje žádnou větší hrozbu pro síťovou infrastrukturu. Pro účely této bakalářské práce byla sestavena tabulka pravidel popisující legitimní, nestandardní a útočný provoz 3.3. Pomocí této tabulky pravidel budou označkována data, která budou v trénovací fázi představovat trénovací množinu vstupních dat neuronové sítě.

Na základě poznatků z článku [34], překročení prahové hodnoty intervalu jednoho nebo i všech parametrů o maximálně 10 % nemusí nutně znamenat výskyt nestandardního provozu nebo útoku. Stejně tomu tak je v případě, kdy se méně jak půlka parametrů vychýlí o více jak 10 %. Takovéto případy jsou označkovány značkou 00. Za nestandardní provoz lze dle kapitoly 2 považovat cokoliv, co se nějakým způsobem odchyluje od běžného a očekávaného. Vychýlení poloviny a více parametrů o více jak 10 % a méně jak 20 % může v síťové infrastruktuře

signalizovat zvýšený provoz nebo potenciální hrozbu, ke které může dojít. Takto zvýšené hodnoty nemusí nutně znamenat výskyt útoku, ale mohou mít určitou vypovídající hodnotu. Tyto případy jsou označkovány značkou 10. Jestliže dojde k vychýlení poloviny a více parametrů o více jak 20 %, pak mohou takové hodnoty znamenat výskyt útoku. Takovéto případy jsou potom označkovány značkou 11.

Tab. 3.3: Pravidla pro označkování trénovací množiny dat.

Počet parametrů	**Přesah [%]**	**Značka**
$\langle 1; 6\rangle$	$\langle 0; 10\rangle$	00
$\langle 1; 3)$	$(10; 20\rangle$	00
$\langle 1; 3)$	$(20; \infty)$	00
$\langle 3; 6\rangle$	$(10; 20\rangle$	10
$\langle 3; 6\rangle$	$(20; \infty)$	11
$\langle 1; 3)$	$\langle 10; 20\rangle$	11
$(1; 4\rangle$	$(20; \infty)$	
$\langle 1; 3)$	$(20; \infty)$	11
$(1; 4\rangle$	$(10; 20\rangle$	

3.4 Realizace neuronové sítě

Po sesbírání vhodných dat charakterizujících provozy popsané v podkapitole 3.2, jejich následné setřídění, analyzování a zpracování, nastává fáze, při které budou tyto data představovat vstupní hodnoty do neuronové sítě. Neuronovou síť je nutné nejdříve vytvořit, natrénovat a otestovat. Pro tvorbu neuronové sítě bylo použito vývojové prostředí PyCharm ve verzi 2018.3 Community Edition od společnosti JetBrains. Samotná neuronová síť je napsána v jazyce Python ve verzi 3.6.7.

3.4.1 Tvorba modelu neuronové sítě

Vhodným nástrojem pro tvorbu modelu neuronové sítě jsou knihovny nebo balíčky, které usnadňují jejich realizaci. Využití knihoven odstraňuje nutnost znalosti složitých matematických výpočtů, které se vykonávají na pozadí. Právě tato vlastnost zjednodušuje tvůrci kódu tvorbu neuronové sítě a zároveň mu poskytuje možnost zaměření své pozornosti na jádro problému. Pro účely této bakalářské práce byla použita open–source knihovna Scikit–learn [35]. Jedná se o volně dostupný a vhodný nástroj pro práci s daty a jejich analýzu. Tato knihovna je i vhodným nástrojem pro řešení problému klasifikace, tedy problému, kdy je nutné rozhodnout do jaké kategorie sledovaný objekt patří.

Parametry modelu neuronové sítě

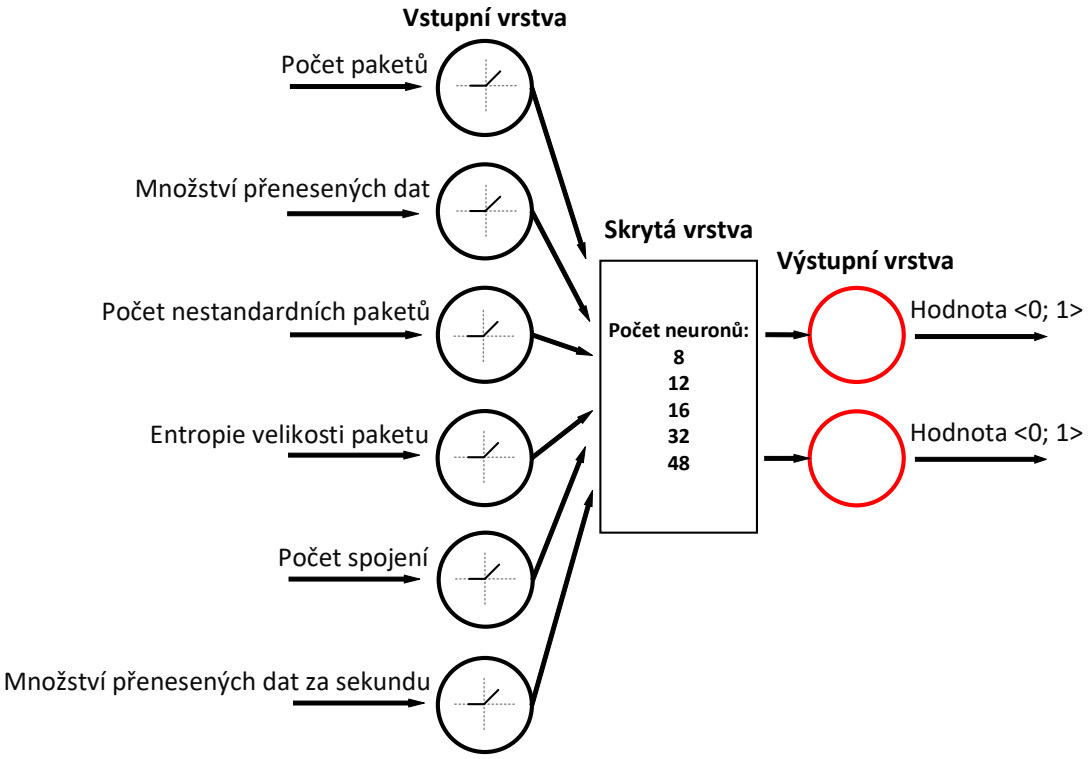
Parametry modelu neuronové sítě určují celkovou kvalitu výstupu. Obecně lze říci, že pokud síť obsahuje malý počet neuronů, tak je její schopnost popsat závislosti v trénovací množině dat slabší. Na druhou stranu, pokud bude síť obsahovat příliš velký počet neuronů, pak může být její schopnost generalizace, tedy vystihnout správný výsledek na nových datech, horší. Takovému jevu se říká přeučení sítě (overfitting). K přeučení může dojít i v případě, kdy model obsahuje velký počet vstupních parametrů a malý počet pozorování. Cílem je tedy dosažení vhodného kompromisu mezi trénovacím výkonem a schopností generalizovat znalosti na nových datech. Celý model neuronové sítě zobrazuje obrázek 3.6.

Mezi parametry neuronové sítě patří:

- *Počet neuronů ve vstupní vrstvě*: Tento počet vychází z počtu parametrů, které popisují síťovou komunikaci. V této bakalářské práci bylo použito 6 parametrů popisující stav síťové komunikace. Jedná se o počet paketů, počet nestandardních paketů, množství přenesených dat, entropii velikosti paketu, množství přenesených dat za sekundu a počet spojení. Jednotlivé parametry jsou podrobně popsány v kapitole 3.1.
- *Počet neuronů ve skrytých vrstvách*: Množství neuronů ve skrytých vrstvách bývá obecně stanoven podle vzorce:

$$N_h = \frac{N_s}{\alpha \times (N_i + N_o)} \tag{3.7}$$

  kde N_h označuje počet neuronů ve skrytých vrstvách, N_s počet vzorků v trénovací množině dat, α škálovací faktor, který nabývá hodnot od 2 – 10 a souvisí se schopností generalizace. N_i označuje počet vstupních neuronů a $N_o$počet neuronů ve výstupní vrstvě. Pro testovací účely bylo množství neuronů ve skryté vrstvě měněno na 8, 12, 16, 32 a 48.
- *Počet neuronů ve výstupní vrstvě*: Výstupem neuronové sítě budou dvě hodnoty, které budou vypovídat o stavu síťové komunikace na základě předložených dat. Na základě značkování popsaného v podkapitole 3.3.1 byl stanoven počet neuronů ve výstupní vrstvě na dva. Oba neurony budou nabývat hodnot 1 a 0. Kombinací těchto hodnot získáme představu o předložených datech.
- *Počet skrytých vrstev*: Velké množství problému lze řešit pomocí jedné skryté vrstvy. Implementace více jak jedné skryté vrstvy je vhodná pro problémy jako rozpoznáváním tváře, obrazu nebo zvuku. Pro účely této bakalářské práce byla počet skrytých vrstev stanoven na 1.
- *Aktivační funkce*: Neurony nacházející se ve skrytých vrstvách neuronové sítě využívají ke své excitaci/inhibici aktivační funkci ReLU, která je podrobně popsána v kapitole 1.2.2.



Obr. 3.6: Schématický model neuronové sítě

3.4.2 Trénovací a testovací fáze

Trénovací množina dat představuje sadu dat, ve které algoritmus nachází určitý vztah, čímž se učí. Trénovací množina dat je reprezentována vstupním vektorem dat společně s odpovídajícím výstupem. Součástí trénovací fáze je metoda Backpropagation, která byla zmíněna v podkapitole 1.3.1. Procentuální zastoupení trénovacích dat v celé množině zpracovaných dat je 67%. Důležitou vlastností trénovací množiny dat by měla být její různorodost. Trénovací množina dat by zároveň měla obsahovat dostatečné množství zástupců jednotlivých kategorii. Nadměrné množství vzorků jedné kategorie by mohlo způsobit snížení rozlišovací schopnosti neuronové sítě. Množina dat, použita pro účely natrénování neuronové sítě, představuje kombinaci síťových provozů popsaných v podkapitole 3.2. Zastoupení dat představujících legitimní, nestandardní a útočný provoz v tomto pořadí se vyskytuje v trénovací množině v poměru 3:1:1. Odpovídající výstup vstupního vektoru představují značky stanovené na základě pravidel popsaných v podkapitole 3.3.1. Všechny útoky, popsané v podkapitole 3.2.3 byly dle zvolených pravidel označeny za útok, jelikož polovina a více parametrů přesáhla odpovídající prahový interval o více jak 20 %.

Testovací množina dat se používá pro ověření kvality naučeného systému. Tato množina dat by měla disponovat určitými odlišnostmi od trénovací množiny dat. Celý systém je naučený tehdy, jestliže vyhodnocuje s podobnou přesností testovací i trénovací množinu dat. Jestliže má systém výrazně vyšší úspěšnost vyhodnocení trénovací množiny, pak je takový systém přeučený. Procentuální zastoupení testovacích dat v celé množině zpracovaných dat je 33%. Samotná knihovna Scikit–learn obsahuje nástroj, který vhodně zvolí kombinaci trénovacích a testovacích dat tak, aby byly zástupci jednotlivých kategorii rovnoměrně a náhodně rozděleni.

Validační data se využívají pro úpravu jednotlivých parametrů systému ve snaze vyhnout se jeho nežádoucímu přeučení. Tyto data se používají mezi trénovací a testovací fází. Validační data vstupují do celého procesu a představují kombinaci trénovacích a testovacích dat.

3.5 Dosažené výsledky

V následující kapitole jsou prezentovány a okomentovány dosažené výsledky této bakalářské práce. Pro dosažení těchto výsledků byly použity provozy popsané v podkapitole 3.2. Součástí testování neuronové sítě byla i změna počtu neuronů ve skryté vrstvě. Vyhodnocení přesnosti a rozlišovací schopnosti neuronové sítě byla sledována a zaznamenávána. Dalším sledovaným parametrem neuronové sítě pak byla závislost změny počtu neuronů ve skryté vrstvě na celkové přesnosti a schopnosti identifikace daného provozu. Všechny výsledky vychází s maximálně 200 cyklů, během kterých byla neuronová síť trénována.

3.5.1 Přesnost neuronové sítě

Přesnost neuronové sítě byla stanovována na základě metody křížové validace. Trénovací množina dat byla rozdělena na určitý počet podmnožin. Jedna z podmnožin slouží jako testovací množina, zbylé podmnožiny slouží jako trénovací množina. Klasifikátor knihovny Scikit–learn trénuje model neuronové sítě a pomocí testovací množiny testuje její přesnost. Tento proces se ve stanoveném počtu iterací opakuje, pokaždé s jinou podmnožinou tvořící testovací a trénovací množinu. Výsledná přesnost je potom průměrem přesností jednotlivých iterací. V rámci této bakalářské práce lze pohlížet na přesnost námi vytvořené neuronové sítě z více pohledů. Jak z tabulky 3.4 vyplývá, schopnost rozlišit mezi legitimním provozem a nestandardním provozem nebo útokem neuronová síť zvládá s 95% úspěšnosti. Jinak tomu však je při rozlišení mezi nestandardním provozem a útokem. V takovémto případě se úspěšnost pohybovala kolem 65%. Takto nízkou úspěšnost mohlo ovlivnit více faktorů. Mezi nejpravděpodobnější faktor patří příliš malé množství trénovacích dat.

Pro úspěšné natrénování neuronové sítě je potřeba disponovat velkou množinou dat sestávající z dostatečného množství zástupců jednotlivých kategorií. V rámci této bakalářské práce nebyl shromážděn dostatečně velký objem dat, který by poskytoval potřebnou různorodost.

Dalším ovlivňujícím faktorem může být neadaptivní prahový interval. Běžné detekční systémy využívají při monitoringu síťového provozu tzv. adaptivní prahové hodnoty nebo intervaly [36]. To znamená že se jejich hodnota nebo intervalový rozsah v průběhu času mění. Při dostatečně velkém množství naměřených hodnot z jednotlivých úseků dne by bylo možné takový adaptivní prahový interval stanovit. Kvalitní detekční systémy takové adaptivní prahové intervaly nebo hodnoty stanovují v řádech týdnů až měsíců. V rámci této bakalářské práce byl stanoven konstantní prahový interval, na základě kterého jsou jednotlivé naměřené hodnoty posuzovány. Takové řešení nebere dostatečný ohled na časové úseky dne, během kterých je provoz přirozeně zvýšený a během kterých ne. Jako další faktor lze zmínit statistické metody, jejichž problematikou se zabývala podkapitola 2.2.1.

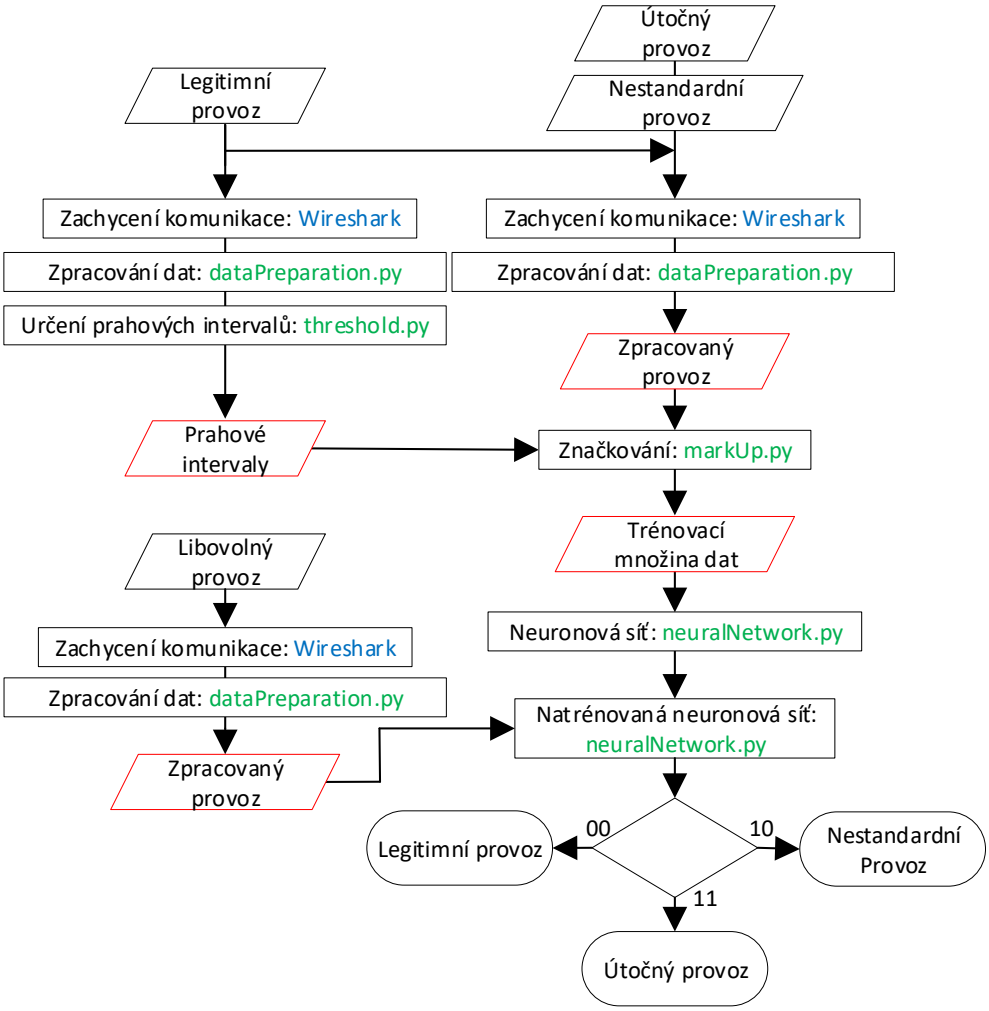
Tab. 3.4: Přesnost neuronové sítě v závislosti na počtu neuronů ve skryté vrstvě.

Druh provozu	**Počet neuronů**	**Přesnost [%]**
Legitimní provoz	8	95,478%
	12	95,510%
	16	95,602%
	32	95,690%
	48	95,701%
Nestandardní provoz	8	64,280%
	12	64,328%
	16	64,414%
	32	64,480%
	48	64,498%
Útočný provoz	8	64,300%
	12	64,330%
	16	64,410%
	32	64,486%
	48	64,498%

Dalším sledovaným parametrem byl vliv počtu neuronů ve skryté vrstvě na celkové přesnosti detekčního systému. Změna počtu nijak zásadně neovlivnila výslednou přesnost neuronové sítě.

Podle předpokladu dosáhla největší přesnosti neuronová síť s největším počtem neuronů. Přesnost se oproti ostatním variantám příliš neliší, a proto by její reálné použití vzhledem k časové a paměťové náročnosti bylo méně vhodné. Jako nejvhodnější se tedy ukázala varianty se 16 neurony ve skryté vrstvě.

Schématické znázornění vytvořeného detekčního systému v podobě vývojového diagramu zobrazuje obrázek 3.7. Celý detekční systém dokáže zpracovat data zaznamenané komunikace a předložit je ve vhodné formě neuronové síti. Systém je schopný s 95% přesností rozlišovat mezi legitimním a jiným provozem a zároveň s 65% přesností identifikovat nestandardní nebo útočný provoz. Neuronová síť implementovaná v detekčním systému využívá aktivační funkci ReLU.



Obr. 3.7: Detekční systém

4 Závěr

Zadáním bakalářské práce bylo navržení a realizace detekčního systému založeného na neuronových sítích, který bude na základě alespoň šesti zvolených parametrů detekovat a klasifikovat anomálie v síťové komunikaci. Dílčím cílem této bakalářské práce byla volba alespoň šesti různých typů anomálií v síťové komunikaci, které bude detekční systém schopen spolehlivě detekovat a klasifikovat.

V první teoretické kapitole byla detailně rozebrána problematika neuronových sítí od biologického neuronu až po matematický pohled na neuron umělý. V rámci kapitoly je rozebrán princip fungování neuronové sítě. Závěrem kapitoly jsou detailně popsány jednotlivé typy neuronových sítí. Druhá teoretická kapitola se zabývá rozdílem mezi legitimním, nestandardním a útočným provozem v podobě DDoS útoků. Kapitola popisuje problémy, které mohou při definici legitimního provozu nastat a zároveň uvádí možná řešení. V kapitole jsou také rozebrány jednotlivé typy útoků, principy, na kterých fungují a jejich možnou detekci.

Praktická část bakalářské práce se skládá z 5 hlavních kapitol. První kapitola popisuje 6 vhodně zvolených parametrů síťové komunikace, které představují vstupy do neuronové sítě. V druhé kapitole je rozebrán proces sběru dat. Součástí této kapitoly je podrobný popis použitých množin dat sestávajících z legitimního, nestandardního a útočného provozu. Třetí kapitola rozebírá proces zpracování dat a možné problémy, které s touto fází procesu tvorby detekčního systému souvisí. Součástí třetí kapitoly je i stanovení prahových intervalů z legitimního provozu a jejich grafické znázornění. Čtvrtá kapitola popisuje realizaci modelu neuronové sítě. V rámci této kapitoly jsou popsány parametry použité neuronové sítě a její schématické znázornění. Součástí kapitoly je i popis trénovací a testovací fáze. Pátá kapitola prezentuje a komentuje dosažené výsledky s ohledem na přesnost a rozlišovací schopnost detekčního systému.

Jako slabý článek ovlivňující přesnost detekčního systému se ukázal proces stanovování prahových hodnot. Během tohoto procesu byly stanoveny konstantní prahové intervaly, z jejichž podstaty bylo nutné zavést určitou míru tolerance. I přes všechny nedostatky byl vytvořen detekční systém schopný s 96% přesností rozlišovat mezi legitimním a jiným provozem a s 65% přesností identifikovat nestandardní a útočný provoz.

Literatura

[1] *Neuron* [online]. [cit. 2018-12-10] Dostupné z URL: <https://cs.wikipedia.org/wiki/Neuron>

[2] CHALUPNÍK, Vitalij *Biologické algoritmy (4) – Neuronové sítě* [online]. [cit. 2018-12-10] Dostupné z URL: <https://www.root.cz/clanky/biologicke-algoritmy-4-neuronove-site/>

[3] *Neuronové sítě* [online]. [cit. 12. 11. 2018]. Dostupné z URL: <https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=21471>

[4] VONDRÁK, Ivo *Umělá inteligence a neuronové sítě.* Ostrava: Vysoká škola báňská - Technická univerzita Ostrava. ISBN 80-707-8259-5. Dostupné z: <http://vondrak.cs.vsb.cz/download/Neuronove_site.pdf>

[5] MALADKAR, Kishan *6 Types of Artificial Neural Networks Currently Being Used in Machine Learning* [online]. [cit. 2018-12-10] Dostupné z URL: https://www.analyticsindiamag.com/6-types

[6] *13 Alarming Cyber Security Facts and Stats* [online]. [cit. 2018-12-10] Dostupné z URL:
<https://www.cybintsolutions.com/cyber-security-facts-stats/>

[7] HOLOVSKÝ, Martin *Seznamte se - DoS a DDoS útoky.* Dostupné z URL: https://www.security-portal.cz

[8] *What's A DDoS Attack And How Does It Work?.* Dostupné z URL: <https://www.anexio.com/whats-ddos-attack-work/>

[9] REO, Joy *What Motivates DDoS Attackers?* [online]. [cit. 2018-12-10] Dostupné z URL: https://www.corero.com/blog/690

[10] *Linode Resets Customer Passwords After Breach, DDoS Attack* [online]. [cit. 12. 11. 2018]. Dostupné z URL: <https://threatpost.com/linode-resets-customer-passwords-after-breach-ddos-attack/115790/?>

[11] *A quarter of companies would be willing to pay ransom to hackers* [online]. [cit. 12. 11. 2018]. Dostupné z URL:
https://www.novinky.cz/internet-a-pc/bezpecnost

[12] *Neustar DDoS Attack Study Quantifies Cost of Attacks* [online]. [cit. 3. 11. 2018]. Dostupné z URL: <https://www.home.neustar/about-us/news-room/press-releases/2015/ddos-attack-quantifed>

[13] PIKORA, Aleš *Útoky DDoS – kriminální ekosystém vydírání* [online]. [cit. 2018-12-10] Dostupné z URL: <https://www.itbiz.cz/clanky/utoky-ddos-kriminalni-ekosystem-vydirani2>

[14] WILES, Jack *Learn more about Flooding Attack.* Dostupné z URL: <https://www.sciencedirect.com/topics/computer-science/flooding-attack>

[15] BAŠTA, Pavel a DURAČINSKÁ Zuzana
Princip amplification útoků zneužívajících DNS, NTP a SNMP [online]. [cit. 2018-12-10] Dostupné z URL: <https://www.root.cz/clanky/princip-amplification-utoku-zneuzivajicich-dns-ntp-a-snmp/>

[16] *NTP amplification attack.* Dostupné z URL: <https://www.imperva.com/learn/application-security/ntp-amplification/>

[17] *TCP 3-Way Handshake (SYN,SYN-ACK,ACK.* Dostupné z URL: <https://www.inetdaemon.com/tutorials/internet/tcp/3-way_handshake.shtml>

[18] *TCP SYN Flood.* Dostupné z URL: <https://www.imperva.com/learn/application-security/syn-flood/>

[19] *Preventing DDoS Attacks.* Dostupné z URL: <https://www.radware.com/resources/preventing_ddos_attacks.aspx>

[20] *Christmas Tree Packet* [online]. [cit. 2018-12-10] Dostupné z URL: <https://www.techopedia.com/definition/20238/christmas-tree-packet>

[21] *Christmas Tree Attack – CompTIA Security+ SY0-401: 3.2.* Dostupné z URL: <https://www.professormesser.com/security-plus/sy0-401/christmas-tree-attack-2/>

[22] *Slowloris DDoS Attack* [online]. [cit. 2018-12-10] Dostupné z URL: <https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/>

[23] *LAND Attacks* Dostupné z URL: <https://www.imperva.com/learn/application-security/land-attacks/>

[24] CALLEGARI Christian, GIORDANO Stefano, PAGANO Michele *An Information-Theoretic Method for the Detection of Anomalies in Network Traffic.* Computers and Security Dostupné z URL: <https://ieeexplore.ieee.org/document/7876150>

[25] WANG, Yun *statistical techniques for network security: modern statistically-based intrusion detection and protection* Hershey: Information Science Reference, c2009. ISBN 978-1-59904-708-9. [cit. 2019-05-05]

[26] DILLARD, John *5 Most Important Methods For Statistical Data Analysis* [online]. [cit. 2018-12-10] Dostupné z URL: <https://www.bigskyassociates.com/blog/bid/356764/5-Most-Important-Methods-For-Statistical-Data-Analysis>

[27] MATISKO, Maroš. *NEURONOVÉ SÍTĚ PRO DETEKCI ANOMÁLIÍ V SÍŤOVÉ KOMUNIKACI.* Dostupné z URL: <https://www.vutbr.cz/studenti/zav-prace/detail/110194> Vysoké učení technické v Brně. Vedoucí práce Petr Blažek.

[28] BUKÁČ, Vít *Traffic characteristics of common DoS tools.* Dostupné z URL: <https://www.fi.muni.cz/reports/files/2014/FIMU-RS-2014-02.pdf>

[29] GARCIA, Sebastian. Malware Capture Facility Project. *SCTU-Normal-28 Dataset. Normal connections to various HTTPs sites in Alexa top 1,000. Using a Kali linux* [online]. Praha: CVUT University, 2017 [cit. 2018-12-07] Dostupné z URL: <https://mcfp.felk.cvut.cz/publicDatasets/CTU-Normal-28/>

[30] *The top 500 sites on the web* [online]. [cit. 2018-12-07] Dostupné z URL: <https://www.alexa.com/topsites>

[31] *Avalanche, Valid Testing–no Guessing.* Dostupné z URL: <https://www.spirent.com/products/avalanche>

[32] *SlowHTTPTest.* Dostupné z URL: <https://github.com/shekyan/slowhttptest>

[33] *Python Data Analysis Library.* Dostupné z URL: <https://pandas.pydata.org/>

[34] *Prahové hodnoty události pro sledování transakcí* [online]. [cit. 2019-05-05] Dostupné z URL: <https://www.ibm.com/support/knowledgecenter/cs/SSMKFH/com.ibm.apmaas.doc/wrt_tt/wrt_ui/wrtui_thresholds.htm>

[35] *Neural network models (supervised)* [online]. [cit. 2019-05-05] Dostupné z URL: <https://scikit-learn.org>

[36] LUNTER, Lubos *Dynamic Baselining and Adaptive Threshold in DDoS Defender* [online]. [cit. 2019-05-05] Dostupné z URL: <https://www.flowmon.com/en/blog/dynamic-baselining-and-adaptive-threshold-in-ddos>

[37] MINAŘÍK, Pavel. *Monitorování datových toků vs. paketová analýza* [online]. [cit. 2018-12-10] Dostupné z URL: <https://www.systemonline.cz/it-security/monitorovani-datovych-toku-vs.-paketova-analyza.htm>

[38] MINAŘÍK, Pavel. *Není monitoring jako monitoring* [online]. [cit. 2018-12-10] Dostupné z URL: <https://www.systemonline.cz/it-security/pokrocila-analyza-provozu-datovych-siti.htm>

[39] MINAŘÍK, Pavel. *Záznam provozu na síti a paketová analýza* [online]. [cit. 2018-12-10] Dostupné z URL: <https://www.systemonline.cz/it-security/pokrocila-analyza-provozu-datovych-siti-2-dil.htm>

[40] *Koncept umělé neuronové sítě* [online]. [cit. 2018-12-10] Dostupné z URL: http://portal.matematickabiologie.cz

[41] ROUSE, Margaret *distributed denial of service (DDoS) attack* [online]. [cit. 2018-12-10] Dostupné z URL: <https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack>

[42] *NTP Amplification* [online]. [cit. 2018-12-10] Dostupné z URL: <https://www.incapsula.com/ddos/attack-glossary/ntp-amplification.html>

[43] *Common DDoS Attack Types* [online]. [cit. 2018-12-10] Dostupné z URL: <https://www.corero.com/resources/glossary.html>

Seznam symbolů, veličin a zkratek

TCP	Transmission Control Protocol – spojově orientovaný protokol transportní vrstvy ISO/OSI modelu
UDP	User Datagram Protocol – nespojově orientovaný protokol transportní vrstvy ISO/OSI modelu
ACK	Acknowledgment – potvrzovací příznak v hlavičce TCP paketu
FIN	Finalize – příznak ukončení spojení v hlavičce TCP paketu
DNS	Domain name system – hierarchický systém doménových názvů
RST	Reset – příznak TCP segmentu, který oznamuje příjemcovi resetování komunikace
SYN	Synchronize – synchronizační příznak v hlavičce TCP paketu zahajující spojení
ISO/OSI	Open Systems Interconnections – referenční model komunikace vytvořený organizací ISO
NS	Neuronová síť
IP	Internet protocol – protokol používaný ke směrování paketů v síti
DDoS	Distributed Denial of Service – distribuovaný útok za účelem znemožnění přístupu k poskytované službě
CSV	Comma seperated values – textový formát, který používá čárku jako oddělovač hodnot v rámci jednoho záznamu
PCAP	Packet capturing – datové soubory obsahující záznam komunikace v síti
HTTP	HyperText Transfer Protocol – protokol aplikační vrstvy ISO/OSI modelu sloužící k výměně hypertextových dokumentů
NTP	Network Time Protocol – protokol sloužící k synchronizaci času v síti
RNN	Recurrent Neural Network – rekurentní neuronové sítě
MNNs	Modular Neural Network – modulární neuronové sítě
CNN	Convolutional Neural Network – konvoluční neuronové sítě
MLP	Multilayer Percepton – vícevrstvý percepton
URG	Urgent – příznak v hlavičce TCP segmentu
PSH	Push – příznak v hlavičce TCP segmentu
HW	Hardware – fyzická část počítače
SW	Software

Seznam příloh

A Obsah přiloženého CD

- `/` ..... kořenový adresář přiloženého CD
  - `DetekceAnomaliiPomociNS.pdf` ..... elektronická verze práce ve formátu PDF
  - `README.txt` ..... návod k použití
  - `dataPreparation.py` ..... skript pro zpracování dat
  - `threshold.py` ..... skript pro určení prahových intervalů
  - `markUp.py` ..... skript pro označkování dat
  - `neuralNetwork.py` ..... skript implementující neuronovou síť
  - `links.txt` ..... odkazy pro stažení provozu síťové komunikace
  - `trafficForThreshold` ..... adresář s provozem pro stanovení prahových intervalů
  - `testingTraffic` ..... adresář pro data testovacího provozu
  - `trainingTraffic` ..... adresář pro data trénovacího provozu
  - `.idea`
  - `venv`
    - `Include`
    - `Lib`
      - `tcl8.6`
      - `site-packages` ..... adresář obsahující použité knihovny
    - `Scripts` ..... adresář obsahující podpůrné moduly jazyka Python
    - `pip-selfcheck.json`
    - `pyvenv.cfg` ..... konfigurační soubor adresáře venv