# Využitie neurónovej siete pri riadení systému zabezpečenia výpočtovej techniky

# Assimilation of neural networks in controlling of the computer safety system

*Igor Halenár,ÚIAM MTF STU*

*Martin Juhás,ÚIAM MTF STU*

**Abstract:** A computer network have to be protected from attacks from internet. This protection can by done by special computer systems, known as firewalls. These firewalls can be based on a classical filtering of packets, depending on a classical boolean rulebase, or we can make advanced, dynamic, firewalls. These can be improved with some commponents for reaction to attacks, dynamic behaviour of systems and some heuristic components. These are presented with some type of a neural network.

**Key words:** network, neural network, safety, system

**Abstrakt:** V súčasnej dobe je čím ďalej potrebnejšie venovať sa k zabezpečeniu výpočtových systémov pred rôznymi typmi útokov z internetu. Túto činnosť zabezpečujú špecializované výpočtové systémy, známe ako firewall-y. Môžu byť buď klasické, kde sa jedná vlastne o paketový statický filter založený na pevnej báze pravidiel s booleanovskou matematikou, alebo o dynamický systém. Tieto môžu byť vylepšené rôznymi modulmi, prípadne neurónovými sieťami, ktoré umožňujú rôzne reakcie systému na útoky.

**Kľúčové slová:** systém, sieť, neurónová sieť, bezpečnosť

## 1. Neurónové siete pri riadení systému zabezpečenia výpočtovej techniky

Tradičné počítače zaisťujúce bezpečnosť počítačových sietí, a následne bezpečnosť výpočtových systémov (firewall-y) sú založené na viac alebo menej komplexných súboroch bezpečnostných pravidiel. Údaje , ktoré vstupujú do takéhoto systému sú spracovávané ako vstup a výstup na základe jedného alebo viac pravidiel v báze pravidiel. Báza pravidiel je štruktúrovaná ako súbor sekvenčne zoradených logických operátorov (Boolean). V prípade ,

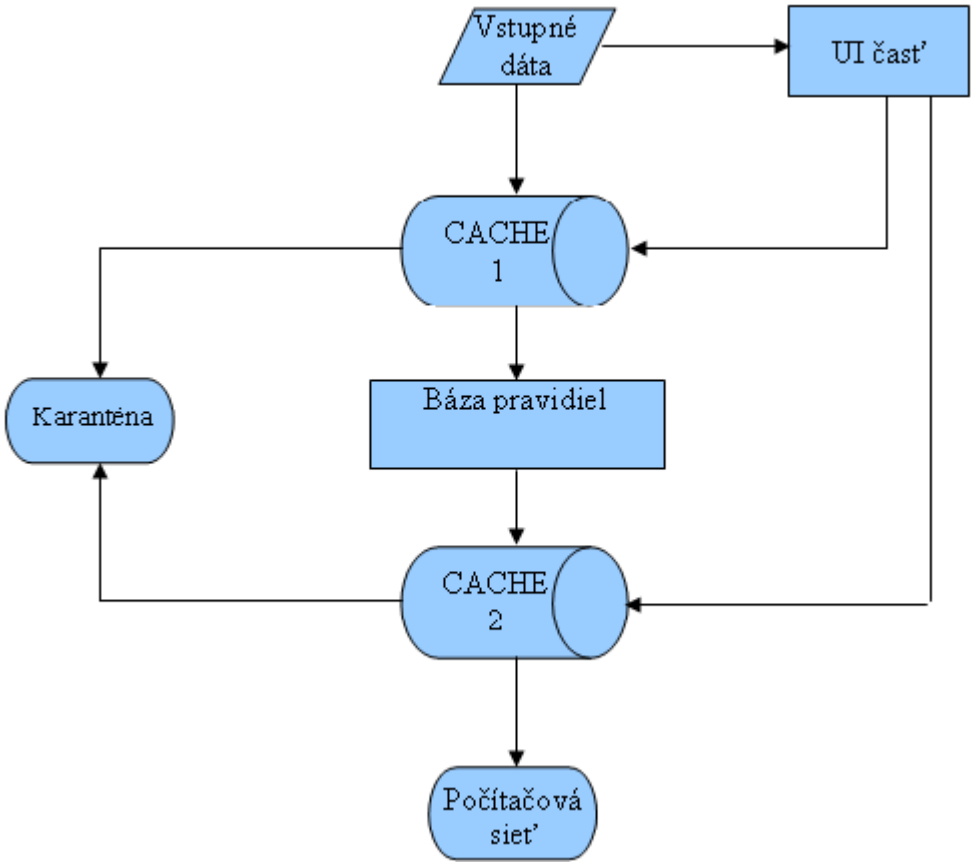
že sa báza pravidiel stáva väčšou, komplexnejšou, prirodzene vyžaduje väčší procesorový výkon a viac systémových zdrojov. Riešením v praxi zvyčajne býva, že súbor pravidiel je kompromisom medzi snahou komplexne pokryť pravidlami všetky možné stavy firewall-u a požadovanou získanou dátovou priepustnosťou. Teda zvyčajne obetujeme bezpečnosť v záujme vyššej priepustnosti.

Je popri tom potrebný častý zásah obslužného personálu pri spravovaní, resp. úpravách bázy pravidiel, a samozrejme aj najrozsiahlejšia báza pravidiel funguje na rovnakom, lineárnom spôsobe spracovania ako tá najjednoduchšia. Navyše, okrem rôznych obmedzeniach platných pri všetkých klasických systémoch, ako sú obmedzená kapacita úložného priestoru, obmedzenia možností logickej matematiky a potreba vysokého výpočtového výkonu pri veľmi veľkých bázach pravidiel, pri klasických firewall-och ide stále o v podstate statické systémy, ktorých úroveň zabezpečenia zodpovedá v priamej úmere schopnostiam a znalostiam operátora. Keďže ide o statické firewall-y, tak nie je možná ich automatická adaptácia a učenie sa z dátových tokov, ktoré prechádzajú počítačovou sieťou. A následne, tieto systémy neumožňujú vykonávať porovnávania a analýzu dátových tokov a odolávať tak nástrahám a bezpečnostným hrozbám, prípadne zjednodušovať prácu administrátorov.

Preto je žiadúce venovať určité zdroje a prostriedky na vývoj zariadení, ktoré môžeme nazvať firewall s umelou inteligenciou. Takéto zariadenie je vlastne spojením funkčnej neurónovej siete a klasického firewall-u. Systém je potom schopný učenia sa z tokov dát, ktoré ním prechádzajú, prípadne je schopný sa adaptovať na zmenené vstupné podmienky, a následne tým lepšie zabezpečuje bezpečnostné požiadavky. Prípadne by bolo dobré zahrnúť do vývoja metódy inteligentného bezpečnostného systému aj požiadavku kombinácie rôznych metód analýzy rizík, čím sa dosiahne vyšší stupeň funkcionality a bezpečnosti, ako pri klasických firewall-och. S využitím neurónových sietí pri návrhun takéhoto systému je možné vytvoriť samostatný inteligentný zabezpečovací sieťový systém – inteligentný firewall, v ktorom sú obsiahnuté znalosti o možných bezpečnostných rizikách a hrozbách v počítačovej sieti, a je schopný sa dynamicky adaptovať na možné napadnutia systému, ako sú exploity, analýza out of band komunikácie a analýza skrytých komunikačných kanálov.

Vo svete existuje viacero návrhov a riešení uvedenej problematiky. Nasledovné riešenie predstavuje sieťový firewall , ktorý spracováva dátové pakety počítačovej komunikácia v nasledovných krokoch. Prvý krokom je analýza dátového toku jedným heuristickým systémom, neurónovou sieťou nakonfigurovaným na rozpoznávanie potenciálne

nebezpečných a škodlivých paketov. V priebehu spracovania sa pridelí dátovému paketu stavový príznak dôveryhodnosti , ktorého úroveň závisí od stupňa škodlivosť paketu v analyzovanom dátovom toku. Firewall s takouto heuristickou analýzou dátových tokov by , pri optimálnej funkcii, mal odstraňovať nedostatky klasických firewall-ov a mal by byť schopný adaptácie na zmenené vstupné podmienky pri počítačovej komunikácií.




Obrázok, resp. bloková schéma, predstavuje základný návrh vnútornej konštrukcia a usporiadania expertného systému, ktorý obsahuje všetky vyššie v texte uvedené časti. Súčasťou takéhoto systému je jednak klasická báza pravidiel, kde sa rozhodovanie o škodlivosti, prípadne neškodnosti dátových paketov vykonáva prostredníctvom klasickej bázy rozhodovacích pravidiel, aké poznáme z klasických stavových firewall-ov. Za druhé je prítomná časť nazvaná „UI časť“, ktorá poskytuje systému väčšie možnosti rozpoznávania potenciálnej nebezpečnosti paketov v dátových tokoch. Predstavuje nejakú, momentálne bližšie nešpecifikovanú neurónovú sieť, natrénovanú na rozpoznávanie potenciálne nebezpečných paketov. Celé takéto zapojenie predstavuje riešenie, v podstate ide o expertný systém, ktoré je schopné veľmi efektívne filtrovať komunikáciu v počítačovej sieti.

Dôležitým prvkom v tomto type firewall-u je neurónová sieť. Môžeme , podľa predchádzajúcich praktických pokusov a s odvolaním na použité zdroje, ako najvhodnejšiu pre tento model definovať neurónovú sieť s metódou spätného šírenia chyby, s dvomi skrytými vrstvami ,s klasickou sigmoidálnou prenosovou funkciou.

Vstupmi siete môžu byť napríklad veľkosť paketu, zdrojová sieť paketu, cieľ paketu, kombinácie zdrojová adresa + zdrojový port, cieľová adresa + cieľový port, TTL (time-to live) paketu a podobne. Výstupom z neurónovej siete môže byť nastavený príznak hodnotenia pre určený dátový paket. Hodnotenie môže byť jednoduché, napríklad môžeme rozdeliť pakety do kategórií podľa škodlivosti - kategórie 1,2,3,4, kde čím vyššie číslo, tým vyššia dôvera v neškodnosť paketu. Kategórie môžeme, kvôli ďalšiemu popisu, slovne odstupňovať napríklad pojmami nebezpečný, menej bezpečný, viac bezpečný a bezpečný.

Postup spracovania dát horeuvedeným modelom je nasledovný. Vstupné dáta, ktoré sú prakticky „surové dáta“ prichádzajúce priamo z nejakého externého zdroja (internetu), sú po príchode pozdržané v zásobníku dát (cache 1), v ktorom sú pozdržané dovtedy, kým je k dispozícii rozhodnutie neurónovej časti firewall-u. V prípade že UI časť dospeje k nejakému hodnoteniu paketu, dáta sú zo zásobníka (cache 1) odovzdané na ďalšie spracovanie. UI časť je nakonfigurovaná na rôzne stupne hodnotenia nebezpečnosti paketu. V prípade, že sú prechádzajúce pakety označené ako „vysoko dôveryhodné“ , prípadne „ dosť dôveryhodné“ , sú preposlané zo zásobníka (cache 1) na spracovanie klasickou časťou systému. Spracovanie prevezme rozhodovacia logika klasického firewall-u, na základe „bázy pravidiel“. Označenie dôveryhodnosti paketov je samozrejme vykonávané na základe rôznych kritérií , ako sú validita, autorizované pakety, pakety pochádzajúce zo zabezpečených sietí a podobne. Je možné , v prípade jednoznačného označenia paketu ako dôveryhodný, môžeme dokonca v rámci urýchlenia celého procesu filtrovania prepustiť paket priamo do výstupného zásobníka dát (cache 2).

Ak nie je možné jednoznačne určiť paket ako bezpečný, priraďuje UI časť hodnotenie nižšej bezpečnosti, prípadne sú vyhodnotené ako nebezpečné. Pakety s nižším ohodnotením sa odovzdávajú tiež na spracovanie klasickej časti firewall-u, prípadne môžu byť spracovávané nejakou rozšírenejšiu, komplexnejšou, bázou pravidiel. Dátové pakety vyhodnotené ako škodlivé sa nespracovávajú, ale sa priamo odkladajú do skladu zlých paketov (sklad). Tu je možné s paketmi vykonávať rôzne operácie. Môžeme pakety podržať v archíve na neurčitú dobu, môžeme ich vymazať, prípadne môže byť súčasťou toho skladu nejaký simulačný stroj, v ktorom nasimulujeme virtuálnu počítačovú sieť a preveríme obsah a funkčnosť týchto

paketov. V prípade takejto simulácie je potom možné zistiť , čo bolo predmetom útoku a z toho extrahovať potrebné informácie pre lepšiu funkciu celého systému.

Po odsúhlasení paketov klasickou firewall-ovou časťou na základe bázy pravidiel, sú vyfiltrované pakety, označené ako vhodné, odovzdané do posledného zásobníka (cache 2 ), odkiaľ sú odovzdané priamo na výstup, napríklad lokálna počítačová sieť.

Takúto schému systému na zabezpečenie počítačovej siete je možné doplniť ďalšími procesmi na spracovanie a vyhodnocovanie dátových tokov. Napríklad je možné pridať ďalšie neurónové siete, ktoré budú vyhodnocovať dátové toky transformované na frekvenčnú doménu (frequency domain, furrierova transformácia).

Všeobecne je možné zhrnúť požadované vlastnosti takého firewall-u do nasledovných bodov:

- analyzovanie dátového toku použitím minimálne jednej UI časti , resp. neurónovej siete, natrénovanej reagovať na vstupy s časopriestorovou nezávislosťou, s označením hodnotenia dôveryhodnosti paketov v analyzovanom toku dát a výberom paketov pre ďalšiu analýzu na základe označeného stupňa dôveryhodnosti.
- výberom paketov pre ďalšiu analýzu na základe označeného stupňa nebezpečnosti
- vypustenie paketov označených ako vysoko dôveryhodné, a následnú ďalšiu analýzu paketov s nižším stupňom bezpečnosti
- rozpoznávanie paketov s príznakom určitej abnormality v dátových (paketových) tokoch
- rozpoznanie takých paketov, ktoré patria aspoň do jednej zo skupín pozostávajúcich z paketov :
    - obsahujúcich príznaky nejakého útoku
    - obsahujúce určité náznaky periodicity
    - pakety zmenené pri prenose
    - príznaky stratených paketov
    - out of band komunikácia (zdanlivo nič neznamenajúce dáta)
    - covert channel komunikácia (skrytý komunikačný kanál)

- odovzdanie paketov, analyzovaných a určených ako škodlivé, simulátoru počítačovej siete, resp. karantény
- vykonať ďalšiu analýzu menej dôveryhodných paketov pravidlami z databázy pravidiel

Samozrejme, vo svete existuje množstvo riešení tejto problematiky. Filtrovanie dát a paketov je možné rozšíriť o ďalšie neurónové siete, zamerané na rôzne iné techniky sledovania prebiehajúcich dátových tokov. Príkladom je transformácia dátového toku na frekvenčnej analýzy, kde je možné lepšie diagnostikovať metódu prenosu dát, známu ako „covert channel“. V takomto zobrazení dátového toku je možné, po určitej úprave, rozpoznávať známe kódy využívane pri podobných skrytých prenosových kanáloch. Príkladom môže byť Morseova abeceda, alebo Cézarova šifra. Uvedený model je možné následne rozšíriť o ďalšie moduly, teda neurónové siete, natrénované na rozpoznávanie takýchto obrazcov v komunikačnom kanáli.

## 2. Zoznam bibliografických odkazov


(1) Hakl F., Holeňa M.: Úvod do teorie neurónových sítí, ČVUT Praha, 1997

(2) Sinčák P., Andrejková G.: Neurónové siete Inžiniersky prístup, Technická univerzita Košice, 1996

(3) Dostálek L. a kol.: Velký pruvodce protokoly TCP/IP: Bezpečnost, Computer Press, 2003


## 3. Adresa autora (-ov):


Igor Halenár, Ing.
ÚIAM MTF STU
Hajdócyho 1
917 01 Trnava
igor.halenar@stuba.sk

Martin Juhás, Ing.
ÚIAM MTF STU
Hajdócyho 1
917 01 Trnava
martin.juhas@stuba.sk