# Analýza ML metód a algoritmov pre detekciu sieťových anomálií

Projekt INNOvative SOC/INNOSOC

# Obsah

Úvod ..... 3
Analýza DoS A DDoS útokov ..... 4
DoS (Denial of Service) ..... 4
DDoS (Distributed Denial of Service) ..... 5
Analýza štatistických parametrov na vybraných DDoS útokoch ..... 6
Variabilnosť, šikmosť a špicatosť ..... 8
Detekčné hodnoty pre autokoreláciu a regresiu ..... 12
Reakcia divergencie na DDoS útok ..... 14
Využitie 3σ-Tunela pre rozpoznanie DDOS útokov ..... 15
Detekčné funkcie pre strojové rozpoznanie DDoS útokov ..... 17
Záver ..... 20

# Úvod

Detekcia behaviorálnych anomálií v počítačových systémoch je nevyhnutným krokom v mnohých obranných mechanizmoch.

Hlavným cieľom detekcie anomálií (AD) je naučiť sa normálne správanie systému počas určitého časového obdobia a potom označiť akúkoľvek aktivitu, ktorá sa od tohto naučeného správania odchyľuje. V mnohých prípadoch si učenie sa normálneho správania vyžaduje monitorovanie a zaznamenávanie všetkých aktivít vykonávaných v systéme, aby sa extrahoval vzorec alebo profil pre každého používateľa/aplikáciu.

Vďaka svojej širokej použiteľnosti sa detektory anomálií úspešne používajú v mnohých oblastiach, ako sú napríklad správa siete alebo operačné systémy.

Detektory anomálií sa zvyčajne skladajú z dvoch modulov, ktorými sú *dátový kolektor* a *dátový analyzátor*. Prvý modul je modul, ktorý zhromažďuje protokoly/logy z monitorovaného systému, zatiaľ čo úlohou druhého modulu je analyzovať zhromaždené protokoly. V závislosti od umiestnenia dátového kolektora existujú dva typy detektorov anomálií: sieťové (network-based) a hostiteľské (host-based). Tieto dva typy detektorov generujú rôzne typy protokolov a preto sa príznaky používané na detekciu anomálií líšia v závislosti od umiestnenia detektorov.

Nad zhromaždenými logmi daný dátový analyzátor vykonáva detekciu anomálií, pričom na túto úlohu sa používajú rôzne druhy metód, ktoré možno všeobecne rozdeliť do kategórií učenie s dohľadom, učenie s čiastočným dohľadom a učenie bez dohľadu. Viac informácií možno nájsť v dokumente V7 Výsledok analýzy vhodných algoritmov.docx. V rámci každej kategórie existuje množstvo rôznych použiteľných algoritmov. Okrem toho sú parametre/príznaky (features), ktoré je možné použiť pre AD, rôznorodé v závislosti od typov logov. Napríklad, zo sieťových paketov môže detektor použiť ako príznaky čas príchodu medzi paketmi alebo počet paketov v jednom smere. Z logov hostiteľa (host logs) môže detektor použiť vyťaženie CPU/pamäte. Príznaky sa taktiež môžu líšiť v závislosti od konkrétnej hrozby, proti ktorej je detektor anomálií nasadený. Napríklad detektor anomálií na detekciu ransomware používa parametre, ktoré sa líšia od parametrov používaných detektorom anomálií na detekciu cryptojacking.

Pri nasadzovaní systémov AD existuje niekoľko výziev. Hlavnou výzvou je, ako získať normálne vzorce správania sa. Je ťažké jednoznačne definovať, čo je to „normálne správanie“ a preto je zhromažďovanie takýchto údajov náročné. Ďalšou výzvou je, že detektor môže trpieť vysokým počtom falošne pozitívnych (false positive) výsledkov a teda vyvolať varovné hlásenie pre akýkoľvek neočakávaný vzor správania sa siete.

Neočakávané vzory bohužiaľ nemusia vždy znamenať, že došlo k narušeniu. Presnejšie povedané, môže existovať veľa neočakávaných normálnych vzorcov správania sa, napríklad v dôsledku preťaženia sietí alebo prekážok či problémov v systémoch. Preto je

zníženie počtu falošne pozitívnych výsledkov kľúčové pre úspešné nasadenie systémov AD.

# Analýza DoS A DDoS útokov

Techniky DoS (angl. Denial of Service) a DDoS (angl. Distributed Denial of Service) sa vyskytujú pri rôznych typoch napadnutia bezpečnosti v IP sieti a pri incidentoch na rôznych úrovniach siete (vid predchádzajúca kapitola).

## DoS (Denial of Service)

Skratka DoS v preklade znamená útok odmietnutia nejakej služby. Tento typ útoku sa používa na zahltenie servera. V tomto prípade útočník využíva zariadenie, ktorým sa pokúša narušiť normálnu prevádzku cieľového servera, služby alebo siete. Veľmi rýchlo sa stali hrozbou kybernetickej bezpečnosti. Sú jednoduché avšak ich dopad môže byť pre jedincov ale aj spoločnosti devastujúci.

DoS útoky sa často používajú pre vypnutie zariadení a sietí a existuje veľa rôznych spôsobov využitia spomínaných DoS útokov. Patria sem napr.:

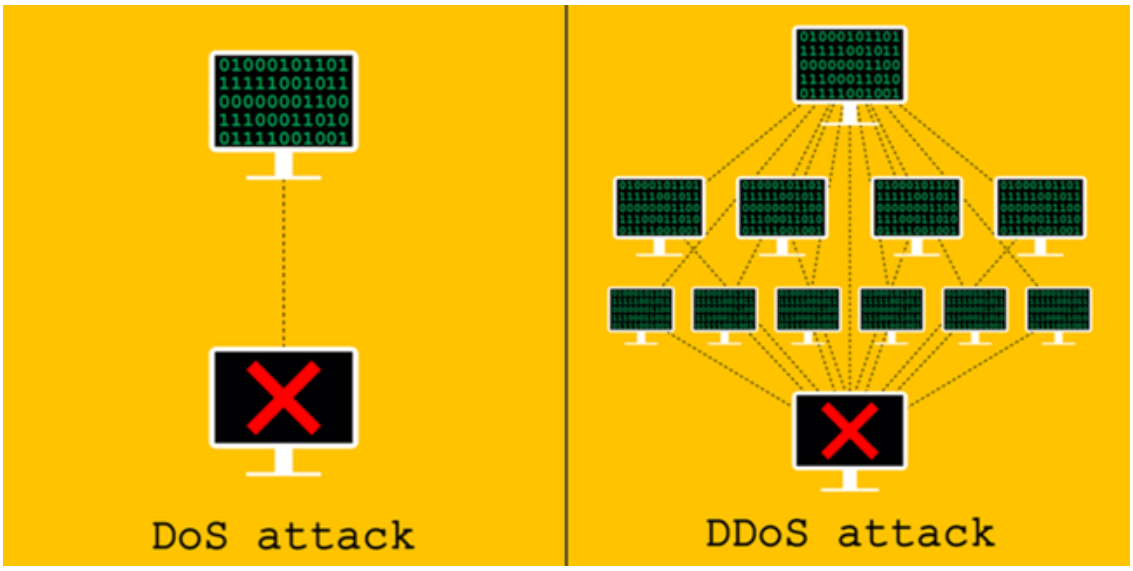
- **Pretečenie vyrovnávacej pamäte** (angl. buffer overflow): Vyrovnávacia pamäť je dočasné úložisko pre ukladanie dát. Ak program alebo systémový proces umiestni viac údajov ako bolo vopred určené, ďalšie údaje potom pretečú a môže sa stať, že niektoré z nich potom uniknú do iných vyrovnávacích pamätí. To má potom za následok poškodenie alebo prepísanie ďalších údajov. Útočník dokáže na základe tohto princípu poškodiť súbory, zmeniť alebo odhaliť rôzne informácie.
- **ICMP útok** (angl. ICMP attack alebo Ping of Death): Tento typ útoku využíva ICMP protokol pričom sa využívajú ICMP echo-requesty tzv. pingy. Všeobecne sa echo-requesty a echo-reply používajú na ping sieťového zariadenia s cieľom overiť konektivitu medzi zariadením a odosielateľom. Ak by útočník zahltil cieľ paketmi požiadaviek, sieť musí odpovedať rovnakým počtom paketov, čo spôsobí nedostupnosť zariadenia pre iné prichádzajúce požiadavky.
- **UDP útok** (angl. UDP attack): Útok je založený na posielaní UDP paketov so zdrojovou IP adresou, ktorú môže útočník sfalšovať a snahou je zahltiť náhodné porty na cieľovom servery. Výhodou UDP protokolu je, že nepotrebuje nadviazať spojenie, ako to je v prípade protokolu TCP. V prípade, že cieľový server príjme UDP paket na porte, ktorý nie je využívaný žiadnou aplikáciou, informuje o tom odosielateľa. Pokiaľ útočník odošle dostatočné množstvo paketov na takýto port, môže byť preťažený.
- **SYN útok** (angl. SYN flood): Toto je útok, ktorý vzniká pri vytváraní TCP spojenia medzi 2 zariadeniami. TCP využíva trojfázové potrasenie rúk (angl. 3-way handshake). Nadviazanie spojenia začína odoslaním správy SYN. Ak je server aktívny odošle sa SYN/ACK správa späť ku klientovi, ktorí chcel nadviazať

spojenie. Server sa snaží odpovedať dokým nevyprší čas na nadviazanie komunikácie, pričom si údaje uchováva v pamäti. Ak je klientom útočník s falošnou a nedostupnou zdrojovou adresou, zaslanie veľkého množstva takýchto paketov môže spôsobiť vyčerpanie pamäte, ktorá je určená pre TCP spojenia a všetky ďalšie pokusy o komunikáciu budú ďalej ignorované.

- **Útok slzy** (angl. Teardrop attack): Počas tohto útoku sa útočník snaží posielať fragmentované pakety a sieť sa potom snaží skompilovať tieto dáta do ich pôvodného stavu. Útočník môže využiť zraniteľnosť zastaraného operačného systému. Je bežné, že mnohé spoločnosti stále využívajú staršie verzie systémov z dôvodu opätovného spúšťania starej aplikácie a keďže niektoré verzie operačných systémov ako sú napr.: Linux či Windows obsahujú chybu pri spätnom zostavení fragmentovaného paketu, server môže byť práve kvôli tejto zraniteľnosti napadnutý.

## DDoS (Distributed Denial of Service)

Na rozdiel od jednoduchého DoS útoku, DDoS útok (Distributed Denial of Service) naberá na sile, pretože útočník využíva viacero systémov naraz a zvyšuje tak závažnosť cielených útokov. Útočník môže použiť malware, ktorý odošle po sieti do zariadení so zámerom ich infikovať. Stanú sa tak súčasťou tzv. botnetu a podľa príkazov útočníka pomocou riadiaceho servera títo boti potom jednotne útočia na cielený server. DDoS útoky je veľmi ťažké odhaliť, pretože útočiaci boti môžu byť rozmiestnený na rôznych miestach po svete. Hlavný a kľúčový rozdiel medzi DoS a DDoS útokom je, že pri DDoS s použitím botov môže útočník posielať obrovské objemy prevádzky.




*Obr. 1: DoS a DDos útoky*

DDoS útoky sa rozdeľujú do 3 hlavných kategórií:

1. Objemový útok (angl. Volumetric attack): Tento typ využíva zraniteľné služby ako sú napr.: NTP, DNS či SSDP. Útočník sa snaží zahltiť cieľ veľkým objemom paketov, na ktoré sa cieľ snaží odpovedať, až kým nedôjde ku kolapsu na strane cielenej sieťovej infraštruktúry. Zvyčajne to je širokopásmový útok, ktorý dokáže presiahnuť 100 GB či dokonca niekoľko TB za sekundu a je okamžite očividný pre poskytovateľov pripojenia. Na detekciu objemových útokov sa osvedčilo monitorovanie siete, analyzovanie toku a prietoková telemetrická analýza.
2. Protokolový útok (angl. Protocol attack): Tento typ útoku sa snaží vyčerpať zdroje servera alebo jeho systémov a spolieha sa na zraniteľnosti internetových komunikačných protokolov. Medzi protokolové útoky patria napr.: SYN útok, UDP útok, ICMP útok. Tieto útoky sa považujú za dostatočne ochromujúce na cielenú infraštruktúru vďaka frekvencii trvania. V roku 2018 útočníci využili BGP protokol na presmerovanie prevádzky, ktorá bola určená pre službu „MyEtherWallet“, čo však bola iba zásterka pre krádež kryptomenových peňaženiek. Trvalo to približne 2 hodiny.
3. Útok na aplikačnú vrstvu (angl. Application layer attack): Tento útok sa zameriava na konkrétnu aplikáciu a jej zraniteľnosti, aby nebola schopná spracovávať, odosielať či prijímať dáta. Útoky sú slabé a pomalé a sústreďujú sa na požiadavky GET a POST. Cieľom je potom ochromiť webový server a meria sa v požiadavkách za sekundu (angl. Requests per second - Rps). Sú nízke a slabé preto, aby boli v súlade s protokolom.

Existuje niekoľko znakov, ktoré nám dokážu pomôcť pri odhalení, či je naša sieť alebo aplikácia alebo celá infraštruktúra pod DDoS útokom. Môže to byť náhly nárast webovej aktivity na serveri, znížený výkon siete alebo náhla neschopnosť komunikovať s aplikáciou.

## Analýza štatistických parametrov na vybraných DDoS útokoch

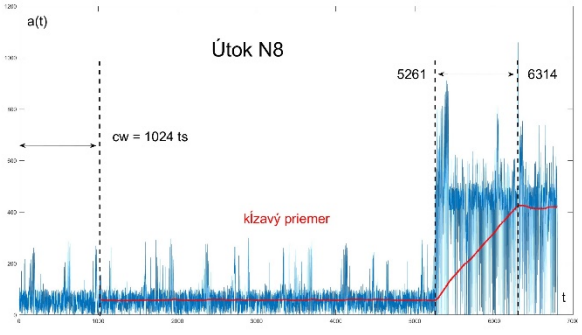
Na rôznych záznamoch DDoS útokov budeme prezentovať reakciu vybraných štatistických parametrov. Vynechali sme množstvo experimentov, ktoré sme realizovali na rôznych simulovaných scenároch. Na týchto scenároch vybrané štatistické parameter fungovali „vzorovo“ a my sme nadobudli prvotnú predstavu o efektívnosti použitia jednotlivých parametrov pri rozpoznaní zmeny a nárastu simulovanej prevádzky. Pri nasadení na rozpoznanie reálneho útoku reakcie štatistických parametrov už neboli také jednoznačné. Pre prezentovanie sme vybrali osem rôznych záznamov DDoS útokov.

Prvé štyri záznamy predstavujú štandardné DDoS útoky (N-normal), pri ktorých sa parametre chovajú obdobne ako ma simulovaných dátach. Ďalšie dva záznamy predstavujú na prvý pohľad tiež štandardné útoky, avšak parametre sa pri nich chovajú podstatne odlišným neurčitým spôsobom (S-special). V poradí siedmy záznam je zástupcom tzv. Low Rate (LR) DDoS útokov, čiže útokov s nízkou priemernou intenzitou toku. Posledný záznam je útok, ktorý sa podľa nášho názoru nedá detegovať uvedenými

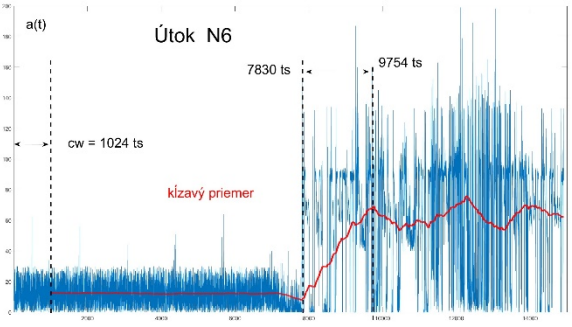
štatistickými parametrami (P-ako problém). Pri záznamoch sme zároveň s počtom prírastkov paketov a(t) zobrazili aj ich kĺzavý priemer m(t) s výpočtovým oknom cw = 1024 ts.

Záznamy sú navzorkované do daných časových okien (ts-time slot), väčšinou ts = 1ms. Pre postupný výpočet parametrov sme použili posun tzv. výpočtového okna (cw – compute window) o jeden ts. Pri prevádzaní experimentov sme pre veľkosti výpočtových okien kvôli odhadu Hurstovho exponentu použili rôzne mocniny dvojky (256,512,1024,2048,4096). Po subjektívnom hodnotení priebehu hodnôt skúmaných parametrov sme sa rozhodli ďalej zaoberať hlavne s výpočtovým oknom o veľkosti cw = 1024 ts. Pri cw = 512 ts dochádzalo k významnému „rozvlneniu“ niektorých parametroch, pri cw = 2048 sa významne zväčšila doba výpočtu parametrov, hlavne Hurstovho exponentu.

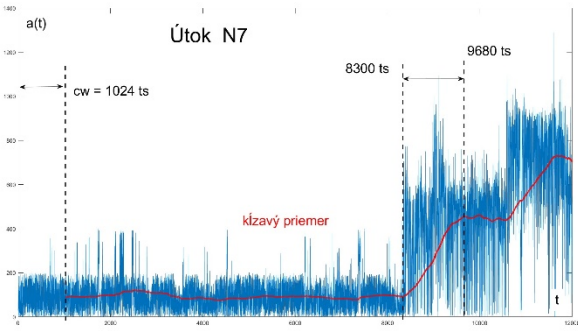
Na grafoch záznamov DDoS útokov sme zobrazili aj priebeh kĺzavého priemeru a zobrazili časový interval, v ktorom kĺzavý priemer m(t) nadobudol od začiatku útoku svoje lokálne maximum. Tento interval využijeme pri subjektívnom hodnotení ostatných štatistických koeficientov. Na všetkých záznamoch DDoS útokov môžeme pozorovať lineárny rast kĺzavého priemeru. Hľadáme koeficienty, ktorým pri začiatku útoku začnú rásť hodnoty rýchlejšie než lineárne.



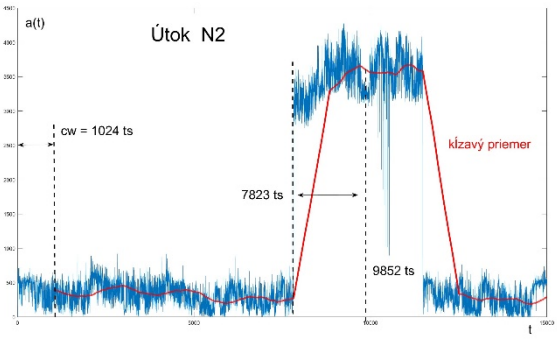

*Obr. 2: Útok N8 a kĺzavý priemer*



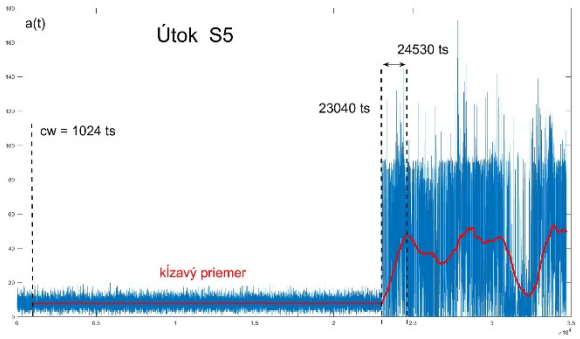

*Obr. 3: Útok N6 a kĺzavý priemer*



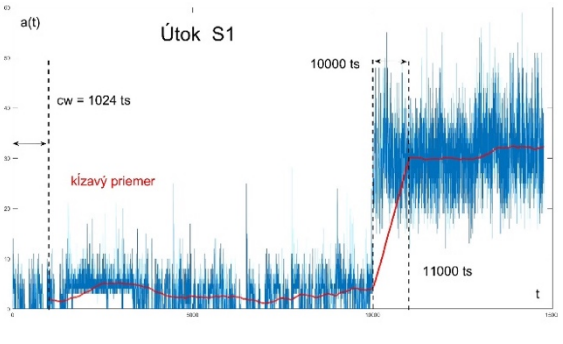

*Obr. 4: Útok N7 a kĺzavý priemer*



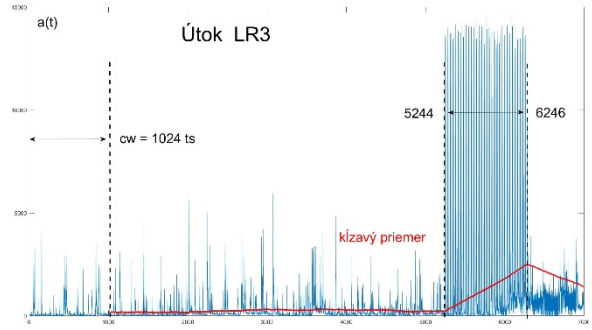

*Obr. 5: Útok N2 a kĺzavý priemer*



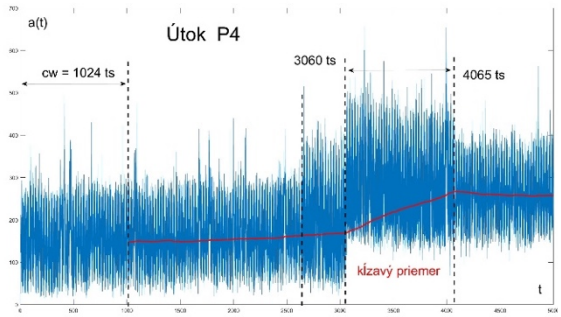

*Obr. 6: Útok S5 a kĺzavý priemer*




*Obr. 7: Útok S1 a kĺzavý priemer*



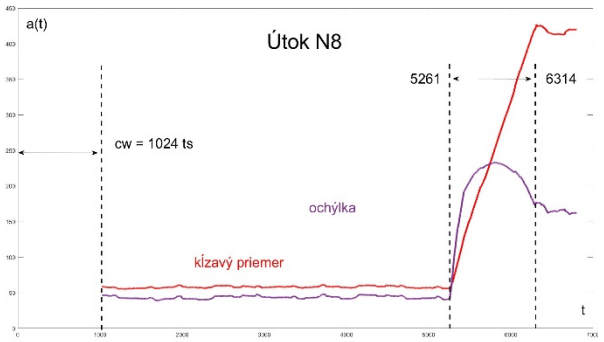

*Obr. 8: Útok LR3 a kĺzavý priemer*



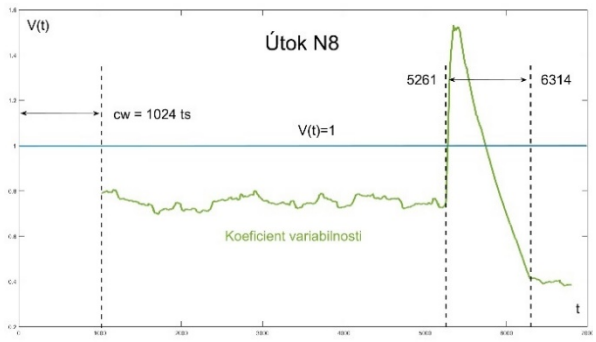

*Obr. 9: Útok P4 a kĺzavý priemer*

## Variabilnosť, šikmosť a špicatosť

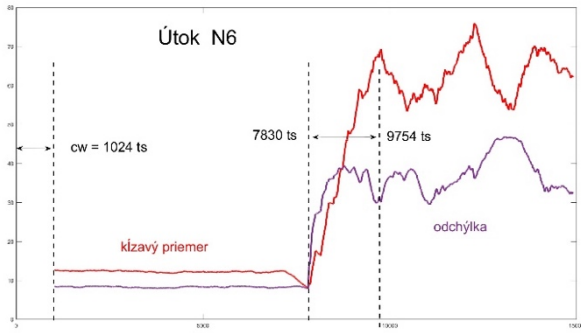
Ako prvými sa budeme zaoberať základnými štatistickými momentami, resp. koeficientami variabilnosti V(t), šikmosti K(t) a špicatosti Skw(t). Koeficient variabilnosti predstavuje podiel smerodajnej odchýlky a strednej hodnoty prírastkov v danom časovom okne cw. Variabilnosť vyjadruje mieru rozptylu prírastkov a(i) okolo strednej hodnoty. V prvom grafe zobrazíme priebeh kĺzavého priemeru a smerodajnej odchýlky, na druhom grafe sú hodnoty koeficientu variabilnosti:



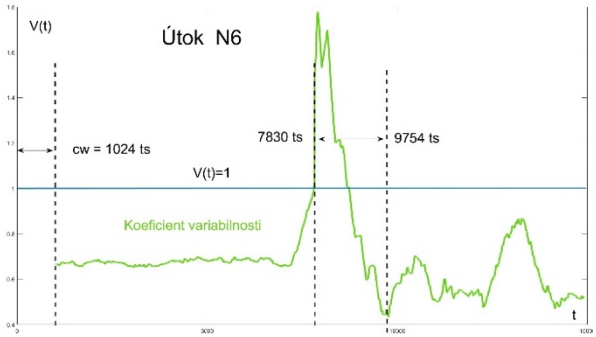

*Obr. 10: Útok N8, priemer a odchýlka*




*Obr. 11: Útok N8, koeficient variabilnosti*

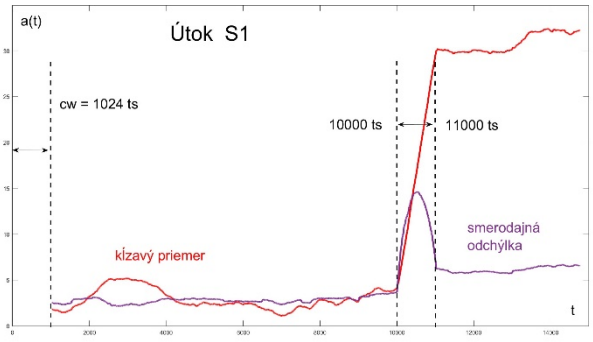



*Obr. 12: Útok N6, priemer a odchýlka*

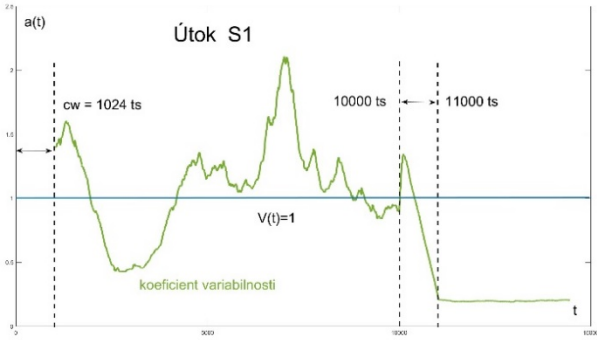



*Obr. 13: Útok N6, koeficient variabilnosti*

V prípade štandardných DDoS útokov (N2,N6,N7,N8) koeficient variabilnosti reagoval rovnako. Štandardná prevádzka predstavovala stacionárny tok s odchýlkou menšou ako stredná intenzita toku. Okamihu nástupu útoku odchýlka zareagovala rýchlejším nárastom hodnôt než bol lineárny rast kĺzavého priemeru, preto podiel odchýlky a priemeru nadobudol v okamihu útoku hodnotu V(tA) = 1. Tento fakt by sa dal využiť pre rýchlu a jednoduchú detekciu pri takomto type útoku. To ale nie je pravidlo, na obr.14 pri útoku S1 vidíme, že počas štandardnej prevádzky je narušená stacionarita a koeficient niekoľko krát pre útokom prekročil hodnotu V(tA) = 1.

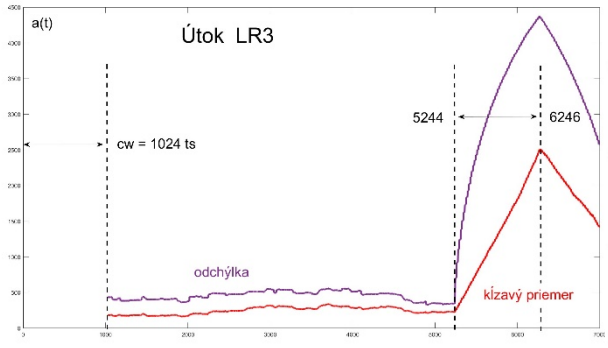



*Obr. 14: Útok S1, priemer a odchýlka*

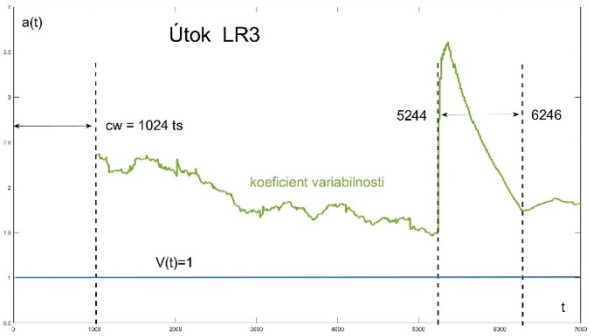



*Obr. 15: Útok S1, koeficient variabilnosti*

Na obr. 16 a 17 sú grafy priemeru, odchýlky a koeficientu variabilnosti pre tzv. Low Rate DDoS útok LR3:




*Obr. 16: Útok LR3, priemer a odchýlka*




*Obr. 17: Útok LR3, koeficient variabilnosti*

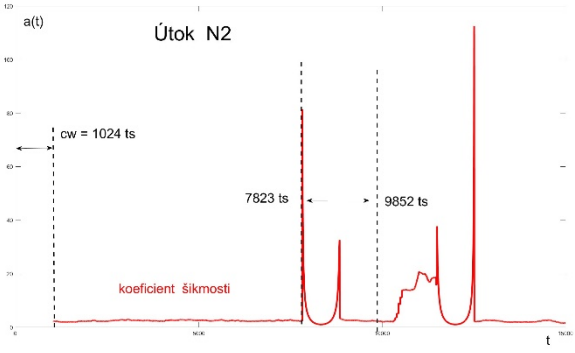
V prípade LR3 je počas bežnej prevádzky odchýlka väčšia než stredná intenzita toku, preto koeficient variabilnosti je počas celého priebehu V(t)>1. Hodnota 1 sa teraz nedá použiť pre rýchlu detekciu. Ale v okamihu útoku hodnoty odchýlky opäť narástli rýchlejšie než lineárny rast strednej intenzity, čo sa prejavilo na výraznom skokovom náraste koeficientu variabilnosti. Táto zmena by sa mala dať rozpoznať pomocou predikčných metód.

Ďalšími jednoduchými štatistickými parametrami sú koeficient šikmosti a koeficient špicatosti. Ide vlastne o tretí a štvrtý centrálny moment vyškálovaný smerodajnou odchýlkou:

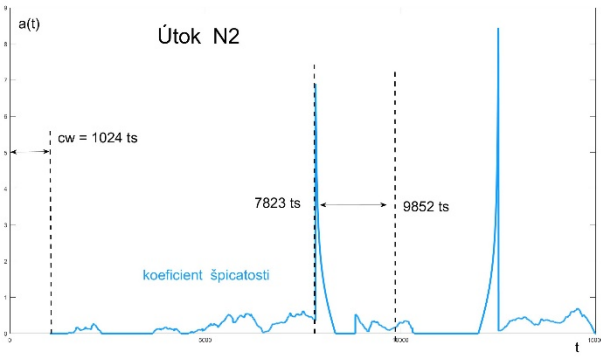
$$\mu_3 = \frac{1}{\sigma^3} E[X - EX]^3 \qquad \mu_4 = \frac{1}{\sigma^4} E[X - EX]^4 \qquad \sigma^2 = E[X - EX]^2$$

V našom prípade realizácie premennej X sú hodnoty prírastkov a(t) a koeficienty popisujú vlastnosti rozdelenia pravdepodobnosti prírastkov v danom výpočtovom okne cw. Pri postupnom načítavaní útočnej prevádzky do vyhodnocovaného okna cw sme predpokladali výraznú zmenu rozdelenia pravdepodobnosti a tým pádom aj zmenu koeficientov. Tento predpoklad sa potvrdil skoro u všetkých analyzovaných tokov. Obidva štatistické koeficienty zareagovali výrazným nárastom svojich hodnôt hneď na začiatku DDoS útoku.

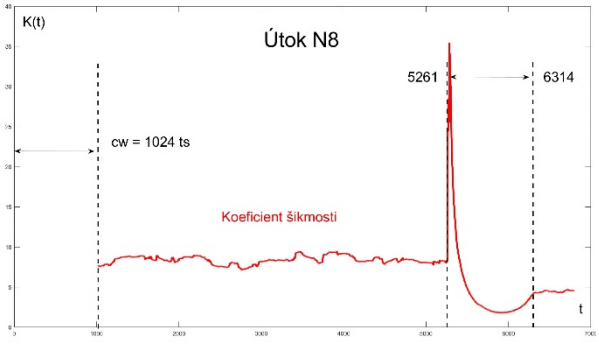
Ako prvé uvádzame grafy koeficientov aplikovaných na vybraných dvoch štandardných útokoch a následne niektoré problematické situácie.



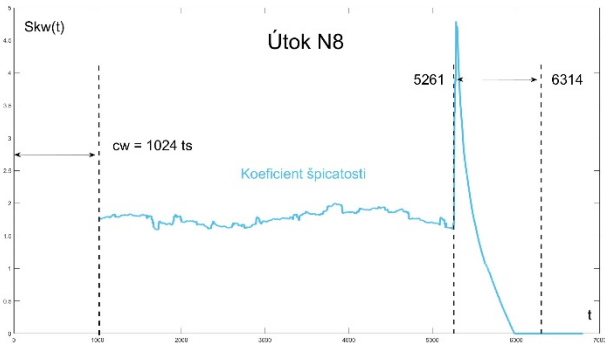

*Obr. 18: Útok N2, koeficient šikmosti*




*Obr. 19: Útok N2, koeficient špicatosti*




*Obr. 20: Útok N8, koeficient šikmosti*

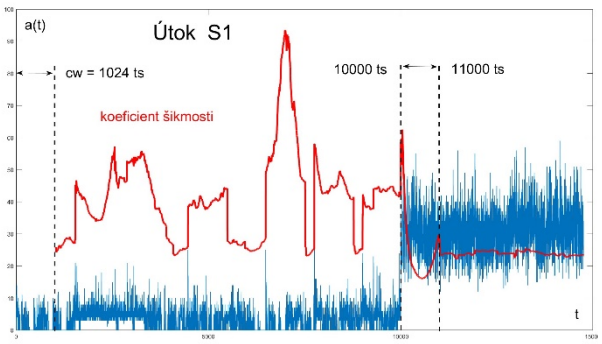



*Obr. 21: Útok N8, koeficient špicatosti*

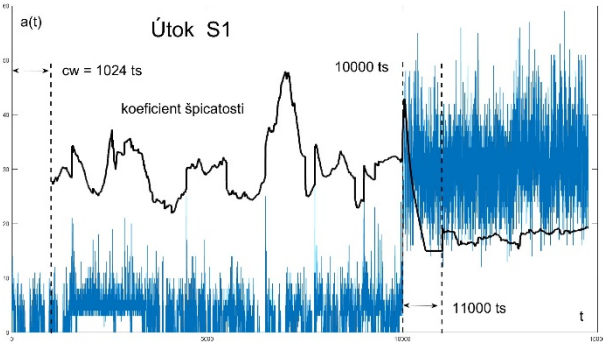
Pri štandardných útokoch typu N koeficienty šikmosti s špicatosti sa počas výpočtu na štandardnej prevádzke vďaka stacionárnosti len mierne vlnia, v okamihu nástupu DDoS útoku sa ich hodnoty výrazne zväčšia. Predpokladáme, že tento výrazný skok budeme vedieť strojovo rozpoznať pomocou vhodných predikčných metód.

Podstatne nepriaznivejšia situácia nastala pri neštandardných útokoch, napr. S1. Vďaka nestacionarite bežnej prevádzky a častému výskytu vysokých peakov obidva koeficienty silne kmitajú, vďaka čomu sa skok pri nástupe útoku stráca v celkovom priebehu toku hodnôt obidvoch koeficientov. Nástup DDoS útoku je v takomto prípade strojovo nerozpoznateľný.

Pre vizualizáciu reakcie koeficientov na zmenu charakteru bežnej prevádzky a na výskyt peakov sme zobrazili hodnoty koeficientov do spoločného grafu spolu s prírastkami toku S1.

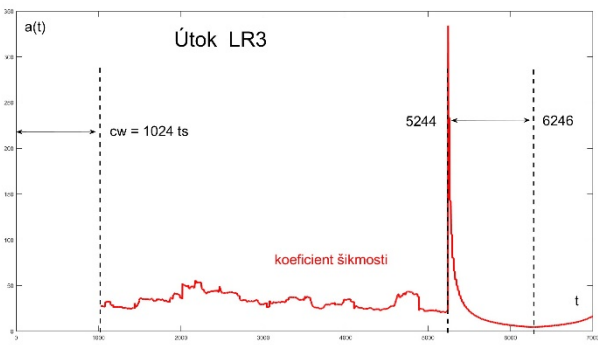



*Obr. 22: Útok S1, koeficient šikmosti*

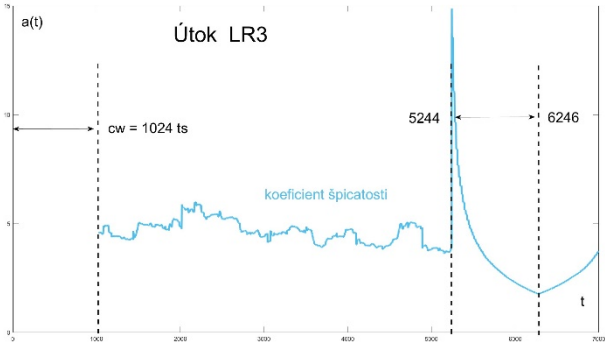



*Obr. 23: Útok S1, koeficient špicatosti*

Reakcia koeficientov pri útoku s nízkou strednou intenzitou LR3 dopadla rovnako pozitívne ako pri štandardných útokoch typu N:




*Obr. 24: Útok LR3, koeficient šikmosti*




*Obr. 25: Útok LR3, koeficient špicatosti*

Opäť vidíme možnosť strojovo rozpoznať výrazný nárast hodnôt koeficientov pri začiatku útoku od hodnôt popisujúcich bežnú prevádzku.

## Detekčné hodnoty pre autokoreláciu a regresiu

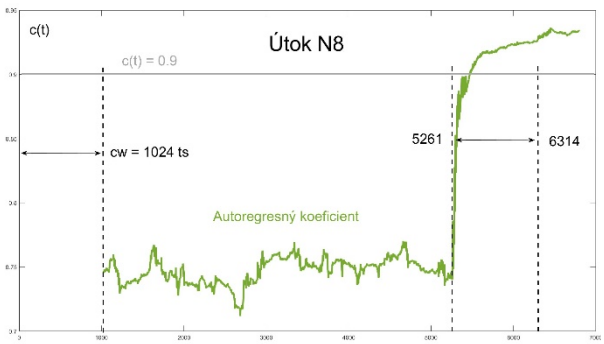
Ďalšie dva koeficienty popisujú autoregresnú a korelačnú závislosť medzi dvoma za sebou idúcimi cw oknami, resp. medzi náhodnými premennými X(t) a X(t-1), ktorých realizácie sú prírastky toku a(t) v uvažovaných oknách.

$$X(t) = c(t).X(t-1) + \varepsilon(t), \qquad \rho(t) = \frac{E[(X(t) - EX(t))(X(t-1) - EX(t-1))]}{\sigma(t)\sigma(t-1)}$$

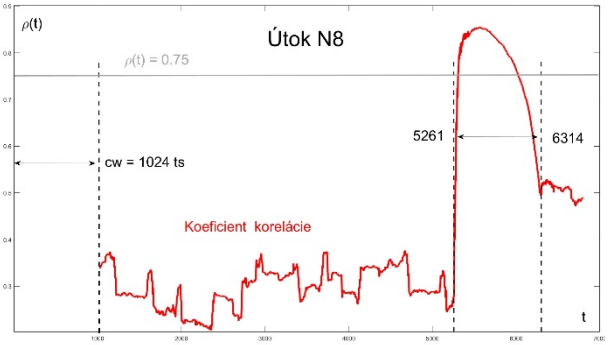
Veľkou výhodou tých koeficientov je, že ich hodnoty sa pohybujú v intervale (-1,1). V okamihu načítavania útoku do vyhodnocovaných cw okien pri väčšine útokoch začali ich hodnoty rýchlo rásť ku hornej hranici 1. Z tohto dôvodu sa je možne pre obidva koeficienty nastaviť určitú medznú hodnotu (threshold), ktorej prekročenie by signalizovalo začiatok DDoS útoku. Čím nižšia je táto hodnota, tým včasnejšia je signalizácia útoku, na druhú stranu moc nízke útoky môžu spôsobiť falošné hlásenia. Na základe prevedených experimentov a v snahe identifikovať čo najväčšie množstvo DDoS útokov bez falošných

hlásení sme nastavili hranicu pre autoregresný koeficient na c(t) = 0.9 a korelačný koeficient na ρ(t) = 0.75.

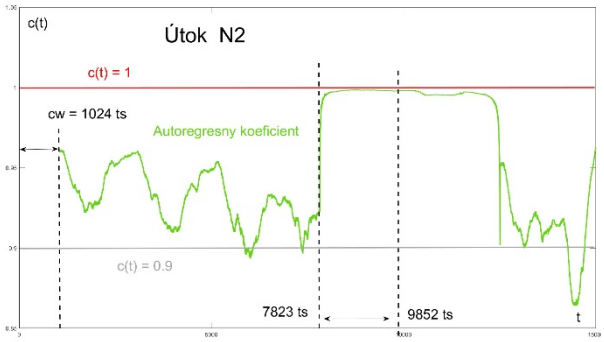
Na nasledujúcich grafoch sme opäť zobrazili vývoj koeficientov pre útoky N8, N2, S1 a LR3. Útok N8 predstavuje chovanie koeficientov pri väčšine štandardných útokov, na N2 vidíme štandardný útok na ktorom ale autokorelačný koeficient má všetky hodnoty väčšie ako 0.9 a detekcia sa nedá použiť. Pri neštandardnom útoku S1 obidva koeficienty pri útoku presiahli detekčné hladiny. Pre útok s nízkou intenzitou LR3 je táto metóda nepoužiteľná.



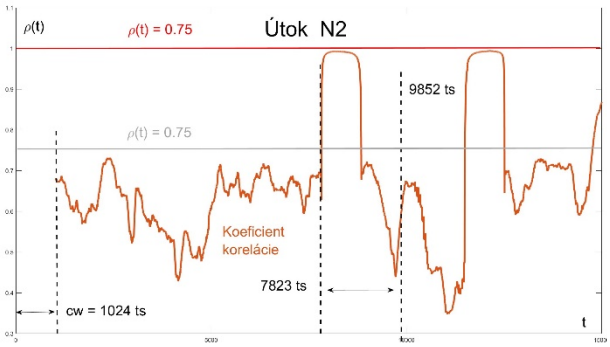

*Obr. 26: Útok N8, Autoregresný koeficient*



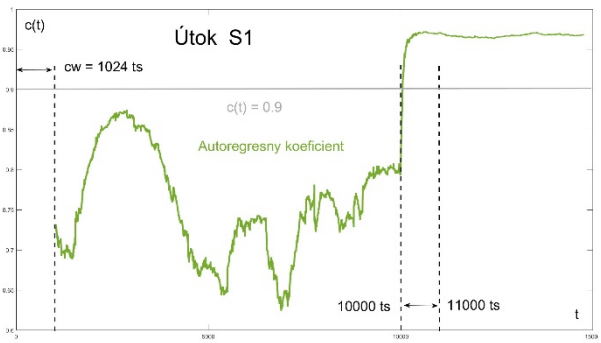

*Obr. 27: Útok N8, koeficient Korelácie*



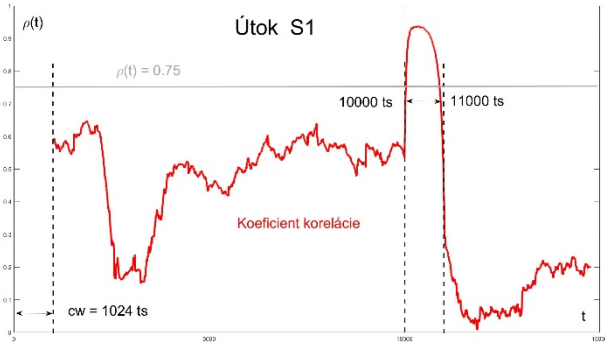

*Obr. 28: Útok N2, Autoregresný koeficient*



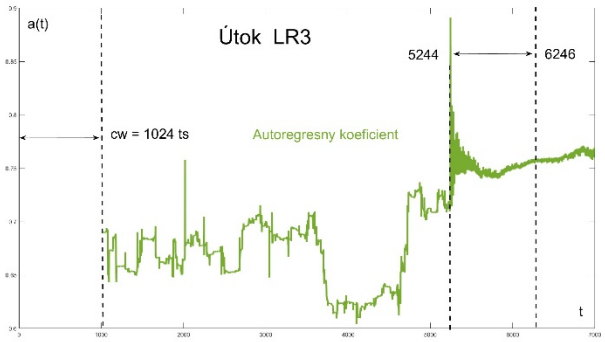

*Obr. 29: Útok N2, koeficient Korelácie*



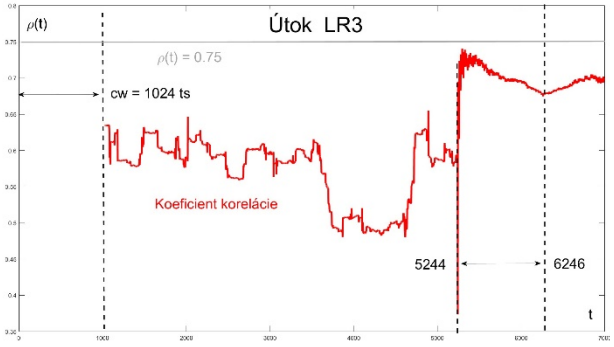

*Obr. 30: Útok S1, Autoregresný koeficient*




*Obr. 31: Útok S1, koeficient Korelácie*




*Obr. 32: Útok LR3, Autoregresný koeficient*




*Obr. 33: Útok LR3, koeficient Korelácie*

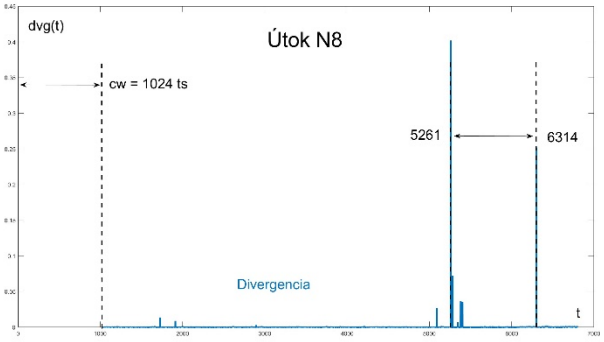
Pre väčšinu útokov sa dá predpokladať, že prekročenie detekčných hodnôt pri autoregresii a korelácii sa bude dať v kombinácii s ďalšími koeficientami využiť pre skorú jednoduchú detekciu záplavového útoku.

## Reakcia divergencie na DDoS útok

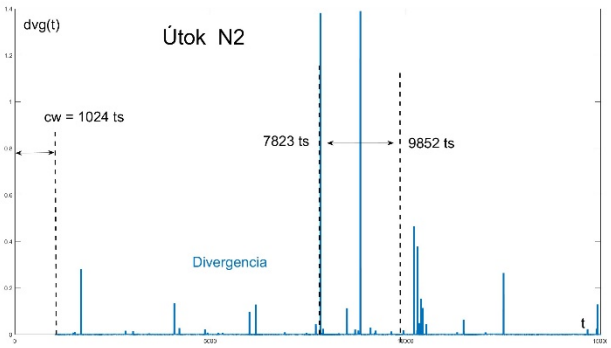
Posledným analyzovaným parametrom Kullback-Leibler divergencia istým spôsobom porovnáva rozdelenie pravdepodobnosti P(.) prírastkov a(t) v za sebou idúcich prekrytých výpočtových oknách cw:

$$dvg(t) = \sum_{k=1}^{n} P(t-1) ln(\mathrm{P(t-1)/P(t)})$$

Výhodou divergencie je, že na sledovaných vzorkách vo väčšine prípadoch reagovala okamžite na nástup DDoS útoku vysokým impulzom (peakom). Nevýhodou je, že mala tendenciu takto reagovať aj na peaky v bežnej prevádzke, čo by mohlo spôsobovať množstvo falošných hlásení.

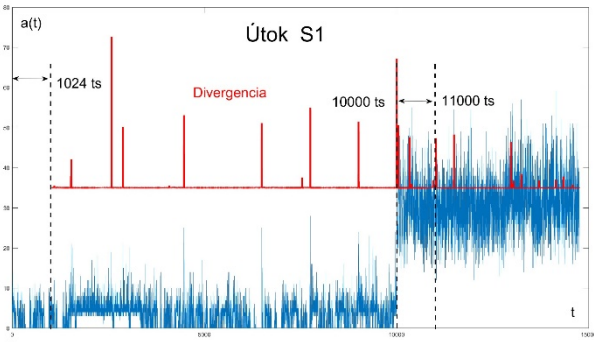



*Obr. 34: Útok N8, Divergencia*

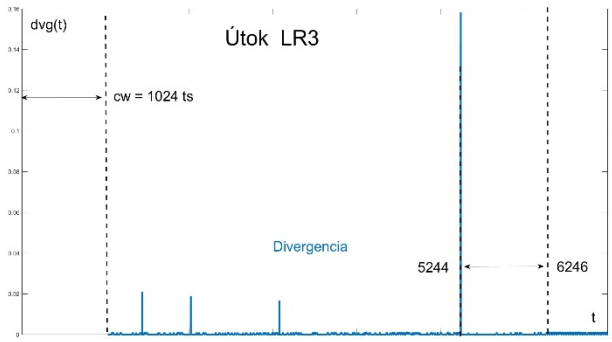



*Obr. 35: Útok N2, Divergencia*

Ďalšou nevýhodou použitia divergencie je fakt, že vysoký impulz pri nástupu útoku trvá veľmi krátko oproti ostatným parametrom, preto jej aplikáciu v kombinácii s ostatnými para-metrami vidíme ako problematickú. Použitie divergencie sme preto odložili do budúcnosti.




*Obr. 36 Útok S1, Divergencia*

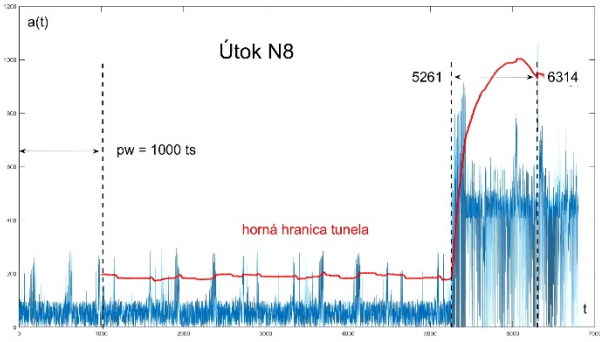



*Obr. 37: Útok LR3, Divergencia*

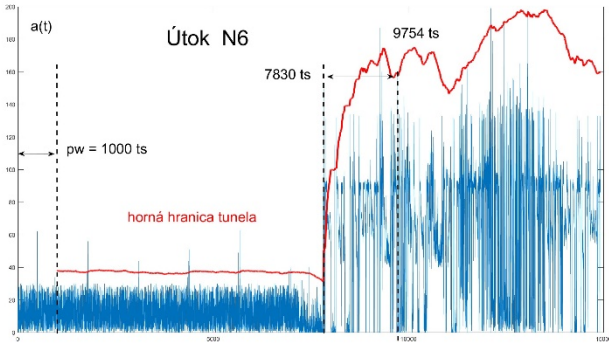
## Využitie 3σ-Tunela pre rozpoznanie DDOS útokov

Na základe experimentov sme pre výpočet priemeru a odchýlky zvolili 1000 predchádzajúcich hodnôt, a šírku interval sme zvolili (EX-3σ, EX+3σ) (pri menšej veľkosti intervalu dochádzalo k častým falošným hláseniam). Túto metódu sme nazvali predikčný 3σ-tunel.

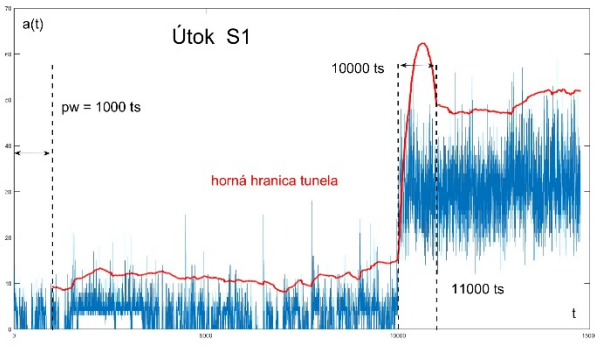
Vzniká prirodzená otázka, prečo nepoužiť predikčný tunel priamo na prírastky IP toku a(t) a nezdržiavať sa výpočtom štatistických koeficientov. Po prevedení experimentov sme zistili, že síce prekročenie hornej hranice tunela deteguje relatívne skoro nástup DDoS útoku, ale zároveň dochádza k častému hláseniu falošného poplachu. Pri zväčšení násobnosti smerodajnej odchýlky sa síce počet falošných hlásení zmenšil ale zároveň sa zmenšila schopnosť detegovať útok. Na nasledujúcich obrázkoch si ukážeme na vybraných útokoch len hornú hranicu 3σ-Tunela.



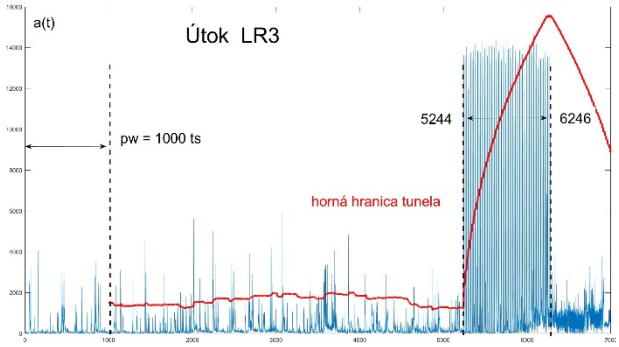

*Obr. 38: Útok N8, horná hranica 3σ-Tunela*




*Obr. 39: Útok N6, horná hranica 3σ-Tunela*

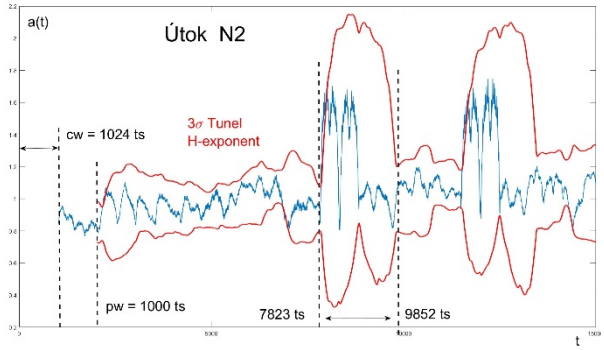



*Obr. 40: Útok S1, horná hranica 3σ-Tunela*

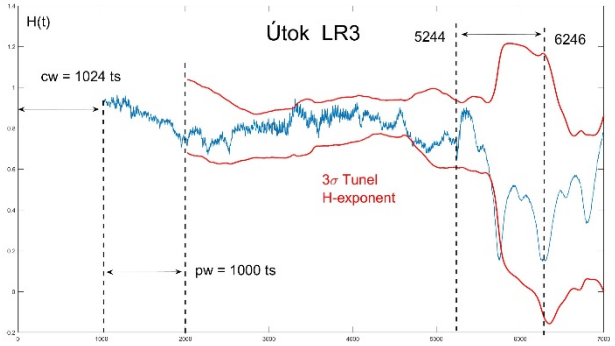



*Obr. 41: Útok LR3, horná hranica 3σ-Tunela*

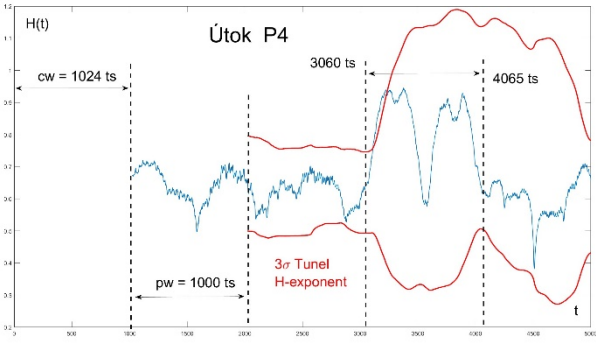
Na nasledujúcich grafoch budeme demonštrovať chovanie sa 3σ-Tunela na parametre s najväčšou variabilitou z pomedzi uvažovaných štatistických koeficientov, a to na Hurstovom exponente (odhadnutého RS štatistikou s odstránením autoregresie AR1).



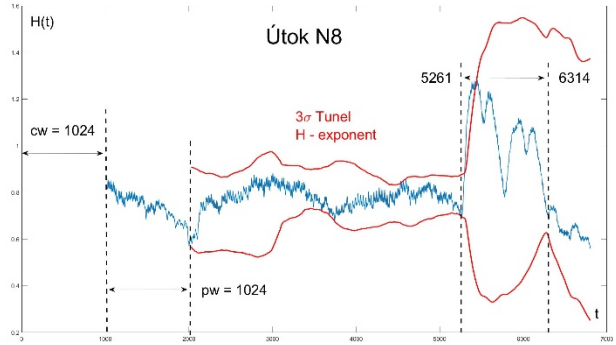

*Obr. 42: N2, 3σ-Tunel pre H-exponent*




*Obr. 43: LR3, 3σ-Tunel pre H-exponent*




*Obr. 44: P4, 3σ-Tunel pre H-exponent*




*Obr. 45: N8, 3σ-Tunel pre H-exponent*

Vo väčšine prípadoch (až na útok LR3) 3σ-Tunel skoro rozpoznal začiatok DDoS útok s minimálnym, niekedy až nulovým počtom falošných hlásení.

Ako sme už uviedli, na základe experimentov sme nastavili veľkosť predikčného okna na 1000 ts a šírku intervalu pre 1001 hodnotu na trojnásobok smerodajnej odchýlky. Pri takomto nastavení sme vo väčšine experimentov (rôzne koeficienty a rôzne útoky) získali skoré rozpoznanie začiatku útoku s minimálnym počtom falošných hlásení. Na predchádzajúcich obrázkoch sú to 3 prípady zo 4. Takto nastavený tunel má dve užitočné vlastnosti:

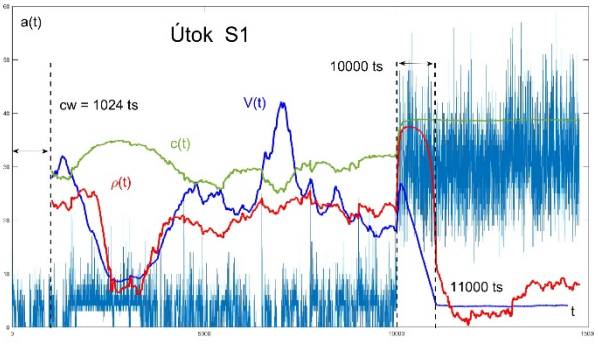
- Má dostatočne „dlhú pamäť“ na to, aby dokázal pokryť lokálnu variabilnosť štatistického koeficientu a nespôsoboval veľké množstvo falošných hlásení
- Má dostatočne „dlhú pamäť“ na to, aby nedokázal zareagovať na relatívne veľký nárast hodnôt skúmaného koeficient pri začiatku DDoS útoku (veľký vzhľadom na relatívnu variabilnosť)

Samozrejme, aby sme mohli vysloviť nejaké relevantnejšie závery a odporúčania, je potrebné previesť množstvo experimentov na záznamov rôznych DDoS útokov.

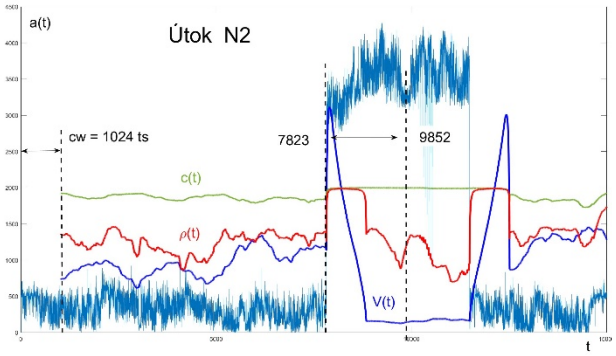
## Detekčné funkcie pre strojové rozpoznanie DDoS útokov

V predchádzajúcich kapitolách sme uviedli dva spôsoby rozpoznania DDoS útokov pomocou štatistických koeficientov. Prvým spôsobom bolo určenie detekčných hodnôt pre vhodné parametre, 1,00 pre variabilnosť V(t) a H-exponent, 0,90 pre autoregresný koeficient c(t) a 0,75 pre korelačný koeficient ρ(t). Druhý spôsob pomocou predikčného tunela bol analyzovaný v predchádzajúcej časti.

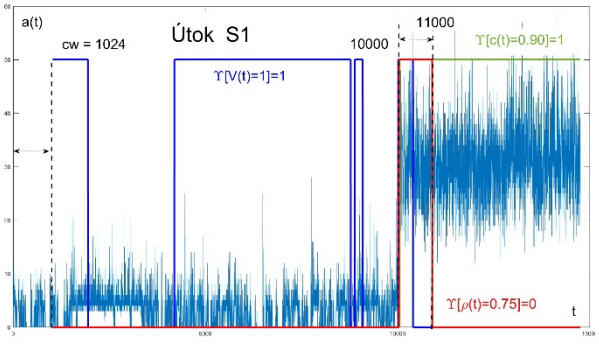
Pri využití hraničných hodnôt sme zaviedli dvojhodnotovú logickú funkciu Y[.], ktorá vyhodnocuje prekročenie hraničnej hodnoty pre daný štatistický koeficient. Nasledujúcich grafoch si ukážeme variabilnosť V(t), autoregresný koeficient c(t) a korelačný koeficient ρ(t) a priebeh ich funkcie Y[.] pre útoky S1a N2:



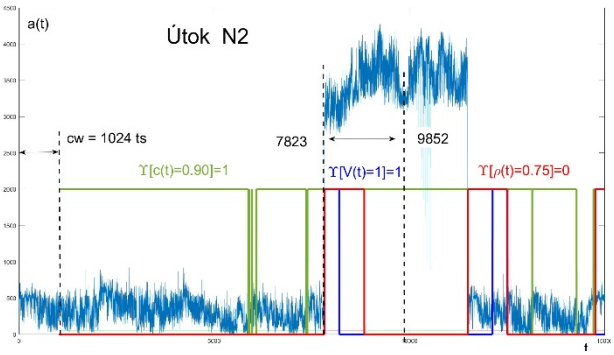

*Obr. 46: S1, koeficienty V(t), c(t), ρ(t)*




*Obr. 47: N2, koeficienty V(t), c(t), ρ(t)*




*Obr. 48: S1, priebeh funkcií ϒ[.]*

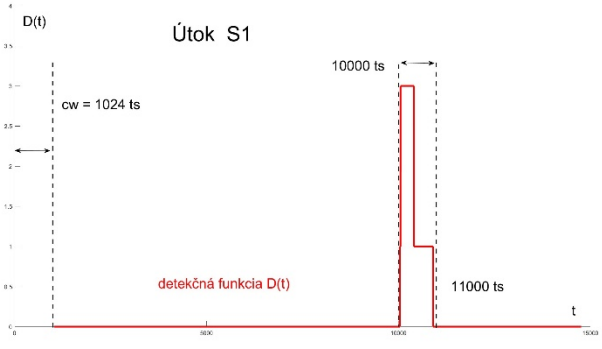



*Obr. 49: N2, priebeh funkcií ϒ[.]*

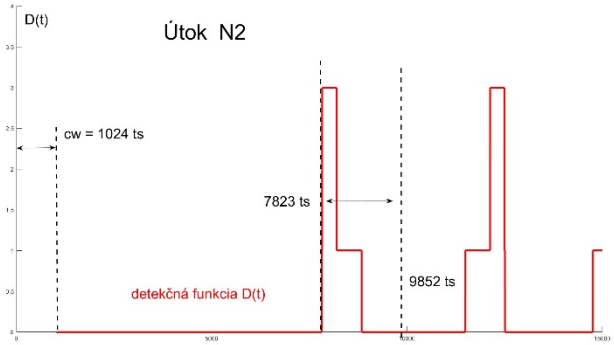
Množiny hodnôt, na ktorých koeficienty prekračujú svoje detekčné hranice, nazveme detekčné intervaly. Na obr. 48 a 49 vidíme, ako sa tieto intervaly navzájom prekrývajú. Aby sme eliminovali falošné hlásenia a zároveň dosiahli včasné rozpoznanie útokov, zavedieme pre sledované koeficienty novú detekčnú funkciu D(t), pričom pre zjednodušenie označíme napr. pre koeficient V(t) funkciu Y[V(t)>1,00] ako YV(t):

$$D(t) = YV(t).YC(t) + YV(t).Y\rho\ (t) + YC(t).Y\rho\ (t)$$

Na nasledujúcich obrázkoch vidíme priebeh detekčnej funkcie pre útoky S1 a N2:




*Obr. 49: S1, priebeh detekčnej funkcie D(t)*




*Obr. 50: N2, priebeh detekčnej funkcie D(t)*

Vďaka tvaru funkcie D(t) sme eliminovali eventuálne falošné hlásenia a zároveň podľa hodnôt 1 alebo 3 vieme rozpoznať, a akom čase detegovali útok dva alebo všetky 3 štatistické parametre.

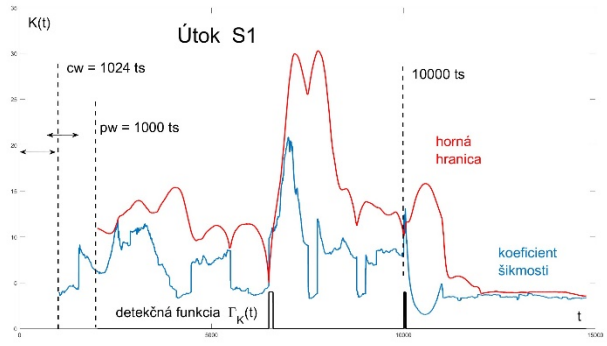
V tabuľke 1 uvádzame vyhodnotenie použitia detekčnej funkcie D(t) pre analyzované útoky. Prvá hodnota predstavuje počet falošných hlásení, druhá určuje dobu, kedy detegovali útok minimálne dva koeficienty a tretia hodnota označuje dobu, kedy detegovali útok všetky tri štatistické koeficienty V(t), c(t) a ρ(t).

| útok | S1 | N2 | LR3 | S5 | N6 | N7 | N8 |
|---|---|---|---|---|---|---|---|
| D(t) | 0 – 34 - 52 | 0 - 5 - 5 | x | x | 0 – 75 - 119 | 0 - 228 - 480 | 0 - 47 - 210 |

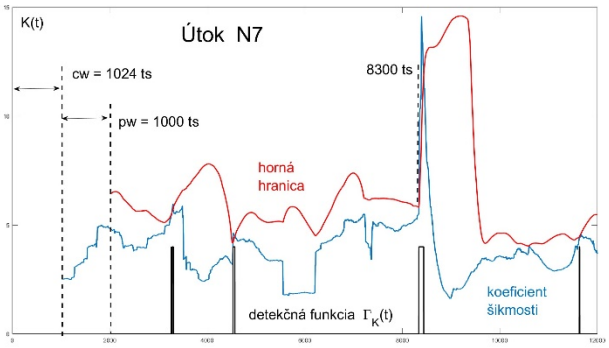
*Tab. 1: Vyhodnotenie rozpoznania DDoS útoku pomocou detekčnej funkcie D(t)*

Rozpoznanie útoku podľa hraničnej hodnoty bolo účinné hlavne pri štandardných útokoch, pričom vo viacerých prípadoch dva koeficienty prekročili svoje hraničné hodnoty podstatne skôr než všetky tri. Pri neštandardných útokoch ako LR3, P4 a S5 žiadne dva detekčné intervaly, ak vôbec vznikli, nemali spoločný prienik, a preto útok nebol rozpoznaný

Rovnakú metodiku budeme aplikovať aj na rozpoznanie útoku pomocou predikčného tunela. V predchádzajúcej kapitole sme určili, pri zohľadnení doby rozpoznania útoku a počtu falošných hlásení, prvé tri najefektívnejšie štatistické koeficienty: šikmosť K(t), špicatosť Skw(t) a variabilnosť V(t). Keďže sme vybrali koeficienty, ktorým sa pri nástupe DDoS útoku výrazne zväčšia hodnoty, preto sa budeme zaoberať len hornou hranicou predikčného tunela. Dobu prekročenia hornej hranice vyhodnotíme ako detekčný interval a popíšeme ho dvojhodnotovou funkciou Γ[.], pričom napr. pre koeficient špicatosti označíme ΓK(t) = Γ[K(t)>Hr(t)], kde Hr(.) je horná hranica predikčného intervalu pre koeficient K(.).




*Obr. 51: S1, priebeh funkcie Γ(t)*




*Obr. 52: N7, priebeh funkcie Γ(t)*

Podobne ako pri predchádzajúcej metóde, pri rozpoznávaní pomocou hraničnej hodnoty, aj teraz zavedieme detekčnú funkciu, ktorá bude kombináciou identifikátorov Γ(t):

$$DP(t) = \Gamma K(t).\Gamma Skw(t) + \Gamma K(t).\Gamma V(t) + \Gamma Skw(t).\Gamma V(t)$$

V tabuľke tab.2 uvádzame vyhodnotenie použitia detekčnej funkcie DP(t).

| útok | S1 | N2 | LR3 | S5 | N6 | N7 | N8 |
|---|---|---|---|---|---|---|---|
| $D_P(t)$ | 1 – 6 - 28 | 0 - 1 - 1 | 1 - 1 - 1 | 1 - 18 - 41 | 1 - 12 - 12 | 1 - 39 - 49 | 0 - 1 - 1 |

*Tab. 2: Vyhodnotenie rozpoznania DDoS útoku pomocou detekčnej funkcie D(t)*

## Záver

Na základe doteraz prevedených experimentoch vidíme využitie vybraných štatistických koeficientov má podstatne väčší potenciál pri rýchlom rozpoznaní DDoS útokov (FAD – Fast Attack Detection) než štandardné sledovanie priemernej a špičkovej intenzity. Pri DDoS útoku je silný predpoklad, že sa tieto intenzity výrazne zvýšia. Avšak priemerná intenzita rastie len lineárne v závislosti od veľkosti kĺzavého okna, čo vedie k neskorej detekcii útoku, a rozpoznávanie útoku pomocou nastavenia nejakého tresholdu pre špičkovú rýchlosť môže viesť k častým falošným hláseniam vďaka výskytu píkov v IP toku.

Pri prechode štandardnej IP prevádzky do DDoS útoku sa výrazne zmení nie len priemerná a špičková intenzita, a zmení sa celková pravdepodobnostná štruktúra záplavového toku. Na zachytenie tejto zmeny sme využili prezentované štatistické koeficienty. Tie môžeme rozdeliť na dva typy, koeficienty, ktoré pri nástupu útoku prekročili nejakú detekčnú hodnotu a koeficienty, ktoré na útok reagovali výraznou zmenou svojich hodnôt resp. impulzom. Niektoré koeficienty dokonca patria do obidvoch skupín. Na základe tohto delenia sme vytvorili:

- Metódu použitia detekčných hraníc (MDH)
- Metóda použitia predikčných tunelov (MPT)

Porovnaním tabuliek 1 a 2 vidíme, že MPT rozpoznala každý uvažovaný typ útoku a to podstatne skôr ako MDH, avšak pri väčšine útokov signalizovala jedno falošné hlásenie. Predpokladáme, že tento problém by sa mohol odstrániť viacerými spôsobmi, napríklad pridaním ďalšieho vhodného detekčného koeficientu, ale nejakým typom vyhladenia hodnôt koeficientu pred použitím predikčného tunela, napr. Exponenciálnym alebo Holtový vyhladením.

Viac informácií možno nájsť v dokumente „Machine Recognition of DDoS Attacks Using Statistical Parameters.pdf“