elektrorevue
ISSN 1213 - 1539

Rok / Year:	Svazek / Volume:	Číslo / Number:	Jazyk / Language
2016	18	4	CZ

Identifikace anomálií v datové komunikaci pomocí entropie

Identification of anomalies in data comunication using the entropy

Petr Blažek, Jan Hajný

blazekpetr@phd.feec.vutbr.cz, hajny@feec.vutbr.cz

Fakulta elektrotechniky a komunikačních technologií, VUT v Brně

DOI: -

Abstract: This article discusses the use of entropy for identifying anomalies in data communication. At testing the attention is focused on the comparison of three types of entropy (Shannon entropy, Rényi entropy, Tsallis entropy) and select the most appropriate one for identification of anomalous traffic. In the article the reader will find a classification of normal data traffic from recorded network traffic, using the above-mentioned entropies and determination of the suitable adjustable parameter for Rényi entropy and Tsallis entropy. Next in this article are the entropies used for the identification of anomalous traffic caused by the DoS attack.

elektrorevue
ISSN 1213 - 1539

Identifikace anomálií v datové komunikaci pomocí entropie

Petr Blažek, Jan Hajný

Fakulta elektrotechniky a komunikačních technologií VUT v Brně
Email: blazekpetr@phd.feec.vutbr.cz, hajny@feec.vutbr.cz

Abstrakt *– Tento článek pojednává o využití entropie pro identifikaci anomálií v datové komunikaci. Pozornost při testování je zaměřena na porovnání tří typů entropií (Shannonova entropie, Rényiho entropie, Tsallisova entropie) a výběr nejvhodnější pro identifikaci anomálního provozu. Čtenář v článku nalezne klasifikaci běžného datového provozu ze zaznamenané síťové komunikace pomocí výše zmíněných entropií a určení vhodného nastavitelného parametru u Rényiho a Tsallisovy entropie. Dále jsou v článku entropie použity pro identifikaci anomálního provozu způsobeného DoS útokem.*

1 Úvod

Kybernetické útoky jsou nedílnou součástí datové komunikace na Internetu. Velký podíl mezi nimi mají útoky založené na odepření některé ze síťových služeb tzv. DDoS (Distribute Denial of Service) útoky. Každý rok počet těchto útoků vzrůstá a útočníci nalézají stále efektivnější metody jak obejít systémy, které mají těmto útokům zabránit. Většina současných metod pro detekci útoků je zaměřena na vzorcích chování jednotlivých útoků. Nevýhodou těchto metod je, že nedokáží identifikovat neznámé útoků. O proti tomu metody založené na matematických modelech sledují změny v datové komunikaci a podle toho vyhodnocují případné anomálie. Nevýhodou těchto metod je, že anomálie nemusí nutně znamenat útok, ale změnu chování datového provozu. Jednou z metod popisující chování datové komunikace je i entropie, která udává míru neuspořádanosti prvků v daném systému. V případě síťové komunikace by se měla míra neuspořádanosti pro běžný datový provoz pohybovat v určitém intervalu. Anomálie ovlivňující síťový provoz by měly změnit míru neuspořádanosti a tedy i výslednou hodnotu entropie. Na základě těchto poznatků tento článek porovnává vhodnost tří typů entropie - Shannonova, Rényiho a Tsallisova.

2 Entropie

S pojmem entropie se můžeme například setkat v matematice, informatice nebo fyzice a to v případech zabývajících se pravděpodobností možných prvků v daném systému. Jak již bylo zmíněno v úvodu tohoto článku entropie udává míru neuspořádanosti prvků v daném systému. Entropie tedy svojí hodnotou vyjadřuje pravděpodobnostní rozdělení všech prvků v daném systému. Maximální hodnoty entropie dosáhne, pokud všechny možné prvky mají stejnou pravděpodobnost výskytu. Nejmenší hodnota entropie nastává, je-li v systému pravděpodobnost výskytu pouze jednoho prvku a ostatní prvky jsou nulové [1], [2].

2.1 Shannonova entropie

Entropie používaná v informatice nám udává míru neurčitosti před přijetím zprávy, která se po přijetí odstraňuje a vyjadřuje tak míru informace. První kdo definoval informační entropii byl Claude E. Shannon, podle kterého je i pojmenovaná. Definoval ji pro množinu pravděpodobností p_1 až p_n a lze ji vypočítat jako střední hodnotu

$$H(p_i) = -\sum_{i=1}^{n}(p_i \cdot \ln p_i), \tag{1}$$

kde p_i představuje pravděpodobnostní výskyt i-tého prvku [3], [4].

2.2 Rényiho entropie

Další z testovaných entropií definoval v padesátých letech dvacátého století maďarský matematik Alfréd Rényi pro množinu pravděpodobností p_1 až p_n. Výsledná hodnota Rényiho entropie se vypočte dle

$$H_\alpha(p_i) = \frac{1}{1\text{-}\alpha} \cdot \log\left(\sum_{i=1}^{n} p_i^\alpha\right) \alpha \geq 0,\ \alpha \neq 1, \tag{2}$$

kde p_i je pravděpodobnost i-tého stavu systému. Parametr α je reálné číslo, pro které platí $\alpha \geq 0$ a $\alpha \neq 1$. V případě, kdy $\alpha \to 0$ započítává všechny hodnoty se stejnou vahou nezávisle na jejich pravděpodobnosti. V opačném případě $\alpha \to \infty$ bude výsledná hodnota entropie určena jen událostmi s největší pravděpodobností výskytu. Pokud by se hodnota parametru $\alpha \to 1$, výsledná hodnota Rényiho entropie konverguje k hodnotě Shannonovy entropie. Díky těmto vlastnostem je Rényiho entropie dobře použitelná v různých oblastech jako jsou například statistika, biomedicína, kryptografie, ekonomie a další [5], [6].

2.3 Tsallisova entropie

Poslední entropií použitou v tomto článku definoval v osmdesátých letech dvacátého století brazilský fyzik Constantino Tsallis při zobecňování Bolzmann-Gibbsovy entropie

elektrorevue
ISSN 1213 - 1539

a stejně jako předchozí entropie je definována pro množinu pravděpodobností p_1 až p_n. Hodnota Tsallisovy entropie se vypočte podle vzorce

$$H_q(p_i) = \frac{1}{q\text{-}1} \cdot \left(1\text{-} \sum_{i=1}^{n} p_i^q\right) q \neq 1, \qquad (3)$$

kde p_i je pravděpodobnost i-tého stavu systému. Hodnota parametrů q musí být reální číslo a $q \neq 1$. V případě, kdy $q \to \infty$ se entropie blíží k 0. Pokud vezmeme opačnou situaci $q \to (\text{-}\infty)$, potom se entropie blíží hodnotě ∞. Stejně jako u Rényiho entropie Tsallisova entropie konverguje k Shannonově entropii pokud parametr $q \to 1$. Tsallisova entropie má uplatnění ve fyzice, statistice nebo dalších odvětvích zabývajících se pravděpodobností [7], [8].

3 Související práce

Jak již bylo zmíněno v kapitole 1, entropie by na základě svých vlastností měla být schopná identifikovat změny v datové komunikaci. Na této myšlence jsou založeny práce [9], [10], [11] a [12]. První tři práce jsou v základu založeny na využití Shannonovy entropie pro identifikaci anomálií v datové komunikaci. Čtvrtá práce [12] se zabývá nejpodobnější problematikou, ve které jsou porovnávány stejné typy entropií na různých typech síťových útoků. V článku autoři došli k závěru, že Rényiho a Tsallisova entropie dosahuje podobně dobrých výsledků při identifikaci anomálií v datové komunikaci. Autoři v článku také určili interval parametrů α u Rényiho entropie a parametru q u Tsallisovy entropie v rozsahu od (-2) do 2. Hodnoty mimo tento interval považují za nevhodné pro identifikaci anomálního provozu.

V případě této práce se zaměřuji na bližší určení parametru α u Rényiho entropie a parametru q u Tsallisovy entropie pro identifikaci DoS a DDoS útoků. Dále se zaměřuji na porovnání všech tří entropií a určení nejvhodnější pro identifikaci DoS útoků a DDoS útoků.

4 Testování

Princip identifikace anomálií použitý v tomto článku, je založen na výpočtu entropie. Hodnota entropie se vypočítává z parametrů zaznamenané datové komunikace z určitého časového intervalu. Parametrem mohou být různá data paketu síťové komunikace, například IP adresy nebo porty [9], [10], [11].

Testování na základě vyhodnocení jednotlivých entropií bylo prováděno na datech, která byla odchycena na serveru v síti Cesnet. Data byla zaznamenávána v průběhu čtrnácti dní a ukládána každou hodinu do souboru ve formátu pcap. Vzhledem k velkému objemu datového provozu bylo odchytáváno pouze prvních 64 bajtů přenášených paketů, tak aby každý paket obsahoval alespoň hlavičku paketu a bylo možné získat data potřebná k analýze.

Pro testování vhodnosti zvolených entropií byl celkový objem zaznamenané komunikace příliš velký, proto bylo třeba vybrat konkrétní hodinu. Ze všech zaznamenaných dnů bylo pro každou hodinu vypočteno množství přenesených paketů, ze kterých se pro každý den určil síťový provoz na serveru. Ze získaných hodnot se pro testování vybírala hodina, která obsahovala největší datovou komunikaci v průběhu všech zaznamenaných dnů. Největší provoz se v daných dnech nacházel mezi 7 až 9 hodinou. Pro analýzu byl vybrán čas mezi 8 a 9 hodinou. Pro vetší detail provozu byly hodinové soubory pro všechny dny rozděleny do 60 minutových souborů. K rozdělení byl použit program editcap, který je součástí programu Wireshark [13]. Takto připravené soubory byly použity pro první část testování.

Pro entropie uvedené v úvodu toho článku, byl vytvořen program v programovacím jazyku Python. Tento program z připravených souborů vybíral z každého zaznamenaného paketu určitý parametr a ukládal ho do tabulky. Pro toto testování byli zvoleny jako parametr zdrojové IP adresy. Pro každou IP adresu uloženou v tabulce program vypočetl její pravděpodobnost výskytu pro daný soubor. Pravděpodobnosti jednotlivých IP adres následně sloužily jako vstupní data pro výpočet entropií.

První částí testování bylo stanovení v jakém intervalu se pohybuje hodnota entropie při běžném datovém provozu. Pro výše zmíněný zaznamenaný síťový provoz, který představoval běžný provoz, se pro každý z připravených souborů vypočetla hodnota entropie a z těchto hodnot se zjistila maximální a minimální hodnota entropie. Tyto hodnoty entropie sloužily k definování intervalu běžného datového provozu. Mimo tento interval jsou hodnoty entropie považovány za anomálii.

Pro druhou část analýzy bylo vybráno náhodně pět dnů a z každého dne byl zvolen jeden soubor. Označení souborů které bylo použito při testování a jejich velikosti jsou v tabulce 1. Takto zvolené soubory sloužily jako základ pro druhou část analýzy, ve které se testovalo, jak se změní hodnota entropie, pokud se k souboru přidá datová komunikace reprezentující anomálii. Jako anomálie byl vybrán DDoS útok typu UDP flood. Útok byl generován pomocí síťového nástroje hping3, který slouží ke generování TCP/IP paketů [14]. UDP flood byl vybrán na základě své jednoduchosti, protože cílem testováni nebylo ověřit identifikaci tohoto útoku, ale otestovat, jak velký vliv má anomální provoz s různými pravděpodobnostními rozděleními na výslednou hodnotu zvolených entropií a jak velký vliv má na výslednou hodnotu nastavitelný parametr u Rényiho a Tsallisovy entropie. Pro parametr α u Rényiho entropie se hodnoty nastavovaly v rozsahu od 0 do $4,8$. U Tsallisovy entropie se parametr q nastavoval v rozmezí od $(\text{-}1,0)$ do $0,8$.

Útok UDP flood byl vytvořen celkem v šestnácti různých variantách. Odlišnost útoků je dána jejich objemem paketů a počtem útočících zdrojů. V tabulce 2 je útok UDP flood uveden ve variantách s různým počtem paketů. Velikost útoků byla volena v závislosti na velikosti vybraných testovaných souborů přestavujících běžný datový provoz. Každý tento útok byl vytvořen ve čtyřech variantách podle počtu zdrojů útoku. Jednotlivé varianty jsou rozděleny na útok z jednoho zdroje, z 1000 zdrojů, z 10000 zdrojů a ná-

elektrorevue
ISSN 1213 - 1539

Tabulka 1: Soubory s běžným provozem vybrané pro testování.

označení souboru	1	2	3	4	5
počet paketů	902669	419738	445643	130228	390035

hodného počtu zdrojů. Různé varianty počtu zdrojů útoků mají ověřit, jak se boudou jednotlivé entropie chovat při odlišných pravděpodobnostních rozděleních.

Tabulka 2: Útoky UDP flood vytvořené pro testování.

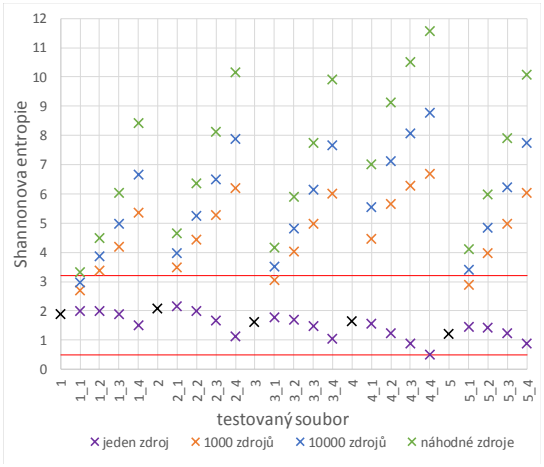
označení útoku	1	2	3	4
počet paketů	100000	200000	500000	1000000

5 Výsledky

V této kapitole jsou prezentovány výsledky, kterých bylo dosaženo během testování. Kapitola je rozdělena do čtyř částí pro každou z použitých entropií a jejich porovnání. Výsledné hodnoty entropií pro nejlepší dosažené výsledky jsou prezentovány v grafech na obrázcích 1, 3 a 5. Y-osa v těchto grafech představuje výsledné hodnoty entropií. Na X-ose jsou uvedeny jednotlivé analyzované soubory. Názvy souborů se skládají z čísla testovaného souboru podle tabulky 1 a čísla označujícího útok podle tabulky 2 oddělenými podtržítkem. Soubory bez útoku jsou označeny pouze číslem testovaného souboru a v grafech jsou prezentovány černou barvou. Soubory s útoky jsou barevně odlišeny podle počtu útočících zdrojů. V každém z těchto grafů je červenými přímkami vyznačen interval definující běžný síťový provoz. Hodnoty mimo tento interval jsou považovány za anomálie. V případě Réniyho a Tsallisovy entropie jsou uvedeny grafy na obrázcích 2 a 4, které zobrazují změnu entropie pro různé hodnoty nastavitelných parametrů z intervalů uvedených v kapitole 4. Pro porovnání hodnot entropií pro různé hodnoty nastavitelného parametru byla provedena normalizace pomocí lineární transformace do intervalu <0,1>.

5.1 Shannonova entropie

První zvolenou entropií pro testování byla Shannonova entropie. Vybrána byla na základě podobných článků [9], [10], [11], kde už byla použita pro identifikaci anomálií v datové komunikaci. Shannonova entropie nemá žádný nastavitelný parametr a nebylo nutné provádět testování jako v případě následujících dvou entropií. Do testování byla začleněna, aby sloužila pro porovnání s ostatními testovanými entropiemi. Výsledné hodnoty entropií pro testované soubory jsou uvedeny v grafu na obrázku 1. Interval entropie definující běžný datový provoz byl vypočten v rozsahu od $0,4956$ do $3,1986$. Mezi těmito hodnotami jsou hodnoty entropií klasifikovány jako běžný provoz. Z grafu na obrázku 1 je



Obrázek 1: Výsledné hodnoty Shannonovy entropie pro testované soubory s útoky.

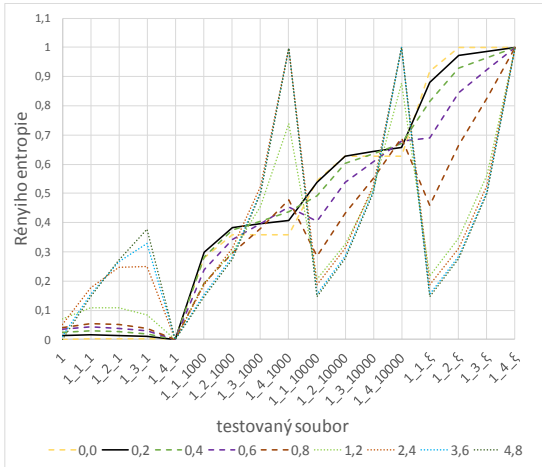
patrné, že při identifikaci větších útoků vedených z více než jednoho zdroje neměla Shannonova entropie problém s identifikací. V případě menších útoků klasifikovala čtyři útoky jako běžný provoz a dalších pět útoků se nacházelo blízko maxima intervalu běžného provozu. Pokud byl útok veden jen z jednoho zdroje, nedokázala Shannonova entropie klasifikovat ani jeden útok jako anomálii.

5.2 Rényiho entropie

Druhou entropií použitou při testování byla Rényiho entropie. Zvolena byla na základě nastavitelného parametru α a na podobnosti se Shannonovou entropií. V první části testování této entropie se určovala vhodná hodnota parametru α. Testovalo se celkem devět hodnot parametru α z intervalu, který byl zmíněn v kapitole 4. Výsledné hodnoty jsou uvedeny v grafu na obrázku 2. Předpokladem pro entropii bylo, aby dobře rozlišila jak velikost útoku tak i počet zdrojů. Podle definice entropie v kapitole 1 by měla křivka v grafu na obrázku 2 pro útoky z více než jednoho zdroje narůstat se zvyšujícím se počtem zdrojů a velikostí útoku. Pro útoky z jednoho zdroje by měla naopak entropie klesat s narůstající velikostí útoku. Obě tyto podmínky splňuje entropie jen v případě, pokud je parametr α nastaven na hodnotu $0,2$ nebo $0,4$. Pro druhou část testování byla vybrána hodnota $0,2$, protože při bližším porovnáním s hodnotou $0,4$ lépe rozlišovala nižší útoky od běžného datového provozu.

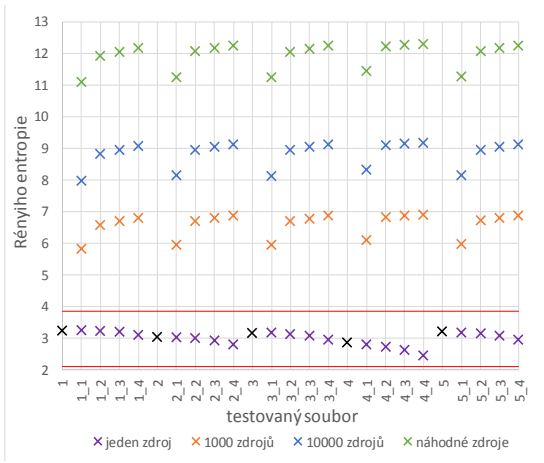
Druhá část testování probíhala stejně jako u Shannonovy entropie. Interval entropie definující běžný datový provozu byl vypočten v rozsahu od $2,1092$ do $3,8419$. Výsledné hodnoty Rényiho entropie pro testované soubory jsou uvedeny v grafu na obrázku 3. V případě útoků vedených z více jak jednoho zdroje dokázala Rényiho entropie spolehlivě

elektrorevue
ISSN 1213 - 1539



Obrázek 2: Výsledky Rényiho entropie pro různé hodnoty parametru α.

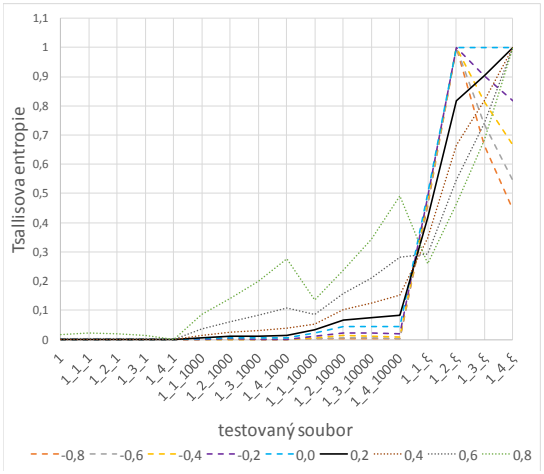
klasifikovat útoky jako anomálie. Pokud byly útoky vedeny z jednoho zdroje, nedokázala Rényiho entropie zařadit ani jeden útok mezi anomálie.



Obrázek 3: Výsledné hodnoty Rényiho entropie pro testované soubory s útoky.

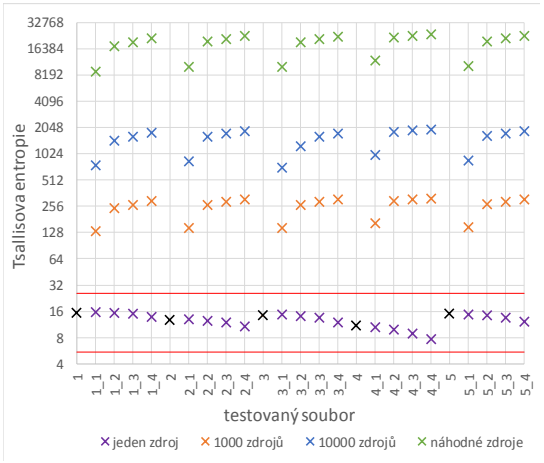
5.3 Tsallisova entropie

Poslední vybranou entropií byla Tsallisova entropie. Testování probíhalo velice podobně jako v případě Rényiho entropie. Stejně jako v případě Rényiho entropie bylo nutné v první částí zvolit vhodnou hodnotu nastavitelného parametru q. Hodnoty se volily z intervalu uvedeného v kapitole 4. Celkem bylo testováno devět hodnot parametru q. Výsledky pro všechny testované hodnoty jsou uvedeny v grafu na obrázku 4. Z testovaných hodnot parametru q vyhovovaly jen hodnoty $0,2$ a $0,4$. Ostatní hodnoty nesplňovaly stejné podmínky jako v případě testování Rényiho entropie. Pro následující část testování se po bližším porovnání vhodných hodnot parametru q jevila lépe Tsallisova entropie s nastaveným parametrem q na hodnotu $0,2$. S takto nastavenou hodnotou parametru q jsou výsledné entropie pro odlišné zdroje útoku dále od sebe a tedy lépe rozlišitelné.



Obrázek 4: Výsledky Tsallisovy entropie pro různé hodnoty parametru q.

V druhé části probíhalo testování stejně jako v případě předchozích dvou entropií. Interval entropie definující běžný síťový provoz se vypočetl v rozmezí od $5,5067$ do $25,7729$. Výsledné hodnoty entropií pro testované soubory jsou uvedeny v grafu na obrázku 5. Tsallisova entropie dokázala dobře rozlišit útoky vedené z více než jednoho zdroje. V případě, že byl útok veden z jediného zdroje nedokázala Tsallisova entropie zařadit útoky mezi anomálie a klasifikovala je jako běžný provoz.



Obrázek 5: Výsledné hodnoty Tsallisovy entropie pro testované soubory s útoky.

5.4 Zhodnocení zvolených entropií

V předchozích kapitolách 5.1, 5.2 a 5.3 byly prezentovány výsledky zvolených entropií. Z výsledků je patrné, že identifikace na základě Shannonovy entropie dopadla nejhůře

elektrorevue
ISSN 1213 - 1539

ze všech použitých entropií. O proti ostatním měla Shannonova entropie problém s identifikací malých útoků vedených z více zdrojů. Na první pohled vypadají výsledky Rényiho a Tsallisovy entropie v grafech na obrázcích 3 a 5 velmi podobně. Pro prezentování hodnot Tsallisovy entropie bylo v grafu na obrázku 5 použito logaritmické měřítko, protože hodnota Tsallisovy entropie narůstá exponenciálně se vzrůstající velikostí útoku. O proti tomu se hodnota Rényiho entropie zvětšuje lineárně se zvětšujícím se útokem. Při porovnání všech tří entropií klasifikuje nejlépe jednotlivé anomálie Tsallisova entropie. Všechny útoky více jak z jednoho zdroje, identifikovala jako anomálie s dostatečným odstupem od běžného datového provozu. Díky exponenciálnímu nárůstu hodnoty entropie při zvětšujícím se útoku dosahuje identifikace anomálií na základě Tsallisovy entropie lepších výsledků než při použití Rényiho entropie.

6 Závěr

Tento článek popisuje možnost využití entropie pro identifikaci anomálií v datové komunikaci. V kapitole 2 jsou popsány tři typy entropie, které jsou v následujících dvou kapitolách použity pro klasifikaci běžného datového provozu a identifikace anomálního provozu způsobeného DoS útokem. Následně jsou entropie porovnány, pro výběr nejvhodnější z nich, pro identifikaci anomálního provozu.

Výsledky pro testované entropie jsou uvedeny v grafech na obrázcích 1, 3 a 5. Z testování vychází, že metoda identifikace anomálií založená na entropii je vhodná v případech, kdy je více zdrojů anomálního provozu. Pokud byl anomální provoz veden jen z jednoho zdroje, výsledná hodnota entropie se pohybovala v hodnotách spadajících do běžného datového provozu. Při testování nastavitelných parametrů α a q u Rényiho a Tsallisovy entropie vycházely nejlepší hodnoty při shodně nastaveném parametru na hodnotu $0,2$. Z celkového výsledku testování zvolených entropií je patrné, že Rényiho a Tsallisova entropie by měly být schopné dobře identifikovat záplavové DDoS útoky.

Poděkování

Výzkum byl podpořen projektem GAČR 14-25298P „Research into cryptographic primitives for secure authentication and digital identity protection“.

Literatura

[1] MACKAY, David J. C. *Information theory, inference, and learning algorithms*. Cambridge: Cambridge University Press, 2003. ISBN 978-0-521-64298-9.

[2] COVER, T. M. a Joy A. THOMAS. *Elements of information theory*. 2nd ed. Hoboken, N.J.: Wiley-Interscience, c2006. ISBN 04-712-4195-4.

[3] SHANNON, C. E. A Mathematical Theory of Communication. *Bell System Technical Journal*. 1948, **27**(3), 379-423. DOI: 10.1002/j.1538-7305.1948.tb01338.x. ISSN 00058580.

[4] HAZEWINKEL, M. *Encyclopaedia of mathematics: an updated and annotated translation of the Soviet "Mathematical encyclopaedia"*. Norwell, Sold and distributed in the U.S.A. and Canada by Kluwer Academic Publishers, 1994. ISBN 15-560-8009-3.

[5] XU, Dongxin a Deniz ERDOGMUNS. *Renyi's Entropy, Divergence and Their Nonparametric Estimators*, 47. DOI: 10.1007/978-1-4419-1570-2_2.

[6] Renyi, A., On Measures of Entropy and Information, *Proc. 4th Berkeley Sympos. on Mathematical Statistics and Probability, Berkeley, CA, 1960*, Berkeley: Univ. of California Press, 1961, vol. 1: Contributions to the Theory of Statistics, 547-561.

[7] DAROONEH, Amir Hossein, Ghassem NAEIMI, Ali MEHRI a Parvin SADEGHI. Tsallis Entropy, Escort Probability and the Incomplete Information Theory. *Entropy*. 2010, **12**(12), 2497-2503. DOI: 10.3390/e12122497. ISSN 1099-4300.

[8] TSALLIS, Constantino. Possible generalization of Boltzmann-Gibbs statistics. *Journal of Statistical Physics*. 1988, **52**(1-2), 479-487. DOI: 10.1007/BF01016429. ISSN 0022-4715.

[9] WAGNER, A. a B. PLATTNER. Entropy Based Worm and Anomaly Detection in Fast IP Networks. *14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise (WETICE'05)*. IEEE, 2005, 172-177. DOI: 10.1109/WETICE.2005.35. ISBN 0-7695-2362-5.

[10] FEINSTEIN, L., D. SCHNACKENBERG, R. BALUPARI a D. KINDRED. Statistical approaches to DDoS attack detection and response. *Proceedings DARPA Information Survivability Conference and Exposition*. IEEE Comput. Soc, 2003, 303-314. DOI: 10.1109/DISCEX.2003.1194894. ISBN 0-7695-1897-4.

[11] LAKHINA, Anukool, Mark CROVELLA a Christophe DIOT. Mining anomalies using traffic feature distributions. *Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications - SIGCOMM '05*. New York, New York, USA: ACM Press, 2005, 217-228. DOI: 10.1145/1080091.1080118. ISBN 1595930094.

[12] BEREZIŃSKI, Przemysław, Bartosz JASIUL a Marcin SZPYRKA. An Entropy-Based Network Anomaly Detection Method. *Entropy*. 2015, **17**(4), 2367-2408. DOI: 10.3390/e17042367. ISSN 1099-4300.

[13] *Wireshark User's Guide* [online]. Lamping, Sharpe, Warnicke, c2004-2014 [cit. 2016-06-14]. Dostupné z: http://www.wireshark.org/docs/wsug_html/

[14] *Hping* [online]. Salvatore Sanfilippo, 2006 [cit. 2016-06-13]. Dostupné z: http://www.hping.org/