RATING ASSOCIATION FOR SHORT DEGREE DDOS ATTACK RECOGNITION

[1] Prof.C.Thangamalar [2] Dr.K.Ravikumar

[1]Research and Development Centre, Bharathiar University, Coimbatore 641046.
[2]Assistant Professor, Dept.of.Computer science, Tamil University Thanjavur, India

Abstract A short degree Distributed Denial of Service (DDoS) attack has the aptitude to opaque its traffic because it is most parallel to genuine traffic. It can effortlessly avoid present recognition tools. Rating association procedures can enumerate noteworthy variances among attack traffic and genuine traffic centered on their rating values. In this manuscript, we practice dual rating association procedures, namely, Quick Rating Association (QRA) and Fractional Rating Association (FRA) to recognize short -degree DDoS attacks. These procedures are empirically appraised using three real time datasets. Tentative outcomes display that both procedures can successfully categorize genuine traffic from attack traffic. We catch that FRA achieves better than QRA in recognition of short degree DDoS attacks in footings of positioning between malicious and genuine traffic.

Keywords: DDoS attack, short -degree, network traffic, rating association.

I. INTRODUCTION

With the rapid growth in the number of applications on Internet-connected computers and the devices and the rise in the sophistication of attacks on the application, early recognition of Internet-based attacks is essential to reduce damage to genuine user's traffic. A DDoS attack is a DoS attack that uses multiple distributed attack sources. Typically, attackers use a large number of compromised computers, also called zombies, to launch a DoS attack against a single target or multiple targets with the intention of making one or more services unavailable to intended users [4]. Botnets have become a powerful way to control a large number of hosts, allowing the launching of sophisticated and stealth DDoS attack on target host(s) quickly [3, 7].

In the recent past, botnets have become more intelligent and capable, and as a consequence the amount of attack traffic has increased targeting servers and components of Internet infrastructure such as firewalls, routers, DNS servers as well as network bandwidth. Regardless of how well secured the victim system may be, its susceptibility to DDoS attacks depends on the state of security in the rest of the global Internet [1, 10]. A lot of different tools are used by attackers to bypass security systems, and as a result, researchers have to upgrade their approaches to handle new attacks simultaneously. Some defense mechanisms concentrate on recognizing an attack close to the victim machine, because the recognition accuracy of these mechanisms is high. Network traffic comes in a stream of packets and it is difficult to distinguish genuine traffic from attack traffic. More importantly, the volume of attack traffic can be much larger than the system can handle. The behavior of network traffic is reflected by its statistical properties [13] because such properties summarize behavior. Association procedures can be used on the traffic summary to identify malicious traffic.

A network or host can be compromised with DDoS attacks using two types of traffic, namely, high-degree DDoS traffic and short -degree DDoS traffic. High-degree traffic is similar to flash crowd, i.e., when a large amount of unexpected genuine traffic comes to a smallest server, and on the other hand, short -degree traffic is similar to genuine traffic. So, it is

very difficult to identify and mitigate either type of DDoS attack within a short time period [2].

Association measurement is a measure that can be used to identify linear relationship between malicious and genuine traffic. In this manuscript, we attempt to use rating association to recognize short -degree DDoS attacks. We use, two rating association techniques, namely, QRA and FRA.

The rest of the manuscript is organized as follows: Section 2 provides related work and observations. Section 3 presents the recognition mechanism for short -degree DDoS attacks using rating association. Experimental results are reported in Section 4. Section 5 presents concluding remarks and future work.

II. RELATED WORK

A DoS attack is characterized by an explicit attempt to prevent the genuine use of a service [10]. A DDoS attack deploys multiple attacking entities to attain this goal. Much research has been devoted to the recognition of DDoS attacks [11]. Abliz et al. [14] propose a rating association based approach to recognize reflection DDoS attacks. Once suspicious flows are found, it estimates the rating association between flow pairs and generates a final alert according to preset thresholds. Angelo Furfaro et al. [12] discuss a measure based on Hurst measurement to recognize short -degree DDoS attacks. Alexandre et al. [2] present an empirical evaluation of the suitability of various information metrics to recognize both short -degree and high-degree DDoS attacks. Udi Ben-Porat [5] propose a covariance analysis model for recognizing SYN flooding attacks. The method can accurately recognize DDoS attacks with different intensities. It can also recognize DDoS attacks which are similar to genuine traffic. R.F.Fouladi [9] propose a light-weight software based approach for short - degree DoS (LDoS) attack Recognition, and integrated it with an existing intrusion recognition system. It does not require any change in existing infrastructure and protocol. Yao Zhang et al. [15] present a generalized information metric to recognize both short -degree and high-degree DDoS attacks. They consider the spacing between genuine traffic and attack traffic in terms of an information distance measure. We observe the following based on literature survey.

- Although a large number of methods have been introduced to recognize high-degree DDoS attacks, the number of methods to recognize short -degree DDoS attacks is small. Most methods to recognize short -degree DDoS attacks suffer from significant large percentage of false alarms.
- Most published recognition methods, attempt to recognize at the packet level for short -degree DDoS attacks. Though

  Net Flow traffic analysis is faster than packet level

  analysis.

III. RATING ASSOCIATION FOR SHOR -DEGREE DDOS ATTACK RECOGNITION

Rating association has been found suitable as a potential metric to differentiate genuine traffic from attack traffic [14]. Short -degree attacks exploit TCP retransmission time-out (RTO) to slowly reduce network throughput. An attacker causes genuine TCP flow by entering the RTO state repeatedly. In a compromised host, it reduces the throughput significantly also reducing the bandwidth of the network simultaneously. A short -degree DDoS attack strategy is given in Figure 1. is the total time interval for a period. indicates the height of the attack burst, i.e., the strength of the attack traffic and represents the burst length that indicates the pulse width. is the time interval between two consecutive attack pulses, i.e., RTO + 2 round trip time (RTT). is the interval between two pulses of high-degree traffic, i.e., genuine traffic, , , and finally , , are the high-degree attack traffic pulses towards a target from common effort of different attackers. The average volume of attack traffic can be calculated as ∗ / , which is much less than the genuine TCP traffic [8]. So, it is difficult to recognize attack traffic within short interval of time. In this work, two procedures are used to recognize short-degree DDoS attack, namely, Quick rating association and Fractional rating association. Table 1 describes the symbols used to describe the method.

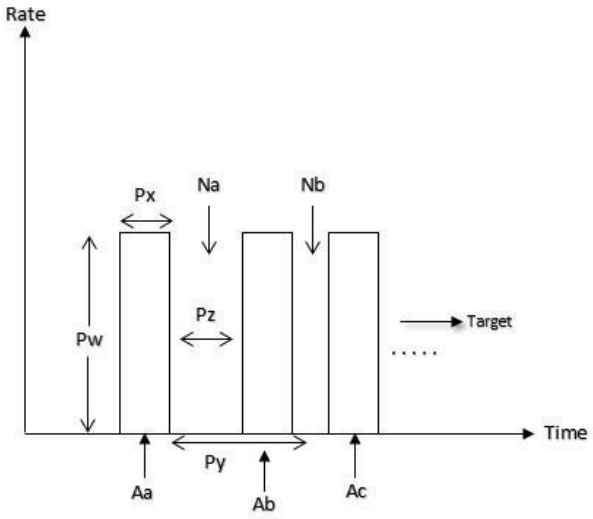

Figure 1: A low-rate DDoS attack strategy

3.1 Quick Rating Association

Quick's association measurement (QRA) procedures the strength of association between two random variables better [14]. Quick rating association measurement between two random variables X and Y is computed as

$$r_{X,Y} = \frac{E(X,Y) - E(X)E(Y)}{\sqrt{E(X^2) - E^2(X)}\sqrt{E(Y^2) - E^2(Y)}} \quad (1)$$

The measurement , is the covariance value normalized by standard deviation, and is the expected value. The use of rating measure association using characteristics that cannot be expressed quantitatively but that lend themselves to being rated. A perfect linear relationship between the rating s yields a rating association measurement of +1 for positive relationship (or -1 for a negative relationship) and no linear relationship between the rating s yields a rating association measurement of 0.

Table 1: Symbol used

Symbols	Definition
P	Period break for processing
Pw	Strength of the attack traffic
Py	Burst length that indicates pulse width
Px	Time interval between two consecutive attack pulse
Pz	Interval between two pulses of high-degree traffic
Na, *Nb*	Genuine traffic
Aa, *Ab*, *Ac*	High-degree attack traffic
ti	I^{th} time interval within
xi	I^{th} instance within *x*
	Threshold for attack recognize
S	Sample traffic
N	Total number of packets within full time interval
N	Represents number of packets within the smaller time interval within

3.2 Fractional Rating Association

Fractional rating association (FRA) computes association between two random variables keeping one or more variables constant. The Fractional association between and with a given set of n controlling variables = 1, 2, 3, ... , written as , , is the association between residual and resulting from the linear regressions of with and of with, respectively [6].

$$r_{xy.z} = \frac{r_{xy} - r_{xz}r_{yz}}{\sqrt{(1 - r_{xz}^2)(1 - r_{yz}^2)}} \quad (2)$$

Where denotes the association between and with constant. The rating association measurement values vary from -1 to +1, where +1 indicates complete linear relationship, -1 indicates a negative linear relationship and 0 indicates no relationship. Fractional association is a measure of the degree of association between two random variables keeping the third variable constant. The steps for rating association based short -degree DDoS attack recognition method is reported in Algorithm 1.

As stated in Algorithm 1, the sample period P considered for experimentation is divided into n intervals with, being the total time interval. Three different network traffic instances, namely, , , and are considered. Rating association measurement is calculated for each sample using Equation (1) or (2) within a sampling period P of the ith sample based on source IP, destination IP and protocol. If the rating association of and is

greater than threshold ≥ δ1 or rating association of , , is greater than threshold ≥ δ2, an alarm will be generated, else the router will send the packet to the next level of routers.

Algorithm 1: The short-degree DDoS attack reorganization

Input: x represents network traffic with respect to time window

P and thresholds δ1 and δ2.

Output: alarm information (attack or genuine).

Step.1: Initialization: sample period = $_1$, $_2$, $_3$, … . where N is the full time interval. , , Represent three different network traffic instances

Step.2: sample the network traffic x received from upstream router R based on sampling period P

Step.3: Compute rating association measurement using Equation (1) or (2) for each sample within P sampling period of ith sample based on traffic features (i.e., source IP, destination IP and protocol).

Step.4: Check whether (,) ≥ δ_1 or (,) ≥ δ_2, if so generate alarm; otherwise, router sends the packets to the next level routers. 5) go to Step 2.

3.3 Complexity Analysis

Both Quick rating association and Fractional rating association work in quadratic time, (^{2}), where n is the number of traffic instances within a sample, P is the time interval. Though the complexity is high the rating association reveals that:

1) It can discriminate genuine traffic from attack traffic correctly.
2) FRA can significantly identify short -degree DDoS attack with high linear association value.

IV. EXPERIMENTAL ANALYSIS

In this section, experimental results are presented for both the rating association procedures using benchmark datasets.

4.1 Datasets

The evaluation of any recognition method is extremely important before deployment in a real-time network. Two different datasets are used, namely: (i) MIT Lincoln Laboratory and (ii) CAIDA DDoS 2007 dataset. The MIT dataset contains pure genuine traffic in tcp dump format. It does not contain any attack traffic. Even though it is old it is still useful and widely used [11]. The CAIDA DDoS 2007 dataset contains 5 minutes of anonymized traffic from a DDoS attack on August 4, 2007. This traffic trace contains only traffic to the victim and responses from the victim. If more than 10,000 attack packets per second are forwarded to the victim machine, it is known as high-degree attack traffic [11]. If up to 1000 attack packets per seconds are forwarded to the victim machine, it is considered short -degree attack traffic [11]. So, short -degree attack may be similar in nature with genuine traffic.

4.2 Results

Initially the total time interval is splits into 10 second subintervals. Three packet attributes are used during the experiment, namely, source IP, destination IP and protocol. For a victim-end based recognition system, source IP is important, especially to find source hosts even though they may be spoofed. The destination IP is also important to identify and to estimate the traffic flowing to a particular target. The attribute protocol is added to identify the attack type. Each sample is processed one at a time. The rating association measure is applied to find the linear relationship between genuine and attack traffic.

Figures 2 and 3 show the probability density of genuine and attack traffic when using the MIT dataset as genuine traffic and the CAIDA dataset as attack traffic. Following Yao Zhang et. al [15], the MIT dataset is considered genuine traffic in our experiment. Quick rating association and Fractional rating association are computed on the two different datasets, namely, MIT genuine and CAIDA attack dataset. These attack traffic instances are assumed to satisfy the short -degree attack properties. Results for both genuine and attack traffic instances are reported for both rating association procedures in Figures 4, 5, and 6 for FRA and 7, 8 and 9 for QRA.

Association values for genuine traffic and attack traffic are reported in Table 2. While using Quick rating association and Fractional rating association, Figures 10 and 11 report results for mixed traffic (i.e. both genuine and attack traffic). We see that FRA can discriminate effectively genuine traffic from attack traffic with rating association with min = 0.9 and max = 1.1. Figure 10 reports the attack and genuine traffic rating values when using QRA and FRA. Figure 11 shows the spacing between genuine traffic and attack traffic when using QRA and FRA. It seems that FRA has higher spacing than QRA. Better results are observed for those ranges of rating association values and are reported in Table 2, when recognizing short -degree DDoS attacks.

Table 2: Ranges of association values

Rating Associations	Traffic Type	Minimum	Maximum
FRA	normal-normal	-0.3	1.1
QRA	normal-normal	-2.4	1.0
FRA	attack-attack	1.0	1.1
QRA	attack-attack	0.99	1.1
FRA	normal-attack	-0.2	1.1
QRA	normal-attack	-2.9	1.0

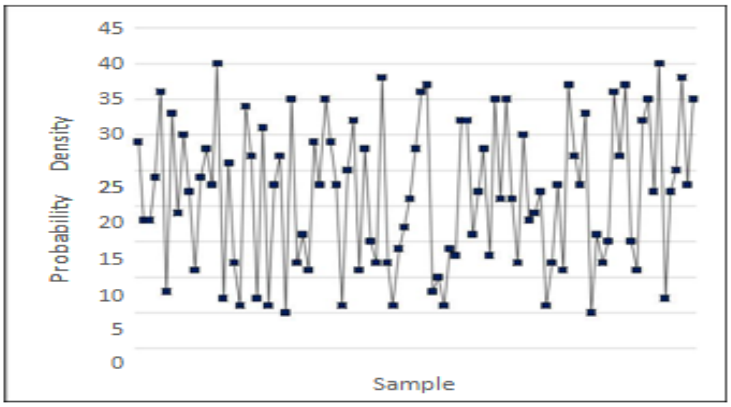

Figure 2: Probability density for legitimate traffic

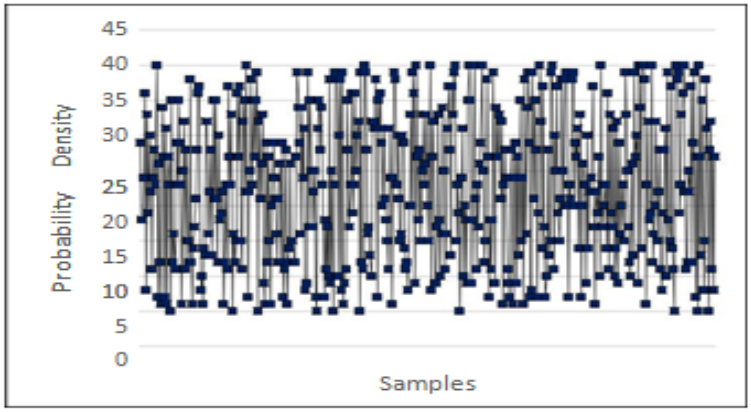

Figure 3: Probability density for attack traffic

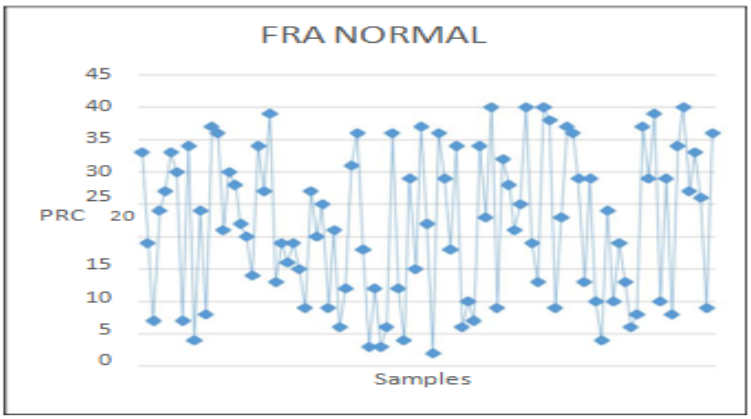

Figure 4: Fractional Rating Association for legitimate traffic

4.3 Discussion

Based on the analysis, we make the following observations.

- QRA uses a small number of parameters to estimate rating association.

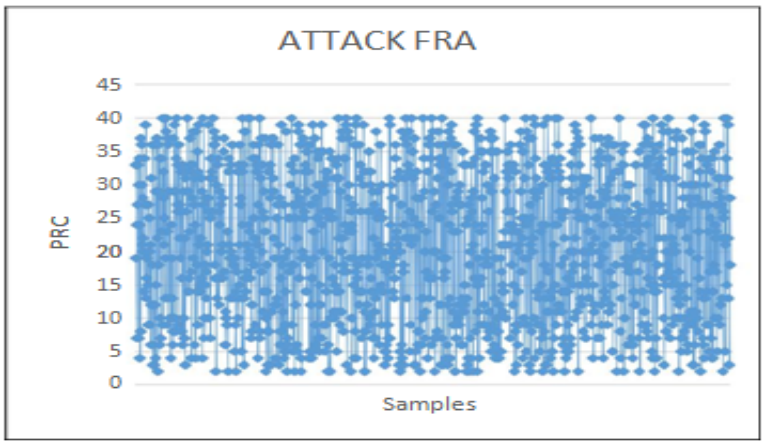

Figure 5: Fractional Rating Association of attack traffic

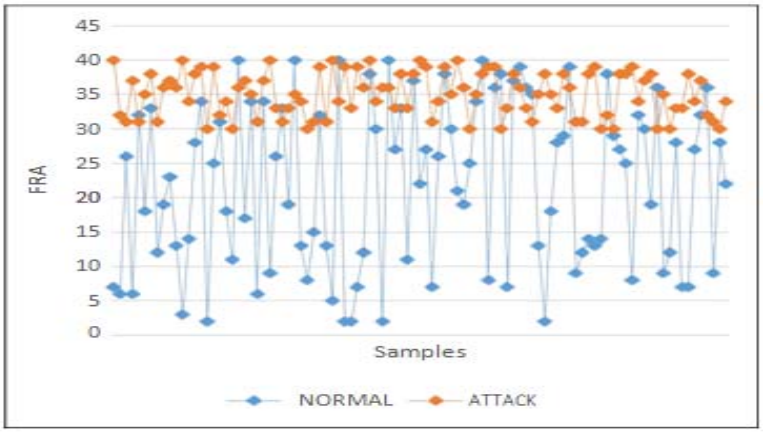

Figure 6: Fractional Rating Association of legitimate and attack traffic

- Both association procedures are capable of differentiating using QRA and FRA genuine traffic from malicious traffic correctly.
- The Fractional rating association measure is effective in reducing false alarms Victim end defense system.
- It is due to higher spacing between genuine and attack traffic.

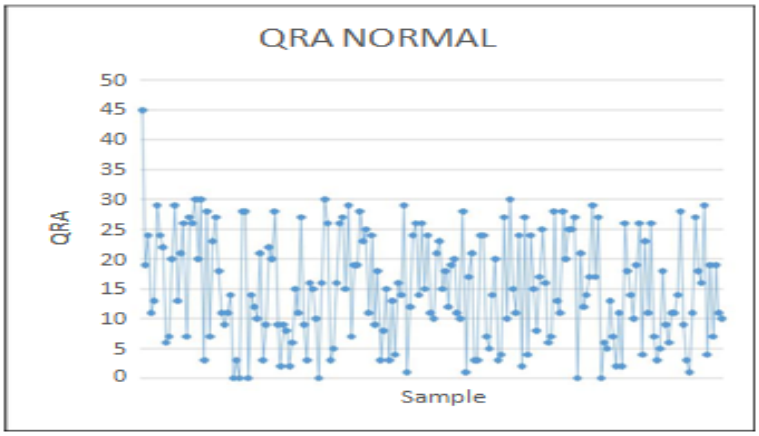

Figure 7: Quick Rating Association for legitimate traffic

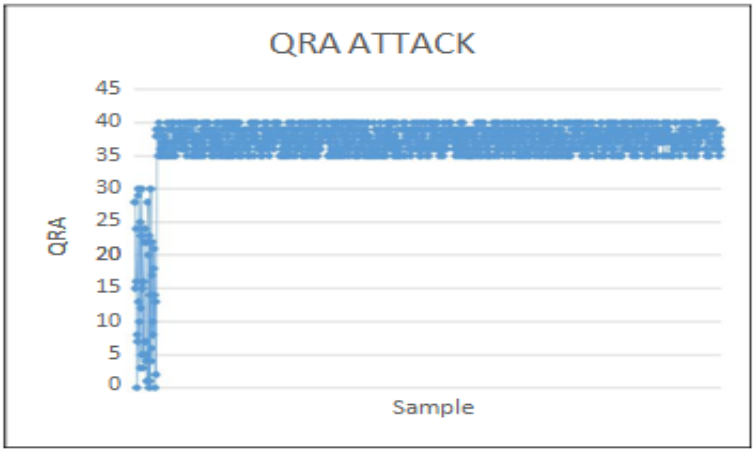

Figure 8: Quick Rating Association for attack traffic

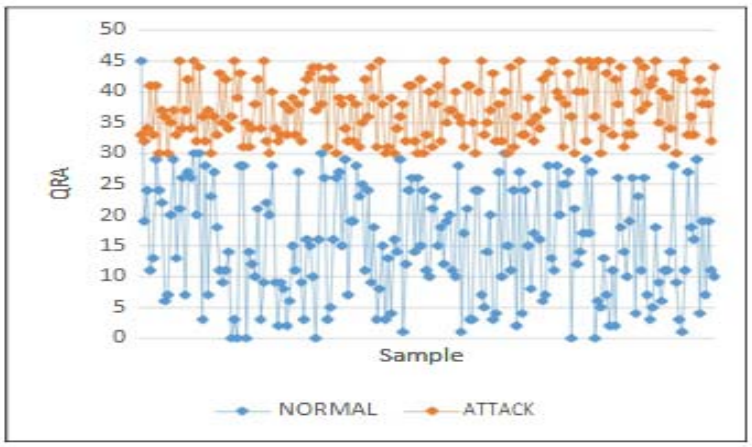

Figure 9: Quick Rating Association of legitimate and attack

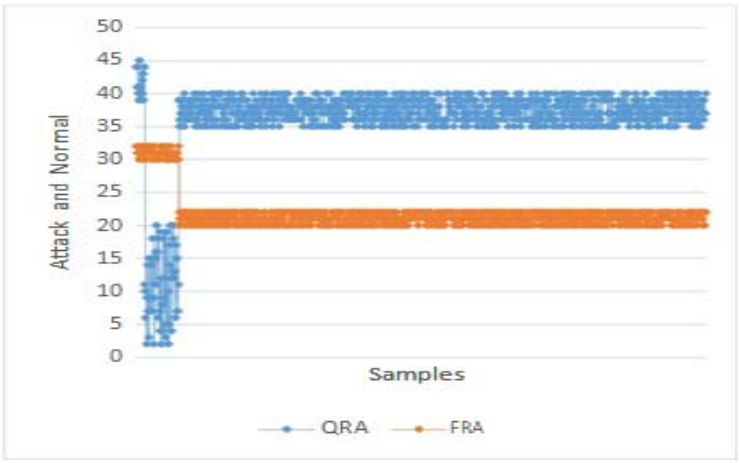

Figure 10: Rating Association for attack and legitimate traffic using QRA and FRA

Figure 11: Shows difference between QRA and FRA

V. CONCLUSION

In this manuscript, we have presented an empirical study of rating association used to recognize short -degree distributed DoS attacks. FRA and QRA both are used to effectively differentiate genuine traffic from malicious traffic. Our experimental study, show that FRA is more effective than QRA in differentiating genuine traffic from attack traffic. Development of a trace back mechanism to support short - degree DDoS attack is underway.

REFERENCES

[1] Yao Zhang, Zhiming Zheng, Lijia Xie & Xiao Zhang, "DRDP: A DDoS-Resilient Data Pricing Mechanism", in IEEE Communications Letters, Volume: 20, Issue: 9, PP: 1752 – 1755, Sept. 2016
[2] Alexandre A. Amaral, Leonardo S. Mendes, Eduardo H. M. Pena, Bruno B. Zarpelão & Mario Lemes Proença, "Network Anomaly Detection by IP Flow Graph Analysis: A DDoS Attack Case Study", in Chilean Computer Science Society (SCCC), 2013 32nd International Conference of the PP: 11-15, Nov. 2013
[3] Shui Yu, Yonghong Tian, Song Guo & Dapeng Oliver Wu, "Can We Beat DDoS Attacks in Clouds?", in IEEE Transactions on Parallel and Distributed Systems Volume: 25, Issue: 9, PP: 2245 – 2254, Sept. 2014
[4] Shui Yu, Wanlei Zhou, Weijia Jia, Song Guo, Yong Xiang & Feilong Tang, "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient", in IEEE Transactions on Parallel and Distributed Systems Volume: 23, Issue: 6, PP: 1073 – 1080, June 2012
[5] Udi Ben-Porat, Anat Bremler-Barr & Hanoch Levy, "Vulnerability of Network Mechanisms to Sophisticated DDoS Attacks", in IEEE Transactions on Computers Volume: 62, Issue: 5, PP: 1031 – 1043, May 2013
[6] Jingtang Luo, Xiaolong Yang, Jin Wang, Jie Xu, Jian Sun & Keping Long, "On a Mathematical Model for Low- Rate Shrew DDoS", in IEEE Transactions on Information Forensics and Security Volume: 9, Issue: 7, PP: 1069 – 1083, July 2014
[7] Saurabh Verma, Ali Hamieh, Jun Ho Huh, Henrik Holm, Siva Raj Rajagopalan, Maciej Korczynski & Nina Fefferman, "Stopping Amplified DNS DDoS Attacks through Distributed Query Rate Sharing", in Availability, Reliability and Security (ARES), 2016 11th International Conference on, Sept. 2016
[8] Kamal Alieyan, Mohammed M. Kadhum, Mohammed Anbar, Shafiq Ul Rehman & Naser K. A. Alajmi, "An overview of DDoS attacks based on DNS", in Information and Communication Technology Convergence (ICTC), 2016 International Conference on PP: 19-21, Oct. 2016
[9] Ramin Fadaei Fouladi, Cemil Eren Kayatas & Emin Anarim, "Frequency based DDoS attack detection approach using naive Bayes classification", in Telecommunications and Signal Processing (TSP), 2016 39th International Conference on PP: 27-29, June 2016
[10] Vincenzo Matta, Mario Di Mauro & Maurizio Longo, "Botnet identification in randomized DDoS attacks", in Signal Processing Conference (EUSIPCO), 2016 24th European, Sept. 2016
[11] Danish Sattar, Ashraf Matrawy & Olufemi Adeojo, "Adaptive Bubble Burst (ABB): Mitigating DDoS attacks in Software-Defined Networks", in Telecommunications Network Strategy and Planning Symposium (Networks), 2016 17th International, Sept. 2016
[12] Angelo Furfaro, Giovanna Malena, Lorena Molina & Andrea Parise, "A Simulation Model for the Analysis of DDoS Amplification Attacks", in Modelling and Simulation (UKSim), 2015 17th UKSim-AMSS International Conference on, PP: 25-27, March 2015
[13] Z.Tsiatsikas, A.Fakis, D.Papamartzivanos, D.Geneiatakis, G.Kambourakis & C.Kolias, "Battling against DDoS in SIP: Is Machine Learning-based detection an effective weapon?", in e-Business and Telecommunications (ICETE), 2015 12th International Joint Conference on, PP: 20-22, July 2015
[14] Mehmud Abliz & Taieb F. Znati, "Defeating DDoS using Productive Puzzles", in Information Systems Security and Privacy (ICISSP), 2015 International Conference on, PP: 9-11, Feb. 2015
[15] Yao Zhang, Zhiming Zheng, Lijia Xie & Xiao Zhang, "DRDP: A DDoS-Resilient Data Pricing Mechanism", in IEEE Communications Letter (Volume: 20, Issue: 9, PP: 1752 - 1755 Sept. 2016).