Improving Learning Skills in Detection of Denial of Service Attacks with Newcombe - Benford's Law using Interactive Data Extraction and Analysis

Kemal Hajdarevic [1], Colin Pattinson [2], Ingmar Besic [1]

[1] *Faculty of Electrical Engineering, University of Sarajevo, Bosnia and Herzegovina*
[2] *Leeds Beckett University, UK*

Abstract **– Denial of Service attacks and the distributed variant of this type of attack called DDoS are attack types which are easy to start but hard to stop especially in the DDoS case. The significance of this type of attack is that attackers use a large number of packets usually created with programs and scripts for creating specially crafted types of packets for different types of attack such as SYN flood, ICMP smurf, etc. These packets have similar or identical attributes such as length of packets, interval time, destination port, TCP flags etc. Skilled engineers and researchers use these packet attributes as indicators to detect anomalous packets in network traffic. For fast detection of anomalous packets in legitimate traffic we proposed Interactive Data Extraction and Analysis with Newcombe-Benford power law which is able to detect matching first occurrences of leading digits – size of each packet that indicate usage of automated scripts for attack purposes. Power law can be used to detect the same first two, three, or second digits, last one or two digits in data set etc. We used own data set, and real devices.**

Keywords **– DoS, Newcombe-Benford law, RMON, SNMP, MIB**

DOI: 10.18421/TEM112-05
https://doi.org/10.18421/TEM112-05

Corresponding author: Kemal Hajdarevic,
Faculty of Electrical Engineering, University of Sarajevo, Bosnia and Herzegovina.
Email: khajdarevic@etf.unsa.ba

Received: 10 February 2022.
Revised: 03 April 2022.
Accepted: 09 April 2022.
Published: 27 May 2022.

1. Introduction

Cyber security company Kaspersky [1] announced in 2022, on its web site that the total number of Distributed Denial of Service DDoS attacks was increased by 24% in Q3 of 2021 compared to the same period of the previous year – Figure 1. While the number of total smart DDoS attacks was increased by 32%.

Figure 1. Increased number of DDoS attacks reported by Kaspersky [1]

DoS type attacks have similar characteristic which is that victim system is attacked with high volume of bogus traffic. Attackers can randomly change traffic payload and make harder to detect this type of malicious traffic. This type of traffic can have other indicators which can be used to detect this type of attacks using already well known mathematical laws such as Newcombe-Benford's law [2] explained below.

1.1. Related Work

This phenomenon was documented in previous work [3] where it was reported that SYN packet inter arrival times conformed to Benford's law. Work done by [4] packet length could be used to detect anomalies because it also follows Newcombe-Benford- law [5], [6]

Simon Newcombe [5] in 1881 discovered that number 1 as first digit in datasets appears more frequently than other numbers and that occurrences of other numbers decrease more as they are closer to number 9. Newcombe [6] used logarithmic tables and explained his discovery by observing that in a physical logarithmic paper book the first pages were far more worn than the later pages [5]. In 1938 Frank Benford [6] rediscovered the same phenomenon in observations that percentage of times the natural numbers 1 to 9 are used as first digits in numbers related to rivers area, population, pressure, post addresses and similar follows the logarithmic relation [4]:

$$F_a = \log\left(\frac{a+1}{a}\right) \quad (1)$$

Where Fa is the frequency of the digit a in the first place of used numbers i.e., a= 1, 2, 3,…9.

Mahyar and Khosrow [7] presented a table (Table 1.) of the distribution of number occurrences based on Banford-Newcombe law [5], [6].

Table 1. First digit occurrence distribution

Digit	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
	0.301	*0.176*	*0.125*	*0.097*	*0.079*	*0.067*	*0.058*	*0.051*	*0.046*

For the sake of better visualization, the above table content is presented in bar chart graph below Figure 2. *Newcombe-Benford power distribution law*:

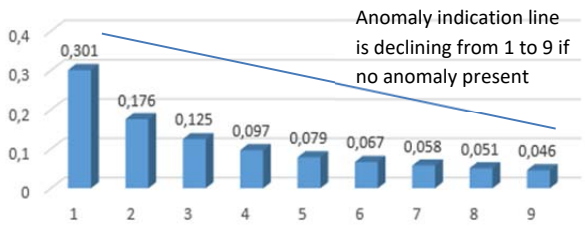

Figure 2. Newcombe-Benford power distribution law

Applying the Newcombe-Benford law, Benford [6] stated that any deviation of digit frequency from observed collected data is considered as anomalous. This phenomenon is used in banking industry by auditors and law enforcement agencies as a tool to detect potential fraud, or to detect:

"falsified numbers in tax returns, invoice payment records, expense account claims, and many other settings often display patterns that aren't present in legitimate records" [7].

Thus the Newcombe-Benford law is used in many areas of professional engagement, including computer and network operations to detect anomalous behavior. We found recent research work [3], [4], [8] where Newcombe-Benford law is used in the information security management process, more specifically for accurate detection of anomalies and attacks in computer communication network flows.

Newcombe-Benford law used for DoS detection in below published papers – shown in Table 2. below:

Table 2. Work related to DoS to Newcombe-Benford law

Indicator - Type of traffic	Published work
SYN packet inter arrival times	[3], [8]
Packet length, TCP traffic flow (src_bytes, dst_bytes[9])	[4] [9]

2. Rationale for Deciding to use Interactive Data Extraction and Analysis Software, Packet Size as Indicator of Attack on Real Network Segment

In above referenced papers [3], [4], [8] are presented approaches to detect anomalous behavior in network traffic flows based on frame length. Research papers [8], [9], [10] reveal that attacking packets had the same or similar packet sizes due to usage of tools intended for scanning and attacking which create customized packets with specific length and flags. In the referenced paper, the researchers used specially made software where Newcombe-Benford law was used. Knowing that producing software for gathering the same results can be challenging and time consuming we decided to search for off the shelf software that can be used for improving Denial of Service Attacks detection skills. It is well known that maximum Ethernet frame can be up to 1518 Bytes in length [14] and minimum 64 Bytes [15].

Special crafted packets are used by attackers [16] in reconnaissance phase to detect victim's operating systems and hardware to gain information which later will be used in attacking phase to conquer attacked system. Specially crafted packets can be used in exploitation, reinforcement, consolidation or pillage phase to steal data or to block a target system from providing legitimate services to their users. As referenced above, similar or same frame / packet size are crafted using programs and scripts to produce large amount of traffic that results into DoS type of attack. This type of network traffic behavior is detectable by automated software by examining and searching for signs of large numbers of the same or similar frame / packet sizes that differ from usual and legitimate network traffic.

2.1. Rationale for Using Interactive Data Extraction and Analysis for Denial of Service Attacks in Education Purposes and for Improving Skills in Attack Detection

In this paper we present an approach for using off the shelf Interactive Data Extraction and Analysis (IDEA) [17] software to assist in detecting DoS attack for free in network flows.

This paper presents a simple approach for quick result presentation. Preparation and data usage is straightforward because no additional time is needed for coding or scripting because Newcombe-Benford law tool is already present in IDEA and for free of charge it is possible to spot DoS attack in 1000 packets. To make more representative tests we used the commercial version and tested traffic that contains DoS malicious traffic and traffic that mostly contains legitimate traffic with more than million packets and then we compared the results.

2.2. Rationale to use Frame Size as an Indicator for Malicious Behavior

Attackers use reconnaissance scripts for scanning purposes to automate and speed the process of detecting vulnerabilities in a victim's systems. They also can start DoS type of attacks using scripts that produce large number of same or similar packet sizes usually without user data in packets with flags that are used such as SYN flood attack [10], [11] to overwhelm the links of attacked resources.

A TCP frame with no TCP payload, and no TCP or IP options, sent over IPv4 over Ethernet, has a 14-byte Ethernet header, a 20-byte IPv4 header, and a 20-byte TCP header, for a total of 54 bytes. When it's transmitted on the Ethernet, it is padded to a minimum of 60 bytes, and has a 4-byte CRC appended to it.

Hping3 and nmap can be used to specify frame size length sent to targeted system that can be recorded with Wireshark and analyzed with IDEA. Knowing the size of user data and 54 bytes of mandatory size TCP segment it is clear that a frame on the wire will be 54 bytes plus additional user data specified in Hping3, this is easy searchable in IDEA as shown below.

2.3. Rationale to Use Real Hardware

We decided to use real hardware and software which can be performed in simulation environments such as GNS3 or other simulation environments. Our decision to use real hardware was due to the nature of DoS attacks that tend to overwhelm resources. These are typically limited in simulated environments, so using real hardware brings our experiments closer to real situations.

3. Hardware and Software Used and Experiment Configuration

We used Cisco hardware components and software available online such as Wireshark, Nmap and commercially available DEA.

3.1. Software Used

Ireasoning MIB Browser with SNMP Browser and SNMP Trap receiver are available on [19], Wireshark available on [20], CaseWare IDEA available on [17], nmap available on [12] and hping3 [13].

3.2. Hardware Used

Cisco SG250-18 [21] 18-Port Gigabit Smart Switch, Wireless access point, one server and three PCs – Figure 3.

3.3. Hardware Configuration of Active Network Components for Experiments

We set up a network environment isolated from other networks but connected to the Internet via 192.168.1.100 wired / wireless router as shown below in Figure 3. Our network segment was established with Cisco SG259-18 Gigabit Smart Switch which is capable to collect RMON statistics that include frame size information among other useful information. This switch is able to use SPAN port that directs traffic from chosen ports which are the object of monitoring to one SPAN port on which a computer with Wireshark or software is used to capture traffic.

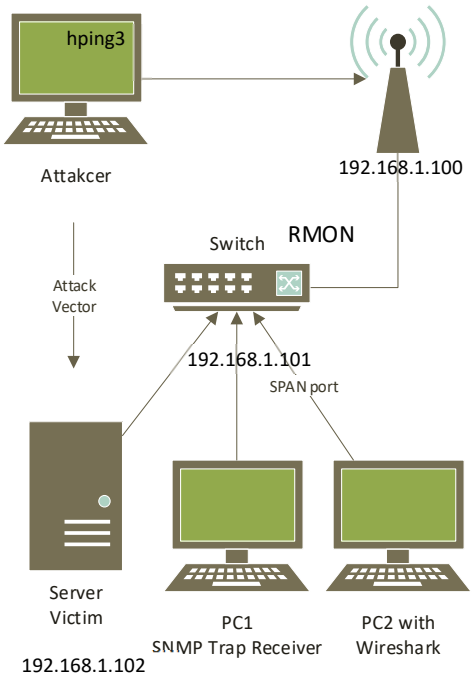

Figure 3. Testbed network environment SPAN port configuration

To be able to collect network traffic on a single port from selected ports we used SPAN port as shown in Figure 4. and Figure 5.

Figure 4. Receiving SPAN port configuration

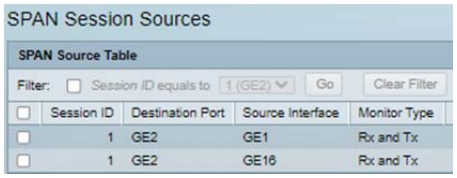

Figure 5. Monitored SPAN ports configuration

3.4. Attacking Hping3 Software Configuration for Experiments

We used *hping3* for scanning and DoS attacks by using different options or flags that informs applications how (specific length of packet, TCP flag types, etc.) packets will be formed to be sent over network.

We used nmap scanning tool and hping3 to produce large amount of SYN packets to simulate SYN DoS attacks similar as DoS and DDoS tools would produce.

We used Wireshark tool to capture whole packets - a similar approach was used by [3], [4], [8].

We used CaseWare IDEA software and built in Newcombe-Benford law analyzer tool to analyze captured data.

We configured Hping3 to be used for DoS attack against a victim with IP address 192.168.1.102, destination port was 139, window size was 64, type of traffic was flood with spoofed IP addresses defined with flag rand-source. Packets are 120 bytes of data and frame size on wire was 174 bytes (120 user data and 54 bytes of TCP and Ethernet data previously explained):

hping3 -c 100000 -d 120 -S -w 64 -p 139 - -flood - -rand-source 192.168.1.102

4. Experiment Results

Every Ethernet frame that carries TCP segments has 20 Bytes of TCP header + 20 Bytes IP header + 14 bytes Ethernet header which is 54 bytes in total plus additional user data as it is explained in section 2.2 Rationale to use frame size as an indicator for malicious behavior.

4.1. Scanning Results

Below are lines of traffic captured by Wireshark that was generated by hping3:

Spoofed address coming from attacker

6402","20.703931","21.182.189.225","192.168.1.102","NBSS","174" ","NBSS Continuation Message"

Attacked address

"6403","20.703932","21.182.189.225","192.168.1.102","TCP","174","", "[TCP Out-Of-Order] 3101 > 139 [SYN] Seq=0 Win=64 Len=120"

Generated hping3 TCP traffic provoke TCP retransmissions to spoofed address 21.182.189.225 from victim IP address 192.168.1.102 as shown below:

Attacked address sent retransmissions to spoofed asddress

"6404","20.704358","192.168.1.102","21.182.189.225","TCP","60","," 139 > 3101 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460"

"6405","20.704359","192.168.1.102","21.182.189.225","TCP","60","","[TCP Out-Of-Order] 139 > 3101 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460"

"11484","21.719987","192.168.1.102","21.182.189.225","TCP","60","", "[TCP Retransmission] 139 > 3101 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460"

"11485","21.719988","192.168.1.102","21.182.189.225","TCP","60","", "[TCP Retransmission] 139 > 3101 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460"

"26502","23.719946","192.168.1.102","21.182.189.225","TCP","60","", "[TCP Retransmission] 139 > 3101 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460"

"26503","23.719947","192.168.1.102","21.182.189.225","TCP","60","", "[TCP Retransmission] 139 > 3101 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460"

"41838","27.721974","192.168.1.102","21.182.189.225","TCP","60","", "[TCP Retransmission] 139 > 3101 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460"

"41839","27.721974","192.168.1.102","21.182.189.225","TCP","60","", "[TCP Retransmission] 139 > 3101 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460"

"57732","35.724210","192.168.1.102","21.182.189.225","TCP","60","", "[TCP Retransmission] 139 > 3101 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460"

"57733","35.724210","192.168.1.102","21.182.189.225","TCP","60","", "[TCP Retransmission] 139 > 3101 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460"

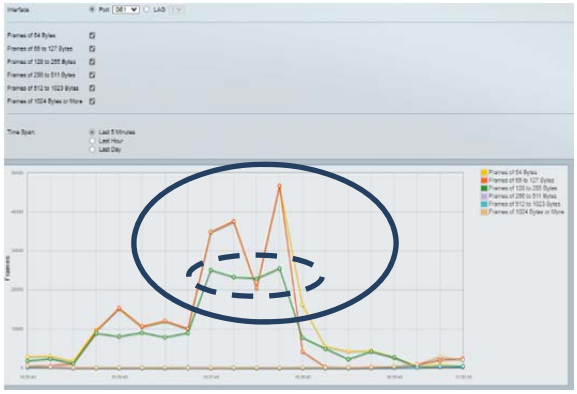

Figure 6. Attack periods circled in oval

4.2. RMON Statistics

To gain a better understanding of the generated traffic on a network where Hping3 has initiated communication that produced large amount of retransmissions, we used RMON statistics.

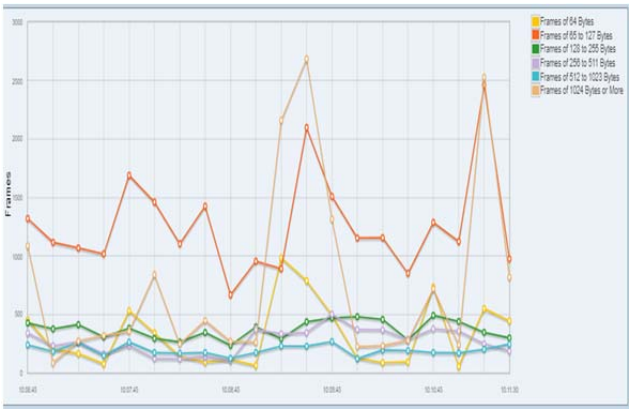

Figure 7. Legitimate traffic

RMON collects data of network flows for frames of 64 Bytes, 64 to 127 bytes, 128 to 256 Bytes which are the relevant for our research results. In Figure 6. above is shown the attack traffic (64 Bytes, 64 to 127 bytes, 128 to 256 Bytes) and where initiating traffic is circled in dashed oval and retransmissions are circled in oval with continuous line.

In Figure 7. is shown the legitimate traffic flow with more different types of length traffic compared to Figure 6.

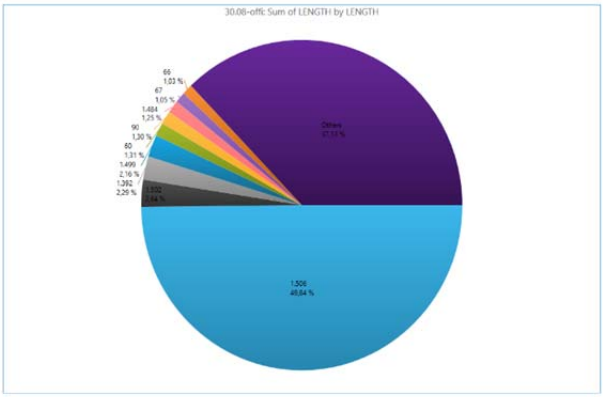

Figure 8. Frame length count - Legitimate traffic

4.3. Validation Results Obtained from Newcombe-Benford Law Using IDEA Software

The figures above show that most packets categorized as suspicious by Newcomb-Benford law analyzer tool are those arriving form attacker host generated with *Hping3* tool. Another conclusion that is clear from Newcombe-Benford law is that a result graph for the first two digits test gives the most accurate detection of anomalous behavior.

Captured network traffic was then converted to an excel file to be manually imported to IDEA software. The IDEA software was used to import data and analyzed by Newcombe-Benford law which offers different test types. With the IDEA it is possible to analyze traffic files that contain 1000 packets in free of charge version of the IDEA software, and in commercial version it is possible to analyze 2,147,483.647 of packets [16]

Figure 10. shows result of regular web browsing activity where the IDEA, using Newcombe- Benford law, didn't recognize significant anomalies.

4.4. Traffic Analysis of Hping3 Generated Traffic

We captured and analyzed 1,048.575 frames that mostly contain legitimate traffic – Figure 8. where almost 50 % of traffic has more than 1500 length frames.

Knowing that 1518 is maximum frame length it is understandable that this indicates real legitimate traffic.

We captured and analyzed 1,289.095 frames that contain legitimate and DoS malicious traffic – Figure 9.

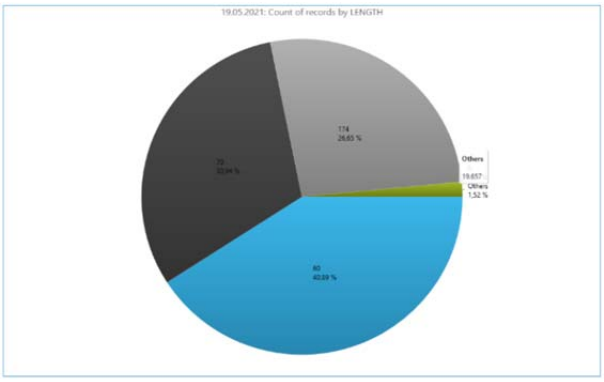

Figure 9. Frame length count - Malicious and Legitimate traffic

From the above figures (Figure 8. and Figure 9.) it can be seen that legitimate traffic contains mostly packets closer to maximum frame size than frames in Figure 9. with high amount of malicious frames.

From Figure 9. it can be seen that most frames were of 174 bytes length (Hping3 option *-d 120* for 120 bytes plus 54 bytes of headers and trailer*)*, than 60 bytes in length (it can be seen from section *4.1 Scanning results* that for two initiated sessions from attackers spoofed source, victim replied with 10 retransmissions with frames of 60 bytes, because operating system deleted 4 CRC bytes).

Frames with 70 bytes were router sends destination unreachable because of unavailability of spoofed addresses:

"296701","132.899336","192.168.1.100","192.168.1.102","ICMP","70","","Destination unreachable (Host unreachable)"

Or resends due to traffic type filtered by remote firewall, as shown below.

"7158","20.861130","188.110.122.44","192.168.1.102","ICMP","70","","Destination unreachable (Communication administratively filtered)"

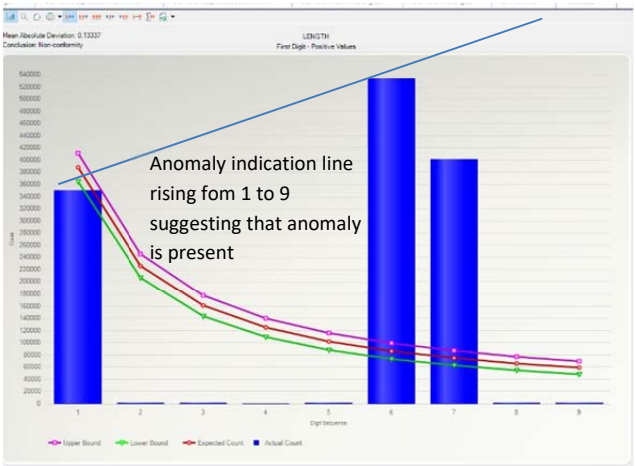

Figure 10. First digit Newcombe-Benford law - Malicious and Legitimate traffic

It can be concluded that *Hping3* initiated 26 % TCP traffic that generated retransmissions to spoofed addresses what as result created 71% additional traffic to overall traffic on laboratory network segment.

Figure 10. above shows the first digit Newcombe-Benford law result, it can be seen that frames with leading number 6 and 7 are indicated as anomalous - an indication in our experiment that due to large number of spoofed addresses there are a lot of retransmissions with frames of 60 or 70 bytes in length.

In Figure 10., it is shown that first two-digit Newcombe-Benford law results where can be seen that frames with leading number 60 and 70 are indicators of anomalous traffic based on Newcombe-Benford law.

Taking brief glance at Figure 10., the first number Newcombe-Benford law in IDEA dashboard it is easy to spot bars with numbers 6 and 7 that indicates anomalous traffic of 6X and 7X frames length in Bytes.

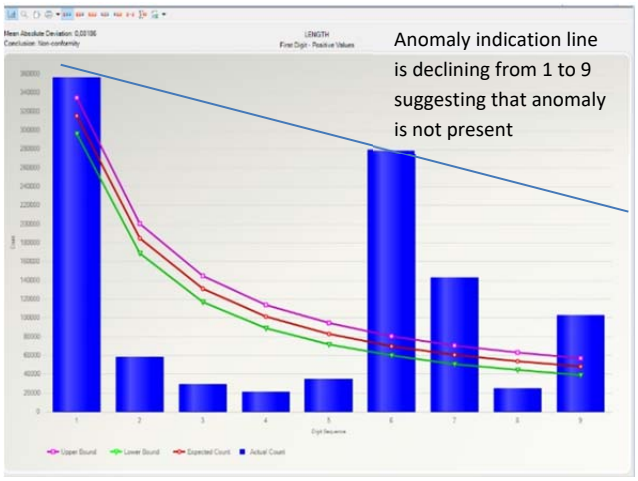

Figure 11. First digit Newcombe-Benford law – Legitimate traffic

In Figure 11. is shown the first number Newcombe-Benford law in IDEA dashboard with mostly legitimate traffic that permits a trained person to use Newcombe-Benford law to spot the difference between two figures: legitimate traffic (Figure 11. has more various length types of frames compared to predominantly malicious traffic in Figure 10.)

Further usage of Newcombe-Benford law leads us to use and compare First two digits Newcombe-Benford law with same data sets. Below in Figure 12., it can be seen that predominant traffic is with frames of leading numbers “15” while in Figure 12. the leading two numbers are “17” that indicates frames of 17x length and not 17xx since maximum frame length is 1518.

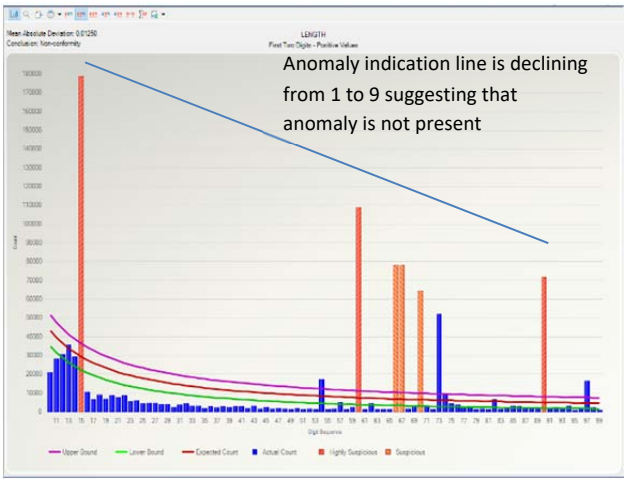

Figure 12. First two digits Newcombe-Benford law – Legitimate traffic

Having this information on the first two digits, Newcombe-Benford law can be used to spot malicious traffic as shown in Figure 13., where most of the traffic is frames with length of 17, 60 and 70 Bytes.

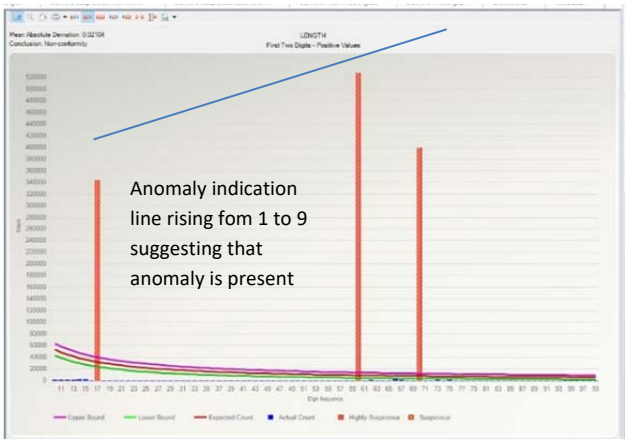

Figure 13. First two digits Newcombe-Benford law – Malicious and Legitimate traffic

We used Newcombe-Benford with first three digits where in Figure 14. is shown the legitimate traffic and in Figure 15. the malicious and legitimate traffic.

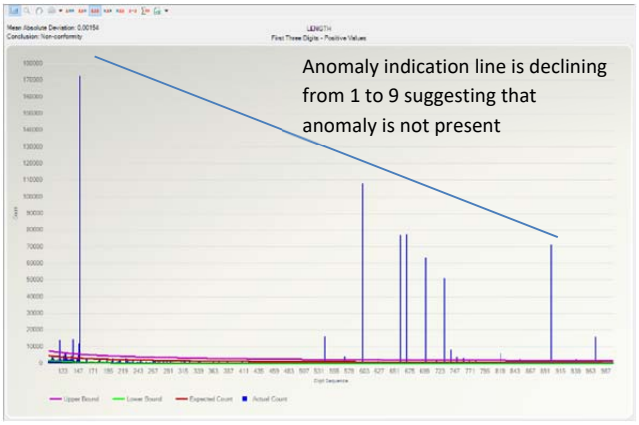

Figure 14. First three digits Newcombe-Benford law – Legitimate traffic

In Figure 15. is shown malicious and legitimate traffic with dominant malicious traffic with significant frames with 60 and 70 Bytes in length.

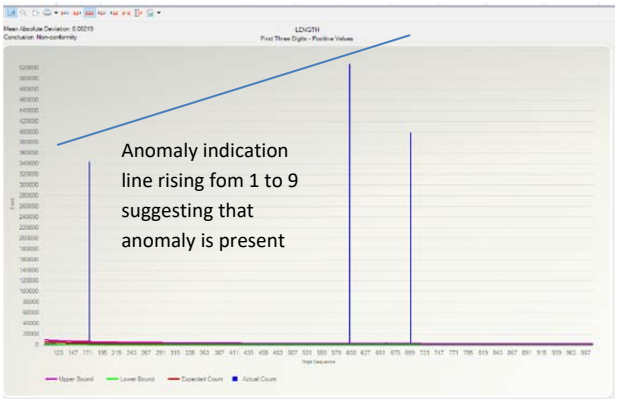

Figure 15. First three digits Newcombe-Benford law - Malicious and Legitimate traffic

5. Resolving Early DoS Detection with RMON Alerting

As suggested by Boyar and Özen Detection [18], the Denial-of-Service Attacks with SNMP/RMON is possible and we used similar approach using Cisco switch to raise an alarm on detection frames with 64 Bytes with OID .1.3.6.1.2.1.16.1.1.1.14. We chose 64 Bytes as indicator revealed in the above analysis using IDEA. Configuration line is shown below in *Figure 16. Actual CLI configuration of Alarm 2* and resulted configuration in web interface shown in *Figure 17. web based description of configured Alarm.*

```
rmon alarm 2 1.3.6.1.2.1.16.1.1.1.14.16 10 100 10 1 1 type delta  owner k
```

Figure 16. Actual CLI configuration of Alarm 2

Alarm Table

Alarm Entry No.	Interface	Counter Name	Counter Value	Sample Type	Rising Threshold	Rising Event	Falling Threshold	Falling Event	Startup Alarm	Interval (sec)	Owner
2	GE16	Frames of 64 Bytes	79	Delta	100	Default Description	10	Default Description	Rising and Falling	10	k

Figure 17. Web based description of configured Alarm

Alarm is configured to generate an alarm when more than 100 frames arrive at the monitored interface every 10 seconds. This alarm uses event 2 as shown below in *Figure 18. Actual CLI configuration of Event 2* to send a trap to the PC with ireasoning trap receiver.

```
rmon event 2 log-trap community cosmo  owner k
```

Figure 18. Actual CLI configuration of Event 2

6. Conclusions

From our experiments it can be concluded that legitimate traffic follows Newcombe-Benford law very closely when no malicious traffic is involved. Using this approach network security specialists can

be trained to recognize and distinguish legitimate from malicious traffic by monitoring Newcombe-Benford dashboards and in our case by comparing dashboards shown in Figures 10. and 11. in real time or to configure system to recognize these events automatically with the help of RMON and SNMP.

References

[1]. Kaspersky. (2022). DDoS attacks in Q3 grow by 24%, become more sophisticated. Retrieved from: https://www.kaspersky.com/about/press-releases/2021_ddos-attacks-in-q3-grow-by-24-become-more-sophisticated, [accessed: 07 January 2022].

[2]. Berger, A., & Hill, T. P. (2011). A basic theory of Benford's Law. *Probability Surveys*, *8*, 1-126.

[3]. Arshadi, L., & Jahangir, A. H. (2014). Benford's law behavior of Internet traffic. *Journal of Network and Computer Applications*, *40*, 194-205.

[4]. Prandl, S., Lazarescu, M., Pham, D. S., Soh, S. T., & Kak, S. (2017, May). An investigation of power law probability distributions for network anomaly detection. In *2017 IEEE Security and Privacy Workshops (SPW)* (pp. 217-222). IEEE.

[5]. Newcomb, S. (1881). Note on the frequency of use of the different digits in natural numbers. *American Journal of mathematics*, *4*(1), 39-40.

[6]. Benford, F. (1938). The law of anomalous numbers. *Proceedings of the American philosophical society*, 551-572.

[7]. Amouzegar M. A., Moshirvaziri K., Snyder D., (2018). Benford's Law And ts Application to Modern Information Security. 47th Annual Meeting, Western Decision Sciences Institute (WDSI).

[8]. Prandl S., (2017). PEIMA: Harnessing Power Laws to Detect Malicious Activities from Denial of Service to Intrusion Detection Traffic Analysis and Beyond, Curtin University. (pp. 1-12)

[9]. Sun, L., Anthony, T. S., Xia, H. Z., Chen, J., Huang, X., & Zhang, Y. (2017, December). Detection and classification of malicious patterns in network traffic using Benford's law. In *2017 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)* (pp. 864-872). IEEE.

[10]. Beardsley, T., & Qian, J. (2010). The TCP Split Handshake: Practical Effects on Modern Network Equipment. *Netw. Protoc. Algorithms*, *2*(1), 197-217.

[11]. Mariam, W. B. W., & Negash, Y. (2021, September). Performance Evaluation of Machine Learning Algorithms for Detection of SYN Flood Attack. In *2021 IEEE AFRICON* (pp. 1-6). IEEE.

[12]. Nmap. (2020). Nmap network scanner. Retrieved from: https://nmap.org/, [accessed: 09 January 2022].

[13]. Hping3 Software, (2020). Retrieved from: https://tools.kali.org/information-gathering/hping3, [accessed: 15 January 2022].

[14]. Anthony R. J., (2016). The Resource View in Systems Programming. Retrieved from: https://www.sciencedirect.com/topics/computer-science/minimum-frame-size, [accessed: 20 January 2022].

[15]. Lee G., (2014). Future Trends in Cloud Networking, Retrieved from: https://www.sciencedirect.com/topics/computer-science/minimum-frame-size, [accessed: 25 January 2022].

[16]. Lynch S., (2015), Packet Crafting: A Serious Crime! Retrieved from: https://resources.infosecinstitute.com/topic/packet-crafting-a-serious-crime/, [accessed: 05 Feb 2022].

[17]. IDEA Limitations. (2013). Retrieved from: http://ideascripting.com/forum/idea-limitations, [accessed: 14 January 2022].

[18]. Boyar, O., Özen, M. E., & Metin, B. (2018, June). Detection of denial-of-service attacks with SNMP/RMON. In *2018 IEEE 22nd International Conference on Intelligent Engineering Systems (INES)* (pp. 000437-000440). IEEE.

[19]. MIB Browser. (2021). Ireasoning MIB Browser Version 14 Build 4712, Retrieved from: https://www.ireasoning.com/mibbrowser.shtml , [accessed: 09 January 2022].

[20]. Wireshark.(2021). Stable release of Wireshark 3.6., Wireshark Software. Retrieved from: https://www.wireshark.org/download.html, [accessed: 15 January 2022].

[21]. Cisco. (2021). Cisco SG250-18 18-Port Gigabit Smart Switch. Retrieved from: https://www.cisco.com/c/en/us/support/switches/sg250-18-18-port-gigabit-smart-switch/model.html, [accessed 20 January 2022].