Supporting Features for Flow-Level Packet Analysis towards Cyber Threat Detection: A Pilot Study

Emmanuel C. Ogu[1, *]; Ojesanmi, O.A.[2]; Awodele, O.[3]; Kuyoro, S.O.[4]

ecoxd1@yahoo.com[1]; dejioje@yahoo.com[2]; delealways@yahoo.com[3]; afolashadeng@gmail.com[4].

[1, 3, 4] Department of Computer Science,
School of Computing and Engineering Sciences,
Babcock University, Ilishan-Remo, Ogun State. Nigeria.

[2] Department of Computer Science,
College of Sciences,
Federal University of Agriculture, Abeokuta, Ogun State. Nigeria.

* *Corresponding Author*

Abstract

Thousands of new threats and threat categories continue to emerge every second in cyberspace, even as known threats keep adapting robustly to existing solutions. This has challenged modern approaches and solutions to threat detection and potentially rendered some of these obsolete even before they are able to find applicability. Much contemporary cyber / network threat detection solutions rely largely on flow-level packet analysis, by monitoring trends and patterns of activity in supporting flow features of interest. However, while this has been the case, little attention has been paid to whether or not such supporting flow features still present an effective means of reaching accurate conclusions regarding imminent or occurrent cyber threat incidents, especially in the face of a rapidly evolving and adapting 21st century cyber threat landscape. This research is therefore a necessary pilot study to a larger research that aims to develop a state-of-the-art detection solution against a newly uncovered category of cyber threats known as subversive cyber threats. The goal of this pilot study being to reinvestigate four of the more commonly used supporting flow features in modern threat detection solutions, *viz.* Flow Packet Count, Flow Packet Throughput (bytes/s), Flow Packet Throughput (packets/s), and Average Flow Packet Size (bytes), in trying to ascertain / verify their continued relevance in the development of new cyber threat detection solutions. The study adopts the methodology of data simulation with descriptive infographic analysis using the recent UNSW-NB15 cybersecurity dataset.

Keywords: *Threat Intelligence; Cyber Threats; Packet Analysis; Flow Features; Threat Detection; Cyber Security; Network Security.*

1.0 Introduction

The 21st century cyber threat landscape has continued to evolve dynamically. Known threats continue to adapt robustly to existing cyber security solutions, just as new threats emerge daily. The 2017 Cybercrime Report of the *Cybersecurity Ventures* has predicted that by 2021, cybercrimes and attacks will cost the global economy in excess of $6 trillion annually, as over 200 billion devices would be connected to the Internet, and global organizations would suffer a cyber-attack at least every 14 seconds. This prediction is expected to be forged into reality by an exponential increase in the nearly one million malware threats that are now being released daily; according to separate 2015 reports by *CNN Money* and *TrendMicro*. To this end, the cybercriminals that sit behind these infamous cyber threats and attacks have continued to advance and sharpen their toolset and skillset in order to sustain this reality and insure the predicted future. This trend and portended realities have daunted and inundated cyber security stakeholders and practitioners, with one source voicing such concerns at one point in saying that, “the inability of the world’s best computer security technologists to gain the upper hand against anonymous but determined cybercriminals is viewed by a growing number of those involved in the fight as evidence of a fundamental security weakness in the global network.” (Markoff, 2009).

Through efforts at assuagement and remediation of the spates that portend these realities, behaviour profiling started making inroads and gaining wide acceptance in the field of cyber and network security. This was based on the understanding that it is possible, and probably more effective, to detect and counter the effects and activities of threats by observing traffic behaviour at the flow-level through packet analysis. Packet analysis attempts to discover and understand the unique and distinguishable characteristics of acceptable and / or unacceptable flow-level traffic behaviours within cyber environments, often based on a set of already known and widely proven threat behaviour profiles. (Foroughi & Luksch, 2018), and (Ritchie, 2017), pointed out how crucial this strategy of behaviour profiling is to modern cyber security. (Abt, Gärtner, & Baier, 2014), further confirmed this reality in stating that it is possible to quite accurately understand and profile the behaviours of agents and actors in a network information using very small amounts of information that are typically contained in the headers of transmission traffic / packets up to the infrastructure’s transport layer, without having to bother about the actual message content being transmitted. This strategy of behaviour profiling quickly became the bedrock of succeeding contemporary anomaly-based detection solutions; and was largely preferred over other techniques because malicious behaviours generally could now be modelled and monitored for, regardless of the details of how they may feature in cyber / network environments, and then isolated accordingly.

Anomaly-based cyber security generally works either by: 1) modelling normal cyber behaviours & interactions, and monitoring for entity / participant behaviours and interactions that are anomalous to these and instructive of the imminence of threat situations / attacks, or 2) modelling known malicious / anomalous cyber behaviours and interactions, and monitoring for entities / participants that exhibit such behaviours. In best case implementations both methods are used complementarily; and in some cases, with one as a product / function of the other. But regardless of the method used, the general principle of flow-level packet analysis is often the same; involving storage and comparative processing of already known behaviour profiles with real-time monitoring and analysis of traffic and packets travelling across links in a cyber environment are common features. Actions, as necessary, may then be taken against such packets / traffic based on the result of the comparative processing. Existing researches by (Wang, Huang, Tsai, & Lin, 2014), (Boukhtouta, Lakhdari, Mokhov, & Debbabi, 2013), (Zhao, et al., 2013) and (Caglayan, Toothaker, Drapeau, Burke, & Eaton, 2012), amongst others, have proposed anomaly-based techniques and systems for security and defence in cyber environments. Figure 1 illustrates a basic abstract operational schema of modern anomaly-based cyber threat detection solutions.

However, it has also been discovered that sometimes it cannot be safely concluded by monitoring flow-level behaviour profiles alone that a packet(s) is/are from a malicious source, as (Xu, Wang, Bhattacharyya, & Zhang, 2010) amongst others have posited. As a result, a number of existing research have proposed that by considering flow-level packet behaviour in light of (other) arrays of associated supporting flow features for inherent or imminent anomalies, it would be possible to enhance the effectiveness of isolating threat agents in cyber and network environments. Some recent examples include: (Gulisano, et al., 2015), which considered disparities in feature histories of average number of packets, the average number of bytes and the average elapsed time, towards detecting DDoS attacks in network flow streams; (Ma & Chen, 2014), which considered anomalies in number of packets / volume of traffic to detect DDoS attacks; (Singh, Guntuku, Thakur, & Hota, 2014), which considered total bytes transferred or average flow inter arrival time, in order to arrive at informed conclusions in P2P botnet detection; and (Xu, Zhang, & Bhattacharyya, 2005), which considered packet size and packet count towards threat detection, amongst others.

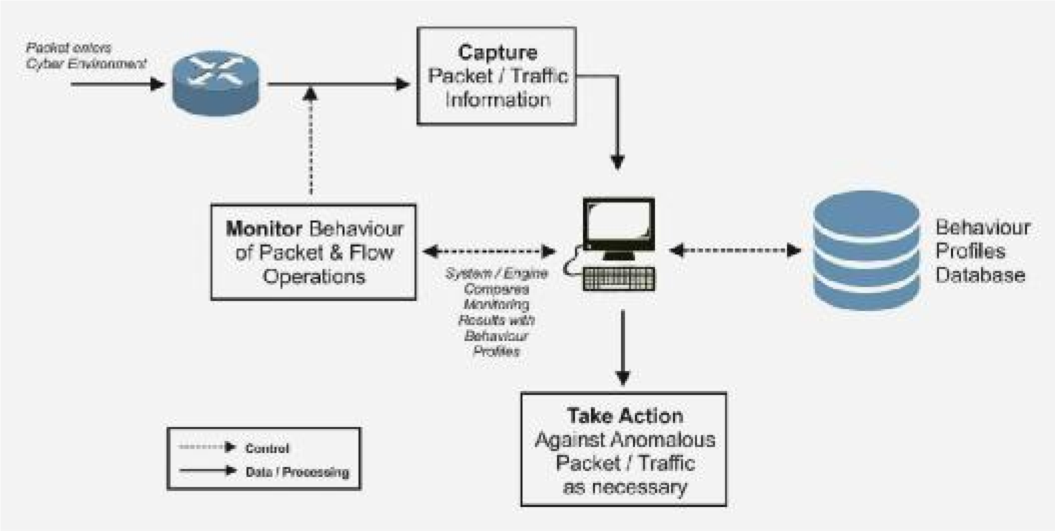
Packet enters Cyber Environment
Capture Packet / Traffic Information
Monitor Behaviour of Packet & Flow Operations
System / Engine Compares Monitoring Results with Behaviour Profiles
Behaviour Profiles Database
Take Action Against Anomalous Packet / Traffic as necessary
Control
Data / Processing

Figure 1: A Basic Abstract Operational Schema of Modern Anomaly-based Cyber Threat Detection Solutions

But then, as the 21st century cyber threat landscape continues to shift, adapt and evolve, with dozens of new threat species and categories emerging every minute and existing threats metamorphosing to be able to evade some of the most advanced modern detection solutions, it has become necessary to re-investigate the effectiveness of incorporating some of the more commonly used supporting flow features with flow-level packet analysis in state-of-the-art anomaly-based cyber security solutions towards detecting modern cyber threats. This pilot study, which is a necessary precursor to an ongoing research aimed at developing a machine learning integrated solution for detecting a newly uncovered class of cyber threats known as subversive cyber threats, which differ from the non-subversive counterparts by virtue of the fact that they are better coordinated in their approach, sophisticated in their design, strategic and multi-staged in their attack delivery, and aim at critical / high-value targets, having become the new faces of various forms of organized and coordinated crimes perpetrated within and through cyberspace; is directed at this purpose.

2.0 Related Works

Some existing state-of-the-art solutions, systems and techniques for the detection, classification and prevention of cyber threats and intrusion incidents have featured some form of flow-level packet analysis with supporting flow features in some cases.

(Hu, 2018), proposed a system that utilizes IP weight metrics for feature selection towards detecting intrusions in cloud environments. This system was evaluated using an ISOT cloud intrusion dataset that was collected couple years before 2015. Similarly, (He, Zhang, & Lee, 2017) proposed a machine-learning-based source side DDoS attack detection system that uses a set of statistical features (relating to DNS, SSH, ICMP and TCP user request packets) collected over a time interval from virtual machines running on cloud servers for detecting DDoS attacks in cloud environments. The detection system was evaluated using data obtained from multiple attack simulations within Virtual Machine environments; recalling to mind the discovery by ... that cyber threats and attacks usually behave differently within virtualised environments, and as such, the conclusions drawn from such virtualised experiments are likely not to portray a circumspect perspective to the issue under investigation.

(Prasad, Reddy, & Rao, 2017), also developed a bio-inspired model strategy for preventing HTTP flood attack by detecting them through observation of the attributes of Get and Post request streams over a time interval. The anomaly-based technique was evaluated using a HTTP transaction dataset that was also collected before 2015. In the same vein, (Chen, Luo, & Zincir-Heywood, 2017) proposed a system for service-based profiling of normal traffic behaviours for botnet detection using unsupervised machine learning algorithms on flow-level data. The system was evaluated using the CTU-13 botnet traffic dataset that was collected in 2011 at the CTU University in the Czech Republic.

(Tang, Tang, Lee, & Tao, 2015), equally proposed a monitoring technique for the detection and prevention of application-layer HTTP GET flooding (DDoS) attacks, based on real-time IP network flow-traffic big (meta-) data analysis. The technique relied on an arguably naïve strategy of collecting and analysing HTTP traffic to identify IP addresses with a significantly anomalous frequency of HTTP requests (>30 requests per second). A blacklist of identified IP addresses is then generated in the form of ACL (Access Control List) rules based on the Classless Inter-Domain Routing (CIDR) format; with which other deployed defence systems can apply further mitigation strategies.

(Xu, Wang, Bhattacharyya, & Zhang, 2010), put forth a system for profiling the behaviour of internet traffic at the link level devices and infrastructure in real-time over a time period based on the leads and findings of their previous (foundational) research – (Xu, Zhang, & Bhattacharyya, 2005), which was evaluated based on multiple datasets collected between April 2003 and January 2004. The behaviour profiling system relied on combining information obtainable at the flow-level (Source and Destination IP addresses & ports, and protocol / service, over a time interval), with data mining, techniques from information theory, and a simple, novel filtering algorithm to monitor and automatically profile behaviours of nodes based on communication patterns, and then developing structural models based on observations for events of significance, so that necessary actions could be taken.

Based on the foregoing, it can be concluded that much of the existing related researches seem to suffer common limitation(s): (1) some of them are premised on rather naïve techniques that do not consider the robustness, stealthiness, and resilience featured by modern cyber threats and attacks; while (2) others rely on datasets that arguably, and to a large extent, may not reflect the modern realities of threats and attacks that have marauded cyberspace in recent times. Most of the datasets featured in existing related works were collated before the daunting realities of attacks such as the *Slack* and *Madison* breaches of 2015, the daunting *Mirai* botnet and the dreaded *Pegasus* mobile spyware of August 2016, the seemingly unquenchable ransomware spates of 2017, the *SingHealth* attack of July 2018, amongst preponderant others, hit cyberspace. As a result, in attempting to combat modern cyber threats and attacks, it may be unsafe to rely completely on the foundations that launched some of these existing researches, as well as some of the conclusions that they arrived at.

More recent cyber security datasets are able to more correctly capture and reflect the contemporary realities associated with combatting modern cyber threats and attacks, including resilient attack behaviours, metamorphosed defence strategies, robust evasion techniques, and shrewd stealth mechanisms, to mention a few. It is on this basis that this research sets out to re-investigate, based on a relatively more recent cyber security dataset, the baseline supporting flow features that have been incorporated in research experiments such as those carried out in the reviewed related works, and which generated remarkable evaluation results within the context of the researches; so as to verify their continued relevance and applicability in building state-of-the-art detection and mitigation solutions against modern cyber threats and attacks.

3.0 **Research Methodology**

The key methodology used by this research is that of data simulation with descriptive infographic analysis. Infographics are graphical / visual representations of information, patterns, and knowledge from simulated data, which when analysed, help to visualise, illustrate and present knowledge and information quickly and clearly in a factual manner; they help to represent large data sets in a coherent manner. Infographic Analysis has found its applications in many broad disciplines such as engineering, social sciences, information technology, security sciences, communication & arts, amongst others. Infographic Analysis helps to quickly extract and visualise patterns and structures hidden within large sets of data using (key) criteria and characteristics of interest. These are then interpreted and analysed using statistical or verbal descriptions to arrive at informed conclusions that can impact effectively on decisions and outcomes.

Four supporting flow features, which have featured frequently and extensively in existing detection solutions, are considered for investigation in this study: Flow Packet Count, Flow Packet Throughput in bytes/s and then in packets/s, and Average Flow Packet Size.

a) Flow Packet Count: This refers to the total number of packets that are present in a traffic or transmission flow (both in the forward and reverse directions).
b) Flow Packet Throughput (bytes/s): This refers to the rate at which flow packets are transmitted within the network every second, based on the packet size in bytes.
c) Flow Packet Throughput (packets/s): This refers to the rate at which flow packets are transmitted within the network every second, based on the number of packets.
d) Average Flow Packet Size (bytes): This refers to the average size of packets transmitted in a traffic flow (in the forward and reverse directions).

The recent UNSW-NB15 cyber security dataset is considered for this research study, which comprises a mix of threat data that are categorized as subversive and non-subversive (normal traffic, and other threat traffic). Next, the flow features of interest are derived, and then two simulations using the dataset (based on pairs of the flow features under consideration) are performed with a source code written in the R statistical programming language; infographics are generated, which are then descriptively analysed and interpreted.

4.0 **Data Simulation**

Two data simulations are carried out in this study: the first featuring average flow throughput (in bytes/s) against total flow packet count, and the second featuring average flow throughput (in packets/s) against mean flow packet size (in bytes). An R program was used in the simulations that involved the UNSW-NB15 dataset, and the resulting infographics are presented and discussed. Trends, patterns and insights revealed by the infographics are descriptively analysed to give recommendations for the development of future threat detection solutions that may rely on some form of flow-level packet analysis.

4.1 The UNSW-NB15 Dataset

The UNSW-NB15 Dataset is a cyber security dataset of raw network packets that was created in 2015 using the IXIA PerfectStorm tool at the Cyber Range Lab of the Australian Centre for Cyber Security (ACCS) for generating a hybrid of real modern normal activities and synthetic contemporary attack behaviours. The dataset was published in 2015 by (Moustafa & Slay, 2015), and made available online at (Moustafa & Slay, 2016). The dataset contains 9 types / categories of attacks including: Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode and Worms (see the referenced dataset documentation for the definitions of these various attack categories).

The total number of network packet records in the UNSW-NB15 Dataset is 2,540,044, featuring forty-nine (49) attributes each. As originally published, partitions from this dataset are configured as training set and testing set, containing 175,341 and 82,332 records respectively, featuring the different types of attacks, as well as normal traffic; however, the entire dataset records are used in the data simulations that are carried out in this pilot study.

In (Moustafa & Slay, 2016), the UNSW-NB15 dataset was proven to be among the benchmark datasets for quantitative cyber security research over and against the existing benchmark KDD99 and NSLKDD datasets, which fall short due to “their lack of modern low footprint attack styles; their lack of modern normal traffic scenarios, and a different distribution of training and testing sets.” The UNSW-NB15 dataset was discovered to be more complex and structured that the KDD99 dataset and its derivatives; thus becoming a new benchmark dataset.

4.2 Traffic re-categorization

Towards achieving the goal of this data simulation, the network traffic featured in the UNSW-NB15 Dataset are re-grouped into three (3) broad categories:

1. Normal Traffic: These are the harmless packet traffic in the dataset, which under ideal circumstances (as is assumed by this research), represents the baseline for acceptable traffic and packet behaviours and characteristics within the cyber environment.
2. Subversive Threats / Attacks: These are those packet traffic that exhibit malicious behaviours that are telltales of subversive intent – aimed at disrupting, overrunning or hijacking (critical) protocols, services, systems or the entire cyber environment.
3. Other Threats / Attacks: These are those packet traffic that exhibit malicious behaviours within the cyber environment, but cannot be explicitly associated with subversive intent.

Table 1 represents a categorization of the packet traffic in the UNSW-NB15 Dataset into the afore-described categories, based on the definitions earlier given for the various attack traffic contained in the dataset and in line with insights received from (Rosch, 1998).

Table 1: Re-Categorization of UNSW-NB15 Dataset Traffic Objects / Observations

Superordinate	**Basic Level**	**Intermediate Level**	**Subordinate**
UNSW-NB15 Dataset	Normal Traffic	Normal Traffic	
	Malicious / Attack Traffic	Subversive Threats / Attacks	Exploits
			Shellcode
			DoS
			Fuzzers

Superordinate	Basic Level	Intermediate Level	Subordinate
			Worms
		Other Threats / Attacks	Generic
			Reconnaissance
			Analysis
			Backdoors

4.3 Feature Selection and Derivation

Table 2 presents the selected and derived features from the UNSW-NB15 dataset that were used in infographic analysis.

Table 2: Table of Selected and Derived Features from the UNSW-NB15 dataset

S/N	Selected Features	Derived Features
1.	Source bits per second	$\boldsymbol{Average\ Flow\ Throughput\ (bytes/s)} = \left(\frac{Source\ bits\ per\ second + Destination\ bits\ per\ second}{2}\right) / 8$
2.	Destination bits per second	
3.	Source to Destination Transaction Bytes	
4.	Destination to Source Transaction Bytes	$\boldsymbol{Average\ Flow\ Throughput\ (packets/s)} = \frac{Average\ Flow\ Throughput\ (bytes/s)}{\left(\frac{(Source\ to\ Destination\ Transaction\ Bytes\ +\ Destination\ to\ Source\ Transaction\ Bytes)}{(Source\ to\ Destination\ Packet\ Count\ +\ Destination\ to\ Source\ Packet\ Count)}\right)}$
5.	Source to Destination Packet Count	
6.	Destination to Source Packet Count	
7.	Source to Destination Packet Count	$\boldsymbol{Total\ Flow\ Packet\ Count} = Source\ to\ Destination\ Packet\ Count + Destination\ to\ Source\ Packet\ Count$
8.	Destination to Source Packet Count	
9.	Mean of the Flow packet size transmitted by the Source	$\boldsymbol{Mean\ Flow\ Packet\ Size} = Mean\ of\ the\ Flow\ packet\ size\ transmitted\ by\ the\ Source + Mean\ of\ the\ Flow\ packet\ size\ transmitted\ by\ the\ Destination$
10.	Mean of the Flow packet size transmitted by the Destination	
11.	Label	

5.0 Infographic Analysis

The infographics resulting from the data simulations are displayed in Figures 2 and 3.

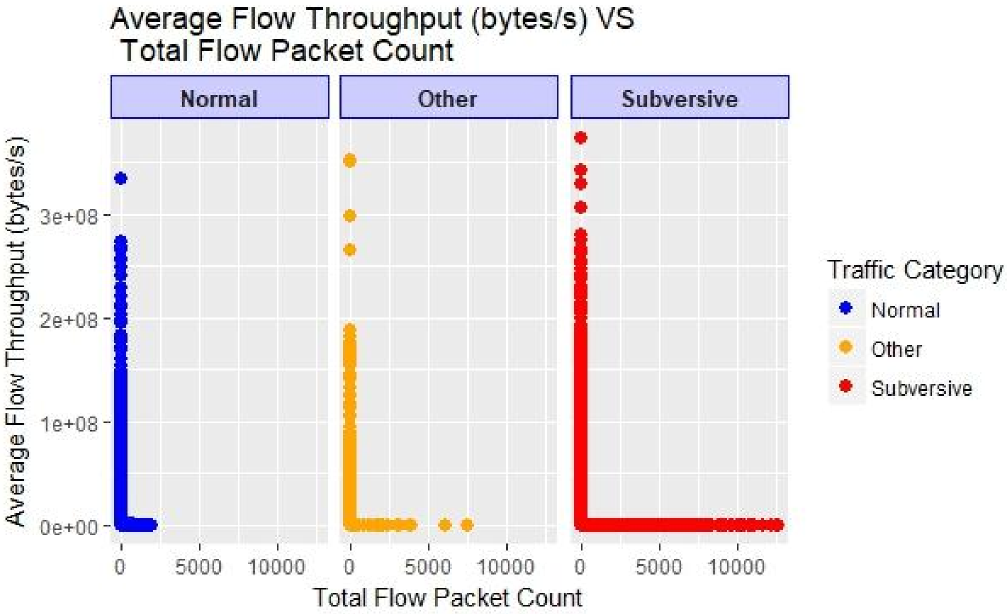

Figure 2: Infographic from Data Simulation I

As shown in Figure 2, subversive cyber threats and attacks transmit flows with a much higher packet count than other forms of non-subversive cyber threats (> 5000 packets), and an exponentially much higher packet count than benign / normal flow traffic (> 2500 packets). As also shown, subversive traffic transmit flows at a higher throughput (in bytes/s) than other forms of non-subversive cyber threats and attacks (> 2e+08), and slightly higher than normal traffic (> 3e+08).

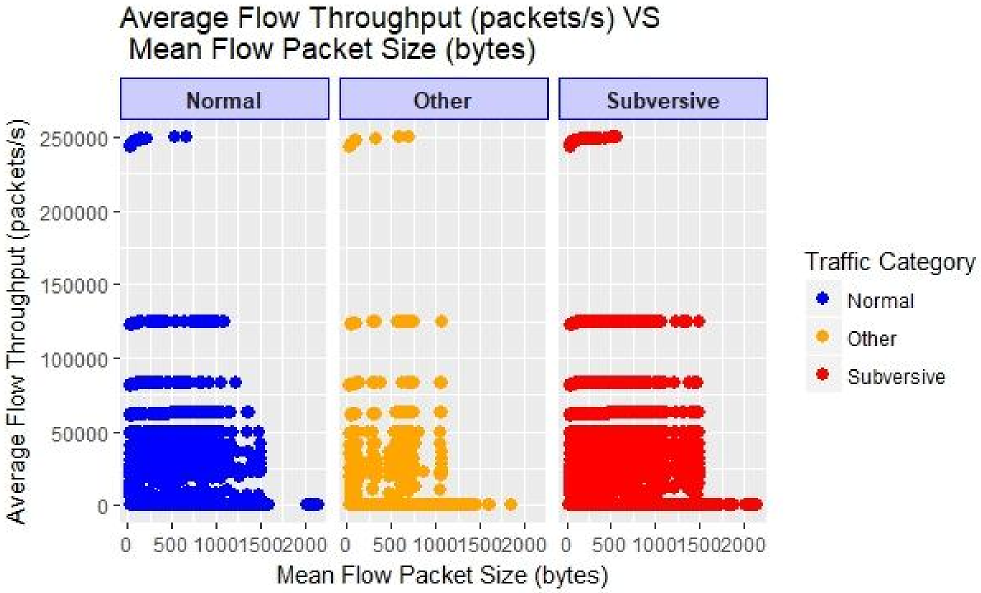

Figure 3: Infographic from Data Simulation II

As shown in the infographic, subversive cyber threats and attacks transmit flows of a slightly higher mean packet size (in bytes) with more traffic density towards the higher parts than other forms of non-subversive cyber threats and benign / normal flow traffic; as evident from the point of > 1500 bytes of flow packet size as shown in the infographic. As also shown, subversive traffic transmit a large density of traffic flows at about the same throughput (in packets/s) rate as other forms of non-subversive cyber threats and attacks, especially as well as normal traffic. Observing the range of throughput (in packets/s) between 0 – 50, 000 reveals this reality.

6.0 Findings & Discussion

The infographic analysis and reports from Figures 2 and 3 reveal that monitoring and observing the combination of flow packet throughput (bytes/s) and total flow packet count would provide more effective results at attempts to accurately detect and distinguish subversive threats and attack traffic from benign traffic and other forms of non-subversive cyber threats and attacks than would the combination of flow packet throughput (packets/s) and mean flow packet size (bytes).

More importantly, however, as is observable from the infographics in Figures 2 and 3, modern subversive threats and attacks seem to have enhanced their decoy capabilities to be able to transmit a much larger percentage volume of their malicious flows in compliance with possible configured constraints on throughput, packet count, packet size, and perhaps other supporting flow features in the native network operating system and environment. This is typically the outcome of strategic and in-depth reconnaissance that could help them evade some of the most advanced detection solutions. This means that modern detection systems need to be robust enough be able to eliminate a large amount of false positives and true negatives from detected possible threat samples and traffic so as to be able to more accurately isolate and distinguish subversive cyber and network threats and attacks traffic from other network traffic.

7.0 Recommendation & Conclusion

The findings of this pilot study reveal that inventors of modern detection solutions would need to look more to the supporting flow features of flow packet throughput (bytes/s) and total flow packet count in developing modern solutions that rely on some form of flow-level packet analysis. It is a recommendation that is based on quite obvious realities that this research has brought to the fore.

More crucially, however, we may be approaching the limits of being able to accurately detect subversive cyber threats and attacks based on flow-level packet analysis alone, as more advanced and sophisticated cyber threats continue to emerge. Perhaps, as Professor Baruch Fischhoff, the Howard Heinz University Professor at Carnegie Mellon University (CMU) suggested, “The strategies and procedures to secure cyber technologies would be improved through a better understanding of the social, behavioural and decision sciences because people are an integral component — in designing technologies, operating them, allocating security resources — and in attacking them … Cybersecurity is headed toward a more multidisciplinary approach”; with Roy Maxion, a Research Professor at CMU’s School of Computer Science further adding that: “More of computer science research, particularly in cybersecurity, could benefit from developing a foundationally sustained science and by incorporating lessons learned in experimental design and analysis from other disciplines into a science of security…” (Ritchie, 2017)

In essence, into the near future, the most effective and adaptive threat detection solutions would be those that have been able to incorporate certain behavioural realities that are able to more correctly circumvent the thought and decision pathways of the shrewd attacker; and in cases where such detection solutions would also rely to some extent on flow-level traffic packet analysis, it would be a more savvy technique to consider the duo supporting flow features of flow packet throughput (bytes/s) and total flow packet count as the invaluable findings of this research pilot study has lucidly amplified based on more recent data evidence.

8.0 Further Research

Based on the foregoing findings of this necessary pilot study, further research would aim at developing a robustly scalable and adaptive solution for detecting subversive cyber threats in modern IP networks. The detection solution would incorporate the relevant and yet applicable supporting flow features that have been discovered based on the investigations of this pilot study, and utilise these in flow-level packet analysis using integrated machine learning capabilities. Further, the experimental evaluation of the new subversive cyber threat detection solution would be based on a yet more recent benchmark cyber security dataset that is currently being collected and collated, so as to further corroborate and authenticate the veracity of the findings of this pilot study, and what they portend for the future of cyber security research and development, especially in the area of threat detection and intelligence.

9.0 References

Abt, S., Gärtner, S., & Baier, H. (2014). A small data approach to identification of individuals on the transport layer using statistical behaviour templates. *Proceedings of the 7th International Conference on Security of Information and Networks* (p. 25). Glasgow, Scotland, UK: ACM.

Boukhtouta, A., Lakhdari, N. E., Mokhov, S. A., & Debbabi, M. (2013). Towards fingerprinting malicious traffic. *Procedia Computer Science, 19*, 548-555. Retrieved November 2015, from http://www.sciencedirect.com/science/article/pii/S1877050913006819

Caglayan, A., Toothaker, M., Drapeau, D., Burke, D., & Eaton, G. (2012). Behavioral analysis of botnets for threat intelligence. *Information Systems and E-Business Management, 10*(4), 491-519.

Chen, W., Luo, X., & Zincir-Heywood, A. N. (2017, May). Exploring a service-based normal behaviour profiling system for botnet detection. *IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 2017* (pp. 947-952). Lisbon, Portugal: IEEE Press. doi:10.23919/INM.2017.7987417

Foroughi, F., & Luksch, P. (2018). Data Science Methodology for Cybersecurity Projects. *arXiv preprint arXiv:1803.04219*, 1-14. Retrieved March 19, 2018, from https://arxiv.org/ftp/arxiv/papers/1803/1803.04219.pdf

Gulisano, V., Callau-Zori, M., Fu, Z., Jiménez-Peris, R., Papatriantafilou, M., & Patiño-Martínez, M. (2015). STONE: A streaming DDoS defense framework. *Expert Systems with Applications, 42*(24), 9620-9633. doi:10.1016/j.eswa.2015.07.027

He, Z., Zhang, T., & Lee, R. B. (2017). Machine Learning Based DDoS Attack Detection from Source Side in Cloud. *IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 2017* (pp. 114-120). New York, NY, USA: IEEE. doi:10.1109/CSCloud.2017.58

Hu, R. (2018). *Assessing IP Weight Metrics for Cloud Intrusion Detection using Machine Learning Techniques.* Retrieved March 31, 2018, from University of Victoria - Graduate Projects (Electrical and Computer Engineering): http://dspace.library.uvic.ca/bitstream/handle/1828/9088/Hu_Ruiqi_MEng_2018.pdf?sequence=3&isAllowed=y

Ma, X., & Chen, Y. (2014). DDoS detection method based on chaos analysis of network traffic entropy. *IEEE Communications Letters, 18*(1), 114-117. doi:10.1109/LCOMM.2013.112613.132275

Markoff, J. (2009, March 18). *Computer Experts Unite to Hunt Worm*. Retrieved October 04, 2016, from The New York Times: http://www.nytimes.com/2009/03/19/technology/19worm.html?_r=0

Moustafa, N., & Slay, J. (2015). UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). *Military Communications and Information Systems Conference (MilCIS), 2015* (pp. 1-6). Canberra, ACT, Australia: IEEE. doi:10.1109/MilCIS.2015.7348942

Moustafa, N., & Slay, J. (2016). The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. *Information Security Journal: A Global Perspective, 25*(1-3), 18-31. doi:10.1080/19393555.2015.1125974

Moustafa, N., & Slay, J. (2016, March 02). *The UNSW-NB15 data set description*. Retrieved February 22, 2018, from UNSW Canberra: https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/cybersecurity/ADFA-NB15-Datasets/

Prasad, K. M., Reddy, A. M., & Rao, K. V. (2017). BIFAD: Bio-inspired anomaly based HTTP-flood attack detection. *Wireless Personal Communications, 97*(1), 281-308. doi:10.1007/s11277-017-4505-8

Ritchie, A. L. (2017, August 03). *Improving Security Science Through Collaboration*. Retrieved October 20, 2017, from Carnegie Mellon School of Computer Science: https://www.cs.cmu.edu/news/improving-security-science-through-collaboration

Rosch, E. (1998). Principles of Categorization. In G. Mather, F. Verstraten, & S. Anstis, *The Motion Aftereffect* (pp. 251-270). Massachusetts: MIT Press.

Singh, K., Guntuku, S. C., Thakur, A., & Hota, C. (2014). Big data analytics framework for peer-to-peer botnet detection using random forests. *Information Sciences, 278*, 488-497. doi:10.1016/j.ins.2014.03.066

Tang, C., Tang, A., Lee, E., & Tao, L. (2015). Mitigating HTTP Flooding Attacks with Meta-data Analysis. *Proceedings of 2015 IEEE 17th International Conference on High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), and 2015 IEEE 12th International Conf on Embedded Software and S* (pp. 1406-1411). New York, NY, USA: IEEE Press. doi:10.1109/HPCC-CSS-ICESS.2015.203

Wang, K., Huang, C.-Y., Tsai, L.-Y., & Lin, Y.-D. (2014). Behaviour-based botnet detection in parallel. *Security and Communication Networks*, John Wiley & Sons Ltd.

Xu, K., Wang, F., Bhattacharyya, S., & Zhang, Z.-L. (2010). Real-time behaviour profiling for network monitoring. *International Journal of Internet Protocol Technology, 5*(1-2), 65-80.

Xu, K., Zhang, Z. L., & Bhattacharyya, S. (2005, August). Profiling internet backbone traffic: behavior models and applications. *ACM SIGCOMM Computer Communication Review, 35*(4), 169-180.

Zhao, D., Traore, I., Sayed, B., Lu, W., Saad, S., Ghorbani, A., & Garant, D. (2013). Botnet detection based on traffic behavior analysis and flow intervals. *Computers & Security, 39*, 2-16.

Authors Biographical Sketch

Emmanuel C. OGU holds a BSc. Degree in Computer Science (Technology), a MSc. Degree in Computer Science (Networking and Telecommunications), and a PhD in Computer Science (Cyber & Network Security), all from Babcock University, Nigeria. His research interests cover a broad range of multidisciplinary topics related to contemporary issues and discourses in Cybersecurity, Security Policy & Legislation, Business Information Technologies, and Sustainable Development. He has authored and co-authored over a dozen peer-reviewed and referred research articles in the areas of his research interests, which have been published by reputable international journals and indexed in global repositories.

Olusegun A. OJESANMI is an Associate Professor of Computer Science at the Department of Computer Science, Federal University of Agriculture, Abeokuta, in Ogun State, Nigeria. He has been actively involved in teaching Computer Science at various academic levels for over a decade. He has authored and co-authored dozens of researches and articles in the discipline of Computer Science and these have been published in reputable journals worldwide.

Oludele AWODELE is a Professor of Computer Science in the Department of Computer Science, School of Computing and Engineering Sciences, Babcock University, Ilishan-Remo, Ogun State, Nigeria. Currently serving as the School Dean, he has been actively involved in teaching Computer Science for over a decade. He has authored and co-authored scores of researches and articles in Computer Science and these have been published in reputable journals worldwide.

'Shade O. KUYORO holds a PhD in Computer Science from the Department of Computer Science, School of Computing and Engineering Sciences, Babcock University, Ilishan-Remo, in Ogun State, Nigeria. She has been actively involved in teaching Computer Science at various academic levels for about a decade. She has authored and co-authored many researches and articles in Computer Science and these have been published in reputable journals worldwide.