DETECTION OF NETWORK TRAFFIC ABNORMALITIES USING LRD BEHAVIOR ANALYSIS OF CONTROL AND DATA PLANES

Basil AsSadhan[*1] and **José M. F. Moura**[2]
[1]Deptartment of Electrical Engineering, College of Engineering, King Saud University, Riyadh, Saudi Arabia
[2]Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA, USA
[*]Corresponding author E-mail: bsadhan@ksu.edu.sa

ABSTRACT**:** *We analyze network traffic behavior using Long-Range Dependence (LRD) behavior analysis of control and data planes. The LRD behavior of control and data planes traffic is examined for different directions with respect to the enterprise network.*

Our results show that network attacks that affect the aggregate traffic cause the incoming control traffic or the outgoing data traffic to fail to exhibit LRD behavior, whereas the traffic as a whole still exhibits LRD behavior. These two subgroups are the only ones that were affected, as the attacks in the dataset are carried via the incoming control traffic, and the response to this traffic appears at the outgoing data traffic. What is interesting about these two subgroups is that they have low traffic volume, hence they significantly reduce the amount of traffic analysis. In addition, LRD behavior analysis of control and data planes traffic will enable the detection of abnormal behaviors that might not be detected by previous work that only look at the traffic as a whole.

Keywords—Network traffic analysis, abnormal behavior, long-range dependence, self-similarity, Optimization method.

I. INTRODUCTION

Traffic abnormal behaviors such as attacks, failures, and malfunctions are common in today's computer networks. They degrade the network's performance and security, and cause substantial financial losses. We propose a method to analyze network traffic behavior and to detect such network violations by analyzing the *Long-Range Dependence* (LRD) behavior of control and data planes traffic. This is motivated by our observation that control and data traffic of aggregate traffic have similar behaviors during benign normal applications. The reason behind this similarity is that data traffic generation is based on control traffic generation. This similarity is affected by certain network abnormal behaviors that affect the aggregate traffic behavior and manifest themselves mainly at one of the two planes. Such analysis is useful to detect certain attacks as reported by AsSadhan et. al [1-3].

In this paper, we examine the LRD behavior of the control and data planes traffic. It is generally accepted that network traffic exhibits LRD and is self-similar, see for example [4-6]. Previous studies looked into the effect of abnormal behaviors on the LRD behavior of network traffic as a whole, and whether it is possible to detect such abnormal behaviors from their effect on the LRD behavior [7-12]. However, no available study has looked at the effect of abnormal behaviors on control and data planes traffic separately.

We report our results on the TCP traffic of the Network Intrusion Dataset provided by the Information Exploration Shootout project [13]. We find that several network attacks in the dataset that affect the aggregate traffic cause the *incoming control* traffic or the *outgoing data* traffic with respect to the enterprise LAN to fail to exhibit LRD behavior. At the same time, the traffic as a whole still exhibits LRD behavior. We note that an attack from outside the LAN will mostly be carried through the incoming control traffic, and the response to this traffic appears mainly in the outgoing data traffic. Hence, these two subgroups are the only ones affected.

What is important about these two subgroups is that their traffic volume is very low when compared to the incoming data and outgoing control traffic. Such result, once it can be generalized, would reduce the amount of traffic to be analyzed and the computations needed to detect abnormal behaviors. In addition, it enables detecting abnormal behaviors that might not be detected by previous work that only look at the traffic as a whole.

The rest of the paper is organized as follows: Section II explains our methodology in analyzing network traffic through LRD behavior analysis of control and data planes traffic, and how we use this to study the LRD behavior of the traffic. The Network Intrusion dataset and our results of applying our methodology on it presented in Section IV. Conclusions and current work is presented in Section IV.

II. METHODOLOGY: LRD BEHAVIOR ANALYSIS OF CONTROL AND DATA PLANES

We analyze network traffic through LRD behavior analysis of control and data planes traffic. We decompose network header traffic into control and data planes and observe the level of similarity between the two in order detect abnormal behaviors that manifest themselves mainly at one of the two planes (typically the control plane). The reason behind our decomposition is our assumption that data traffic generation is based on control traffic generation. Hence, they would have similar behaviors during benign normal applications. Dissimilarities are considered to be an indication of some abnormal behavior.

In our work, we analyze enterprise LAN packets, where control packets are the ones that set, maintain, or tear down a connection, and data packets are the ones that are concerned with the actual transmission of data [1, 2]. We limit our study to TCP traffic as it constitutes most of the Internet traffic, and is easily decomposed into control and data planes. We treat packets having one of the following flags:

SYN, FIN, or RST, as control packets. Bare acknowledgment packets are also treated as control packets as they do not have payloads. All other TCP packets are treated as data packets [1, 2].

LRD Behavior of Control and Data Planes

We analyze control and data planes traffic to study the LRD behavior of the traffic, and examine the effect of abnormal behavior on it. It is generally accepted that network traffic exhibits LRD and is self-similar, see, for example, [4-6]. This behavior arises from the multiplexing of a large number of ON/OFF sources that transfer files whose sizes are heavy tailed [4, 14]. The effect of abnormal behaviors on the LRD of the control and data traffic sequences is examined for different count features. We use *the Optimization method* [15, 16] to analyze the LRD behavior of the traffic. The Optimization method is simple and fast. It is also more accurate when compared to the well-known Wavelet method [17] as reported in [15, 16].

The method is used to test whether a given traffic sequence is a second-order self-similar (SOSS) process or a fractional ARIMA (FARIMA) process. If the network traffic trace is either one of these two, then the process is LRD. If the process fails both tests, then the traffic fails to exhibit LRD.

The Optimization method's test is based on minimizing the error function of fitting the autocorrelation function's curve $\rho(k)$ of the model (i.e., SOSS or FARIMA(0,*d*,0) process) to the curve of the estimated autocorrelation of the traffic sequence $\hat{\rho}(k)$ [15].

For SOSS processes, the error function is defined as:

$$E_K(H) = \frac{1}{4K}\sum_{k=1}^{K}\{\rho_H(k) - \hat{\rho}(k)\}^2,$$

The error function is computed for all possible values of the Hurst parameter *H*. If the minimum error value is less than a threshold ε, the process is considered to be second-order self-similar with Hurst parameter *H* that achieved this minimum error. We choose ε = 1e-3, which was selected by [15], so that the probability of the false alarm is less than 0.05. A false alarm here is deciding that the process is not SOSS, where in fact it is. If the minimum error value is greater than ε, then the process is not second-order self-similar or the data is not large enough to make the right decision.

The procedure for testing whether a process is FARIMA(0,*d*,0) is exactly the same after replacing the autocorrelation function $\rho_H(k)$ by $\rho_H(k)$ and using *d* instead of *H*.

Splitting the control and data traffic groups further based on their direction with respect to the enterprise LAN (e.g., incoming or outgoing) is helpful to detect certain abnormal behaviors that might not be detected when looking at the two directions of traffic combined in the bidirectional traffic.

To test if a traffic sequence is LRD or not, we first select an aggregation interval over which we count the number of bytes and the number of packets in that interval. Second we select a time-window to apply the test. The aggregation interval to count the bytes and packets is selected based on the traffic rate, the higher the traffic rate, the smaller the aggregation interval can be. The objective is to have a high count variability (variance). This translates into not having a too small or too large aggregation interval, as either will result in low variability.

The selection of the size of the time-window over which the test is applied is based on the aggregation interval. The smaller the aggregation interval, the smaller the size of the time-window can be. The time-window should be large enough to observe the LRD behavior of the traffic sequence during normal benign normal traffic. However, it should not be too large that a short-duration abnormal behavior would not affect the LRD behavior of the traffic. Otherwise, it will be missed since it is suppressed by the remaining background traffic. Idris et. al discuss the tradeoff in selecting the time-window between reducing the miss rate by selecting a smaller window and reducing the false alarm rate by selecting a larger window [18]. Selecting a smaller time-window is useful in narrowing down where the abnormal behavior took place. But the same outcome can be achieved by using a sliding period (e.g., 50% of the window's size) to slide the time-window. This achieves narrowing down the time interval where the abnormal behavior took place. It also allows for faster detection as it doesn't wait for the next time-window to fully pass.

III. EXPERIMENTAL SETUP

A. The Network Intrusion Dataset

We use the Network Intrusion dataset provided by the Information Exploration Shootout project [13] in our study. Packet *header* information of the traffic passing by the network interface of the gateway connecting the enterprise LAN with the external network (Internet) is captured using tcpdump. The captured traffic consists of the communication between the LAN and the Internet, and the traffic communication within the LAN. tcpdump's filters were specified to only collect TCP and UDP packets. We only consider TCP packets. The packets' information is preprocessed and nicely organized in comma separated value (CVS) files. For each TCP packet, the following information is provided in the dataset:

Time stamp

- Source IP address
- Source port
- Destination IP address
- Destination port
- TCP Flag (e.g., SYN, FIN, PUSH, RST, or no flag is set)
- Data sequence number of the packet
- Data sequence number of the data expected in return
- Acknowledgment sequence number of the next data expected from the other direction on this connection
- Receiver window, which is number of bytes of receive buffer space available
- Length of the packet's payload

The IP addresses of *external* hosts are anonymized to protect the identity of the hosts during their network traffic collection. The IP addresses of *internal* hosts, however, are all anonymized to a *single* IP address. This is done to hide the enterprise network topology and ensure its privacy. The

latter anonymiztion highly limits the analysis of the traffic communication *within* the LAN.

The dataset consists of four files[1], each having 16-20 minutes of traffic. Based on our calculations, the average bit rate in these files is on the order of 1 Mbps. The first file, which we will refer to as the base file is clean and doesn't contain any simulated attacks. The remaining three files, each has instances of a single different *simulated* attack behavior. Although the attacks are injected by the collectors of the dataset, their targets and times are not given.

The three attacks stored in the files are: IP Spoofing, Password Guessing, and Port Scanning [13]. The first attack is widely known as TCP SYN flooding Denial of Service (DoS) attack. It works by an attacker that usually spoofs other IP source addresses. Then initiates many TCP connections to a victim's machine and leave them *half-open* to consume the victim's memory resources, hence, denying the service to other legitimate users. The second attack uses the content of the packet to guess passwords. The third attack looks for possible vulnerabilities to be exploited by scanning the ports of a network to see which ones are advertised by the network. This type of attack usually involves high packet data rates per host using different port numbers in these packets.

B. Results

In this section, we report the effect of the attacks in the Network Intrusion dataset on the LRD behavior of the packet and byte counts of the traffic. We look at the effect of the attacks on the control and data traffic sequences in different directions with respect to the LAN.

We first select an aggregation interval of 1 second to count the number of packets and the number of bytes. The 1-second aggregation interval is selected since it is suitable for the average traffic rate in the dataset, which is 132.7 K Bytes/second. The time window used to test the traffic sequences in the Network Intrusion dataset is the whole time period in each file, which is on the order of 1000 seconds. This is done to assure that enough amount of traffic is used to detect LRD behavior. Using a smaller time window (e.g., 500 seconds) is not sufficient to detect LRD behavior in the base file.

We apply *the Optimization method* [15] to test if the packet and byte counts of the incoming, outgoing, bidirectional, and intraLAN traffic sequences are LRD. The test checks whether the error function of either the second-order self-similar (SSOS) or fractional ARIMA (FARIMA) tests is below the threshold ε = 1e-3. If so, then the traffic sequence is LRD, otherwise it is not. We start by listing our observations followed by our analysis.

Tables 1 and 2 show the results of applying the test on the packet and byte counts in the base file, respectively. We observe that the error function of traffic sequences of the base file in all of the subgroups is less than the ε for the SOSS and for the FARIMA(0, *d*, 0) tests. Since LRD is implied by either one of the two tests, all traffic sequences in the base file exhibit LRD behavior.

Tables 3 and 4 show the results of applying the test on the packet and byte counts in the Attack 1 file, respectively. We observe in five cases that the error function of several traffic sequences is above ε (shown in bold) for *only* one of the two tests and not the other, therefore, they exhibit LRD. However, the error functions of both the packet and byte counts of the outgoing data traffic in the Attack 1 file is affected by the injected attack (TCP SYN) and are above ε, which cause this traffic not to exhibit LRD behavior in both of the packet and byte counts. This effect appears also in the byte count of the outgoing traffic when looked as a whole. However, it does not appear in the packet count of the outgoing traffic when looked as a whole. This is due to the fact that data packets have significantly more bytes than control packets, and hence affect the total byte count.

Tables 5 and 6 show the results of applying the test on the packet and byte counts in the Attack 2 file, respectively. As can be seen from the two tables, the injected attack (password guessing) did not affect the LRD behavior of the traffic. This means that the test failed to detect the attack with the window used. Tables 7 and 8 show the results of applying the test on the packet and byte counts in the Attack 3 file, respectively. The incoming control traffic is affected by the injected attack (port scan), which causes it not to exhibit LRD behavior. The effect only took place at the packet count.

We summarize our observations by noting that only the *incoming control* traffic or the *outgoing data* traffic fails to exhibit LRD behavior, whereas the traffic as a whole still exhibits LRD behavior. We reason that an attack from outside the LAN will mostly be carried through the incoming control traffic, and the response to this traffic appears mainly in the outgoing data traffic. Hence, these two subgroups are the only ones affected.

The first attack (TCP SYN flooding), is carried by few packets in the incoming control traffic, however, its damage affects the outgoing data traffic as the target machines' resources is depleted and the machines stop sending enough traffic for the outgoing data to be LRD. The third attack (port scan), is carried by many packets in the incoming control traffic, which causes it to not exhibit LRD behavior. The second attack (password guessing), uses both control and data planes traffic and is not as dense as a port scan, hence, it did not affect the LRD behavior.

Table 1. Testing LRD behavior of the packet count traffic sequences of the base file.

Traffic Sequence		SOSS Test		FARIMA Test		LRD?
Direction	Type	$\hat{H}$	Error	$\hat{d}$	Error	
incoming	control	0.85	5.18e-04	0.36	4.08e-04	Yes
	data	0.95	5.18e-04	0.45	4.12e-04	Yes
	whole	0.93	4.98e-04	0.44	4.56e-04	Yes
outgoing	control	0.90	7.78e-04	0.41	5.52e-04	Yes
	data	0.84	6.69e-04	0.35	5.34e-04	Yes
	whole	0.89	8.86e-04	0.40	6.93e-04	Yes
bidirectional	control	0.88	5.55e-04	0.39	4.54e-04	Yes
	data	0.93	6.97e-04	0.44	6.42e-04	Yes
	whole	0.91	7.49e-04	0.42	5.11e-04	Yes
interLAN	control	0.83	6.18e-04	0.34	4.28e-04	Yes
	data	0.91	5.81e-04	0.42	5.00e-04	Yes
	whole	0.91	5.23e-04	0.42	4.70e-04	Yes

[1] There is actually an additional fifth file, but surprisingly it is almost identical to the second file, thus, we discarded it.

Table 2. Testing LRD behavior of the byte count traffic sequences of the base file.

Traffic Sequence		SOSS Test		FARIMA Test		LRD?
Direction	Type	$\hat{H}$	Error	$\hat{d}$	Error	
incoming	control	0.85	9.48e-04	0.36	7.08e-04	Yes
	data	0.95	4.84e-04	0.45	4.03e-04	Yes
	whole	0.95	4.23e-04	0.45	4.21e-04	Yes
outgoing	control	0.89	9.41e-04	0.40	7.60e-04	Yes
	data	0.79	2.37e-04	0.30	2.59e-04	Yes
	whole	0.79	2.60e-04	0.30	2.83e-04	Yes
bidirectional	control	0.87	8.40e-04	0.38	6.53e-04	Yes
	data	0.94	5.47e-04	0.44	4.70e-04	Yes
	whole	0.94	4.98e-04	0.44	4.38e-04	Yes
interLAN	control	0.84	6.19e-04	0.35	4.25e-04	Yes
	data	0.86	9.79e-04	0.37	8.50e-04	Yes
	whole	0.86	9.72e-04	0.37	8.40e-04	Yes

Table 3. Testing LRD behavior of the packet count traffic sequences of the Attack 1 file.

Traffic Sequence		SOSS Test		FARIMA Test		LRD?
Direction	Type	$\hat{H}$	Error	$\hat{d}$	Error	
incoming	control	0.88	2.86e-04	0.39	2.34e-04	Yes
	data	0.87	**1.09e-03**	0.38	7.90e-04	Yes
	whole	0.89	6.88e-04	0.40	5.02e-04	Yes
outgoing	control	0.73	9.31e-04	0.25	8.10e-04	Yes
	data	0.90	**1.21e-03**	0.41	**1.39e-03**	**No**
	whole	0.82	5.48e-04	0.33	4.00e-04	Yes
bidirectional	control	0.78	9.40e-04	0.30	7.69e-04	Yes
	data	0.89	5.08e-04	0.40	4.49e-04	Yes
	whole	0.86	5.52e-04	0.37	3.71e-04	Yes
interLAN	control	0.89	6.88e-04	0.40	5.02e-04	Yes
	data	0.88	2.86e-04	0.39	2.34e-04	Yes
	whole	0.98	5.21e-04	0.48	4.90e-04	Yes

Table 4. Testing LRD behavior of the byte count traffic sequences of the Attack 1 file.

Traffic Sequence		SOSS Test		FARIMA Test		LRD?
Direction	Type	$\hat{H}$	Error	$\hat{d}$	Error	
incoming	control	0.87	7.90e-04	0.38	5.69e-04	Yes
	data	0.88	**1.06e-03**	0.39	7.83e-04	Yes
	whole	0.88	**1.07e-03**	0.39	7.84e-04	Yes
outgoing	control	0.73	9.31e-04	0.25	8.08e-04	Yes
	data	0.91	**1.76e-03**	0.41	**1.91e-03**	**No**
	whole	0.90	**1.76e-03**	0.41	**1.90e-03**	**No**
bidirectional	control	0.82	**1.12e-03**	0.34	8.82e-04	Yes
	data	0.90	8.75e-04	0.41	9.65e-04	Yes
	whole	0.90	8.26e-04	0.41	9.27e-04	Yes
interLAN	control	0.98	5.84e-04	0.48	5.06e-04	Yes
	data	0.98	8.44e-04	0.49	**1.06e-03**	Yes
	whole	0.98	8.40e-04	0.49	**1.07e-03**	Yes

Table 5. Testing LRD behavior of the packet count traffic sequences of the Attack 2 file.

Traffic Sequence		SOSS Test		FARIMA Test		LRD?
Direction	Type	$\hat{H}$	Error	$\hat{d}$	Error	
incoming	control	0.87	4.28e-04	0.38	3.00e-04	Yes
	data	0.94	7.04e-04	0.44	4.25e-04	Yes
	whole	0.91	4.41e-04	0.42	3.60e-04	Yes
outgoing	control	0.90	3.77e-04	0.41	2.04e-04	Yes
	data	0.90	2.75e-04	0.41	2.99e-04	Yes
	whole	0.89	2.51e-04	0.40	2.39e-04	Yes
bidirectional	control	0.89	5.40e-04	0.40	3.43e-04	Yes
	data	0.91	2.72e-04	0.42	1.33e-04	Yes
	whole	0.90	2.01e-04	0.41	1.92e-04	Yes
interLAN	control	0.85	**1.04e-03**	0.36	7.61e-04	Yes
	data	0.88	4.77e-04	0.39	3.19e-04	Yes
	whole	0.89	4.61e-04	0.40	3.31e-04	Yes

Table 6. Testing LRD behavior of the byte count traffic sequences of the Attack 2 file.

Traffic Sequence		SOSS Test		FARIMA Test		LRD?
Direction	Type	$\hat{H}$	Error	$\hat{d}$	Error	
incoming	control	0.87	**1.07e-03**	0.38	7.76e-04	Yes
	data	0.95	4.39e-04	0.45	2.17e-04	Yes
	whole	0.95	2.73e-04	0.45	2.45e-04	Yes
outgoing	control	0.90	4.08e-04	0.41	3.37e-04	Yes
	data	0.91	5.11e-04	0.41	5.78e-04	Yes
	whole	0.90	5.62e-04	0.41	6.03e-04	Yes
bidirectional	control	0.88	7.46e-04	0.39	5.07e-04	Yes
	data	0.91	2.03e-04	0.42	2.44e-04	Yes
	whole	0.91	1.97e-04	0.42	2.87e-04	Yes
interLAN	control	0.85	**1.05e-03**	0.36	7.69e-04	Yes
	data	0.89	5.67e-04	0.40	4.42e-04	Yes
	whole	0.89	5.65e-04	0.40	4.38e-04	Yes

Table 7. Testing LRD behavior of the packet count traffic sequences of the Attack 3 file.

Traffic Sequence		SOSS Test		FARIMA Test		LRD?
Direction	Type	$\hat{H}$	Error	$\hat{d}$	Error	
incoming	control	0.92	**1.66e-03**	0.43	**1.72e-03**	**No**
	data	0.94	6.37e-04	0.45	4.49e-04	Yes
	whole	0.91	3.70e-04	0.41	2.49e-04	Yes
outgoing	control	0.92	2.14e-04	0.43	1.77e-04	Yes
	data	0.91	6.42e-04	0.42	6.41e-04	Yes
	whole	0.90	3.71e-04	0.41	3.91e-04	Yes
bidirectional	control	0.89	1.52e-04	0.40	1.12e-04	Yes
	data	0.90	4.05e-04	0.41	2.30e-04	Yes
	whole	0.90	2.23e-04	0.41	2.00e-04	Yes
interLAN	control	0.87	9.30e-04	0.38	6.92e-04	Yes
	data	0.89	2.87e-04	0.39	3.16e-04	Yes
	whole	0.90	2.97e-04	0.40	2.39e-04	Yes

Table 8. Testing LRD behavior of the byte count traffic sequences of the Attack 3 file.

Traffic Sequence		SOSS Test		FARIMA Test		LRD?
Direction	Type	$\hat{H}$	Error	$\hat{d}$	Error	
Incoming	control	0.91	4.14e-04	0.41	3.03e-04	Yes
	data	0.95	4.24e-04	0.46	3.56e-04	Yes
	whole	0.95	3.98e-04	0.46	4.17e-04	Yes
Outgoing	control	0.91	3.35e-04	0.42	2.00e-04	Yes
	data	0.93	9.39e-04	0.43	**1.17e-03**	Yes
	whole	0.93	9.67e-04	0.43	**1.16e-03**	Yes
Bidirectional	control	0.88	3.97e-04	0.39	2.35e-04	Yes
	data	0.92	3.37e-04	0.43	3.07e-04	Yes
	whole	0.92	3.64e-04	0.43	2.94e-04	Yes
interLAN	control	0.86	9.92e-04	0.37	7.56e-04	Yes
	data	0.89	3.23e-04	0.40	2.62e-04	Yes
	whole	0.89	3.21e-04	0.40	2.57e-04	Yes

The LRD behaviors of the bidirectional and intraLAN traffic sequences, on the other hand, are not affected by any of the attacks. This is also the case for the outgoing control and incoming data traffic sequences. This is interesting since the incoming control and outgoing data traffic volume (measured in Bytes/second) constitutes less than 8% of the total traffic in the Network Intrusion dataset. This is useful, as it reduces the amount of traffic to be processed, hence, the amount of computations needed.

The results of using LRD behavior analysis of control and data planes traffic in the Network Intrusion dataset based on its direction show that it enables us to detect abnormal

behaviors that might not be detected by previous work that only look at the traffic as a whole. Moreover, this type of analysis requires less data to analyze, thus less computational effort when compared to looking at the whole traffic. This is true provided that the traffic is known to be LRD during the time of the day that the traffic is examined.

IV. CONCLUSIONS AND CURRENT WORK

We decomposed network header traffic into control and data planes to detect network abnormal behaviors that affect the aggregate traffic behavior. This is done based on our assumption that data traffic generation is based on control traffic generation. Hence, both traffic sequences have similar time variations, during normal benign behavior.

We analyzed the control and data planes of the TCP traffic of the Network Intrusion dataset to examine the LRD behavior of the traffic. We observed that the attacks in the dataset only caused the downstream control traffic or the upstream data traffic to not exhibit LRD behavior, whereas the traffic as a whole still exhibits LRD behavior. These two traffic subgroups, generally, have lower volume than the other two traffic subgroups, which are the downstream data and upstream control traffic. This significantly reduces the amount of network traffic in need of processing to detect network abnormal behavior. The LRD analysis of control and data planes traffic also allows us to detect abnormal behaviors that might not be detected by previous work that only looks at the traffic as a whole without its decomposition into control and data planes.

It was noted that we have applied the same analysis to the 1999 DARPA dataset [19]. However, our results show that the TCP traffic containing attacks in the different traffic subgroups still exhibit LRD behavior [20]. This implies that the various attacks did not affect LRD and therefore are not detectable by our methodology. To test the effectiveness of the methodology, we are currently analyzing a recently captured network traffic dataset [21]. We aim to reach more accurate conclusions about the LRD behavior of the control and data planes traffic.

ACKNOWLEDGEMENTS

Basil AsSadhan extends his appreciation to the Saudi National Science, Technology, and Innovation Plan (NSTIP) for funding this work through Research Project No. 10-INF1279-02.

REFERENCES

[1] B. AsSadhan, H. Kim, J. M. F. Moura, and X. Wang, "Network Traffic Behavior Analysis by Decomposition into Control and Data Planes," in *International Workshop on Security in Systems and Networks (SSN) in conjunction with the IEEE International Parallel and Distributed Processing Symposium (IPDPS)*, Miami, FL, USA, Apr. 18, 2008.

[2] B. AsSadhan and J. M. F. Moura, "An Efficient Method to Detect Periodic Behavior in Botnet Traffic by Analyzing Control Plane Traffic," *Journal of Advanced Research*, **5**(4), 435-448 (2014).

[3] B. AsSadhan, H. Kim, and J. M. F. Moura, "Long-Range Dependence Analysis of Control and Data Planes Network Traffic," presented at the Saudi International Innovation Conference (SIIC), Leeds, UK, Jun. 9 – 10, 2008.

[4] M. Crovella and A. Bestavros, "Self-similarity in World Wide Web traffic: Evidence and possible causes," *IEEE/ACM Transactions on Networking*, **5**(6), 835-845 (1997).

[5] W. Leland, M. Taqqu, W. Willinger, and D. Wilson, "On the self-similar nature of ethernet traffic (extended version)," *IEEE/ACM Transactions on Networking*, **2**(1), 1-15 (1994).

[6] V. Paxson and S. Floyd, "Wide-area traffic: The failure of Poisson modeling," *IEEE/ACM Transactions on Networking*, **3**(3), 226-244 (1995).

[7] P. R. M. Inacio, M. M. Freire, M. Pereira, and P. P. Monteiro, "Analysis of the Impact of Intensive Attacks on the Self-Similarity Degree of the Network Traffic," in *2nd International Conference on Emerging Security Information, Systems and Technologies (SECURWARE)*, Cap Esterel , France, Aug. 25 – 31, 2008.

[8] G. Kaur, V. Saxena, and J. P. Gupta, "A Novel Multi Scale Approach for Detecting High Bandwidth Aggregates in Network Traffic," *International Journal of Security and Its Applications (IJSIA),***7**(5), 81-100 (2013).

[9] M. Li, "Change trend of averaged Hurst parameter of traffic under DDOS flood attacks," *Computers & Security*, **25**(3), 213-220 (2006).

[10] M. Mazurek and P. Dymora, "Network anomaly detection based on the statistical self-similarity factor for HTTP protocol," *Przegląd Elektrotechniczny,* **1**, 127-130 (2014).

[11] P. Owezarski, "On the impact of DoS attacks on Internet traffic characteristics and QoS," in *Proceedings of 14th International Conference on Computer Communications and Networks (ICCCN)*, San Diego, CA, USA, Oct. 17–19, 2005, pp. 269 – 274.

[12] M. F. Rohani, M. A. Maarof, A. Selamat, and H. Kettani, "Multi-level sampling approach for continuous loss detection using iterative window and statistical model," *IIUM Engineering Journal*, **11**(2), 137-149 (2010).

[13] *Information Exploration Shootout Project*. Available: http://ivpr.cs.uml.edu/shootout/about.html. Accessed June 2014.

[14] O. Cappe, E. Moulines, J. C. Pesquet, A. Petropulu, and X. Yang, "Long-Range Dependence and Heavy-Tail Modeling for Teletraffic Data," *IEEE Signal Processing Magazine*, **19**(3), 14- 27 (2002).

[15] H. Kettani, "A Novel Approach to the Estimation of the Long-Range Dependence Parameter," Univ. of Wisconsin, 2002.

[16] H. Kettani and J. Gubner, "A Novel Approach to the Estimation of the Long-Range Dependence Parameter," *IEEE Transactions on Circuits and Systems*, **53**(6), 463-467 (2006).

[17] P. Abry and D. Veitch, "Wavelet Analysis of Long-Range Dependent Traffic," *IEEE Transactions on Information Theory*, **44**(1), 2-15 (1998).

[18] M. Y. Idris, A. H. Abdullah, and M. A. Maarof, "Iterative Window Size Estimation on Self-Similarity Measurement for Network Traffic Anomaly Detection," *International Journal on Computing and Information Sciences*, **2**(2),84-92 (2004).

[19] R. Lippmann, J. Haines, D. Fried, J. Korba, and K. Das, "The 1999 DARPA Off-Line Intrusion Detection Evaluation," in *the 3rd International Workshop on Recent Advances in Intrusion Detection (RAID)*, Toulouse, France, Oct. 2 – 4, 2000.

[20] B. AsSadhan, "Network Traffic Analysis Through Statistical Signal Processing Methods," Carnegie Mellon Univ., 2009.

[21] A. Bashaiwth, B. AsSadhan, J. Al-Muhtadi, and S. Alshebeili, "Efficient Detection of Real-World Botnets' Command and Control Channels Traffic," in *International Conference on Information and Communication Systems (ICICS)*, Irbid, Jordan, Apr. 1 – 3, 2014.