An Intrusion Detection Technique Based on Change in Hurst Parameter with Application to Network Security

C. M. Akujuobi, N. K. Ampah and Matthew N.O. Sadiku

Center of Excellence for Communication Systems Technology Research (CECSTR)
Prairie View A&M University, Prairie View, Texas 77446, USA

Summary

Securing Enterprise networks has been considered under two broad topics (i. e. Intrusion Detection Systems - IDS and Intrusion Prevention Systems - IPS). So far, there is no algorithm, which guarantees absolute protection for a given network from intruders. Most existing IDS and IPS techniques introduce high false positive and false negative rates, which need to be eliminated or reduced considerably. This paper will concentrate on network packets behavior leading to network-based intrusion detection. It will employ anomaly detection as its analysis strategy. In the field of signal analysis, the methods of wavelet transform have gotten wide application because of its unique merit. That novel idea will be tapped in this paper. The self-similarity property of real network traffic will be used together with the signal detection abilities of wavelets in detecting attacks. The justification for using change in Hurst parameter as an estimator for detection is given here. The technique used here will also try to reduce the effectiveness of distributed attacks, which deny authorized users access to system resources. Securing of all network security data, which is an important limitation to existing IDS and IPS is ensured by the techniques we used.

Key words:
Intrusion detection and prevention, enterprise network, anomaly detection, self-similarity, multi-resolution technique.

1. Introduction

Network security management has become very complex and dynamic in nature due to the rate at which the Internet is expanding and also due to the increase in the use of the Internet for various economic activities [1]. This has made the Internet or any network connected to the Internet a target to all sorts of attack. As a result, security incidents have escalated in frequency and economic seriousness. The development of intrusion detection and prevention systems has therefore acquired increasing commercial importance in order to block or prevent all possible attacks on a given network [2] [3] [4].

Generally, attacks are assumed to emanate from outside a given network, but the most dangerous attacks come from within the enterprise network itself. A layer approach is used since there is no single technique that guarantees absolute security against all attacks on a given network. Intrusion detection, which is a traditional technique, detects attacks only after they have entered the network. Intrusion prevention, which is a proactive technique, prevents the attacks from entering the network. Unfortunately, some of the attacks still bypass the intrusion prevention systems.

All previous works involving intrusion detection and prevention in enterprise network used both signature-based and/or anomaly detection [2] [3] [5] [6]. The following are their shortcomings: Under anomaly detection anything unusual is considered suspect, thereby introducing high false positive and false negative rates; managing security data and normal enterprise network data on the same network poses greater security risk; and managing security data and normal network data on the same network also reduces bandwidth for normal operations of enterprise network.

The conventional network-based, anomaly intrusion detection system will employ change in Hurst parameter as its parameter for detection just like the new approach. This is because the objective here focuses on the application of multi-resolution techniques and its effects on the intrusion detection and prevention system. Figure 1 shows how the network for the conventional technique will look like. Here, data collected from each IDS is transmitted to the Central Detection Point through the network itself and finally through the Central Security Server or Central Router Device. This means that the Central Detection Point is only connected to the Central Security Server or Central Router Device.

The new approach will make use of multi-resolution techniques and that will form the basis for the first scenario. Here, data collected from each IDS is transmitted directly to the Central Detection Point without going through the network itself. The transmission can be by any means (i. e. wired or wireless). This means that the Central Detection Point is not connected to the Central Security Server or Central Router Device as was described in the conventional approach. Instead, each IDS is connected directly to the Central Detection Point. Figure 2 shows how the network for the new technique (approach) will look like.

Manuscript received May 5, 2007
Manuscript revised May 20, 2007

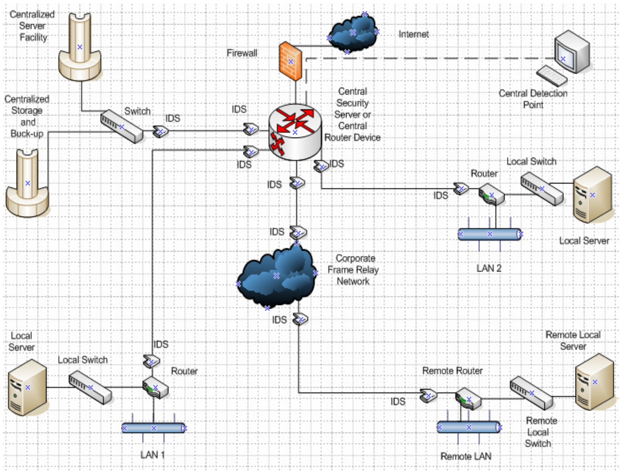

Fig. 1. Conventional technique with network-based IDS.

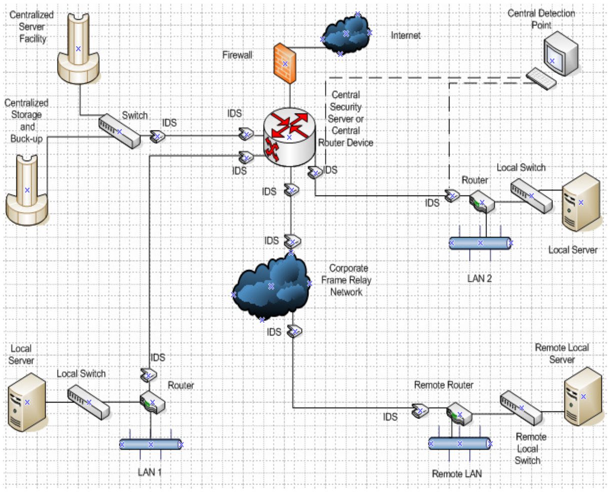

Fig. 2. New approach with network-based IDS.

The general objective of this research work was to design and develop a network-based intrusion detection system, which uses anomaly detection techniques. In anomaly detection anything unusual is considered a suspect. Unlike all anomaly detection techniques, which depend on just the behavior of the network, this system used a quantitative approach. The quantity used was the change in Hurst parameter of the network traffic at specific points in the network after an attack or intrusion [5]. No matter the type of attack traffic present, there will always be a change in Hurst parameter registered, thereby enabling the IDS to detect the attack. The novelty of this approach lies in the fact that no existing intrusion detection system (IDS) employs the change in Hurst parameter as a parameter for detecting intrusion. Multi-resolution technique was used to transmit data from the network to the Central Detection Point instead of transmitting through the network itself [5] [6].

Only the signal processing applications of wavelets is taken advantage of in this work. In the field of signal analysis, the methods of wavelet transform have gotten wide application because of its unique merit. One of the important applications is multi-resolution techniques, which will be used to decompose, transmit and reconstruct signals from the enterprise network to a Central Detection Point for further analysis (i. e. in the case of the new approach). The outcome of all new detections made will eventually be used to update the attack list of the intrusion prevention systems [7]. Two scenarios will be considered in this research work. The first scenario applies multi-resolution techniques, but the second will not. Results from both scenarios will be compared and conclusions made.

Section 2 describes self-similar stochastic process mathematically. It further relates the existence of self-similarity to Hurst parameter. Section 3 shows how the new approach was modeled. Section 4 discusses the simulation results using both the new approach and the conventional method. Section 5 states the conclusions and section 6 outlines the future works. This is followed by the references used for this work.

2. Self-Similar Stochastic Process

The m-aggregated time series

$$\mathrm{X}^{(m)} = \{\mathrm{X}_k^{(m)}, k = 0, 1,\ 2, ...\} \text{ is defined as:}$$

$$\mathrm{X}_k^{(m)} = \frac{1}{m}\sum_{i=km-(m-1)}^{km} \mathrm{X}_i \qquad (1)$$

If the process has the same statistical properties at all values of m (all aggregations), then that process is self-similar. Self-similarity for a process is defined in terms of its var[X(t)] and autocorrelation R(t_1, t_2):

$$\mathrm{Var}[\mathrm{X}(t)]=\mathrm{E}[\mathrm{X}^2(t)]-\mu^2(t), \qquad (2)$$

where

μ - The mean of X.

$$\mathrm{R}(t_1,t_2)=\mathrm{E}[\mathrm{X}(t_1)\mathrm{X}(t_2)] \qquad (3)$$

A process X is exactly self-similar with parameter β ($0 < \beta < 1$) if for all m = 1, 2, …,

$$Var(X^{(m)}) = \frac{Var(X)}{m^{\beta}} \qquad (4)$$

$$R_{X^{(m)}}(X) = R(t_1, t_1 + k) = R_X(k) \tag{5}$$

In many cases a weaker definition is needed: A process X is asymptotically self-similar with parameter β (0 < β < 1) if for all k large enough,

$$Var(\mathrm{X}^{(m)}) = \frac{Var(\mathrm{X})}{m^{\beta}} \tag{6}$$

$$R_{X^{(m)}}(k) \rightarrow R_X(k) \ as \ m \rightarrow \infty \tag{7}$$

The variance of a self-similar process decreases proportional to $1/m^{\beta}$ as *m* approaches infinity. Equation 7 shows that the autocorrelation of the aggregated process has the same form as the original one, which suggests that the degree of variability is the same at all time resolutions. The variable

$$H = 1 - \frac{\beta}{2}, \quad 0 < \beta < 1 \tag{8}$$

is known as the Hurst parameter, and gives the degree of self-similarity of a process. When H = 0.5, self-similarity doesn't exist. The degree of self-similarity increases as H approaches one. Network traffic has been proven to exhibit self-similar properties [8], [9], [10].

3. Modeling the Estimator

A reasonable model for estimating the change in Hurst parameter, ΔH will be based on the model for detecting a DC signal or level in the presence of White Gaussian Noise, WGN [11]. That model is represented by the following equation:

$$x[n] = A + w[n], \ n = 0, 1, \ldots, N-1. \tag{9}$$

where $x[n]$ - Data for the DC signal or level with WGN (with intrusion);
A - The DC signal level to be estimated;
$w[n]$ - WGN samples with each sample having the PDF N(0, σ^2), which denotes a Gaussian distribution with a zero mean and a variance of σ^2. Please note that intrusion is represented by White Gaussian Noise under this model.
The expression for the change in Hurst parameter with and without noise will be:

$$\Delta H = H_1 - H \tag{10}$$

where ΔH - Change in Hurst parameter, which is assumed to be always positive;
H_1 - Hurst parameter of signal with WGN (intrusion);
H - Hurst parameter of signal without WGN (no intrusion).
Re-writing equation (10) in the form of equation (9) gives:

$$H[n] = \Delta H + H_1[n], \ n = 0, 1, \ldots, N-1. \tag{11}$$

Please note that there is no negative sign in front of ΔH, since it is assumed to be always positive.
The probability density function of the distribution $x[n]$ will be:

$$p(x; A) = \prod_{n=0}^{N-1} \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left[-\frac{1}{2\sigma^2}(x[n] - A)^2\right]$$

$$p(x; A) = \frac{1}{(2\pi\sigma^2)^{N/2}} \exp\left[-\frac{1}{2\sigma^2}\sum_{n=0}^{N-1}(x[n] - A^2)\right] \tag{12}$$

Similarly, the PDF of the distribution, H[n] will be:

$$p(H; \Delta H) = \frac{1}{(2\pi\sigma^2)^{N/2}} \exp\left[-\frac{1}{2\sigma^2}\sum_{n=0}^{N-1}(H[n] - \Delta H^2)\right] \tag{13}$$

The log-likelihood function of equation (13) will be:

$$\ln p(H; \Delta H) = -\ln[(2\pi\sigma^2)^{N/2}] - \frac{1}{2\sigma^2}\sum_{n=0}^{N-1}(H[n] - \Delta H)^2$$

$$\ln p(H; \Delta H) = -\frac{N}{2}\ln[(2\pi\sigma^2)] - \frac{1}{2\sigma^2}\sum_{n=0}^{N-1}(H[n] - \Delta H)^2 \tag{14}$$

The maximum likelihood estimation (MLE) of ΔH is found by equating the derivative of the log-likelihood function (i.e. equation (14)) to zero:

$$\frac{\partial \ln p(H; \Delta H)}{\partial \Delta H} = \frac{1}{\sigma^2}\sum_{n=0}^{N-1}(H[n] - \Delta H) = 0 \tag{15}$$

$$\sum_{n=0}^{N-1}(H[n] - \Delta H) = 0$$

$$\sum_{n=0}^{N-1} H[n] - \sum_{n=0}^{N-1} \Delta H = 0$$

$$\sum_{n=0}^{N-1} H[n] - N\Delta H = 0$$

$$\therefore \Delta\hat{H} = \frac{1}{N}\sum_{n=0}^{N-1} H[n] \tag{16}$$

Although the maximum likelihood procedure yields an estimator that is asymptotically efficient, it also sometimes yields an efficient estimator for finite data records. It follows

from equation (16) that the estimation of ΔH is the same as finding the sample mean of $H[n]$, which is already known to be an efficient estimator. Hence the MLE of ΔH found here is efficient. For the purpose of this work, values of ΔH will be used instead of $H[n]$ in order to analyze the effect ΔH on detection. It is also clear from equation (11) that, H [n] is directly proportional to ΔH for any given value of "n".
Equation (15) can be re-written as follows:

$$\frac{\partial \ln p(H;\Delta H)}{\partial \Delta H}=\frac{1}{\sigma^2}\sum_{n=0}^{N-1}(H[n]-\Delta H)=\frac{N}{\sigma^2}(\overline{H}-\Delta H) \quad (17)$$

where $\overline{H}$ - The sample mean of $H[n]$.
To find the Crame-Rao Lower Bound (CRLB) of the estimator ΔH , we need to take the second derivative of equation (17):

$$\frac{\partial^2 \ln p(H;\Delta H)}{\partial \Delta H^2}=-\frac{N}{\sigma^2} \quad (18)$$

The variance of any unbiased estimator $\hat{\theta}$ must satisfy the following expression:

$$Var(\hat{\theta}) \geq \frac{1}{-E\left[\frac{\partial^2 \ln p(x;\theta)}{\partial \theta^2}\right]} \quad (19)$$

where the derivative is evaluated at the true value of θ and the estimation is taken with respect to $p(x;\theta)$. But,

$$-E\left[\frac{\partial^2 \ln p(x;\theta)}{\partial \theta^2}\right]=-\left[-\frac{N}{\sigma^2}\right]=\frac{N}{\sigma^2} \quad (20)$$

since N/σ^2 is a constant.
From expression (19) and equation (20), we get the following:

$$Var(\Delta\hat{H}) \geq \frac{\sigma^2}{N} \quad (21)$$

An unbiased estimator may be found that attains the bound for all θ if and only if:

$$\frac{\partial \ln p(x;\theta)}{\partial \theta}=I(\theta)(g(x)-\theta) \quad (22)$$

for some functions g and I. That estimator, which is the minimum variance unbiased estimator (MVUE) is $\hat{\theta}=g(x)$, and the minimum variance is $1/I(\theta)$, where $I(\theta)$ is the Fisher Information. Comparing equations (17) and (22), it is clear that the MVUE of ΔH (i. e. $\Delta\hat{H}$) is the sample mean of $H[n]$ (i. e. $\overline{H}$) just as obtained for the MLE case and $I(\theta)$ will be equal to

$$\frac{N}{\sigma^2} \text{ or } \frac{1}{Var(\Delta\hat{H})}.$$

It is clear from the analysis made in finding the MLE and CRLB for $\Delta\hat{H}$ that the proposed estimator, $\Delta\hat{H}$ is asymptotically unbiased and asymptotically achieves the CRLB. Hence, it is asymptotically efficient.

4. Simulation Studies

4.1 New Approach (with Multi-resolution Technique)

For the purpose of this work, MATLAB codes for Pareto Distribution was used to generate the network traffic, but real traffic will be used at the implementation stage of this research work. Figure 3 shows the graph of the generated network traffic with a target Hurst Parameter, H_T of 0.75. MATLAB codes were used for the entire work.

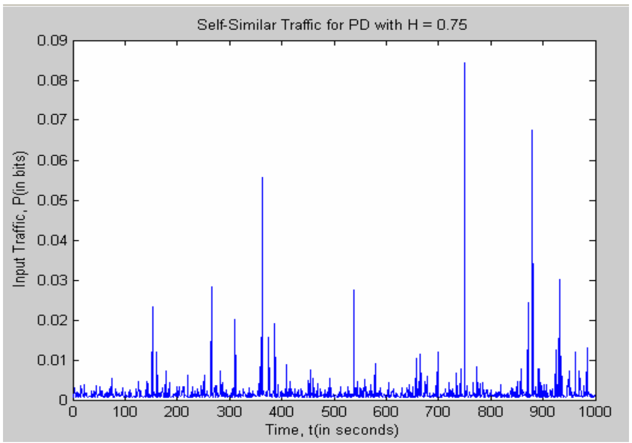

Fig. 3. Self-similar Input Traffic or Input Network Traffic without Intrusion (for H_T =0.75).

The Rescaled Adjusted Range Statistic Analysis (i.e. R/S Analysis) was used to test the generated self-similar input traffic. It estimated the Hurst Parameter (i. e. Calculated H_E) and compared it to H_T. Figure 4 shows the results after calculating the estimated Hurst Parameter, H_E.

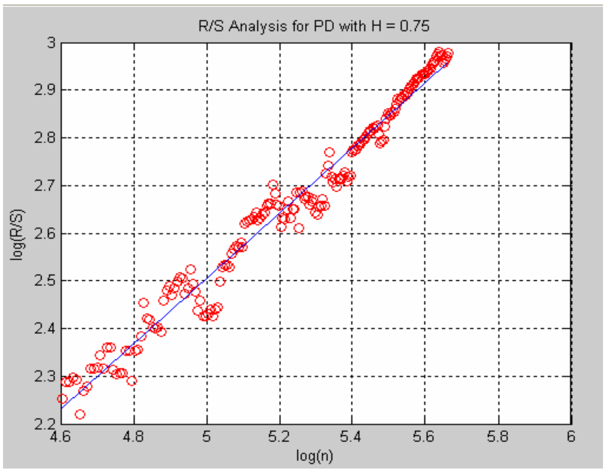

Fig. 4. Best Straight Line obtained from testing the generated traffic without intrusion or noise.

Please note that the gradient of the best straight line is the same as H_E. The equation of the best straight line from the simulation was:

Y = 0.6848X - 0.9196

so, H_E = <u>0.6848</u>

As stated earlier, the final analysis of the network traffic will be carried out at the Central Detection Point. Transmission of traffic from the network to the Central Detection Point was done using a Two-stage Multi-resolution Techniques. Haar Wavelets was applied here. Figure 5 shows the scheme for the multi-resolution technique.

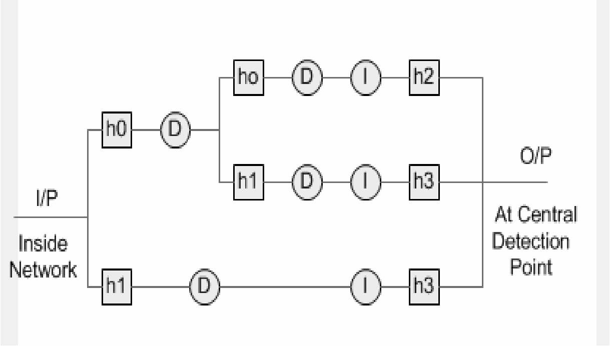

Fig. 5. Scheme for the multi-resolution technique.

The Rescaled Adjusted Range Statistic Analysis (i.e. R/S Analysis) was again used to test the received self-similar output traffic. Here, the estimated Hurst Parameter, H_E was calculated for the received output signal and compared to that obtained during the test before the transmission. Figure 6 shows the results after calculating the estimated Hurst Parameter, H_E.

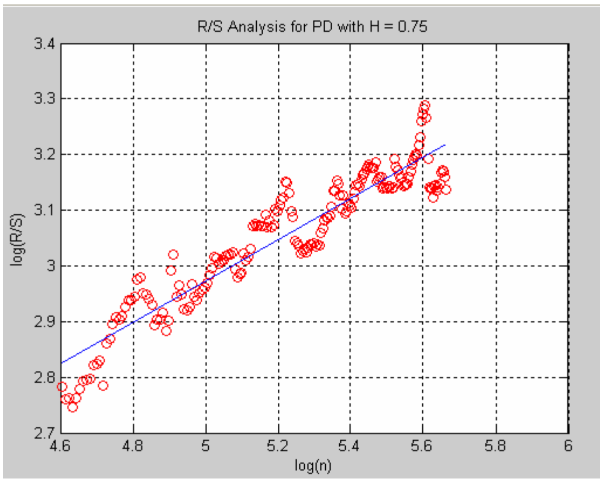

Fig. 6. Best Straight Line obtained from testing the output traffic.

Here also, the gradient of the best straight line is the same as H_E. The equation of the best straight line from the simulation was:

Y = 0.3704X + 1.1204

so, H_E = <u>0.3704</u>

The value for H_E should have been closer to its value for the test before the multi-resolution technique (i. e. H_E =0.6848) as observed for the other values of H_T. But, since Pareto Distribution itself involves the use of random number generation, it is expected to occasionally experience such an anomaly.

The worst network attacks are known to be distributive by nature, so all the generators considered in modeling intrusion generate distributive noise. Gaussian Noise Generator was chosen to model intrusion because unlike Rayleigh Noise Generator and Rician Noise Generator, it generates distributive noise with given mean and variance values. The others generate distributive noise without given mean and variance values, hence they are less flexible to use [6]. The chosen Gaussian Noise Generator added Additive White Gaussian Noise (AWGN) to the input signal with the assumption that the signal-to-noise ratio was 10dB. Figure 7 shows the graph of input traffic without intrusion or noise and input traffic with intrusion or noise.

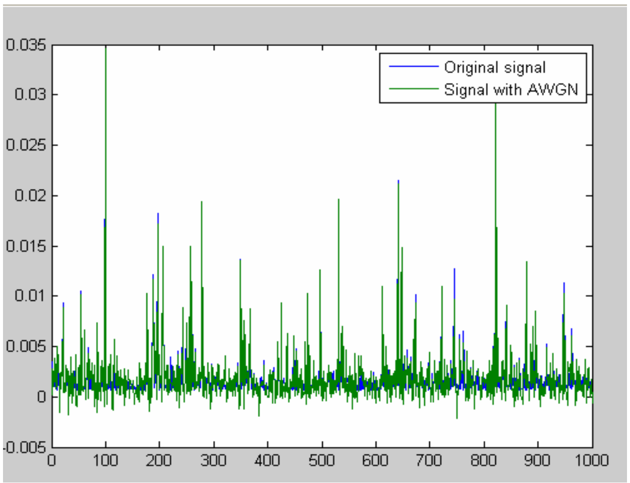

Fig. 7. Original Input Traffic and Original Input Traffic with Intrusion (Noise).

Testing (Here, H_E was not compared to any targeted value as before.), and transmission of the generated self-similar input traffic with intrusion or noise was done as before. Testing of the received self-similar output traffic with intrusion or noise was also done as before. (But here, the estimated Hurst Parameter, H_E was compared to that obtained during the test before the transmission.) Figure 8 shows the results of calculating the estimated Hurst Parameter, H_E for the signal with intrusion or noise, and Figure 9 shows the results of calculating the estimated Hurst Parameter, H_E for the output signal after applying multi-resolution technique.

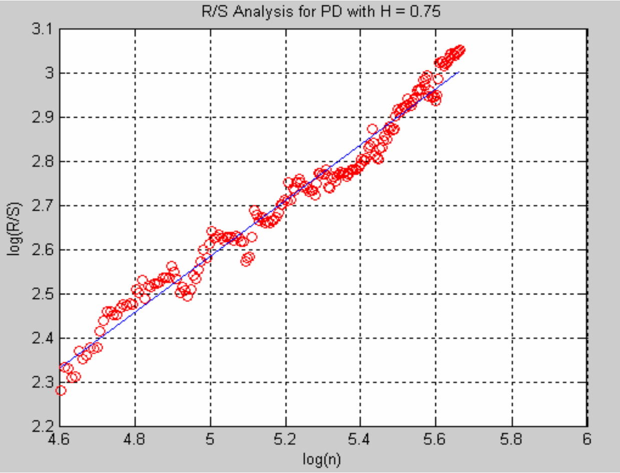

Fig. 8. Best Straight Line obtained from testing the generated traffic with intrusion or noise.

Here also, the gradient of the best straight line is the same as $H_{E.}$ The equation of the best straight line from the simulation was:

Y = 0.6349X - 0.5914

so, H_E = <u>0.6349</u>

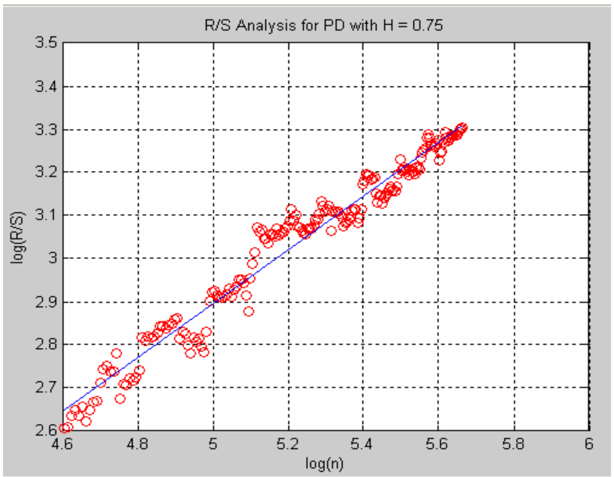

Fig. 9. Best Straight Line obtained from testing the output traffic.

Here also, the gradient of the best straight line is the same as $H_{E.}$ The equation of the best straight line from the simulation was:

Y = 0.6255X - 0.2321

so, H_E = <u>0.6255</u>

Everything done so far was for H_T = 0.75. An extension form this stage compared H_E values before and after transmission for input traffic without intrusion (noise) and for input traffic with intrusion (noise). The values of H_T used for this analysis were: 0.55, 0.65, 0.75, 0.85, and 0.95. Table 1 shows the results of all the tests and the changes in Hurst parameter for all H_T.

For a better analysis of the results, ten sets of values were used instead of one. This helped to substantiate the above changes involving the Hurst Parameters of the output signals without and with intrusion. The Hurst Parameters of output signals without and with intrusion in figure 10 are the most important statistics out of the rest because it clearly shows the differences or changes in the various values.

TABLE 1: Results of all tests and changes in Hurst parameter.

Targeted Hurst parameter	Signal without intrusion (noise)		Signal with intrusion (noise)		Change in Hurst parameter (outputs)
	Input Signal	Output Signal	Input Signal	Output Signal	$\Delta H_{E4}= H_{E2}-H_{E4}$
H_T	H_{E1}	H_{E2}	H_{E3}	H_{E4}	
0.55	0.54	0.45	0.64	0.46	-0.01
0.65	0.40	0.52	0.49	0.67	-0.16
0.75	0.68	0.37	0.63	0.63	-0.26
0.85	0.60	0.49	0.53	0.51	-0.01
0.95	0.46	0.47	0.60	0.50	-0.04

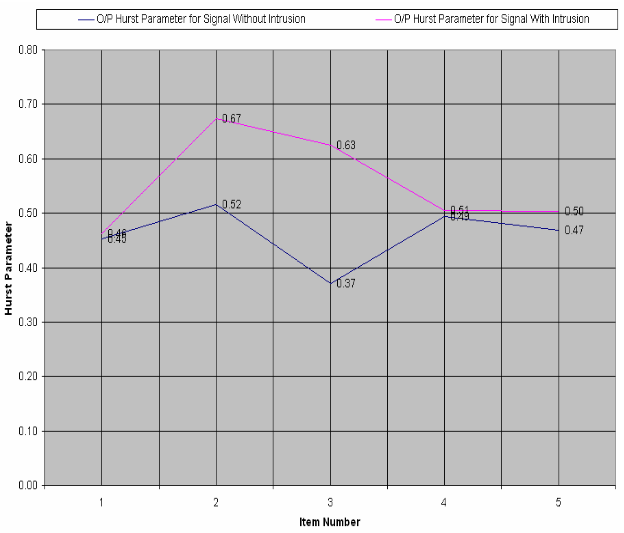

Fig. 10. Hurst Parameter for O/P signals without/with intrusion.

The power of output signals without and with intrusion did not show any substantial differences or changes, so investigations on power values were not considered further. The differences or changes in the Hurst Parameter will be very relevant at the Central Detection Point for detecting the presence of an intrusion.

Given a collection of data, statistics may be employed to summarize or describe the data by applying a descriptive statistics approach. Descriptive statistics refers to any of the many techniques used to summarize a set of data. Here, the data on members of a set are used to describe the set. For the purpose of this work, arithmetic mean and standard deviation were applied to verify how the changes were related to each other across 0.55 < H < 0.95. Mean and standard deviation were calculated for each of the 10 simulations. Table 2 shows three sets of results indicating the changes in Hurst parameter for the chosen H_T values out of the ten simulations. The mean and standard deviation values were calculated using the following equations:

$$\bar{x}=\frac{1}{N}\sum_{i=1}^{N}x_i \qquad (23)$$

$$\sigma=\sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i-\bar{x})^2} \qquad (24)$$

TABLE 2: Results from three out of ten tests showing changes in Hurst parameter, mean and standard deviation.

H_T	H_{E2}	H_{E4}	$\Delta H_{E4}=H_{E2}-H_{E4}$		Mean	Standard deviation
			Raw value	Absolute value		
First set of data						
0.55	0.45	0.46	-0.01	0.01	0.1	0.1
0.65	0.52	0.67	-0.16	0.16		
0.75	0.37	0.63	-0.26	0.26		
0.85	0.49	0.51	-0.01	0.01		
0.95	0.47	0.50	-0.04	0.04		
Second set of data						
0.55	0.60	0.75	-0.15	0.15	0.16	0.1
0.65	0.60	0.29	0.31	0.31		
0.75	0.44	0.47	-0.03	0.03		
0.85	0.48	0.39	0.09	0.09		
0.95	0.41	0.63	-0.22	0.22		
Third set of data						
0.55	0.66	0.64	0.02	0.02	0.11	0.07
0.65	0.50	0.40	0.10	0.1		
0.75	0.45	0.37	0.08	0.08		
0.85	0.52	0.63	-0.11	0.11		
0.95	0.61	0.37	0.24	0.24		

The nominal value of change in Hurst Parameter was the minimum value that indicated the presence of intrusion. This value was the mean of all the means (i. e. for the 10 sets of simulations) calculated from Table 3. Again, the standard deviation needed to be calculated for the 10 sets of mean to ensure that all its values were really close to the new mean or nominal value of change [7]. Although there were mean values lower than the mean of all the ten mean values, the target here was to get the most serious distributive attacks, which will definitely cause large changes in Hurst parameter.

TABLE 3: Mean and standard deviation for ten simulations.

Simulation number	Mean	Standard deviation
1	0.096	0.0989
2	0.16	0.098
3	0.11	0.0721
4	0.07	0.039
5	0.174	0.0587
6	0.136	0.106
7	0.062	0.0461
8	0.092	0.0736
9	0.076	0.0485
10	0.106	0.0618

From Table 3, the new mean or the nominal value of change, $\Delta \mathrm{H}$ and the standard deviation, σ_x was found as follows:

$$\Delta \mathrm{H} = \underline{0.108} \quad \text{and} \quad \sigma_x = \underline{0.0358}$$

Considering the above value for $\Delta \mathrm{H}$ and the range of "H" used in the simulation studies (i. e. 0.55 < H < 0.95), the nominal value of change in percentage was calculated as follows:

$$\Delta \mathrm{H}(\%) = \frac{0.108}{(0.95 - 0.55)} \times 100\% = 27\%$$

4.2 Conventional Method (without Multi-resolution Technique)

Everything done to this stage involved the application of multi-resolution techniques in decomposing, transmitting and reconstructing signals from the network to the Central Detection Point. The whole exercise was repeated, but without using multi-resolution techniques. In this case, the input signals were the same as the output signals because of the absence of the multi-resolution techniques. This implies that all the previous codes were reused up to and not beyond the input stages.

The nominal value of change in Hurst Parameter was found just as in the first scenario. The new mean or the nominal value of change, $\Delta \mathrm{H}$ and the standard deviation, σ_x were found as follows:

$$\Delta \mathrm{H} = \underline{0.1084} \quad \text{and} \quad \sigma_x = \underline{0.0302}$$

Considering the above value for $\Delta \mathrm{H}$ and the range of "H" used in the simulation studies (i. e. 0.55 < H < 0.95), the nominal value of change in percentage was calculated as follows:

$$\Delta \mathrm{H}(\%) = \frac{0.1084}{(0.95 - 0.55)} \times 100\% = 27.1\%$$

The following are the specific reasons why the approach used here is better than previous ones:

- The technique used in [1] depended solely on data from the TCP and IP headers, which can be compromised by an intruder launching attacks from a trusted host (zombie);
- The performance metric (ψ – precision) used in [2] and [3], depended on parameters from only the network security data files and not from the entire network characteristic with and without intrusion as described here by the Hurst parameter;
- The technique in [4] was an authentication method, but it is well known that authentication methods are good till they are broken. IDS techniques work better;
- The authors in [5] used Hurst parameter alright, but they did not investigate how the presence of intrusion affects Hurst parameter and further helps in detecting intrusion;
- The technique used in [6] depended on TCP/IP connections, which can be compromised by an intruder launching attacks from a trusted host (zombie).

5. Conclusion

The standard deviations for all the 10 sets of values (with and without multi-resolution techniques) were almost the same and very close to zero. This means that the changes or differences in Hurst Parameter were very close to each other across all values of "H" (i. e. 0.55 < H < 0.95).

Also, the nominal values of change in Hurst Parameter, $\Delta \mathrm{H}$ (with and without multi-resolution techniques) were equal to 0.108 and 0.1084 respectively. The corresponding standard deviations, σ_x were also 0.0358 and 0.0302 respectively. This also proved that both 10 sets of mean values were close to each other and also close to ΔH, since both σ_x values were close to zero.

The $\Delta H(\%)$ values (with and without multi-resolution techniques) which were equal to 27% and 27.1% respectively of the range of "H" used for the entire simulation, represented effective minimum changes beyond which an intrusion can be detected. Therefore, setting a minimum value of $\Delta H(\%)$ will ensure effective detection at the Central Detection Point making $\Delta H(\%)$ a strong parameter for intrusion detection. This will further help reduce high false positive and false negative rates.

Finally, $\Delta H(\%)$ values for both scenarios (with and without multi-resolution techniques) were the same due to the unique merit of multi-resolution techniques in signal analysis. The scenario with multi-resolution techniques has the following advantages:

- Analysis of data after detection can be done anywhere (i.e. way beyond the network);
- Transmission of data after detection can be done separately without going through the network itself thereby saving bandwidth.
- Handling security data separately from the main network makes it more difficult for attackers to attack the security network or system itself.

6. Future Work

The following areas will be considered for further investigation:

- Implementation of technique (i. e. Where to place detectors in the network.);
- The effect of different signal-to-noise ratios after adding AWGN to the input traffic on the change in Hurst parameter and the intrusion detection criterion;
- The use of confidence interval in the estimation of change in Hurst parameter;
- The best type of multi-resolution technique to use (i. e. 1-D, 1-Stage or 1-D, 2-Stage or 1-D, 3-Stage etc.);
- The best type of wavelet to use (i. e. Haar, Daubechies, Morlet etc.);
- Using of real network traffic and real intrusion for better results;
- Power studies for output signals without and with intrusion;
- Choice of noise generator to be reconsidered for improvement if possible;
- Choice of network traffic generator to be reconsidered for improvement if possible;
- Other statistics should be considered apart from mean and standard deviation.

References

[1] Hixon, R. and Gruenbacher, D. M. "Markov chains in network intrusion detection", *Proc. of IEEE SMC, 2004,* pp. 432 – 433.

[2] Wu Liu; Hai-Xin Duan; Ping Ren; Xing Li; Jian-Ping Wu, "Wavelet based data mining and querying in network security databases", *Machine Learning and Cybernetics, Vol. 1, 2003,* pp. 178 – 182.

[3] Wu Liu, Hai-Xin Duan, Peng Wang, Jian-Ping Wu, Lu Yang, "Wavelet-based analysis of network security databases", *Communication Technology Proceedings, Vol. 1, 2003,* pp. 372 – 377.

[4] Yong Sheng; Phoha, V. V.; Rovnyak, S. M. "A parallel decision tree-based method for user authentication based on keystroke patterns", *Systems, Man and Cybernetics, Part B, IEEE Transactions, 2005,* Vol. 35, pp. 826 – 833.

[5] Nash, D. A. and Ragsdale D. J. "Simulation of self-similarity in network utilization patterns as a precursor to automated testing of intrusion detection systems", *Systems, Man and Cybernetics, Part A, IEEE Transactions, 2001, Vol. 31,* pp. 327 – 331

[6] Garcia, R. C.; Sadiku, M. N. O.; Cannady, J. D. "WAID: wavelet analysis intrusion detection", *Circuits and Systems, 2002, vol. 3,* pp. 688 – 691.

[7] Graps, A. "An introduction to wavelets", Computer Science and Engineering, 1995, Vol. 2, pp. 50 – 61.

[8] Song Shibin, J. K.-Y. Ng, and Tang Bihai, "Some results on the self-similarity property in communication networks," *IEEE Trans. Communications*, vol. 52, no. 10, 2004, pp. 1636 – 1642.

[9] Sun Qinghua, and Liang Xiongjian, "The fractal feature of telecommunication network" in Poc. *IEEE ICCT , 2003*, vol. 1, pp. 77 – 80.

[10] Erramilli, M. Roughan, D. Veitch, and W. Willinger, "Self-similar traffic and network dynamics" in Poc. *IEEE, 2002*, vol. 90, no. 5, pp. 800 – 819.

[11] Kay, S. M. "Fundamentals of Statistical Signal Processing - Estimation Theory", Prentice Hall Signal Processing Series, 1993, Chapters 1 – 7.

Cajetan M. Akujuobi received the B.S. degree from Southern University, Baton Rouge, LA, in 1980, the M.S. degree from Tuskegee University, AL, in 1983, and the Ph.D. degree from George Mason University, Fairfax, VA, in 1995, all in electrical engineering, and the M.B.A. degree from Hampton University, Hampton, VA, in 1987. He is a Professor in the Department of Electrical Engineering and is the founding Director of Analog Mixed Signal, DSP Solutions and High Speed (Broadband) Communication Programs at Prairie View A & M University, Prairie View, TX. He is also the founding Director of the Center of Excellence for Communication System Technology Research. His research interests include signal/image processing and communication systems (broadband telecommunications) using such tools as wavelet and fractal transforms. His other research interests are in the areas of DSP solutions, analog mixed-signal systems, and control system-based communications. He was a participant and collaborative Member of ANSI TIE1.4 Working Group that had the technical responsibility of developing T1.413, Issue 2 ADSL standard. He has published extensively and has also written many technical reports. He was selected as one of the U.S. representatives for engineering educational and consultation mission to Asia in 1989. Prof. Akujuobi is a Senior Member of IEEE, ISA, ASEE, SPIE, and Sigma Xi, the Scientific Research Society. He is one of the founding corporate members of the IEEE Standards Association (IEEE-SA), Industry Advisory Committee (IAC).

Matthew N. O. Sadiku is presently a professor at Prairie View A&M University. He was a professor at Temple University, Philadelphia and Florida Atlantic University, Boca Raton. He is the author of over 150 papers and 26 books including *Elements of Electromagnetics* (Oxford, 4th ed., 2007) and *Numerical Techniques in Electromagnetics* (CRC, 2nd ed. 2001), *Metropolitan Area Networks* (CRC Press, 1995), and *Fundamentals of Electric Circuits* (McGraw-Hill, 3rd ed., 2007, with Charles Alexander). His current research interests are in the areas of numerical techniques in electromagnetics and computer communications networks. He is a senior member of the IEEE.

Nana K. Ampah is currently a post-graduate student at Prairie View A & M University. He is a student member of IEEE and belongs to organizations such as Ghana Institute of Engineers - GhIE (Associate Member) and Ghana Institute of Management and Public Administration (GIMPA) Alumni Association (Member). Nana K. Ampah graduated from Prairie View A & M University with an M.S.E.E. in Communications in May, 2004. He also graduated from Kiev Polytechnic Institute (KPI) in Kiev, Ukraine in June, 1993 with an M.S.E.E. specializing in Power Systems and Networks. He was also awarded a Post-graduate Certificate in Urban Management by GIMPA in June, 2001. He worked with the Electricity Company of Ghana for 8 years and has over 6 years experience in the design, construction, commissioning and management of urban and rural electrification projects. He was a Project Engineer under a World Bank funded urban/rural electrification project from 1996 to 2002. He also worked with Skanska Jensen International as a Materials Coordinator (Consultant) on a World Bank funded rural electrification project in 1997. He is currently doing research work in the communications network security area involving the development of Intrusion Detection and Prevention Systems (IDS/IPS) for Homeland Security and Enterprise Networks.