MedCrave
Step into the World of Research

Physics & Astronomy International Journal

Review Article

Open Access

CrossMark

# Multifractal formalism to recognize changes in the dynamics of Internet routing caused by the Slammer worm and WannaCrypt ransomware attacks

## Abstract

We investigated the dynamical and multiscale features of the Internet routing process in periods of Slammer worm and WannaCrypt ransomware attacks in 2003 and 2017. Border Gateway Protocol (BGP) updates from 8 RIPE RIS collectors were used. To focus on the nonlinear dynamical structure of Internet routing process, we have composed a magnitude time series from original BGP updates data. We used methods of Local variation, Lempel and Ziv complexity measure and Tsallis entropy calculation. Multifractal properties of the BGP updates process were analyzed by multifractal detrended fluctuation analysis (MFDFA).

The purpose of the study was to analyze dynamical patterns of the BGP updates process. The main research task was to assess the efficiency of different dynamical and multiscale testing methods to recognize possible changes in the patterns of Internet routing process caused by attacks of Internet worm Slammer and ransomware WannaCrypt. It is shown that multifractal testing enables to recognize changes in the dynamical patterns of the routing process caused by Slammer worm and ransomware WannaCrypt even when other methods proved ineffective in analyzing relatively short routing time series.

It was found, that during periods of Slammer worm and ransomware WannaCrypt attacks, the dynamics of the multifractal Internet routing process underwent a transient, albeit noticeable, shift toward monofractality. Thus, according to results of present analysis, the most efficient in recognizing multiscale and dynamical patterns of changes in the long-range correlated Internet routing process is a multifractal analysis when it is used for relatively short magnitude time series of BGP updates variation.

Volume 9 Issue 2 - 2025

Teimuraz Matcharashvili,[1,2] Nato Jorjiashvili[2]
[1]Tbilisi State University, Georgia
[2]Ilia State University, Georgia

**Correspondence:** Teimuraz Matcharashvili, Tbilisi State University, Ilia State University, Tbilisi 0179, Georgia

**Received:** December 27, 2024 | **Published:** May 12, 2025

## Introduction

Even a brief survey of existing literature data indicates that an increasing amount of interdisciplinary research works are devoted to studying the different aspects of processes in the Internet network.[1-5] One of the most important subjects of these researches remains the recognition and prevention of anomalous changes of various origins that may occur in the network and harm the normal functioning of the Internet services. In this respect special interests invoke network anomalies caused by different Internet worms and ransomware. Very often related to this question interdisciplinary researches are focused on the investigation of the character of changes in the process of updates of the Internet Border Gateway Protocol (BGP) [see e.g. [1,6,7]]. In general, BGP makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator and plays a critical role in Internet delivery services.[7] Logically, failures in routing protocols will cause serious damage to the normal operation of the Internet. Therefore, the necessity of as possible complete understanding of general features of the BGP updates process is obvious. Advance in this research direction also will help in the better recognition of possible Internet threats and prevention of failures related to routing problems.[7,8] Meanwhile, though the question of investigation of internet routing attracts wide interdisciplinary attention, many aspects of the BGP updates variation remain unclear.[1,7-9] This is caused by numerous factors like the enormous size of the Internet, the complicated character of its network topology, the complexity of interdomain routing, volatility of information flow,

Along with the further efforts to the development of new approaches effective for such tasks, no less important are efforts aimed at the correct selection and competent use of existing methods enabling quantification of complex Internet processes. In the line of such efforts in the present research, we aimed at the selection of the most effective for short BGP time series, analysis methods that may help in the solution of practical tasks related to the recognition of changes that occurred in the routing process. In addition to said, it should be noted that the hard issue of understanding the inherent character of BGP updates variation becomes especially complicated when we aim to analyze Internet routing anomalies caused by unwanted influences of different origins (e.g. related to malware and ransomware attacks, etc.).[12] According to the contemporary view, these anomalies may not always be in time recognized and detected or sometimes may even remain completely unnoticed especially, when we rely only on the traditional standard approaches of data analysis.[10,12] This makes obvious the importance of mentioned above efforts toward better recognition of patterns of changes that may occur in the process of BGP updates as a consequence of different influences. Namely, in this research, we aimed the selection of methods that may be most efficient for the analysis of the dynamical nonlinear structure of BGP updates and recognize changes that could have been caused by Slammer worm and WannaCrypt ransomware attacks.

In general judging by the nature of the destructive influence of Slammer worm and WannaCrypt ransomware on the functioning of the Internet [e.g [8-10]], it was easy to assume that their attacks would cause distortion of original dynamical patterns of the routing process.

So, it was interesting to clarify which methods of complex data analysis may be most appropriate to recognize these changes.

To answer questions about the recognition of dynamical changes in the nonlinear dynamical structure of BGP updates under the influence of Slammer and ransomware we used so called magnitude time series. Namely, instead of the original BGP time series, we analyzed magnitude time series composed from original data sets that retain the nonlinear structure of the targeted BGP updates process. In general, magnitude time series are often used to study the the nonlinear structure and the character of long-term fractal correlations in a time series of different origin [see e.g.[13-15]].

Let's now briefly touch on the question about the Slammer worm and WannaCrypt ransomware. According to the most trustworthy reports, the first-ever attack of the Slammer worm began at 05:30 UTC on Saturday, 25 January 2003.[16,17] Rapidly maximizing network traffic activity, this aggressive computer worm, within 10 minutes has infected 90% of vulnerable hosts and led to a severe distortion in the Internet network, this led to denial of service and as a result in millions of dollars of loss.[16,17] Here needs to be added that some Internet security experts do not exclude that, much weaker cases of Slammer attacks possibly took place also in 2014 and 2016.[3,18,19]

Opposite to SQL Slammer, WannaCrypt (or WannaCry) is a cryptoworm ransomware. It targets computers running the Microsoft Windows operating system and demands ransom payments. The first known and strongest WannaCrypt attack was reported in 2017 and lasted from May 12 to May 15. During this period over 230,000 computers were infected in 150 countries.[20,21] According to available literature data, some experts suppose that the weaker case of WannaCrypt attack took place also in 2018. In the present work, we do not consider these, not so strongly documented cases of Slammer and WannaCrypt attacks and will restrict our analysis by the mentioned above two cases of Slammer (2003) and WannaCrypt (2017) attacks. As far as we aimed at recognition of dynamical changes that occurred in the routing process, we need to mention the known fact of the large increase (surge) in the number of BGP update messages caused by the Slammer worm attack in 2003 [see e.g. [8]]. At the same time, during the WanaCrypt attack such quantitative changes (surges) in the form of drastic typical increases of BGP updates, have not been reported. Thus, by analyzing the nonlinear dynamical structure of the BGP updates process, we aimed to assess the possible dynamical and scaling changes caused by Slammer and WanaCrypt ransomware attacks. No less important was to compare dynamic patterns of the routing process in two distant in time periods in 2003 and 2017 having in mind essential changes in the Internet network system in recent years.

## Used data and methods of analysis

We used BGP time series from the route collectors installed at 8 geographically different and distant locations: rrc03 and rrc00 (Amsterdam), rrc01 (London), rrc04 (Geneva), rrc08 (San Jose USA), rrc06 (Otemachi, Japan), rrc05 (Vienna), rrc07 (Sweden), (available from the International data repository - the European network coordination center https://www.ripe.net).

In relevance to our research purpose, we analyzed the BGP time series recorded in periods of mentioned above two cases of Slammer worm and WannaCrypt ransomware attacks. Namely, BGP time series recorded 4 days prior (21.01.03-24.01.03), 4 days during (25.01.03-28.01.03) and 4 days after (29.01.03-01.02.03) attack of the Slammer worm (25.01. 05.30 in 2003), as well as BGP time series recorded 4 days prior (08.05.17-11.05.17), 4 days during (12.05.17-15.05.17) and 4 days after (16.05.17-19.05.17) attack of the WannaCrypt ransomware (May 12 to 15 in 2017), have been analyzed. Here should be pointed that Slammer worm attack lasted about 20 hours while as mentioned above WannaCrypt ransomware attack lasted 4 days. For the present work, for both considered cases, we choose to analyze routing data sets in 4 days long windows. This was done in order to compare changes that occurred in windows of equal length prior, during and after attacks of Slammer and WannaCrypt. All selected BGP time series have been normalized to standard deviation (SD).

In addition, to better understand the original dynamics of BGP updates, we also analyzed four-day data sets recorded earlier and later than the periods that we named above as periods prior to and after the actual attacks. Namely we analyzed mag BGP time series from 21.01.03 to 24.01.03, and from 02.02.03 to 05.02.03. Also, from 08.05.17 to 11.05.17 and from 20.05.17 to 23.05.17. These periods obviously should be regarded as free of effects caused by Slammer (2003) and WannaCrypt (2017) attacks.

As said, we aimed to find out whether attacks of the mentioned worm and ransomware may affect dynamical patterns of BGP updates and recognize the character of these changes. In general, identifying and extracting important dynamical features from complex, nonstationary and often noisy BGP traffic is regarded as a challenging problem.[6,11,21] For our research purpose, aimed at checking of possible changes in the nonlinear dynamical structure of the BGP updates process, that can be connected to Slammer and WannaCrypt attacks, it was important to ensure that the long-range correlated character of analyzed data sets is preserved. Thus, we decompose original BGP data sets into magnitude and sign time series according to Ashkenazi.[13] Obtained in this way time series are effective to analyze dynamics of unknown processes assessing the character of fluctuations of its absolute values (magnitudes) and signs (directions).[13,15] According to the decomposition procedure: we generate increment time series from original data sets $\Delta x(i) = x(i+1) - x(i)$ which are decomposed in magnitude $|\Delta x(i)|$ and sign series.[13,14]

As long as sign time series are related to linear properties of the process, in this work we used magnitude series. Magnitude time series showing how big are changes in the measurements, according to the definition,[13,15] are related to the inherent nonlinear structure and multifractal properties of analyzed process. Consequently, we regard the use of the magnitude time series as most appropriate to recognize possible changes in the nonlinear dynamical patterns of the BGP updates process. As stated above in the present research we have been targeted the recognition of patterns of changes in the dynamical and scaling properties of the routing process that can be caused by Slammer worm and WannaCrypt ransomware attacks.[22,23]

Thus, we aimed to analyze the nonlinear structure of the BGP update process from dynamical and multiscale points of view. We started to analyze the dynamical properties of the BGP updates process in periods prior during and after Slammer and WannaCrypt attacks using three data analysis methods appropriate for the targeted task.

Namely, the extent of the regularity of BGP updates time series have been analyzed by symbolic techniques of Lempel and Ziv algorithmic complexity calculation (*LZC*)[24-26] which maps a time series into a sequence retaining features of original dynamics. Allowing for the quantification of the degree of order (or randomness) of time series, Lempel and Ziv testing begins from converting the analyzed datasets into a symbol sequence. Usually, the original time series is converted into a 0, 1, sequence by comparing it to a certain threshold value which usually is the median of the original data set.

After, the symbolic sequence is parsed to obtain distinct words, and the words are encoded. Denoting the length of the encoded sequence for those words, the LZ complexity can be defined as:

$$C_{LZ} = \frac{L(n)}{n} \quad (1)$$

where *L(n)* is the length of the encoded sequence and *n* is the total length of the sequence [Lempel&Ziv, 1976]. The lower level of *LZC* indicates an increased extent of regularity in analyzed time series.

Further on, as a regularity metric, we used the local variation (*Lv*) method. *Lv* is useful to characterize the extent of randomness in the spiking data[27] and thus is adequate for the spiky BGP updates time series.[9] *Lv* is defined as:

$$Lv = \frac{3}{n-1}\sum_{i=1}^{n-1}\left(\frac{I_i - I_{i+1}}{I_i + I_{i+1}}\right)^2 \quad (2)$$

where $I_i$ and $I_{i+1}$ are *i*-th and *i*+1th BGP updates accordingly and *n* is the number of BGPs. *Lv* =0 if considered time series is perfectly regular and *Lv* =1 for random sequences consisting of completely independent events.[25,28]

Next, we proceed to the entropy calculation of time series of magnitudes of BGP updates. In general, larger values of entropy are expected when analyzed process is more random (irregular), while it is expected to be small when the amount of uncertainty is small (the process is more regular).[5,29,30] To quantify the extent of randomness in the BGP updates process we have applied often used for data sets of different origin method of Tsallis entropy calculation.[29] The main idea of the method is that the Boltzmann-Gibbs-Shannon condition of extensivity is rarely satisfied for the real world systems. Consequently, long and short range correlations in such systems are far from being regarded as negligible at all scales. Thus, we face a nonextensive case for which Tsallis[29] introduced a special entropic expression:

$$S_q = k\frac{1}{q-1}\left(1 - \sum_{i=1}^{W} p_i^q\right) \quad (3)$$

where $p_i$ are probabilities of existing macroscopic configurations, *W* is the total number of these configurations, *k* is Boltzmann's constant, and *q,* the nonextensivity measure is a real number.[29] Quantifying the dynamic changes of the complexity of the system, the Tsallis entropy *Sq* is lower for the cases that are characterized by lower complexity (are less random).

After that, for the needs of our study, we moved on to analyzing the features of multifractal scaling of BGP update datasets. Previously, studies similar in meaning to our analysis were conducted by some other authors [see, for example, [6,31-33]). Exactly we used multifractal detrended fluctuation analysis (MFDFA).[23,34] MFDFA is a well-known data analysis method often used to unveil the multifractal features of complex processes [see e.g.[34-37]]. It is especially useful to understand scaling features of time series that are characterized by variations over diverse scales. MFDFA, is also often used for analysis of scaling features of magnitude series. Thus, we use it for a magnitude time series of BGP updates. In general, the analysis of scaling properties of complex processes is always important because the temporal evolution of most natural and technical processes exhibits the presence of a multitude of scales and rarely may be monofractal i.e. cannot be described by a single scaling exponent. As pointed out, the MFDFA is effective for such processes that are characterized by a multitude of scales (scaling exponents). It differs from the standard detrended fluctuation analysis (DFA)[23,38] in the calculation of the fluctuation function that depends on the parameter *q*. Exactly, after considering fluctuations on certain segments and removing local trends, *q-th* order fluctuation function can be obtained by averaging fluctuation functions over all segments:[39]

$$F_q(S) = \left\{\frac{1}{2N_s}\sum_{i=1}^{2N_s}\left[F^2(s,v)\right]^{q/2}\right\}^{1/q} \quad (4)$$

Here *N* is a number of non-overlapping segments of length *S*. $F(s,v)$ is the variance calculated for each segment $v$ after removing trends by polynomial fitting.

For negative *q*, the fluctuation function is more sensitive to the portions of the signal in which the fluctuation is small, and for positive *q* it is more sensitive to those portions in which the fluctuation is large. For *q* = 2, the standard DFA procedure is retrieved. It is well known from the basics of MFDFA that, in the case when considered process is power law correlated the following function is obtained:

$$F_q(n) \sim n^{H(q)}, \quad (5)$$

where *H(q)* is the generalized scaling exponent. For monofractal time series, *H(q)* is independent of *q*, while if small and large fluctuations scale differently, then *H(q)* depends on *q* and in that case the data series is multifractal. Next, according to multifractal formalism, *H(q)* can be related to exponents characterizing the partition function and through its Legendre transform we can obtain the singularity spectrum $f(\alpha) = q[\alpha - H(q)] + 1$, where $\alpha = H(q) + qH'(q)$.[29,40] Because of the heterogeneous distribution of variability, the singularity spectra of data sets from multifractal processes are much wider as compared with monofractals. Critical for multifractal analysis scale, *q* and *m* parameters have been selected according to standards in.[25,26]

Further, to avoid misunderstandings in the interpretation of obtained results we additionally accomplished MFDFA analysis on Fourier phase randomized magnitude time series.[23] Using this type of surrogate data set was important for our analysis. Indeed, the Fourier phase randomization procedure eliminates nonlinearities in the original time series preserving only linear features of the analyzed process. Such analysis will help us to answer the question of whether possible changes in the dynamical patterns of BGP updates evolution may indeed be related to the influence of Slammer worm and ransomware on the inherent nonlinear structure of routing processes. This question needs to be answered because seemingly similar changes may be caused by different linear factors which may not directly be related to Slammer worm and ransomware influences.

## Results of analysis and discussion

As it was said in the previous section, we analyzed magnitude time series (Figure 1 and 2) reconstructed from the averaged BGP measurement data sets, that were obtained by averaging measurement recordings from all selected observation sites.

Averaging over 8 collectors, chosen for this study, was quite logical, given the general similarity of changes viewed in BGP updates time series recorded at each of the collectors [for details see 19]. Analysis of these averaged datasets allowed us to focus on the most important features of the BGP updates process for the periods of observation. Most important is that averaged data sets provide an opportunity to speak about the general character of changes that could be caused by attacks of the Slammer worm and WannaCrypt ransomware in the dynamics of Internet interdomain routing.

Magnitude time series composed from averaged BGP data have been prepared for above mentioned periods prior during and after both analyzed attacks. In Figure 1 and 2, we show a magnitude time

series, of averaged BGP updates data, over 12 days involving periods prior to, during and, after attacks of the Slammer worm in 2003 and WannaCrypt ransomware in 2017. It deserves to be pointed out that in the corresponding magnitude time series (see Figure 1), it is still possible to distinguish the typical surge of BGP updates as it was often reported for original data sets during the Slammer worm attack (on 01/25/2003).[4,7,11]

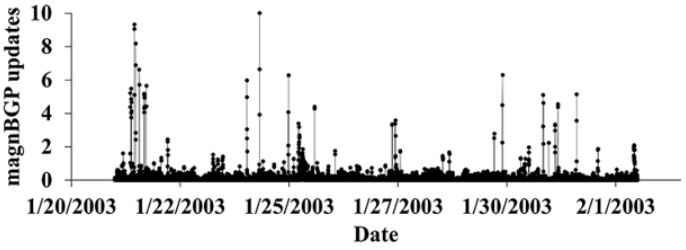



**Figure 1** Magnitude time series of averaged BGP updates in a period of Slammer worm attack, 2003.

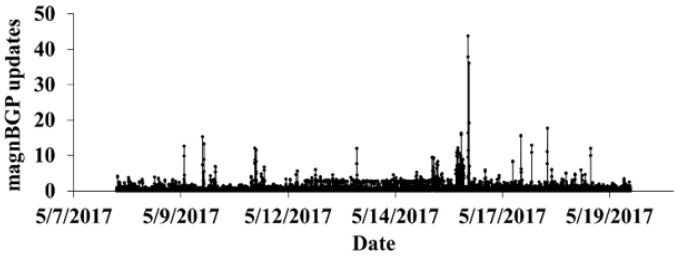



**Figure 2** Magnitude time series of averaged BGP updates in a period of the WannaCrypt attack, 2017.

It is known that such surges are caused by a rapid doubling of the number of machines infected with Slammer, approximately every 9 seconds.[7,11] In the case of the WannaCrypt ransomware attack (May 12 to 15 in 2017), we do not observe such surges neither in the original nor in magnitude time series (see Figure 2), which was quite expected according to mentioned above. Thus, the Slammer worm and the WannaCrypt ransomware show a clear difference in the sense of caused by their attacks' quantitative changes in the BGP updates process.

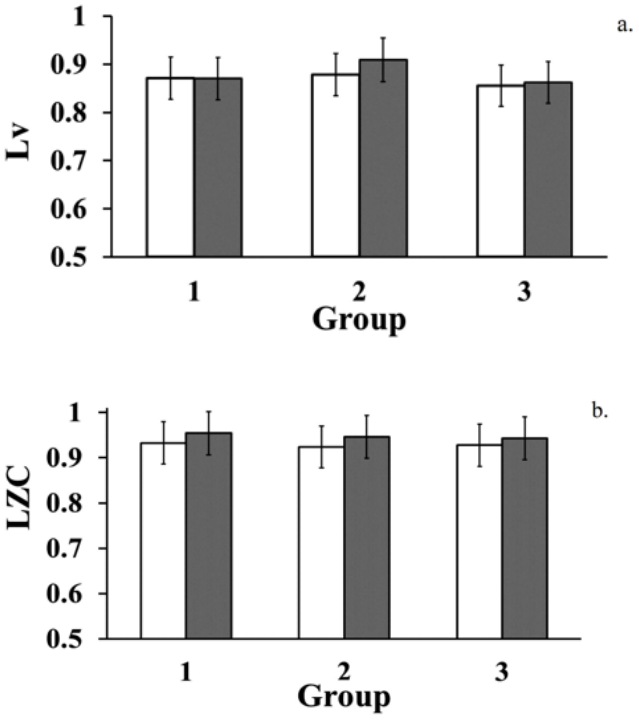
In light of such difference, it was interesting to analyze the character of possible qualitative changes in the dynamical and scaling properties of the BGP updates process in periods of the Slammer worm and WannaCrypt ransomware attacks. No less interesting was the comparison of the initial dynamics of BGP updates over two periods significantly distant in time — in 2003 and 2017.

Thus, as is pointed out above we pursued three main tasks of this research. Namely, the first two have been the analysis of possible quantitative and qualitative changes in the dynamical and scaling features of the routing process during attacks of Slammer worm (in 2003) and WannaCrypt ransomware (in 2017). The third task was the comparison of the character of dynamical and scaling features of the original BGP updates process in two distant in time periods without attacks of Slammer or WannaCrypt (i.e. in 2003 and 2017).

It needs to be understood that though we analyze relatively small data sets of BGP updates in periods prior during and after attacks we, in fact, deal with global processes related to the entire Internet. The term global changes are quite relevant here because we base our analysis on BGP time series from the listed above 8 collectors - a very important part of the global network. Consequently, it is quite reasonable that the behavior of the BGP updates process in the analyzed part of the Internet will mainly reflect the character of routing processes in the global network. This is true for the periods without external influences (prior to and after analyzed attacks) as well as for periods of actual attacks.

To answer the posed research questions, we began with the assessment of the general character of dynamics of the BGP updates process by standard tools of complex data analysis. First, we accomplished DFA calculation of original BGP updates time series for periods immediately prior, during and immediately after the Slammer worm and WannaCrypt attacks. According to this analysis DFA scaling features of considered averaged time series show non-random persistent character of BGP updates variation, with scaling exponent $\alpha$ in the range 0.6-0.95 prior and after attacks. The only exception is the 4-day period of Slammer attack 25.01.03-28.01.03 with $\alpha$=1.3, pointing to the appearance of non-power-law type behavior in the BGP updates fluctuation. Regardless of the reasons, this fact could have influenced the results of further dynamical structure testing and multiscale analysis, as well as complicate their interpretation.[25,28] Therefore, the conversion of the original BGP updates data sets into magnitude time series was regarded as correct solution. This ensured our analysis to be focused on the character of possible changes in the scaling and nonlinear dynamical structure of original routing process, that could have been caused by Slammer and WannaCrypt attacks. DFA scaling exponent, $\alpha$, for magnitude series prior to, during, or after worm and ransomware attacks always was in the range 0.6-0.8 which is important in the light of the further multiscaling analysis of routing data.[25]

As said above, proceeding to the analysis of whether dynamical patterns of the BGP updates process have changed under Slammer worm and WannaCrypt ransomware attacks, we used *Lv*, *LZC* and, Tsallis entropy calculation. The results of these analyses are presented in Figure 3.




**Citation:** Matcharashvili T, Jorjiashvili N. Multifractal formalism to recognize changes in the dynamics of Internet routing caused by the Slammer worm and WannaCrypt ransomware attacks . *Phys Astron Int J.* 2025;9(2):88–96. DOI: 10.15406/paij.2025.09.00369

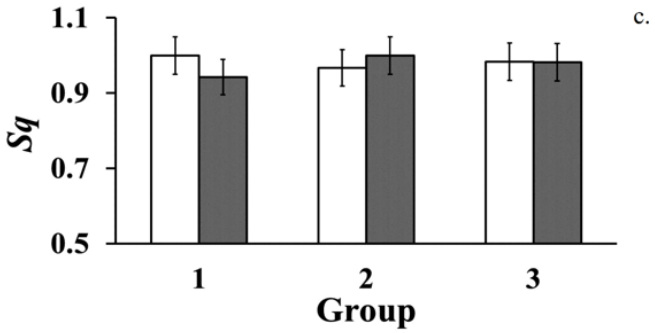



**Figure 3** Calculated for magn time series of averaged BGP updates data, a) *Lv* measures, b) *LZ* complexity values, and c) Tsallis entropy. Calculations have been performed for 4-day windows prior (group 1), during (group 2) and, after (group 3) Slammer worm (white) and WannaCrypt (grey) attacks

Exactly, in Figure 3a and b results of local variation and Lempel, Ziv analysis of magn BGP updates time series are presented for three analyzed groups (i.e. periods immediately prior, during, and immediately after attacks). In Figure 3c we show the results of Tsallis entropy, *Sq,* calculation at entropic index $q$ =5.

From results and corresponding error bars presented in Figures 3-5, it follows that by measured *Lv, LZC* and Tsallis entropy characteristics of magnitude time series of BGP updates, there is practically no statistically significant difference between 4-day periods prior, during, and after Internet worm and ransomware attacks. Also, calculated measures are not statistically different for periods during attacks in 2003 or 2017 (compare groups 2 in Figure 3a-c). All this is an indication that Slammer worm or WannaCrypt ransomware attacks do not lead to quantifiable changes in the symbolic complexity, variability features, or entropic characteristics of dynamics of Internet routing, at least in the case of considered 4-day periods. In other words, according to analyzed dynamical characteristics, the processes of BGP updates variation during periods of actual attacks are not distinguishable from periods preceding or following these attacks. The results of these analyses (presented in Figures 3a-c) are particularly interesting in the sense that they are obtained by methods based on different basic principles, and thus we can convincingly state that the conclusions made here will not be biased by the possible drawbacks of certain used methods.

Then we proceed to the analysis of multiscaling features of a time series of magnitudes of BGP updates using MFDFA. Figures 4-7, reveal obvious multifractal character of analyzed routing process. We see that, fluctuations in magnitudes of routing data sets differ on different scales. On small scales at negative $q$ values, fluctuations are stronger than at positive $q$ values (see triangles in Figure 4 and 6). Furthermore, we see that the width of the singularity spectrum i.e. the range of $H(q)$ or $H_{max}(q)$-$H_{min}(q)$, which often is regarded as a quantitative measure of multifractality, is different for magnitude time series of BGP updates for different considered (4 day long) periods. The smallest this range, reflecting obvious changes in the fractal structure of the routing process, turned out to be for periods of actual attacks (triangles in Figure 5 and 7), compared with periods immediately before and immediately after attacks. This decreases in width of the singularity spectrums, in periods of the actual attacks points to the shift of dynamical patterns of the routing process to less multifractality compared to periods prior to or after attacks. Thus, we learn that attacks of Slammer worm and WannaCrypt ransomware, led to noticeable distortion of scaling multifractal character of intact process of BGP updates in 2003 as well as in 2017. This distortion in scaling features, compared to periods with no attacks, is revealed in the form of a shift toward less multifractality of the BGP updates process (compare Figure 4 and 6 with 8).

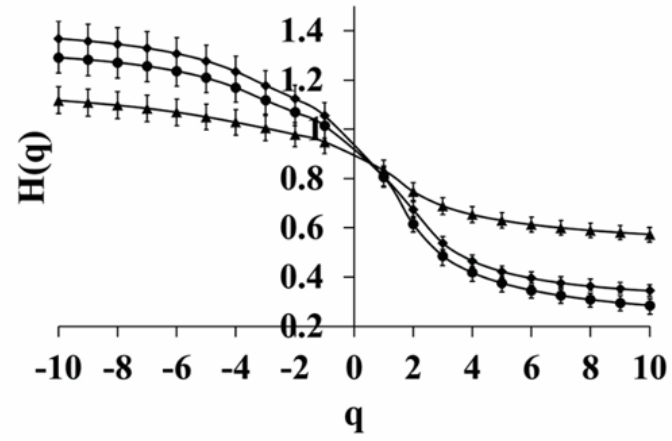



**Figure 4** Generalized Hurst exponent $H(q)$ as a function of $q$ of the magn time series of averaged BGP updates, calculated for 4-day windows prior (circles), during (triangles) and after (diamonds) Slammer worm attack.

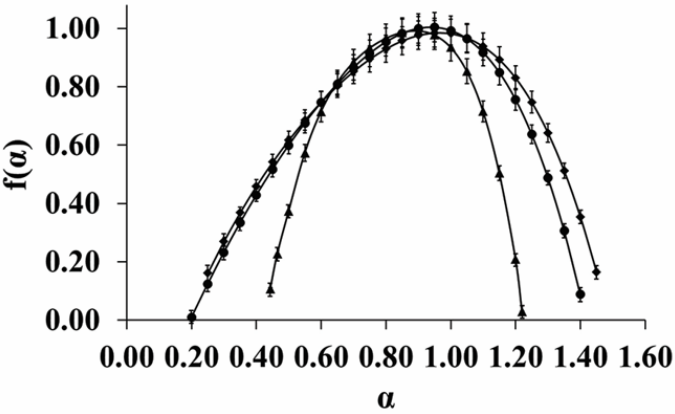



**Figure 5** Singularity spectrums of BGP updates data sequence of averaged BGP updates data calculated for 4-day windows prior (circles), during (triangles) and after (diamonds) Slammer worm attack.

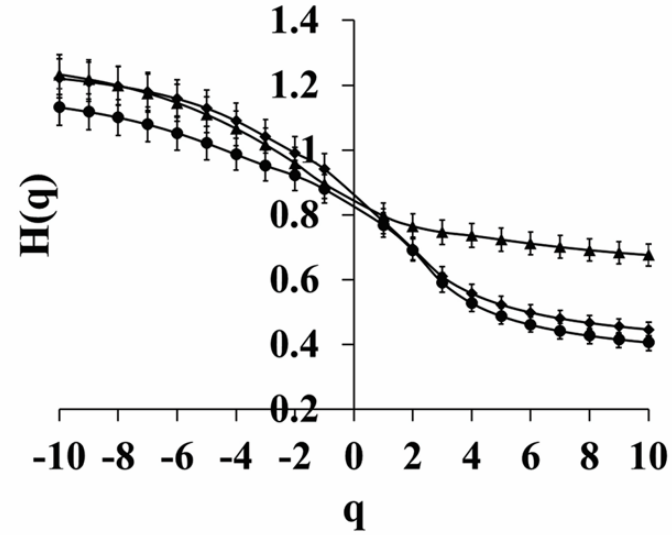



**Figure 6** Generalized Hurst exponent H(q) as a function of q of the magn time series of averaged BGP updates, calculated for 4-day windows prior (circles), during (triangles) and after (diamonds WannaCrypt ransomware attack.

**Citation:** Matcharashvili T, Jorjiashvili N. Multifractal formalism to recognize changes in the dynamics of Internet routing caused by the Slammer worm and WannaCrypt ransomware attacks . *Phys Astron Int J.* 2025;9(2):88–96. DOI: 10.15406/paij.2025.09.00369

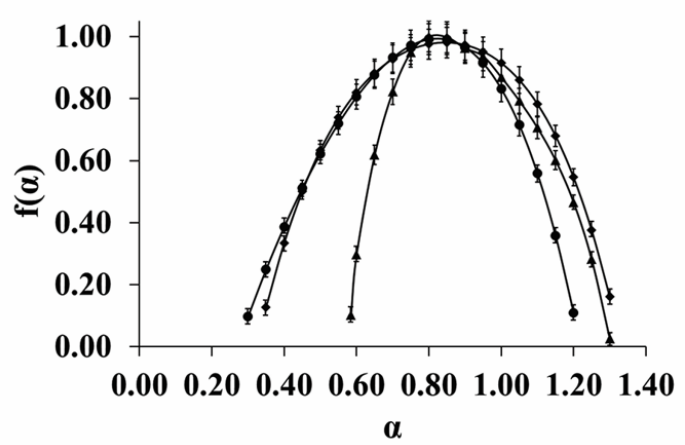



**Figure 7** The singularity spectrums of BGP updates data sequence of averaged BGP updates data calculated for 4-day windows prior (circles), during (triangles) and after (diamonds) WannaCrypt ransomware attack.

At the same time, it deserves to be pointed out that changes that occurred in the scaling patterns of the BGP updates process by Slammer worm in 2003 and WannaCrypt in 2017, do not differ qualitatively. Indeed, according to Fig. 8, we can speak just about slight quantitative differences observed at larger fluctuations i.e. at positive $q$ values. This points to the quite resembling effects of the influence of two very different threat factors on the scaling features of the process of BGP updates. In this regard, it was interesting to know whether scaling patterns of the original process of BGP updates have been changed for the long-time span between Slammer and WannaCrypt attacks.

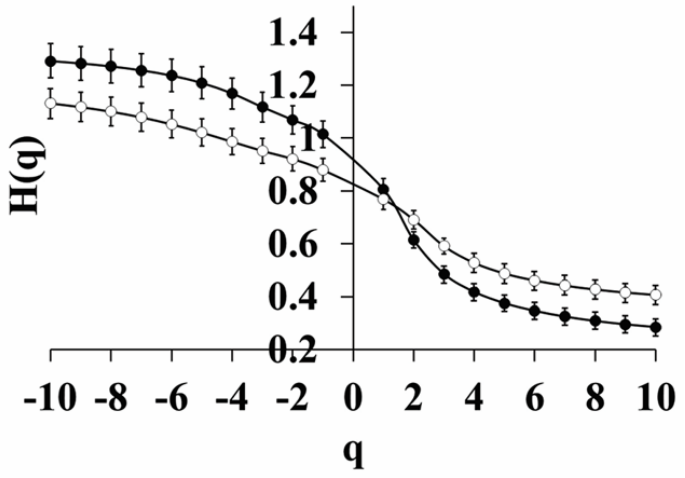



**Figure 8** Generalized Hurst exponents $H(q)$ of original magn time series of averaged BGP updates data calculated for 4-day windows during Slammer worm (2003) and WannaCrypt ransomware (2017) attacks (black and white circles).

To save space and not to overburden text we further show results of generalized Hurst exponents calculation. In Figure 9 and 10, there are presented generalized Hurst exponents of time series of magnitudes of BGP updates in periods immediately prior to and immediately after these attacks in 2003 and 2017. It follows from these figures that there are no strong qualitative differences between scaling patterns of BGP updates for analyzed 4-day periods, prior (Figure 9) or after (Figure 10) attacks in 2003 and 2017. What we observe is slight quantitative shift of scaling features in the magnitude time series of BGP updates to the less multifractality in 2017 compared to 2003. Singularity spectrum analysis of these data sets leads to the same conclusion and as said above are not shown here. Given how similar the curves look in Figs. 9 and 10, it can be assumed that observed quantitative differences in the scaling patterns of the BGP update process are due to changes in the network characteristics. Such changes in the Internet network look quite expected given the fast growth of the Internet network and that 14 years have passed between the attacks in question. Thus, some quantitative differences observed between the BGP updates process in 2003 and 2017 (see figures Figure 9 and 10) should not be directly connected with Slammer and WannaCrypt influences and are obviously connected with changes in the network features (e.g. architecture, topology, etc.). This is further confirmed by results presented in Figure 11 and 12. In these figures generalized Hurst exponents calculations for 4-day periods of BGP updates variability are presented starting from the 8th day prior to attacks and ending to 8th day after attacks in 2003 and 2017 (i.e. earlier and later than for periods named as "immediately prior" and "immediately after").

Here again, we see slight quantitative changes in scaling features of BGP updates under WannaCrypt attack as it is shown in Figure 9 and 10.

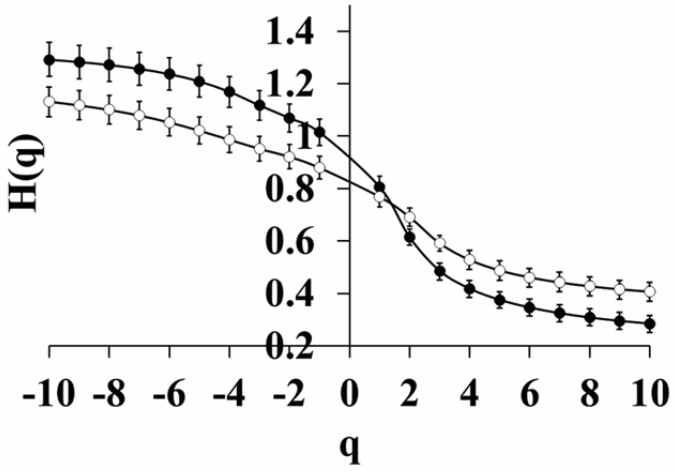



**Figure 9** Generalized Hurst exponents $H(q)$ of original magn time series of averaged BGP updates data calculated for 4-day windows prior to Slammer worm and WannaCrypt ransomware attacks (black and white circles).

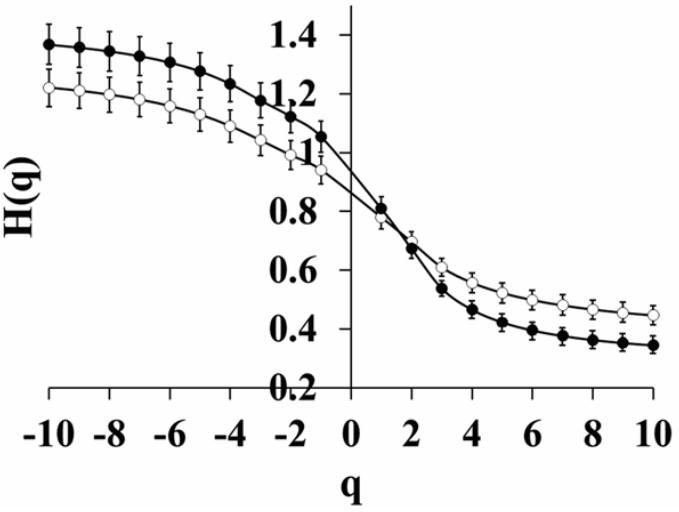



**Figure 10** Generalized Hurst exponents $H(q)$ of original magn time series of averaged BGP updates data calculated for 4-day windows after Slammer worm and WannaCrypt ransomware attacks (black and white circles).

**Citation:** Matcharashvili T, Jorjiashvili N. Multifractal formalism to recognize changes in the dynamics of Internet routing caused by the Slammer worm and WannaCrypt ransomware attacks . *Phys Astron Int J.* 2025;9(2):88–96. DOI: 10.15406/paij.2025.09.00369

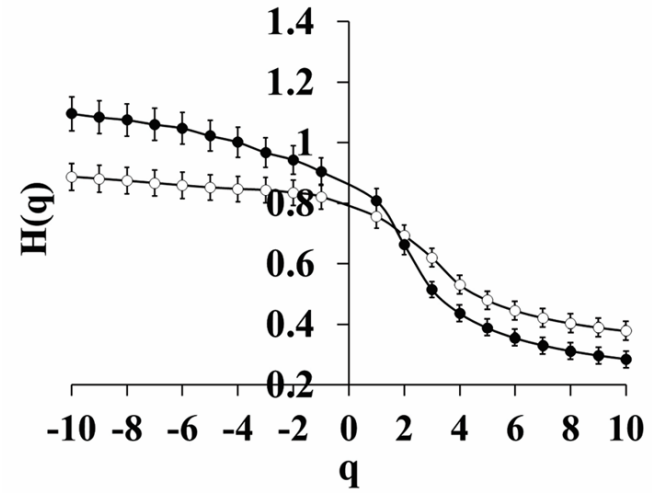



**Figure 11** Generalized Hurst exponents *H(q)* of original magn time series of averaged BGP updates data calculated for 4-day windows located 8 days after to Slammer worm and WannaCrypt ransomware attacks (black and white circles).

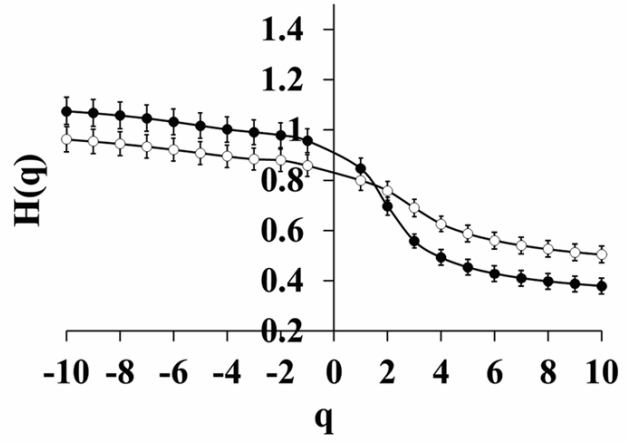



**Figure 12** Generalized Hurst exponents *H(q)* of original magn time series of averaged BGP updates data calculated for 4-day windows located 8 days prior to Slammer worm and WannaCrypt ransomware attacks (black and white circles).

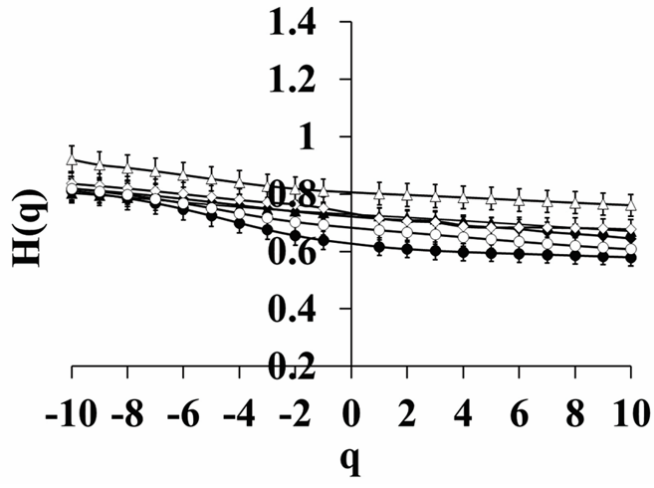



**Figure 13** Generalized Hurst exponent *H(q)* s a function of the phase randomized magn time series of averaged BGP updates data, calculated for 4-day windows prior (circles), during (triangles) and, after (diamonds) Slammer worm (black) and WannaCrypt ransomware (white) attacks.

It is important that these changes occurred in the original character of BGP updates from 2003 to 2017, have not strongly reflected in the noticed shifts to the less multifractality caused by attacks of Slammer and WannaCrypt.

In light of the results presented in Figure 8, the observed quantitative changes in the scaling features of BGP updates in the period between attacks are of particular importance. This points out that different attacking factors (here Slammer and WannaCrypt) may lead to very similar changes in the scaling features of BGP updates. Thus, proper testing of the scaling patterns of the routing process will allow us to recognize important changes that cannot be detected otherwise. On the other hand, we may not be able to achieve correct threat identification – and may not be able to determine which factor caused the observed changes in the scaling patterns of BGP updates. At the same time, this does not diminish the importance of the fact that testing of scaling features of BGP updates, enables us to recognize patterns of dynamic changes caused by attacks of Slammer and WannaCrypt. This is of immense importance since, as has been pointed, such changes can often remain completely unnoticed by other methods.

All said makes us believe that observed changes in the scaling patterns of analyzed magnitude time series that occurred during attacks are really caused by the distortion of the inherent original nonlinear structure of the BGP updates process under attacks of Slammer worm and WannaCrypt ransomware.

To further testing of this assumption we additionally accomplished an analysis of multifractal properties of phase randomized magnitude series of BGP updates. In other words, we tested a magnitude series of BGP updates in which the nonlinear dynamical structure was intentionally distorted while a linear one was retained. Presented in Figure 13 results convince that observed above (in Figure 4-11) changes are related to the influence of Slammer and WannaCrypt on the inherent dynamical structure of the analyzed process. Indeed, as we see in Figure 13, distortion of this structure completely changes the observed multifractal character of BGP updates. What is still retained is obviously caused by unknown linear factors which do not present our interest now. Especially should be pointed out that as follows from Figure 13 (open figures), the distortion of these inherent dynamical features, by Fourier phase randomization, leads to the practical disappearance of differences in periods prior during, or after actual influences.

Presented results of our research indicate that while methods of complex data analysis like Lv, LZC, and Tsallis entropy calculation does not reveal changes in the short BGP updates time series, MFDFA performs well in the sense of scaling pattern recognition occurred in the nonlinear dynamical structure of the routing process. This is clear when comparing periods of actual attacks and periods prior to and after attacks of Slammer as well as WannaCrypt (see Figure 4-7). The multifractal characteristics, as shapes and positions of Generalized Hurst exponent and singularity spectrums of BGP updates time series, enabled to discriminate occurred changes. Indeed, the shift to the less multifractality of the routing process, revealed in the decreased width of the singularity spectrum as well as by the character of *H(q)* vs *q* relation, indicate noticeable changes in scaling and long range correlation features occurred as a consequence of attacks of the Slammer worm and WannaCrypt ransomware.

All said above convince that the multifractal testing of dynamical patterns of BGP updates has a valuable sensitivity in the recognition of changes that, for the relatively short data sets, apparently remained un-recognized by other used analysis methods. It need to be pointed that in general this is in good agreement with reported earlier by Willinger

et al.[36] efficiency of multifractal logic for short Internet traffic on small time scales. In this regard, it can be said that a comprehensive interdisciplinary study of the multifractal features of the BGP updates process still remains extremely important for a further understanding of the nature of the Internet routing. It becomes also clear that the multifractal scaling analysis of the routing process has an advantage over other methods of dynamical testing and thus certainly will be helpful in better understanding processes in the Internet, especially when we use relatively short time series.

Finally, it can be said that multi-scale analysis of the routing process in addition to the above-mentioned advantages in the better detection and identification of already occurred unwanted influences, can also help in recognizing dynamical patterns of occurring in the network weak changes that may signal upcoming threats able to harm Internet services.

## Conclusion

In the present research we aimed to investigate the character of changes that occurred in the process of Internet routing caused by attacks of Internet worm Slammer and ransomware WannaCrypt. The exact task of the research was to assess the efficiency of different data analysis methods in the recognition of dynamical and multiscale features of the Internet routing caused by Slammer worm and WannaCrypt ransomware attacks. We have used methods of Local variation, Lempel and Ziv complexity measure, and Tsallis entropy calculation. Multifractal properties of the BGP updates process have been analyzed by (MFDFA).

We showed that multifractal analysis performs better in the pattern recognition and enables us to detect caused by Slammer worm and ransomware WannaCrypt changes in the character of the Internet routing process, even in the case when other methods appear ineffective. It was found that attacks of Slammer worm and WannaCrypt ransomware caused noticeable changes in the multifractal patterns of the BGP updates process. Thus, according to results of present analysis the most efficient in the recognition of multiscale and dynamical patterns of changes in the long-range correlated process of Internet routing for used 4 day relatively short magnitude time series of BGP updates variation appeared a multifractal analysis.

## Acknowledgments

The authors express sincere gratitude to Dr. A. Elmokashfi from Simula Norway, for useful comments and discussion.

## References

1. Rekhter Y, Li T, Hares S. A border gateway protocol 4 (BGP–4). RFC 4271. RFC Editor; 2006.
2. Elmokashfi A, Dhamdhere A. Revisiting BGP churn growth. *ACM SIGCOMM Comput Commun Rev.* 2014;44(1):5–12.
3. Work J. Rapid capabilities generation and prompt effects in offensive cyber operations. SocArXiv. Center for Open Science. 2022.
4. Bhuyan MH, Bhattacharyya DK, Kalita JK. An empirical evaluation of information metrics for low–rate and high–rate DDoS attack detection. *Pattern Recognit Lett.* 2015;51:1–7.
5. Kumar G, Narducci F, Bakshi S. Knowledge transfer and crowdsourcing in cyber–physical–social systems. *Pattern Recognit Lett.* 2022;164:210–215.
6. Matcharashvili T, Elmokashfi A, Prangishvili A. Analysis of the regularity of the Internet Interdomain Routing dynamics. *Physica A.* 2020;124142.
7. Lad M, Massey D, Zhang L. Visualizing internet routing changes. *IEEE Trans Vis Comput Graph.* 2006;12(6):1450–1460.
8. Lad M, Zhao X, Zhang B, et al. Analysis of BGP update surge during Slammer worm attack. In: Lecture Notes in Computer Science. Vol 2918. Springer; 2004:66–79.
9. Al–Musawi B, Branch P, Armitage G. BGP anomaly detection techniques: a survey. *IEEE Commun Surv Tutor.* 2017;19(1):377–396.
10. Al–Musawi B, Branch P, Armitage G. Detecting BGP instability using recurrence quantification analysis (RQA). In: IEEE 34th International Performance Computing and Communications Conference (IPCCC). Nanjing, China; 2015:1–8.
11. Matcharashvili T, Prangishvili A. Quantifying regularity of the Internet Interdomain Routing based on Border Gateway Protocol (BGP) databases. In: ICECCE. 2020:1–5.
12. Karimi M, Jahanshahi A, Mazloumi A, et al. Border gateway protocol anomaly detection using neural network. *In: IEEE International Conference on Big Data (Big Data).* 2019:6092–6094.
13. Ashkenazy Y, Ivanov PC, Havlin S, et al. Magnitude and sign correlations in heartbeat fluctuations. *Phys Rev Lett.* 2001;86(9):1900–1903.
14. Kantelhardt JW. Fractal and multifractal time series. In: Meyers R, ed. Mathematics of Complexity and Dynamical Systems. Springer; 2012.
15. Gómez–Extremera M, Carpena P, Ivanov PCh, et al. Magnitude and sign of long–range correlated time series: decomposition and surrogate signal generation. *Phys Rev E.* 2016;93:042201.
16. Moore D, Paxson V, Savage S. Inside the Slammer worm. *IEEE Secur Priv.* 2003;1(4):33–39.
17. Kristoff J. Remembering SQL Slammer. 2023.
18. Chindipha S, Irwin B. An analysis on the re–emergence of SQL Slammer worm using network telescope data. In: Southern Africa Telecommunication Networks and Applications Conference (SATNAC). 2017:218–223.
19. Pauli D. Slammer worm slithers back online to attack ancient SQL servers. The Register. 2017.
20. Asgari S, Sadeghiyan B. Towards generating benchmark datasets for worm infection studies. In: 10th International Symposium on Telecommunications (IST). 2020.
21. Li Z, Rios A, Trajković LG. Detecting Internet worms, ransomware, and blackouts using recurrent neural networks. In: IEEE International Conference on Systems, Man, and Cybernetics (SMC). 2020:2165–2172.
22. Kalisky T, Ashkenazy Y, Havlin S. Volatility of fractal and multifractal time series. *Isr J Earth Sci.* 2007;56(1):47–56.
23. Ihlen E. Introduction to multifractal detrended fluctuation analysis in Matlab. *Front Physiol.* 2012;3:1–18.
24. Lempel A, Ziv J. On the complexity of finite sequences. *IEEE Trans Inf Theory.* 1976;22(1):75–81.
25. Aboy M, Hornero R, Abásolo D, et al. Interpretation of the Lempel–Ziv complexity measure in the context of biomedical signal analysis. *IEEE Trans Biomed Eng.* 2006;53(11):2282–2288.
26. Hu J, Gao J, Principe JC. Analysis of biomedical signals by the Lempel–Ziv complexity: the effect of finite data size. *IEEE Trans Biomed Eng.* 2006;53(12).
27. Shinimoto S, Kim HH, Shimokawa T, et al. Relating neuronal firing patterns to functional differentiation of cerebral cortex. *PLoS Comput Biol.* 2009;5(7).
28. Ozar B. The 20th anniversary of the SQL Slammer worm. 2023.
29. Tsallis C. Possible generalization of Boltzmann–Gibbs statistics. *J Stat Phys.* 1988;52:479–487.

30. Gu Y, McCallum A, Towsley D. Detecting anomalies in network traffic using maximum entropy estimation. In: Proceedings of the 5th ACM SIGCOMM Conference on Internet Measurement. USENIX Association; 2005:32–32.

31. Feldmann A, Gilbert AC, Huang P, et al. Dynamics of IP traffic: a study of the role of variability and the impact of control. *Comput Commun Rev.* 1999;29:301–313.

32. Willinger W, Govindan R, Jamin S, et al. Scaling phenomena in the Internet: critically examining criticality. 2002;99(1):2573–2580.

33. Fiedler M. Traffic Measurement, Characterization, and Modeling. Springer; 2006.

34. Kantelhardt JW, Ashkenazy Y, Ivanov PC, et al. Characterization of sleep stages by correlations in the magnitude and sign of heartbeat increments. *Phys Rev E.* 2002;65:051908.

35. Kantelhardt SA, Zschiegner E, Koscielny–Bunde S, et al. Multifractal detrended fluctuation analysis of nonstationary time series. *Physica A.* 2002;316(1–4):87–114.

36. Meng K, Yang S, Cattani P, et al. Multifractal characterization and recognition of animal behavior based on deep wavelet transform. *Pattern Recognit Lett.* 2024;180:90–98.

37. Saâdaoui F. Structural self–similarity pattern in global food prices: utilizing a segmented multifractal detrended fluctuation analysis. *Pattern Recognit Lett.* 2024;184:74–79.

38. Eichner JF, Koscielny–Bunde E, Bunde A, et al. Power–law persistence and trends in the atmosphere: A detailed study of long temperature records. *Phys Rev E.* 2003;68:046133.

39. Matcharashvili T, Elmokashfi A, Zhukova N. An analysis of BGP updates dynamics during Slammer worm attack. Preprint. 2006.

40. Shinomoto S. Memory maintenance in neural networks. *J Phys A Math Gen.* 1987;20:L1305.

**Citation:** Matcharashvili T, Jorjiashvili N. Multifractal formalism to recognize changes in the dynamics of Internet routing caused by the Slammer worm and WannaCrypt ransomware attacks . *Phys Astron Int J.* 2025;9(2):88–96. DOI: 10.15406/paij.2025.09.00369