საქართველოს მეცნიერებათა ეროვნული აკადემიის მოამბე, ტ. 18, №2, 2024
BULLETIN OF THE GEORGIAN NATIONAL ACADEMY OF SCIENCES, vol. 18, no. 2, 2024

Informatics

Comparison of Changes Caused by the Internet Worm and Ransomware in Fractal Properties of Border Gateway Protocol (BGP) Updates Time Series

Archil Prangishvili[*], Teimuraz Matcharashvili[**], Aleksandre Sborshchikovi[**], Ekaterine Mepharidze[**], Dimitri Tepnadze[**], Levan Laliashvili[**], Elene Chikviladze[§,], Tea Khutsishvili[§], Zurab Chelidze[**]**

[*] *Academic Member, Georgian Technical University, Tbilisi, Georgia*
[**] *M. Nodia Institute of Geophysics, Ivane Javakhishvili Tbilisi State University, Tbilisi, Georgia*
[§] *Faculty of Informatics and Control Systems, Control Systems Department, Georgian Technical University, Tbilisi, Georgia*

Analysis of variation of Border Gateway Protocol (BGP) updates remains the focus of important interdisciplinary research. Most important is an investigation of the dynamical features of BGP updates variation in general, especially under the influence of different internal or external factors that can affect the Internet. In this paper, we use time series of BGP update messages, collected at international collectors. Fractal properties of intact BGP updates process in periods of attacks of self-propelling worm Slammer as well as WannaCrypt crypto worm are investigated. We used the method of multifractal detrended fluctuation analysis (MDFA). It was found that the BGP updates process always reveals multifractal properties. Under the Slammer worm attack and WannaCrypt ransomware, noticeable changes in the BGP updates process occurred. At the same time, for the two considered cases, changes are different as far as multifractal properties have mostly been destroyed by the influence of Slammer worm compared to WannaCrypt. The detected differences may help in better recognition of the character of Ransomware attacks. *© 2024 Bull. Georg. Natl. Acad. Sci.*

Internet, Border Gateway Protocol, slammer self-replicating worm, MDFA, dynamics

It is well accepted that further understanding of processes in the core of the Internet is tied with better knowledge of the routing process. From this point of view, the analysis of Border Gateway Protocol (BGP) data sets [1-3] becomes popular among researchers from different fields of science. In general, the BGP is an incremental path-vector routing protocol managing network reachability information ensuring optimal route data between Internet autonomous systems (ASes). Thus, BGP is a kind of a scheme whose primary function is to exchange network reachability information [1]. As far as the Internet represents a dynamical system with a complicated topology of the network and complex character of information flow in it, the analysis of the BGP update process necessitates the

competent using of modern data analysis tools [2,3].

The most important aspect of the present research interests is focused on changes caused by the influence of different unwanted factors. Indeed it is known that BGP is prone to anomalies that impede the successful exchange of reachability [4]. Such anomalies may be caused e.g. by worms (e.g. Slammer), ransomware attacks (WannaCrypt), routing misconfigurations [2], Internet Protocol (IP) prefix hijacks, etc.

In this research, we aimed to analyze and compare the character of changes in the fractal features of BGP updates were caused by attacks of Slammer worm and ransomware Wannacript during corresponding attacks in 2003 and 2017.

Used Data and Methods of Analysis

In the frame of the present work, we used BGP updates time series from the site of the European network coordination center (https://www.ripe.net). In relevance to our research purpose, we selected the BGP time series, recorded in periods of two cases of Slammer worm and WannaCrypt ransomware, attacks. We started from the case of a self-propagating Slammer computer worm attack in 2003. Namely, BGP time series were recorded in the period 13.01.2003 to 06.02.2003. For WannaCrypt ransomware, we selected the period from 01.05.2017 to 27.05.2017 (Fig. 1). Separately we analyzed the BGP time series recorded prior to and during attacks of Slammer worm and WannaCrypt. Exactly, prior to the Slammer attack period from 21.03.2003 to 24.03.2003 was selected. Correspondingly, during the Slammer worm attacks BGP recordings in the period from 25.01.2003 to 28.01.2003 were considered. Next, we analyzed the BGP time series recorded in the period prior to the WannaCrypt ransomware attack, from 10.05.2017 to 12.05.2017, as well as the period during actual ransomware attack, from 12.05.2017 to 15.05.2017.

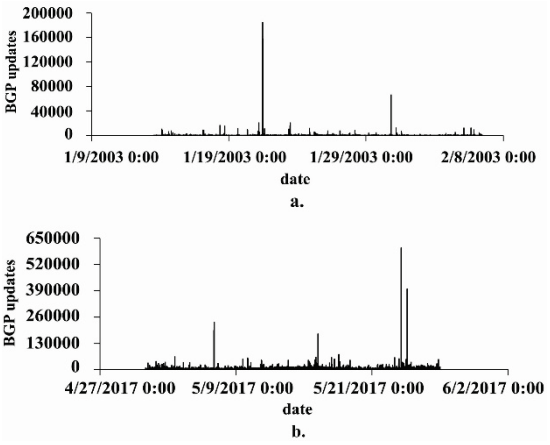

Fig. 1. BGP updates time series recorded in the period of a) Slammer worm attack and b) WannaCrypt ransomware attack.

After selecting appropriate for our research needs data sets, we proceeded to the analysis of the extent of multifractal long-range features using the method of multifractal detrended fluctuation analysis (MF-DFA). The selection of MF-DFA as a main method of targeted research was quite logical as far as the time evolution of most of the natural and technical processes, including BGP updates variability, rarely reveal exactly mono-fractal features. In such cases, MF-DFA is useful for the quantitative analysis of processes with a multitude of scaling exponents [5]. Additionally, different from the standard detrended fluctuation analysis (DFA) [6-8], MF-DFA enables to calculate of the fluctuation function, in relation to the parameter q

$$F_q(n) = \left[\frac{1}{N} \sum_{i=1}^{N} \left[Y(i) - Y_n(i) \right]^q \right]^{1/q}.$$

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. Similarly to the DFA, the following function is obtained: $F_q(n) \sim n^{H(q)}$, where H(q) is the generalized scaling exponent. For the mono-fractal time series, H(q) is independent of q, while when small and large fluctuations scale differently,

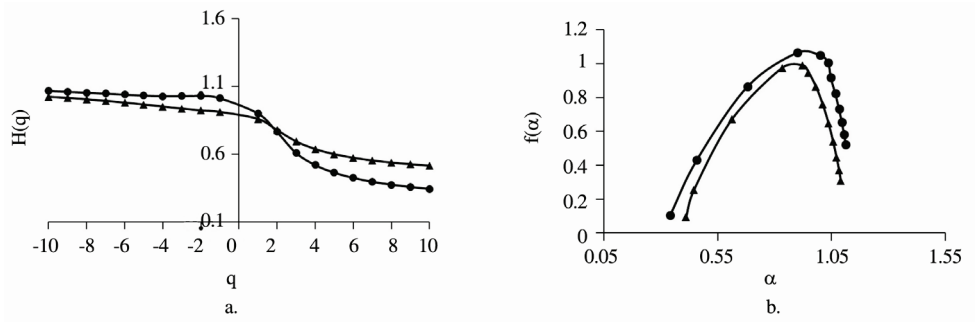

Fig. 2. a) Generalized Hurst exponent *H(q)* as a function of *q* and b) singularity spectra of BGP updates data sequence for periods of Slammer attack (13.01.2003 to 06.02.2003) (circles), and WannaCrypt ransomware attack (13.01.2017 to 06.02.2017) (triangles).

then it depends on q. This is a typical characteristic of multifractal data series. Next, according to multifractal formalism, H(q) can be related to exponents, characterizing partition function and through its Legendre transform the singularity spectrum can be calculated, where $\alpha = H(q) + qH'(q)$ [5]. As mentioned above, because of the heterogeneous distribution of variability, the singularity spectra of most data sets from multifractal processes are much wider compared to monofractals.

Results and Discussion

Because essential practical and fundamental research interests variation in BGP, updates time series remains the subject of different interdisciplinary analyses [2, 3, 9]. In our recent research, we have focused on the comparison of dynamical changes that occurred in the BGP updates process under the influence of Slammer worm and WannaCrypt ransomware through the assessment of fractal features of considered time series.

We started with the analysis of multifractal features of BGP data sets recorded for entire periods of observation in 2003 and 2017. As said above, for this we applied a robust to possible nonstationarities method – MF-DFA, which is often used for complex data sets of different origins. As we see in Fig. 2, MF-DFA at polynomial fitting $p = 2$, indicates obvious multifractal patterns selected for our analysis BGP updates time series recorded for the entire period of observation (13.01.2003 to 06.02.2003 for Slammer worm and period from 01.05.2017 to 27.05.2017 for WannaCrypt ransomware).

Though both data sets reveal multifractality, anyway we mention that in a period of a WannaCrypt attack, the BGP updates process is closer to monofractality compared with the case of a Slammer worm attack. This follows from the different character of fluctuations which are different for different scales (compare curves given by circles and triangles in Figs. 2a and 2b). We observe that for the Slammer worm attack case, fluctuations on small scales at negative q values are stronger than the contribution of larger fluctuations at positive q values (see Fig. 2a). Further, we note differences in the range of H(q) or Hmax(q)-Hmin(q), which is a quantitative measure of the multifractality [5]. Fig. 2b shows that the width of the singularity spectrum for BGP updates time series recorded in the period of the Slammer attack is wider than in the case of a ransomware attack. In spite of these differences, we underline that in both cases BGP updates time series reveal clear multifractality of considered process in both cases mentioned attacks.

Next, we proceed to the analysis of fractal properties of BGP updates time series recorded in periods prior to and during considered attacks. Comparison of these periods was important to have an understanding of the character of similarities

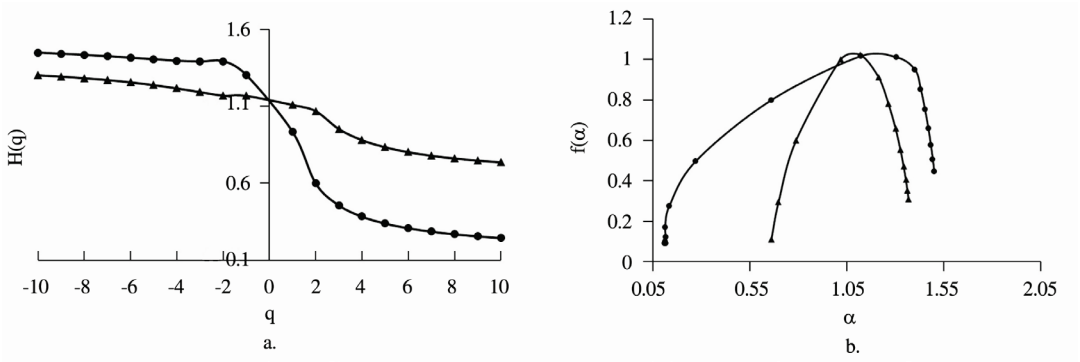

Fig. 3. a) Generalized Hurst exponent *H(q)* as a function of *q* and b) singularity spectra of BGP updates data sequence, prior (21.03.2003-24.01.2003) (circles) and during (25.01.2003-28.01.2003)(triangles) Slammer worm attack.

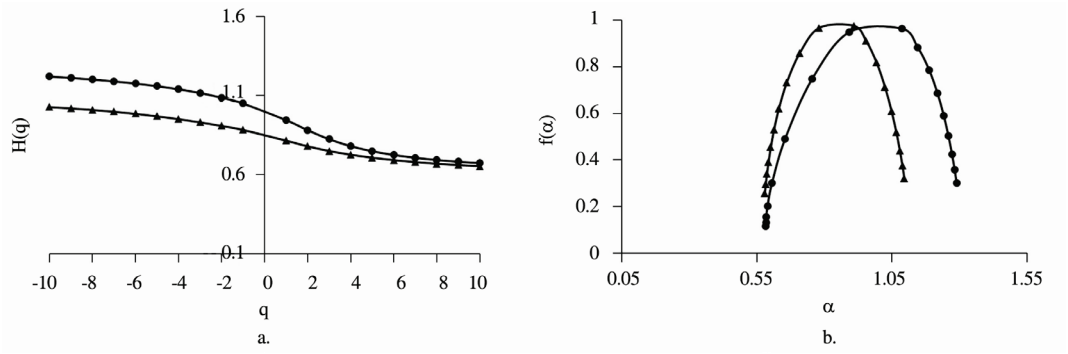

Fig. 4. a) Generalized Hurst exponent *H(q)* as a function of *q* and b) singularity spectra of BGP updates data sequence, prior (10.05.17-12.05.17) (circles) and during (12.05.2017 to 15.05.2017) (triangles) WannaCrypt ransomware attack.

or differences in changes caused by Slammer attacks compared to a ransomware attacks. This analysis is of immense importance taking into consideration that from the available for us scientific literature we were unable to find information about such analysis carried out elsewhere.

Results of the analysis aimed at assessment of fractal features of BGP time series prior to and during attacks are presented in Figs. 3 and 4. First of all, it should be pointed out that closeness to monofractal behavior observed for BGP time series recorded in the period of a ransomware attack (in 2017) is preserved for the shorter period before actual WannaCrypt attack as follows from left plots in Figs. 3 and 4 (compare upper curves). This is an interesting fact and apparently may point to global changes in the process of BGP updates that occurred for long period from 2003 to 2017. At the same time, we underline that despite such possible changes general multifractality feature of BGP updates has not been changed.

As for the comparison of changes caused by the Slammer worm and ransomware attacks, we in Figs. 3 and 4, see that the Slammer worm caused stronger changes. Indeed, the multifractality measure or the range of Hmax(q)-Hmin(q), in the case of a Slammer worm attack (Fig.3) reveals much more multifractal behavior than for the case of a ransomware attack (Fig.4).

Further, we see, that in both cases of attacks, the extent of multifractality in the BGP updates dynamics decreases. Considered process slightly but tends to become closer to monofractality. At the same time, such a shift to the monofractality is most noticeable in the case of the Slammer worm attack in 2003.

Conclusions

In this work, we have analyzed BGP updates data sets for the periods of self-propelling worm Slammer as well as WannaCrypt cryptoworm attacks. We used time series of BGP update messages, collected at international collectors. We investigated fractal properties of intact BGP updates process based on the method of multifractal detrended fluctuation analysis. It was found that the BGP updates process always reveals multifractal properties, though for different periods of analysis, the extent of multifractality may be different. Under the attack of Slammer worm, and WannaCrypt ransomware noticeable changes occurred in the process of BGP updates, which is revealed in the slight but noticeable qualitative shift to the mono-fractality. At the same time, quantitative changes are different. Multifractal properties have been mostly destroyed by the influence of Slammer compared to Wanacript. Found differences may help in the better recognition of the character of BGP updates dynamics caused by Internet worms and different ransomware attacks.

ინფორმატიკა

BGP-ის დროითი განახლებების ფრაქტალურ მახასიათებლებში (თვისებებში) Worm-ების და Ransomware-ს ზემოქმედების შედეგად წარმოქმნილი ცვლილებების შედარება

ა. ფრანგიშვილი*, თ. მაჭარაშვილი**, ა. სბორშჩიკოვი**, ე. მეფარიძე**, დ. ტეფნაძე**, ლ. ლალიაშვილი**, ე. ჩიკვილაძე§,**, თ. ხუციშვილი§, ზ. ჭელიძე**

*აკადემიის წევრი, საქართველოს ტექნიკური უნივერსიტეტი, თბილისი, საქართველო
**ივანე ჯავახიშვილის სახ. თბილისი სახელმწიფო უნივერსიტეტი, მ. ნოდიას გეოფიზიკის ინსტიტუტი, თბილისი, საქართველო
§საქართველოს ტექნიკური უნივერსიტეტი, ინფორმატიკისა და მართვის სისტემების ფაკულტეტი, მართვის სისტემების დეპარტამენტი, თბილისი, საქართველო

BGP-ის განახლებების ვარიაციის ანალიზი კვლავ რჩება ინტერდისციპლინარული კვლევების ყურადღების ცენტრში. ყველაზე მნიშვნელოვანია BGP-ის განახლებების ცვლილებების დინამიკური მახასიათებლების როგორც ზოგადი გამოკვლევა, ასევე, განსაკუთრებით, მათი გამოკვლევა სხვადასხვა გარე და შიდა ფაქტორების ზემოქმედების დროს, რამაც შესაძლოა გავლენა

იქონიოს ინტერნეტის ფუნქციონალზე. წარმოდგენილ ნაშრომში ჩვენ ვიყენებთ საერთაშორისო კოლექტორებისგან შეგროვებულ BGP-ის განახლებების დროით რიგებს. გამოვიკვლიეთ BGP-ის განახლების დაუზიანებელი პროცესის ფრაქტალური მახასიათებლები Slammer-ის და WannaCrypt-ის შეტევების დროს. გამოვიყენეთ მულტიფრაქტალური დეტრენდირებული რყევების ანალიზის მეთოდი (MDFA). აღმოჩნდა, რომ BGP-ის განახლების პროცესი ყოველთვის ავლენს მულტიფრაქტალურ თვისებებს. Slammer-ის და WannaCrypt-ის შეტევების დროს განახლების პროცესში დაფიქსირდა მნიშვნელოვანი ცვლილებები. ამავე დროს, ამ ორ განხილულ შემთხვევაში ცვლილებები განსხვავდება ერთმანეთისგან. მულტიფრაქტალური თვისებები უფრო მეტად დაზიანდა Slammer-ის შეტევისას, ვიდრე WannaCrypt-ის შემთხვევაში. აღმოჩენილი განსხვავებები შესაძლოა დაგვეხმაროს Ransomware ტიპის შეტევების ხასიათის უკეთ ამოცნობაში.

REFERENCES

1. Rekhter Y., Li T., Hares S. (2006) Border Gateway Protocol 4, RFC 4271, Internet Engineering Task Force.
2. Elmokashfi A., Dhamdhere A. (2014) Revisiting BGP Churn Growth, *ACM SIGCOMM Computer Communication Review (CCR)*, **44**, 1: 5-12.
3. Kitsak M., Elmokashfi A., Havlin S., Krioukov D. (2015) Long-range correlations and memory in the dynamics of internet interdomain routing, *PLOS ONE,* **10**, 11: e0141481.
4. Li Z., Rios A. L. G., Trajković L. (2020) Detecting internet worms, ransomware, and blackouts using recurrent neural networks, 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2165-2172.
5. Kantelhardt J. W., Ashkenazy Y., Ivanov P. C., Bunde A., Havlin S., Penzel T., Peter J., Stanley H. E. (2002) Characterization of sleep stages by correlations in the magnitude and sign of heartbeat increments, *Phys. Rev. E* **65:** 051908.
6. Peng C. K., Mietus J., Hausdorff J., Havlin S., Stanley H. E., Goldberger A. L. 1993 Long-range anticorrelations and non-Gaussian behavior of the heartbeat, *Phys. Rev. Lett.* **70**: 1343-1346.
7. Peng C.K., Havlin S., Stanley H. E., and Goldberger A. L. (1995) Quantification of scaling exponents and crossover phenomena in nonstationary heartbeat time series, *Chaos*, **5**: 82–87.
8. Eichner J. F., Koscielny-Bunde E., Bunde A., Havlin S., Schellnhuber H. J. (2003) Power-law persistence and trends in the atmosphere: a detailed study of long temperature records, *Phys. Rev. E,* **68**: 046133.
9. Prangishvili A., Matcharashvili T., Davitashvili I., Mepharidze E., Tepnadze D., Laliashvili L., Sborshchikovi A. (2021) Changes occurred in the variation of internet border gateway protocol updates, caused by influence of self-propagated slammer worm. *Bull. Georg. Natl. Acad. Sci.*, **15**, 4: 25-30.

Received December, 2023