საქართველოს მეცნიერებათა ეროვნული აკადემიის მოამბე, ტ. 15, №4, 2021
BULLETIN OF THE GEORGIAN NATIONAL ACADEMY OF SCIENCES, vol. 15, no. 4, 2021

Informatics

Changes Occurred in the Variation of Internet Border Gateway Protocol Updates, Caused by Influence of Self-Propagated Slammer Worm

Archil Prangishvili[*], Teimuraz Matcharashvili[§], Irma Davitashvili[**], Ekaterine Mepharidze[§], Dimitri Tepnadze[§], Levan Laliashvili[§], Aleksandre Sborshchikovi[§]

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

We analyzed variability of the border gateway protocol time series recorded at three Remote Route Collectors (RRC), located in Geneva and London. The aim of the research was to assess the character of changes in the period of commencement of the self-propagated Slammer worm in 2003. We used Singular Spectrum Analysis (SSA) and Hilbert Huang transformation (HHT) to assess changes in the frequency content of BGP updates. It was shown, that time period followed after the Slammer worm commencement was characterized by essential changes in the frequency content of BGP updates variation. Wide frequency range typical for original process of BGP updates was essentially narrowed. Such changes usually indicate to the rise of quasi-periodic components and points to the increased extent of regularity of considered BGP updates process. Such changes occurred in all data sets recorded at three different and distantly located RRC–es. We explain observed changes as caused by the influence of Slammer worm. We also compared the results obtained with the results of the research carried out earlier on other BGP updates time series from four largest Internet provider companies. In that analysis we also documented strong and simultaneous changes in the time series of BGP updates, though causes of changes were not identified. Based on the results of present research we conclude that, the changes found in the former work could have been caused by the influence of other worm which apparently acted mainly like Slammer worm though was not recognized that time. *© 2021 Bull. Georg. Natl. Acad. Sci.*

Internet, border gateway protocol, Slammer self replicating worm, Hilbert-Huang transformation, singular value decomposition, dynamics

Internet is the one of the main world's infrastructures and presently applies to all spheres of human activity ranging from: science, business, education, health, to art and entertainment [1-5]. One third of today's world population has access to the Internet and this number is fast increasing [6]. Therefore, safety and security of Internet acquires critical concern. Indeed, there are known many facts when the Internet was subjected to different types of attacks [6,7]. This is why, the number of

researches aimed at investigation of Internet dynamics and Internet security increases [6-8].

In this work we focused on the analysis of Border Gateway Protocol (BGP) time series. BGP provides important Internet Network Reachability Information. The question of vulnerability of routing process from different unwanted influences is of great research and practical interest. Presently, it is known that, BGP anomalies may consist of different harmful changes in the protocol's behavior and may be related with number of factors influencing dynamics of processes in the core of internet [9]. For example, BGP instability and anomalies may occur when Internet web servers are attacked by worm programs - self-replicating codes that exploit the systems vulnerabilities and propagate via networks. Slammer is the one of such worms that self-propagated by using the User Datagram Protocol (UDP) and commenced on January 23, 2003 at 05:31 (GMT). It is known that this worm only exists as a network packet and acts by running processes in the victim's host though does not store itself in the memory of affected hosts.

In present research we aimed to investigate the character of BGP updates process in the period prior and after Slammer worm commencement. BGP updates time series were obtained from different and distantly located collectors.

The main research idea is to compare these changes with changes which we reported in the frame of our previous researches [3,4]. Namely we reported noticeable changes occurred in the dynamics of BGP updates process in time series simultaneously recorded for 4 main international Internet providers [3,4]. Here we continued our analysis for BGP updates time series recorded at three International monitors located in Geneva and London. We used Hilbert-Huang transformation and singular value decomposition to test changes occurred in the variability of BGP time series prior and after influence of self-propagated Slammer worm in January 2003. We assumed that in case if self-propagated Slammer worm causes changes in the character of Internet processes, then we should expect appearance of quantifiable similar changes in the process of BGP updates at all three considered collectors simultaneously.

Materials and Methods

In present research we used BGP updates time series collected from the European network coordination center (RIPE) site, prior and after commencement of the self-propagated Slammer computer worm on 23.01.2003,from 05.31 to 19.30 GMT. In order to exclude influence of any local effects on the targeted process of BGP updates variation, for the first stage of our analysis, we selected BGP time series from three collectors located in Amsterdam, London, and Geneva (to save space we present just two typical time series in Fig. 1).

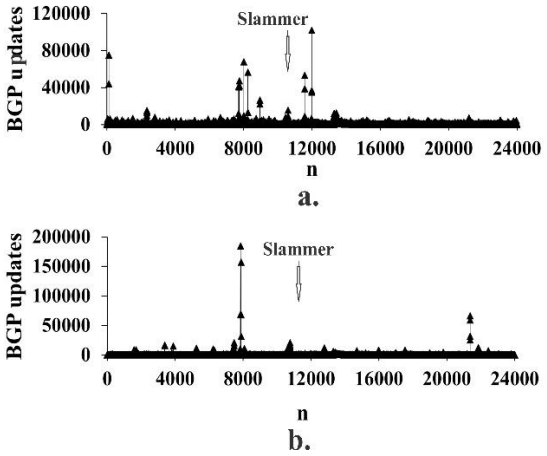

Fig. 1. BGP recordings (16.01.2003 to 02.02.2003) collected from collectors located in London (a) and Geneva (b).

In order to know whether different possible noises affect our analysis we started from Singular Spectrum Analysis (SSA) decomposition as de-noising technique. The SSA is helpful to investigate oscillatory components in considered data sets [10]. The original BGP time series were decomposed and noise free reconstruction was accomplished based on the first 5 SSA components thus removing by

this the rest of noisy components. Then we used the Hilbert-Huang Transform (HHT) [11]. HHT is an approach suitable for the analysis of non-stationary series, and is based on the use of an adaptive time-frequency decomposition that does not impose a fixed basis on the data. Therefore, unlike the other decomposition methods the HHT is not limited by the time-frequency uncertainty relationship. During the first part of HHT procedure (the so-called empirical mode decomposition - EMD), the analyzed time series is decomposed into Implicit Mode Functions (IMFs) [11] by means of the sifting procedure. Resulting IMFs represent a simple oscillatory modes which play the role similar to a simple harmonic function for spectral analysis. At the same time IMF is much more general because it can have an amplitude and frequency varying with time, contrarily to the constant amplitude and frequency of a simple harmonic component. The second part is the Hilbert transformation of the IMFs, yielding the time-frequency representation (Hilbert spectrum) of each IMF. Indicating as *x(t)* a real signal and as $X_n(t)$ the IMFs, their Hilbert transform $H\left[X_n(t)\right]$ is $Y_n(t)=\frac{1}{\pi}P\int_{-\infty}^{\infty}\frac{X_n(\tau)}{t-\tau}d\tau,$ where *P* is the operator called Cauchy Principal Value. The analytic signals, $Z_n(t)$ are given by $h_f=\int_0^T A(f,t)dt.$ Here *i* is the imaginary unit. From the analytic signals instantaneous amplitude $A_n(t)=\sqrt{X_n(t)^2+Y_n(t)^2}$ and phase $\phi_n(t)=\arctan\left(\frac{Y_n(t)}{X_n(t)}\right)$ can be determined. The instantaneous frequency is given by $f_n(t)=\frac{d\phi_n}{dt}.$ The total amplitude (or energy) from each frequency component is given by the marginal spectrum h_f, $h_f=\int_0^T A(f,t)dt.$

Results and Discussions

As we see in Fig. 2, two typical data sets, reconstructed from original BGP time series from London and Geneva collectors, after remove of noise part still reveal different cycles location of which not always coincide. It is noticeable, that at different collectors, location of larger or smaller increase in the reconstructed main components of BGP update time series occurred both prior or after Slammer worm commencement (for Amsterdam BGP time series situation is the same). Thus, it is not clear whether these changes are related directly to influence of self propagated Slammer worm or not.

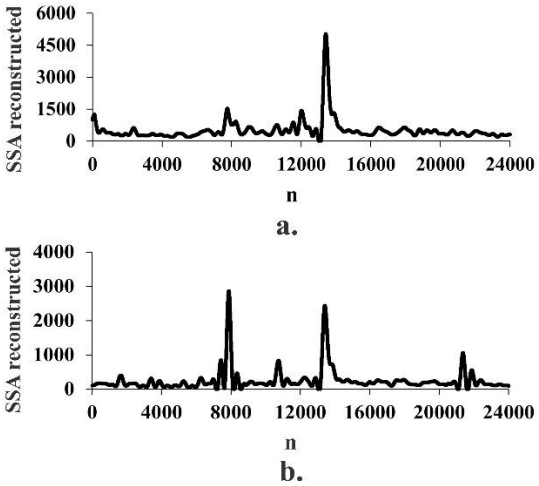

Fig. 2. Data sets reconstructed from the main SSA components of BGP time series recorded at collectors located in London (a) and Geneva (b).

Next in order to clear up whether Slammer worm influenced in the process of BGP updates variation we used HHT. The results for London and Geneva presented in Fig. 3 clearly show dominance of low frequency range after the period of actual Slammer worm commencement. Such changes are obvious for all three considered locations (for Amsterdam BGP time series the situation is the same) and points to the similar character of influence of Slammer worm on the variability of BGP updates process. This part of frequency range variation in analyzed data sets is

marked by grey in Fig. 3. Observed changes obviously are caused by the influence of Slammer worm and point to noticeable changes in frequency content of BGP updates process. Changes occurred almost at the same time in all three analyzed BGP updates time series and point to essential changes in the extent of regularity of analyzed process.

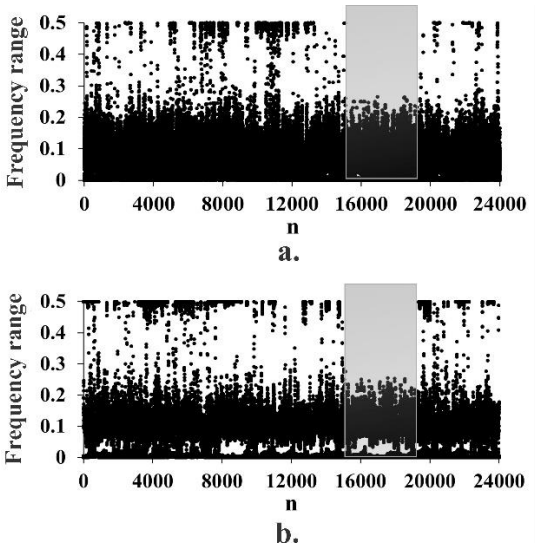

Fig. 3. Variation of frequency content of IMFs of BGP updates time series collected from collectors located in London (a) and Geneva (b).

Presented here results are interesting itself and also gives arguments in favor to propose the explanation of changes observed earlier for data sets collected from the four world's largest internet provider companies (for further details about the mentioned data sets and RouteViews project see [3,8]. Namely BGP updates time series recorded at AT&T, NTT, IIJ, and Tinet AS-es revealed simultaneous drastic changes in the process of BGP updates occurred in 2011 [3,4]. Base on findings described in the present research we suppose that changes found in BGP data sets of four mentioned International AS-es in 2011 could be explained as the effects caused by the influence of certain, possibly Slammer like, worm which apparently has remained unrecognized.

Conclusion

We analyzed BGP updates time series recorded at three International collectors in the period of commencement of the self-propagated Slammer worm, 2003. Modern data analysis methods such as SSA and HHT were used to assess changes occurred in frequency content of BGP updates time series. It was found that the time period followed the Slammer worm influence is characterized by essential changes in the frequency content of BGP updates process taking place in the core of Internet. Namely, frequency range is decreased that points to the increase in the extent of regularity in the considered process of BGP updates. As far as such changes occurred simultaneously in all three data sets recorded at three different and distant collectors after commencement of self-propagated worm, we come to conclusion that changes should be explained as a cause of Slammer worm influence. By comparing the findings with those of our previous analysis, where we also recorded strong and simultaneous changes in the time series of BGP updates from four different vendors, we conclude that those changes may also have been caused by the influence of another worm, which apparently acted mainly as a Slammer worm but was not recognized at that time.

ინფორმატიკა

ინტერნეტის სასაზღვრო კარიბჭის პროტოკოლის განახლებების ცვალებადობაში თვითგავრცელებადი სლამერ კომპიუტერული ვირუსის გავლენით გამოწვეული ცვლილებები

ა. ფრანგიშვილი*, თ. მაჭარაშვილი§, ი. დავითაშვილი**, ე. მეფარიძე§, დ. ტეფნაძე§, ლ. ლალიაშვილი§, ა. სბორშჩიკოვი§

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

წინამდებარე კვლევაში გავაანალიზეთ ინტერნეტის სასაზღვრო კარიბჭის პროტოკოლის განახლებების (BGP) დროითი მწკრივები, რომელიც მიღებულია დისტანციური მარშრუტების სამი კოლექტორისგან. მოცემული კოლექტორები მდებარეობს ჟენევასა და ლონდონში. კვლევის მიზანი იყო 2003 წელს თვითგავრცელებადი კომპიუტერული ვირუსის – სლამერის (Slammer) გავრცელების პერიოდში ინტერნეტის ბირთვში აღძრული ცვლილებების ხასიათის შეფასება. ამ მიზნით, BGP განახლებების დროს დროითი მწკრივების სიხშირულ კონტენტში მომხდარი ცვლილებების შესაფასებლად გამოვიყენეთ მონაცემთა ანალიზის ისეთი მეთოდები, როგორიცაა სინგულარული სპექტრული ანალიზი და ჰილბერტ ჰუანგის გარდაქმნა. შედეგებმა აჩვენა, რომ სლამერ კომპიუტერული ვირუსის გაშვებისთანავე ინტერნეტ ბირთვში BGP განახლებების პროცესის სიხშირულმა კონტენტმა მნიშვნელოვანი ცვლილებები განიცადა. BGP განახლებებისთვის მახასიათებელი ფართო სიხშირული დიაპაზონი მნიშვნელოვნად შევიწროვდა. პროცესის ანალიზისას ასეთი ცვლილებები ჩვეულებრივ მიუთითებს კვაზი-პერიოდული კომპონენტების გავლენის ზრდაზე, რაც თავის მხრივ BGP განახლებების რეგულარობის ხარისხის ამაღლებაზე მიუთითებს. მსგავსი ცვლილებებით ხასიათდება BGP განახლებების სამივე განხილული დროითი მწკრივი, რომლებიც ტერიტორიულად განსხვავებულ, სამ ერთმანეთისაგან დაშორებულ კოლექტორზეა ჩაწერილი. მომხდარ ცვლილებას ჩვენ ვხსნით, როგორც სლამერ ვირუსის გავლენის შედეგს. ვადარებთ რა ამჟამად მიღებულ შედეგს ჩვენივე წინა კვლევის შედეგებს, სადაც ვაჩვენეთ სხვა ოთხი კოლექტორიდან მიღებული BGP განახლებების დროით მწკრივში მომხდარი ძლიერი და ერთდროული ცვლილებების ფაქტი, შეგვიძლია დავასკვნათ, რომ ის ცვლილებები შესაძლოა გამოწვეული ყოფილიყო სხვა რომელიმე კომპიუტერული ვირუსის მიერ, რომელიც, როგორც ჩანს, მოქმედებდა სლამერ ვირუსის მსგავსად, თუმცა არ იყო აღმოჩენილი დროის იმ მომენტისთვის.

REFERENCES

1. Crovella M., Krishnamurty B. (2006) Internet measurement: infrastructure, traffic and applications, Wiley.
2. Angrisani L., Botta A., Miele G., Pescapè A., Vadursi M. (2014) Experiment-driven modeling of open-source internet traffic generator, *IEEE Transaction on Instrumentation and Measurement*, **63**, 11: 2529-2538.
3. Matcharashvili T., Elmokashfi A., Prangishvili A. (2020) Analysis of the regularity of the internet interdomain routing dynamics, *Physica A*, 124142.*a*
4. Matcharashvili T., Prangishvili A., Tsveraidze Z., Laliashvili L. (2020) Scale Features of a Network Echo Mechanism: case study for the Different Internet Paths, *Journal of Computer Networks and Communications*, 4065048.*b*
5. Matcharashvili T., Prangishvili A. (2020) Quantifying regularity of the internet interdomain routing based on border gateway protocol (BGP) data bases. 2020 International conference on electrical, communication and Computer Engineering (ICECCE), 1-5. *c*, Istanbul, Turkey.
6. Elmokashfi A. (2011) On BGP Inter-domain Routing: an investigation of scalability with respect to Churn, PhD Thesis, Oslo, Norway.
7. Pescapè A. (2007) Entropy-based reduction of traffic data, *IEEE Communications Letters*, **11**, 2: 191-193.
8. Kitsak M., Elmokashfi A., Havlin S., Krioukov D. (2011) Long-range correlations and memory in the dynamics of Internet Interdomain Routing, *PLOS ONE*, **10**, 11: e0141481.
9. Li Z., Rios A.L.G., Trajković L. (2020) Detecting Internet Worms, Ransomware, and Blackouts Using Recurrent Neural Networks, in Proc. IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2165-2172.
10. Vautard R., Yiou P., Ghil M. (1992) Singular-spectrum analysis: a toolkit for short, noisy chaotic signals, *Physica D*, **58**, 1-4: 95–126.
11. Huang N., Wu Z. (2008) A review on Hilbert-Huang transform: method and its applications to geophysical studies, *Reviews of Geophysics*, **46**: 1- 23.

Received July, 2021