Formation of informative characteristics of network traffic states using its dynamic filtration

A Krasnov¹, D Nikol'skii¹, D Repin¹, O Galtseva²

¹Federal State Autonomous Educational Establishment of Additional Professional Education “Center of Realization of State Educational Policy and Informational Technologies”, Moscow, Russia
²National Research Tomsk Polytechnic University, Tomsk, Russia
E-mail: krasnovmgutu@yandex.ru

Abstract. The approach to the task of detecting DDoS attacks based on the formation of secondary informative characteristics of its states on the observed parameters of data packets headers of network traffic is considered. Secondary informative characteristics characterize the traffic time structure or its behavioral character. The problem is solved by the method of dynamic filtering of traffic using various operators: the causal transformation operator and the evolution operator.

1. Introduction
Traditionally, the traffic anomaly detection is carried out according to the results of identification of deviation of its current state from patterns of normal states. At the same time, various methods of intellectual analysis are used such as method of principle component analysis [1], wavelet analysis [2], histogram analysis [3], support vector machines [4, 5] and detection of shifts in spatial-temporal traffic patterns [6]. Secondary informative features which are formed as logical fingerprints for various network protocols [7], entropic [8], correlational [9] and structural functions of primary informative features of traffic [10] are used for more in-depth analysis. Various difference measures and metrics are used to detect DDoS attacks against the background of changing legitimate traffic, including taking into account the “flash crowds” effect [11, 12].

The use of signatures to detect DDoS attacks requires the accumulation of a significant amount of data for all types of attacks; it is used in a similar way to virus detection methods [13]. Neural networks are widely used as part of complex systems for detecting and protecting against DDoS attacks [14–16]. Another approach is based on identifying group anomalous behavior, which is typical for botnets and differs from the usual actions of legitimate users. IP addresses of the traffic originator [17] and packet identification numbers [18] can be used to detect DDoS attacks. A detection system was proposed which effectively identifies the anomalous state of the system using patterns of group activity of network nodes [19]. Known clustering methods were used to detect malicious packets in traffic and identify botnets [20–23].

It should be noted that there are no publications in the network security field in which issues of formation and productive use of the space of secondary informative features of traffic from the standpoint of statistical dynamics are. Network traffic in the works mentioned above is considered as a set of static data (for example, the number of packets per second) without taking into account their
dynamic structure, which is determined by the statistics of time consecution and the corresponding stable connections of the primary features. However, in fact any network channels and traffic passing through them are the dynamic systems [24]. It is necessary to take into account both the speed of changes in traffic and the instant values of network loads for their adequate description.

The aim of the this work is to summarize the results of theoretical and experimental studies of the authors on the analysis of network traffic [10, 24, 25] and to substantiate the methods of formation of secondary informative features of network traffic on the basis of its consideration as a dynamic system.

2. Research Method

Dynamic filtering is performed by scanning the vector \( P_n = (P_{1n}, P_{2n}, \ldots, P_{Mn})^T \) of the stream \( M \) of parameters of network traffic data packet headers \( n = 1, 2, \ldots, N \) by dynamic window \( w_{(n, AN)} \) with an aperture \( \Delta N \). The formation of vector of secondary informative features of network traffic \( F_n = (F_{1n}, \ldots, F_{K})^T \cdot K \) occurs at every \( n-m \) window position. In the general case, each \( k \)-th secondary informative attribute is formed by the action of the corresponding functional or operator \( F_k \) on the set of vectors of parameters of the packet headers of network traffic data packets included in the window \( w_{(n, AN)} \):

\[
F_{kn} = F_k(P_n, P_{n-1}, \ldots, P_{n-AN+1}), \; k = 1, 2, \ldots, K. \tag{1}
\]

The formation of vectors of secondary informative features is necessary for account the statistical relationship of vectors traffic parameters \( AN \) (primary informative features) to take into account the temporal structure of its behavior. Normalized frequency distributions \( o(F_i), \ldots, F_k(r) \) formed from a set of observations \( N \) of vectors \( F_n \) in different states of \( St \) of traffic \( r = 0, 1, \ldots, R-1 \) are used for a stable description of such connection. Normalized frequency distribution was considered as the conditional probability of values of the secondary informative features of traffic under specified states. Some trajectory in the phase space of its secondary informative features corresponds to traffic dynamic filtering in such a formulation of the problem. The trajectory passes through various subspaces corresponding to different traffic states \( St \) \( r = 0, 1, \ldots, R-1 \). In this case, the subspaces can overlap, which is typical for real network traffic containing a mixture of attacking packets. Therefore, the detection of fact of entry of the traffic trajectory into any subspace and the classification of the subspace type are probabilistic procedures.

3. Results and Discussion

The following operators were used for dynamic filtering.

3.1 The causal transformation operator

This operator converts auxiliary features \( X_{mn} \), calculated from the primary informative features of traffic \( P_{mn} (m = 1, \ldots, M) \), into its intermediate features \( Y_{mn} \). Hilbert's FIR filter with finite impulse characteristic is used for transformation \( h_n [24] \):

\[
Y_{mn} = h_1(X_{(m, n+1)} - X_{(m, n+3)}) + h_3(X_{(m, n-3)} - X_{(m, n+3)}) + h_5(X_{(m, n+5)} - X_{(m, n-5)}) + h_{MN}(X_{(m, n+\Delta N)} - X_{(m, n-\Delta N)}). \tag{2}
\]

Filter coefficients \( h_k \in (1, 1/3, 1/5, \ldots, 1/\Delta N) \) provide orthogonality of sequences \( X_{mn} \) and \( Y_{mn} \):

\[
\sum_{m} X_{mn} Y_{mn} = 0 \text{ for } m = 1, 2, \ldots, M. \tag{3}
\]

Intermediate features of traffic describe the generalized rates of its change, because they depend on higher-order derivatives of auxiliary features \( \Delta N \), which correspond to generalized coordinates. Wherein odd central differences should be used for linear independence of intermediate features in (2) so that each \( Y_{mn} \) does not depend on \( X_{mn} \) \( \forall n = 1, 2, \ldots, N \).

The set of intermediate and auxiliary features of traffic allows to consider the functioning of network data transmission channel as the behavior of multidimensional dynamic system of the \( \Delta \)-th order with generalized coordinates \( X_{mn} \) and generalized speeds \( Y_{mn} \). It is enough to use \( \Delta N = 7 \ldots 13 \) for practice.
In accordance with the approach of Ludwig Boltzmann, Henri Poincare and Willard Gibbs [26], the states of multidimensional dynamic system with generalized coordinates $X_m$ and generalized velocities $Y_m$ are described by a family of phase portraits which do not contain time explicitly, but describe the change of the states of the system, i.e., its dynamics in the form of phase trajectories in the corresponding phase spaces $\{X, Y\}_m$. Figure 1 shows examples of phase portraits corresponding to the normal state of traffic and its abnormal state (the case of TCP Syn Flood attack) [24]. The ratio of parameters (number of octets to the number of packets) of the load part of the headers of traffic data packets received from the edge router of the network via the Net Flow Protocol is taken as a generalized coordinate $X$.

It is quite difficult to perform the numerical calculations, which are necessary to detect attacks with predetermined probability at describing traffic conditions in the form of phase portraits. Therefore, generalized coordinates and pulses were converted into one-dimensional secondary informative features by hashing to simplify the calculations [24]:

$$F_{mn} = X_{mn} + Y_m, \quad m = 1, 2, \ldots, M; \quad n = 1, 2, \ldots, N.$$  \hspace{1cm} (4)

![Figure 1. Examples of phase portraits of normal state of traffic (a) and its abnormal state (b) (TCP Syn Flood attack) [24].](image)

Normalized frequency distributions $\omega(F_1, \ldots, F_K|r)$ of hash functions were formed. Figure 1 shows example of normalized one-dimensional frequency distributions $\omega (FK|r)$, formed in relation of the parameters (number of octets to the number of packets) of the load part of the traffic for $N=4000$ counts of observations at different states $r \in \{\text{Normal; HTTP Flood; Slow Loris}\}$.

The frequency distributions of all traffic states differ significantly on different intervals of values $F$ of its informative feature (Figure 2).

### 3.2 The evolution operator

It is assumed that the continuous vector $P(t) = [P_1(t), \ldots, P_M(t)]^T$ of traffic characteristics $P_m(t)$ ($m=1, \ldots, M$) at forming this operator is described by the differential equation [10, 25]:

$$dP(t)/dt = (1/\Delta t) \cdot H(t) \cdot P(t),$$  \hspace{1cm} (5)

where the dynamic operator $H(t)$ is unknown, and only the values of the components of the vector $P$ of the parameters of the packet headers of traffic data observed at various discrete moments of time $t_n \in (t_0, t_N]$ are known. The time interval $\Delta t$ is introduced into (5) because of dimension reasons. It is also assumed that there is an operator $S(t, t)$ for $H(t)$, which gives the solution of the Equation (5):

$$P(t) = S(t, t) \cdot P(t), \quad S(t, t) = E,$$  \hspace{1cm} (6)

where $E$ is unit matrix.
Figure 2. Example of normalized one-dimensional frequency distributions $\omega(F|r)$ for three traffic states ($N = 4000, \Delta N = 7$).

The operator $S(t, \tau)$ is called the matriciant or Cauchy matrix in mathematics and the evolution operator or the time shift operator in physics. The connection of the evolution operator of the dynamic system $S(t, \tau)$ with its dynamic operator $H(t)$ is described as a series [25]:

$$S(t, \tau) = E + \frac{1}{\Delta t} \int_{\tau}^{t} H(t_1) dt_1 + \frac{1}{2!} \left( \frac{1}{\Delta t} \right)^2 \int_{\tau}^{t} dt_1 \int_{\tau}^{t} dt_2 \ J\{H(t_1) \cdot H(t_2)\} + \cdots ,$$

(7)

where $J$ is Dyson chronological operator [27] ($J\{H(t_1) \cdot H(t_2)\} = H(t_1) \cdot H(t_2)$, if $t_1 > t_2$ and $J\{H(t_1) \cdot H(t_2)\} = H(t_2) \cdot H(t_1)$, if $t_1 < t_2$).

Normalized frequency distributions $\omega(F|r)$ for different traffic states $S_r (r = 0, 1, 2, \ldots, R)$ were formed by observing all its counts $N$. For example, Figure 3 shows the normalized frequency distributions $\omega(F|r)$, formed by two parameters (number of octets and packets) of the load part of the traffic for $N=4000$ observations of adjacent counts $t$ and $\tau$ at different states $r \in \{\text{Normal; HTTP Flood; Slow Loris}\}$.

Frequency distributions of all traffic states differ significantly on different intervals of values $F$ of its informative feature (Figure 3). However, the window for the formation of secondary informative features by the evolution operator method was used; its size is significantly smaller than the size of the window at the causal operator method.

Figure 3. Example of normalized one-dimensional frequency distributions $\omega(F|r)$ for three traffic states ($N = 4000, \Delta N = 2$).

Normalized frequency distributions $\omega(F|r)$, formed by any known method of dynamic filtering, are peculiar images (patterns) of traffic states $S_r (r = 0, 1, \ldots, R-1)$. Additional experiments using the tools...
developed by the authors [28, 29] have shown that the use of frequency distributions allows to adjust automatically the decision-making thresholds at given probabilities of detection and errors based on the use of the method of Wald's sequential analysis [30,31].

4. Conclusion
The method of formation of secondary features of network traffic states, which is necessary to detect DDoS-attacks; it is based on its dynamic filtering is developed. The causal transformation operator and the evolution operator are used for dynamic traffic filtering. Experimental studies shown the principal possibility of using the developed method in the intelligent systems for detection and identification of the main types of DDoS attacks. The advantage of the developed method is unified approach to the description of traffic states and the ability to detect anomalies by automatic setting of thresholds of decision making at given probabilities of detection and errors. These provisions are fundamental for solving of the tasks of network traffic analysis of super-large volume (more than 100 Gbit/s). Thus, the proposed methods can complement and significantly expand the methods used in real systems of protection against DDoS-attacks.

Acknowledgments
The investigation was carried out with financial support of the state represented by the Ministry of Education and Science of Russia on the lot with the code 2017-14-579-0002 on the topic “Design of effective network attack detection algorithms based on detecting deviations in the traffic of super-large volumes coming to the data transfer network border routers, and creation of specimen of software complex on their basis for detecting and preventing threats to the security of information aimed at rejection in the service”, agreement No. 14.578.21.0261 on the provision of a grant from 09/26/2017, a unique identifier of work (project) RFMEFI57817X0261.

References
[1] Liu Y. et al 2010 Proc. of IEEE Int Conf ICDCS 807–816 doi: 10.1109/ICDCS.2010.45
[2] Srihari V., Anitha R. 2014 Proc of Int Symposium SSCC 291–303 doi: 10.1007/978-3-662-44966-0_28
[3] Kind A. and Stockeclin M. P. 2009 IEEE Trans on Netw Serv Manag 6(2) 110–121
[4] Catania C. A. et al 2012 Expert Syst Appl 39(2) 1822–1829
[5] Ye J. et al 2018 Secur Commun Netw 2018 9804061 doi:10.1155/2018/9804061
[6] Yuan J. and Mills K. 2005 IEEE T Depend Secure 2(4) 324–335
[7] Crotti M. et al 2007 ACM Sigcomm Comp 37(1) 5–16
[8] Reddy V. S. et al 2012 IOSR J Comput Eng 7(1) 13–18
[9] Yu Sh. et al 2012 IEEE T Parall Distr 23(6) 1073–1080 doi: 10.1109/TPDS.2011.262
[10] Galayev V. S. et al 2016 IJAR 12 10781–10790
[11] Ke L. et al 2009 Proc of IEEE Int Conf NNS 9–17
[12] Chawla Sh. et al 2016 ICSIS 14(10) 382–389
[13] Malina L. et al 2015 Proc of Int Conf SPI 113–128
[14] Chen J. H. et al 2012 Proc of IEEE Int Conf GrC 38–43
[15] Gupta B. B. et al 2012 Int J Comput Sci Netw 14(2) 61–70
[16] Saied A. et al 2016 Neurocomputing 72 385–393 doi: 10.1016/j.neucom.2015.04.101
[17] Baishya R. C. et al 2017 IJISA 19(6) 929–939 doi: 10.6633/IJNS.201711.19(6).09
[18] Thang T. M. and Nguyen V. K. 2017 Software Networking 1 213–228 doi: 10.13052/jsn2445-9739.2016.012

[19] Chen Ch. – M. and Lin H. – Ch. 2015 JISA 21 42–51 doi: 10.1016/j.jisa.2014.05.002
[20] Dietrich Ch. J. et al 2013 Computer Networks 57(2) 475–486 doi: 10.1016/j.comnet.2012.06.019
[21] Terzi D. S. et al 2017 Proc of IEEE Int Conf UBMK 592–597 doi: 10.1109/UBMK.2017.8093473
[22] Lu W. et al 2011 Computer Communications 34(3) 502–514 doi: 10.1016/j.comcom.2010.04.007
[23] Wang K. et al 2011 Computer Networks 55(15) 3275–3286 doi: 10.1016/j.comnet.2011.05.026
[24] Krasnov A. E. et al 2018 IAER 13(8) 5647–5654
[25] Krasnov A. E. et al 2018 The Bulletin of Udmurt University. Mathematics. Mechanics. Computer Science 28(3) 407–418 doi: 10.20537/vm180310 (in Russian)
[26] Nolte D. D. 2010 Physics Today 63(4) 31–33 doi: 10.1063/1.3397041
[27] Dyson F. J. 1949 Physical Review 75(11) 1736–1755 doi: 10.1103/PhysRev.75.1736
[28] Repin D. S. et al 2018 Program Comlex “DDoS Attacks Simulator The Certificate on Official Registration of the Computer Program 2018615691 (in Russian)
[29] Krasnov A. E. et al 2018 Proc of All-Russian Pospelov’ Conference Hybrid Synergistic Intelligent Systems 349–354
[30] Serikov T. G. et al 11th International Forum on Strategic Technology (IFOST 2016) 7884168 510-514
[31] Wald A. 1947 Sequential analysis (J. Wiley & Sons, Inc.: New York)