HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

IMPROVEMENT OF A FIXED-PARAMETER STATISTICAL CONTROL METHOD FOR AUTOMATIC ELIMINATION OF NETWORK ANOMALIES

Maxmudov Shohruhbek Toxirjon Ugli

Institute of information and communication technologies and military communications

Abstract. This paper proposes an improved threshold value method for real-time detection and automatic elimination of network anomalies. Network traffic is modelled as a stochastic process governed by statistical regularities under normal conditions. Based on statistical process control theory, upper and lower control limits are derived from the mean traffic value and a maximum permissible deviation parameter. A binary indicator function formalises the detection logic, while an eight-stage functional architecture integrates statistical modelling, real-time monitoring, and automated response. When an anomaly is detected, the system immediately applies predefined countermeasures — including traffic throttling, IP blocking, and IDS/IPS alerting — without human intervention, thereby ensuring continuous network stability.

Keywords: network anomaly detection, statistical process control, stochastic traffic modelling, control limits, threshold method, indicator function, automated elimination, real-time monitoring.

One of the most critical challenges in the process of network anomaly detection is the accurate interpretation of temporal variations in traffic parameters and the identification of deviations from normal operating conditions. The theoretical foundation for anomaly detection in network monitoring systems is rooted in statistical process control theory [1,2], while the applied dimension corresponds to statistical anomaly detection methods [3,4]. In these approaches, network traffic is treated as a time series, modelled as a stochastic process [8] - meaning that traffic metrics such as packet counts, byte volumes, and flow rates vary over time. Since these variations are neither entirely predictable nor arbitrarily disordered, traffic is regarded as a stochastic process. Within such a framework, the instantaneous traffic value at any given moment cannot be determined in advance with certainty; however, it is not completely random either - it conforms to well-defined statistical regularities.

For instance, during a typical working day, network traffic fluctuates around a stable mean, and minor deviations from that mean are considered normal. In other words, traffic values exhibit a characteristic statistical distribution: values near the mean occur most frequently, whereas extremely low or extremely high values are rare. This statistical model provides a reference of what constitutes normal traffic behaviour. Given such a model, a sudden sharp increase or decrease that exceeds the established bounds is classified as an anomaly [5,6]. As a practical illustration: if a server ordinarily receives 500 packets per second, values of 480 or 520 per second are within the normal range; however, a sudden rise to 5,000 packets per second may indicate a probable attack or system fault. In general, network traffic varies stochastically, yet these variations conform to a specific statistical order, and any departure from that order is classified as an anomaly.

Network traffic is treated as a stochastic process that is assumed to comply with certain statistical laws under normal operating conditions. A statistical analysis based on historical data is performed to characterise the normal behaviour of network traffic. This analysis yields the primary statistical descriptors of traffic parameters. The mean value represents the level around which traffic typically stabilises under normal conditions and characterises the overall traffic volume. The variance indicates the degree to which traffic values deviate from the mean - that is, the degree of traffic

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

variability. In addition, permissible fluctuation bounds are established, defining the interval within which traffic parameters may vary under normal operating conditions. These statistical descriptors collectively form a model characterising the normal state of the system. In subsequent stages, real-time observations of traffic values are compared against this model, and deviations from normal behaviour are identified. If observed values fall outside the permissible fluctuation bounds, the situation is assessed as a probable network anomaly.

According to statistical process control theory [1,2], the system is considered to be operating in a stable state when the variations in process parameters remain natural - for example, when packet counts fluctuate slightly from second to second, latency oscillates within a narrow range, and load is higher during working hours and lower at night. However, if observed values exceed the established control limits, or if the distributional properties of traffic change significantly, this indicates the presence of an uncontrolled external factor influencing the system.

From an applied perspective, this implies that the monitoring system continuously observes traffic parameters in real time and compares them against a pre-established statistical model. When a significant deviation from the model is detected, the system generates an anomaly alert. Thus, the core of the methodology consists of characterising normal behaviour by means of a mathematical model and interpreting statistically significant deviations from that model as anomalies. To formalise this approach, network traffic is modelled as a stochastic process [8]:

$$A(t)= m + e(t) \quad \textbf{(1)}$$

where m - denotes the mean value under normal operating conditions, and e(t) represents natural fluctuation - small random deviations around the mean. According to statistical process control theory, the permissible fluctuation region of the process is defined by upper and lower control limits:

$$UCL = m + \Delta, \quad LCL = m - \Delta \quad \textbf{(2)}$$

where Δ - denotes the maximum permissible deviation. The real-time observed value A(t) is then compared against this interval. If A(t) > UCL or A(t) < LCL, the system classifies the situation as an anomaly. This condition can be expressed by the following binary indicator function:

$$\text{Signal} = \begin{cases} 1, & A(t) \in [LCL, UCL] \\ 0, & \text{otherwise} \end{cases} \quad \textbf{(3)}$$

The graphical interpretation of this process is reflected in the control chart presented in Figure-1.

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

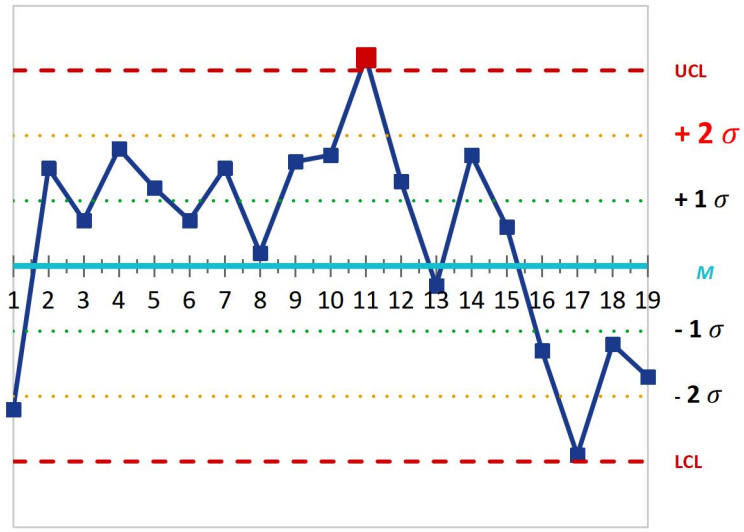


Figure - 1. Control chart based on statistical process control theory

In the chart, the centre line corresponds to the mean m, while the upper and lower boundaries represent UCL and LCL, respectively. If any data point in the time series exceeds UCL - that is, A(t) > UCL - then the indicator takes the value A(t) = 1 and an anomaly is recorded. From a probabilistic standpoint, such a departure from the control region is a rare event and signals the presence of an external influence or a system fault.

This theoretical model is operationalised through the functional architecture depicted in Figure 2. Specifically, the process of detecting anomalies in network traffic based on the statistical control model consists of eight interrelated stages executed sequentially. These stages enable the characterisation of normal network traffic behaviour and the identification of anomalies through real-time comparison against that baseline. The first stage involves the mathematical modelling of the process.

Network traffic is treated as a time-dependent indicator and is expressed in the form:

$$A(t) = m + e(t) \quad \textbf{(4)}$$

where - m is the mean value under normal operating conditions, and e(t) is a random deviation representing natural fluctuation. This model provides a theoretical justification for the oscillation of network parameters around the mean under ideal conditions.

The second stage encompasses real-time monitoring and the collection of traffic observations. In this stage, network traffic is observed in real time and the current values A(t) of the traffic parameters are recorded continuously. Monitoring is conducted via network devices, SNMP systems, or dedicated monitoring applications. The result is a sequential time series of traffic observations that serves as the primary input for subsequent statistical computations.

In the third stage, the mean level m of the observed traffic values is determined as follows:

$$m=\frac{1}{n}\sum_{i=1}^{n} A_i \quad \textbf{(5)}$$

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

where:

m - the mean value of network traffic, Ai - the i-th observed traffic value, n - the number of observations, ∑ - the summation operator over all observed values.

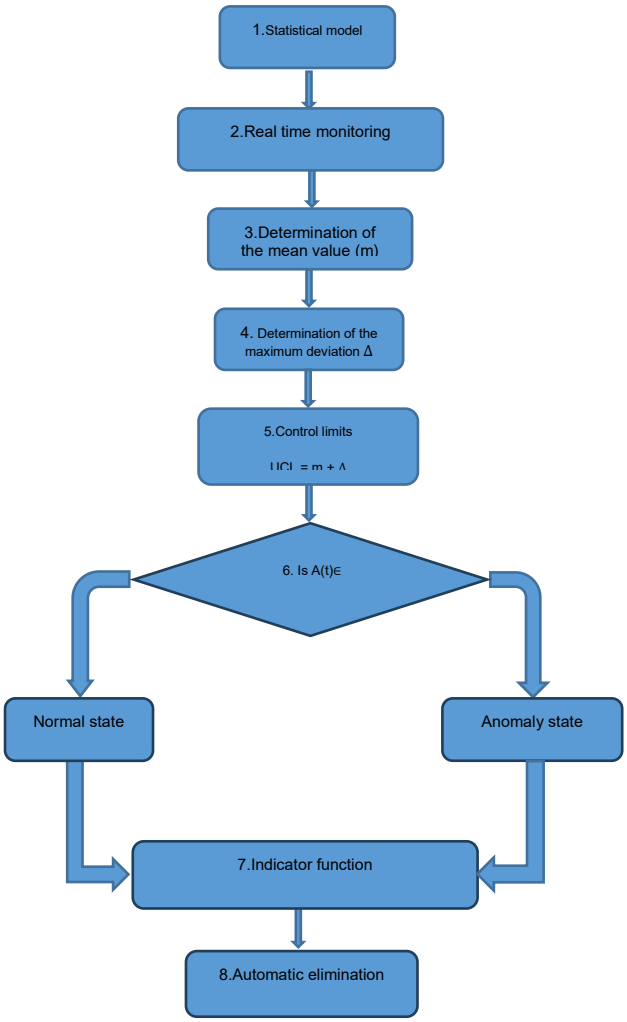


Figure 2. Functional architecture of the anomaly detection process

This value is computed on the basis of historical data or observations collected over a defined time window. The mean represents the stable operating state of the system and serves as the baseline parameter for subsequent computations.

In the fourth stage, the maximum permissible deviation Δ is established. This stage defines the extent to which traffic values may deviate from the mean during normal system operation. To this end, the maximum permissible deviation parameter Δ is introduced. This parameter represents the natural variation bound of network traffic and is used to delimit the range of values considered normal for the system. The value of Δ is selected as a practical criterion and directly determines the sensitivity of the system. If Δ is set to a small value, the system classifies even minor deviations as anomalies, thereby increasing detection sensitivity but potentially leading to a higher rate of false positives. Conversely, if

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

Δ is large, only substantial deviations are detected, which enhances operational stability but increases the risk of missing certain anomalies.

Accordingly, the selection of the Δ parameter depends on the operating conditions of the system, the characteristics of network traffic, and the objectives of the monitoring process. In practice, Δ may be determined empirically or in relation to statistical measures such as the standard deviation.

In the fifth stage, control limits that define the normal operating state of the system are established. These limits delimit the permissible deviation range around the mean traffic value and serve as the primary criterion for anomaly detection. The control limits are determined by the following equations:

$$UCL = m + \Delta \quad (6)$$

$$LCL = m - \Delta \quad (7)$$

where: - UCL - Upper Control Limit, LCL - Lower Control Limit, m - the mean value of network traffic, Δ - the maximum permissible deviation.

These limits define the normal operating interval of the system: when traffic values fall within this range, the system is considered to be functioning in a stable state. Graphically, this corresponds to symmetrically positioned bounds on both sides of the mean m. In practice, the control limits constitute the primary criterion for anomaly detection. If a real-time traffic observation falls within these bounds, the system is assessed as operating normally. Conversely, if the traffic value exceeds either the upper or the lower limit, an anomalous condition is indicated.

It should be noted that the accuracy of the control limits depends directly on the proper selection of the Δ parameter. An incorrect choice may result in excessive false alarms or, conversely, in the failure to detect genuine anomalies. For this reason, the stage of establishing control limits is one of the most critical steps in the anomaly detection process.

The sixth stage activates the comparison mechanism. In this stage, real-time traffic observations are compared against the pre-established control limits. This process constitutes the core mechanism for anomaly detection [6,7] and enables the assessment of the current system state. The comparison is performed by verifying the following condition for the current traffic value A(t):

$$LCL \leq A(t) \leq UCL \quad (8)$$

If this condition is satisfied - that is, the traffic value falls within the defined interval - the system is deemed to be operating normally. In this case, the variation in traffic is treated as a natural process and no corrective action is required. Conversely, if the observed value exceeds the control limits - that is:

$$A(t) < LCL \text{ or } A(t) > UCL \quad (9)$$

this indicates the presence of an anomaly in the system. Such a condition is typically associated with a sharp increase or decrease in traffic volume and may indicate a system fault, traffic overload, or the presence of an external threat such as a network attack. The primary function of this stage is to rapidly and accurately assess the system state by comparing current traffic values against the normal operating interval. The outcome of this comparison is formalised in the subsequent stage using an indicator function and is forwarded to the decision-making process.

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

In the seventh stage, the result of detecting the presence or absence of an anomaly is formalised by means of a binary indicator function. This function expresses the system state in a simplified numerical form and serves as the basis for subsequent control processes. The indicator function is defined as follows:

$$\text{Signal}(t)=\begin{cases} 0, \text{LCL}\le A(t)\le \text{UCL} \\ 1, A(t)<\text{LCL or } A(t)>\text{UCL} \end{cases} \quad \textbf{(10)}$$

where: Signal(t) = 0 - the system is operating in normal mode, Signal(t) = 1 - an anomaly has been detected in the system.

This indicator function translates the results of statistical analysis into a practical decision-making mechanism. Specifically, when a real-time traffic observation exceeds the control limits, the system automatically generates an anomaly signal. The significance of this stage lies in the fact that it converts complex statistical computation results into a simple, rapidly processable form. As a result, the monitoring system is capable not only of detecting anomalies but also of issuing a timely response.

The final stage involves the application of automated control measures in response to the detected anomaly. This stage extends beyond mere detection and incorporates a practical mechanism aimed at eliminating the anomaly. The anomaly elimination process is expressed through the following functional relation:

$$E(t) = f(\text{signal}(t), R) \quad \textbf{(11)}$$

where: E(t) - the control action executed by the system, signal(t) - the output of the indicator function, R - the set of predefined control rules and security policies.

When signal(t) = 1 - that is, when an anomaly is detected - the system may automatically apply one or more of the following countermeasures [3,4,5]:

- throttling of traffic flows;
- blocking of suspicious IP addresses;
- isolation at the port or VLAN level;
- forwarding an alert to intrusion detection and prevention systems (IDS/IPS);
- escalation of the monitoring level.

If signal(t) = 0, the system continues to operate in normal mode and no additional action is required. This stage integrates the statistical control model with practical network management. As a result, the system not only detects anomalies but also responds to them in real time, thereby ensuring network stability.

The proposed method demonstrates that statistical process control theory provides a rigorous and computationally tractable foundation for automated network anomaly management. By treating network traffic as a stochastic process with a stable mean and bounded natural fluctuations, the approach establishes a formally defined normal operating state against which real-time observations are continuously evaluated. The eight-stage functional architecture ensures that detection, decision-making, and response are tightly integrated. Crucially, the coupling of the binary indicator function to predefined control rules enables fully automated elimination of detected anomalies — including traffic

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

throttling, address blocking, port isolation, and IDS/IPS notification — without operator involvement, thereby ensuring network stability in real time. Future work should focus on adaptive tuning of the deviation parameter Δ through machine learning techniques to accommodate evolving traffic patterns and previously unseen attack vectors.

References:

1. Shewhart, W. A. Economic Control of Quality of Manufactured Product. Van Nostrand, New York, 2021. - 501 p.

2. Montgomery, D. C. Introduction to Statistical Quality Control. 7th ed. John Wiley & Sons, New Jersey, 2022. - 754 p.

3. Chandola, V., Banerjee, A., Kumar, V. Anomaly detection: A survey // ACM Computing Surveys. - 2019. - Vol. 41, No. 3. — P. 1–58.

4. Ahmed, M., Mahmood, A. N., Hu, J. A survey of network anomaly detection techniques // Journal of Network and Computer Applications. - 2024. - Vol. 60. - P. 19–31.

5. Lakhina, A., Crovella, M., Diot, C. Diagnosing network-wide traffic anomalies // ACM SIGCOMM Computer Communication Review. - 2024. - Vol. 34, No. 4. - P. 219–230.

6. Barford, P., Kline, J., Plonka, D., Ron, A. A signal analysis of network traffic anomalies // Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurement (IMW). - Marseille, 2022. - P. 71–82.

7. Brauckhoff, D., Salamatian, K., May, M. Applying PCA for traffic anomaly detection: problems and solutions // Proceedings of IEEE INFOCOM. - Rio de Janeiro, 2019. - P. 2866–2870.

8. Papoulis, A., Pillai, S. U. Probability, Random Variables, and Stochastic Processes. 4th ed. McGraw-Hill, New York, 2022. - 852 p.