ENSURING CYBERSECURITY IN DATA TRANSMISSION SYSTEMS BASED ON PHYSICAL PROCESSES AND MATHEMATICAL MODELING

Turgunov Nozimjon Abdumannopovich
Kurbonova Firuza Zaripovna
Karimov Dilshod Ismatovich
Doctor of Physical and Mathematical Sciences, Professor, Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan, Tashkent
Doctor of Philosophy (PhD) in Technical Sciences, Associate Professor, Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan, Tashkent
Lecturer, Department of Exact Sciences, Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan, Tashkent.

https://doi.org/ 10.5281/zenodo.23694710

Abstract. This article examines cybersecurity in data transmission systems using physical process analysis and mathematical modeling. The influence of signal attenuation, electromagnetic interference, signal-to-noise ratio, packet loss, and transmission delay on the reliability of information systems is considered. A network assessment approach based on statistical indicators and probabilistic models is described. A composite cyber-risk index is proposed to support anomaly detection through the combined analysis of physical parameters and network traffic characteristics. The article outlines the principles of a mathematical approach that integrates physical processes and network metrics to improve information security monitoring.

Keywords: cybersecurity, data transmission, physical processes, mathematical modeling, electromagnetic interference, signal-to-noise ratio, information security, probabilistic model, network monitoring, anomaly detection.

Introduction

The rapid development of information and communication technologies is increasing the importance of data transmission systems within public administration, industry, finance, transport, and law enforcement. Ensuring the confidentiality, integrity, and availability of information within these systems is a key objective of cybersecurity.

The process of data transmission depends not only on software algorithms but also on physical principles. Factors such as the propagation of electrical signals, electromagnetic interference, signal attenuation within communication channels, and the specific characteristics of the transmission medium all influence the quality of data exchange. Consequently, the mathematical modeling of physical processes and the statistical analysis of network parameters are essential for enhancing

cybersecurity.

Certain anomalous conditions within a network may arise from technical malfunctions, natural interference, or system overload. In other instances, however, such anomalies may be linked to cyberattacks. Distinguishing between these causes requires the integrated examination of multiple parameters.

The objective of this research is to develop a method for detecting anomalous conditions in data transmission systems and assessing cyber threats by utilizing physical processes and mathematical modeling techniques. The research objectives are as follows:

- to study the physical factors affecting the data transmission process;
- to mathematically represent signal quality and network performance metrics;
- to develop statistical criteria for identifying anomalous conditions;
- to formulate a comprehensive risk index based on physical and network parameters;
- to define a method for evaluating the proposed model using experimental data.

Physical Foundations of Data Transmission Systems

In a data transmission system, information is conveyed via electrical, electromagnetic, or optical signals. Signal quality depends on the transmission medium, distance, frequency, noise level, and the technical specifications of the equipment.

1. Signal-to-Noise Ratio

The signal-to-noise ratio is a key physical indicator of a communication channel. It is defined by the following formula [1], [2]:

$$SNR = \frac{P_s}{\mathrm{P_n}}$$

Here: SNR is the ratio of signal power to noise power, P_s is the useful signal power, and P_n is the noise power.

To express this ratio in decibels, the following formula is used:

$$\mathrm{SNR(dB)} = 10 \times \log_{10} \frac{P_s}{\mathrm{P_n}}$$

A decrease in the signal-to-noise ratio may indicate a degradation in communication quality. However, this occurrence alone does not prove the existence of a cyberattack. Therefore, signal parameters are analyzed in conjunction with other network indicators[1].

2. Signal attenuation

In wireless communication systems, signal power may decrease as the distance between the transmitter and the receiver increases. Under ideal free-space conditions, signal losses are estimated using the following formula:

$$L_{FS}(\text{dB}) = 20 \times \log_{10} \frac{4\pi df}{\text{c}}$$

where: L_{FS} is the free-space signal loss (in dB), d is the distance between the transmitter and the receiver (in meters), f is the signal frequency (in Hz), and c is the speed of light (approximately) $3 \cdot 10^8$ m/s.

This formula describes propagation in an ideal free space. Under real-world conditions, obstacles, reflections, and other factors must also be taken into account.

3. Channel Capacity

According to Shannon's theory, the theoretical capacity of an ideal noisy channel is defined as follows:

$$C = B \times \log_2(1 + SNR)$$

where: C is the theoretical channel capacity (bit/s), B is the channel bandwidth (Hz), and SNR is the signal-to-noise power ratio.

This equation expresses the relationship between the physical characteristics of a channel and its data transmission capability [1].

Mathematical Model of a Data Transmission System

Several parameters can be used to evaluate the state of a network. We represent them using the following vector:

$$X(t) = \{SNR(t), P_{loss}(t), D(t), V(t), N(t)\}$$

where:

SNR(t) – signal-to-noise ratio;

$P_{loss}(t)$– packet loss rate;

D(t) – average packet delay;

V(t) – volume of traffic transmitted per unit of time;

N(t) – number of connections within a specified time interval.

This vector allows for the assessment of the system state based on several parameters.

1. Packet loss rate

If the number of transmitted packets is n and the number of lost packets is m, the empirical packet loss rate is calculated as follows [3]:

$$P_{loss} = \frac{m}{n},$$

where n > 0.

For example, if 20 out of 1,000 packets are lost:

$$P_{loss} \frac{20}{1000} = 0{,}02.$$

thus, the packet loss rate is 2 percent.

Packet loss may be related to connection quality, network load, or technical malfunctions. In some cases, this metric serves as a basis for investigating security incidents.

2. Average Packet Delay

If the measured delay values for n packets are denoted as d_1, d_2, ..., d_n, the average delay is defined as follows:

$$D_{\text{avg}} = \frac{d_1 + d_2 + \ldots + d_n}{n}$$

Using summation notation:

$$D_{\text{avg}} = \frac{1}{n} \times \sum_{i=1}^{n} d_i$$

where $i = \overline{1,n}$.

An increase in delay may be attributed to network congestion, changes in routing, or other factors.

Statistical detection of anomalous conditions

To identify unusual changes in the network, current indicators are compared with values observed during normal operating conditions.

The standardized deviation is calculated as follows[]:

$$z = \frac{x - \mu}{\sigma}$$

where $\sigma > 0$.

Here: x is the current observed value, μ is the mean value under normal conditions, σ is the standard deviation, and z is the standardized deviation.

If the condition $|z| > \tau$ is met, the observed value is considered to fall outside a defined statistical threshold. Here, τ is a pre-selected threshold value.

For example, if $\tau = 3$ is chosen, values lying beyond three standard deviations in data that approximates a normal distribution may be flagged for further investigation. It should be noted that a statistical deviation does not directly confirm a cyberattack; it merely helps to identify an anomalous state within the system.

Developing a Composite Cyber-Risk Index

A composite risk index can be used to evaluate physical and network indicators collectively.

First, a normalized risk score is determined for each parameter[5]:

$$r_j = min\left(1, \frac{\max(0, z_j)}{\tau_j}\right)$$

This formula applies to indicators where an increase in value signifies an escalation in risk. For indicators where a decrease in value signals a potential problem such as the signal to noise ratio the deviation is calculated in the opposite

direction. The composite index is defined as follows:

$$R = w_1 r_1 + w_2 r_2 + \ldots + w_k r_k \text{ or } R = \sum_{j=1}^{k} w_j \times r_j$$

The weights must satisfy the following conditions:

$$w_j \geq 0, \;\; w_1 + w_2 + \ldots + w_k = 1$$

where:

R is the composite risk index;

r_j is the normalized score of an individual parameter;

w_j is the weight of the corresponding parameter;

k is the number of parameters being considered.

If each value r_j falls between 0 and 1, the composite index will also fall within this range.

An increase in the index value indicates greater deviations from the norm in the observed indicators. However, to consider this index a calibrated estimate of the probability of a cyberattack, it must be empirically validated against known events.

Integrating physical and mathematical models

Analyzing physical processes and network indicators together helps to distinguish the potential causes of anomalous conditions.

For example, if the signal-to-noise ratio decreases while packet loss increases, the possibility of a degradation in the quality of the physical connection is examined. If, however, the signal quality remains stable while traffic volume and the number of connections rise sharply, further investigation into network load or suspicious activity is required.

The system dynamics can be expressed in a general form as follows [1,2]:

$$X(t+1) = f\big(X(t), U(t)\big) + \varepsilon(t)$$

where: X(t) is the current state of the system; U(t) represents external influences and parameters defining the operating mode; f is the function describing the system dynamics; and ε(t) is a random error.

Using the model, a forecast of the subsequent state is calculated and compared against actual observations, determined by the following formula:

$$e(t) = X(t) - X_{\text{forecast}}(t)$$

If the error exceeds standard limits, an unexpected change in the system state may have occurred. The cause of this change is then investigated using additional data.

Cybersecurity Assurance Algorithm

1. The proposed approach can be implemented through the following stages:

2. Data collection. Signal quality, packet loss, latency, and traffic volume are recorded.

3. Data processing. Checks are performed for missing values, measurement errors, and temporal inconsistencies.

4. Defining the normal state. Statistical indicators are calculated for the network's standard operating mode.

5. Anomaly detection. Current indicators are compared against the model of the normal state. Calculating the risk index. Parameters are combined using a weighted sum.

6. Verifying results. Suspicious instances are cross-referenced with network logs and security records.

7. Selecting protective measures. Appropriate security measures are implemented based on the type of confirmed incident.

This algorithm can help improve network monitoring. Its effectiveness should be evaluated using data from real-world scenarios or controlled experiments.

Evaluating model performance

To validate the proposed model, a dataset comprising both normal and anomalous network states is compiled. The model's outputs are then compared against pre-identified incidents[7].

Accuracy indicator:

$$Precision = \frac{TP}{TP + FP}$$

Completeness indicator:

$$Recall = \frac{TP}{TP + FN}$$

F1-criterion:

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

Here:

TP – correctly identified anomalous conditions;

FP – incorrectly identified anomalous conditions;

FN – unidentified (missed) anomalous conditions.

These metrics allow for the evaluation of the model's ability to detect anomalous conditions. Furthermore, it is advisable to consider the rate of false alarms, detection time, and computational costs. It is not possible to provide specific percentages regarding the model's accuracy or efficiency until experimental results are obtained.

Integrating physical processes with mathematical modeling expands the capabilities for analyzing security incidents in data transmission systems. This approach enables the consideration of the relationship between the physical state of the communication channel and network activity.

However, when applying the model in practice, factors such as differences in communication technologies, the variability of network traffic, and the reliability of measurements must be taken into account. Additional diagnostics are required to

distinguish deviations caused by physical noise or technical malfunctions from signs of a cyberattack.

Therefore, it is appropriate to use the composite risk index not as an independent diagnostic tool, but rather as a monitoring instrument that helps isolate suspicious events for further, in-depth investigation. Conclusion

This article examined the issue of ensuring cybersecurity in data transmission systems based on physical processes and mathematical modeling. Methods for analyzing physical indicators such as the signal-to-noise ratio, signal attenuation, and channel bandwidthn as well as network parameters such as packet loss, latency, and traffic volume were discussed.

An approach for developing a comprehensive cybersecurity risk index by integrating physical and network indicators was proposed. This approach can be utilized to identify deviations from the norm within a system and to isolate instances that require further investigation.

Future work may involve implementing the model using the Python programming environment, conducting controlled experiments, and evaluating the results through statistical criteria. Such efforts will contribute to the advancement of scientific connections between the modeling of physical processes, applied mathematics, and cybersecurity.

REFERENCES:

1. Cover T. M., Thomas J. A. Elements of Information Theory. 2nd ed. Hoboken, NJ: Wiley-Interscience, 2006. 748 p.
2. Shannon C. E. A Mathematical Theory of Communication. Bell System Technical Journal, 1948, Vol. 27, pp. 379–423, 623–656.
3. Stallings W. Data and Computer Communications. 10th ed. Harlow, England: Pearson Education Limited, 2014. 907 p.
4. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. 9th ed. Pearson, 2025.
5. Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks (5th ed.). Boston, MA: Pearson Prentice Hall. 933 pp.
6. NIST. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29, 2024.
7. Bishop, C. M. (2006). Pattern Recognition and Machine Learning. New York, NY: Springer. 738 pp.