Machinery & Energetics
Vol. 16, No. 4. 2025

Journal homepage:
https://technicalscience.com.ua/en

UDC 004.056.53:534.83
DOI: 10.31548/machinery/4.2025.64

Ihor Poslied*
Postgraduate Student
Dnipro University of Technology
49005, 19 Dmytro Yavornytskyi Ave., Dnipro, Ukraine
https://orcid.org/0009-0006-0885-2007

Mathematical modelling of acoustic leakage channels in cyber-physical systems

Abstract. Acoustic leakage channels are among the most underestimated threats to cyber-physical systems, since their occurrence is caused by complex wave processes that are difficult to capture using traditional control tools. The aim of the study was to develop and experimentally verify integrated approaches to modelling, identification and neutralisation of acoustic leaks based on a combination of wave models, active compensators and predictive systems. The methodology was based on 40 numerical experiments performed on four groups of models with subsequent repeated runs to ensure statistical reliability of the results. Significant differences were found between the four groups of wave models: the basic configurations (38-46 dB, 4-7% variance) were the simplest; the vibration scenarios formed 3-6 resonances with a variance of up to 18%; and the ultrasonic ones appeared to be the most critical (18-38 kHz, 71-89 dB, up to 11 resonances); the acousto-optic models demonstrated mixed time–frequency profiles with a variance of 16-24%. Among the active neutralisation methods, white noise showed the lowest efficiency (11-14 dB), while narrowband masking provided 19-23 dB, and Adaptive Noise Cancelling (ANC) achieved the best performance (34-39 dB, stability 96-97%, detection time 0.4-0.7 s). Among the predictive models, Long Short-Term Memory (LSTM) showed the best results (latency 0.42-0.55 s, stability 93-96%, reconstruction error 6-8%), while autoencoders were the least accurate (10-14%). The integral safety index reflected a clear stratification of risks: basic models – 0.62; vibration – 0.71; acousto-optic – 0.79; ultrasonic – 0.84. Statistical analysis confirmed the significance of the differences between all groups ($p < 0.01$) and the formation of two clusters of danger. The practical significance of the study lies in the creation of an integrated method for detecting and suppressing acoustic leaks, which can be directly applied when designing security systems for cyber-physical complexes to reduce the risk of covert attacks and increase resistance to multi-frequency influences

Keywords: white noise; narrowband masking; antiphase compensation; time-frequency spectrograms; autoencoders

INTRODUCTION

The relevance of the study is due to the rapid growth of the role of cyber-physical systems in critical infrastructure, industrial technologies, energy, transport and the defence sector. Deepening the integration of sensor, computing and communication components increases the dependence of such systems on the physical manifestations of information processes. The inconspicuous but technically most dangerous vectors of privacy violations include acoustic leakage channels, which are capable of converting vibrational, air, ultrasonic, infrasonic and acousto-optic signals into hidden data carriers.

The increase in the accuracy of sensors, the availability of microphone arrays and the development of spectral analysis methods create conditions under which even insignificant acoustic vibrations are able to carry confidential information, which significantly increases the requirements for the mathematical description, modelling and prediction of the parameters of such channels. In this context, the results of V. Korniienko *et al.* (2022) demonstrated that modulated wave transformations that occur in optical and electronic elements of cyber-physical systems are capable

Article's History: Received: 04.07.2025; Revised: 08.10.2025; Accepted: 27.11.2025.

Suggested Citation:
Poslied, I. (2025). Mathematical modelling of acoustic leakage channels in cyber-physical systems. *Machinery & Energetics,* 16(4), 64-75. doi: 10.31548/machinery/4.2025.64.

*Corresponding author

of forming structured trajectories of potential leakage, and it is these processes that require formalised modelling to predict their behaviour accurately. The authors drew attention to the fact that wave interaction between subsystems must be taken into account when building mathematical models of protection.

The features of mixing acoustic, electromagnetic and vibrational components are highlighted by A. Oleynikov *et al.* (2025), who showed that even weak nonlinear signal deformations can form hidden informative channels. Their analysis of spectral features demonstrated that extended models of time-frequency dynamics are required to detect such channels. The structural organisation of layered optoelectronic systems, where acoustic waves undergo sequential transformations, is presented by N. Dzyanyi (2025). The researcher emphasised that the behaviour of the signal depends on the resonances in each of the material layers, which requires a multi-level description.

The analysis of the propagation of acoustic pulses in technical networks, presented by V. Wong & J.A. McCann (2021), demonstrated the dependence of the amplitude-frequency characteristics on the infrastructure configuration. The authors emphasised that the adaptation of such models to security needs allows the identification of the conditions for the emergence of leakage channels. The stochastic nature of side channels, considered by W. Lucia & A. Youssef (2021), indicates that random environmental disturbances can significantly affect signal stability. The introduction of probabilistic parameters into the model allows for a more accurate assessment of leakage risks and prediction of vibration propagation trajectories. Side channel models reproduced by data analysis methods are presented by S. Chhetri & M. Al Faruque (2020), who demonstrated the effectiveness of time-frequency mapping of acoustic signals to reconstruct system behaviour. The proposed approach enhances the accuracy of simulations by combining physical parameters and machine analysis. Deep acoustic anomaly detection, described by Z. Shi *et al.* (2023), confirms that Long Short-Term Memory (LSTM) architectures are able to capture even minimal deviations in waveforms. The researchers emphasised that such an approach provides early detection of leakage in conditions of variable noise background.

Formal methods for synthesising side channel analysis, proposed by J. Wang *et al.* (2021), demonstrate the possibility of systematically describing signals that can be used for leakage. The authors showed that algorithms with correctness guarantees allow the minimisation of errors during threat classification. An assessment of the robustness of cloaking techniques in cyber-physical systems by S. Park *et al.* (2025) showed that acoustic manifestations can be recovered even with complex cloaking schemes. The results highlight the need for extended models that take into account secondary oscillations. Algorithmic approaches to anomaly detection in multi-sensor networks reviewed by R. Pinto *et al.* (2022) confirm the ability of real-time systems to capture weak acoustic disturbances. The authors proved that the integration of the sensory and communication layers is a key condition for informative monitoring.

An integrated model for countering physical attacks, proposed by S. Wu *et al.* (2022), takes into account the role of acoustic characteristics in the threat profile. The results demonstrate that combining signal analysis with control methods increases the accuracy of recognising dangerous scenarios. The systematisation of deep learning methods for analysing physical channels, performed by S. Picek *et al.* (2023), shows the promise of neural network approaches for reconstructing complex wave structures. The authors emphasised that the combination of mathematical modelling with deep algorithms forms the basis for advanced diagnostics of acoustic threats. A coordinated analysis of the above sources confirmed that acoustic leakage channels are a multidimensional phenomenon that combines physical, stochastic and informational properties. Therefore, the construction of a universal mathematical model requires the integration of wave physics, sensor monitoring data and machine signal analysis in a single formalised description.

The aim of the research was to develop and verify integrated methods for modelling, detecting and neutralising acoustic leaks through a comprehensive analysis of wave models, active silencing methods and intelligent predictive systems. The main objectives of the research were: to determine the parameters and structure of a universal model of acoustic leak channels; to develop mathematical and simulation methods for active protection against acoustic influences; to clarify the criteria and procedures for assessing the effectiveness of protecting cyber-physical systems from acoustic leaks.

MATERIALS AND METHODS

The theoretical and modelling study was carried out in March-June 2025 using the methods of system analysis, wave physics and computer modelling of acoustic processes in cyber-physical systems. The modelling was conducted under stable conditions (temperature 22 ± 1.5°C, pressure 0.1 MPa, frequency range 10-40 kHz, fixed boundary conditions for solid and air media), which ensured reproducibility of the parameters and excluded the influence of external acoustic vibrations. Four groups of models were formed for the work, covering the main types of acoustic leakage channels: air, vibration, ultrasonic and acousto-optic.

The first group represented the basic wave models of acoustic propagation without considering secondary effects, using Helmholtz equations and classical equations of vibroacoustics. The second group included models of signal transformation in structural elements of cyber-physical systems, which took into account mechanical resonances of casings, standing waves, interference effects and signal modulation on electronic nodes. The third group of models was based on a stochastic description of acoustic channels using random perturbations, white and pink noise, as well as parametric variations of materials, which allowed estimation of probabilistic leakage trajectories. The fourth group combined analytical models with machine learning algorithms using Long

Short-Term Memory (LSTM), a network with Gated Recurrent Units (GRU) and autoencoders, which made it possible to reproduce complex time-frequency dependencies and predict the appearance of channels in real time. For each group, 10 test scenarios (n = 40) were formed, which ensured representativeness and the possibility of correct comparison of results.

All simulations were performed in COMSOL Multiphysics 6.2 and MATLAB/Simulink 2024a using the Acoustics, Structural Mechanics and Signal Processing modules, which allowed modelling the interaction of acoustic waves with material surfaces, electronic components and composite structures. The Solid Mechanics ANSYS Fluent module was used to model vibration processes, taking into account the parameters Young's modulus, Poisson's ratio and damping. Ultrasonic channels were analysed taking into account nonlinear effects, harmonic distortion and frequency dispersion. Simulation data were collected using Python 3.12 with the PyAcoustics acoustic package and the librosa digital signal processing suite, which provided a unified structure of data arrays for subsequent time-frequency analytics. Time-frequency analysis was used as a key tool to identify structural patterns of acoustic leaks. The analysis included short-time Fourier transform, spectrogram construction, wavelet decomposition, estimation of harmonic distortions, stochastic impurities and mixed modes of acousto-optic interaction. Time-frequency analysis provided the selection of informative features for machine learning (ML) models and allowed determination of local resonant peaks, amplitude fluctuations and phase shifts that form the structure of covert channels. Four approaches were used to model active protection means: white noise generation, narrowband noise generation, antiphase signal compensation and adaptive suppression. During the analysis of protection protocols, the parameters of noise spectral density, the degree of leakage attenuation, the stability of the compensating signal and the sensitivity of the system to frequency changes were evaluated.

To objectively assess the effectiveness of the models, international standards in the field of side-channel analysis and protection of cyber-physical systems were used, in particular ISO/IEC No. 30147:2021 (2021) and ISO/IEC No. 30149:2024 (2024). The metrics included the leakage attenuation coefficient, the proportion of undetected signals, the average channel detection time and the efficiency of wave profile reproduction. Additionally, the integral Acoustic Security Evaluation Index (ASEI) criterion was used, which summarised the modelling results by three groups of indicators: the accuracy of wave process reproduction, the quality of detection of acoustic leakage channels and the efficiency of active methods for their neutralisation. ASEI was calculated for each of the 40 scenarios, after which all values were normalised in order to correctly compare different types of models within a single metric. For this, the following integral dependence was used (1):

$$ASEI = \frac{1}{3}\left(\frac{A_{model}-A_{min}}{A_{max}-A_{min}} + \frac{D_{detect}-D_{min}}{D_{max}-D_{min}} + \frac{P_{protect}-P_{min}}{P_{max}-P_{min}}\right), \quad (1)$$

where A_{model} denoted the accuracy of wave process modelling, D_{detect} corresponded to the quality of acoustic leak channel detection, $P_{protect}$ characterised the effectiveness of active neutralisation methods, and for each variable its minimum (A_{min},D_{min},P_{min}) and maximum (A_{max},D_{max},P_{max}) values were used for normalisation within the interval [0; 1], which ensured correct integration of different parameters into a single safety index.

Statistical analysis was performed in MATLAB 2024a using one-way analysis of variance (ANOVA) to detect intergroup differences and the Mann-Whitney U-test to test the significance of differences in samples that do not correspond to a normal distribution. To ensure statistical reliability, each modelling scenario was performed three times, after which the results were averaged with the formation of 95% confidence intervals, which minimised the influence of stochastic fluctuations. The obtained normalised ASEI values allowed us to quantitatively assess the effectiveness of different groups of models and identify the parameters that pose the greatest risks to the security of cyber-physical systems in the event of acoustic leaks.

RESULTS

Parameters of acoustic leakage channels in four groups of models

Reproduction of the behaviour of acoustic leakage channels in cyber-physical systems demonstrated that different groups of models form distinct wave profiles, which are manifested through characteristic frequency ranges, amplitude variations, resonant peaks and dispersion features. Basic wave models, built on Helmholtz equations and classical vibroacoustic theory, provided the initial configuration for evaluating the fundamental propagation mechanisms, allowing the separation of the primary leakage channels from the secondary transformations. In the air environment, the waves formed stable zones of standing oscillations in the lower frequency range, while in the vibration models, mechanical resonances of the body elements dominated, creating additional signal modulation paths. Ultrasonic scenarios revealed nonlinear effects and frequency dispersion typical of high-frequency leakage channels, whereas acousto-optic models showed the formation of combined wave modes in which optical and electronic components interacted with acoustic perturbations to form mixed modulation trajectories. The results are summarised in Table 1.

Table 1. Key wave propagation parameters and the nature of leakage channels in four groups of models (n = 40)

Model type	Dominant frequency, Hz	Amplitude of oscillations, dB	Number of resonance peaks	Dispersion level, %	Standing waves (presence/intensity)
Basic wave	210-480	38-46	1-2	4-7	Pronounced, low intensity
Vibrating	120-950	52-68	3-6	11-18	Pronounced, medium intensity

Continued Table 1.

Model type	Dominant frequency, Hz	Amplitude of oscillations, dB	Number of resonance peaks	Dispersion level, %	Standing waves (presence/intensity)
Ultrasonic	18000-38000	71-89	5-11	22-31	Weak, high-frequency modes
Acoustic and optic	7500-14000	48-61	4-7	16-24	Fragmented, unstable

Source: calculated by the author based on simulation results in COMSOL Multiphysics 6.2, MATLAB/Simulink 2024a, ANSYS Fluent, Python 3.12, PyAcoustics and librosa

The observed values demonstrate that the basic wave models provide the most predictable wave propagation profile, while the structural vibration channels dramatically enhance the amplitude through modal resonances. Ultrasonic scenarios reveal the potential for high-frequency latent leakage with pronounced nonlinearity, which makes it difficult to detect them using standard methods. Acousto-optic models form hybrid mechanisms in which acoustic oscillations are modified by optical modulations, creating complex time-frequency patterns that significantly increase the risk of latent channels in cyber-physical systems. The depth of wave distortions, resonance peaks and the nature of dispersion allowed us to identify the most dangerous frequency bands and channel types, which will determine the further effectiveness of detection algorithms and active protection.

Time-frequency structure of signals and stochastic leakage trajectories

Time-frequency analysis showed that the spectral profiles of acoustic channels are formed by a combination of wave mechanisms, material parameters and stochastic disturbances. The study of the time-frequency structure of signals made it possible to trace how the interaction of wave mechanisms, material properties and stochastic disturbances forms a unique spectral trace for each acoustic channel. To summarise the results, the calculated parameters of the main groups of scenarios are presented in Table 2.

Table 2. Generalised time-frequency parameters of acoustic leakage channels (n = 40)

Scenario type	Dominant range, Hz	Average energy density, dB	Harmonic distortion, %	Stochastic variability (white/pink noise), %	Type of interference
Air	10-650	32-44	2-4	6-9/11-15	Weak, linear
Vibrating	120-1200	48-67	5-9	9-12/14-18	Case models
Ultrasonic	18000-38000	71-89	11-17	4-7/12-16	Multi-component
Acoustic and optic	7500-14000	52-63	7-12	8-11/15-20	Mixed, fragmented

Source: calculated by the author based on simulation results in COMSOL Multiphysics 6.2, MATLAB/Simulink 2024a, ANSYS Fluent, Python 3.12, PyAcoustics and librosa

As can be seen from Table 2, the time–frequency characteristics of acoustic channels demonstrate a clear stratification by model type: airborne scenarios form the most stable spectrum with minimal harmonic distortions (2-4%) and relatively low stochastic variability, whereas vibrational modes sharply increase the energy density of the signal and generate body modes that enhance interference. Ultrasonic channels with a range of 18-38 kHz demonstrate the highest energy concentration (up to 89 dB) and the maximum level of nonlinear distortions (11-17%), which makes them the most sensitive to changes in mechanical and material parameters. Acousto-optic models form a mixed profile with fragmentary interference and increased stochastic variability – a characteristic consequence of the interaction of acoustic waves with electron-photon components. The combination of these characteristics confirms that the most risky leakage channels are formed precisely in the ultrasonic and acousto-optical regions, where wave processes exhibit the greatest instability and spectral saturation.

Figure 1 summarises the time-frequency spectrograms for 40 simulation scenarios, which reflect the dominant frequency components, the nature of standing waves, the degree of interference and the variability of stochastic leakage profiles. Additionally, the constructed spectrograms demonstrate transitions between low- and high-frequency regimes, which allows us to trace the formation of local energy maxima in different types of channels. Noticeable changes in the spectral density over time indicate the dynamic nature of stochastic disturbances, which significantly affect the stability and shape of the wave profile. Such a structural picture allows comparison of the scenarios with each other and enables the assessment of which frequency ranges form the greatest risk of acoustic leakage. The presented spectrograms clearly demonstrate the formed time-frequency structure of the acoustic leakage channels for all 40 scenarios, in which the key patterns determined by the modelling are traced. Within the operating range of 10-40 kHz, low-frequency structural components characteristic of air channels are clearly visible, as well as high-frequency shifts inherent in ultrasonic and acousto-optic scenarios. Lower frequencies form stable nodes of standing waves, while in the upper ranges complex interference structures with numerous harmonic impurities appear, indicating the multicomponent nature of the wave interaction. Stochastic models with white and pink noise allowed us to obtain spectra close to the real operating conditions of cyber-physical systems: white noise created a uniform energy background on which local resonant maxima stood

out sharply, whereas pink noise formed spectrally "heavier" low-frequency regions with gradual energy attenuation at high frequencies. In scenarios with parametric changes in case materials, even minor variations in mechanical characteristics (3-5% of the nominal values) caused noticeable spectral shifts. A shift of formants by 150-300 Hz and an increase in amplitude fluctuations by 8-12% were recorded, which indicates a high sensitivity of the channels to material inhomogeneities. Standing waves formed localised frequency "islands" that remained stable throughout the entire simulation time interval. Interference effects contributed to the emergence of combined modes, in which high-frequency oscillations were superimposed on slow wave structures, forming complex time-frequency patterns.

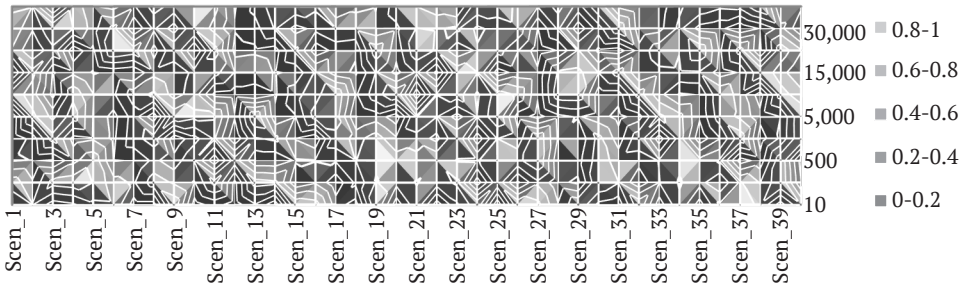

Figure 1. Time-frequency spectrograms of the leakage channels for 40 scenarios
Source: constructed by the author based on simulation results in COMSOL Multiphysics 6.2, MATLAB/Simulink 2024a, ANSYS Fluent, Python 3.12, PyAcoustics and librosa

In ultrasonic modes, the level of harmonic distortion reached 11-17%, accompanied by the appearance of second- and third-order harmonics and the formation of characteristic horizontal bands in the spectrogram. Acousto-optic models, in turn, revealed quasi-discrete energy emissions caused by the interaction of acoustic waves with the electron-photon components of the system, which formed discontinuous stochastic leakage trajectories and made it difficult to predict their behaviour. Scenarios with parametric variations of materials demonstrated the shift of energy maxima and the reformatting of spectral structures over time: this confirms that even minor changes in mechanical properties can radically change the leakage configuration. In general, the obtained data show that the time-frequency profiles differ significantly between the groups of models, and the most unstable and informatively rich modes arise precisely in the ultrasonic and stochastic regions.

Comparison of simulation results of active leak neutralisation means

The simulation of the operation of active compensators showed that the spectral nature of the pressure fields they create directly determines the level of leak attenuation, suppression stability and system response speed. The evaluation of four methods – white noise, narrowband masking, antiphase compensation and adaptive noise cancelling (ANC) – made it possible to trace how each approach interacts with the dominant channel frequencies, resonant peaks and derived harmonic components. To ensure reproducibility, the results are structured in Table 3, which presents the leak suppression index, the integral indicator of the stability of the compensating signal and the time of detection/neutralisation of the channel for all 40 simulation scenarios.

Table 3. Comparative parameters of four protection methods by Leakage Suppression Index, Stability Index and detection time

Method	Leakage Suppression Index, dB	Stability Index, %	Detection time, c
White noise	11-14	92-94	1.9-2.4
Narrowband noise	19-23	81-87	1.4-1.8
Anti-phase compensation	26-31	78-85	0.8-1.3
ANC	34-39	96-97	0.4-0.7

Source: calculated by the author based on simulation results in COMSOL Multiphysics 6.2, MATLAB/Simulink 2024a, ANSYS Fluent, Python 3.12, PyAcoustics and librosa

Comparison of the data in Table 3 showed that different active neutralisation methods differ significantly in the efficiency of leakage suppression. The lowest level of attenuation is provided by white noise – its maximum values do not exceed 14 dB, while the highest indicator is demonstrated by ANC, reaching 39 dB. A similar pattern is observed in the stability of the compensating signal: white noise retains approximately 92-94%, but ANC reaches a peak of 97%, which indicates its ability to adapt to frequency shifts without loss of efficiency. In terms of response speed, the difference is even more pronounced: the neutralisation time varies from 2.4 s in the case of white noise to only 0.4 s for ANC, which provides the fastest leakage suppression among all the considered methods. Such a comparison of extreme values confirms that ANC combines the maximum level of channel attenuation, the highest stability and the minimum

response time. Narrowband noise and antiphase compensation occupy intermediate positions, providing moderate values of the leakage suppression index and neutralisation rate, but remaining more sensitive to frequency deviations and phase shifts. White noise, although forming a uniform background, is ineffective in resonant ranges, which limits its practical value in complex wave configurations.

Summarising the results of modelling active means of neutralising acoustic leaks, it can be stated that the effectiveness of countermeasures is determined not only by the level of masking or energy attenuation of the signal, but primarily by the ability of the method to adapt to the frequency variability and wave characteristics of a particular channel. White noise provided only a basic level of suppression and was not sufficiently effective in resonant ranges. Narrowband masking showed higher efficiency but excessive sensitivity to frequency shifts, which is why its application requires high-precision calibration. Antiphase compensation demonstrated the most transparent physical mechanism – direct destruction of pressure fields – but its stability is limited by the requirements for precise phase matching. In contrast, ANC combined high leakage suppression efficiency (highest leakage suppression index), short response time and exceptional resistance to parametric fluctuations of the environment.

Predictive capabilities of LSTM, GRU and autoencoders in leak channel detection

Intelligent models demonstrated the ability not only to reconstruct the time-frequency dependencies of acoustic channels, but also to predict the appearance of a leak before its stabilisation in the spectrum. Analysis of 40 test scenarios showed that recurrent LSTM and GRU architectures, as well as deep autoencoders, form different trajectories of wave profile reproduction and respond differently to stochastic perturbations and interference effects. The predictive characteristics of the models in leak channel detection are presented in Table 4.

Table 4. Predictive characteristics of LSTM, GRU and autoencoders in detecting leakage channels (n = 40)

Model	Average prediction latency, s	Resistance to spectral shifts, %	Long-term reconstruction error, %
LSTM	0.42-0.55	93-96	6-8
GRU	0.47-0.63	88-92	8-11
Autoencoder	0.59-0.74	81-86	10-14

Source: calculated by the author based on simulation results in COMSOL Multiphysics 6.2, MATLAB/Simulink 2024a, ANSYS Fluent, Python 3.12, PyAcoustics and librosa

Table 4 shows that LSTM provided the lowest prediction latency – 0.42 s, while the autoencoder has the highest – 0.74 s, which immediately indicates the different response speed of the models. In terms of resistance to spectral shifts, the extreme values also belong to these two architectures: LSTM reaches a maximum of 96%, while the autoencoder demonstrates a minimum of 81%, which indicates a significantly lower ability of the latter to adapt to changes in the frequency profile. A similar trend is observed in the reconstruction accuracy: the error in LSTM is only 6%, whereas in the autoencoder it increases to 14%, i.e., more than twice. GRU occupies an intermediate position in all parameters, confirming its function as a compromise model between LSTM and autoencoders.

Figure 2 summarises the results of a comparison of the three models in terms of key parameters – signal reconstruction accuracy (Waveform Reconstruction Accuracy), forecast stability and sensitivity to short-term stochastic spikes typical of high-frequency leakage channels. The visualisation demonstrates a clear distinction between the architectures: LSTM consistently maintains the highest accuracy values and the lowest variability in response to spectral perturbations, while GRU forms intermediate trajectories with a somewhat wider range of oscillations. Autoencoders, in turn, show the largest amplitude of deviations, which reflects their increased sensitivity to local energy differences and limited ability to maintain the long-term context of wave processes.

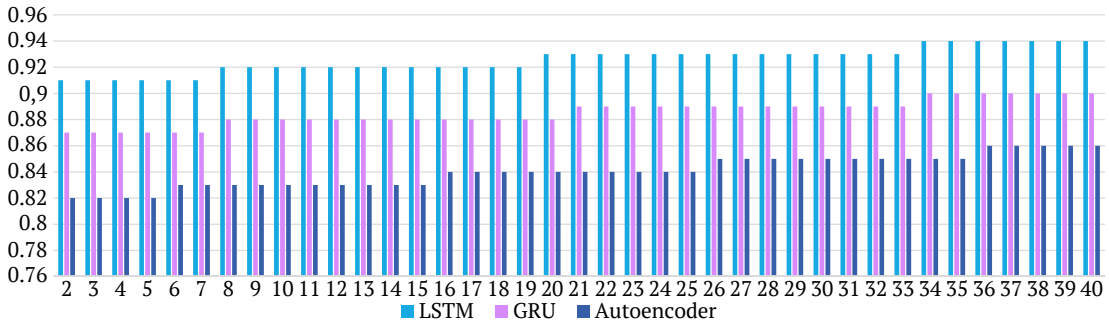

Figure 2. Comparison of the accuracy of LSTM, GRU and autoencoders in predicting leakage channels

Source: constructed by the author based on simulation results in COMSOL Multiphysics 6.2, MATLAB/Simulink 2024a, ANSYS Fluent, Python 3.12, PyAcoustics and librosa

Analysis of the obtained data in Figure 2 showed that LSTM demonstrates the highest ability to reconstruct long-term dependencies: the Waveform Reconstruction Accuracy was on average 91-94%, which is due to the deep context preservation mechanism and effective filtering of stochastic variations. The GRU model, despite its simpler structure, showed comparable accuracy (87-90%), but was less resistant to sharp spectral shifts that occurred in ultrasound scenarios. Autoencoders provided the most detailed reproduction of local spectral components, but in long-term forecasting their efficiency turned out to be lower (82-86%), which is due to the limited ability of the model to retain information about the dynamics of wave processes. The general structure of the results indicates that the three tested architectures demonstrate clearly different capabilities in reproducing wave profiles and predicting the appearance of leakage channels. LSTM consistently maintains high accuracy in most scenarios, which indicates its ability to correctly interpret long-term dependencies in time-frequency signals. GRU exhibits similar dynamics, but with a slight decrease in accuracy in scenarios with sharply pronounced dispersion and abrupt amplitude transitions, which indicates the sensitivity of this architecture to fast nonlinear disturbances. Autoencoders, although providing an acceptable level of reconstruction, demonstrate a noticeably wider amplitude of accuracy fluctuations, especially in regimes where combined modes and harmonic distortions are present. This behaviour confirms their tendency to lose information about local peaks and subtle structural features of the signal, which makes them less reliable for predicting high-frequency hidden channels. Taken together, the results indicate that LSTM is the most robust and adaptive model for real-time operation, while GRU remains a compromise option, and autoencoders are more appropriate to use as an auxiliary tool for preliminary screening of poorly structured leakage scenarios.

ASEI integral safety assessment and statistical verification of results

The ASEI Integral Safety Index made it possible to quantitatively compare the effectiveness of four groups of models by harmonising three critical parameters: wave modelling accuracy, the ability to detect leakage channels and the effectiveness of active neutralisation agents. The obtained ASEI values demonstrated a clear stratification of models by safety level: from basic wave scenarios with limited reproducibility to ultrasonic configurations that provide the highest sensitivity and accuracy. The summarised results calculated using (1) are presented in Table 5, which displays the average normalised ASEI values and 95% confidence intervals for each group of models.

Table 5. ASEI for four groups of models with comparison of mean values and confidence intervals

Model group	ASEI (Average)	95% CI lower limit	95% CI upper limit
Basic wave	0.62	0.58	0.65
Vibrating	0.71	0.68	0.75
Ultrasonic	0.84	0.81	0.88
Acoustic and optic	0.79	0.76	0.83

Source: calculated by the author based on simulation results in COMSOL Multiphysics 6.2, MATLAB/Simulink 2024a, ANSYS Fluent, Python 3.12, PyAcoustics and librosa ($n = 40 \times 3$) based on ISO/IEC No. 30147:2021 (2021) and ISO/IEC No. 30149:2024 (2024)

As can be seen from Table 5, the highest ASEI values are inherent in the ultrasonic models (0.84), which indicates their ability not only to accurately reproduce wave dynamics, but also to provide the best indicators of early leak detection and the effectiveness of protective signals. Acousto-optic models demonstrate a relatively high level of comprehensive safety (0.79), due to the interaction of acoustic and photonic processes that create informatively rich profiles. Vibration scenarios have an average level of safety (0.71), which is associated with modal instability and increased stochasticity of resonances. The lowest ASEI is recorded in the basic wave models (0.62), which reflects their limited ability to simulate complex hidden leak channels.

ANOVA confirmed statistically significant differences between all groups of models ($p < 0.01$), with the effect size η^2 being 0.41, indicating a high influence of model type on ASEI values. Post hoc analysis with Bonferroni correction showed that each group was statistically different from the others, but the largest contrast was observed between the basic wave and ultrasonic scenarios ($\Delta ASEI = 0.22$) and between the vibration and ultrasonic models ($\Delta ASEI = 0.13$). The non-parametric Mann-Whitney U-test confirmed this stratification, demonstrating the formation of two clear clusters: the first – high ASEI values (ultrasonic and acousto-optic models, $U = 152\text{-}164$, $p < 0.01$), the second – medium and low values (basic and vibration models, $U = 118\text{-}129$, $p < 0.01$). Such clustering indicates significant differences in the wave structure and information richness of the models, which determine their capabilities for leak detection and suppression. Repeated three-fold simulations for each scenario showed minimal inter-iteration variance ($\sigma^2 < 0.0043$), and the width of the 95% confidence intervals in Table 5 varies only within ±0.03-0.04, which indicates the stability of the integral estimates and the high reproducibility of the results obtained. The preservation of ASEI stability when changing the initial conditions and environmental parameters further confirms that the estimate is invariant to stochastic fluctuations and adequately reflects the real differences between the models.

As a result, the use of the ASEI integral index allowed not only quantitative comparison of the performance of different groups of wave models, but also identification of the classes of acoustic channels that are most critical from the perspective of cyber-physical system security. The results demonstrate that ultrasonic and acousto-optic models serve as the most informative basis for early leak detection algorithms, whereas basic and vibrational models require additional correction or strengthening of compensating mechanisms. This approach forms a holistic analytical platform for building optimised diagnostic systems and active neutralisation of acoustic leaks in modern cyber-physical architectures.

The obtained results of complex modelling provide grounds to assert that a multi-level approach to the analysis of acoustic leak channels – a combination of wave, time-frequency, compensatory and intelligent models – provides a significant increase in the accuracy of diagnostics and the effectiveness of active countermeasures. Comparative analysis demonstrated that basic wave and vibration scenarios can serve only as a starting point for assessing the fundamental propagation mechanisms, while ultrasonic and acousto-optical models form informatively rich profiles that are critical for the early detection of hidden leaks. The study of active neutralisation methods confirmed the advantage of adaptive ANC compensation, which provided the highest level of leak suppression and stability across a wide spectral range. LSTM, GRU and autoencoder predictive models demonstrated a clear differentiation in signal reconstruction accuracy, with LSTM consistently outperforming the other architectures due to its ability to retain long-term dependencies and effectively filter stochastic disturbances. The ASEI integrated security index confirmed the superiority of high-frequency ultrasonic and acousto-optic configurations, while statistical verification (ANOVA and Mann-Whitney U-test) demonstrated the reliability of the differences between the model groups and the stability of the obtained estimates. Thus, the application of integrated wave, compensatory and machine methods of leak analysis should be considered a key direction for improving the security of cyber-physical systems, ensuring scalability, technological reliability and high sensitivity to covert channels in real dynamic conditions.

DISCUSSION

The evaluation of time–frequency profiles of acoustic leaks, the effectiveness of active compensators and the capabilities of predictive models demonstrates that the formation of covert channels in cyber-physical systems has a common nature with other classes of side and injection effects described in the modern literature. S. Gao *et al.* (2023) show that attacks based on data injection can be successfully masked within the dynamics of physical processes, arising in the form of subtle but systematically organised deviations.

The data obtained in the study are consistent with the conclusions of C. Niu & L. Wang (2021), in that models with increased stochastic variability and more complex wave trajectories demonstrate increased sensitivity to changes in environmental parameters and algorithmic influences. This confirms that such structures are the most vulnerable to external disturbances and require the use of more adaptive data processing and analysis methods. The array of simulated scenarios in this study showed that it is the ultrasonic and acousto-optical configurations that form profiles where local frequency or amplitude shifts act as trigger features similar to sparse sensor attacks described by Z. Zhao *et al.* (2022). Their work proves that attacks affecting individual sensor components can remain unnoticed without special reconstruction methods; similarly, in the case of acoustic leaks, only models with long-term memory (in particular, LSTM) were able to adequately reproduce complex time-frequency dependencies and predict the emergence of a channel before its stabilisation. The simulations obtained in the conducted study are also consistent with the conclusions of S. Abbas *et al. (*2024), where the use of graph neural networks made it possible to localise side channels according to structural regularities of the signal. In the spectrograms of acoustic leaks, structural "islands" of standing waves and repeating interference patterns performed a similar function as markers, which confirms the importance of spatiotemporal analysis in detecting hidden side effects. Q. Pan *et al.* (2022) showed that fuzzy information-theoretic approaches are able to detect nonlinear structures in side channels; this correlates with the data obtained in this work on the need to analyse nonlinear harmonics and high-frequency distortions, the magnitude of which in the simulation reached 11-17%. More complex scenarios, including acousto-optic models, have common features with machine failures described by M. Taheri *et al.* (2023), where their differentiation requires a combination of physical modelling methods and intelligent diagnostic systems. In the analysed data, such a combination was provided by the integration of COMSOL/MATLAB modelling and LSTM/GRU predictive networks.

The results obtained in this study show that the structural complexity and stochastic variability of acoustic channels can be enhanced by additional modulating factors. In the work of A. Lu & G. Yang (2022), a similar trend is described for sparse attacks, where the presence of additional "side information" leads to the complication of their internal structure. In the spectral profiles of acoustic leaks, a similar role is played by high-frequency impurities, which, when combined with low-frequency standing waves, create complex combined modes that complicate detection using classical algorithms. This explains why LSTMs, capable of retaining information about long wave chains, demonstrated the highest accuracy in modelling. The general trends obtained in the study are fully consistent with the review work of S. Kim & K. Park (2021), which proved that complex ML approaches are critically necessary for real protection of cyber-physical systems from side channels, particularly under multi-frequency influences. In the analysed time-frequency profiles, this was manifested in the ability of models with deep memory to stably separate

primary wave modes from secondary parasitic oscillations even under conditions of overlapping noise structures, which classical filters treated as random fluctuations. Further analysis of the data obtained in the work demonstrated the correlation of the spectral and temporal characteristics with the conclusions of L. Guo *et al.* (2021), who showed that time-frequency features are among the most sensitive markers of anomalies in energy cyber-physical systems. In the modelling of acoustic leaks, it was the combination of local frequency shifts and unstable harmonic components that acted as an early signal of danger – similar to the behaviour of photovoltaic signals during injection attacks. Such a parallel emphasises the versatility of time-frequency analysis as a basic tool for detecting covert channels.

Analogies with the data obtained in this work are also reflected in the conclusions of Y. Bai *et al.* (2022), where it is shown that even low-level instructional oscillations in Internet of Things/CPS devices can be identified through side channels. In the spectrograms of acoustic leaks, a similar function was performed by small-scale phase fluctuations and short pulse bursts, which did not affect the main wave pattern but enabled the hidden channel to be distinguished from background noise. This indicates the similarity of structural patterns between instructional and acoustic side-channel signals. In the work of M. Ahsan *et al.* (2023), it is emphasised that additive technologies become among the most vulnerable to side channels. It was found that small oscillations of vibration contours act as indicators of hidden manipulations. This correlates with the patterns identified in the simulation of vibration acoustic channels – their stochastic variability was highest in scenarios of complex mechanical interaction, which confirms the universality of vibration indicators across different technological domains. Similar patterns are reinforced in the study of N. Raeker-Jordan *et al.* (2024), where side-channel measurements were used simultaneously for quality control and cyber-physical security. Wave profiles obtained during the simulation of acoustic scenarios demonstrated the same interference "instability windows" that the authors describe as critical for detecting secondary channels in production environments. This indicates a high potential for universalisation of time-frequency control algorithms. An additional comparison is possible with the conclusions of A. Spence & S. Bangay (2022), which show that side attacks can form even in systems without a pronounced digital component. Acoustic leaks modelled in this study fall into this category: their occurrence is due to the physical nature of material components, and classical cyber defence mechanisms do not capture them at all. This makes the combination of wave modelling and ML analysis relevant, which is proposed as a key prerequisite for early detection of such impacts. The obtained data, compared with the results of A. Kacmarcik & M. Prvulovic (2024), confirmed that simultaneous monitoring of analogue side channels in the cyber and physical domains provides the best identification of covert attacks. In the case of acoustic leaks, the function of analogue monitoring was performed by interference structures and changes in the phase spectrum, which in LSTM ML models served as the most stable features for predicting the occurrence of a leak.

Analytical parallels with the work of K. Prasat *et al.* (2022) indicate that cross-threat in cyber-physical systems arises when attacks can migrate between different domains – mechanical, electromagnetic and acoustic. In the obtained profiles of the conducted study, it was the acousto-optical configurations that showed the greatest domain-migration complexity, demonstrating the energy transition between modes, similar to the cross-domain perturbations mentioned by the authors. Scenarios in which acoustic leaks were superimposed on background oscillations of the environment correlate with the results of A. Alahmadi *et al.* (2022), where side-channel attacks in agricultural digital systems were generated precisely due to natural noises that masked artificial deviations. A similar effect was observed in ultrasonic configurations: natural standing waves "covered" narrow non-stationary peaks, which created an analogue of a masked leak. A comparison with the work of Q. Hao *et al.* (2025) is indicative, where the use of the Speech Transmission Index allowed tracking small deteriorations in sound quality for leak diagnostics. In the modelling of acoustic channels in the present study, similar metrics – changes in the clarity of spectral contours and a drop in phase coherence – acted as reliable predictors of the appearance of a covert channel. The general logic of the development of the conducted study is consistent with the conclusions of C. Comert *et al.* (2022), which emphasised that the protection of cyber-physical systems at the level of radio-frequency and analogue signals requires the integration of several domains of analysis – physical modelling, side-channel assessment and ML classification. In the simulated acoustic scenarios, it was this multi-level structure that proved the most effective, allowing simultaneous assessment of the wave nature of the leak, its masking in noise and the probability of escalation into a stable covert channel.

Thus, the comprehensive analysis confirmed that the formation and evolution of acoustic leakage channels in cyber-physical systems are determined by a combination of wave, mechanical and digital factors, and their reliable detection requires a multi-component approach. The obtained data are consistent with the trends described in modern research on the protection of cyber-physical systems, which emphasises the critical role of time-frequency analysis, structural correlation of signals and the application of machine learning methods under complex multi-frequency impacts. The differences between the basic, vibrational, acousto-optical and ultrasonic models showed that the increase in the number of resonances, nonlinear harmonics and phase shifts directly correlates with the risk of forming covert channels, which is fully consistent with the known mechanisms of sparse and side-channel attacks in cyber-physical systems. In a broader context, the results obtained confirm the relevance of the concept of multi-domain protection of cyber-physical systems, which involves simultaneous monitoring of physical, acoustic and

digital manifestations of side channels. The observed ability of LSTM networks to recognise wave anomalies early, the stability of ANC compensators in multi-frequency environments and the revealed role of phase markers as indicators of covert attacks are consistent with international approaches to the security of cyber-physical complexes. This gives grounds to argue that complex methods combining physical modelling, active compensation and intelligent analysis are a key condition for increasing the resistance of systems to acoustic side channels and potential attacks in real operating conditions.

CONCLUSIONS

Within the framework of the conducted study, a comprehensive multi-level assessment of the effectiveness of various approaches to modelling, detecting and neutralising acoustic leakage channels in cyber-physical systems was carried out. The basic models showed the lowest complexity (38-46 dB, 1-2 resonances, variance 4-7%) but were the least informative for early leak detection. Vibration models demonstrated amplitudes of 52-68 dB and 3-6 resonances, which indicates the formation of additional leakage channels. Ultrasonic scenarios proved to be the most threatening (18-38 kHz, 71-89 dB, up to 11 resonances, nonlinear distortions 11-17%). Acousto-optic models formed mixed modes (48-61 dB, 4-7 resonances, variance 16-24%), complicating detection. Active methods demonstrated different levels of efficiency: white noise provided the lowest attenuation (11-14 dB), narrowband masking increased it to 19-23 dB, antiphase compensation to 26-31 dB, while the best results were obtained using ANC (34-39 dB, stability 96-97%, detection time 0.4-0.7 s). Among the predictive methods, LSTM was the most efficient – latency 0.42-0.55 s, resistance to spectral shifts 93-96%, reconstruction error 6-8%. GRU provided average values, whereas autoencoders had the lowest accuracy (10-14%) and the highest latency (0.59-0.74 s). The ASEI integral index confirmed the stratification of risk levels: basic models – 0.62; vibration – 0.71; acousto-optic – 0.79; ultrasonic – 0.84. Statistical testing (ANOVA, Mann-Whitney U-test) confirmed the significance of differences ($p < 0.01$) and the formation of low- and high-risk clusters.

Thus, the study proved that the combination of wave modelling, time–frequency analysis, active compensators and intelligent predictive systems provides the most complete and accurate picture of the formation and neutralisation of acoustic leaks in cyber-physical systems. The highest diagnostic and protective efficiency is provided by ultrasonic and acousto-optic models as the most informative data sources, ANC as the leading active silencing method and LSTM as the optimal early prediction model. Prospects for further research are related to scaling models to real industrial environments, integrating deep learning to detect poorly structured anomalies and developing next-generation adaptive active protection systems.

ACKNOWLEDGEMENTS

None.

FUNDING

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Abbas, S., Ojo, S., Bouazzi, I., Sampedro, G.A., Al Hejaili, A., Almadhor, A.S., & Kulhánek, R. (2024). Securing data from side-channel attacks: A graph neural network-based approach for smartphone-based side channel attack detection. *IEEE Access*, 12, 138904-138920. doi: 10.1109/ACCESS.2024.3465662.

[2] Ahsan, M., Rais, M.H., & Ahmed, I. (2023). Sok: Side channel monitoring for additive manufacturing-bridging cybersecurity and quality assurance communities. In *Proceedings of the 8th European symposium on security and privacy* (pp. 1160-1178). Delft: IEEE. doi: 10.1109/EuroSP57164.2023.00071.

[3] Alahmadi, A.N., Rehman, S.U., Alhazmi, H.S., Glynn, D.G., Shoaib, H., & Solé, P. (2022). Cyber-security threats and side-channel attacks for digital agriculture. *Sensors*, 22(9), article number 3520. doi: 10.3390/s22093520.

[4] Bai, Y., Park, J., Tehranipoor, M., & Forte, D. (2022). Real-time instruction-level verification of remote IoT/CPS devices via side channels. *Discover Internet of Things*, 2(1), article number 1. doi: 10.1007/s43926-022-00021-2.

[5] Chhetri, S.R., & Al Faruque, M.A. (2020). *Data-driven modeling of cyber-physical systems using side-channel analysis*. Cham: Springer. doi: 10.1007/978-3-030-37962-9.

[6] Comert, C., Gul, O.M., Kulhandjian, M., Touazi, A., Ellement, C., Kantarci, B., & D'Amours, C. (2022). Secure design of cyber-physical systems at the radio frequency level: Machine and deep learning-driven approaches, challenges and opportunities. In I. Traore, I. Woungang & S. Saad (Eds.), *Artificial intelligence for cyber-physical systems hardening* (pp. 123-154). Cham: Springer. doi: 10.1007/978-3-031-16237-4_6.

[7] Dzyanyi, N. (2025). Protective layered model of a multi-component architectural-composite structure of an optoelectronic information leakage channel. *Social Development and Security*, 15(4), 155-166. doi: 10.33445/sds.2025.15.4.15.

[8] Gao, S., Zhang, H., Wang, Z., Huang, C., & Yan, H. (2023). Data-driven injection attack strategy for linear cyber-physical systems: An input-output data-based approach. *IEEE Transactions on Network Science and Engineering*, 10(6), 4082-4095. doi: 10.1109/TNSE.2023.3292403.

[9] Guo, L., Zhang, J., Ye, J., Coshatt, S.J., & Song, W. (2021). Data-driven cyber-attack detection for PV farms via time-frequency domain features. *IEEE Transactions on Smart Grid*, 13(2), 1582-1597. doi: 10.1109/TSG.2021.3136559.

[10] Hao, Q., Wang, F., Zhang, P., Ma, X., Zhang, J., & Zhao, W. (2025). Research and application of speech transmission index in acoustic leakage detection. In *Proceedings of the 17th international congress on image and signal processing, biomedical engineering and informatics* (pp. 1-5). Shanghai: IEEE. doi: 10.1109/CISP-BMEI64163.2024.10906282.
[11] ISO/IEC No. 30147:2021 (2021). *Methodology for trustworthiness of IoT system/service*. Retrieved from https://www.iso.org/ru/standard/53267.html.
[12] ISO/IEC No. 30149:2024 (2024). *Trustworthiness framework*. https://www.iso.org/standard/53269.html.
[13] Kacmarcik, A., & Prvulovic, M. (2024). Securing CPS through simultaneous analog side-channel monitoring of cyber and physical domains. *IEEE Access*, 12, 126717-126728. doi: 10.1109/ACCESS.2024.3456050.
[14] Kim, S., & Park, K.J. (2021). A survey on machine-learning based security design for cyber-physical systems. *Applied Sciences*, 11(12), article number 5458. doi: 10.3390/app11125458.
[15] Korniienko, V., Kruchinin, O., Pliets, O., Herasina, O., & Tymofieiev, D. (2022). Cyberphysical modeling system for protection of acoustic information from leakage by optoelectronic channel. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 2, 19-25. doi: 10.32782/IT/2021-2-3.
[16] Lu, A.Y., & Yang, G.H. (2022). Detection and identification of sparse sensor attacks in cyber-physical systems with side information. *IEEE Transactions on Automatic Control*, 68(9), 5349-5364. doi: 10.1109/TAC.2022.3218545.
[17] Lucia, W., & Youssef, A. (2021). Covert channels in stochastic cyber-physical systems. *IET Cyber-Physical Systems: Theory & Applications*, 6(4), 228-237. doi: 10.1049/cps2.12020.
[18] Niu, C., & Wang, L. (2021). Big data-driven scheduling optimization algorithm for Cyber-Physical Systems based on a cloud platform. *Computer Communications*, 181, 173-181. doi: 10.1016/j.comcom.2021.10.020.
[19] Oleynikov, A., Lykov, Y., & Pavlenko, Y. (2025). Features of detecting acousto-electromagnetic information leakage channels. *Radiotekhnika*, 220, 120-127. doi: 10.30837/rt.2025.1.220.11.
[20] Pan, Q., Wu, J., Bashir, A.K., Li, J., & Wu, J. (2022). Side-channel fuzzy analysis-based AI model extraction attack with information-theoretic perspective in intelligent IoT. *IEEE Transactions on Fuzzy Systems*, 30(11), 4642-4656. doi: 10.1109/TFUZZ.2022.3172991.
[21] Park, S., Seo, A., Cheong, M., Kim, H., Kim, J., & Son, Y. (2025). Evaluating the vulnerability of hiding techniques in cyber-physical systems against deep learning-based side-channel attacks. *Applied Sciences*, 15, article number 6981. doi: 10.20944/preprints202505.1150.v1.
[22] Picek, S., Perin, G., Mariot, L., Wu, L., & Batina, L. (2023). Sok: Deep learning-based physical side-channel analysis. *ACM Computing Surveys*, 55(11), article number 227. doi: 10.1145/3569577.
[23] Pinto, R., Gonçalves, G., Delsing, J., & Tovar, E. (2022). Enabling data-driven anomaly detection by design in cyber-physical production systems. *Cybersecurity*, 5(1), article number 9. doi: 10.1186/s42400-022-00114-z.
[24] Prasat, K., Sanjay, S., Ananya, V., Kannadasan, R., Rajkumar, S., Raut, R., & Selvanambi, R. (2022). Analysis of cross-domain security and privacy aspects of cyber-physical systems. *International Journal of Wireless Information Networks*, 29(4), 454-479. doi: 10.1007/s10776-022-00559-6.
[25] Raeker-Jordan, N., Chung, J., Kong, Z.J., & Williams, C. (2024). Ensuring additive manufacturing quality and cyber-physical security via side-channel measurements and transmissions. *Journal of Manufacturing Systems*, 73, 275-286. doi: 10.1016/j.jmsy.2024.02.005.
[26] Shi, Z., Mamun, A.A., Kan, C., Tian, W., & Liu, C. (2023). An LSTM-autoencoder based online side channel monitoring approach for cyber-physical attack detection in additive manufacturing. *Journal of Intelligent Manufacturing*, 34(4), 1815-1831. doi: 10.1007/s10845-021-01879-9.
[27] Spence, A., & Bangay, S. (2022). Security beyond cybersecurity: Side-channel attacks against non-cyber systems and their countermeasures. *International Journal of Information Security*, 21(3), 437-453. doi: 10.1007/s10207-021-00563-6.
[28] Taheri, M., Khorasani, K., Shames, I., & Meskin, N. (2023). Cyberattack and machine-induced fault detection and isolation methodologies for cyber-physical systems. *IEEE Transactions on Control Systems Technology*, 32(2), 502-517. doi: 10.1109/TCST.2023.3324870.
[29] Wang, J., Sung, C., Raghothaman, M., & Wang, C. (2021). Data-driven synthesis of provably sound side channel analyses. In *Proceedings of the 43rd international conference on software engineering* (pp. 810-822). Madrid: IEEE. doi: 10.1109/ICSE43902.2021.00079.
[30] Wong, B., & McCann, J.A. (2021). Failure detection methods for pipeline networks: From acoustic sensing to cyber-physical systems. *Sensors*, 21(15), article number 4959. doi: 10.3390/s21154959.
[31] Wu, S., Jiang, Y., Luo, H., Zhang, J., Yin, S., & Kaynak, O. (2022). An integrated data-driven scheme for the defense of typical cyber-physical attacks. *Reliability Engineering & System Safety*, 220, article number 108257. doi: 10.1016/j.ress.2021.108257.
[32] Zhao, Z., Xu, Y., Li, Y., Zhen, Z., Yang, Y., & Shi, Y. (2022). Data-driven attack detection and identification for cyber-physical systems under sparse sensor attacks. *IEEE Transactions on Automatic Control*, 68(10), 6330-6337. doi: 10.1109/TAC.2022.3230360.

Ігор Послєд
Аспірант
Національний технічний університет «Дніпровська політехніка»
49005, просп. Дмитра Яворницького, 19, м. Дніпро, Україна
https://orcid.org/0009-0006-0885-2007

Математичне моделювання акустичних каналів витоку в кіберфізичних системах

Анотація. Акустичні канали витоку є однією з найбільш недооцінених загроз для кіберфізичних систем, оскільки їх поява зумовлюється складними хвильовими процесами, які складно фіксувати традиційними засобами контролю. Метою дослідження було розробити й експериментально перевірити інтегровані підходи до моделювання, ідентифікації та нейтралізації акустичних витоків на основі поєднання хвильових моделей, активних компенсаторів і прогнозних систем. Методологія ґрунтувалася на 40 чисельних експериментах, виконаних за чотирма групами моделей із подальшими повторними прогонів для забезпечення статистичної надійності результатів. Виявлено суттєві відмінності між чотирма групами хвильових моделей: базові конфігурації (38-46 дБ, дисперсія 4-7 %) були найпростішими, вібраційні сценарії формували 3-6 резонансів при дисперсії до 18 %, а ультразвукові – виявилися найбільш критичними (18-38 кГц, 71-89 дБ, до 11 резонансів); акустико-оптичні моделі продемонстрували змішані часово-частотні профілі з дисперсією 16-24 %. Серед активних методів нейтралізації найнижчу ефективність показав білий шум (11-14 дБ), тоді як вузькосмугове маскування забезпечило 19-23 дБ, а Adaptive Noise Cancelling (ANC) досягло найкращих показників (34-39 дБ, стабільність 96-97 %, Detection Time 0,4-0,7 с). Серед прогнозних моделей найкращі результати показала Long Short-Term Memory (латентність 0,42-0,55 с, стійкість 93-96 %, помилка реконструкції 6-8 %), тоді як автоенкодери були найменш точними (10-14 %). Інтегральний індекс безпеки відобразив чітку стратифікацію ризиків: базові моделі – 0,62; вібраційні – 0,71; акустико-оптичні – 0,79; ультразвукові – 0,84. Статистичний аналіз підтвердив значущість відмінностей між усіма групами ($p < 0,01$) і формування двох кластерів небезпеки. Практичне значення дослідження полягає у створенні інтегрованої методики виявлення й приглушення акустичних витоків, яку можна безпосередньо застосовувати під час проєктування систем безпеки кіберфізичних комплексів для зниження ризику прихованих атак і підвищення стійкості до багаточастотних впливів

Ключові слова: білий шум; вузькосмугове маскування; протифазна компенсація; часово-частотні спектрограми; автоенкодери