Cybersecurity in Intelligent Transport Systems: Current Challenges and Solutions*

Iryna Mashkina[1,†], Svitlana Rzaieva[1,†], Yuliia Kostiuk[1,†], Nataliia Mazur[1,*,†] and Zoreslava Brzhevska[1,†]

[1] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine*

Abstract

The paper discusses the current cybersecurity challenges in intelligent transport systems (ITS), in particular, the growing number of IoT devices, the need to process large amounts of data, and vulnerability to DDoS attacks. One of the key approaches to ensuring cybersecurity is the use of mathematical models for risk assessment. The paper analyses the use of mathematical models for risk assessment and prediction of attacks and anomalies based on historical data and current observations. The risks are modeled using the exponential distribution and the Weibull distribution, which allow assessing the dynamics of threats over time, taking into account the accumulation of vulnerabilities and the effectiveness of security measures. Mathematical functions for modeling the probability of cyberattacks and anomalies are presented, which are key to automating threat response processes. Examples of practical application of models for congestion forecasting, anomaly analysis, and cyberattack risk assessment in real-world ITS conditions are given.

Keywords

intelligent transport systems, cybersecurity, IoT, big data, machine learning, anomaly probability, DDoS attacks, risk management, multi-level protection, response automation

1. Introduction

An Intelligent Transport System (ITS) is a transport system that uses innovative developments in modeling and regulating traffic flows, which provides end users with greater information and safety, as well as qualitatively improves the level of interaction between traffic participants compared to conventional transport systems [1, 2].

ITS is the systematic integration of modern information, communication technologies, and automation tools with transport infrastructure, vehicles, and users, which focuses on improving the safety and efficiency of the transport process, as well as comfort for drivers and transport users [3].

They are complex cyber-physical systems that use the Internet of Things (IoT), artificial intelligence (AI), and big data technologies to manage urban traffic. Ensuring the cybersecurity of ITS is a critical task, as vulnerabilities in these systems can lead to serious disruptions in transport infrastructure, threats to public safety, and significant economic losses [5, 6].

Cybersecurity in ITS is becoming increasingly important due to the growing number of connected devices and the volume of data. A low level of protection for such systems can lead to serious consequences, including manipulating traffic lights, interfering with autopilots, or blocking emergency services [7–9].

One of the key approaches to cybersecurity is to use mathematical models to assess threats. Such models help predict the likelihood of attacks and anomalies based on historical data and current observations. This allows us to identify potential risks on time [10].

* *CPITS 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2025, Kyiv, Ukraine*

* Corresponding author.

† These authors contributed equally.

i.mashkina@kubg.edu.ua (I. Mashkina); s.rzaieva@kubg.edu.ua (S. Rzaieva); y.kostiuk@kubg.edu.ua (Y. Kostiuk); n.mazur@kubg.edu.ua (N. Mazur); z.brzhevska@kubg.edu.ua (Z. Brzhevska)

0000-0003-0667-5749 (I. Mashkina); 0000-0002-7589-2045 (S. Rzaieva); 0000-0001-5423-0985 (Y. Kostiuk); 0000-0001-7671-8287 (N. Mazur); 0000-0002-7029-9525 (Z. Brzhevska)

Among the main threats to ITS are unauthorized access to the network, denial of service (DDoS) attacks, and the introduction of malicious code. All these threats can seriously affect the operation of the transport system. Probability models also allow us to assess the effectiveness of cyber defense measures [10].

For example, it is possible to analyze how the introduction of new security protocols or system upgrades affects the level of ITS security. An important component of security is modeling anomalies in network traffic. Anomalies can indicate intrusion or malfunction in the system. Detection of such anomalies is based on machine learning algorithms and Bayes' theorem. The combination of threat models and anomaly analysis provides a multi-level security system. This allows you to identify both global risks and local problems in network traffic.

2. Issues

ITS is constantly evolving, introducing new technologies to improve efficiency and safety. The growing complexity of ITS is accompanied by an increase in cyber threats that can lead to serious consequences. One of the key issues is the risk of cyberattacks on critical ITS components, which can cause not only technical malfunctions but also threaten the safety of citizens. Thus, attacks can disrupt the operation of traffic management systems or autopilot vehicles. The ability of ITSs to detect anomalies in network traffic is the basis for randomly responding to some threats. However, this requires the use of complex algorithms and modeling to effectively assess and respond to risks. ITS cybersecurity requires the integration of various approaches for monitoring and analyzing risks. The use of probabilistic models allows you to predict threats, and assess their likelihood and impact on the system.

The problem of ensuring the stability of ITS operations is complicated by the availability of both historical data and current observations. This requires the development of mathematical models that can efficiently obtain both types of information. To assess the likelihood of a cyberattack, threat probability functions are used that take into account the time dependence of risks. This allows for the adaptation of defense mechanisms to a changing threat level. Modeling anomalies in network traffic is an aspect of security. Using machine learning algorithms and Bayes' theorem, we can detect deviations from the normal system behavior [11].

The integration of threat and anomaly probability models into the monitoring process creates a multi-level protection system that covers both global and local risks. Implementing new security protocols requires evaluating their effectiveness. Using probabilistic models, you can analyze how these measures affect the likelihood of attacks and anomalies. Automating threat response processes is critical to minimizing the risk of human error. This allows you to automatically activate response measures based on predefined probability thresholds.

Various distributions, such as the exponential distribution and the Weibull distribution, are used to model the probability of a cyberattack, taking into account constant and changing attack intensities. The exponential distribution models the constancy of the attack intensity, where the risk remains unchanged over time, while the Weibull distribution allows for a reduction in the change in threat intensity. The choice of parameters of the Weibull distribution allows the model to be adapted to different scenarios, for example, the growth or reduction of risks over time depending on the security measures taken.

Growing threat scenarios imply an increase in probability due to the accumulation of vulnerabilities in the system. This requires continuous improvement of security mechanisms. Risk mitigation scenarios show the effectiveness of security measures that reduce the likelihood of an attack. This is achieved through regular software updates and the introduction of new technologies. Mathematical models not only predict threats but also detect anomalies in network traffic, which are major indicators of deviations from the normal system of operation [12].

Anomaly detection based on traffic characteristics allows you to respond quickly to potential threats. This reduces risks and increases system reliability. The use of probabilistic models for

anomaly assessment allows you to integrate existing data and knowledge about the system to accurately predict deviations.

Machine learning algorithms are used to estimate the probability of an anomaly, which has lost various traffic characteristics, such as data volume, response time, and request frequency.

Continuous improvement of anomaly detection models and algorithms is essential to maintain a high level of ITS security. This allows for adaptive risk management and minimization of certain threats.

The main challenges in the field of ITS cybersecurity are:

- A high number of IoT devices.
- Real-time processing of big data.
- Vulnerability to DDoS attacks and unauthorized access. Let's take a closer look at the above challenges [13, 14].

2.1. Vulnerabilities of IoT devices

The growing number of IoT devices is leading to a significant increase in vulnerabilities in ITS. Every device connected to the network becomes a potential entry point for attackers. Many of these devices have limited security resources, making them easy targets. Typically, IoT device manufacturers are more focused on functionality and usability than security. This results in devices that often have outdated or non-existent security mechanisms such as encryption or authentication [15–17].

Many IoT devices do not support regular software updates, leaving them vulnerable to hacker attacks. The lack of uniform security standards for IoT devices makes it difficult to implement effective security measures. Each manufacturer of IoT devices implements its approaches to cyber defense, which leads to fragmentation and an overall reduction in security.

2.2. Processing big data in real-time

Processing large amounts of data in real-time is critical for modern ITS and requires significant computing resources and efficient algorithms to ensure a quick response to potential threats. Sophisticated cryptographic methods are required to ensure the confidentiality and integrity of data, which in turn puts an additional burden on intelligent systems, especially in real-time data processing.

Balancing security and performance is another challenge. The use of complex cryptographic methods reduces processing speed, which is unacceptable for many critical applications.

2.3. Vulnerability to DDoS attacks and unauthorized access

DDoS attacks remain one of the most common threats to ITS. They can be extremely large-scale, using thousands or even millions of zombie devices to generate powerful traffic impacts and lead to the shutdown of critical services, with significant consequences for business and society.

Effective protection against DDoS attacks requires the implementation of specialized solutions, such as continuous monitoring and analysis of traffic, traffic filtering, the use of cloud-based security services, and other methods.

The threat of unauthorized access also remains a concern for many ITSs. Hackers can use a variety of methods, such as password guessing, exploiting software vulnerabilities, or social engineering, to gain access to an intelligent transport system. To prevent unauthorized access, comprehensive security measures should be used, including multi-level authentication, data encryption, regular software updates, and cybersecurity training for staff.

Real-time threat analysis is critical to minimizing risks. This is achieved by combining predictive models with network traffic monitoring mechanisms. However, for maximum

effectiveness, it is necessary to integrate these models with multi-factor analysis that takes into account both the current state of the system and the probability of future threats.

To improve the efficiency of security systems, it is advisable to use multivariate analysis methods. The use of probabilistic models also opens up the possibility of automating threat response processes. For example, when a certain probability threshold is reached, the system can automatically activate response measures, such as blocking suspicious traffic or notifying operators. This significantly improves the efficiency of ITS operations, minimizing the risk of human error.

Thus, the probability functions of threats and anomalies are fundamental elements for building reliable and safe intelligent transport systems. The following sections describe these approaches, their mathematical foundations, and examples of real-world applications.

3. Presentation of the main material

In today's world, ITS plays a key role in ensuring the efficient operation of transport infrastructure, improving road safety, and reducing negative environmental impact. Through the integration of IoT, big data, and artificial intelligence, ITS can process huge amounts of information in real-time, enabling traffic optimization, road condition monitoring, and interaction between vehicles and infrastructure. However, the high dependence on digital technologies makes these systems vulnerable to cyberattacks, technical failures, and network anomalies. For a detailed understanding of the principles of ITS functioning and approaches to their protection, it is advisable to consider the Model of Intelligent Transportation System.

The intelligent transport system model consists of three key components: the ITS Architecture Level, the Integrated Management Level, and the ITS protection levels. The model of an intelligent transport system is shown in Fig. 1.

An intelligent transport system consists of a multi-level architecture that integrates transport infrastructure, digital technologies, and users. The main modules of the ITS architectural layer are the Physical Level, the Communication Level, and the Computational Level.

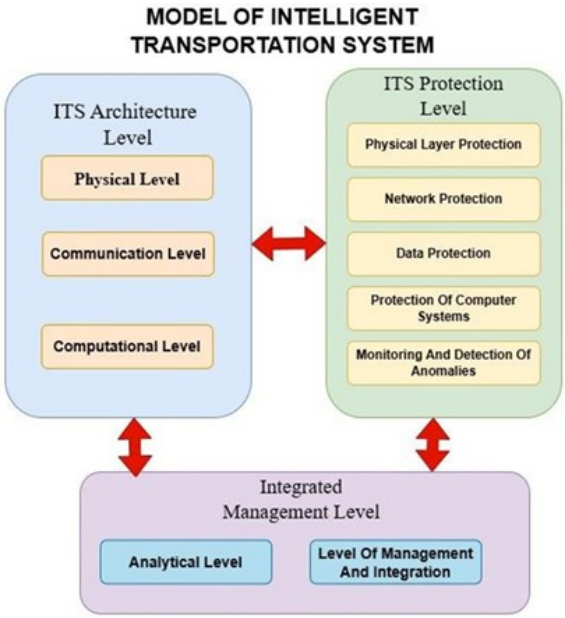

Figure 1: Model of Intelligent Transportation System

The physical layer is the foundation of the ITS architecture and includes road transport infrastructure such as roads, bridges, tunnels, traffic lights, parking meters, sensors, and IoT devices [18]. Equipment at this level collects data on traffic flows, road surface conditions, weather conditions, etc.

IoT devices are key elements of the physical layer and provide continuous monitoring and data transmission:

- Traffic sensors detect the intensity and speed of traffic flows.
- Weather sensors detect environmental conditions such as temperature, humidity, and precipitation that affect road safety.
- GPS trackers provide accurate positioning of vehicles in real-time.
- Video cameras analyze the traffic situation, detecting traffic violations or emergencies.

The physical layer not only collects data but also actively interacts with other layers of the system. For example, traffic sensors and traffic lights change the traffic lights in real time depending on the traffic volume, and V2I (Vehicle-to-Infrastructure) technologies provide vehicles with data on the traffic situation, accidents, or speed limits.

The main challenges of the physical level are:

- Reliability of IoT devices, which must operate stably even in difficult weather conditions or in the presence of high traffic loads [19].
- Thorough real-time monitoring.
- The physical layer is vulnerable to physical attacks, such as damage to sensors or malicious access to equipment.

This layer is the basic component for collecting data that is then analyzed at the integrated management layer, namely: sensor data is transmitted to the communication layer, where it is processed; video streams from cameras are analyzed at the analytical layer to detect violations; the collected data helps the management layer make decisions on traffic optimization or emergency.

The communication layer ensures data transfer between all components of the intelligent transport system. The goal of this layer is to organize efficient, reliable, and secure information exchange between physical devices, computing centers, and users and includes wireless protocols (Wi-Fi, 5G, V2X), fiber-optic communication lines, and satellite systems [20]. This layer provides low latency and reliable real-time data exchange and is responsible for ensuring that data from traffic lights, motion sensors, and vehicles is transmitted in real-time for processing and analysis.

The communication layer integrates various technologies using modern communication protocols, such as:

- V2X (Vehicle-to-Everything) protocols for the exchange of data between vehicles (V2V), vehicles and infrastructure (V2I), pedestrians (V2P), and cloud platforms (V2C).
- 5G provides high bandwidth, minimal latency, and stable communication even in congested networks, which is critical for transmitting video from surveillance cameras or coordinating traffic in real time.
- The use of fiber-optic networks and wireless devices for high-speed data transmission between large data centers and servers.

The communication layer faces many challenges, including delays in data transmission; ensuring that data transmitted over the network is protected from interception, tampering, or loss; supporting a system consisting of different types of devices and communication protocols that may have different technical standards, etc.

The communication layer is critical to the operation of the entire system, as, without reliable communication, coordination between vehicles, infrastructure, and control centers is impossible. It provides the basis for the other layers of the architecture, such as the analytics and control layers. For example, fast and accurate data exchange allows machine learning algorithms to detect anomalies in traffic or predict congestion, and users to receive up-to-date information about traffic conditions.

The Computational Level provides the computing power of the intelligent transport system, which includes servers, cloud platforms, and data centers where the collected data is processed and analyzed; it is responsible for executing artificial intelligence algorithms to predict traffic and manage resources. For example, data from sensors, such as vehicle speed, number of cars at intersections, or road surface conditions, are sent to computing platforms, and distributed computing systems quickly analyze the information, transmitting the results to the analytical level or directly to control devices (e.g. traffic lights).

At the computing level, machine learning and artificial intelligence algorithms are implemented to help analyze traffic flows, predict congestion, and detect emergencies and deviations in the system's functioning.

The computing layer plays the role of a link between the physical, communication, and analytical layers, receives data from the physical layer through the communication layer, processes it, and transmits the results for further analysis.

3.1. Integrated management level

This component consists of the following modules: Analytical level and Management and Integration level.

The analytical level analyses big data collected from sensors and communication systems and uses machine learning algorithms to analyze and interpret the collected data, detect anomalies, and support decisions to optimize transport processes. This level uses advanced Big Data technologies and machine learning algorithms. Systems at this level are capable of processing both structured and unstructured data, such as video streams, sensor signals, and event logs. Clustering, prediction, neural network, and anomaly detection algorithms help:

- Analyse historical data and current conditions to predict scenarios such as traffic congestion and journey times.
- Adapt the system's behavior to the current conditions.
- In finding optimal solutions for the distribution of vehicles, traffic lights, parking spaces, and other elements of transport infrastructure.
- Detect deviations from normal system behaviour, such as suspicious network activity, equipment failures, anomalies in traffic lights power consumption, or inconsistencies in traffic flow.
- Model possible scenarios and assess risks associated with various factors, such as weather conditions, accidents, or cyberattacks.

The analytical layer works in close connection with the computing layer, which provides it with processed data, and with the management layer, which uses the results of the analysis to make decisions. For example, the traffic forecast generated by the analytical layer can be transmitted to traffic light control systems to dynamically change their operation. Analytics results can also be sent to the user interface to provide drivers with up-to-date information about the traffic situation.

The management and integration layer provides the interaction between users, control systems, and other infrastructure components and ensures the strategic management of the entire transport network in real-time. Its main function is to coordinate the work of all system components to achieve optimal efficiency, safety, and convenience.

The management and integration layer collects data from the other layers (physical, communication, computing, and analytical) and uses this data to make decisions about optimizing the system, which is then passed on to the other layers for execution. For example, data from the analytical layer that indicates an increase in traffic in a particular area can be used to redirect traffic through alternative routes.

The management layer provides integration with other important infrastructure elements:

- For energy systems, we manage charging stations for electric vehicles, monitor energy consumption, and plan the operation of low-carbon vehicles.
- For the public safety system, data is transmitted to emergency response services in the event of accidents or natural disasters.
- For the environmental system, the level of emissions of pollutants such as nitrogen oxides (NOx), carbon dioxide (CO2), and particulate matter from vehicles is monitored and measures are taken to minimize their environmental impact.

The level of governance and integration is critical to creating reliable and flexible transport systems that can operate efficiently even in complex urban environments.

3.2. Levels of ITS protection

Since intelligent transport systems are vulnerable to cyberattacks and technical failures, it is necessary to provide multi-level protection covering all components of the model. The main levels of protection:

1. Physical Layer Protection (Physical Layer Protection) ensures the security of equipment and physical sensors; and provides access to equipment only for authorized persons using surveillance cameras and other physical security features.
2. Network Protection uses firewalls, VPNs, traffic encryption, and protection of communication protocols (for example, V2X). The main goal is to prevent unauthorized access to the network and reduce the risk of DDoS attacks.
3. Data Protection provides data encryption, user authentication, and access control; and minimizes the risks of data leakage and privacy breaches.
4. Protection of Computer Systems (POCS) involves regular software updates, monitoring of server activity, and the use of intrusion detection systems (IDS). Cloud computing is protected through access control and backup policies.
5. Monitoring and detection of anomalies uses algorithms to analyze traffic in real-time to detect anomalies and respond to suspicious activity.

To analyze risks and ensure the stability of ITS operations, it is important to use mathematical models that allow you to estimate the probability of threats and anomalies. These models are based on probabilistic approaches that take into account both historical data and current observations, making them indispensable for predicting potential problems.

One of the key tasks is to estimate the probability of a cyberattack on ITS at a certain point in time. This task is solved with the help of a threat probability function that takes into account the dependence of risks on time. The use of an exponential distribution or its generalizations, such as the Weibull distribution, allows the modeling of both fixed and variable risks, including those that increase due to the accumulation of vulnerabilities in the system or decrease due to security measures.

Another important aspect is the modeling of anomalies in network traffic, which is the basis for timely threat detection. The anomaly probability functions are based on machine learning algorithms and use Bayes' theorem to estimate the probability of anomalies based on current traffic characteristics. This approach takes into account both the normal behavior of the system and its deviations that indicate potential problems.

The integration of these two approaches into the monitoring process allows you to create a multi-level security system that takes into account both global risks (e.g. cyberattacks) and local network anomalies. This is especially important to ensure security in the face of the ever-increasing complexity of ITS and the growing number of connected devices.

Mathematical probability models allow not only to predict potential threats but also to assess the effectiveness of security measures. For example, when implementing new security protocols, it

is possible to analyze how the probability of attacks and anomalies changes over time, which is critical for adaptive risk management.

The use of probabilistic models also opens up the possibility of automating threat response processes. For example, when a certain threshold of probability is reached, the system can automatically activate response measures, such as blocking suspicious traffic or notifying operators. This greatly improves the efficiency of ITS, minimizing the risk of human error.

To model the probability of a cyberattack *P(T)* on a transport system over a certain time *T*, one can use, for example, an exponential distribution, which is often used to describe the time between random events such as attacks or system failures.

The probability function has the form:

$$P(T)=1-e^{-\lambda T}, \quad (1)$$

where $\lambda > 0$ is the intensity frequency) of cyberattacks, which reflects the average number of attacks per unit of time; $T \geq 0$ is the time for which the probability of an attack is considered.

P(T) increases as *T* increases since the probability of a cyberattack increases over time. The coefficient λ determines how fast *P(T)* grows. The larger λ, the more frequent the attacks are, and thus the higher the probability of an attack occurring in a fixed time *T*.

If the attacks have different intensities over time, a generalization can be used, such as a function based on the Weibull distribution. This function is a generalized model for describing the time to an event that has a variable intensity over time. So the probability function for cyber attacks looks like this:

$$P(T)=1-e^{-(\lambda T)^k}, \quad (2)$$

where $\lambda > 0$ is a scale parameter that reflects the basic intensity of attacks; $k > 0$ is a shape parameter that takes into account the dependence of the frequency of attacks on time (for example, the risk increases over time).

Interpretation of the parameter *k*:

- When $k = 1$, the model reduces to an exponential distribution, where the intensity of attacks remains constant.
- When $k > 1$, the intensity of attacks increases over time. This can model a situation where threats accumulate or cybercriminals become more active over time.
- When $k < 1$, the intensity of attacks decreases over time, which may reflect a situation where cyber defense or threat mitigation efforts reduce the likelihood of attacks.

Let's take an example of situations that may arise when changing the parameter *k*:

Situation 1, when the parameter $k = 1$, the Weibull distribution model reduces to an exponential distribution:

$$P(T)=1-e^{\lambda T}, \quad (3)$$

where $\lambda > 0$ is the attack intensity that remains constant over time. A constant attack intensity (λ) means that the risk does not increase or decrease over time.

The ITS traffic monitoring system on the highway is equipped with a standard set of network devices, such as cameras and motion sensors. All of these devices have the usual levels of protection that are not updated but also do not have obvious vulnerabilities, i.e. the presence of self-driving cars that are connected to the network but operate at a standard level of cyber protection; traffic management systems with fixed authentication rules, where the risk of attacks is stable. This is a typical scenario for systems with fixed security parameters, where there is no accumulation of vulnerabilities or improvement of protection mechanisms.

The function *P(T)* linearly approaches 1 as *T* grows, which means that the more time passes, the more likely it is that an attack will occur. In this case, the probability of cyberattacks remains constant, as the intensity of hacking attempts does not depend on time.

Thus, the scenario with *k=1* is a basic model for situations where there are no complex risk dynamics over time. This is a good choice for systems that are stable in terms of complexity and security.

Situation 2, when the parameter *k>1*, i.e. the scenario of an increasing threat.

The intelligent transport system operates in an environment where risks are increasing due to the accumulation of vulnerabilities, which is what is happening:

- Increase in connected devices and IoT sensors without proper security updates.
- An increase in the amount of data on the network (which creates new points for potential attacks).
- Adaptation of attackers to existing security mechanisms.

In this case, the probability of an attack increases over time as the system becomes more vulnerable. To model such a scenario, you can use a Weibull distribution with $k > 1$, which takes into account the increasing intensity of attacks. The probability function in this situation looks like this:

$$P(T)=1-e^{-(\lambda T)^k}, k>1. \quad (4)$$

This situation is possible if the traffic management system in a large metropolis has not been updated for several years. Every month, the likelihood of cyberattacks on servers that control traffic lights and exchange data with vehicle autopilots is increasing.

Situation 3, when the parameter $k < 1$, i.e. the risk reduction scenario.

Let's consider a situation where an intelligent transport system is constantly improving its protection mechanisms, i.e:

- Regular updates of ITS software.
- Implementing machine learning algorithms to detect anomalies in real time.
- Installing additional cybersecurity measures (firewalls, encryption, etc.).

In this case, the risk of cyberattacks decreases over time due to these measures. To model such a scenario, you can use a Weibull distribution with $k < 1$, which takes into account the decrease in attack intensity. The probability function looks like this:

$$P(T)=1-e^{-(\lambda T)^k}, k<1. \quad (5)$$

This situation is possible if the intelligent transport system and software of self-driving cars are regularly updated and algorithms for detecting suspicious activity in the network are improved. As a result, the likelihood of successful attacks is significantly reduced every month.

The mathematical formula (1) is based on the exponentially distributed time between events (cyberattacks) and is used to assess the reliability and security of a system. It allows us to predict the probability of a successful attack depending on the time and intensity of the attacks.

Imagine a situation in which an ITS serving a large metropolitan area is subject to a cyberattack, and the probability of a cyberattack increases over time if the system is operated without intervention or updates. You can graphically visualize the probability function of the time to a cyberattack. First, let's write a Python code to visualize this function:

```
import matplotlib.pyplot as plt
import numpy as np
```

```
# Define the parameters for the formula
lambda_value = 0.1
T = np.linspace(0, 50, 400)
P_T = 1 - np.exp(-lambda_value * T)

# Create the plot

plt.figure(figsize=(8, 6))
plt.plot(T, P_T, label=r'$P(T) = 1 - e^{-\lambda T}$', colour='blue')
plt.title('Probability of Cyber Attack Over Time')
plt.xlabel('Time (T)')
plt.ylabel('Probability $P(T)$')
plt.grid(True)
plt.legend()
plt.tight_layout()

# Save the plot to a file
plt.savefig("/mnt/data/probability_formula_plot.png") plt.show()
```

The X-axis displays the time (*Time (T)*) elapsed since the start of the system operation and displays time in the range from 0 to 50 (time units can be seconds, hours, or days, depending on the system context). This is an independent variable that defines the point in time before which the probability of an attack is estimated.

The Y-axis represents *the probability* that a cyberattack will occur by time *T*. At the beginning, *P(T)* = 0 means that the probability of an attack is zero. *P(T) = 1* means that the probability of a cyberattack is almost 100% (given a sufficiently long time).

The parameter λ = 0.1 (attack intensity) reflects the average frequency with which cyberattacks occur (Fig. 2).

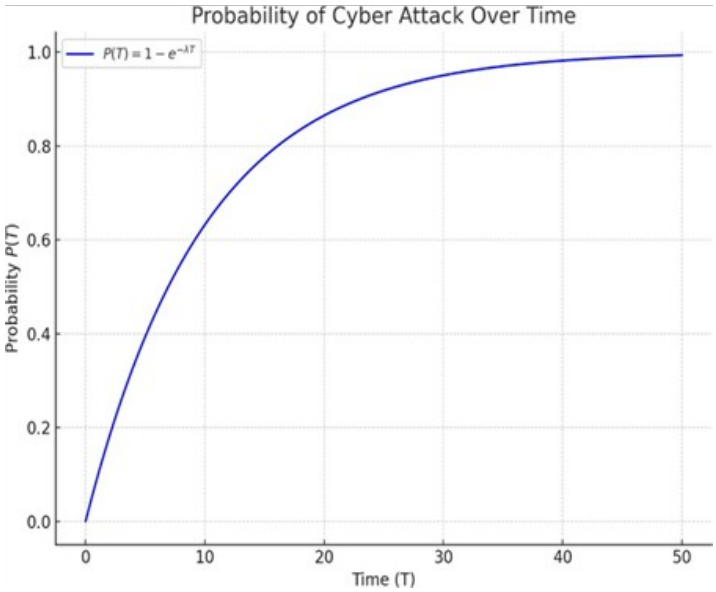

Figure 2: Probability of cyber attack over time

The graph shows the dependence of the probability of a cyberattack on time. Initially, *P(T)* is low, as the probability of an attack in a short time is negligible. As T increases, the probability of a cyberattack increases and asymptotically Approaches 1.

Analyzing the above graph allows you to assess the risks to the system and identify critical time points when security measures need to be taken.

The probability density function of the Weibull distribution for ITS has the following mathematical expression:

$$f(T)=k\lambda^{k}T^{k-1}+e^{-(\lambda T)^{k}}, \tag{6}$$

where *f(T)* shows how likely an attack is at a given time *T*.

Thanks to the *k* parameter, the model can adapt to different scenarios (increasing or decreasing risks over time).

The expected time to attack can be calculated as the average time between attacks:

$$E[T] = \lambda^{-1} \times \Gamma(1 + {}^{1}/_{k}), \tag{7}$$

where *Γ()* is the gamma function.

To ensure effective analysis of the state of an intelligent transport system, it is important not only to model the likelihood of threats but also to assess the likelihood of anomalies that may indicate potential cyberattacks or malfunctions. Anomalies in network traffic are important indicators of deviations from normal behavior, and their detection allows for a quick response to risks.

For this purpose, machine learning algorithms based on probabilistic models can be used. Let *X(t)* be *a* set of network traffic characteristics at time *t*. Then the probability of an *anomaly P(Anomaly|X(t))* can be described based on Bayes' theorem, which allows the integration of available data and knowledge about the system.

Another important aspect is the use of machine learning algorithms to detect anomalies in network traffic. Let *X(t)* be a set of network traffic characteristics at time *t*. The anomaly probability function can be defined as follows:

$$P(Anomaly|X(t))=\frac{P(X(t)|Anomaly)\times P(Anomaly)}{P(X(t))} \tag{8}$$

where *P(Anomaly| X(t))* is the probability that the anomaly occurs given the observed characteristics of X(t); *P(X(t)| Anomaly)* is the probability of observing the characteristics *of X(t)* if the presence of an anomaly is known; *P(Anomaly)* is the a priori probability of an anomaly (the probability of an anomaly without taking into account *X(t); P(X(t))* is the total probability of observing the characteristics *of X(t)*.

Model (8) allows us to estimate the probability of an anomaly based on the characteristics of network traffic *X(t)*.

The total probability of observation *X(t)* is defined as:

$$P(X(t)) = P(X(t)|Anomaly)\times P(Anomaly)+P(X(t)|-Anomaly)\times P(-Anomaly) \tag{9}$$

where *P(–Anomaly) = 1 – P(Anomaly)* is the probability of no anomaly; *P(X(t)| –Anomaly)* is the probability of observing *X(t)* in the absence of an anomaly. Thus, the formula for calculating *P(Anomaly|X(t))* is:

$$P(Anomaly|X(t)) = \frac{P(X(t)\vee Anomaly)\times P(Anomaly)}{P(X(t)/Anomaly)\times P(Anomaly)+P(X(t)/-Anomaly)\times P(-Anomaly)} \tag{10}$$

Thus, model (10) allows us to estimate the probability of an anomaly based on the characteristics of network traffic *X(t)*.

Consider an intelligent transport system (ITS) that exchanges data between vehicles, roadside sensors, and a central control server. Under normal conditions, the traffic between the system components has stable characteristics such as data volume, request frequency, and response time. However, anomalies, such as a sharp increase in the number of requests or a change in packet structure, can indicate potential cyberattacks or system malfunctions.

To estimate the probability of an anomaly $P(Anomaly| X(t))$, a set of network traffic characteristics $X(t)$ is used, such as:

- $X_1(t)$ is the amount of data per unit of time.
- $X_2(t)$ is the average response time.
- $X_3(t)$ is the frequency of requests per device.

Suppose that the system has recorded the following traffic characteristics at time t:

- $X_1(t)$ = 500 MB/s (a significant excess of the average data volume).
- $X_2(t)$ = 5 seconds (increase in response time).
- $X_3(t)$ = 2000 requests/second (abnormally high request frequency).

Determined based on historical data:

- $P(X(t)| Anomaly)$ = 0.9 (such characteristics often occur in anomalies).
- $P(Anomaly)$ = 0.01 (a priori probability of anomaly is low).
- $P(X(t))$ = 0.02 (the total probability of observing such characteristics). Let's calculate the probability of an anomaly using formula (8):

$$P\left(Anomaly\middle|X\left(t\right)\right)=\frac{0.9\times 0.01}{0.02}=0.45.$$

The probability of an anomaly in the system is 45%. This is high enough for the system to activate response protocols, for example:

- Blocked suspicious traffic.
- Notified the operators of the potential threat.
- Performed an additional network check.

This example demonstrates how the anomaly probability function helps an intelligent transport system detect suspicious activity in network traffic. The use of such models allows ITS to provide high reliability and security.

Conclusion

Intelligent transport systems are becoming increasingly complex systems where the processing of large amounts of data in real-time is critical. An important component in automating threat response processes is coordination between different ITS components, such as traffic control centers, self-driving vehicles, and infrastructure sensors. The use of machine learning algorithms and Bayes' theorem allows for the identification of deviations from normal system behavior, which is critical to preventing cyberattacks.

Consistency of data and cybersecurity protocols is a key factor in system reliability. Modern approaches to ITS cybersecurity involve the use of hybrid models that combine statistical methods, machine learning algorithms, and predictive analysis. Further research should focus on improving these mathematical models and algorithms for even more effective risk management and cybersecurity in ITS.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] F. J. Ferrández-Pastor, et al., Deployment of IoT edge and fog computing technologies to develop smart building services, Sustainability, 10(11) (2018) 3832. doi:10.3390/su10113832

[2] M. Malatji, Management of enterprise cyber security: A review of ISO/IEC 27001:2022, in: IEEE International Conference on Cyber Management and Security, 1, 2023, 45–52. doi:10.1109/cymaen57228.2023.10051114

[3] S. Goswami, A. Kumar, Traffic flow prediction using deep learning techniques, in: Int. Conference on Computing Science, Communication and Security, 1, 2022, 187–198.

[4] R. D. Bretherton, SCOOT urban traffic control system-philosophy and evaluation, IFAC Proc. Vol. 23(2) (1990) 127–132. doi:10.1016/s1474-6670(17)52676-2

[5] A. Zanella, et al., Internet of things for smart cities, IEEE Internet Th. J. 1(1) (2014) 22–32.

[6] W. Shi, et al., Edge computing: Vision and challenges, IEEE Internet Th. J. 3(5) (2016) 637–646.

[7] H. P. Nguyen, P. Q. P. Nguyen, V. D. Bui, Applications of big data analytics in traffic management in ITS, JOIV: Int. J. Inf. Visualisation, 6(2) (2022) 123–135. doi:10.30630/joiv.6.1-2.882

[8] K. Zhang, S. Batterman, Air pollution and health risks due to vehicle traffic, Sci. Total Environ. 450–451 (2013) 307–316. doi:10.1016/j.scitotenv.2013.01.074

[9] S. Rzaieva, et al., Methods of modeling database system security, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654, 2024, 384–390.

[10] V. Lakhno, et al., Continuous investing in advanced fuzzy technologies for smart city, in: Computational Intelligence and Data Analytics, Lecture Notes on Data Engineering and Communications Technologies, vol. 142, 2023, 313–327. doi:10.1007/978-981-19-3391-2_24

[11] V. Lakhno, et al., Computer support system for choosing the optimal managing strategy by the mutual investment procedure in smart city, in: Complex, Intelligent and Software Intensive Systems, CISIS 2020, Advances in Intelligent Systems and Computing, vol. 1194, 2020, 278–288. doi:10.1007/978-3-030-50454-0_26

[12] S. O. Kliuyev, S. V. Tsymbal, A. E. Sigonin, Development of intelligent transport systems, Bull. Mech. Eng. Transp. (2023) 80–86.

[13] A. Lavrenchuk, The future of cybersecurity: Challenges of artificial intelligence and machine learning, Kyiv, Young Scientist, 2024.

[14] N. Dovzhenko, et al., Integration of IoT and artificial intelligence into intelligent transport systems, Cybersecur. Educ. Sci. Technol. 2(26) (2024) 430–444. doi:10.28925/2663-4023.2024.26.708

[15] R. Chernenko, et al., Encryption method for systems with limited computing resources, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 142-148.

[16] A. Bessalov, et al., Implementation of the CSIDH algorithm model on supersingular twisted and quadratic Edwards curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3187, no. 1 (2022) 302–309.

[17] A. Bessalov, V. Sokolov, P. Skladannyi, Modeling of 3- and 5-isogenies of supersingular Edwards curves, in: 2nd International Workshop on Modern Machine Learning Technologies and Data Science, no. I, vol. 2631 (2020) 3039.

[18] V. Sokolov, et al., Method for increasing the various sources data consistency for IoT sensors, in: IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PICST) (2023) 522–526. doi:10.1109/PICST57299.2022.10238518

[19] V. Dudykevych, et al., Platform for the security of cyber-physical systems and the IoT in the intellectualization of society, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 449–457.
[20] V. Sokolov, P. Skladannyi, N. Mazur, Wi-Fi repeater influence on wireless access, in: IEEE 5th International Conference on Advanced Information and Communication Technologies (2023) 33–36. doi:10.1109/AICT61584.2023.10452421