

Predictive maintenance and security co-design with intelligent transportation systems

Bipin Sule [†]

Department of Engineering Science and Humanities

Vishwakarma Institute of Technology

Pune 411037

Maharashtra

India

Amit Gaurav ^{*}

School of Engineering and Technology

Noida International University

Greater Noida 201312

Uttar Pradesh

India

Subhasri Telkar [§]

Department of Electronics & Communication Engineering

Pragati Engineering College

Kakinada 533437

Andhra Pradesh

India

Allama Prabhu [‡]

Department of Computer Science and Engineering (Artificial Intelligence & Machine Learning)

Vardhaman College of Engineering

Shamshabad

Hyderabad 501218

Telangana

India

[†] E-mail: bipin.sule@vit.edu

^{*} E-mail: coe@niu.edu.in (Corresponding Author)

[§] E-mail: subhasritelkar@gmail.com

[‡] E-mail: allamaprabhu1625@vardhaman.org

K. Shree Jayaram [@]

*MAHER Innovation and Incubation Centre
Meenakshi Academy of Higher Education & Research
Chennai 600087
Tamil Nadu
India*

Monali Gulhane [#]

*Department of Computer Science and Engineering
Symbiosis Institute of Technology
Symbiosis International (Deemed to be University)
Nagpur Campus
Nagpur 440008
Maharashtra
India*

Abstract

Intelligent Transportation Systems (ITS) are becoming dependent on connected vehicles, roadside infrastructure, IoT devices, communication networks, and intelligent computing platforms, which introduces major reliability and cybersecurity challenges. The present paper presents a co-design framework for predictive maintenance and cyber security based on artificial intelligence (AI) for improving the cyber-physical resilience in ITS. The framework will combine equipment health, maintainability data, operational sensor data, and network-security data to analyze both the physical degradation and cyber threats. A hybrid model of XGBoost-BiLSTM-Attention is designed, in which XGBoost picks informative features, BiLSTM models the temporal dependency and attention focuses on important observations. The framework enables the detection of the health of the equipment, the detection of anomalies, failure prediction, remaining useful life estimation, intrusion detection and identification of cyber-attacks. There is a joint classification mechanism which separates normal operation, physical faults, cyber-attacks and simultaneous fault-attack conditions. The coordinated risk assessment is enabled by Unified risk assessment. The proposed approach helps to mitigate false alarms, enhance fault-attack discrimination, enable proactive maintenance and boost the reliability, security, and resiliency of next generation ITS infrastructures.

Subject Classification: 68M25.

Keywords: Artificial intelligence, Cybersecurity, Predictive maintenance, Cyber-physical systems, Attention mechanism, Intrusion detection.

[@] E-mail: shreejayaram@maher.ac.in

[#] E-mail: monali.gulhane4@gmail.com

1. Introduction

Intelligent Transportation Systems (ITS) are an integral component of today's transportation infrastructure, combining sensing, communication, computing, and intelligent decision-making technologies [1]. All of these are connected to one another and to vehicles, to roadside units and traffic controllers, to Internet of Things (IoT) sensors, to edge devices and to cloud platforms, as they all exchange information to enhance traffic management, mobility, safety, and operational efficiency. Automated analysis of large amounts of operational and network data is another benefit of artificial intelligence (AI) and machine learning (ML) to enhance ITS [2]. As the connectivity increases, however, so do the risks to the transportation infrastructure of equipment deterioration, unplanned failures, communication impairments and cybersecurity attacks, which require reliability and cyber resilience [3]. Predictive maintenance works by continuously analyzing equipment status, and predicting future equipment failures as early as possible, which increases the reliability of the infrastructure [4]. Unlike corrective or schedule-based preventive maintenance, predictive approaches are based on sensor measurements, machine operational data and historical maintenance knowledge to identify trends of degradation, to evaluate the health of the equipment, to look for anomalies, and to estimate the remaining useful life (RUL) [5]. These can lead to less time spent on downtime, maintenance costs, need for unnecessary component replacement and disruption to transportation services [6].

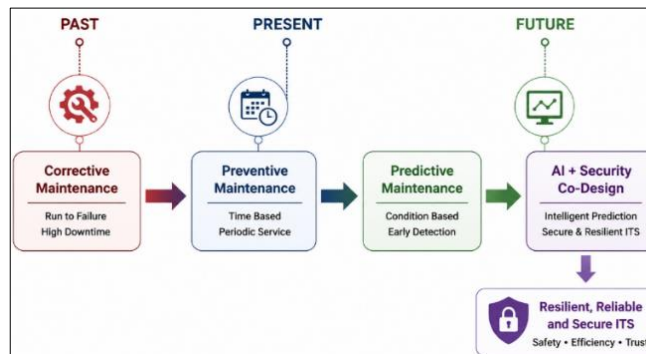


Figure 1
Maintenance Strategies toward AI-enabled cyber-physical co-design

Cyber security is also paramount due to the multiple attack surface that is created from connected ITS components. The following denial-of-service, spoofing, false-data injection, malware, unauthorized access, and communication manipulation attacks may occur in vehicles, roadside devices, wireless networks, traffic controllers and cloud services as shown in Figure 1. This type of attacks can affect the sensor data, decisions made by the controllers, reliability of the communication, and availability of the system [7].

A key issue is that the anomalies that can be observed due to physical faults and those due to cyberattacks can be the same. This leads to a possibility of false alarms and unnecessary actions being taken as part of the maintenance and/or cyber monitoring of the equipment, as well as incorrect interpretation of equipment degradation as malicious operation and/or data manipulation as physical failure [8]. Hence, in this work, it is proposed to develop a new framework for the co-design of predictive maintenance and cyber security system for resilient ITS based on Artificial Intelligence. It features a single cyber-physical monitoring architecture that brings together various pieces of information related to the health of the equipment, operational measurements, maintenance log, vehicle data and network-security features, to be used for health assessment, fault prediction, remaining useful life estimation, anomaly detection, intrusion detection and identification of cyber-attacks.

2. System Model and Problem Formulation

The research is based on an Intelligent Transportation System (ITS) which is a cyber-physical system that includes Internet of Things (IoT) sensors, communication networks, edge nodes, cloud-based transportation services, surveillance devices, traffic controllers, and roadside units (RSUs) that are connected with the vehicles (V), as shown in Figure 1, [9]. They continually share operational and network info about the traffic, vehicles, infrastructure and safety-critical use cases. The behaviour of the physical equipment and communication activities are tightly coupled and failure or cyber-attacks on one can impact several ITS services [10]. Thus, the system model simultaneously takes into account the operational reliability and cyber security. Physical layer includes the transportation infrastructure and sensing devices which gather the information on condition and operation. Examples of representative variables are the temperature, vibration, voltage, current, speed of a vehicle, traffic density, equipment utilization, signal status, quality of communication, and the environment. In addition, historical maintenance records and component ages, operating time, fault history and parts replacement data are included. At time t , the feature vector representing the physical and operational feature is given as:

$$Xp(t) = [xp1(t), xp2(t), \dots, xpm(t)],$$

The cyber layer is related to vehicle, RSU, edge device and transportation server communication and network behaviour. Some of the features that can be included are packet rate, packet size, protocol type, connection duration, frequency of transmission, failed communications attempt, and traffic-flow statistics [11]. These measurements enable denial of service attacks, spoofing, false data injection, malware, unauthorized access and communication manipulation to be detected. cybersecurity FEV has the value of:

$$Xc(t) = [xc1(t), xc2(t), \dots, xcn(t)],$$

In which, n is the number of features relating to security.

The physical features, cyber security features and maintenance information $Xm(t)$ are combined into one.

$$X(t) = X_p(t) \oplus X_c(t) \oplus X_m(t).$$

This comprehensive view enables the AI model to detect patterns and connections between equipment degradation and network anomalies.

The main goal is to classify each observation into the four operational states, namely, normal operation (N), physical fault (F), cyberattack (A) and simultaneous fault and attack condition (FA). A learnable AI model $f\theta$ is used to estimate the state of the system, the joint (particular) classifier.

$$Y^t = f\theta(XCP(t))$$

At the same time, the predictive maintenance module calculates the health level and remaining useful life of equipment and the cybersecurity module the probability and impact of attack [12], [13]. These outputs are then aggregated into a single cyber-physical risk score which is used for decision making such as continuing operation, preventive maintenance, immediate repair, a cybersecurity action, component isolation or coordinated maintenance-security intervention. Therefore, the formulation can be used to effectively detect and distinguish faults and enhance the resilience of the overall ITS system. The framework employs both physical condition monitoring and network threat analysis to minimize misclassification, minimize false alarms and facilitate response to interconnected transportation infrastructure components in a timely fashion.

3. Proposed Predictive Maintenance and Security Co-Design Framework

The proposed framework combines predictive maintenance and cyber security monitoring in a single AI-based framework, improving reliability, security and resilience of Intelligent Transportation Systems (ITS). The proposed co-design approach is different from the traditional design approaches that process the information about the health of the equipment and the security of the network separately, by combining the physical, operational, maintenance and communication information to differentiate equipment degradation, cyberattacks and simultaneous cyber-physical disturbances. To begin, multi-source data acquisition from connected vehicles, roadside communications, traffic controllers, cameras, IoT sensors, edge devices and communications networks. The variables that affect the operation are temperature, vibration, voltage, current, vehicle speed, traffic density, equipment utilization, signal state and communication quality. Component age and operating hours, previous failures, repairs, replacements and service intervals are included in maintenance records. The components of cybersecurity data are packet frequency, packet size, characteristics of the protocol, duration of connection, errors that occur during transmission, and access attempts that are abnormal. The end states of the final system can then be made as presented in Table 1:

Table 1
System Condition Class Definitions

Class	System condition	Interpretation
C0	Normal	Healthy equipment + benign communication
C1	Physical Fault	Equipment degradation/failure without attack
C2	Cyberattack	Healthy physical system under malicious activity
C3	Fault + Attack	Physical degradation accompanied by cyberattack

The features selected are merged as $F_{CP} = F_P \oplus F_M \oplus F_C$, with F_P, F_M and F_C representing the physical, maintenance and cybersecurity features, respectively. The predictive maintenance module then evaluates the health of the equipment, recognizes signs of degradation, determines when it will fail and estimates the remaining useful life of the equipment, and the cybersecurity module analyzes malicious network activity.

Normal $\rightarrow$ Physical Fault $\rightarrow$ Cyberattack $\rightarrow$ Fault + Cyberattack

The combined condition of a physical fault and a cyber-attack is distinguished by a joint AI classifier, which also classifies four states: normal operation, physical fault, cyber-attack and combined fault-attack. Third, unified risk assessment integrates the probability of fault, the probability of attack, the condition of the equipment and the severity of the event to suggest continued operation and maintenance, immediate repair, security mitigation, equipment isolation or coordinated intervention to minimize false alarms, and enhance the overall resilience of ITS. Such an integrated architecture enhances the efficiency of maintenance operations, accuracy of attack response, resource allocation and operational continuity as well.

4. Proposed XGBoost–BiLSTM–Attention methodology

The proposed system uses an integrated approach and artificial intelligence/machine learning technology to assess the condition of the equipment and detect cyber threats in Intelligent Transportation Systems (ITS). The idea is different from the traditional method of analyzing maintenance and security information separately, which is achieved by the coordinated learning modules of processing operational sensor measurements, historical maintenance information, and vehicular information and network traffic. The proposed model is based on hybrid XGBoost, BiLSTM and Attention to utilize the importance of features and the temporal dependency of cyber-physical information. The methodology enables the following: Equipment health assessment, Anomaly detection, Failure prediction, remaining useful life (RUL) estimation, Intrusion detection, Attack identification, multi-class system-state classification. The data collected is preprocessed before being used, which includes handling missing values, removing duplicates, filtering out noise, encoding categorical variables, normalizing the data and synchronizing it in time. Class-balancing methods are used to prevent the prediction bias that can be introduced by normal operating

observations that can often far outweigh the number of failure or attack observations.

Step -1: The processed input at time t is represented as

$$X_t = [X_{p,t}, X_{m,t}, X_{n,t}]$$

Where, $X_{p,t}$ are the physical, operational and maintenance-related measurements, and features of network and cybersecurity respectively. XGBoost is used start off with feature importance estimation and feature selection. Transportation data might include a lot of irrelevancies or correlated data, which makes it hard to calculate and make decisions from the data and might also make it difficult for the model to generalize. XGBoost computes the importance of the attributes to the fault and attack discrimination.

Step -2: The estimated health condition can be expressed as

$$H_t = f_{\theta}(X_{p,t}, X_{m,t})$$

Where, f_{θ} is the model that has been learned using the predictive model. The health indicator's changes over time are analysed for progressive degradation. The anomaly detection mechanism also compares abnormalities in the observed behavior to learned normal operating patterns. Observations are passed on for further fault and security analysis if they are greater than the learned threshold for anomalies.

Step -3: BiLSTM is employed to capture temporal dependencies within sequential measurements

$$H_t = [h_t; h_t]$$

Would enable the model to learn complex patterns relating to the deterioration of the components and communication behaviour changes over time.

Step -4: These influential temporal observations are then given more weight in Step -4, an attention mechanism:

$$C = \sum T_{at} H_t$$

The architecture of this model is shown in Figure 2, in which the attention weight α_t is used to weight the context representation C .

Step -5: RUL estimation. Failure probability is expressed as

$$PF = P(F | X_p, X_m)$$

While the regression branch that estimates the RUL is based on the RUL.

$$RUL = f_{RUL}(C)$$

The number that indicates the duration of the component's operation when the failure condition is reached, as predicted. These outputs are used to determine the maintenance needs, without causing an unexpected breakdown of

the equipment. The cybersecurity module consists of an analysis of the characteristic of the network traffic and vehicular communication for intrusion detection. The analysis of abnormal packet behaviour, communications frequency, connection nature, protocol activities and message patterns enables the detection of denial-of-service, spoofing, false-data injection, unauthorized access, communication manipulation, etc. attacks.

Step -6: The attack probability is estimated as

$$PA = P(A | Xn)$$

Step -7: Softmax classification layer:

$$Y = \text{Softmax}(WcC + bc)$$

$$Y \in \{\text{Normal}, \text{Physical Fault}, \text{Cyberattack}, \text{Fault} + \text{Attack}\}.$$

Therefore, the proposed XGBoost–BiLSTM–Attention method offers a single framework for assessing the health of the equipment, detecting anomalies, predicting failures, estimating RUL, detecting intrusions, and classifying attacks. These predictions are the basis for the joint cyber-physical decision mechanism that allows the ITS to decide whether the degradation is a natural phenomenon or an attack and take the necessary actions, such as maintenance, security or combined.

5. Results and Discussion

The experimental results validate the proposed XGBoost–BiLSTM–Attention framework to be effective in the integrated predictive maintenance and cybersecurity in ITS. Failure prediction and remaining useful life (RUL) estimation, cyberattack detection and joint cyber-physical classification are evaluated. The proposed approach is compared to: LR, SVM, RF, XGBoost, LSTM and BiLSTM. The predictive maintenance module is a very good solution to deduce deterioration of equipment based on a series of operational data. The LR and SVM have poor performance in capturing the nonlinear

Table 2
Comparative Performance Analysis of Machine Learning and Deep Learning Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
LR	90.42	89.76	89.31	89.53
SVM	92.18	91.65	91.27	91.46
RF	94.36	93.91	93.58	93.74
XGBoost	95.82	95.37	95.06	95.21
LSTM	96.71	96.28	96.13	96.20
BiLSTM	97.48	97.11	96.94	97.02
Proposed XGBoost–BiLSTM–Attention	98.63	98.31	98.17	98.24

temporal behaviour, while the RF and XGBoost have better fault detection performance. LSTM and BiLSTM then learn about the degradation patterns that evolve over time, to further improve accuracy. Proposed XGBoost–BiLSTM–Attention model outperforms the rest by performing efficient feature selection, temporal learning and identifying critical degradation pattern by paying attention to important features.

The improvement suggests that combining feature importance with temporal modelling is a good approach to detect early equipment deterioration. Attention further allows the model to pay more attention to the operating intervals that include more degradation information. The RUL estimation can be used to estimate the remaining life of an ITS component until it reaches the failure state. For evaluating the proposed model, we have used MAE, RMSE and R2. The lower the value of MAE and RMSE, the more accurate the prediction while the higher the value of R2, the more agreement there will be between the predictions and the actual RUL. The trend of the current improvement can be noted from the conventional classifiers to temporal deep-learning classifiers. The SVM and RF models increasing the performance of the accuracy and the F1-score, respectively; LR model has the lowest values of 90.42% and 89.53%. With the nonlinear feature learning as shown in Table 2, XGBoost is able to further enhance the accuracy with 95.82%. Including the time information in equipment-health and cyber-physical observations is found to significantly improve the accuracy of the models, with the LSTM and BiLSTM models having 96.71% and 97.48% accuracy, respectively. The proposed XGBoost–BiLSTM–Attention model is the most accurate one with an accuracy of 98.63% and F1 score of 98.24%. It is worth noting how comparatively little the difference between its accuracy and F1-score is, which also means that it made balanced classifications. The results confirm the benefits of using feature selection, bi-directional temporal learning and attention-based feature weighting to accurately assess the condition of an ITS.

Table 3
Comparative Regression Performance Analysis of Machine Learning and Deep Learning Models

Model	MAE	RMSE	R2
RF	18.42	23.16	0.912
XGBoost	15.37	20.24	0.936
LSTM	12.68	17.31	0.957
BiLSTM	10.94	15.26	0.968
Proposed Model	8.73	12.41	0.981

The proposed approach achieves lower prediction error because it can learn the relationship of the features in a nonlinear manner and learn the temporal degradation behaviour. The better that RUL can be estimated, the more accurate the timing will be for maintenance interventions, leading to a decrease in unnecessary maintenance and possible failure.

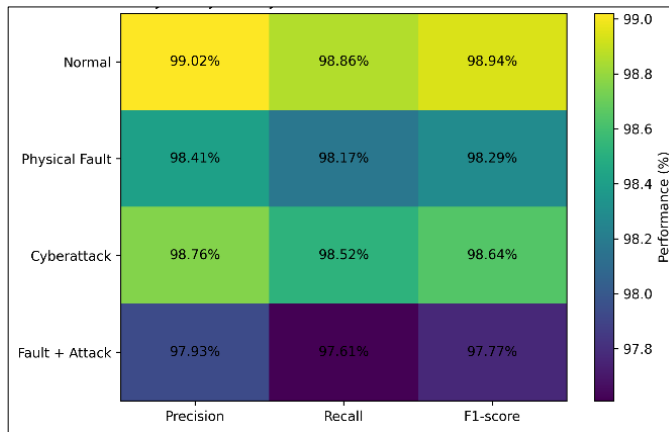


Figure 2

Performance matrix of the proposed model for normal, physical fault, cyberattack, and combined fault–attack conditions

The precision, recall and F1 Score, shown in Table 3 that are achieved in the four operating states of the cyber-physical system by the proposed model are presented in 2. The normal state obtains the highest precision, recall and F1-score of 99.02%, 98.86% and 98.94% respectively, which means that it is able to accurately recognize the ITS operation. The proposed architecture obtains F1-scores of 98.29% and 98.64% for physical fault and cyberattack events, respectively, showing that the architecture is able to successfully distinguish between the two classes. The condition of both fault and attack yielded relatively good (97.93%, 97.61%, and 97.77% respectively) values of precision, recall and F1-score. This decrease is anticipated due to the possibility of the cyber-physical attributes being common to multiple attacks and degradation. Despite challenging performance in each of the four states, the overall performance is excellent, showing the utility of the joint feature learning to distinguish naturally occurring equipment failures from intentionally injected cyber-attacks that is a key goal in the proposed maintenance/security co-design framework.

6. Conclusion and Future Work

This study introduced a framework of AI-driven Predictive Maintenance (PM) and Cybersecurity (CS) co-design as a way to enhance the reliability, security and resilience of Intelligent Transportation Systems (ITS) by fusing operational and equipment-health, maintenance, and network-security data. The XGBoost–BiLSTM–Attention model involves feature selection, temporal learning, and attention mechanism to enable the identification of health assessment, fault prediction, RUL estimation, anomaly detection, intrusion detection, and cyber-attack identification. Its major function is the ability to classify the various operating conditions—normal operation, physical fault,

cyber-attack and simultaneous fault-attack – to decrease false maintenance and security alarms. The built-in risk assessment allows for risk coordination and the subsequent maintenance and cybersecurity responses. Experimental analysis is conducted to assess the performance of the proposed method when compared to the conventional method, showing better results in terms of fault prediction, RUL estimation and cyber-physical state discrimination. The edge computing, federated learning, explainable AI, adaptive threat detection and real world ITS validation are among the areas that will be explored for future studies.

References

- [1] S. Fernandes, M. Antunes, A. R. Santiago, J. P. Barraca, D. Gomes, and R. L. Aguiar, “Forecasting appliances failures: A machine-learning approach to predictive maintenance,” *Information*, vol. 11, Art. no. 208 (2020).
- [2] M. Călin, D. T. Cotfas, and P. A. Cotfas, “A review of smart photovoltaic systems which are using remote-control, AI, and cybersecurity approaches,” *Appl. Sci.*, vol. 14, Art. no. 7838 (2024).
- [3] A. Mohanty, K. N. R. Praveen, P. Mahalle, K. S. Rao, and A. S. Kumar, “Investigating time-sensitive security threats and their impact on networked communication systems in real-time environments,” *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 2-A, pp. 421–428 (2025), doi: 10.47974/JDMSC-2473.
- [4] M. Han, S. Liu, S. Ma, and A. Wan, “Anonymous-authentication scheme based on fog computing for VANET,” *PLoS ONE*, vol. 15, Art. no. e0228319 (2020).
- [5] S. Suman, D. Chatterjee, and R. Mohanty, “Power quality improvement for microgrid-connected PV-based converters under partial shading conditions using mixed optimisation algorithms,” *Int. J. Bio-Inspired Comput.*, vol. 21, no. 3, pp. 123–136 (2023), doi: 10.1504/IJBIC.2023.131918.
- [6] C. Özarpa, İ. Avcı, and B. F. Kınacı, “Critical level analysis of subsystems used in smart rail systems,” *J. Railw. Eng.*, vol. 14, pp. 143–153 (2021).
- [7] X. Jin, C. Feng, D. Ponnamma, Z. Yi, J. Parameswaranpillai, S. Thomas, and N. V. Salim, “Review on exploration of graphene in the design and engineering of smart sensors, actuators and soft robotics,” *Chem. Eng. J. Adv.*, vol. 4, Art. no. 100034 (2020).

- [8] S. Aldhaheri, D. M. AlGhazzawi, L. Cheng, B. A. Alzahrani, and A. Al-Barakati, "DeepDCA: Novel network-based detection of IoT attacks using artificial immune system," *Appl. Sci.*, vol. 10, Art. no. 1909 (2020).
- [9] H. M. Mohi, I. Z. Mushttt, M. Z. Salman, and H. A. Mohamad, "Sufficient conditions for the oscillation of solutions of third-order neutral difference equations with alternating coefficients," *J. Interdiscip. Math.*, vol. 29, no. 5-A, pp. 1085–1090 (2026), doi: 10.47974/JIM-2287.
- [10] M. Rafat and S. Azadi, "A novel flexible lane changing (FLC) method in complicated dynamic environment for automated vehicles," *J. Appl. Comput. Mech.*, vol. 9, no. 2, pp. 318–331 (2023), doi: 10.22055/JACM.2021.36276.2818.
- [11] H. Bangui and B. Buhnova, "Recent advances in machine-learning driven intrusion detection in transportation: Survey," *Procedia Comput. Sci.*, vol. 184, pp. 877–886 (2021).
- [12] J. L. C. Choy, J. Wu, C. Long, and Y.-B. Lin, "Ubiquitous and low power vehicles speed monitoring for intelligent transport systems," *IEEE Sens. J.*, vol. 20, no. 11, pp. 5656–5665 (2020), doi: 10.1109/JSEN.2020.2974829.
- [13] E. Cheek, H. Alghodhaifi, C. Adam, R. Andres, and S. Lakshmanan, "Dedicated short range communications used as fail-safe in autonomous navigation," in *Unmanned Systems Technology XXII*, vol. 11425, Art. no. 114250P (2020), doi: 10.1117/12.2558925.

Received March, 2026