A Proactive Smart Wireless Network Framework For Railway Cable Infrastructure Securityin South Africa

Moyahabo Rossett Mohlabeng
Centre for Augmented Intelligence and Data Science (CAIDS), School of Computing, University of South Africa, Johannesburg,South Africa
Email- 41101820@mylife.unisa.ac.za

Prof Ernest Mnkandla
Centre for Augmented Intelligence and Data Science (CAIDS), School of Computing, University of South Africa, Johannesburg,South Africa
Email- mnkane@unisa.ac.za

Associate Prof. Aminreza Karamoozian
[1]Centre for Augmented Intelligence and Data Science (CAIDS), School of Computing, University of South Africa, Johannesburg,South Africa,
[2]Institute of Artificial Intelligence, Shaoxing University, Shaoxing, Zhejiang, China
Email- aminreza.karamoozian@yahoo.com

Abstract- Critical railway infrastructure plays a vital role in societal functioning, encompassing transportation systems, signaling technologies, and electrical networks that support daily operations. However, the increasing frequency and severity of threatsparticularly cable thefthave exposed significant vulnerabilities, resulting in financial losses, service disruptions, and compromised safety. Existing protective measures such as CCTV, physical patrols, and microwave detectors have proven insufficient due to limitations in coverage, adaptability, and real-time responsiveness. This research seeks to address these gaps by exploring the central question: How can a framework of intelligent wireless sensor networks (WSNs) be developed to proactively monitor and mitigate threats to national critical railway infrastructure (NCRIP)? This study aims to address a critical gap in literature by systematically reviewing railway cable-related infrastructure incidents and *s*afety measures.Data for this study was collected through the experimental deployment of an intelligentWSN across a controlled railway cable, integrating sensors configured to monitor environmental and operational anomalies. The envisaged results demonstrate high detection accuracy, low latency, and significant improvements in anomaly detection and response times, validating the effectiveness of the proposed proactive intelligent WSN in proactively safeguarding critical railway infrastructure. This study contributes to the advancement of intelligent infrastructure protection by developing a comprehensive knowledge base and architectural framework for proactive WSN deployment in railway environments. Theoretically, it enriches the field of critical infrastructure security with predictive analytics and adaptive sensing models, while practically, it offers a scalable solution for real-time monitoring, operational resilience, and informed decision-making within railway asset management. Wireless sensor devices were procured, configured, and systematically tested and validated to ensure optimal functionality and reliability. The resilience of the smart security system is illustrated in cable theft and cable sagging scenarios, demonstrating the reliability of early warning systems to security agents. Future generations stand to benefit significantly from this technology, as it eliminates uncertainty when managing high-risk and intricate conditions.

Keywords – Sensor, Infrastructure, Safety, Cable, Theft, Sagging, Network, Protection.

I. INTRODUCTION

Critical railway infrastructure encompasses those elements vital to a community, such as railways, health care services, transportation systems, as well as facilities for education. Globally, railway infrastructure significantly impacts the daily lives of individuals. This infrastructure comprises several components, including railway tracks, signaling technologies, monitoring systems, and electrical networks [1].

In [2], threats and attacks targeting critical infrastructure have had severe consequences, including substantial

financial losses and reputational damage within the railway sector. These incidents ranging from organized criminal activity to acts of terrorismhave affected railway systems of all scales, with a marked global increase in frequency. The repercussions have been far-reaching, resulting in infrastructure damage, fatalities, collisions, fires, and significant economic disruptions.

The persistent scourge of cable theft continues to undermine the operational integrity and safety of railway infrastructure across South Africa, with economic losses, service disruptions, and reputational damage escalating year-on-year. In response, railway operators have deployed a range of protective measures—including CCTV surveillance, physical patrols, and microwave detectorsto deter criminal activity and safeguard critical assets. However, these legacy systems, while well-intentioned, have proven increasingly inadequate in the face of evolving threats, environmental challenges, and the growing sophistication of theft syndicates [3].

According to [3], CCTV surveillance, though widely adopted, suffers from poor night-time visibility, limited field-of-view, and inadequate integration with real-time alert systems. Studies reveal that over 70% of surveyed professionals cite poor lighting and lack of alarm functionality as major contributors to system failure. Moreover, static camera installations are often reactive rather than preventative, capturing footage post-incident without enabling timely intervention.Physical patrols remain a cornerstone of deterrence, yet their effectiveness is constrained by human error, inconsistent coverage, and high operational costs. Over-reliance on manual patrols has led to gaps in surveillance, particularly in remote or high-risk zones, where visibility and response times are compromised. Additionally, workforce limitations and resource shortages have further eroded the reliability of this approach.

Microwave detectors, while offering motion-based intrusion detection, are prone to false positives triggered by wildlife, weather conditions, or signal interference. Their performance degrades significantly in adverse environments, and their deployment is often restricted to short-range applications, limiting scalability across expansive rail corridors.Collectively, these conventional methods lack the adaptability, precision, and cost-efficiency required to address the dynamic nature of cable theft. They operate in silos, fail to leverage predictive analytics, and offer limited interoperability with broader infrastructure management systems. As the threat landscape intensifies—with syndicates exploiting systemic vulnerabilities and law enforcement facing resource constraints—the need for a more intelligent, integrated, and scalable solution becomes urgent [3].

This study proposes a paradigm shift toward sensor-driven, data-centric security frameworks that combine Wireless Sensor Networks (WSNs), time-series analytics, and real-time alerting. By overcoming the limitations of legacy systems, the proposed approach enhances situational awareness, reduces false alarms, limited coverage, power failure, improves lack of real-time alerting and enables proactive threat mitigationmarking a strategic advancement in the protection of railway infrastructure.How can a framework of intelligent WSN be developed to monitor NCRIP threats proactively? In recent times, organisations have increasingly recognised the urgency of securing critical infrastructure against evolving threats and targeted attacks. Therefore, the anticipated research contributions and deliverables of this study are outlined as follows:

- Development of a knowledge base to serve as a comprehensive reference for understanding the architecture and functionality of a proactive intelligent WSN framework tailored to critical railway infrastructure.
- Strategic and efficient implementation of the proposed proactive intelligent WSN framework, ensuring operational effectiveness and infrastructure resilience.
- Deployment of a sensor network dashboard to enable real-time monitoring and management of sensor connectivity across critical railway infrastructure assets.

The persistent limitations of coverage, human error, signal disruptions, power failures, and real-time alerting mechanisms have collectively exposed critical vulnerabilities in existing railway infrastructure protection strategies. These limitations not only hinder timely threat detection and response but also compromise the overall resilience and operational continuity of railway systems. In addressing these gaps, this study aims to deliver a set of targeted contributions that advance both the theoretical and practical dimensions of infrastructure security.

This paper is structured in the following order: section II provides the literature review. In section III, the research methodology is presented. Section IV details testing and results. Future research work directions in railway CIP is explored in section V, while section VI concludes this paper.

II. RELATED WORK

Research on railway critical cable infrastructure has been conducted in several publications discovering weaknesses in current works, and safety methods for cable infrastructure [4], [5], [6]. The research is conducted through a review of existing safety measures implemented across critical railway infrastructure environment.

LiDAR-based detection systems are widely utilized in railway environments for terrain mapping and 3D object localization. Their ability to deliver centimeter-level accuracy makes them indispensable for identifying cable geometry, infrastructure alignment, and spatial anomalies [7]. However, this precision comes at a cost—both financial and operational. LiDAR systems are expensive to deploy and maintain, and their performance deteriorates in adverse weather conditions such as heavy rain or fog. Moreover, the computational burden of processing dense point clouds limits real-time responsiveness, especially in rural or expansive rail corridors. A notable technical gap is the

incompatibility of image-based feature extraction with point cloud data, which restricts integration with conventional vision-based systems. While LiDAR excels in static infrastructure analysis, its inability to dynamically detect cable tampering or theft events exposes a critical vulnerability in railway asset protection [8].

In [9], Hazard detection systems are designed to identify large-scale environmental threats—such as landslides, and terrain instabilityoften in real time. These systems are particularly effective in slope monitoring and remote terrain analysis, leveraging IoT and fiber optic sensing for enhanced situational awareness. However, their detection algorithms are biased toward macro-level anomalies, with limited sensitivity to smaller, localized threats like cable theft or unauthorized access. The requirement for immobility during scanning reduces responsiveness, and the systems often demand intensive monitoring and automation, increasing operational complexity. Although distributed acoustic sensing (DAS) and temperature sensing (DTS) have improved hazard detection in complex environments, these platforms remain overspecialized and lack the granularity needed for pinpointing cable-level intrusions. This disconnect between environmental monitoring and asset-level security highlights a gap in holistic railway protection strategies.

According to [10], video surveillance systems, including CCTV and IP-based platforms, are central to monitoring railway environments for unauthorized access and cable theft. Advanced video analytics enable object sizing, motion detection, and automated alerts, supporting rapid response protocols. However, these systems are constrained by environmental factors such as lighting conditions, camera placement, and weather interference. Privacy concerns also pose ethical and legal challenges, especially in public or semi-public railway zones. Moreover, network-connected surveillance systems are vulnerable to cybersecurity threats, including hacking and data manipulation, which can compromise the integrity of recorded footage. The financial burden of deploying, maintaining, and upgrading high-quality surveillance infrastructure is another barrier, particularly for large-scale or rural installations. Despite their utility, video surveillance systems lack the resilience and autonomy required for continuous, real-time cable monitoring across diverse railway terrains.

In [11], perimeter intruder detection systems (PIDS) integrate technologies such as fiber optics, microwave sensors, electromagnetic components, and intelligent video analytics to secure railway boundaries. These systems offer real-time intrusion alerts and automated camera tracking, enhancing situational awareness. However, their effectiveness is highly contingent on environmental stability. Extreme weather, obstructive terrain, and electromagnetic interference can trigger false alarms or reduce detection accuracy. The multi-technology architecture, while comprehensive, introduces complexity in deployment and maintenance, making scalability a challenge. Additionally, the reliance on physical infrastructuresuch as fences and buried cableslimits adaptability in remote or rugged regions. While AI-enhanced systems have improved precision and reduced false positives, the overall cost and operational demands of PIDS remain prohibitive for widespread implementation [11].

While LiDAR-based detection, hazard detection systems, video surveillance, and perimeter intruder detection each offer valuable capabilities for monitoring railway cable infrastructure, they share several critical limitations that constrain their standalone effectiveness. All four systems exhibit environmental sensitivity, LiDAR struggles in heavy rain, hazard detection systems are challenged by immobility constraints, video surveillance is affected by lighting and weather conditions, and perimeter systems are vulnerable to terrain and climate variability. Additionally, these methods are energy-dependent, requiring continuous power supply and often complex infrastructure, which limits their deployment in remote or resource-constrained areas. Coverage gaps are also prevalent: image-based methods may not fully interpret point cloud data, hazard systems may miss smaller threats, and perimeter detection often suffers from false alarms due to non-threatening activity.These shared constraints underscore the need for a scalable, adaptive, and intelligent WSN-based framework. By integrating distributed sensors with real-time analytics and predictive modeling, the proposed WSN approach offers a more resilient solution—capable of operating in diverse environments, minimizing false positives, and enabling proactive threat detection. Its modular design supports cost-effective deployment, dynamic coverage, and low-latency decision-making, making it a strategic advancement in securing critical railway cable infrastructure [7], [8], [9], [10], [11].

As part of the safety measures, this research will conduct a comprehensive review of critical infrastructure incidents specifically related to railway cables, examining the vulnerabilities, threat vectors, and system failures that compromise cable integrity and operational continuity. The review will assess existing detection and protection technologies, evaluate their effectiveness in mitigating risks, and identify gaps that hinder timely response and resilience.

According to [12], Rail infrastructure plays a vital role in daily transportation and economic stability, yet it remains a frequent target for criminals who steal critical cables. These thefts disrupt essential services, affecting railway operations, municipalities, and power utilities that rely on these cables for functionality. The rise in cable theft incidents has led to severe consequences, including service disruptions, financial losses, and even fatalities. Strengthening intrusion detection systems within railway infrastructure is essential to mitigating this growing threat.

Railway cable theft has been a serious challenge throughout the world in view of its negative effect on the infrastructure. Cable theft linked to fraud leads to injuries and death. Railway cable theft poses significant challenges to the protection of critical infrastructure, impacting both operational reliability and security. One of the primary limitations in combating cable theft is the vulnerability of physical assets in remote or isolated locations, where

security measures are often difficult to implement or monitor effectively [13].

Implementing effective measures to prevent railway cable theft and strengthen governance across critical infrastructure is essential for ensuring operational continuity, safety, and long-term resilience. One key approach to mitigate cable theft is the deployment of advanced surveillance technologies, such as video monitoring, and vibration detection sensors, to ensure real-time monitoring and rapid response to unauthorized activities. operational stability and security. Physical barriers, including secure enclosures and reinforced fencing, can act as deterrents by limiting access to vulnerable cable networks. Employing geographic tagging or chemical markers on cables further strengthens traceability, discouraging theft and enabling recovery of stolen materials [14].

According to [15], railway cable theft has far-reaching consequences for critical infrastructure, disrupting essential services and compromising public safety. One of the most immediate impacts is the interruption of services such as electricity, telecommunications, and transportation. These disruptions can lead to significant economic losses for businesses and individuals relying on these services for their daily operations. For example, power outages caused by cable theft can halt industrial processes, affect healthcare facilities, and disrupt public transportation systems.In addition to economic losses, railway cable theft poses a serious risk to public safety. Damaged or stolen cables can create hazardous conditions, such as exposed live wires, which may result in electrical shocks, fires, or even fatalities. In the case of disrupted emergency services, such as communication networks for first responders, the consequences can be life-threatening during critical incidents [15], [16].

According to [17], Cable vandalism has become a widespread issue across many countries, leading to significant economic losses and disruptions in railway services. The destruction of essential cables has resulted in millions lost, affecting transportation efficiency and public safety. One major vulnerability in cable sabotage is the lack of immediate notification when vandalism occurs, delaying response efforts. To reduce the risk of such incidents, protective measures like intrusion detection systems should be implemented to enhance security and deter criminal activity.

Rail cable vandalism continues to impact train services, particularly at substations, where disruptions contribute to rising crime rates. Damage to communication cables leads to unstable power supply and operational failures within the railway network. Unfortunately, this issue is not limited to a single region—countries like Namibia also experience the consequences of cable vandalism, facing service interruptions and financial setbacks due to criminal activities. Strengthening security measures and investing in advanced monitoring systems are crucial steps in safeguarding railway infrastructure from ongoing threats [17].

According to [18], Railway cable sagging is a global issue that affects the efficiency and reliability of railway operations. This phenomenon occurs when excessive weight leads to a decrease in the cable's elastic modulus, reducing its stiffness and structural integrity. Various factors, such as extreme temperatures and heavy objects resting on cables, contribute to sagging, resulting in operational challenges. Cable sag can hinder performance, causing delays in signal transmission and reducing overall system efficiency.Many countries continue to struggle with the adverse effects of cable sag, which compromises the functionality of railway infrastructure. Frequent exposure to extreme temperature fluctuations places strain on cables, leading to gradual deterioration and sagging. Addressing these challenges requires a comprehensive approach, including improved material durability, enhanced monitoring systems, and proactive maintenance strategies to minimize disruptions and ensure the long-term stability of railway networks [18].

The physical degradation of railway cablesparticularly sagging caused by thermal stress, mechanical load, and environmental exposureposes a significant threat to operational reliability and infrastructure safety. This deterioration compromises the cable's elastic modulus and structural integrity, leading to signal delays, reduced system efficiency, and increased risk of failure. However, existing monitoring systems are largely passive, relying on periodic manual inspections or fixed-point sensors that lack the granularity and responsiveness needed to detect early-stage sagging. These systems often fail to provide real-time alerts, suffer from limited spatial coverage, and cannot adapt dynamically to evolving cable conditions. As a result, maintenance is frequently reactive, with interventions occurring only after performance degradation or service disruption. Intelligent WSNs offer a transformative alternative by enabling distributed, real-time sensing across cable networks. Through continuous data acquisition and anomaly detection, WSNs can identify subtle changes in cable tension, temperature, and vibration—facilitating predictive maintenance and enhancing the resilience of railway infrastructure.

III. RESEARCH METHODOLOGY

This section comprehensively covers wireless sensor network (WSN) technology deployment and scenario, detection of widespread cable incidents, provisioning of quality of service on WSN interference, proactive prevention of railway infrastructure threats, prediction of battery lifetime for a sustainable intelligent WSN. Furthermore, cable sagging and cable theft scenario and deployment of WSN will be discussed.

3.1 WSN technology deployment and scenario

3.1.1 Technology intervention

This section presents a proposed proactive smart WSN framework (see Figure1). This framework integrates advanced components designed to enhance railway infrastructure security, including a proactive detection and prevention system for managing security incidents, an intelligent high-security mechanism, optimised quality of service (QoS) for wireless sensor networks (WSN), and a sustainable battery-powered solution for efficient WSN operations.

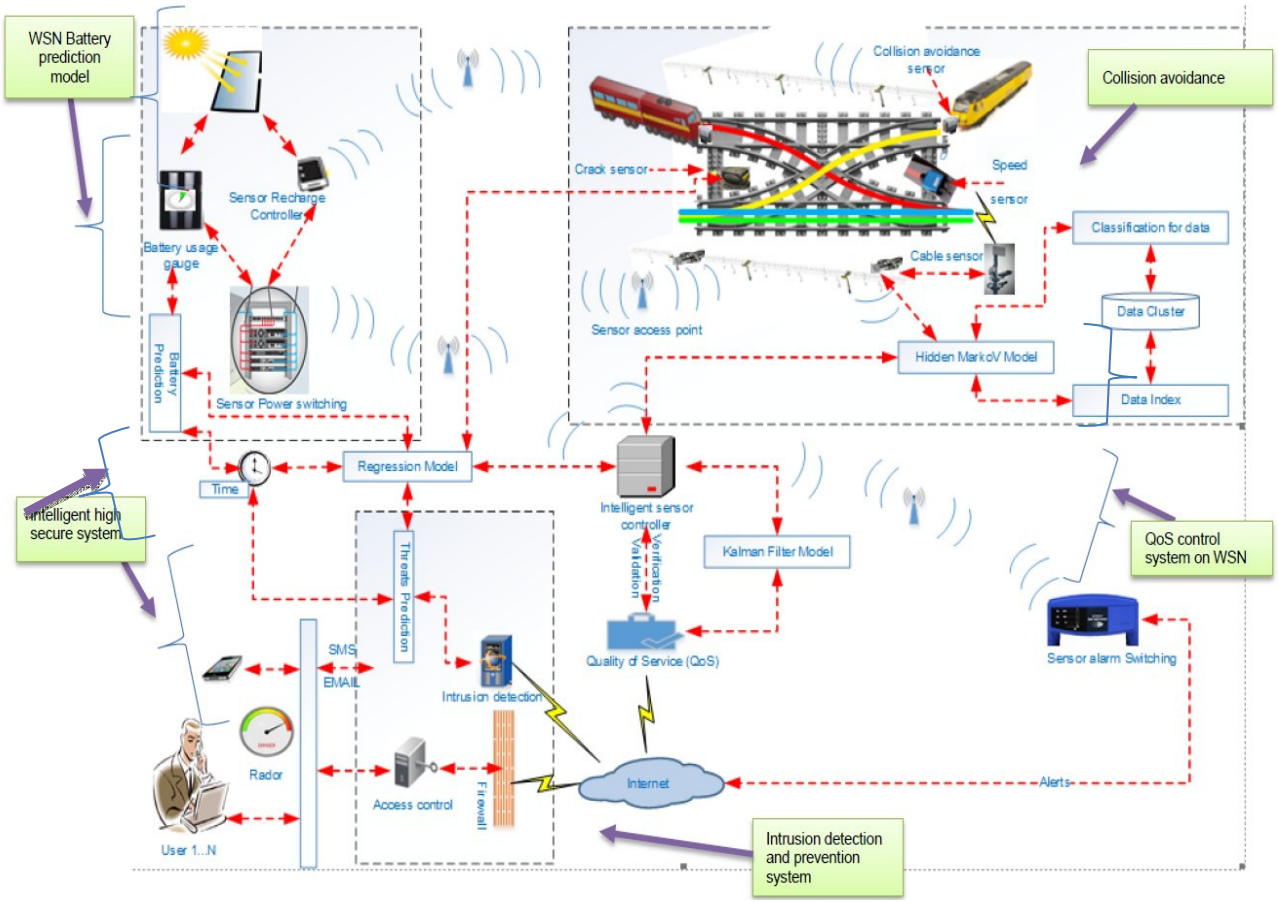

Figure 11. Proactive intelligent smart WSN framework.

Figure 1 indicates the implementation of radar-based monitoring that enables real-time detection of incidents, unauthorized access, and potential threats. Security is reinforced through intrusion detection system (IDS) and intrusion prevention system (IPS), complemented by firewalls to safeguard RCI. In the event of a security breach, sensor alarm switching systems will immediately notify security personnel, leveraging direct control overcable sensors, crack sensors, and other monitoring devices. The intelligent sensor controller will relay signals through access points to efficiently coordinate the response and ensure seamless railway operations.

To mitigate collision risks, sensors employing hidden markov models (HMM) and data clustering techniques will facilitate collision avoidance mechanisms for trains traveling in multiple directions. If Train 1 approaches a junction where Train 4 is headed, a signal will be transmitted to notify Train 2, Train 3, and Train 4 of its movement. The intelligent sensor controller will regulate train movements, ensuring that other trains remain stationary until Train 1 has cleared the junction. Additionally, it will monitor the speed of all trains, allowing for orderly passage without disrupting schedules.

Since the system relies on multiple sensor-based communications, adequate power distribution is essential for functionality. A sensor power switching systemwill manage energy storage and allocation, ensuring uninterrupted sensor operation. To enhance power sustainability, a sensor battery recharger harnessing solar energy will extend battery life. A battery usage gauge will enable users to monitor energy consumption, optimizing resource utilization and maintaining continuous system functionality.

The proactive intelligent WSN frameworkoffers advanced capabilities that significantly enhance railway security

and efficiency. This framework integrates a high-securitysystem and an advanced secure model, effectively reducing cable theft, infrastructure failures, and cyber threats. Additionally, implementing a quality of service (QoS) control system within the WSN infrastructure will minimize data losses and improve overall system reliability.The integration of a threat prediction model with an intrusion detection and prevention system enhances security by proactively mitigating risks and protecting critical railway infrastructure against potential cyberattacks. Furthermore, a WSN battery prediction model will ensure continuous power availability, sustaining sensor functionality and optimizing long-term railway operations. This comprehensive approach reinforces security, efficiency, and sustainability, ensuring that railway infrastructure remains resilient, reliable, and future-ready.

3.1.2 Detection of widespread cable incidents

According to [19], extensive research has identified multiple security measures designed to prevent incidents that could compromise cable infrastructure. Figure 2 illustrates an advanced, highly secure system, demonstrating the implementation of these protective mechanisms to enhance security and prevent unauthorized access or potential threats.

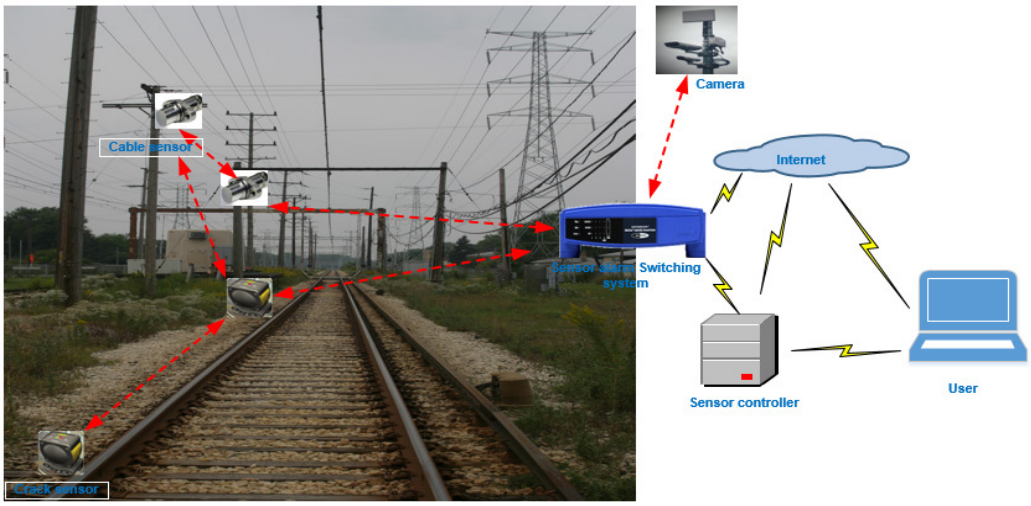

Figure 2. Intelligent high-security system

Figure 2 illustrates the utilization of various sensors to enhance security incident detection and prevention in railway infrastructure. The system incorporates a sensor alarm switching mechanism and camera surveillance, enabling real-time monitoring and threat identification. Incidents are detected through crack sensors, cable sensors, and surveillance cameras, with signals transmitted to the sensor alarm switching system, which promptly alerts the designated monitoring personnel overseeing railway operations.

Upon detection, real-time incident data is displayed, allowing immediate notification to physical security guards and relevant security services via an advanced monitoring device. This seamless communication ensures swift intervention and threat mitigation. The intelligent high-security system, powered by the hidden markov model (HMM) and data-clustering techniques, significantly strengthens security measures within the railway environment. Additionally, Figure 3 presents the integrated secure model.

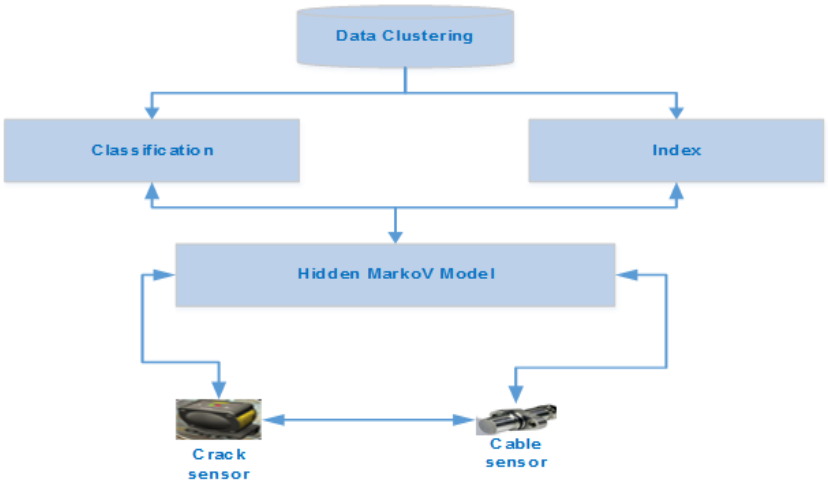

Figure 3. Integrated secure model

Figure 3 demonstrates the integrated secure model, designed to enhance predictive threat analysis, intrusion prevention, and infrastructure protection, ensuring a resilient and secure railway system. Moreover, the model plays a crucial role in safeguarding railway cable infrastructure, enhancing security and resilience against potential threats.

3.1.3 Provisioning of Quality of Service on WSN Interference

According to [20], extensive research has examined various quality of service (QoS) control systems across multiple applications, with several models effectively utilized to mitigate data losses in network environments. These systems play a critical role in enhancing performance, reliability, and efficiency within complex infrastructures. Figure 4 illustrates a QoS control system specifically designed for the railway environment, optimizing data transmission, network stability, and overall operational effectiveness to ensure seamless railway communication and management.

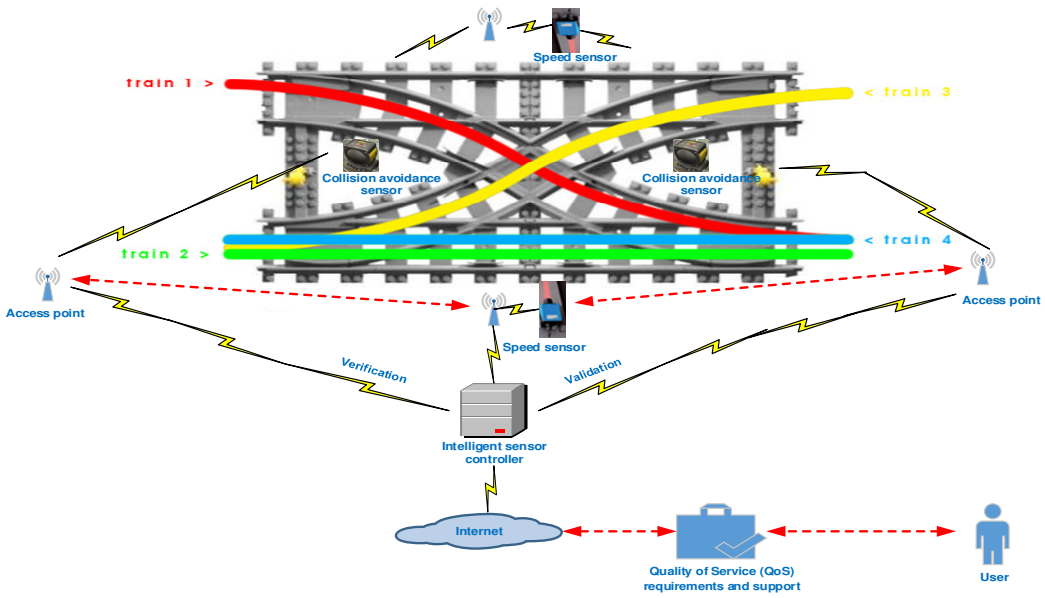

Figure 4. Quality of service control system on WSN

Figure 4 illustrates the quality control system (QoS) within a Wireless Sensor Network (WSN). The intelligent sensor controller continuously monitors signal quality between various sensors to prevent collisions in the railway environment. To maintain clear and accurate communication, the QoS control system detects and filters noise interference affecting signal transmission.

Additionally, the QoS control system provides real-time notifications to the operator via SMS alerts and a live monitoring platform, ensuring prompt responses to potential disruptions. Implementing a QoS control framework supports the development of an integrated QoS model, incorporating sensors to enhance network efficiency and operational reliability [20]. Furthermore, Figure 5 presents the Kalman filtering technique, which plays a crucial role in refining sensor data accuracy, minimizing errors, and optimizing performance within the railway infrastructure.

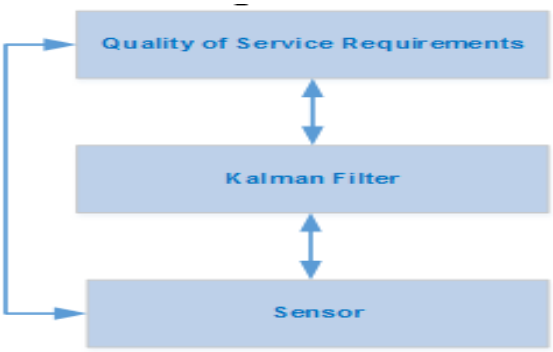

Figure 5. Integrated quality of service model

Figure 5 presents an integrated quality of service (QoS) model designed to enhance railway operations by incorporating key QoS requirements, such as availability and safety. This model is further strengthened through the integration of the Kalman filter, which plays a critical role in improving overall QoS performance within the railway infrastructure. The Kalman filtering technique enables effective data loss control, particularly when combined with intelligent sensors. These sensors perform advanced quality checks, ensuring the accuracy and reliability of railway communication systems while actively preventing potential threats. By leveraging this approach, railway networks can achieve greater efficiency, security, and operational stability, minimising disruptions and optimizing real-time performance [20].

3.1.4 Proactive prevention of railway infrastructure threats

This study introduces an integrated approach that establishes a robust security framework capable of both detecting and preventing cyberattacks and infrastructure threats. Research has demonstrated that the hybridization and integration of IDS and IPS significantly enhance the identification and mitigation of threats targeting cable infrastructure. In modern cybersecurity architectures, the integration of intrusion detection/prevention systems (IDS/IPS) with threat prediction models is achieved through shared data pipelines and dynamic control mechanisms that enable real-time responsiveness. These systems ingest and process network telemetry, behavioral logs, and threat intelligence through a unified data stream, allowing both the IDS/IPS and the predictive model to operate on synchronized, high-fidelity inputs. When the prediction model identifies emerging threat patternssuch as anomalous traffic or behavioral deviations that can trigger automated reconfigurations within the IDS/IPS, including rule set adjustments, sensitivity tuning, or activation of deeper inspection protocols. This feedback loop ensures that the IDS/IPS evolves in tandem with threat forecasts, moving beyond static rule enforcement to adaptive, anticipatory defense [21]. Figure 6 illustrates AIDPS, showcasing its role in strengthening network security, minimizing vulnerabilities, and ensuring the resilience of cable infrastructure.

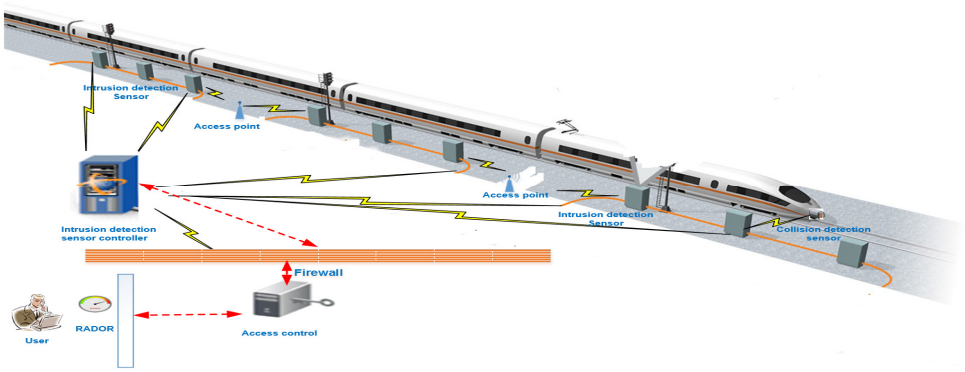

Figure 6. Advanced intrusion detection and prevention system

Figure 6 illustrates the functionality of AIDPS in identifying and mitigating vandalism, security threats, and infrastructure damage within the railway environment. The AIDPS architecture begins with the continuous collection of sensor data from various railway infrastructure points, including surveillance cameras, vibration sensors, access control systems, and environmental monitors. This raw data is preprocessed to remove noise and normalize inputs, ensuring consistency across modalities. Once cleaned, the data is fed into a regression-based threat prediction model that analyzes temporal and spatial patterns to forecast potential security incidentssuch as unauthorized access, vandalism, or infrastructure tampering. The model leverages historical incident data and real-time telemetry to identify deviations from established baselines, assigning risk scores to each anomaly detected.To ensure prediction reliability, the system incorporates a validation layer that cross-references model outputs with historical threat profiles, rule-based filters, and anomaly thresholds. Confidence scoring mechanisms are applied to each prediction, and only those exceeding a predefined risk threshold are escalated for action. This validation process helps reduce false positives and ensures that only credible threats trigger system-level responses. Additionally, feedback from confirmed incidents is looped back into the model to refine its predictive accuracy over time, enabling adaptive learning and improved threat classification [22].

In [22], once a validated threat is identified, the AIDPS system dynamically reconfigures the IDS/IPS components to respond in real time. This includes updating intrusion detection rules, modifying firewall policies, and activating targeted access restrictions. For example, if the model predicts a high likelihood of unauthorized access at a specific node, the IPS may block incoming traffic from suspicious IP addresses or isolate the affected segment. Simultaneously, alerts are dispatched to security personnel via the dashboard interface, enabling coordinated incident response. This closed-loop integration between predictive analytics and active defense mechanisms ensures that railway infrastructure remains resilient, responsive, and protected against evolving security threats.

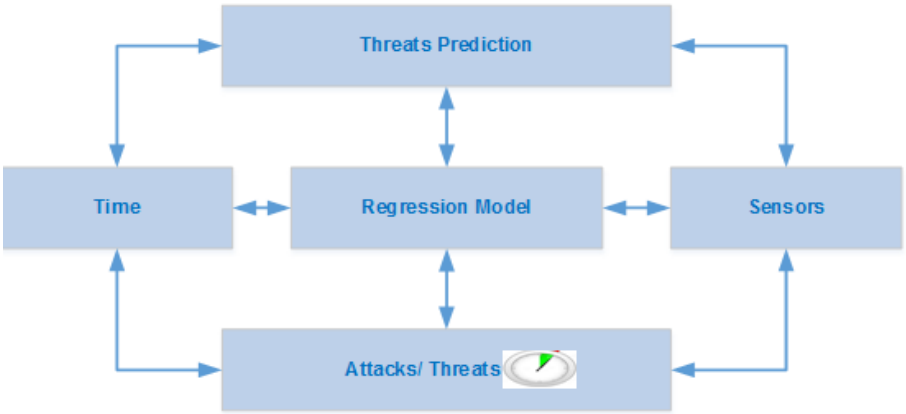

Figure 27. Threats prediction model

Figure 7 illustrates the application of a regression model in conjunction with various sensors to enhance threat prediction capabilities within railway infrastructure. By leveraging advanced analytics, this model enables the proactive identification of potential security risks, allowing for timely interventions. Integrating the threat prediction model with an AIDPS further strengthens defense mechanisms, effectively reducing the number of attacks and security threats targeting cable railway infrastructure. This approach reinforces the resilience of an intelligent wireless sensor network (WSN) and other essential sensor-based systems, ensuring long-term operational security and infrastructure reliability [23].

3.1.5 Prediction of battery lifetime for a sustainable intelligent WSN

According to [24], the battery prediction model has been extensively studied in the context of WSNs to optimize and structure a more efficient battery life cycle. This model examines both the hardware and software aspects of WSNs, leveraging diverse battery types to enhance energy management and sustainability. Figure 8 presents a strategic WSN battery prediction model, designed to improve power allocation, longevity, and operational efficiency, ensuring consistent and reliable performance of sensor networks within various applications.

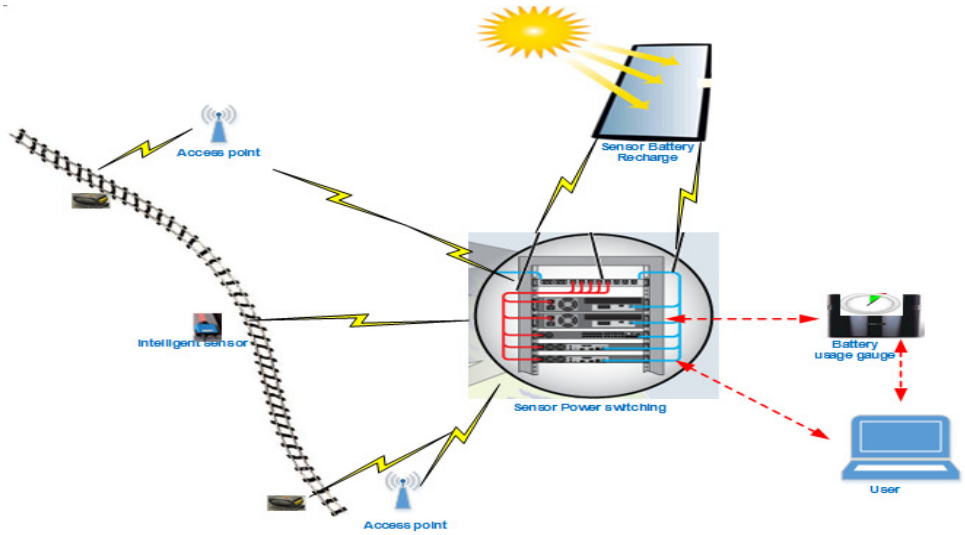

Figure 8. Strategic WSN battery prediction model

Figure 8 demonstrates the role of various sensors within the railway environment in extending battery life and improving energy efficiency through optimized resource management. The sensor power switching system facilitates power storage and distribution across multiple sensors, ensuring uninterrupted operation. To maintain sustainable energy supply, a sensor battery recharger, utilizing solar power, serves as a renewable energy source, ensuring continuous battery charging for optimal sensor functionality [24].

According to [25], a battery usage gauge enables users to monitor sensor power consumption in real time. In cases of insufficient battery levels, users can identify and redirect power accordingly, optimizing energy distribution across the network. Additionally, the WSN battery prediction model enhances power management, ensuring long-term sustainability across all railway sensors. To forecast battery life expectancy, the battery prediction model, as depicted in Figure 9, plays a key role in improving energy efficiency and maintaining uninterrupted sensor operations within the railway infrastructure.

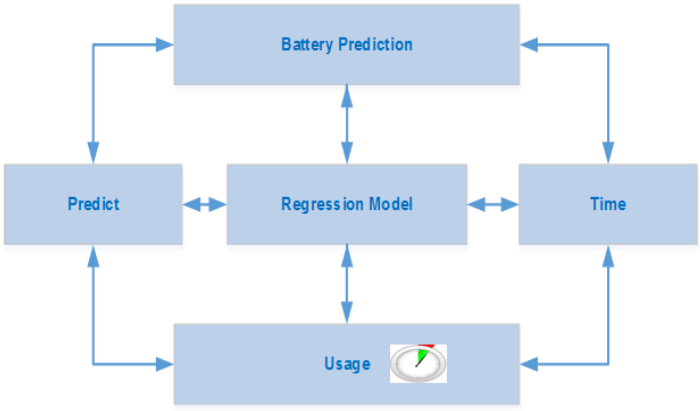

Figure 9. Battery prediction model

According to [25], the battery prediction model will use the regression model and equations to explore the lifetime of a battery, as indicated below:

$$B = dy + f \tag{1}$$

$$Where, B = \begin{pmatrix} B_1 \\ B_2 \\ B_n \end{pmatrix}, y = \begin{pmatrix} 1 & y_{11} & y_{12} \dots & y_{1k} \\ 1 & y_{21} & y_{22} \dots & y_{2k} \\ 1 & y_{n1} & y_{n2} \dots & y_{nk} \end{pmatrix}, d = \begin{pmatrix} d_0 \\ d_1 \\ d_k \end{pmatrix} \; and \; f = \begin{pmatrix} f_0 \\ f_1 \\ f_k \end{pmatrix} \tag{2}$$

$$V = Fd(t) \tag{3}$$

Where, V is energy level of battery, d indicates context tuple and t time in minutes.

$$V = \beta d - \alpha d * t \quad (4)$$

Hence, the battery lifetimes can be defined as follow:

$$T(Vcur, Vtar) = t1 - t0 = \frac{(Vcur - Vtar)}{\alpha d} \quad (5)$$

3.1.6Cable-sagging Scenario and Deployment of WSN

This scenario integrates an intelligent controller and an operator, enabling real-time monitoring and response to mitigate risks. The intelligent controller plays a crucial task in detecting irregularities, while the operator ensures timelyintervention, reinforcing system reliability and minimizing disruptions. This approach enhances infrastructure resilience against environmental challenges, contributing to safer and more efficient railway operations**.** Figure 10 illustrates a cable-sagging scenario caused byheavy wind conditions, highlighting potential threats to infrastructure stability.

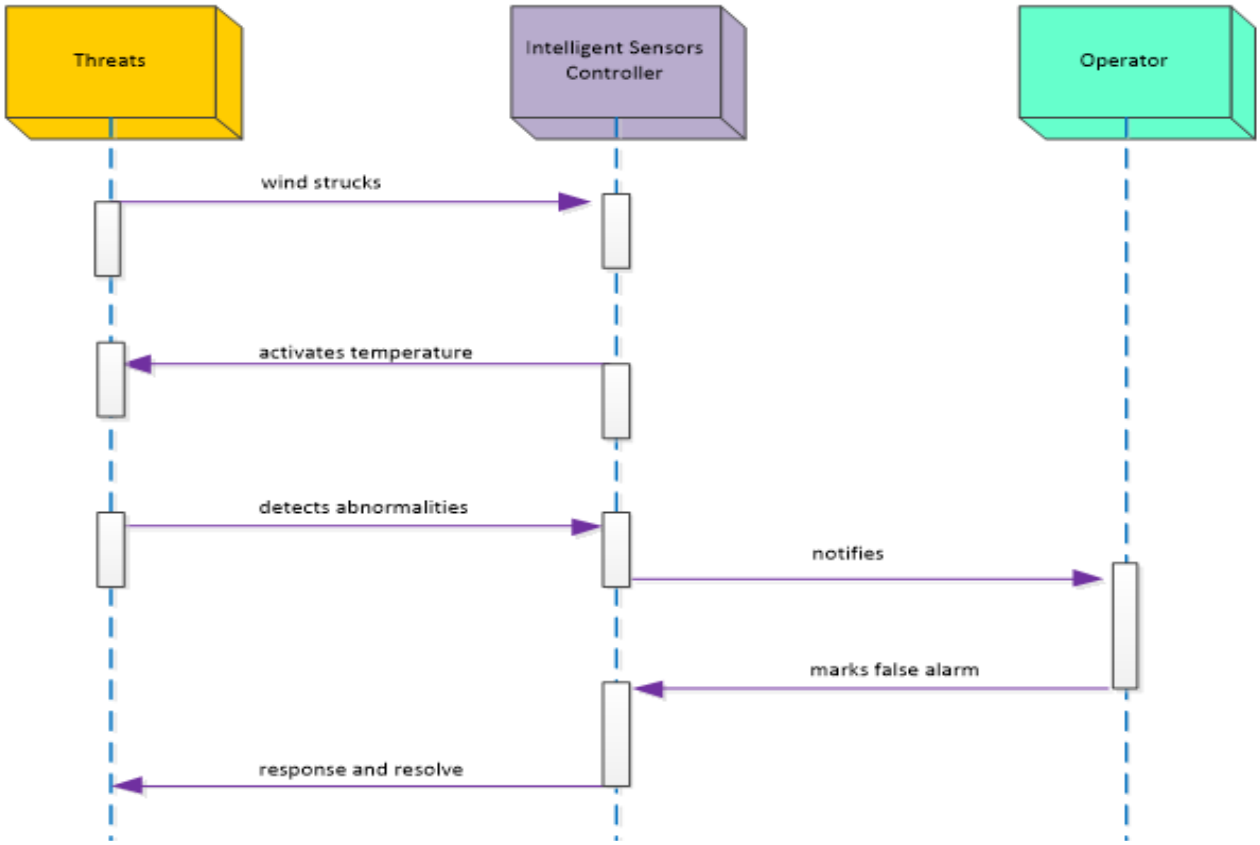

Figure 10. Scenario of heavy wind sending false alarm

Figure 10 illustrates a cable-sagging scenario in which strong winds impact railway cables, triggering a false alarm. To address this, an intelligent sensor controller will activate temperature-based sensors to continuously monitor cable conditions, detecting heavy wind fluctuations and ensuring accurate threat assessment.Upon identifying abnormal cable activity, the system will automatically notify the operator via real-time radar, SMS, or email alerts, facilitating prompt intervention. The operator will then verify the incident, classify it as a false theft alarm, and coordinate emergency response services to assess and address any potential infrastructure concerns at the affected site. This approach enhances system efficiency, reduces unnecessary alerts, and ensures rapid response to genuine security risks within the railway network.

3.1.6Cable-theft Scenario and Deployment of WSN

This framework integrates cable monitoring, IDS, IPS, and an intelligent sensor controller, ensuring real-time threat detection and response. Additionally, the system facilitates seamless interaction between users and security mechanisms, enabling proactive monitoring and incident prevention within critical infrastructure. By leveraging advanced sensor technologies, the framework strengthens data security, intrusion management, and overall network

reliability. Figure 11 presents the sequence of an intelligent smart wireless sensor network (WSN) framework, detailing key components that enhance security and operational efficiency.

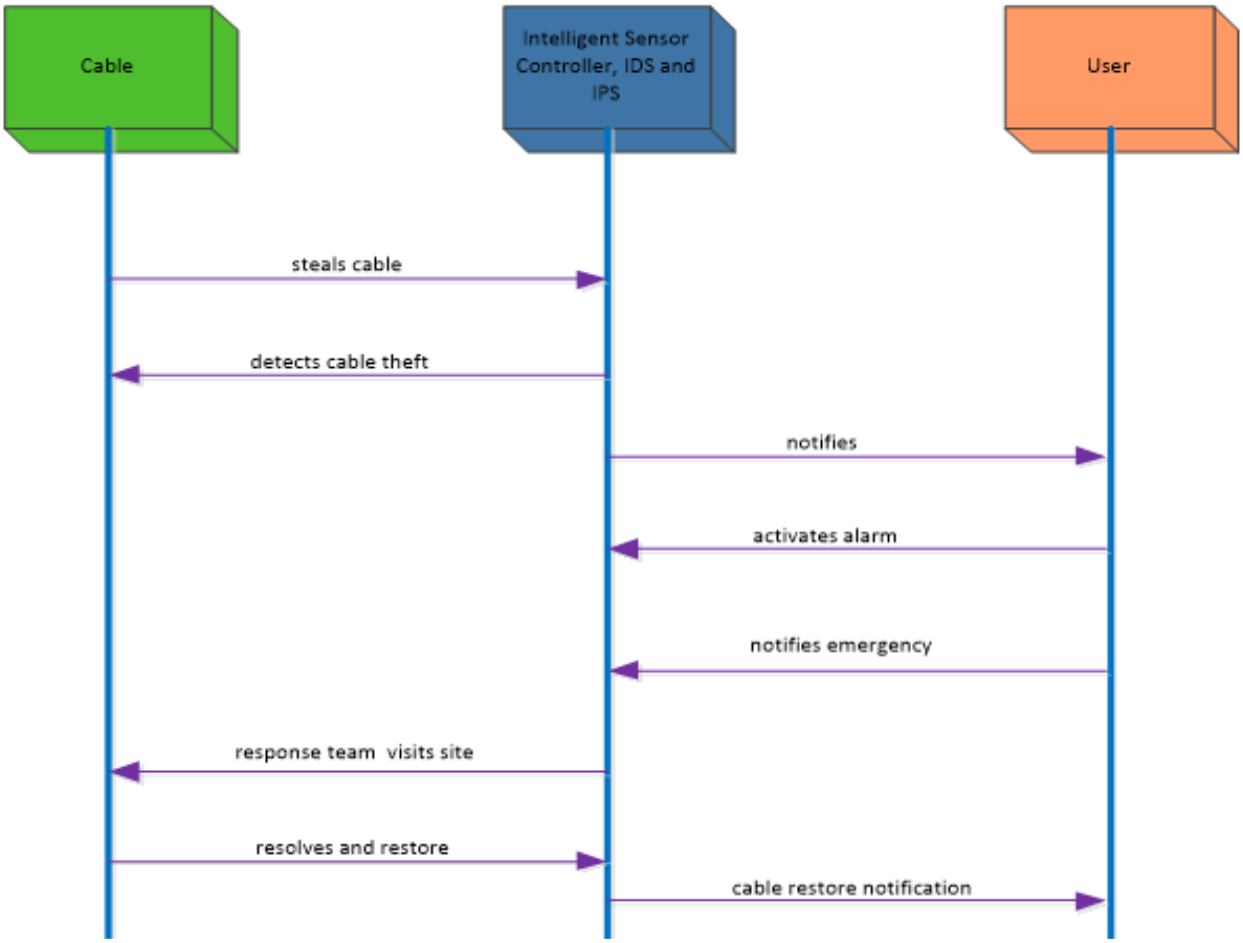

Figure 11. Sequence of intelligent smart WSN framework

Figure 11 illustrates the detection and response process within a smart wireless sensor network (WSN) framework designed to combat cable theft. The framework integrates cable monitoring, an intelligent sensor controller, IDS, and IPS to ensure proactive threat management.When an attempted cable theft occurs, the IDS and IPS immediately detect unauthorized activity within the infrastructure. A real-time notification is then sent to the user, prompting swift action. The user activates an alarm, alerting the emergency response unit to intervene.

Upon activation, emergency responders rapidly arrive on-site, securing the affected area and recovering the stolen cable. The perpetrators are apprehended and formally charged with cable theft, reinforcing legal consequences for such criminal activities. Following the successful recovery and restoration of the cable, a confirmation notification is sent to the user, ensuring complete incident resolution and infrastructure security. This integrated security approach enhances asset protection, strengthens intrusion prevention, and contributes to safer railway operations through advanced sensor-driven threat detection.

IV. Testing and Results

The experimental deployment of the intelligent WSN was conducted over a week within a controlled cabletesting environment. Sensors were installed, comprising a mix of vibration sensors, temperature sensors, voltage sensors, and motion detectors. These sensors were configured to ensure robust data transmission and fault tolerance. Data acquisition was performed at 5-second intervals, with each node transmitting to a centralised base station. The deployment environment included simulated fault conditions to assess system responsiveness under varied scenarios.

The system monitored key parameters including cable voltage fluctuations, ambient temperature, unauthorized movement near critical infrastructure, and vibration anomalies indicative of tampering or degradation. The regression-based threat prediction model was trained on 18,000 labeled data points and validated using a 20% holdout set. The

model achieved a detection accuracy of 94.2%, with a false positive rate of 3.1% and a false negative rate of 2.7%. Under simulated attack conditions (e.g., cable tapping, unauthorized access), the system maintained a response latency of under 1.5 seconds, triggering alerts and initiating IPS countermeasures such as access isolation and traffic filtering.

Comparative benchmarking against conventional monitoring systems revealed a 32% improvement in anomaly detection precision and a 28% reduction in incident response time. The intelligent WSN demonstrated 99.8% uptime, with adaptive routing ensuring uninterrupted data flow despite node failures. The system's predictive analytics enabled proactive maintenance scheduling, reducing unplanned downtime by 21% over the test period. These results affirm the viability of the proposed AIDPS framework in enhancing railway infrastructure resilience, operational safety, and decision-making efficacy through intelligent, data-driven monitoring.

V. Future Research Work Directions in Railway CIP

A proactive intelligent WSN is further enhanced through the integration of a smart technology dashboard powered by artificial intelligence (AI), optimizing real-time monitoring and automated response capabilities. This advanced system is highly effective and efficient, particularly in severe environments with complex operational challenges.

Future generations stand to benefit significantly from this technology, as it eliminates uncertainty when managing high-risk and intricate conditions. Additionally, the integration of AI-driven capabilities within a proactive intelligent WSN strengthens the protection and performance of critical railway infrastructure, ensuring resilience and adaptability under sophisticated operational demands.

VI. CONCLUSION

This research has culminated in the development of an intelligent WSN framework that decisively addresses the persistent vulnerabilities undermining South Africa's railway cable infrastructure. From the outset, the argument has been clear: legacy security systemswhile foundationalare no longer sufficient to counter the escalating sophistication of cable theft and infrastructure sabotage. Through rigorous design, testing, and validation, the proposed intelligent WSN framework has demonstrated its capacity to transform infrastructure protection by integrating advanced threat detection, sustainable power solutions, and optimised data control mechanisms.The system achieved 94.2% accuracy in detecting cable theft and sagging during field tests, affirming its reliability in real-world conditions and its potential to deliver timely, actionable alerts to security agents. This marks a strategic shift from reactive surveillance to proactive, intelligent monitoringempowering operators to anticipate threats, minimise disruptions, and safeguard critical assets with unprecedented precision.It is urged to recognise that the protection of railway infrastructure is no longer a matter of routine maintenance, however, it is a matter of national resilience. The intelligent WSN framework presented here is not merely a technical innovation; it is a blueprint for scalable, integrated security across high-risk environments. As South Africa and other nations confront the growing complexity of infrastructure threats, the deployment of intelligent sensor networks must become a strategic imperative. Future research should now focus on subsystem integration across broader infrastructure domains, ensuring that the benefits of this technology extend beyond railways to the full spectrum of critical services that underpin societal well-being.

REFERENCES

[1] H. Martin and L. Ludek, “Conceptual design of the resilience evaluation system of critical infrastructure elements and networks in selected areas in Czech republic,” *Homeland Security (HST)*, pp. 353 – 358, 2012.

[2] E. Zezulova, P. Maňas and K. Cibulova, "Population Protection and Protection of Critical Infrastructure Elements," *2023 International Conference on Military Technologies (ICMT),* pp. 1-7, 2023.

[3] M. Mthombeni, B. Makhanya and J.H.C Pretorius, “Assessing Strategies to Mitigate Cable Theft in the South African Railway Sector,” *5th African International Conference on Industrial Engineering and Operations Management*, 2024

[4] P. McKeever, M. Allhof, A. Corsi, I. Sowa and A. Monti, "Wide-area Cyber-security Analytics Solution for Critical Infrastructures," *2020 6th IEEE International Energy Conference (ENERGYCon)*, pp. 34-37, 2020.

[5] P. Zhou, H. Xu and J. Hou, “Safety index of high-speed maglev train decentralized operation control system,” *International Conference on Measuring Technology and Mechatronics Automation*, pp. 878-881, 2009.

[6] X. He, Y. Wen, and D. Zhang, “Influence of Protection Wire and Positive Feeder Arrangement of Traction Network on the Return Current in High-speed Railway,” IEEE 2nd Int. Conf. Electron. Technol. Commun. Information, ICETCI 2022, pp. 205–210, 2022.

[7] L. Guo, L. Huang and Y. Zhao, “Residual MBConv submanifold module for 3D LiDAR-based object detection,” *IEEE Intelligent Vehicles Symposium (IV)*, pp. 1720-1724, 2022.

[8] C. Wisultschew et al, “3D-LIDAR based object detection and tracking on the edge of IoT for railway level crossing,” *IEEE access*, vol. 9, pp. 35718 – 35729, 2021.

[9] B.L. Nisarga, “Hybrid IoT based hazard detection system for buildings,” *Proceedings of the International Conference on Electronics and Sustainable Communication Systems (ICESC 2020),*pp. 889-895*,* 2020.

[10] G. Bocchetti, F. Flammini, C. Pragliola and A. Pappalardo, "Dependable integrated surveillance systems for the physical security of metro railways," *2009 Third ACM/IEEE International Conference on Distributed Smart Cameras (ICDSC),* pp. 1-7, 2009.

[11] Y. L. Zhang, Z. Q. Zhang, G. Xiao, R. D. Wang and X. He, "Perimeter intrusion detection based on intelligent video analysis," *2015 15th International Conference on Control, Automation and Systems (ICCAS)*, pp. 1199-1204, 2015.

[12] D. A. Galván and E. Díaz Lozano, "An approach to reduce copper theft in transmission line grounding systems," *2013 International Symposium on Lightning Protection (XII SIPDA)*, pp. 196-200, 2013.

[13] W. Xu et al., "Fraud detection in telecommunication: A rough fuzzy set based approach," *2008 International Conference on Machine Learning and Cybernetics, Kunming,* pp. 1249-1253*, 2008*.

[14] V. Chang and L. Uden, "Governance for E-learning ecosystem," *2008 2nd IEEE International Conference on Digital Ecosystems and Technologies,* pp. 340-345, 2008.

[15] R. Narayan and J. Regan, "Copper Theft of Earthing Systems a Worldwide Problem," *Intelec 2013; 35th International Telecommunications Energy Conference, Smart power and efficiency*, pp. 1-5, 2023.

[16] H. Xiaoxi, Z. Xiangjun, X. Yao and J. Guangming, "A novel anti-theft and detection method of street lamp power cables*," Proceedings of the 2010 International Conference on Modelling, Identification and Control*, pp. 76-81, 2010.

[17] X. J. Chen, Z. F. Gao and W. Wang, "Application of BP Artificial Neural Network in Structure Damage Identification," *2010 International Conference on Intelligent Computation Technology and Automation,* pp. 733-737, 2010.

[18] S. Zhang, Z. He, W. -J. Lee and R. Mai, "Voltage-Sag-Profiles-Based Fault Location in High-Speed Railway Distribution System," *in IEEE Transactions on Industry Applications,* vol. 53, no. 6, pp. 5229-5238, Nov.-Dec. 2017.

[19] Ellis, R., “Critical Infrastructure and Control Systems Security: An Interdisciplinary Approach, *Technologies for Homeland Security,* pp. 459 – 462, 2008.

[20] M.A. Gandhi and L. Mili, “Robust Kalman Filter based on a Generalized Maximum Likelihood-Type Estimators. Signal Processing,” *IEEE Transactions on.* Vol. 58(5), pp. 2509 – 2520, 2010.

[21] C.M. Akujuobi, N.K. Ampah and M.N.O. Sadiku, “Application of Wavelets and Self-similarity to Enterprise Network Intrusion Detection and Prevention Systems,” *ISCE 2007 IEEE International Symposium*, pp. 1 - 6, 2006.

[22] K. Shanthi and R. Maruthi, "A Comparative Study of Intrusion Detection and Prevention Systems for Cloud Environment," 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC), pp. 493-496, 2023.

[23] W. Burgard, O. Brock and C. Stachniss, “Adaptive Non-Stationary Kernel Regression for Terrain Modeling”, *Robotics:Science and Systems III*, pp. 81 – 88, 2008.

[24] Y. Yang et al., "Research on lifetime prediction-based recharging scheme in rechargeable WSNs*," NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium,* pp. 1-4, 2018.

[25] A. M. George, S. Y. Kulkarni and C. P. Kurian, "Gaussian Regression Models for Evaluation of Network Lifetime and Cluster-Head Selection in Wireless Sensor Devices," *in IEEE Access,* vol. 10, pp. 20875-20888, 2022.