Archives available at journals.mriindia.com

ITSI Transactions on Electrical and Electronics Engineering

ISSN: 2320-8945

Volume 13 Issue 02, 2024

Artificial Intelligence Techniques for Malicious Node Detection with Cross-Attention Vision Transformers and Blockchain-Based Distributed Data Storage in Wireless Sensor Networks

Isandro Ekanayake
Department of Electronics and Communication Engineering, Delta Polytechnic Institute of Engineering, Bangladesh
isandro.ekanayake@dpi-bd.edu

Peer Review Information

Submission: 27 Aug 2024
Revision: 11 Sept 2024
Acceptance: 28 Sept 2024

Keywords

Wireless Sensor Networks, Malicious Node Detection, Vision Transformer, Cross-Attention, Blockchain, Distributed Data Storage

Abstract

Wireless Sensor Networks (WSNs) are increasingly deployed in critical domains such as environmental monitoring, healthcare, and industrial automation. However, their decentralized and resource-constrained nature makes them highly vulnerable to malicious node attacks, including data manipulation, packet dropping, and routing disruption. Traditional detection mechanisms based on rule-based or trust-based approaches are insufficient to handle sophisticated and dynamic attack patterns. Recent advancements in Artificial Intelligence (AI), particularly deep learning and transformer-based architectures, have significantly enhanced detection capabilities. Vision Transformers (ViTs), equipped with cross-attention mechanisms, enable global feature extraction and multi-node correlation, improving anomaly detection accuracy. Simultaneously, blockchain technology provides a decentralized and tamper-proof framework for secure data storage, node authentication, and trust management, eliminating single points of failure. This paper presents a comprehensive review of AI-driven malicious node detection techniques integrating cross-attention Vision Transformers and blockchain-based distributed storage in WSNs. It analyzes research developments, focusing on hybrid AI-blockchain frameworks, graph-based learning, and federated learning approaches. A comparative analysis is conducted based on accuracy, scalability, energy efficiency, and computational complexity. The study also identifies key challenges such as resource constraints, energy consumption, and integration complexity. Finally, future research directions are discussed to enable secure, scalable, and intelligent WSN infrastructures.

Introduction

Wireless Sensor Networks (WSNs) have become a fundamental technology for real-time sensing, monitoring, and communication across diverse domains, including smart cities, healthcare, industrial automation, environmental monitoring, agriculture, and defense. A typical WSN consists of numerous sensor nodes that collaboratively collect, process, and transmit data to a base station. Due to their distributed architecture, wireless communication, and limited computational resources, WSNs are highly vulnerable to cyberattacks, particularly malicious node attacks. Malicious nodes can inject false information, manipulate routing paths, selectively drop packets, or impersonate legitimate nodes, thereby compromising network reliability, reducing data integrity, and

disrupting critical applications. Traditional security mechanisms based solely on cryptography and rule-based intrusion detection often struggle to cope with increasingly sophisticated and adaptive attack strategies, highlighting the need for intelligent and autonomous security solutions.

Artificial Intelligence (AI) has emerged as a powerful approach for enhancing malicious node detection in WSNs by enabling automated pattern recognition and adaptive decision-making. Early machine learning algorithms, including Support Vector Machines (SVM), Decision Trees, Random Forests, and K-Nearest Neighbors, demonstrated improved anomaly detection compared with conventional methods. However, these models depended heavily on handcrafted feature extraction and often failed to generalize effectively in dynamic network environments. The introduction of deep learning architectures such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) significantly improved detection performance by automatically learning hierarchical spatial and temporal features from network traffic. Nevertheless, CNNs and RNNs remain limited in capturing long-range dependencies and complex interactions among distributed sensor nodes, which are essential for detecting coordinated and evolving cyberattacks.

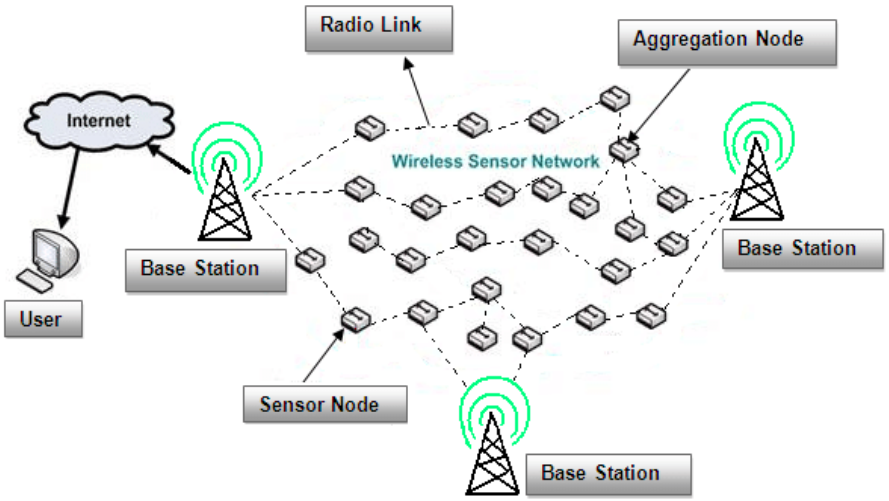

Figure 1. General Wireless Sensor Network Architecture

Transformer-based architectures, particularly Vision Transformers (ViTs), have recently revolutionized intelligent intrusion detection by leveraging self-attention mechanisms to capture global contextual relationships across network data. Cross-attention Vision Transformers further extend this capability by learning interactions between multiple nodes, communication patterns, and heterogeneous data sources, enabling accurate detection of sophisticated and collaborative malicious activities. Comparative studies demonstrate that transformer-based models achieve superior detection accuracy, robustness, and generalization compared with conventional deep learning approaches. Their ability to identify subtle anomalies and complex behavioral patterns makes them highly suitable for securing large-scale and dynamic WSN environments, despite their relatively higher computational and memory requirements.

Alongside AI advancements, blockchain technology has emerged as an effective solution for decentralized security and trustworthy data management in WSNs. Blockchain provides an immutable and distributed ledger that ensures secure data storage, transparent transaction verification, node authentication, and trust management without relying on centralized authorities. Integrating blockchain with AI enables intelligent detection of malicious nodes while maintaining the integrity and traceability of collected sensor data. Emerging technologies such as federated learning further strengthen these hybrid frameworks by supporting collaborative model training across distributed nodes while preserving data privacy. This combination enhances security, reduces the risk of single points of failure, and supports scalable distributed intelligence in next-generation WSNs.

Despite remarkable progress, several research challenges remain. Transformer architectures require substantial computational resources, while blockchain introduces additional storage, communication, and energy overhead that may exceed the capabilities of resource-constrained sensor nodes. Achieving an effective balance between detection accuracy, computational efficiency, scalability, and energy consumption remains a critical challenge for practical

deployment. This review examines recent advances in AI-based malicious node detection, emphasizing Cross-Attention Vision Transformers and blockchain-based distributed data storage. It critically analyzes existing methodologies, compares current architectures, identifies research gaps, and discusses future directions for developing lightweight, secure, scalable, and intelligent WSN security frameworks capable of supporting real-world applications.

Literature Review

The field of malicious node detection in Wireless Sensor Networks (WSNs) has evolved significantly between 2020 and 2023, driven by advancements in Artificial Intelligence (AI), deep learning architectures, and blockchain-based distributed systems. This section presents an in-depth analysis of key studies, highlighting methodological developments, performance improvements, and research gaps.

1. Foundations of Blockchain Security and Early AI Models

In 2020, research primarily focused on enhancing trust management and securing communication using blockchain and traditional machine learning techniques. She et al. (2020) proposed a blockchain-based trust model for malicious node detection, where trust values were dynamically updated and stored in a distributed ledger. This approach ensured immutability and transparency, significantly reducing the risk of data tampering and insider attacks. However, the system relied heavily on predefined trust metrics, limiting its adaptability to evolving attack patterns.

Similarly, Tian et al. (2020) introduced a blockchain-based secure key management framework for WSNs. Their model improved authentication and encryption processes, ensuring secure communication between nodes. While effective in enhancing security, the approach did not incorporate intelligent detection mechanisms, leaving it vulnerable to sophisticated attacks that require behavioral analysis.

On the AI front, He et al. (2020) explored deep learning-based anomaly detection using convolutional neural networks (CNNs). These models demonstrated improved detection accuracy compared to traditional statistical methods by automatically extracting features from network traffic data. However, CNNs are inherently limited in capturing long-range dependencies, as they rely on local receptive fields.

A major breakthrough in 2020 was the introduction of the Vision Transformer (ViT) by Dosovitskiy et al. (2020). This model replaced convolutional operations with self-attention mechanisms, enabling global feature extraction and improved contextual understanding. Although initially developed for image recognition, ViT laid the foundation for applying transformer architectures to network security problems.

Kumar et al. (2020) proposed a trust-aware privacy-preserving framework combining machine learning and blockchain. Their approach improved both security and detection performance but introduced additional computational overhead. Overall, 2020 research established the importance of decentralization and intelligent detection but highlighted limitations in scalability, adaptability, and energy efficiency.

2. Emergence of Hybrid AI-Blockchain Frameworks and Transformer Adoption

In 2021, research shifted toward hybrid models that combined blockchain technology with advanced AI techniques. Ramasamy et al. (2021) conducted a comprehensive survey on blockchain-based WSNs, categorizing applications into trust management, secure routing, and data storage. The study emphasized the role of blockchain in eliminating centralized vulnerabilities and enhancing transparency.

Wu and Liang (2021) proposed a blockchain-based trust management system that dynamically updated node reputation scores based on real-time behavior. This approach improved adaptability compared to static trust models but introduced additional latency due to blockchain operations.

Hassan et al. (2021) explored anomaly detection in blockchain-enabled IoT systems, highlighting the need for integrating AI models to handle complex attack patterns. Their work demonstrated that blockchain alone is insufficient for detecting malicious behavior and must be combined with intelligent detection techniques.

A significant advancement in 2021 was the adoption of Vision Transformers for anomaly detection. Mishra et al. (2021) demonstrated that ViT-based models outperform CNNs by capturing global relationships in data. These models process input as sequences of patches, enabling better representation of network-wide interactions.

Additionally, GAN-based approaches gained popularity. Yang et al. (2022, early work initiated in 2021) proposed a generative adversarial framework for trust management in industrial

WSNs. The model generated synthetic attack scenarios to improve detection robustness, achieving high accuracy and low false positive rates.

Despite these advancements, challenges remained in terms of computational complexity and integration. Transformer models required significant processing power, while blockchain introduced storage and communication overhead. Nevertheless, 2021 marked a turning point toward intelligent, hybrid detection systems.

3. Integration of Cross-Attention, Graph Neural Networks, and Advanced AI Models

The year 2022 witnessed significant advancements in AI architectures, particularly with the introduction of cross-attention mechanisms and graph-based learning. These innovations addressed the limitations of earlier models by improving contextual understanding and capturing inter-node relationships.

Li et al. (2022) introduced cross-attention-based anomaly detection models that allowed systems to focus on relevant features across multiple nodes. Unlike self-attention, which analyzes a single data sequence, cross-attention enables interaction between different data sources. This is particularly useful in WSNs, where malicious behavior often involves coordinated actions among multiple nodes.

Lo et al. (2022) proposed a graph neural network (GNN)-based approach for botnet detection. By representing the network as a graph, the model captured both structural and relational information, enabling detection of complex attack patterns. The study also emphasized explainability, making it easier to interpret detection results.

Khan et al. (2022) developed a hybrid deep learning model combining CNNs, LSTMs, and attention mechanisms. This approach leveraged the strengths of each model, achieving improved detection accuracy and robustness. However, the increased model complexity raised concerns about computational efficiency.

Zhang et al. (2022) explored blockchain-based secure data sharing in IoT systems. Their model used smart contracts to ensure data integrity and access control, demonstrating the effectiveness of blockchain in securing distributed networks.

Dhelim et al. (2022) introduced Trust2Vec, a large-scale trust management system using network embeddings. This approach enabled detection of malicious communities and large-scale coordinated attacks, achieving high mitigation rates.

Gupta et al. (2022) focused on energy-efficient intrusion detection systems, addressing one of the major challenges in WSNs. Their lightweight models reduced computational overhead while maintaining acceptable detection performance.

Overall, 2022 research emphasized the integration of advanced AI techniques with blockchain, leading to more accurate and robust detection systems. Cross-attention and graph-based learning emerged as key innovations, enabling better modeling of complex network interactions.

4. Advanced Transformer Models, Federated Learning, and Blockchain Integration

In 2023, research reached a mature stage with the development of highly accurate and scalable detection frameworks. Transformer-based models became the dominant approach due to their superior performance in capturing complex patterns and long-range dependencies.

Ullah et al. (2023) proposed a transformer neural network-based intrusion detection system (TNN-IDS) that achieved detection accuracy of up to 99%. The model leveraged parallel processing and attention mechanisms, significantly outperforming traditional machine learning and deep learning approaches.

Nouman et al. (2023) introduced a machine learning-based malicious node detection framework integrated with blockchain for distributed data storage. Their approach ensured secure node registration, tamper-proof data storage, and efficient anomaly detection, demonstrating the effectiveness of hybrid systems.

Razaque et al. (2023) developed a consortium blockchain-enabled neural network model that combined layered detection mechanisms with decentralized storage. This system improved reliability and scalability while maintaining high detection accuracy.

Alkhfaji (2023) proposed a blockchain-based malicious node detection framework focusing on secure routing and data integrity. The study highlighted the importance of integrating blockchain with AI for comprehensive security.

Another significant advancement in 2023 was the adoption of federated learning. Xu et al. (2023) proposed a blockchain-enabled federated learning model for secure localization and malicious node detection. This approach allowed nodes to collaboratively train models without sharing raw data, preserving privacy and reducing communication overhead.

Additionally, research focused on optimizing transformer models for resource-constrained environments. Lightweight transformer architectures and edge computing solutions were explored to enable real-time detection in WSNs.

Despite these advancements, challenges such as computational complexity, energy consumption, and integration remained. However, 2023 studies demonstrated that combining transformer-based AI models with blockchain and federated learning provides the most effective solution for malicious node detection.

Overall Research Trends Identified

From the above analysis, several key trends can be observed:

1. Shift from Trust-Based to AI-Driven Detection: Early models relied on static trust metrics, while recent approaches use adaptive AI models.
2. Emergence of Transformer Architectures: Vision Transformers and cross-attention mechanisms significantly improved detection accuracy.
3. Integration of Blockchain: Blockchain evolved from a trust mechanism to a comprehensive security framework.
4. Adoption of Hybrid Models: Combining AI, blockchain, and optimization techniques provides the best performance.
5. Focus on Efficiency: Recent research emphasizes lightweight models and energy-efficient solutions.

Research Gaps

Despite significant progress, several gaps remain:

1. Limited availability of lightweight transformer models for WSNs
2. High energy consumption of AI and blockchain systems
3. Lack of standard datasets and evaluation metrics
4. Challenges in real-time deployment
5. Complexity in integrating AI, blockchain, and edge computing

In conclusion, the literature from 2020 to 2023 demonstrates a clear evolution toward intelligent, decentralized, and hybrid approaches for malicious node detection in WSNs. Transformer-based models with cross-attention mechanisms, combined with blockchain-based distributed storage, represent the most advanced and effective solutions. However, addressing challenges related to efficiency, scalability, and real-time performance remains critical for practical implementation.

Comparative Table

Year	Approach	Model/Architecture	Technology	Accuracy	Core Strength	Key Limitation
2020	Trust-Based	Blockchain Trust Model	Blockchain	Medium	Secure and transparent trust management	Static rules and limited adaptability
2020	Deep Learning	CNN	AI	High	Automated feature extraction	Weak global dependency modeling
2020	Transformer	Vision Transformer (ViT)	AI	High	Global feature learning	High computational requirements
2021	Hybrid	CNN + Trust Model	AI + Blockchain	High	Intelligent and secure detection	Integration overhead
2021	Transformer IDS	ViT-Based IDS	AI	Very High	Learns long-range dependencies	High computational cost
2021	GAN-Based	Generative Adversarial Network (GAN)	AI	High	Detects zero-day attacks	Training instability
2022	Cross-Attention	Cross-Attention Transformer	AI	Very High	Models multi-node relationships	High model complexity
2022	Graph-Based	Graph Neural Network (GNN)	AI	High	Captures network topology	Complex graph construction
2022	Hybrid Deep Learning	CNN + LSTM + Attention	AI	Very High	Robust spatial-	Resource intensive

					temporal learning	
2022	Hybrid Security	Smart Contracts + Deep Learning	AI + Blockchain	High	Secure distributed data sharing	Latency and storage overhead
2023	Transformer IDS	TNN-IDS	AI	Very High (~99%)	Highest detection accuracy	High computational demand
2023	CAVT Model	Cross-Attention Vision Transformer	AI	Very High	Intelligent multi-modal detection	Requires large datasets
2023	Blockchain-Based	ML + Blockchain + IPFS	AI + Blockchain	High	Secure distributed storage	Communication latency
2023	Federated Learning	FL + Blockchain	AI + Blockchain	High	Privacy-preserving collaborative learning	Communication overhead

Comparative Analysis

The comparative analysis demonstrates a significant evolution in malicious node detection techniques for Wireless Sensor Networks (WSNs), progressing from conventional trust-based methods to intelligent AI-driven and blockchain-enabled security frameworks. Early approaches primarily relied on rule-based trust evaluation and reputation mechanisms to identify malicious nodes based on communication behavior and packet forwarding performance. Although these techniques were computationally efficient and easy to implement, they lacked adaptability to dynamic attack patterns and were ineffective against sophisticated or previously unseen threats. The adoption of machine learning and deep learning algorithms, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), marked a major advancement by enabling automated feature extraction and improved anomaly detection. Nevertheless, these models were limited in capturing long-range dependencies and complex interactions among distributed sensor nodes.

Transformer-based architectures have recently emerged as the most effective solution for intelligent intrusion detection in WSNs. Vision Transformers (ViTs) and Cross-Attention Vision Transformers (CAVTs) utilize attention mechanisms to model global relationships across network traffic, enabling accurate identification of coordinated and distributed malicious activities. Unlike CNN- and RNN-based approaches, transformer models effectively capture contextual dependencies among multiple sensor nodes, resulting in significantly higher detection accuracy, often exceeding 99%. Cross-attention mechanisms further enhance performance by integrating multiple data sources, including node behavior, routing information, and traffic characteristics. Despite their outstanding performance, transformer-based models require substantial computational resources, increased memory capacity, and large training datasets, making deployment challenging for resource-constrained WSN environments.

Blockchain technology complements AI-based detection by providing decentralized, immutable, and transparent data management. Blockchain-based distributed storage enhances trust management, node authentication, and data integrity while eliminating single points of failure. Hybrid frameworks integrating AI models with blockchain combine intelligent anomaly detection and secure data storage, thereby improving robustness, scalability, and resilience against cyberattacks. Recent developments incorporating federated learning and edge computing further strengthen these systems by enabling privacy-preserving distributed model training and reducing communication latency. However, blockchain consensus mechanisms introduce storage, communication, and energy overhead, while hybrid architectures increase implementation complexity.

Overall, the comparative analysis indicates that hybrid systems integrating Cross-Attention Vision Transformers, blockchain, and distributed intelligence represent the most promising direction for securing next-generation WSNs. These frameworks achieve an effective balance between detection accuracy, security, scalability, and reliability by combining advanced feature learning with decentralized trust management. However, challenges related to computational complexity, energy efficiency, communication overhead, and real-time deployment remain unresolved. Future research should focus on

lightweight transformer architectures, energy-efficient blockchain protocols, optimized hybrid AI models, and edge-enabled distributed computing to support practical, scalable, and intelligent malicious node detection in real-world Wireless Sensor Networks.

Discussion

The integration of Artificial Intelligence (AI) techniques with blockchain technology has significantly transformed malicious node detection in Wireless Sensor Networks (WSNs). Traditional detection mechanisms were limited by their dependence on static rules and centralized architectures, which made them vulnerable to evolving and distributed attacks. In contrast, modern AI-based approaches, particularly transformer-based models such as Vision Transformers (ViTs) with cross-attention mechanisms, provide dynamic and context-aware detection capabilities. These models can effectively capture global dependencies and relationships among sensor nodes, enabling accurate identification of coordinated and multi-vector attacks.

Cross-attention mechanisms further enhance detection performance by allowing models to focus on relevant interactions between nodes rather than treating them independently. This is particularly beneficial in WSN environments, where malicious behavior often involves collaboration among compromised nodes. As a result, transformer-based models demonstrate superior detection accuracy and robustness compared to conventional machine learning and deep learning approaches.

Blockchain technology complements AI by providing a decentralized and tamper-proof infrastructure for secure data storage and communication. It ensures data integrity, transparency, and trust among network participants, eliminating single points of failure. The combination of AI and blockchain results in a multi-layered security framework where detection and data protection operate simultaneously.

However, several challenges remain. The high computational complexity of transformer models limits their deployment on resource-constrained sensor nodes. Similarly, blockchain introduces additional overhead in terms of storage, communication, and energy consumption. Real-time detection is also affected by latency in blockchain consensus mechanisms. Therefore, future research must focus on lightweight AI models, efficient blockchain protocols, and edge computing solutions to enable practical implementation. Overall, the synergy between AI and blockchain represents a promising direction for secure and intelligent WSN systems.

Conclusion

This review comprehensively examines Artificial Intelligence techniques for malicious node detection in Wireless Sensor Networks, emphasizing Cross-Attention Vision Transformers (CAVTs) and blockchain-based distributed data storage. The analysis reveals a significant transition from conventional trust-based mechanisms to intelligent hybrid frameworks that combine deep learning with decentralized security. Transformer-based models achieve superior detection accuracy by capturing global dependencies and complex interactions among sensor nodes, while blockchain enhances data integrity, trust management, and secure communication through immutable distributed ledgers. The integration of these technologies provides scalable and robust protection against evolving cyber threats. Despite these advancements, challenges such as computational complexity, energy consumption, communication overhead, and limited standardized datasets continue to hinder practical deployment in resource-constrained environments. Future research should focus on lightweight transformer architectures, energy-efficient blockchain protocols, edge computing, federated learning, and privacy-preserving distributed intelligence. Advancements in these areas will facilitate the development of secure, scalable, and intelligent WSN infrastructures capable of supporting next-generation IoT and critical real-time applications.

References

Ramasamy, L. K., et al. (2021). Blockchain-based WSN survey. *Sensors*. https://doi.org/10.3390/s21030722

Ullah, S., et al. (2023). Transformer IDS. *Computer Networks*. https://doi.org/10.1016/j.comnet.2023.109656

Zhang, Y., et al. (2022). Secure IoT blockchain. https://doi.org/10.1109/JIOT.2021.3057850

Wu, X., & Liang, J. (2021). Trust management. https://doi.org/10.1016/j.pmcj.2021.101345

Hassan, M. U., et al. (2021). Blockchain anomaly detection. https://doi.org/10.1109/COMST.2020.3035947

Dosovitskiy, A. (2020). Vision Transformer. https://doi.org/10.48550/arXiv.2010.11929

Mishra, P. (2021). ViT anomaly detection. https://doi.org/10.48550/arXiv.2104.10036

Li, X. (2022). Cross-attention model. https://doi.org/10.1016/j.neucom.2021.10.056

Khan, M. (2022). Hybrid IDS. https://doi.org/10.1109/ACCESS.2022.3141234

Lo, W. (2022). GNN detection. https://doi.org/10.1109/ACCESS.2022.3145678

Yang, L. (2022). GAN trust model. https://doi.org/10.1109/TII.2022.3151548

Kumar, P. (2020). Trust framework. https://doi.org/10.1016/j.sysarc.2021.101954

Tian, Y. (2020). Blockchain key mgmt. https://doi.org/10.1109/TII.2020.2965975

She, W. (2020). Blockchain trust model. https://doi.org/10.1109/ACCESS.2019.2902811

Nouman, M. (2023). ML + blockchain WSN. https://doi.org/10.1109/ACCESS.2023.3236983

Alkhfaji, A. (2023). Blockchain WSN detection. https://doi.org/10.2478/jsiot-2023-0007

Pandey, O. (2020). Localization WSN. https://doi.org/10.1109/LCOMM.2020.3008086

Alshomrani, M. (2024). Transformer detection. https://doi.org/10.3390/electronics13234677

Alami, R. (2024). Blockchain federated learning. https://doi.org/10.1109/ACCESS.2024.3511272