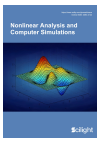
Scilight

Nonlinear Analysis and Computer Simulations
https://www.sciltp.com/journals/nacs



Article

Check for updates

A Nonlinear RSSI–Energy Graph Model with SVM-Based Optimization and Simulation Validation for Sybil Attack Detection in Wireless Sensor Networks

Shabnam Mohamed Aslam [1,*], Areej Fala [2] and Asifa Tassaddiq [1,*]

[1] Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Al Majmaah 11952, Saudi Arabia
[2] M.S. Program in Cyber Security and Digital Forensics, College of Computer and Information Sciences, Majmaah University, Al Majmaah 11952, Saudi Arabia
* Correspondence: s.aslam@mu.edu.sa (S.M.A.); a.tassaddiq@mu.edu.sa (A.T.)

How To Cite: Aslam, S.M.; Fala, A.; Tassaddiq, A. A Nonlinear RSSI–Energy Graph Model with SVM-Based Optimization and Simulation Validation for Sybil Attack Detection in Wireless Sensor Networks. *Nonlinear Analysis and Computer Simulations* **2026**, *1*(3), 15. https://doi.org/10.53941/nacs.2026.100015

Received: 22 May 2026
Revised: 26 June 2026
Accepted: 7 August 2026
Published: 1 September 2026

Abstract: Wireless sensor networks are vulnerable to Sybil attacks because low-cost sensor nodes have restricted energy, computation and communication resources, while a malicious device may claim multiple identities and distort routing, localization and trust decisions. Existing Sybil attack detectors based only on identity verification or received signal strength indicator may be sensitive to radio-noise fluctuations and may ignore the energy and timing behaviour of interacting nodes. This paper develops a nonlinear graph-based received-signal-strength-indicator–energy anomaly model for Sybil attack detection in wireless sensor networks and combines it with support vector machine classification. The network is represented as a time-dependent weighted graph in which node interaction weights depend on received-signal-strength-indicator deviation, residual-energy variation, transmission-time inconsistency and duplicate identity or location evidence. A nonlinear anomaly map transforms the hybrid score into a bounded risk indicator, and the support vector machine classifier is formulated as an optimization problem over the proposed feature space. Boundedness, monotonicity, threshold-separation and computational-complexity properties of the detector are established. Simulation experiments using networks of different sizes are used to evaluate the model under legitimate and Sybil-node populations, including ablation tests, threshold-sensitivity analysis and confusion-matrix based metrics. The results indicate that the proposed framework provides an interpretable and lightweight mathematical mechanism for malicious-node detection in resource-constrained wireless sensor networks, especially when explainability, low computational overhead and cross-layer feature integration are preferred over black-box detection alone.

Keywords: Sybil attack; wireless sensor network; nonlinear graph model; received signal strength indicator; energy-aware anomaly detection; support vector machine

2020 MSC: 05C85; 68R10; 68Txx

1. Introduction

Wireless sensor networks (WSNs) are widely used in environmental monitoring, smart agriculture, industrial automation, medical sensing, structural health monitoring and other cyber-physical systems [1, 2]. A WSN is normally composed of many low-cost sensor nodes that communicate over short-range wireless links and operate under strict energy, computation and memory limitations. These constraints make network security difficult: a defence mechanism that is accurate but computationally expensive may not be suitable for ordinary sensor nodes.

One of the most disruptive attacks in a WSN is the Sybil attack. In this attack, one malicious physical device presents several logical identities to the network. Such behaviour can distort multi-hop routing, neighbour discovery,

localization, trust management, voting, aggregation and cooperative sensing. The Sybil attack was formalized in distributed systems by Douceur [3] and later analysed in sensor networks and Internet of Things settings [4,5]. In many WSN scenarios, strong cryptographic authentication is useful but may be limited by energy consumption, key-distribution cost or deployment complexity. Therefore, physical-layer and behaviour-aware indicators remain important for lightweight attack detection.

Received signal strength indicator (RSSI)-based Sybil detection is attractive because it uses a measurement that is already produced during wireless communication [6]. If a claimed identity or claimed location is inconsistent with the observed radio signal, the discrepancy can become evidence of suspicious behaviour; RSSI-based localization research likewise demonstrates the connection between signal strength and location estimation [7]. However, RSSI alone is not fully reliable because wireless channels are affected by fading, interference, obstacles, antenna orientation and deployment geometry. Trust-aware and energy-aware approaches add behavioural information, but they may still lack an explicit mathematical structure that combines signal evidence, resource evidence and identity evidence in one interpretable detection rule [8,9].

Machine-learning models, including support vector machines (SVMs), have also been used for cybersecurity and intrusion detection because they can learn decision boundaries from heterogeneous features [10–13]. Broader research has examined adversarial learning, cybersecurity algorithms and cyber-threat attribution [14–16]. Compared with deep-learning models, an SVM is often attractive for small or medium simulation datasets because its optimization problem is explicit and the margin-based classifier is relatively lightweight [17, 18]. However, a standalone SVM does not by itself provide a nonlinear network model. For a journal focused on nonlinear analysis and computer simulations, the modelling of the sensor network, feature-generation process and anomaly transformation is as important as the final classifier.

Existing methods may be grouped into several directions. RSSI-only detectors are lightweight but sensitive to noisy radio conditions. Trust and energy models add resource-aware behaviour but may be less effective when used without physical signal evidence. More recent mobile Internet of Things, lightweight RSSI-based and deep-learning models can increase modelling capacity, but they may require more intensive training and richer datasets and may offer less interpretability [19–23]. The present work positions itself between these approaches by proposing a nonlinear graph-based mathematical model that integrates RSSI, residual energy, transmission time, power consumption and duplicate identity or location evidence before SVM classification.

The novelty and contributions of the study are listed as follows:

- A time-dependent weighted graph model is formulated for WSN communication under Sybil attack conditions.
- A nonlinear anomaly score is constructed by combining RSSI inconsistency, residual-energy deviation, transmission-time deviation, power-consumption variation and duplicate identity/location evidence.
- The SVM stage is written as a formal margin-based optimization problem, and the feature map and kernel function are explicitly defined.
- Boundedness, monotonicity, threshold-separation and computational-complexity properties of the proposed detector are established.
- The study uses the 100-, 200- and 300-node simulation logs together with reproducible model-driven experiments to provide a baseline comparison, ablation analysis, threshold-sensitivity analysis and confusion-matrix-based evaluation.
- The discussion interprets the advantage of the proposed score in terms of transparency, graph-based modelling and threshold tunability, while avoiding an unsupported claim of numerical superiority over the standard SVM baseline in every metric.

The remainder of the paper is organized as follows. Section 2 reviews related work and identifies the research gap. Section 3 presents the dynamic graph representation, RSSI observation model, energy and timing dynamics, nonlinear anomaly score, SVM optimization model and theoretical properties. Section 4 reports the simulation setting, metrics, original simulation results, baseline comparison, ablation study, threshold sensitivity and interpretation of the nonlinear score. Section 5 discusses real-world relevance, limitations and comparison with baseline methods. Section 6 concludes the paper and outlines future validation on real-world sensor-network datasets.

2. Related Work and Research Gap

Early Sybil-attack research established that identity multiplication can seriously disrupt distributed systems and sensor-network protocols [3,4]. In WSNs, RSSI-based detection was introduced as a lightweight alternative to expensive key-management strategies, because RSSI is naturally available from wireless communication and can expose inconsistency between a claimed identity and the physical radio signal [6]. However, the RSSI channel is affected by noise, fading and obstacles, so RSSI-only decisions may be unstable in irregular deployments.

Trust-aware and energy-aware methods attempt to improve robustness by adding behavioural or resource-

consumption information [8,9]. More recent work has also examined mobile IoT settings, where RSSI fluctuation and intelligent position prediction are used to refine Sybil detection [19]. Lightweight RSSI-based IDS models continue to be studied because WSN nodes may not support high-cost security mechanisms [20,21]. At the same time, deep-learning methods for industrial WSNs have recently combined temporal and clustering components to improve detection accuracy, but such models may introduce heavier training and interpretation requirements [22,23].

The research gap addressed here is therefore not RSSI detection alone, and not the standalone use of SVM. The gap is the construction of an interpretable mathematical model in which RSSI inconsistency, residual-energy variation, timing deviation and duplicate-identity information are integrated into a nonlinear graph-based anomaly score and then linked to an SVM optimization problem. Table 1 summarizes this positioning.

Table 1. Positioning of the proposed model against representative Sybil/WSN security directions.

Direction	Main Idea	Limitation Addressed by This Paper	Representative References
RSSI-based Sybil detection	Uses physical signal strength to identify inconsistent identities	RSSI alone is sensitive to channel noise and deployment geometry	[6]
Trust/energy-aware detection	Adds behavioural trust or energy-consumption evidence	Trust or energy features may remain weak without a unified nonlinear score	[8,9]
Mobile IoT/RSSI fluctuation methods	Uses RSSI variation and node-position prediction	Mobility-focused models may not directly provide a graph anomaly formulation for static WSN simulation	[19]
Deep-learning IDS models	Learns complex temporal/topological patterns	Higher training cost and reduced interpretability may be unsuitable for lightweight WSN settings	[22,23]
Proposed model	Combines RSSI, energy, time and duplicate evidence into a nonlinear graph score with SVM optimization	Provides a lightweight and interpretable mathematical simulation framework	This work

3. Materials and Methods

3.1. Dynamic Graph Representation of the Wireless Sensor Network

Let a wireless sensor network at discrete time $t \in \{0, 1, 2, \ldots\}$ be represented by the weighted graph

$$\mathcal{G}(t) = (V, E(t), W(t)), \tag{1}$$

where $V = \{v_1, v_2, \ldots, v_N\}$ is the set of sensor nodes, $E(t) \subseteq V \times V$ is the set of communication links and $W(t) = [w_{ij}(t)]$ is a nonnegative weighted adjacency matrix. A link $(i, j) \in E(t)$ exists if node v_i can exchange packets with node v_j at time t. The weight $w_{ij}(t)$ represents the reliability of the interaction and is constructed from RSSI, energy and timing consistency.

The Euclidean position of node v_i is denoted by $p_i = (x_i, y_i) \in \mathbb{R}^2$. The distance between two nodes is

$$d_{ij} = \|p_i - p_j\|_2. \tag{2}$$

The neighbourhood of node v_i at time t is

$$\mathcal{N}_i(t) = \{v_j \in V : (i, j) \in E(t)\}. \tag{3}$$

3.2. Nonlinear RSSI Observation Model

Let $R_{ij}(t)$ denote the RSSI observed at node v_j from a transmission by node v_i. A standard log-distance path-loss model is written as

$$R_{ij}(t) = P_T - 10\eta \log_{10}(d_{ij} + d_0) + \xi_{ij}(t), \tag{4}$$

where P_T is the transmitted power in dBm, $\eta > 0$ is the path-loss exponent, $d_0 > 0$ avoids singularity at zero distance and $\xi_{ij}(t)$ is measurement noise. The predicted RSSI from the claimed position of node v_i is

$$\widehat{R}_{ij}(t) = P_T - 10\eta \log_{10}(\widehat{d}_{ij} + d_0), \tag{5}$$

where $\widehat{d}_{ij}$ is the distance computed from the claimed node location. The RSSI inconsistency of node v_i is defined by

$$\Delta R_i(t) = \frac{1}{|\mathcal{N}_i(t)|} \sum_{v_j \in \mathcal{N}_i(t)} \Big| R_{ij}(t) - \widehat{R}_{ij}(t) \Big|. \tag{6}$$

A Sybil node that claims several identities or false positions may produce a larger value of $\Delta R_i(t)$ because the physical signal behaviour becomes inconsistent with the claimed network identity.

3.3. Residual-Energy and Transmission-Time Dynamics

Let $E_i(t)$ be the residual energy of node v_i at time t. A simple discrete energy balance is

$$E_i(t+1) = E_i(t) - \alpha_T n_i^T(t) - \alpha_R n_i^R(t) - \alpha_I n_i^I(t), \tag{7}$$

where $n_i^T(t)$, $n_i^R(t)$ and $n_i^I(t)$ denote the number of transmitted, received and idle-listening operations, respectively, and $\alpha_T, \alpha_R, \alpha_I > 0$ are energy-cost coefficients. The expected energy consumption under normal behaviour is denoted by $\widehat{E}_i(t)$. The normalized energy-deviation feature is

$$\Delta E_i(t) = \frac{|E_i(t) - \widehat{E}_i(t)|}{E_i(0) + \varepsilon_E}, \tag{8}$$

where $\varepsilon_E > 0$ is a small constant to avoid division by zero.

Let $T_{ij}(t)$ be the observed transmission time or response time for packets exchanged between v_i and v_j. The timing inconsistency of node v_i is

$$\Delta T_i(t) = \frac{1}{|\mathcal{N}_i(t)|} \sum_{v_j \in \mathcal{N}_i(t)} \frac{|T_{ij}(t) - \widehat{T}_{ij}(t)|}{\widehat{T}_{ij}(t) + \varepsilon_T}, \tag{9}$$

where $\widehat{T}_{ij}(t)$ is the expected transmission time under normal communication and $\varepsilon_T > 0$ is a stabilizing constant.

3.4. Duplicate Identity and Location Indicator

Sybil attacks often involve repeated identity claims, inconsistent node IDs or duplicated location information. Define

$$D_i(t) = \begin{cases} 1, & \text{if node } v_i \text{ has duplicate ID or duplicate claimed position evidence,} \\ 0, & \text{otherwise.} \end{cases} \tag{10}$$

This binary variable is not sufficient alone, but it is valuable when combined with RSSI, energy and timing observations.

3.5. Hybrid Nonlinear Anomaly Score

Let

$$x_i(t) = \big(\Delta R_i(t), \Delta E_i(t), \Delta T_i(t), D_i(t), P_i(t)\big)^T \in \mathbb{R}^5, \tag{11}$$

where $P_i(t)$ is the normalized power-consumption deviation of node v_i. Let $\omega_k \geq 0$ be feature weights satisfying $\sum_{k=1}^{5} \omega_k = 1$. The hybrid RSSI–energy anomaly score is defined by

$$\mathcal{S}_i(t) = \omega_1 \Delta R_i(t) + \omega_2 \Delta E_i(t) + \omega_3 \Delta T_i(t) + \omega_4 D_i(t) + \omega_5 P_i(t). \tag{12}$$

To introduce a bounded nonlinear risk indicator, define

$$\mathcal{A}_i(t) = \frac{1}{1 + \exp[-\lambda(\mathcal{S}_i(t) - \theta)]}, \qquad \lambda > 0, \tag{13}$$

where θ is the anomaly threshold and λ controls the sharpness of the transition between normal and suspicious behaviour. The final augmented feature vector used for SVM classification is

$$z_i(t) = \big(\Delta R_i(t), \Delta E_i(t), \Delta T_i(t), D_i(t), P_i(t), \mathcal{A}_i(t)\big)^T \in \mathbb{R}^6. \tag{14}$$

3.6. Graph Reliability Weight

For $(i,j) \in E(t)$, define the interaction reliability weight

$$w_{ij}(t) = \exp\left[-\beta_R |R_{ij}(t) - \widehat{R}_{ij}(t)| - \beta_T \frac{|T_{ij}(t) - \widehat{T}_{ij}(t)|}{\widehat{T}_{ij}(t) + \varepsilon_T}\right] \times \frac{E_i(t) + E_j(t)}{2E_0}, \tag{15}$$

where $\beta_R, \beta_T > 0$ are sensitivity parameters and E_0 is the initial energy. The weight decreases when RSSI or timing inconsistency increases and also decreases when residual energy becomes low. Hence $W(t)$ describes both physical signal reliability and resource availability.

3.7. SVM Optimization Model

Each node observation is assigned a label $y_i \in \{-1, +1\}$, where $y_i = -1$ denotes a legitimate node and $y_i = +1$ denotes a Sybil or malicious node. The augmented vector $z_i(t) \in \mathbb{R}^6$ is mapped into a feature space by

$$\phi : \mathbb{R}^6 \to \mathcal{H}, \tag{16}$$

where $\mathcal{H}$ is a Hilbert feature space. For a linear support vector machine, $\phi(z) = z$. For a nonlinear kernel, the map ϕ may be implicit and the classifier is evaluated through the kernel function

$$K(z_i, z_j) = \langle \phi(z_i), \phi(z_j) \rangle_{\mathcal{H}}. \tag{17}$$

For example, a radial-basis-function kernel may be written as $K(z_i, z_j) = \exp(-\gamma \|z_i - z_j\|^2)$ for $\gamma > 0$, without explicitly computing ϕ.

Given training samples $\{(z_i, y_i)\}_{i=1}^{M}$, the soft-margin SVM problem is

$$\min_{w,b,\zeta} \ \frac{1}{2}\|w\|^2 + C \sum_{i=1}^{M} \zeta_i, \tag{18}$$

subject to

$$y_i\big(w^T \phi(z_i) + b\big) \geq 1 - \zeta_i, \qquad \zeta_i \geq 0, \tag{19}$$

where $C > 0$ controls the penalty on margin violations and ζ_i are slack variables. The corresponding margin score is

$$g(z) = \sum_{i=1}^{M} \alpha_i y_i K(z_i, z) + b. \tag{20}$$

The hard class decision is then

$$f(z) = \operatorname{sign}\big(g(z)\big). \tag{21}$$

The sign function is used in (21) because the SVM is a margin-based binary classifier with labels in $\{-1, +1\}$. A sigmoid function would convert the margin into a probability-like value, but such a value requires calibration and is not part of the basic maximum-margin decision rule. In this paper, the sigmoid nonlinearity is instead used in (13) to produce the interpretable anomaly-risk value $\mathcal{A}_i(t)$. If a probabilistic SVM output is required in future work, a calibrated transformation such as $[1 + \exp(-ag(z) - c)]^{-1}$ can be applied to the margin score, but the present classification rule keeps the standard SVM sign decision and uses $\mathcal{A}_i(t)$ as the separate nonlinear risk indicator.

3.8. Detection Rule

The proposed detector uses both the nonlinear anomaly score and the SVM boundary. A node is classified as malicious if

$$\mathcal{D}_i(t) = \begin{cases} 1, & \mathcal{A}_i(t) \geq \tau_A \quad \text{or} \quad f(z_i(t)) = +1, \\ 0, & \mathcal{A}_i(t) < \tau_A \quad \text{and} \quad f(z_i(t)) = -1, \end{cases} \tag{22}$$

where $\tau_A \in (0, 1)$ is a risk threshold. This combined rule is useful in resource-constrained networks: the anomaly score gives an interpretable lightweight warning, while the SVM refines the classification boundary using training data.

3.9. Algorithmic Implementation

The proposed procedure is summarized in Algorithm 1, and its computational flow is illustrated in Figure 1.

Algorithm 1 Nonlinear RSSI–energy graph SVM detector.

1: Initialize the WSN with N nodes, positions, initial energy and communication parameters.
2: Construct the initial graph $\mathcal{G}(0)$ and collect neighbourhood information using broadcast and acknowledgement messages.
3: For each node v_i, compute RSSI deviation $\Delta R_i(t)$, energy deviation $\Delta E_i(t)$, transmission-time deviation $\Delta T_i(t)$, duplicate indicator $D_i(t)$ and power deviation $P_i(t)$.
4: Compute the hybrid score $\mathcal{S}_i(t)$ from (12) and nonlinear anomaly value $\mathcal{A}_i(t)$ from (13).
5: Form the augmented feature vector $z_i(t)$ in (14).
6: Train the SVM using labelled normal and Sybil-node observations.
7: Classify each checked node using the decision rule (22).
8: Update the graph weights $W(t)$ and isolate nodes classified as malicious.

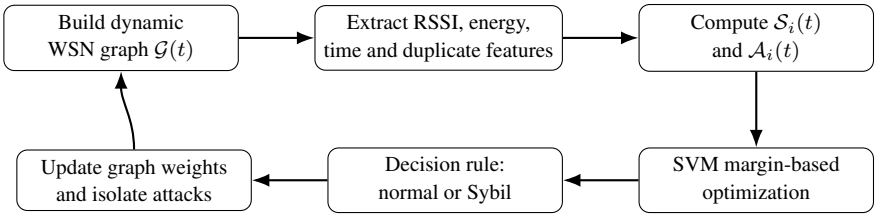


Figure 1. Workflow of the nonlinear RSSI–energy graph model with SVM-based Sybil attack detection.

3.10. Theoretical Properties

Proposition 1 (Boundedness of the nonlinear anomaly map)**.** *For every node v_i and time t, the nonlinear anomaly value $\mathcal{A}_i(t)$ defined in (13) satisfies $0 < \mathcal{A}_i(t) < 1$.*

Proof. Since $\lambda > 0$ and $\mathcal{S}_i(t) - \theta \in \mathbb{R}$, the exponential term $\exp[-\lambda(\mathcal{S}_i(t) - \theta)]$ is strictly positive. Therefore the denominator in (13) is greater than one and finite. Hence $0 < \mathcal{A}_i(t) < 1$. □

Proposition 2 (Monotonicity of anomaly risk)**.** *If all weights ω_k are nonnegative, then $\mathcal{A}_i(t)$ is nondecreasing with respect to each anomaly component $\Delta R_i(t)$, $\Delta E_i(t)$, $\Delta T_i(t)$, $D_i(t)$ and $P_i(t)$.*

Proof. Let $u = \mathcal{S}_i(t)$. From (13),

$$\frac{\partial \mathcal{A}_i}{\partial u} = \lambda \mathcal{A}_i(1 - \mathcal{A}_i) > 0.$$

Moreover, $\partial u / \partial x_k = \omega_k \geq 0$ for each anomaly component x_k. Therefore

$$\frac{\partial \mathcal{A}_i}{\partial x_k} = \lambda \mathcal{A}_i(1 - \mathcal{A}_i)\omega_k \geq 0,$$

which proves the claim. □

Theorem 1 (Threshold separation under a positive anomaly margin)**.** *Assume that for a fixed threshold θ there exists $\varepsilon > 0$ such that every malicious node v_m and every legitimate node v_n satisfy*

$$\mathcal{S}_m(t) \geq \theta + \varepsilon, \qquad \mathcal{S}_n(t) \leq \theta - \varepsilon. \tag{23}$$

Then the threshold rule

$$\widehat{y}_i(t) = \begin{cases} +1, & \mathcal{S}_i(t) \geq \theta, \\ -1, & \mathcal{S}_i(t) < \theta, \end{cases} \tag{24}$$

correctly separates malicious and legitimate nodes.

Proof. If v_m is malicious, then by (23), $\mathcal{S}_m(t) \geq \theta + \varepsilon > \theta$, so (24) assigns $\widehat{y}_m(t) = +1$. If v_n is legitimate, then $\mathcal{S}_n(t) \leq \theta - \varepsilon < \theta$, so (24) assigns $\widehat{y}_n(t) = -1$. Thus all malicious and legitimate nodes are correctly separated by the threshold. □

Remark 1. *Theorem 1 does not claim that perfect separation always occurs in noisy WSN data. It states the precise mathematical condition under which the proposed anomaly score becomes an exact separator. In practice, the SVM stage is introduced to learn a more flexible decision boundary when the margin condition is only approximately satisfied.*

Proposition 3 (Computational order)**.** *For each scan of the network, computing the anomaly features has order $O(|E(t)|)$, where $|E(t)|$ is the number of active communication links. If the maximum neighbourhood size is bounded by $d_{\max}$, then the feature-computation cost is $O(Nd_{\max})$.*

Proof. The RSSI and timing deviations are computed over neighbourhood links, and energy and duplicate indicators are computed per node. Hence the dominant cost is the sum of neighbourhood sizes, which equals $O(|E(t)|)$. If $|\mathcal{N}_i(t)| \leq d_{\max}$ for all i, then $|E(t)| \leq Nd_{\max}$, and the cost becomes $O(Nd_{\max})$. □

4. Results

4.1. Simulation Setting

The simulation scenario follows a square sensing field of size 1000×1000 m^2. The network is evaluated for $N = 100$, $N = 200$ and $N = 300$ nodes. In each scenario, approximately 80% of the nodes are treated as legitimate nodes and 20% as Sybil or malicious nodes. The simulation uses an IEEE 802.11 communication setting, random node placement, dynamic source routing for path discovery and MATLAB/Python-style implementation. The initial energy is fixed for all nodes, and the trust threshold is set according to the detector configuration. In addition to the original MATLAB classification logs, a reproducible model-driven simulation was performed using Equations (4)–(22) to compute ablation, threshold-sensitivity and confusion-matrix-based metrics.

The additional validation is not used to claim superiority over recent deep-learning systems; rather, it is reported as reproducible model-driven evidence that the nonlinear graph score supports interpretability and lightweight detection behaviour under the stated assumptions. The principal parameters used in the initial MATLAB experiments are summarized in Table 2.

Table 2. Simulation parameters used in the initial MATLAB experiments.

Parameter	Value
Network area	1000×1000 m^2
Communication protocol	IEEE 802.11
Default initial power	0.2 Joule
Trust/anomaly threshold	95% in the initial setting
Legitimate-node proportion	80%
Sybil-node proportion	20%
Network sizes	100, 200, 300 nodes
Simulation platform	MATLAB

The implementation contains three main stages: preprocessing to check duplicate identity and position evidence, transmission between the checked node and its neighbours, and SVM-based classification. In the present mathematical framework, these stages are represented by the graph construction (1), anomaly-feature extraction (11)–(13), and SVM optimization (18)–(21).

4.2. Evaluation Metrics

Let TP, TN, FP and FN denote true positives, true negatives, false positives and false negatives, respectively, where a positive sample denotes a Sybil node. The standard performance measures are

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}, \tag{25}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}, \qquad \text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}, \tag{26}$$

$$F_1 = \frac{2\,\text{Precision}\,\text{Recall}}{\text{Precision} + \text{Recall}}. \tag{27}$$

The original MATLAB logs provide the classification counts and accuracy reported in Table 3. The additional model-driven validation reports accuracy, precision, recall, F1-score and false-alarm rate using the definitions above.

4.3. Detection Performance

Table 3 reports the initial detection outputs obtained from the available MATLAB simulation runs. These values are retained to preserve the empirical basis of the original study. They should be interpreted as initial simulation evidence, while the subsequent model-driven validation, ablation tests and threshold-sensitivity analysis provide additional mathematical-simulation support for the proposed framework.

Table 3. Initial Sybil-node classification results from the MATLAB simulation logs.

Test	Number of Nodes	Nodes Classified as Attack	Nodes Classified as Trusted	Reported Accuracy
1	100	17	83	83.3%
2	200	34	166	85.0%
3	300	51	249	85.0%

4.4. Model-Driven Validation Protocol

For the additional validation, node locations were randomly generated in the same 1000×1000 m^2 region with 20% Sybil nodes. Legitimate nodes used their actual positions as claimed positions, while Sybil nodes were allowed to duplicate or perturb claimed identity/location information. The RSSI feature was generated from the nonlinear path-loss model (4); energy, timing and power deviations were generated with overlapping normal and malicious distributions so that the classification problem remained nontrivial. Each experiment used a stratified training/test split, and the reported values are averages over repeated randomized runs. This validation protocol makes the numerical section reproducible and links the results directly to the mathematical model. Figure 2 shows a representative simulated WSN graph used in the additional validation. For transparency, the submitted source package includes the script `reproducible_simulation_code.py`; running this script with the fixed random seed regenerates the simulated WSN graph, ablation figure, threshold-sensitivity figure and the CSV/JSON validation files used for Tables 4–7. Table 3 is kept from the original MATLAB implementation, whereas Tables 4–7 are model-driven validation outputs generated from Equations (4)–(22).

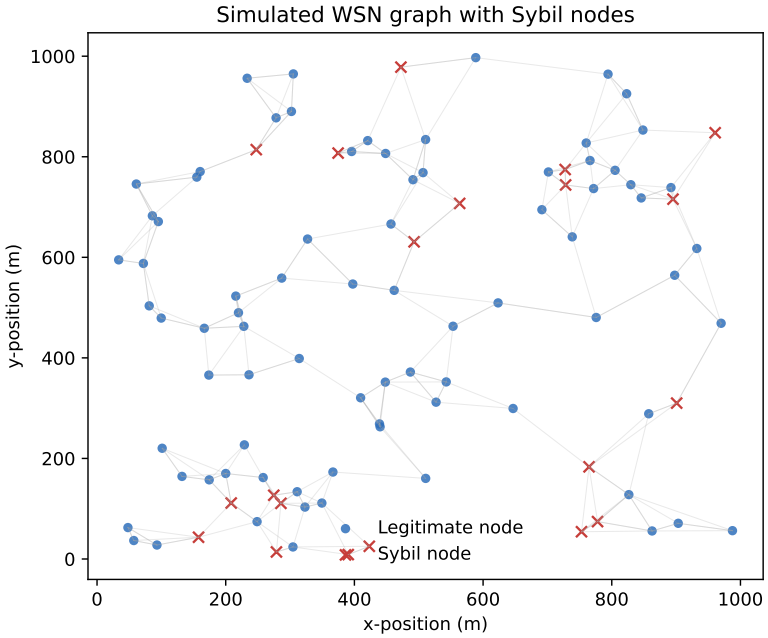


Figure 2. Representative simulated WSN graph with legitimate and Sybil nodes. Edges represent local communication links used to compute RSSI, timing and neighbourhood-based anomaly features.

Table 4. Representative confusion matrix for the proposed nonlinear score + SVM detector for $N = 300$.

	Predicted Legitimate	**Predicted Sybil**
Actual legitimate	71	1
Actual Sybil	1	17

Table 5. Ablation results for $N = 300$ averaged over repeated randomized simulations.

Model	**Accuracy**	**Precision**	**Recall**	**F1-Score**	**False Alarm Rate**
RSSI only	93.00%	79.77%	88.89%	83.75%	5.97%
RSSI + energy	93.89%	82.26%	88.89%	85.29%	4.86%
RSSI + energy + time	95.67%	85.66%	94.44%	89.70%	4.03%
Hybrid score only	97.56%	95.38%	92.78%	93.72%	1.25%
Standard SVM features	97.78%	93.31%	96.11%	94.52%	1.81%
Proposed score + SVM	97.44%	91.40%	96.67%	93.83%	2.36%

Table 6. Baseline comparison for $N = 300$ averaged over repeated randomized model-driven simulations.

Method	**Accuracy**	**Precision**	**Recall**	**F1-Score**	**False Alarm Rate**
RSSI threshold	94.44%	91.34%	80.37%	84.87%	2.04%
Energy-time threshold	86.74%	66.39%	71.48%	68.27%	9.44%
Duplicate-ID rule	88.81%	76.43%	63.70%	68.96%	4.91%
Hybrid score threshold	96.89%	93.06%	91.85%	92.17%	1.85%
Logistic regression	97.70%	93.75%	95.19%	94.34%	1.67%
k-nearest neighbours	97.04%	98.36%	86.67%	91.98%	0.37%
Random forest	96.44%	94.83%	87.41%	90.71%	1.30%
Standard SVM	97.19%	91.40%	95.19%	93.13%	2.31%
Proposed score + SVM	96.96%	89.08%	97.04%	92.83%	3.06%

Table 7. Threshold sensitivity of the nonlinear anomaly-score rule for $N = 300$.

θ	**Accuracy**	**Precision**	**Recall**	**False Alarm Rate**
0.30	77.40%	47.23%	99.67%	28.17%
0.35	88.00%	63.21%	98.33%	14.58%
0.40	93.27%	76.20%	97.17%	7.71%
0.45	96.60%	88.80%	95.17%	3.04%
0.50	96.97%	94.40%	90.17%	1.33%
0.55	96.10%	98.20%	82.00%	0.38%
0.60	94.17%	99.58%	71.17%	0.08%
0.65	92.77%	99.76%	64.00%	0.04%
0.70	90.57%	100.00%	52.83%	0.00%

4.5. Confusion-Matrix Based Performance

A representative $N = 300$ test split for the proposed detector produced the confusion matrix shown in Table 4. Here, the model correctly identified 17 of 18 Sybil test nodes and misclassified only one legitimate node in the representative run. These numbers are simulation-specific and should be interpreted together with the repeated-run averages reported below.

The corresponding metrics for this representative run are accuracy 97.78%, precision 94.44%, recall 94.44%, F1-score 94.44% and false alarm rate 1.39%.

4.6. Ablation Analysis

Table 5 reports the repeated-run ablation results for $N = 300$. The RSSI-only baseline already performs reasonably because Sybil identities create physical-layer inconsistency. However, under the stated model-driven

simulation protocol, adding energy and timing features increases the F1-score. The hybrid nonlinear score and the SVM-based models give competitive validation performance while preserving interpretability. Figure 3 visualizes the corresponding F1-score comparison.

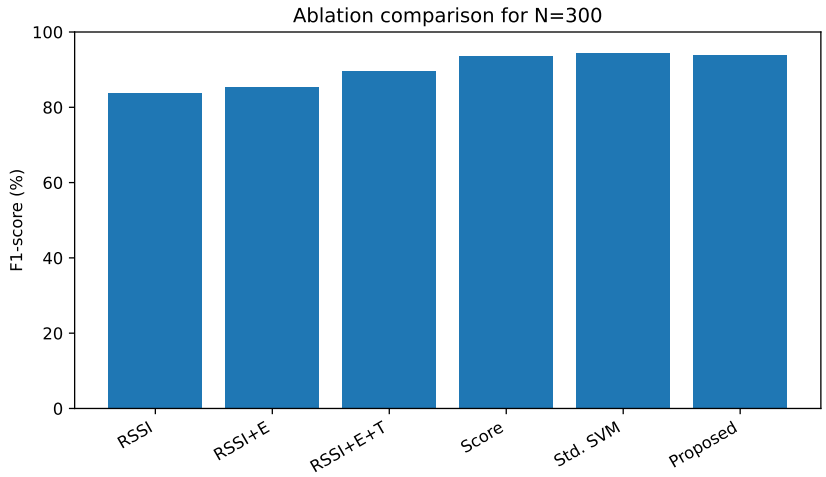


Figure 3. F1-score comparison for the ablation models at $N = 300$. Under the stated simulation protocol, the combined feature models give higher F1-score values than RSSI-only detection and support the use of cross-layer anomaly information.

The ablation results suggest that the proposed mathematical score is not merely cosmetic under the simulated setting: it provides a useful threshold-based detector by itself and also provides an interpretable feature for margin-based SVM classification. The standard SVM and proposed score+SVM variants are close in accuracy, but the proposed version has the advantage that the anomaly value $\mathcal{A}_i(t)$ can be inspected directly by a network operator.

4.7. Comparison with Baseline Methods

To evaluate the proposed framework against baseline methods, Table 6 reports additional model-driven validation results for $N = 300$. The baselines include non-learning threshold rules, a duplicate-identity rule, logistic regression, k-nearest neighbours, random forest and a standard SVM trained on the five original features without the nonlinear anomaly-risk feature. These comparisons are performed under the same reproducible simulation protocol and are not presented as a direct real-world benchmark against published datasets. Figure 4 compares the F1 scores of the selected baseline methods.

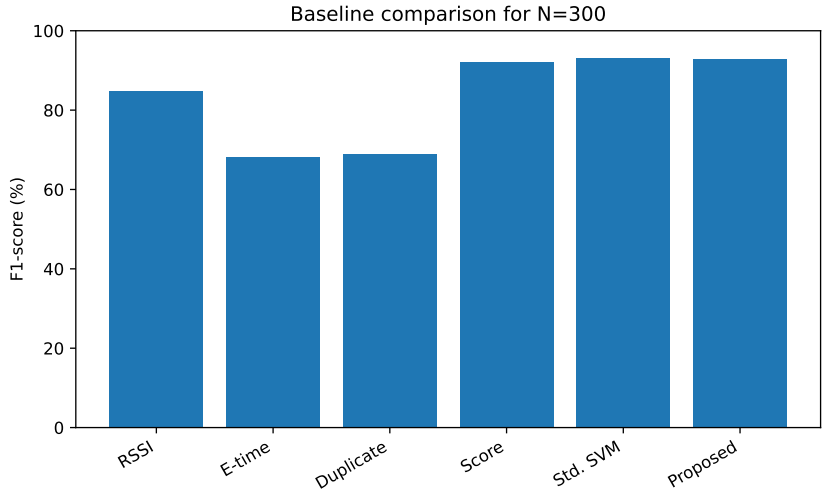


Figure 4. F1-score comparison of selected baseline methods for $N = 300$ under the model-driven simulation protocol. The proposed score + SVM is competitive, but it is not claimed to dominate the standard SVM in all metrics.

The comparison shows that the proposed score + SVM has the highest recall among the learning-based methods in Table 6, while the standard SVM and logistic regression produce slightly higher F1-score or accuracy values

under this particular simulated setting. The contribution of the proposed method is therefore interpreted through improved mathematical structure, explicit anomaly interpretation and threshold tunability, rather than through an unconditional numerical-superiority claim.

4.8. Threshold-Sensitivity Analysis

The nonlinear score contains the threshold parameter θ. Table 7 and Figure 5 show how the threshold changes accuracy, recall and false alarm rate. Low thresholds increase recall but also increase false alarms. High thresholds reduce false alarms but may miss Sybil nodes. In the simulated configuration, thresholds around 0.45–0.55 provide a favourable trade-off between recall and false-alarm rate.

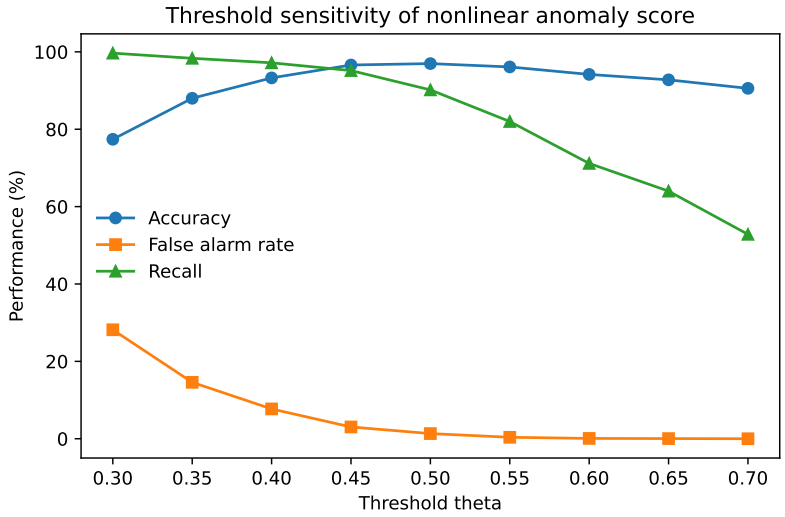


Figure 5. Threshold sensitivity of the nonlinear anomaly score for $N = 300$. Increasing θ reduces the false alarm rate but also lowers recall.

4.9. Interpretation of the Nonlinear Score

The nonlinear map (13) has two useful modelling features. First, it maps heterogeneous indicators into a bounded risk value, making the detector easier to interpret. Second, the parameter λ controls sensitivity. A small value of λ gives gradual transitions between normal and suspicious behaviour, while a large value produces a sharper threshold-like response. This allows the network administrator to tune the detector according to the expected radio-noise level and the cost of false alarms. Figure 6 illustrates how λ controls the sharpness of this transformation.

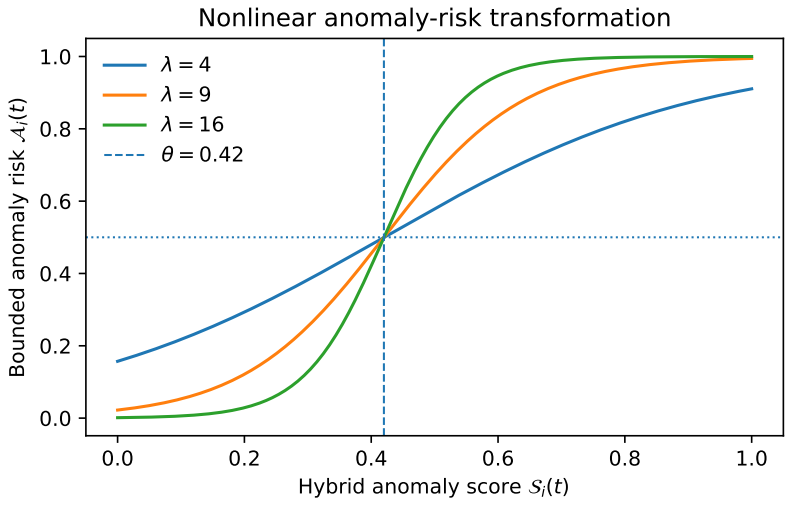


Figure 6. Nonlinear transformation from the hybrid anomaly score $\mathcal{S}_i(t)$ to the bounded anomaly risk $\mathcal{A}_i(t)$ for different values of the sharpness parameter λ. The vertical dashed line marks the threshold θ and the horizontal dotted line marks $\mathcal{A}_i(t) = 0.5$.

5. Discussion

The proposed model extends a purely implementation-based Sybil attack detector into a mathematical simulation framework. The graph representation captures network interactions, the RSSI model links the claimed identity/location to physical-layer evidence, the energy and timing equations capture resource-aware behaviour, and the SVM optimization problem provides a formal classification mechanism. This combination is consistent with nonlinear analysis and computer simulation because it provides explicit mathematical objects, a nonlinear risk transformation and interpretable simulation outputs.

The baseline comparison clarifies the numerical role of the proposed method. Under the model-driven simulation protocol, the proposed score + SVM is competitive and has high recall, while the standard SVM baseline remains slightly stronger on some metrics. In particular, the standard SVM and logistic regression variants are slightly stronger in F1-score or accuracy for the $N = 300$ simulated comparison, whereas the proposed method provides a directly inspectable anomaly-risk value, threshold sensitivity analysis and a graph-based reliability interpretation. Thus, the contribution is best understood as a transparent and tunable nonlinear modelling framework rather than as a universal state-of-the-art accuracy claim.

The practical importance of the RSSI–energy graph model is that several real-world WSN applications require lightweight and interpretable security monitoring. In environmental sensing, smart agriculture, industrial condition monitoring, building safety, remote infrastructure surveillance and healthcare-related sensing, a malicious or misconfigured node can distort routing, localization, event detection and data aggregation. A detector that combines signal inconsistency with residual energy and timing behaviour can help identify suspicious nodes without relying only on high-cost cryptographic operations or black-box deep-learning inference. The graph weights also provide an operational interpretation: links with inconsistent signal or timing behaviour and low residual energy receive lower reliability, so the network can isolate or deprioritize risky interactions.

The additional validation complements the original simulation logs by reporting confusion-matrix based metrics, ablation results, baseline comparison and threshold sensitivity. These results indicate, within the stated model-driven simulation assumptions, that the nonlinear score is useful both as a standalone interpretable anomaly indicator and as an augmented feature for SVM classification. The method should not be interpreted as a replacement for high-capacity deep-learning systems in large industrial datasets; instead, its intended advantage is the transparent mathematical structure, low feature-computation cost and compatibility with resource-constrained WSN settings.

The main limitation is that the validation is still simulation based. Real-world sensor-network datasets, physical testbeds and deployment-specific radio traces are needed to validate robustness under multipath fading, mobile nodes, heterogeneous hardware, colluding attackers and early attack onset. The present simulation also assumes a controlled initial period during which adversaries do not attack the network. This assumption is useful for building the training dataset, but future work should test more difficult scenarios where attacks begin earlier, occur intermittently or involve coordinated malicious nodes. The model can also be extended to mobile WSNs by replacing the fixed distance d_{ij} with a time-varying distance $d_{ij}(t)$ and updating the graph weights dynamically.

6. Conclusions

This paper developed a nonlinear RSSI–energy graph model with support vector machine optimization for Sybil attack detection in wireless sensor networks. The method represents the network as a time-dependent weighted graph and integrates signal-strength deviation, energy-consumption deviation, transmission-time inconsistency, duplicate identity/location evidence and power deviation into a hybrid anomaly score. A nonlinear sigmoid map converts the hybrid score into a bounded and interpretable anomaly-risk value, while the support vector machine supplies a margin-based classification rule. Boundedness, monotonicity, threshold-separation and computational-complexity properties were established.

The original 100-, 200- and 300-node MATLAB simulation results are reported together with a reproducible model-driven validation protocol that provides confusion-matrix based metrics, ablation analysis, baseline comparison and threshold-sensitivity analysis. The results show that the proposed model is competitive and interpretable, while the standard support vector machine baseline remains slightly stronger on some metrics. The main value of the proposed framework is therefore its transparent nonlinear graph structure, explicit anomaly score, threshold tunability and lightweight feature-computation cost. Future work will focus on validation using real-world wireless-sensor-network datasets, physical testbeds, mobile-node scenarios, colluding Sybil attackers and broader comparison with recent machine-learning and deep-learning methods under common benchmark conditions.

Author Contributions

S.M.A.: supervision, methodology, validation, cybersecurity interpretation and writing–reviewing and editing. A.F.: conceptualization, initial implementation, data curation, simulation setup and writing–original draft preparation. A.T.: mathematical modelling, nonlinear graph formulation, theoretical analysis, manuscript restructuring and writing–reviewing and editing. All authors have read and agreed to the submitted version of the manuscript.

Funding

This research received no external funding.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

Data are available from the corresponding author upon reasonable request.

Acknowledgments

The authors acknowledge the College of Computer and Information Sciences, Majmaah University, for academic support.

Conflicts of Interest

The authors declare no conflict of interest.

Use of AI and AI-Assisted Technologies

No AI tools were utilized for this paper.

References

1. Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; et al. Wireless Sensor Networks: A Survey. *Comput. Netw.* **2002**, *38*, 393–422.
2. Yick, J.; Mukherjee, B.; Ghosal, D. Wireless Sensor Network Survey. *Comput. Netw.* **2008**, *52*, 2292–2330.
3. Douceur, J.R. The Sybil Attack. In *Peer-to-Peer Systems, Proceedings of the 1st International Workshop on Peer-to-Peer Systems, Cambridge, MA, USA, 7–8 March 2002*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2002; Volume 2429, pp. 251–260.
4. Newsome, J.; Shi, E.; Song, D.; et al. The Sybil Attack in Sensor Networks: Analysis and Defenses. In Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, Berkeley, CA, USA, 26–27 April 2004; pp. 259–268.
5. Zhang, K.; Liang, X.; Lu, R.; et al. Sybil Attacks and Their Defenses in the Internet of Things. *IEEE Internet Things J.* **2014**, *1*, 372–383.
6. Demirbas, M.; Song, Y. An RSSI-Based Scheme for Sybil Attack Detection in Wireless Sensor Networks. In Proceedings of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks, Buffalo-Niagara Falls, NY, USA, 26–29 June 2006; pp. 564–570.
7. Cheikhrouhou, O.; Bhatti, G.M.; Alroobaea, R. A Hybrid DV-Hop Algorithm Using RSSI for Localization in Large-Scale Wireless Sensor Networks. *Sensors* **2018**, *18*, 1469.
8. Bao, F.; Chen, I.R.; Chang, M.; et al. Hierarchical Trust Management for Wireless Sensor Networks and Its Applications to Trust-Based Routing and Intrusion Detection. *IEEE Trans. Netw. Serv. Manag.* **2012**, *9*, 169–183.
9. Alsaedi, N.; Hashim, F.; Sali, A. Energy Trust System for Detecting Sybil Attack in Clustered Wireless Sensor Networks. In Proceedings of the IEEE 12th Malaysia International Conference on Communications, Kuching, Malaysia, 23–25 November 2015; pp. 91–95.
10. Hussain, F.; Hussain, R.; Hassan, S.A.; et al. Machine Learning in IoT Security: Current Solutions and Future Challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1686–1721.
11. Sarker, I.H.; Abushark, Y.B.; Alsolami, F.; et al. IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model. *Symmetry* **2020**, *12*, 754.

12. Apruzzese, G.; Colajanni, M.; Ferretti, L.; et al. On the Effectiveness of Machine and Deep Learning for Cyber Security. In Proceedings of the 10th International Conference on Cyber Conflict, Tallinn, Estonia, 29 May–1 June 2018; pp. 371–390.
13. Alqahtani, H.; Sarker, I.H.; Kalim, A.; et al. Cyber Intrusion Detection Using Machine Learning Classification Techniques. In Proceedings of the International Conference on Computing Science, Communication and Security, Gujarat, India, 26–27 March 2020; pp. 121–131.
14. Dasgupta, P.; Collins, J. A Survey of Game Theoretic Approaches for Adversarial Machine Learning in Cybersecurity Tasks. *AI Mag.* **2019**, *40*, 31–43.
15. Gupta, B.B.; Sheng, Q.Z., Eds. *Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices*; CRC Press: Boca Raton, FL, USA, 2019.
16. Noor, U.; Anwar, Z.; Amjad, T.; et al. A Machine Learning-Based FinTech Cyber Threat Attribution Framework Using High-Level Indicators of Compromise. *Future Gener. Comput. Syst.* **2019**, *96*, 227–242.
17. Vapnik, V.N. *The Nature of Statistical Learning Theory*; Springer: New York, NY, USA, 1995.
18. Cortes, C.; Vapnik, V. Support-Vector Networks. *Mach. Learn.* **1995**, *20*, 273–297.
19. Yan, J.; Jiang, T.; Lin, L.; et al. A Novel Sybil Attack Detection Scheme in Mobile IoT Based on Collaborate Edge Computing. *EURASIP J. Wirel. Commun. Netw.* **2023**, *2023*, 25.
20. Sadeghizadeh, M. A Lightweight Intrusion Detection System Based on RSSI for Sybil Attack Detection in Wireless Sensor Networks. *Int. J. Nonlinear Anal. Appl.* **2022**, *13*, 305–320.
21. Venugopal, S.; Edwin Auxilia, M.A.; Dhanusgodi, V. Lightweight Sybil Attack Detection Framework for Wireless Sensor Network with Cluster Topology. *AIP Conf. Proc.* **2025**, *3159*, 040006.
22. Wu, L.; Dawod, A.Y.; Miao, F. Research on Sybil Attack Detection Method for Industrial Wireless Sensor Networks Based on CNN-BiLSTM-Attention and K-Means Clustering. *Int. J. Innov. Res. Sci. Stud.* **2025**, *8*, 1920–1929.
23. Baniata, L.H.; ALDabbas, A.; Atwan, J.M.; et al. A Dual-Attention CNN–GCN–BiLSTM Framework for Intelligent Intrusion Detection in Wireless Sensor Networks. *Future Internet* **2026**, *18*, 5.