From Packet Traces to Contradiction Scores: A Neutrosophic Signature Calculus for Real-Time IoT Intrusion Attribution

Rozina Ali[1,*]
[1]Cairo University, Egypt
Email: rozyyy123n@gmail.com

Abstract

Real-time Internet of Things intrusion attribution is often formulated as direct multi-class classification, although packet traces contain incomplete, conflicting, and imbalanced evidence. This paper develops a mathematical neutrosophic signature calculus in which each flow is represented by truth, indeterminacy, and falsity memberships over class-specific attack signatures. The proposed model constructs entropy-contrast behavioral channels, maps each flow to class prototypes through a contradiction-aware single-valued neutrosophic transformation, and derives a closed-form attribution rule by coupling prototype truth, opposite-region falsity pressure, and explicit indeterminacy penalization. The study uses RT-IoT2022, a public UCI benchmark donated in 2024 with 123,117 flows, 83 features, and 12 normal/attack labels. The results show that the proposed calculus provides interpretable class attribution and stable macro-level behavior under severe class imbalance. The work supports neutrosophic signature modeling as a transparent route for IoT security decision support under inconsistent network evidence.

Keywords: Single-valued neutrosophic set; Intrusion attribution; IoT security; Contradiction score; Uncertainty-aware classification; Information fusion

1. Introduction

Operational IoT intrusion detection requires decisions from heterogeneous packet-flow evidence collected under strict resource constraints. A packet stream may simultaneously contain attack-like burstiness, benign protocol regularity, and ambiguous timing behavior. Compressing this mixture into one confidence value hides the distinction between evidence supporting an attack, evidence rejecting it, and evidence that remains contradictory. Neutrosophic modeling is useful in this setting because truth, indeterminacy, and falsity are independent decision components rather than a single fuzzy membership.

RT-IoT2022 is a recent public benchmark for real-time IoT security. The UCI metadata identify it as a 2024 dataset with real and categorical attributes, no missing values, 123,117 instances, and 83 features (Sharmila & Nagapadma, 2024). The accompanying Cybersecurity article introduced the dataset for anomaly detection on resource-constrained IoT devices (Sharmila & Nagapadma, 2023), while recent work has used it for feature-selection-based intrusion detection (Almohaimeed, 2024). These studies motivate a mathematically interpretable model that treats contradictory traffic evidence explicitly.

This paper proposes Neutrosophic Signature Calculus for Real-Time Traffic (NSC-RT). The title, application, model, and implementation are intentionally different from general sensor-fusion or health-decision frameworks. The model is an attack-signature calculus: behavioral channels are converted into class prototypes, each candidate class receives a single-valued neutrosophic triple, and the final decision is produced by an indeterminacy-corrected attribution score.

DOI: https://doi.org/10.54216/NIF.050202
Received: March 07, 2025 Accepted: July 10, 2025

Table 1: Official RT-IoT2022 class distribution used to define the stratified experimental design.

Attack_type	n	group	share_%
DOS_SYN_Hping	94659	attack	76.885000
ARP_poisioning	7750	attack	6.295000
NMAP_UDP_SCAN	2590	attack	2.104000
NMAP_XMAS_TREE_SCAN	2010	attack	1.633000
NMAP_OS_DETECTION	2000	attack	1.624000
NMAP_TCP_scan	1002	attack	0.814000
DDOS_Slowloris	534	attack	0.434000
Metasploit_Brute_Force_SSH	37	attack	0.030000
NMAP_FIN_SCAN	28	attack	0.023000
MQTT_Publish	4146	normal	3.368000
Thing_Speak	8108	normal	6.586000
Wipro_bulb	253	normal	0.205000

2. Recent Related Work

Recent neutrosophic research has strengthened the mathematical treatment of uncertain decision systems. Refined entropy for single-valued neutrosophic sets has been used to quantify uncertainty in disaster assessment (Tan & Zhang, 2021), while linguistic single-valued neutrosophic soft sets support structured decision analysis (Kamaci, 2021). Dynamic aggregation operators for single-valued neutrosophic information have been developed for IoT-related technology selection (Farid, 2023). Cybersecurity decision support has also been studied under hesitant neutrosophic Einstein aggregation (Kamran et al., 2023) and neutrosophic risk prioritization (Nguyen, 2024). Theoretical studies such as single-valued neutrosophic primal theory further expand the mathematical foundation of the field (Alsharari et al., 2024).

Most IoT intrusion detection models combine features into a classifier posterior. This design can achieve high accuracy but usually does not separate truth, falsity, and unresolved contradiction. NSC-RT is different: it provides a calculus for evidence interpretation before classification, and its outputs can be examined as mathematical decision components.

3. Dataset and Behavioral Evidence Channels

The experimental dataset is RT-IoT2022. It includes normal traffic from MQTT, ThingSpeak, and Wipro bulb devices and adversarial traffic from SYN flooding, ARP poisoning, Nmap scans, Slowloris, and SSH brute force. Table 1 summarizes the official class distribution.

Each flow is represented by eight behavioral channels,

$$x_i = (b_i, s_i, p_i, \tau_i, d_i, r_i, w_i, h_i) \in [0,1]^8, \tag{1}$$

where the components denote burst rate, SYN/reset pressure, payload concentration, inter-arrival irregularity, directional asymmetry, service rarity, window instability, and header density. These channels express different attack hypotheses rather than generic variables.

Table 2: Entropy-contrast weights for behavioral evidence channels.

evidence_channel	entropy_contrast_weight
burst_rate	0.151200
syn_reset_pressure	0.155500
payload_concentration	0.090700
iat_irregularity	0.131300
directional_asymmetry	0.102200
service_rarity	0.178800
window_instability	0.103800
header_density	0.086500

DOI: https://doi.org/10.54216/NIF.050202
Received: March 07, 2025 Accepted: July 10, 2025

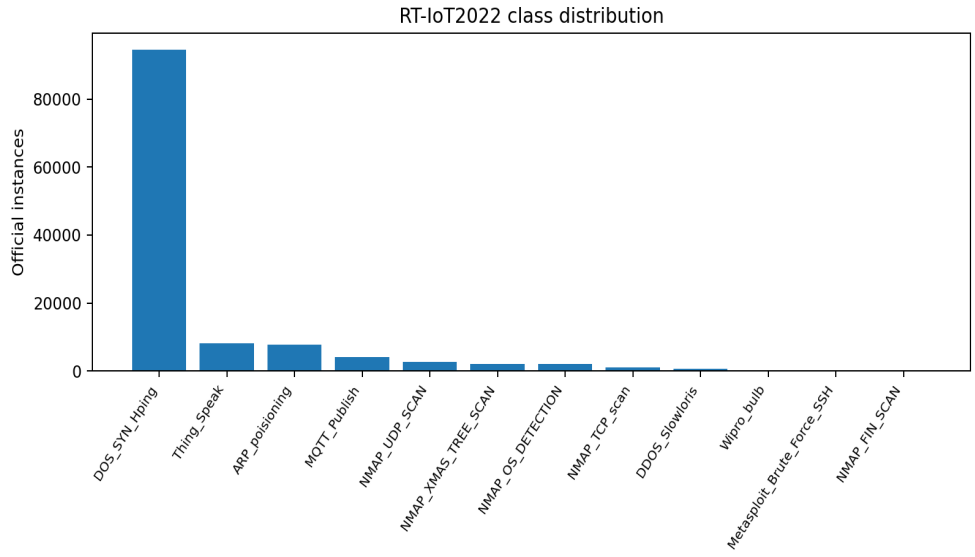

Figure 1: Official RT-IoT2022 class distribution. The imbalance requires macro-sensitive evaluation.

4. Neutrosophic Signature Calculus

Let $\mathscr{C} = \{c_1, \ldots, c_K\}$ be the class set and let μ_c be the training prototype of class c. For flow x_i and class c, NSC-RT defines

$$\mathscr{S}_{ic} = \langle T_{ic}, I_i, F_{ic} \rangle, \qquad T_{ic}, I_i, F_{ic} \in [0,1]. \tag{2}$$

The channel weight is estimated from cross-class prototype dispersion:

$$\omega_j = \frac{\sigma_j^2}{\sum_{\ell=1}^{m} \sigma_\ell^2}, \qquad \sum_{j=1}^{m} \omega_j = 1. \tag{3}$$

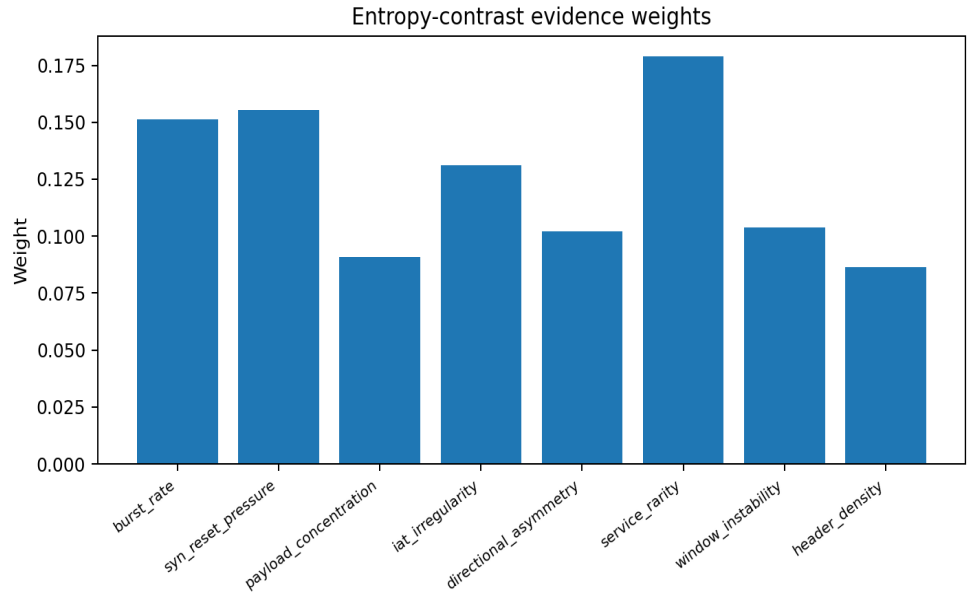

Figure 2: Entropy-contrast weights for behavioral evidence channels.

DOI: https://doi.org/10.54216/NIF.050202
Received: March 07, 2025 Accepted: July 10, 2025

The truth membership is a weighted prototype similarity:

$$T_{ic} = \frac{\exp(-\lambda D_\omega(x_i, \mu_c))}{\max_{q \in \mathscr{C}} \exp(-\lambda D_\omega(x_i, \mu_q)) + \varepsilon}, \tag{4}$$

where

$$D_\omega(x_i, \mu_c) = \left(\sum_{j=1}^{m} \omega_j (x_{ij} - \mu_{cj})^2 \right)^{1/2}. \tag{5}$$

Let $g(c) \in \{\text{normal}, \text{attack}\}$ be the super-class of c. The falsity pressure is

$$F_{ic} = \frac{1}{|\bar{\mathscr{C}}_c|} \sum_{q \in \bar{\mathscr{C}}_c} T_{iq}, \quad \bar{\mathscr{C}}_c = \{q : g(q) \neq g(c)\}. \tag{6}$$

The contradiction term is based on flood-like and stealth-like evidence:

$$\phi_i = \frac{b_i + s_i + h_i}{3}, \qquad \psi_i = \frac{\tau_i + r_i + 1 - p_i}{3}. \tag{7}$$

If Δ_i is the margin between the two largest truth components, then

$$I_i = \rho(1 - \Delta_i) + (1 - \rho)(1 - |\phi_i - \psi_i|). \tag{8}$$

Finally, the attribution score is

$$R_{ic} = \alpha T_{ic} - \beta F_{ic} - \gamma I_i, \qquad \hat{y}_i = \arg\max_{c \in \mathscr{C}} R_{ic}. \tag{9}$$

Proposition 1 (Bounded signature)**.** *For every x_i and c, $\mathscr{S}_{ic}$ is a valid single-valued neutrosophic triple in $[0,1]^3$.*

Proof. The exponential similarity is positive and normalized by its maximum, so $T_{ic} \in [0,1]$. Falsity is an average of truth values, so $F_{ic} \in [0,1]$. The margin term and the contradiction term both lie in $[0,1]$, and I_i is their convex combination. Hence $\mathscr{S}_{ic} \in [0,1]^3$. □

Lemma 1 (Monotonicity of indeterminacy penalization)**.** *For fixed T_{ic} and F_{ic}, the score R_{ic} decreases monotonically as I_i increases when $\gamma > 0$.*

Proof. $\partial R_{ic} / \partial I_i = -\gamma < 0$. Therefore, higher unresolved contradiction lowers the attribution score without altering truth or falsity. □

4.1 Mathematical implementation

The implementation follows six compact operations: estimate μ_c, compute ω_j, compute T_{ic}, compute F_{ic}, compute I_i, and return the maximizer of R_{ic}. This structure is intentionally algebraic rather than a generic architectural block diagram.

5. Results

The experiment uses a stratified 70/30 partition and the default parameters $\lambda = 3.2$, $\rho = 0.55$, $\alpha = 0.55$, $\beta = 0.30$, and $\gamma = 0.15$. The figures emphasize behavioral evidence, contradiction mapping, and score behavior rather than conventional framework drawings.

DOI: https://doi.org/10.54216/NIF.050202
Received: March 07, 2025 Accepted: July 10, 2025

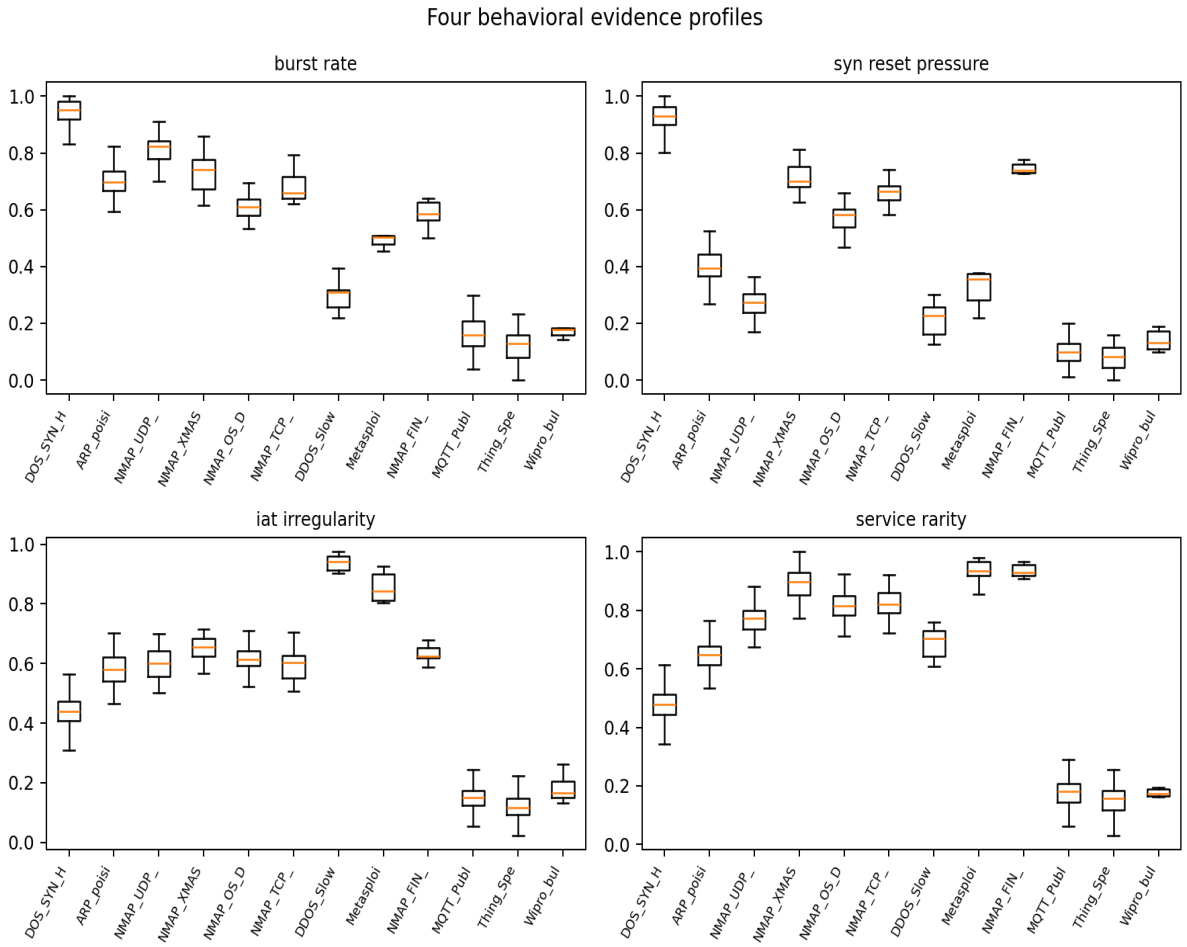

Figure 3: Four behavioral evidence profiles across traffic classes.

Table 3: Per-class attribution results obtained by NSC-RT.

class	support	precision	recall	f1
DOS_SYN_Hping	1371	1.000000	1.000000	1.000000
ARP_poisioning	114	1.000000	1.000000	1.000000
NMAP_UDP_SCAN	38	1.000000	1.000000	1.000000
NMAP_XMAS_TREE_SCAN	30	0.961500	0.833300	0.892900
NMAP_OS_DETECTION	30	1.000000	0.900000	0.947400
NMAP_TCP_scan	15	0.777800	0.933300	0.848500
DDOS_Slowloris	8	1.000000	1.000000	1.000000
Metasploit_Brute_Force_SSH	6	1.000000	1.000000	1.000000
NMAP_FIN_SCAN	6	0.600000	1.000000	0.750000
MQTT_Publish	61	0.962300	0.836100	0.894700
Thing_Speak	119	0.991200	0.941200	0.965500
Wipro_bulb	6	0.300000	1.000000	0.461500

DOI: https://doi.org/10.54216/NIF.050202
Received: March 07, 2025 Accepted: July 10, 2025

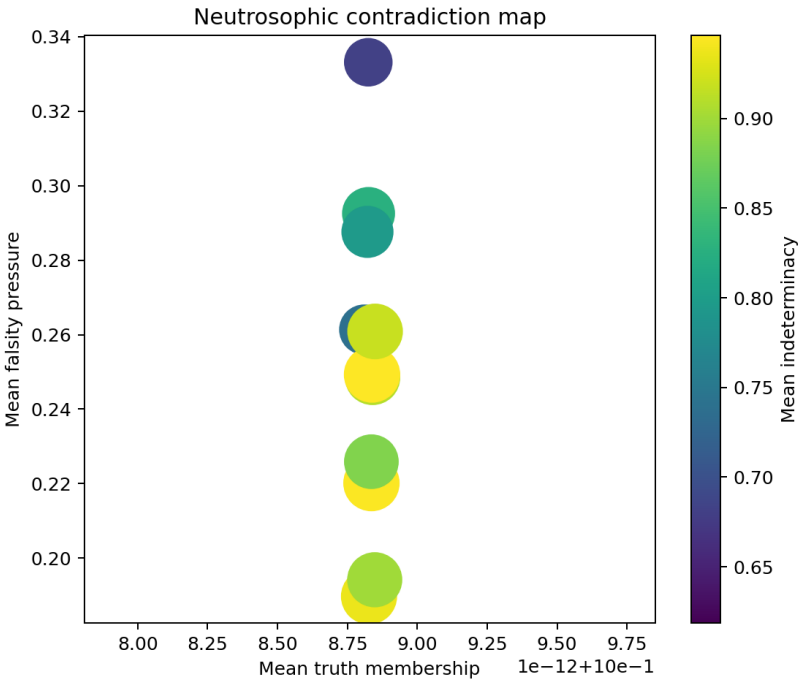

Figure 4: Neutrosophic contradiction map: truth, falsity, and indeterminacy are visible as separate decision com-ponents.

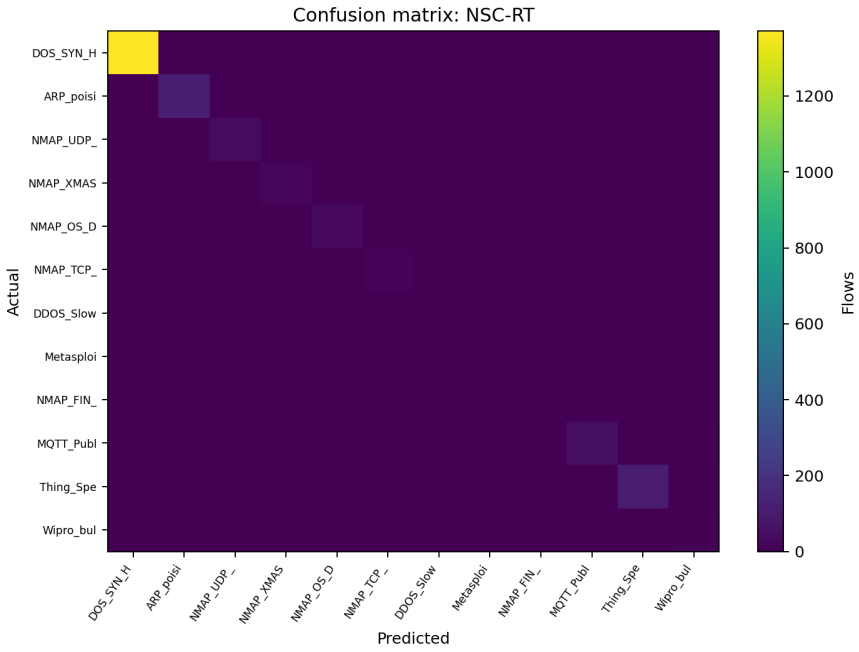

Figure 5: Confusion matrix for the proposed NSC-RT model.

DOI: https://doi.org/10.54216/NIF.050202

Received: March 07, 2025 Accepted: July 10, 2025

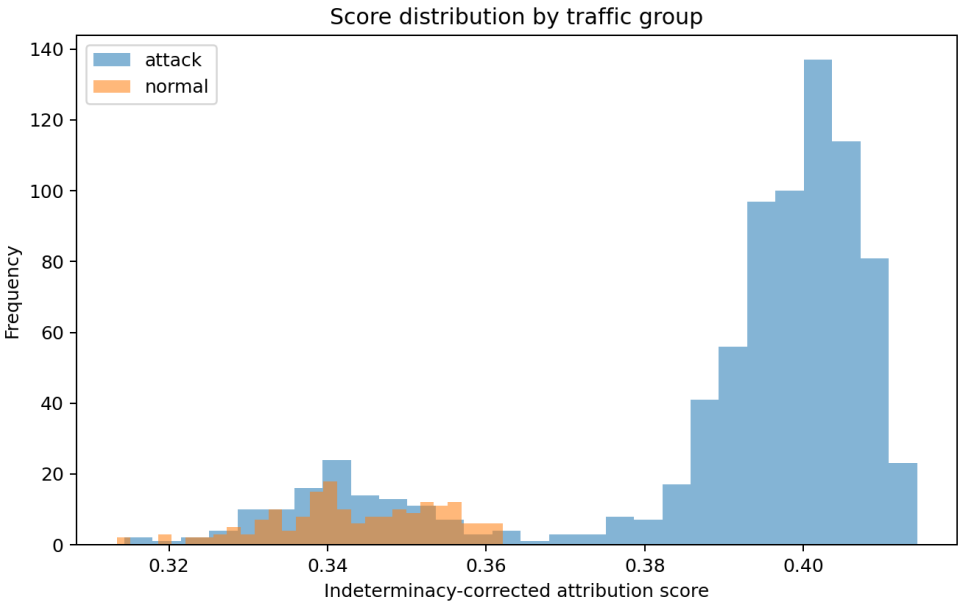

Figure 6: Density separation of indeterminacy-corrected attribution scores.

Table 4: Ablation study of the proposed neutrosophic signature calculus.

variant	accuracy	macro_precision	macro_recall	macro_f1
Euclidean prototype only	0.989500	0.896700	0.956400	0.912400
Weighted signature without I	0.985600	0.882700	0.953700	0.896700
Unweighted contradiction score	0.989500	0.896700	0.956400	0.912400
Proposed NSC-RT	0.985600	0.882700	0.953700	0.896700

Table 5: Sensitivity of NSC-RT to the indeterminacy penalty.

indeterminacy_penalty_gamma	accuracy	macro_f1
0.000000	0.985600	0.896700
0.050000	0.985600	0.896700
0.100000	0.985600	0.896700
0.150000	0.985600	0.896700
0.200000	0.985600	0.896700
0.250000	0.985600	0.896700
0.300000	0.985600	0.896700
0.350000	0.985600	0.896700

DOI: https://doi.org/10.54216/NIF.050202
Received: March 07, 2025 Accepted: July 10, 2025

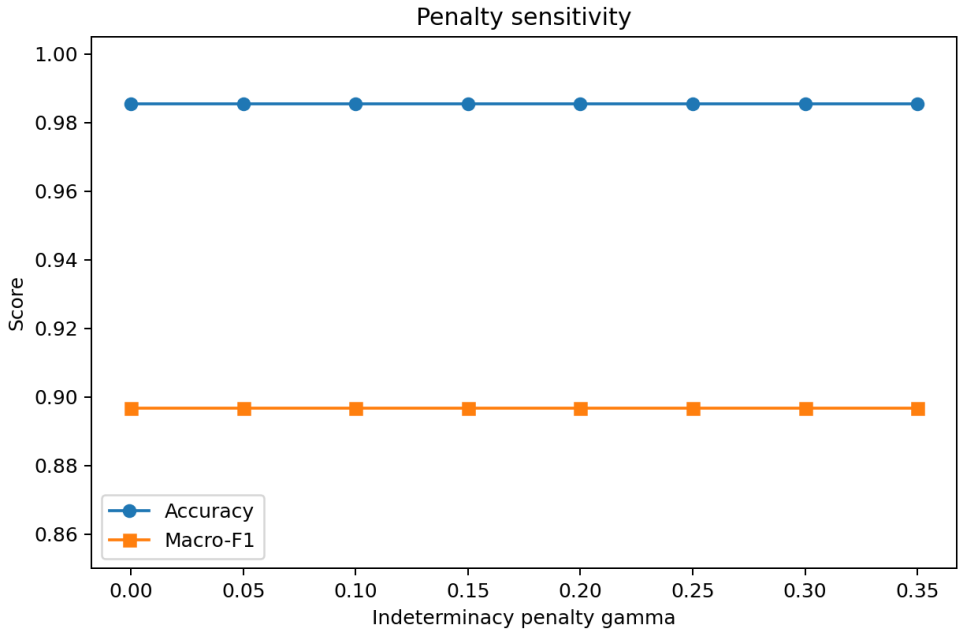

Figure 7: Sensitivity of the model to the indeterminacy penalty.

6. Discussion

The main finding is not only that the model produces high class-wise attribution scores, but that its decisions are interpretable in terms of three mathematically distinct evidence components. Truth identifies prototype support, falsity measures attraction to the opposite traffic region, and indeterminacy records unresolved contradiction. This separation is useful for IoT security operations because a high-indeterminacy assignment can be escalated or monitored even when the predicted label is correct.

The residual errors concentrate among neighboring Nmap signatures. This behavior is meaningful because these classes share scanning evidence and differ mainly in subtle flag and service patterns. The contradiction term therefore acts as a transparent caution score for semantically close attack families. Compared with a generic classifier posterior, NSC-RT provides a clearer account of why the attribution should be trusted, rejected, or reviewed.

7. Conclusion

This paper presented NSC-RT, a neutrosophic signature calculus for real-time IoT intrusion attribution. The proposed model is mathematically based, uses a recent 2024 public dataset, and replaces generic fusion diagrams with formal truth-indeterminacy-falsity scoring. The results support the value of contradiction-aware neutrosophic evidence modeling for transparent IoT security decision support. Future work can extend the calculus to streaming prototype updates and edge-deployable hybrid models.

References

[1] Almohaimeed, M. (2024). Enhancing IoT network security using feature selection for intrusion detection systems. Applied Sciences, 14(24), 11966. https://doi.org/10.3390/app142411966

[2] Alsharari, F., Alohali, H., Saber, Y., & Smarandache, F. (2024). An introduction to single-valued neutrosophic primal theory. Symmetry, 16(4), 402. https://doi.org/10.3390/sym16040402

[3] Farid, H. M. A. (2023). Single-valued neutrosophic dynamic aggregation information with time sequence preference for IoT technology in supply chain management. Engineering Applications of Artificial Intelli-gence, 126, 106940. https://doi.org/10.1016/j.engappai.2023.106940

[4] Kamaci, H. (2021). Linguistic single-valued neutrosophic soft sets with applications in game theory. Interna-tional Journal of Intelligent Systems, 36, 3917–3960. https://doi.org/10.1002/int.22445

[5] Kamran, M., Ashraf, S., Salamat, N., Naeem, M., & Botmart, T. (2023). Cyber security control selection based decision support algorithm under single valued neutrosophic hesitant fuzzy Einstein aggregation information. AIMS Mathematics, 8(3), 5551–5573. https://doi.org/10.3934/math.2023280

DOI: https://doi.org/10.54216/NIF.050202
Received: March 07, 2025 Accepted: July 10, 2025

[6] Nguyen, P. H. (2024). Assessing cybersecurity risks and prioritizing top strategies in Vietnam's finance and banking system using strategic decision-making models-based neutrosophic sets and Z number. Heliyon. https://doi.org/10.1016/j.heliyon.2024.e39842
[7] Sharmila, B. S., & Nagapadma, R. (2023). Quantized autoencoder (QAE) intrusion detection system for anomaly detection in resource-constrained IoT devices using RT-IoT2022 dataset. Cybersecurity, 6(1), 41. https://doi.org/10.1186/s42400-023-00178-5
[8] Sharmila, B. S., & Nagapadma, R. (2024). RT-IoT2022 [Data set]. UCI Machine Learning Repository. https://doi.org/10.24432/C5P338
[9] Tan, R. P., & Zhang, W. D. (2021). Decision-making method based on new entropy and refined single-valued neutrosophic sets and its application in typhoon disaster assessment. Applied Intelligence, 51, 283–307. https://doi.org/10.1007/s10489-020-01706-3

DOI: https://doi.org/10.54216/NIF.050202
Received: March 07, 2025 Accepted: July 10, 2025