Security System for Detecting Interest Flooding Attacks in Vehicular Named Data Networks

Vishakha Bhosale[1], Sakshi Desai[2], and Tushar Dhangar[3], Prajwal Shelar[4], Dr. D.S. Waghole[5]
[1-2-3-4-5]*JSPM's JSCOE Pune, India*

***Abstract*—Interest Flooding Attacks (IFAs) jeopardise Vehicular Named Data Networks (VNDN) by saturating Pending Interest Tables and delaying safety-critical content delivery. This overview paper introduces a lightweight hybrid detection framework that blends gradient-boosted trees (XGBoost), temporal sequence learning (LSTM), and spatial pattern extraction (CNN); their probabilities are fused by a shallow Deep Neural Network meta-classifier. Using SUMO and ndnSIM, we simulate realistic mobility and network conditions to generate labelled traffic traces. The ensemble attains 97 % detection accuracy while maintaining an average classification latency of ≈ 50 ms, surpassing individual learners and meeting the hard real-time requirements of vehicular environments. Because the model is compact and platform-agnostic, it can be deployed on roadside units or in-vehicle processors to restore network reliability, mitigate IFAs in situ, and ultimately enhance road-user safety with minimal computational overhead.**

***Index Terms*—Vehicular Named Data Networking; Interest Flooding Attack; Ensemble Learning; XGBoost-LSTM- CNN; Real-time Detection; Intelligent Transportation Systems**

I. INTRODUCTION

Vehicular Named Data Networking (VNDN) extends the Named Data Networking paradigm to intelligent-transport systems by letting vehicles request content by name rather than host address. The content-centric design improves caching efficiency and supports intermittent connectivity, yet it also exposes the network to Interest Flooding Attacks (IFA) malicious bursts of interest packets that overflow Pending Interest Tables, exhaust node CPU/DRAM, and delay the delivery of safety messages such as collision-warnings or signal-phase timing. In a high-mobility environment where milliseconds can decide passenger safety, even brief congestion triggered by an IFA can propagate through hundreds of vehicles and roadside units, crippling real-time services and eroding driver trust in V2X infrastructure.

Traditional counter-measures static rate limiting, rule-based anomaly filters, or probabilistic forwarding tweaks either underperform when traffic patterns shift or impose unacceptable latency overheads. Recent studies have explored single machine-learning classifiers; however, each model captures only a subset of the complex temporal, spatial, and statistical cues present in vehicular traffic. As a result, detection precision or response speed often degrades under realistic load variations.

This paper presents a lightweight hybrid ensemble that unifies three complementary learnersXGBoost for tabular feature relations, Long Short-Term Memory (LSTM) networks for sequential trends, and Convolutional Neural Networks (CNN) for spatial traffic signaturesstacked under a shallow Deep Neural Network meta-classifier. Simulated in SUMO + ndnSIM across diverse city-grid scenarios, the system achieves 97 % IFA detection accuracy at ≈50 ms average decision latency, satisfying the timing constraints of on-board units and roadside gateways.

The remainder of this overview is organized as follows: Section II reviews related work and open gaps; Section III outlines the proposed framework; Section IV describes the experimental setup and key results; Section V concludes with findings and future directions toward deployable, edge-ready defences against IFA in VNDN.

II. LITERATURE SURVEY

Early analyses of Named Data Networking (NDN) security highlighted Interest Flooding Attacks as a primary vulnerability. Afanasyev et al. [1] quantified how excessive interests deplete Pending Interest Table (PIT) space and showed that fixed rate-limiting rules become ineffective once attacker behaviour adapts. To improve scalability, Compagno et al. proposed

Poseidon [2], a probabilistic defence that throttles prefixes with abnormal request rates; while effective in wired NDN test-beds, Poseidon relies on manually tuned thresholds and introduces detection delays that are ill-suited to sub-100 ms vehicular safety deadlines. A comprehensive survey by Benmoussa et al. [3] catalogued more than twenty IFA counter-measureshash-based filters, satisfaction-based pushback, and statistical anomaly detectorsyet concluded that none were validated under the high mobility, bursty loads, and heterogeneous link qualities found in VNDN.

These studies reveal three persistent gaps:

1) Static parameters - most schemes hard-code PIT or rate thresholds that fail when traffic intensity or mobility patterns change.

2) Single-perspective analysis - rule-based or single-model detectors capture either temporal or statistical cues, not both, leading to false positives under benign bursts.

3) Limited real-time evaluation - only a handful of works report end-to-end latency, and even fewer meet the sub-50 ms window required for in-vehicle processors.

The hybrid ensemble presented in this paper addresses these issues by learning multi-modal features, adapting online to traffic drift, and demonstrating millisecond-scale inference in realistic SUMO + ndnSIM scenarios.

III. PROPOSED SYSTEM

Figure 1 sketches the end-to-end pipeline we adopt for detecting Interest Flooding Attacks (IFAs) in a Vehicular Named Data Network. Real-time traffic statistics interest rate, hop-count variance, Pending Interest Table (PIT) occupancy, etc.are tapped at roadside units (RSUs) or in-vehicle On-Board Units (OBUs), normalized, and forwarded in parallel to three complementary base learners. Their class-probability outputs are then fused by a shallow Deep Neural Network (DNN) meta-classifier that issues a binary decision benign or malicious within ≈50 ms; confirmed attacks trigger rate-limiting or blacklist rules in the forwarding plane.

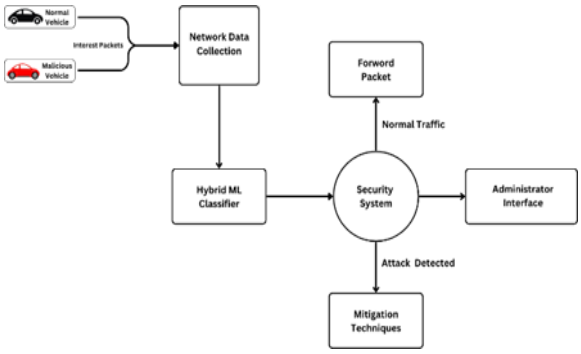

Fig. 1 Hybrid IFA-detection architecture Base-Learner Highlights

XGBoost - structured insights

Captures non-linear relations among tabular features (e.g., interest lifetime vs. PIT hits), delivers feature-importance scores for explainability, and trains quicklyeven on modest RSU CPUs.

LSTM - temporal vigilance

Learns sequential drift in request patterns, spotting slow-ramp attacks invisible to static thresholds; gated memory mitigates noise from sporadic link outages.

CNN - spatial pattern mining

Transforms multivariate traffic snapshots into 2-D "traffic images"; convolutional filters expose local anomalies such as burst clusters or prefix hot-spots, all in parallel for low latency.

Meta-Classifier (Shallow DNN)

A 3-hidden-layer network ingests the soft-probabilities from the three experts, calibrates confidence, and outputs the final verdict. This stacking strategy resolves contradictionse.g., when XGBoost flags a flow benign but the LSTM detects a suspicious burstand consistently delivers higher F1 and lower false-positive rates than any single model. Its lightweight (≈35 k parameters) footprint allows deployment alongside the base learners on the same edge device without exceeding a 50 ms inference deadline.

IV. EXPERIMENT SETUP

Tools & Simulation Stack Realistic vehicular mobility traces were generated in SUMO 1.19 over a 3 × 3 km urban grid containing 400 vehicles travelling at up to 60 km h^{-1}. Packet-level forwarding and content dissemination followed the ndnSIM 2.9 Vehicular NDN extension, ensuring authentic Interest–Data behaviour. All feature extraction, model training, and inference tasks ran on Google Colab

equipped with a Tesla T4 GPU (12 GB VRAM) and 12 GB system RAM, using TensorFlow 2.14 for deep-learning components and scikit-learn 1.4 for traditional classifiers.

Dataset & Feature Extraction The simulator produced 110 000 labelled Interest flows, of which roughly 15 % were malicious. Three traffic-density scenarios (low, medium, high) were used to capture a broad range of network loads. Each flow was distilled into 18 numerical featuresincluding Interests-per-second, Pending Interest Table (PIT) hit ratio, hop-count variance, and inter-arrival skewthat collectively capture statistical, temporal, and spatial characteristics relevant to Interest Flooding behaviour. Data were split 80 % for training and 20 % for stratified testing, with z-score normalisation applied to all continuous attributes and sequence padding used where required for the LSTM model.

V. CONCLUSION & FUTURE SCOPE

This overview paper presented a lightweight hybrid ensembleXGBoost + LSTM + CNN stacked under a shallow DNNthat detects Interest Flooding Attacks in Vehicular Named Data Networks with 97 % accuracy and ≈ 50 ms latency in SUMO + ndnSIM simulations. By fusing statistical, temporal, and spatial traffic cues, the system outperforms single-model baselines while remaining deployable on edge hardware such as RSUs and OBUs. The results demonstrate that multi-modal machine learning can restore real-time content delivery and bolster safety in data-centric vehicular environments.

Future work:
Edge-friendly federated learning: distribute lightweight model updates across vehicles and roadside units to maintain accuracy without sharing raw traffic data, thus preserving privacy and reducing back-haul load.

Adversarial-robust defence stack: integrate adversarial example detection and adaptive rate-limiting so the framework remains resilient against evolving IFA strategies and other emerging NDN threats (e.g., cache poisoning).

REFERENCES

[1] Afanasyev, A., I. Moiseenko, and L. Zhang. “Interest flooding attack and countermeasures in Named Data Networking.” Proceedings of IFIP Networking, 2013.

[2] Compagno, M., M. Conti, G. Tsudik, and C. Ghali. “Poseidon: Mitigating interest flooding DDoS attacks in Named Data Networking.” Proceedings of IEEE LCN, 2015.

[3] Benmoussa, A., C. A. Kerrache, N. Lagraa, S. Mastorakis, A. Lakas, and A. E.-K. Tahari. “Interest flooding attacks in Named Data Networking: Survey of existing solutions, open issues, requirements, and future directions.” ACM Computing Surveys 55, no. 1 (2022): 1-37.

[4] Min, H., Y. Fang, X. Wu, X. Lei, S. Chen, R. Teixeira, B. Zhu, X. Zhao, and Z. Xu. “A fault diagnosis framework for autonomous vehicles with sensor self-diagnosis.” Expert Systems with Applications 224 (2023): 120002.

[5] Shelke, S., and A. Pundge. “A comparative analysis and study of Vehicular Ad Hoc Network.” In Proceedings of the International Conference on Applications of Machine Intelligence and Data Analytics (ICAMIDA 2022), pp. 366-381.Amsterdam, 2023.

[6] Chen, S., J. Hu, L. Zhao, R. Zhao, J. Fang, Y. Shi, and H. Xu. Cellular Vehicle-to-Everything (C-V2X). Berlin: Springer, 2023.

[7] Liang, L., H. Peng, G. Y. Li, and X. Shen. “Vehicular communications: A physical-layer perspective.” IEEE Transactions on Vehicular Technology 66, no. 12 (2017): 10647-10659.

[8] Naeem, M. A., M. A. U. Rehman, R. Ullah, and B.-S. Kim. “A comparative performance analysis of popularity-based caching strategies in Named Data Networking.” IEEE Access 8 (2020): 50057-50077.

[9] Khelifi, H., S. Luo, B. Nour, H. Moungla, Y. Faheem, R. Hussain, and A. Ksentini. “Named Data Networking in Vehicular Ad Hoc Networks: State-of- the-art and challenges.” IEEE Communications Surveys & Tutorials 22, no. 1 (2019): 320-351.

[10] Xylomenos, G., C. N. Ververidis, V. A. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K. V.

Katsaros, and G. C. Polyzos. "A survey of information-centric networking research." IEEE Communications Surveys & Tutorials 16, no. 2 (2013): 1024-1049.

[11] Jacobson, V., D. K. Smetters, J. D. Thornton, M.F. Plass, N. H. Briggs, and R. L. Braynard."Networking named content." In Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies (CoNEXT 2009), pp. 1-12. Rome, 2009.

[12] Ambrosin, M., A. Compagno, M. Conti, C. Ghali, and G. Tsudik. "Security and privacy analysis of National Science Foundation future Internet architectures." IEEE Communications Surveys & Tutorials 20, no. 2 (2018): 1418-1442.

[13] Ahmed, S. H., S. H. Bouk, M. A. Yaqub, D. Kim, H. Song, and J. Lloret. "CODIE: Controlled data and interest evaluation in Vehicular Named Data Networks." IEEE Transactions on Vehicular Technology 65, no. 6 (2016): 3954-3963.

[14] Song, T., H. Yuan, P. Crowley, and B. Zhang. "Scalable name-based packet forwarding: From millions to billions." In Proceedings of the 2nd ACM Conference on Information-Centric Networking (ICN 2015), pp. 19-28. San Francisco, 2015.

[15] Punam V. Maitri, D. S. Waghole, and V. S. Deshpande. "Low latency for file encryption and decryption using Byte Rotation Algorithm." In Proceedings of the IEEE International Conference on Pervasive Computing (ICPC 2015), pp. 1-5, 2015.

[16] Deshpande, V. S., and D. S. Waghole. "Performance analysis of FMAC in wireless sensor networks." In Proceedings of the 11th IEEE International Conference on Wireless and Optical Communications Networks (WOCN 2014), pp. 1-5, 2014.

[17] Waghole, D., V. Deshpande, D. Midhunchakkaravarthy, and M. Jadhav. "Position aware congestion control (PACC) algorithm for disaster management system using WSN to improve QoS." Design Engineering (2021): 11470-11478.

[18] Waghole, D. S., V. S. Deshpande, and P. V. Maitri. "Byte-rotation-based encryption for low-latency mobile sensing." Proceedings of the IEEE International Conference on Pervasive Computing (ICPC 2015): 1-5.

[19] Waghole, D. S., and V. S. Deshpande. "Analyzing the QoS using CSMA and TDMA protocols for wireless sensor networks." In Proceedings of the IEEE International Conference for Convergence in Technology (2014): 1-5.

[20] Udawant, O., N. Thombare, D. Chauhan, A. Hadke, and D. Waghole. "Smart ambulance system using IoT." Proceedings of the International Conference on Big Data, IoT and Data Science (BID 2017), pp. 171-176, 2017.

[21] Shaikh, S., D. Waghole, P. Kumbhar, V. Kotkar, and P. Awaghade. "Patient monitoring system using IoT." Proceedings of the International Conference on Big Data, IoT and Data Science (BID 2017), pp. 177- 181, 2017.

[22] Waghole, D. S., and V. S. Deshpande."Techniques of data collection with mobile and static sinks in WSNs: A survey." International Journal of Scientific & Engineering Research 5, no. 10 (2010): 501-505.

[23] Waghole, D. S., and V. S. Deshpande."Reducing delay in data dissemination using a mobilesink in wireless sensor networks." International Journal of Soft Computing and Engineering 3, no. 1 (2013): 305-308.

[24] Patil, P., D. Waghole, V. Deshpande, and M. Karykarte. "Sectoring method for improving QoS parameters of wireless sensor networks to extend network lifespan." Design Engineering 10, no. 6 (2022): 37-43.