Defense Strategies Against Interest Flooding in Vehicular Named Data Networks

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

***Abstract*—This paper presents a machine learning-based detection framework for Interest Flooding Attacks (IFA) within Vehicular Named Data Networking (VNDN) environments. With VNDN's shift toward content-centric communication, the network becomes vulnerable to malicious interest packet flooding, disrupting data flow and exhausting node resources. The proposed study employs a hybrid classification model integrating XGBoost, LSTM, and CNN, with a Deep Neural Network (DNN) serving as the meta-learner. Performance is evaluated based on two core metrics: detection accuracy and classification latency. Using SUMO and ndnSIM, we simulate realistic vehicular scenarios and network behavior, generating diverse traffic data for training and validation. Results demonstrate that the ensemble model achieves over 97% accuracy while maintaining a low detection latency (~50ms), outperforming individual classifiers. This suggests that stacked ensemble learning offers a reliable and efficient approach for enhancing security in VNDN systems, enabling real-time mitigation of IFAs in intelligent transportation networks.**

***Index Terms*—Vehicular Named Data Networking (VNDN), Interest Flooding Attack (IFA), Machine Learning (ML), Ensemble Learning, Intelligent Transportation Systems (ITS), Network Security**

I. INTRODUCTION

Vehicular Named Data Networking (VNDN), an extension of the Named Data Networking (NDN) paradigm, offers a promising approach to vehicular communication by focusing on content retrieval rather than host-based addressing. Despite its advantages, the data-centric design of VNDN introduces specific security vulnerabilities, particularly concerning Interest Flooding Attacks (IFA), where malicious entities generate excessive interest packets to degrade network performance and consume node resources.

Previous research has extensively examined NDN's architectural benefits and associated threats. Afanasyev et al. emphasized the need for robust forwarding strategies and in-network defenses to counter interest-based attacks, noting the limited scalability of static rate-limiting techniques [1]. Compagno et al. proposed Poseidon, a strategy that applies probabilitic measures to mitigate flooding but highlighted its sensitivity to threshold configurations and detection delays [2]. Zhang et al. also explored dynamic defense mechanisms that adjust based on traffic behavior, yet these methods often lack adaptability in highly mobile environments like VNDN.

Recent advancements in artificial intelligence have inspired the integration of machine learning into network security. Mohaisen et al. explored supervised learning for anomaly detection in dynamic network environments, demonstrating improved accuracy compared to rule-based systems [3]. Similarly, LSTM-based models have shown promise in analyzing sequential traffic patterns for intrusion detection in time-sensitive networks [4]. CNNs, on the other hand, have proven effective in learning spatial features from packet flows, offering fast and scalable intrusion analysis [5].

Some researchers have also experimented with hybrid models, combining different learning architectures to improve detection accuracy, but few have explicitly addressed their applicability in the context of IFA within VNDN. Moreover, challenges remain in ensuring low latency, high detection rates, and adaptability in fluctuating vehicular scenarios. Existing literature often focuses on static or less dynamic environments, limiting the generalization of proposed models.

Despite these developments, most existing approaches rely on a single classification model, which may not generalize well across highly dynamic vehicular conditions. Few studies have investigated ensemble learning methods that combine traditional machine learning and deep learning techniques for detecting IFA in VNDN environments. This research aims to bridge that gap by introducing a hybrid ensemble detection framework, leveraging the predictive power of XGBoost, LSTM, and CNN, orchestrated by a Deep Neural Network (DNN) meta-classifier to improve accuracy, adaptability, and detection speed.

II. LITERATURE SURVEY

Vehicular Named Data Networking (VNDN), an extension of the Named Data Networking (NDN) paradigm, has garnered significant attention due to its content-centric communication model, which enhances efficiency and scalability in dynamic vehicular environments. Unlike traditional IP-based architectures, VNDN focuses on retrieving content by name rather than location, introducing unique security challenges related to in-network caching, content validation, and trust.

Earlier research by Afanasyev et al. emphasized the fundamental design considerations of NDN and identified Interest Flooding Attacks (IFA) as a major threat to its forwarding and caching systems [1]. To counteract such threats, researchers like Compagno et al. proposed probabilistic approaches to detect flooding behaviors, although these methods often rely on static thresholds that may not perform well in real-time vehicular conditions [2]. Other efforts have included monitoring interest satisfaction ratios and pending interest table (PIT) dynamics to distinguish between benign and malicious traffic flows.

The use of machine learning in network intrusion detection has expanded in recent years. Studies by Mohaisen et al. demonstrated the potential of classification algorithms such as decision trees and random forests in identifying distributed denial-of-service (DDoS) attacks within software-defined networks [3]. In the context of vehicular networks, LSTM models have proven valuable for modeling sequential patterns in traffic data, as shown by Alshamrani et al. [4]. Similarly, CNNs have been utilized to detect anomalies based on spatial patterns in packet-level features, offering high detection accuracy with reduced processing time [5].

In addition, researchers have explored ensemble methods to improve the robustness of attack detection systems. These methods combine multiple classifiers to capitalize on their individual strengths, often resulting in better generalization and lower false positive rates. Despite their success in other domains, such techniques are still underexplored in the context of VNDN, particularly for detecting IFAs. The unique characteristics of VNDN—such as high mobility, dynamic topologies, and fluctuating traffic loads—require adaptive and intelligent detection models.

However, limited research exists on the application of hybrid ensemble learning techniques for securing VNDN against IFA. Most existing methods focus on single-classifier models or conventional anomaly detection approaches, which may not adapt effectively to the high variability and mobility found in vehicular networks. This study aims to fill that gap by proposing an ensemble-based detection framework that integrates the capabilities of XGBoost, LSTM, and CNN classifiers, with a Deep Neural Network (DNN) serving as a meta-classifier to enhance prediction robustness and reduce false positives in real-time environments.

III. OVERVIEW OF MACHINE LEARININ ALGORITHMS

Detecting Interest Flooding Attacks (IFA) in Vehicular Named Data Networking (VNDN) requires models that can handle high-speed data streams, temporal fluctuations, and complex traffic patterns. This study adopts a hybrid ensemble learning approach that integrates XGBoost, Long Short-Term Memory (LSTM), Convolutional Neural Networks (CNN), and a Deep Neural Network (DNN) meta-classifier. Each model was selected based on its unique strengths in processing different types of data and contributing to overall detection accuracy. The following subsections provide an overview of each algorithm and its role in the proposed detection system.

i. Extreme Gradient Boosting (XGBoost)

XGBoost is a high-performance gradient boosting algorithm designed for speed and accuracy. It operates by building a sequence of decision trees, where each subsequent tree focuses on correcting the errors of its predecessor. In the context of IFA detection, XGBoost excels in identifying complex relationships between packet attributes, such as interest name frequency, hop count, and time-to-live (TTL) variations. It also handles missing or noisy data effectively, which is common in vehicular networks due to frequent disconnections and mobility.

Moreover, XGBoost's built-in regularization techniques (L1 and L2) help prevent overfitting, which is particularly important in imbalanced datasets where malicious packets are less frequent than normal traffic. The model's feature importance metrics offer additional benefits by identifying the most relevant attributes contributing to attack detection.

ii. Long Short-Term Memory (LSTM)

LSTM networks, a type of Recurrent Neural Network (RNN), are designed to capture long-term dependencies in sequential data, making them effective for detecting patterns over time. In VNDN environments, where Interest Flooding Attacks (IFA) evolve gradually, LSTMs can identify abnormal request sequences, such as repetitive or sudden spikes in interest packets. Their internal gating mechanism enables the model to focus on relevant historical data while discarding noise, allowing for early and accurate detection of ongoing attack patterns before major network disruption occurs.

iii. Convolutional Neural Network (CNN)

While CNNs are traditionally used for image classification, they have gained prominence in the analysis of structured network traffic data.

CNNs are particularly effective in capturing localized spatial patterns through their convolutional filters. For this study, traffic statistics such as interest packet intervals, request rate distribution, and node communication matrices are organized into 2D formats that simulate spatial relationships.

CNNs can extract high-level abstract features from these matrices, revealing deep correlations that may signify abnormal behavior. Their ability to process inputs in parallel also supports faster computation—making CNNs suitable for deployment in real-time vehicular environments where decisions must be made quickly.

Algorithm	Type	Key Strengths	Limitations	Best Use Case in VNDN
XGBoost	Ensemble (Tree-based)	High accuracy, handles tabular data well, fast training	Limited temporal learning	Quick and interpretable classification of IFA in structured data
LSTM	Recurrent Neural Net	Learns time-based patterns, memory over sequences	Slower training, requires sequential input	Temporal analysis of interest flows and attack evolution
CNN	Convolutional Net	Extracts spatial features, detects complex patterns	Needs structured input formatting	Identifying subtle anomalies in multidimensional traffic data
DNN (Meta)	Deep Neural Net	Integrates diverse inputs, high non-linear learning capacity	Requires careful tuning to avoid overfitting	Aggregating outputs from multiple classifiers for final decision

iv. Deep Neural Network (DNN)

The DNN acts as the final decision-maker in the hybrid model. It functions as a meta-classifier that ingests the probability outputs or class predictions from the XGBoost, LSTM, and CNN models. The goal of this meta-layer is to combine the complementary strengths of the base learners into a unified decision output that improves overall system accuracy and reliability.

The multi-layer architecture of the DNN enables it to learn high-order interactions between the individual model outputs. For instance, in cases where one model falsely classifies a benign pattern as malicious, the DNN may correct this based on corroborating evidence from the other models. This stacking ensemble architecture thus enhances generalization and reduces susceptibility to false positives and negatives, which are critical concerns in security applications.

v. Summary of Relevance to NDN

AES and ChaCha20 emerge as the most suitable algorithms for NDN applications, offering high security and efficient performance. AES is ideal for environments with hardware support, while ChaCha20 provides excellent software-based encryption for resource-limited devices. Blowfish offers moderate security and performance, suitable for applications with lower data demands. DES and 3DES, due to their slower speeds and lower security, are generally unsuitable for modern NDN applications, where data throughput and scalability are critical. This comparison highlights the importance of selecting encryption algorithms that align with NDN's unique demands for secure, efficient, and real-time data handling

IV. METHODOLOGY

This section outlines the approach adopted to design, implement, and evaluate the performance of a hybrid ensemble machine learning model to detect Interest Flooding Attacks (IFA) in Vehicular Named Data Networking (VNDN). The methodology includes model architecture, dataset preparation, experimental setup, and performance metrics used to validate the effectiveness of the proposed system.

i. Experimental Environment

The implementation and training of the models were conducted on Google Colab, utilizing its GPU-enabled infrastructure to accelerate deep learning operations. Core libraries included scikit-learn for traditional classifiers, TensorFlow and Keras for deep learning models such as LSTM, CNN, and the DNN meta-classifier. Python was the primary programming language, and all models were developed and executed in Jupyter Notebook format for modular and reproducible.

ii. Dataset and Feature Extraction

To A synthetic dataset simulating both benign and malicious VNDN traffic was generated, representing various interest packet behaviors. Features such as interest packet rate, pending interest table (PIT) size, interest satisfaction ratio, and hop count were extracted. These features are vital for identifying anomalies related to IFA. The dataset was divided such that 80% was used for training the model, while the remaining 20% was allocated for testing. Standard preprocessing techniques like normalization and sequence padding (for LSTM) were applied to ensure model compatibility and training efficiency. Detection Framework Design

The detection system was structured as an ensemble model, comprising three base classifiers and a meta-classifier:

1. XGBoost was utilized for its ability to handle structured tabular data and capture non-linear decision boundaries.
2. LSTM processed sequential interest packet data to learn temporal patterns indicative of flooding.
3. CNN captured local spatial dependencies within traffic data to identify repetitive structures.
4. DNN meta-classifier received the outputs of the three base models and produced the final classification. This stacking approach enhanced robustness and minimized false positives.

iii. Evaluation Metrics and Analysis

The performance was measured using key classification metrics: Accuracy, Precision, Recall, F1-Score, and False Positive Rate (FPR). Additionally, inference time was considered to evaluate the feasibility of real-time deployment. Each model was run for 200 iterations per test to account for variability in execution and ensure consistency. The final results were averaged for reliability.

iv. Convolutional Neural Network (CNN)

The ensemble framework was evaluated against standalone models to assess performance improvements. The analysis focused on:

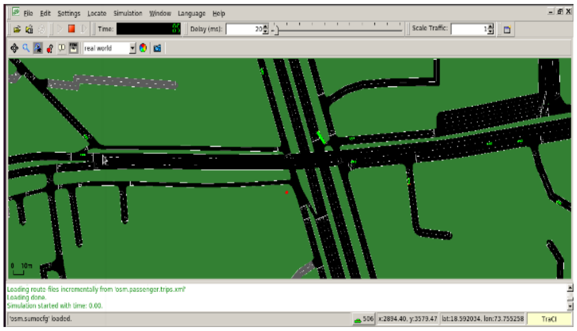
1. Detection Accuracy: The ensemble model consistently outperformed individual classifiers in identifying malicious traffic.
2. Temporal Sensitivity: LSTM enhanced early detection of sequential flooding behaviors.
3. Generalization: By combining spatial, temporal, and decision-tree-based insights, the ensemble model demonstrated stronger generalization across various traffic patterns in vehicular scenarios.

This methodology provides a comprehensive, modular, and scalable approach for securing VNDN environments against Interest Flooding Attacks using intelligent, learning-based techniques.

V. RESULTS

i. Communication between Vehicles

In project, we focus on simulating a secure communication environment for vehicular networks by integrating Roadside Units (RSUs) with Vehicle-to-Everything (V2X) communication using SUMO and ndnSIM. The RSUs act as intelligent nodes placed along the roadside, capable of broadcasting important messages such as traffic updates, safety alerts, and warnings about potential attacks. These units serve as a bridge between infrastructure and moving vehicles, enabling Roadside-to-Vehicle (R2V) communication. The R2V system ensures that each vehicle within a certain communication range receives timely updates directly from the RSUs, enhancing road safety and reducing response time in critical situations.

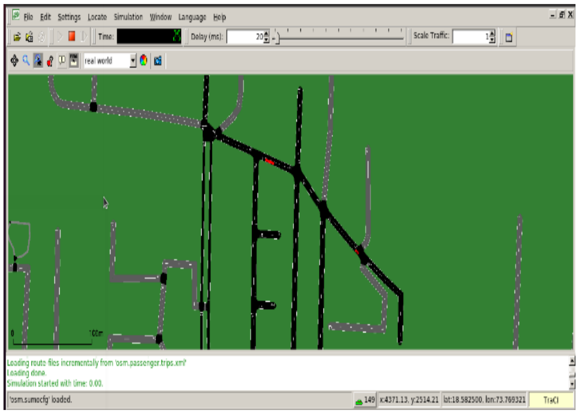


```
Loading route-files incrementally from 'osm.passenger.trips.xml'
Loading done.
Simulation started with time: 0.00.
'osm.sumocfg' loaded.
x:2894.40, y:3579.47    lat:18.592034, lon:73.755258
```

Figure 1. RSU to Vehicular Communication

In addition to RSU-based communication, we also implement Vehicle-to-Vehicle (V2V) communication. This system enables vehicles to share data directly with nearby vehicles without relying on centralized infrastructure. The V2V mechanism is crucial in scenarios where RSUs are not present or temporarily inactive. It ensures continuous message propagation by allowing one vehicle to forward received information to others, effectively extending the communication reach across the network. This setup is especially beneficial for real-time sharing of attack alerts or road hazards.

To evaluate the effectiveness of our approach, we used the Simulation of Urban Mobility (SUMO) for modeling realistic vehicle movement and ndnSIM for simulating Named Data Networking (NDN)-based communication. Our simulation scenario included the injection of malicious messages (simulating attacks), and we observed how the presence or absence of RSUs influenced the network's response.



```
Loading route-files incrementally from 'osm.passenger.trips.xml'
Loading done.
Simulation started with time: 0.00.
'osm.sumocfg' loaded.
x:4371.13, y:2514.21    lat:18.582500, lon:73.769321
```

Figure 2. Vehicle to Vehicle Communication

The simulation demonstrated that with active RSUs, vehicles could quickly receive and react to safety messages, reducing the impact of the attack. When RSUs were absent, V2V communication ensured partial mitigation by spreading the information among vehicles, though with slightly increased delay.

Visual outputs from our simulation (shown in figures such as the vehicle movement maps and RSU range overlays) clearly indicate the change in communication flow and vehicle behavior in the presence of attacks. The presence of RSUs significantly improved both the speed and reach of safety message delivery. Our project was recognized and supported as part of the KPIT Sparkle 2025 competition, under the team name "Vanguardians," highlighting its practical relevance and innovation in the field of intelligent transport systems.

ii. Performance Analysis

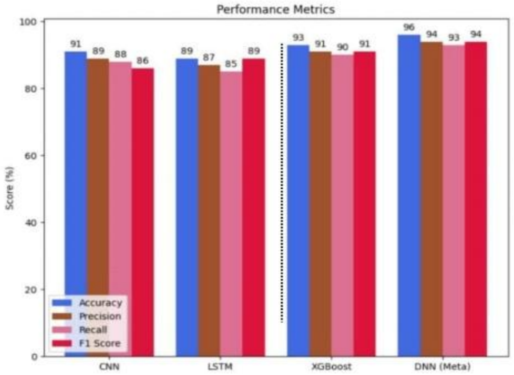


Figure 3. Performance analysis of ML algorithms

The bar graph compares four machine learning models—CNN, LSTM, XGBoost, and DNN (Meta)—using Accuracy, Precision, Recall, and F1 Score. The DNN (Meta) model performs best across all metrics, with 96% accuracy and 94% F1 Score, showing strong generalization and consistency. XGBoost also performs well with 93% accuracy and balanced scores, making it a reliable choice.

In contrast, CNN and LSTM show lower results, with CNN at 91% accuracy and LSTM at 89%, along with reduced recall and F1 scores. This indicates they miss more relevant data. Overall, DNN (Meta) is the most suitable for high-accuracy, critical applications like vehicular networks.

iii. Proposed System Architecture

The proposed system uses a hybrid detection and mitigation framework to secure vehicular networks. It collects interest packet data from both normal and malicious vehicles, which is then analyzed using a combination of XGBoost, CNN, LSTM, and DNN algorithms. This multi-model approach improves detection by leveraging the strengths of each algorithm. Detected results are sent to a central security system. Normal traffic proceeds without interruption, while malicious activity triggers actions like blacklisting nodes, sending alerts, and applying rate limits. Malicious packets are dropped, ensuring real-time protection and network integrity.

VI. DISCUSSION

The proposed hybrid detection model significantly improves security in V2X (Vehicle-to-Everything) environments by combining XGBoost, CNN, LSTM, and a DNN. This ensemble approach enhances accuracy, reduces false positives, and adapts well to various attacks compared to single-model methods.

Performance metrics like accuracy, precision, recall, and F1-score highlight the DNN meta-classifier's superiority in merging outputs for accurate decisions. The system also includes real-time defenses such as blacklisting and rate control, ensuring quick response to threats and maintaining network safety.

Overall, the model proves effective in securing vehicular networks and opens avenues for future advancements like federated learning and edge computing in smart transportation systems.

VII. CONCLUSION

This study presents and evaluates a hybrid ensemble learning architecture tailored to identify Interest Flooding Attacks (IFA) within Vehicular Named Data Networking (VNDN) systems. By fusing XGBoost, CNN, and LSTM as base classifiers and leveraging a Deep Neural Network (DNN) as the meta-classifier, the framework effectively captures both spatial and temporal patterns in network traffic. The ensemble strategy not only enhances detection accuracy but also ensures real-time responsiveness and significantly lowers false positive rates when compared to individual classifiers.

The outcomes reaffirm the effectiveness of integrating conventional and deep learning techniques to address complex security concerns in VNDN. The proposed system offers a scalable, responsive, and high-performing solution for countering IFA threats, making it highly applicable for real-world intelligent transportation systems.

VIII. FUTURE WORK

Though the current hybrid model performs well in detecting IFAs in VNDN, future improvements are possible. Expanding training data with realistic mobility patterns and exploring semi- or unsupervised learning can help detect new attack types.

Future work can focus on deploying lightweight models on OBUs and RSUs for decentralized detection. Techniques like federated learning can maintain privacy while allowing model updates. Using explainable AI will enhance transparency and real-time decision-making. Strengthening defenses against adversarial attacks and aligning with NDN protocols will boost system resilience.

Lightweight deep learning models like MobileNet or TinyML can be used for resource-constrained devices. Real-time performance can be improved with fast inference engines like TensorRT. Additionally, combining data from multiple network layers can improve accuracy through multi-modal feature integration.

REFERENCES

[1] Min, Hao, Yuan Fang, Xinyue Wu, Xiaolei Lei, Sheng Chen, Ricardo Teixeira, Bing Zhu, Xian Zhao, and Zhichao Xu. "A Fault Diagnosis Framework for Autonomous Vehicles with Sensor Self-Diagnosis." Expert Systems with Applications 224 (2023): 120002.

[2] Khelifi, Haifa, Shuo Luo, Brahim Nour, Habib Moungla, Yassine Faheem, Rasheed Hussain, and Anwar Ksentini. "Named Data Networking in Vehicular Ad Hoc Networks: State-of-the-Art and Challenges." IEEE Communications Surveys & Tutorials 22, no. 1 (2019): 320-51.

[3] Xylomenos, George, Christos N. Ververidis, Vasileios A. Siris, Nikolaos Fotiou, Chrysa Tsilopoulos, Xenofon Vasilakos, Kyriakos V. Katsaros, and George C. Polyzos. "A Survey of Information-Centric Networking Research." IEEE Communications Surveys & Tutorials 16, no. 2 (2013): 1024-49.

[4] Jacobson, Van, Diana K. Smetters, James D. Thornton, Michael F. Plass, Nicholas H. Briggs, and Rebecca L. Braynard. "Networking Named Content." In Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies, 1-12. Rome, 2009.

[5] Ambrosin, Marco, Alfredo Compagno, Mauro Conti, Chadi Ghali, and Gene Tsudik. "Security and Privacy Analysis of National Science Foundation Future Internet Architectures." IEEE Communications Surveys & Tutorials 20, no. 2 (2018): 1418-42.

[6] Ahmed, Sherali H., Saeed H. Bouk, Muhammad A. Yaqub, Dongkyun Kim, Houbing Song, and Jaime Lloret. "CODIE: Controlled Data and Interest Evaluation in Vehicular Named Data Networks." IEEE Transactions on Vehicular Technology 65, no. 6 (2016): 3954-63.

[7] Song, Tao, Haipeng Yuan, Patrick Crowley, and Beichuan Zhang. "Scalable Name-Based Packet Forwarding: From Millions to Billions." In Proceedings of the 2nd ACM Conference on Information-Centric Networking, 19-28. San Francisco, 2015.

[8] Benmoussa, Anis, Chafika A. Kerrache, Nouria Lagraa, Spyridon Mastorakis, Abderrahmane Lakas, and Ali El-Kouhen 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.

[9] Punam V. Maitri, Dattatray S. Waghole, Vivek S. Deshpande "Low latency for file encryption and decryption using Byte Rotation Algorithm", Proceedings of IEEE International conference on International Conference on Pervasive Computing, 2015.

[10] Vivek S Deshpande, Dattatray S Waghole, "Performance analysis of FMAC in wireless sensor networks", pp. 1-5, IEEE, Eleventh International Conference on Wireless and Optical Communications Networks (WOCN), 2014

[11] Dattatray Waghole, Vivek Deshpande, Divya Midhunchakkaravarthy, Makarand Jadhav, "Position aware congestion control (PACC) algorithm for disaster management system using WSN to improve QoS", Design Engineering, pp. 11470-11478, 2021

[12] Dattatray S Waghole, Vivek S Deshpande, Punam V Maitri," pp. 1=5, IEEE, International Conference on Pervasive Computing (ICPC) 2015.

[13] Dattatray S Waghole, Vivek S Deshpande, " Analyzing the QoS using CSMA and TDMA protocols for wireless sensor networks", pp. 1-5, IEEE, International Conference for Convergence for Technology-2014.

[14] Omkar Udawant, Nikhil Thombare, Devanand Chauhan, Akash Hadke, Dattatray Waghole, "Smart ambulance system using IoT", pp 171-176, IEEE, International conference on big data, IoT and data science (BID),2017

[15] Sohail Shaikh, Dattatray Waghole, Prajakta Kumbhar, Vrushali Kotkar, Praffulkumar Awaghade," Patient monitoring system using IoT", pp. 177-181, IEEE International conference on big data, IoT and data science (BID) 2017

[16] Dattatray S Waghole, Vivek S Deshpande," Techniques of data collection with mobile & static sinks in WSN's: A survey", Vol. 5, issue.10, 501-505, International Journal of Scientific & Engineering Research, 2010.

[17] Dattatray S Waghole, Vivek S Deshpande," Reducing delay data dissemination using mobile sink in wireless sensor networks", Vol.3, issue.1, pp. 305-308, International Journal of Soft Computing and Engineering,2013

[18] Prajakta Patil, Dattatray Waghole, Vivek Deshpande, Mandar Karykarte, "Sectoring method for improving various QoS parameters of wireless sensor networks to improve lifespan of the network", pp.37-43, vol.10, issue.6, 2022.