Journal of Advances in Science and Technology
Vol.22, Issue No. 4 September-2025, ISSN 2230-9659

Bandwidth-Optimal Group-Based Malinformation Filtering for Secure Data Aggregation in Wireless Sensor Networks

Priyanka Soni[1]*, Dr. Rajeev Yadav[2]

1 Research Scholar, Shri Krishna University, Chhatarpur, M.P., India

baghelrashmi805@gmail.com

2 Professor, Shri Krishna University, Chhatarpur, M.P., India

Abstract: Wireless Sensor Networks (WSNs) are finding more and more application in sensitive areas which include environmental control, healthcare, industrial control, and military surveillance. Their unrestricted wireless broadcast, unsupervised deployment, and extreme resource limitations however render them extremely susceptible to malinformation attacks and especially to the false data that have been propagated by groups of sensor nodes that have been compromised. These attacks do not only distort sensing results, but also consume too much bandwidth and drain energy fast. The article explores the nature and the effects of group-based malinformation attacks on multipath WSN systems, and draws attention to the weaknesses of the conventional node-centric and probabilistic detection strategies. To overcome these issues, a Bandwidth-Optimal Group-Injected Data Filtering (BO-GIDF) architecture is highlighted which combines collaborative filtering with data aggregation and authentication schemes. The proposed strategy can significantly reduce the spread of false data by identifying coordinated malicious behavior in the middle of data transmission and, consequently, saving network resources, and increasing the stability of the entire network. The paper shows that group-aware filtering is a key to scalable, power-efficient, and reliable data aggregation in the current WSNs.

Keywords: Wireless Sensor Networks, Malinformation Attacks, Secure Data Aggregation, Group-Based Filtering

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are composed of many highly inexpensive resource limited sensor nodes that collaboratively sense, process and relay information to a sink or base station. The use of these networks is important in a broad variety of applications, such as environmental monitoring, smart agriculture, healthcare systems, managing disasters, industrial control, and military surveillance. In spite of its strengths, WSNs have serious security problems because of low computing capacity, limited memory, limited battery availability, and wireless communication. These natural limitations render the direct application of traditional security systems inapplicable and lightweight but security-insurances

specific to sensor networks need to be utilized. Malinformation injection is one of the worst security threats in WSNs where hacked sensor nodes intentionally produce fake or counterfeit data that look valid. In contrast to the traditional denial-of-service attacks which are based on the number of traffic volumes, malinformation attacks capitalize on the trusting and cooperative characteristic of the WSN protocols. Malicious nodes will be involved in sensing, routing and aggregation as usual where false data will be spread throughout the network without the realization of other nodes. Consequently, the malinformation attacks are especially hard to detect and prevent, particularly in the cases when the attackers attentively design the data values to work within anticipated thresholds.

This is much more complicated when it comes to group-injected attacks of malinformation. In this type of attack, a group of compromised sensor nodes works to deliver reliable false information, and the plausibility of the malicious information is supported by spatial and temporal correlation. Owing to the fact that most WSNs use redundancy, majority voting, or statistical deviation to be validated, organized malicious activity can easily overcome these checking systems. Aggregated data within a cluster-based and multipath routing setting can be easily polluted by the group-based malinformation and will provide erroneous sensing results and faulty decision-making at the application layer. In addition to the issue of data integrity, malinformation attacks have far-reaching effects on the performance of the network and resource optimization. Each spurious data packet uses bandwidth to be relayed and energy to be processed, aggregated and forwarded. Since WSN communication is multi-hop, the resource cost of malinformation increases the more the packet will pass through multiple intermediate nodes until the sink is reached. Such over resource usage over time will hasten battery depletion, reduce the life of the network, cause congestion and even cause network partitioning. Malinformation attacks, therefore, pose a threat of security and a resource-exhaustion threat. The current security strategies used in WSNs are mostly node based, they involve analyzing behavior of individual nodes by use of trust scores, probabilistic verification, or detection of anomalies. Although such methods can help identify isolated malicious nodes, coordinated group attacks can usually go unnoticed. In addition, detecting nodes at a node level places significant computational and communication burden, incompatible with the severe resource constraints of sensor nodes. The late detection also enables the malinformation to diffuse to many people before the countermeasures come into effect and this lowers the effectiveness of the solutions.

In order to address such limitations, team-based and group conscious security mechanisms are increasingly sought after and analyze group behaviour instead of individual node behaviours. Malinformation filtering Group-based malinformation filtering is based on the fact that a coordinated malicious activity can be detected early in the data flow by using the correlations between neighboring nodes and route paths. This filtering is especially essential in multipath WSNs where false information can spread across several paths at the same time and therefore increase its adverse effect. Essential protection against bogus data injection is offered by secure data aggregation and authentication protocols (the Data Aggregation and Authentication (DAA) protocol and Secure Data Filtering and Confidentiality (SDFC) algorithms). Nevertheless, it is often not viable to enable such mechanisms in all sensor nodes because of energy and bandwidth costs. Thus, it is necessary to combine group-based filtering with bandwidth-efficient strategies of detection. Inspired by these issues, the purpose of this paper is to dwell on why Bandwidth-Optimal Group-Injected Data Filtering (BO-GIDF) is necessary in WSNs. BO-GIDF seeks to curt malinformation early-stage by focusing on coordinated malinformation detection and detection via cooperation to suppress the spread of false data, minimize communications overhead needless, and improve resilience of the network. The paper gives emphasis on the benefits of using group-aware filtering, secure aggregation, and lightweight authentication to enhance data integrity, energy efficiency, and performance in hostile WSN environments.

2 SECURITY CHALLENGES IN WIRELESS SENSOR NETWORKS

Wireless Sensor Networks (WSNs) operate under stringent resource constraints while performing continuous sensing, data processing, and multihop communication. These intrinsic limitations significantly shape the security landscape of WSNs, making conventional security mechanisms designed for wired or high-capacity wireless networks unsuitable. Security challenges in WSNs arise not only from external adversaries but also from compromised internal nodes that exploit the cooperative and unattended nature of sensor deployments. As a result, ensuring data integrity, authenticity, availability, and energy efficiency simultaneously remains a critical research challenge.

2.1 Resource Constraints and Attack Surface

Sensor nodes in WSNs are typically characterized by limited computational capability, constrained memory, finite battery power, and restricted communication bandwidth. These constraints severely limit the feasibility of computationally intensive cryptographic operations

and continuous monitoring mechanisms. Unlike conventional networks, where devices can sustain complex encryption and frequent rekeying, sensor nodes must prioritize longevity and energy conservation. Consequently, attackers can exploit lightweight security configurations by injecting malicious data that appears legitimate, thereby bypassing traditional authentication and integrity checks. The expansive attack surface of WSNs is further amplified by their open wireless communication medium and large-scale distributed deployment. Data packets traverse multiple intermediate nodes before reaching the sink, and each hop introduces an opportunity for interception, manipulation, or replay. Since routing and data aggregation rely on cooperation among nodes, compromised sensors can participate in normal network operations while stealthily injecting malinformation. Moreover, multipath routing—commonly employed to improve reliability—can unintentionally increase exposure by allowing malicious data to propagate through multiple routes simultaneously, intensifying bandwidth usage and energy depletion.

From a resource perspective, security attacks in WSNs are particularly damaging because even small volumes of malicious traffic can trigger disproportionate energy consumption. Processing, validating, aggregating, and forwarding false data drains node batteries and shortens network lifetime. This asymmetry between attack cost and defensive resource expenditure makes WSNs especially vulnerable to resource-exhaustion and malinformation-based attacks, emphasizing the need for early-stage and bandwidth-efficient filtering mechanisms rather than reactive security enforcement at the sink.

2.2 Vulnerabilities Specific to WSN Environments

Beyond resource limitations, WSNs exhibit structural and operational vulnerabilities that distinguish them from traditional network architectures. Sensor nodes are often deployed in unattended, hostile, or physically inaccessible environments, such as battlefields, forests, industrial plants, and disaster zones. This exposure enables adversaries to physically capture nodes, extract cryptographic credentials, and reintroduce compromised devices into the network as trusted participants. Once compromised, such nodes can generate well-formed yet malicious data, making detection significantly more challenging. WSNs also rely heavily on data aggregation techniques to minimize communication overhead. While aggregation improves efficiency, it introduces a critical vulnerability: corrupted data from even a small subset of nodes can contaminate aggregated results and mislead the entire network. Since aggregation nodes typically do not verify the authenticity or plausibility of each individual

data contribution, malinformation injected upstream can propagate downstream unchallenged. This vulnerability is especially severe in hierarchical and cluster-based WSNs, where compromised cluster heads can exert disproportionate influence on aggregated outcomes.

Another key vulnerability arises from trust assumptions embedded in cooperative routing protocols. WSNs often presume benign behavior from neighboring nodes to ensure scalability and efficiency. However, this implicit trust becomes a liability under coordinated or group-based attacks, where multiple compromised nodes collaborate to reinforce each other's malicious behavior. Such coordination allows attackers to evade detection mechanisms based on majority voting or statistical deviation, as malicious data aligns with group behavior patterns.

3 CHARACTERISTICS AND IMPACT OF MALINFORMATION ATTACKS

Malinformation attacks in Wireless Sensor Networks (WSNs) are distinct from conventional network attacks because they exploit the cooperative, resource-constrained, and distributed nature of sensor networks. These attacks are particularly damaging as they are often executed by legitimate but compromised sensor nodes, enabling malicious activity to remain concealed within routine network operations. The defining characteristics of malinformation attacks involve deceptive data generation, coordinated behavior, and disproportionate impact on network resources and performance.

3.1 False Data Injection

False data injection is one of the most prevalent forms of malinformation attacks in WSNs. In this attack, compromised sensor nodes deliberately transmit fabricated or manipulated sensor readings that appear valid in format and range. Since WSNs commonly rely on threshold-based validation or simple plausibility checks, injected data that mimics legitimate sensor values often bypasses detection mechanisms. As a result, false data becomes indistinguishable from authentic measurements during data aggregation and forwarding processes. The consequences of false data injection extend beyond incorrect sensing outcomes. Each injected packet must be processed, authenticated, aggregated, and transmitted across multiple hops, consuming critical network resources. In applications such as environmental monitoring or healthcare, these distorted data streams can lead to erroneous decisions and reduced system reliability. Over time, persistent false data injection degrades trust in the sensor network and undermines its operational integrity.

3.2 Group-Injected Malinformation

Group-injected malinformation represents a more sophisticated and severe threat, wherein multiple compromised sensor nodes collaborate to inject corroborative malicious data. Unlike isolated false data injection, group-based attacks exploit spatial and temporal correlations among sensor nodes to reinforce the credibility of injected information. By aligning their data reports, malicious nodes can evade detection mechanisms that rely on majority voting, statistical deviation, or redundancy-based validation. In multipath and cluster-based WSNs, group-injected malinformation can propagate rapidly across multiple routing paths, contaminating aggregated results at various stages of the network. This coordinated behavior significantly complicates detection, as malicious patterns appear consistent within local neighborhoods. Consequently, group-injected malinformation can exert disproportionate influence on network operations, causing widespread misinformation even when the majority of nodes remain uncompromised.

3.3 Bandwidth, Energy, and Performance Degradation

Beyond compromising data integrity, malinformation attacks have a profound impact on the resource efficiency and performance of WSNs. Every malicious packet consumes bandwidth during transmission and energy during processing and forwarding. In resource-constrained sensor networks, these expenditures accumulate rapidly, leading to accelerated battery depletion and reduced network lifetime. Since malinformation often traverses multiple hops, its impact multiplies as packets propagate toward the sink. From a performance perspective, excessive malinformation increases packet collisions, transmission delays, and network congestion. In multipath routing environments, redundant forwarding of malicious data exacerbates these effects, leading to decreased packet delivery ratios and higher latency. Furthermore, uneven energy depletion caused by repeated forwarding of malinformation can result in network partitioning, isolating regions of the network and degrading overall sensing coverage. Thus, malinformation attacks function not only as security threats but also as resource exhaustion mechanisms, significantly impairing WSN performance.

4 MOTIVATION FOR GROUP-BASED MALINFORMATION FILTERING

The evolving nature of malinformation attacks in WSNs exposes fundamental limitations in existing security mechanisms. Traditional approaches often fail to address coordinated and

resource-draining attacks effectively, necessitating a shift toward collaborative and behavior-aware filtering strategies.

4.1 Limitations of Node-Centric and Probabilistic Approaches

Most existing malinformation detection techniques operate at the individual node level, employing probabilistic verification, trust scores, or threshold-based anomaly detection. While these approaches may detect isolated malicious nodes, they are largely ineffective against coordinated group-based attacks. Compromised nodes can adapt their behavior to remain within acceptable thresholds, thereby evading probabilistic detection mechanisms. Additionally, node-centric approaches incur high computational and communication overhead, as each node independently performs verification and trust evaluation. In resource-constrained WSNs, this overhead leads to increased energy consumption and reduced scalability. Probabilistic techniques also suffer from delayed detection, allowing malinformation to propagate through the network before malicious nodes are identified and isolated. These limitations highlight the inadequacy of isolated detection strategies in addressing complex malinformation patterns.

4.2 Need for Collaborative Filtering in Multipath WSNs

Given the cooperative architecture and multipath routing characteristics of WSNs, effective malinformation mitigation requires a collaborative filtering approach that evaluates group-level behavior rather than isolated node actions. By analyzing correlations among neighboring nodes and routing paths, collaborative filtering enables early identification of coordinated malinformation injection and prevents its propagation across redundant routes. In multipath WSNs, collaborative filtering is particularly critical, as malicious data can simultaneously traverse multiple paths, amplifying its resource impact. Group-based filtering mechanisms can intercept malinformation at intermediate nodes, reducing unnecessary packet forwarding and conserving bandwidth and energy. By integrating group-based analysis with lightweight authentication and validation mechanisms, collaborative filtering supports scalable, efficient, and robust security enforcement in hostile WSN environments. This motivation directly underpins the proposed Bandwidth-Optimal Group-Injected Data Filtering (BO-GIDF) mechanism, which leverages group-based neighbor evaluation to suppress malinformation early, optimize resource utilization, and enhance overall network resilience.

5 THREAT MODEL FOR MALINFORMATION IN WIRELESS SENSOR NETWORKS

This research considers malinformation injection as the primary security threat targeting the wireless sensor network. Malinformation attacks originate from compromised sensor nodes that deliberately inject fabricated or manipulated data into the network while maintaining syntactic validity and plausible value ranges. These malicious data packets are designed to evade basic validation mechanisms and propagate through the network as legitimate sensor reports. The threat model assumes that adversarial nodes aim to disrupt data integrity, degrade network performance, and exhaust critical network resources. Unlike denial-of-service attacks that rely on overwhelming traffic volumes, malinformation attacks exploit the cooperative nature of WSNs by embedding malicious behavior within normal communication patterns. Malicious nodes may selectively inject false data during critical sensing periods or adapt their behavior to avoid detection, thereby maximizing attack impact while minimizing exposure. A particularly severe threat considered in this study is group-injected malinformation, where multiple compromised nodes collaborate to generate consistent false data reports. By coordinating their transmissions, adversarial nodes can exploit spatial and temporal correlations among neighboring sensors, making malicious data appear credible during aggregation and routing. This coordinated behavior significantly reduces the effectiveness of node-centric and probabilistic detection mechanisms, necessitating group-aware security strategies.

6 ATTACKER CAPABILITIES AND ASSUMPTIONS

The attacker model assumes a bounded but realistic adversary with the capability to compromise a limited subset of sensor nodes through physical capture or software exploitation. Compromised nodes retain valid cryptographic credentials and can participate fully in network operations, including sensing, routing, aggregation, and forwarding. However, the attacker does not possess unlimited resources and cannot compromise the sink or a majority of sensor nodes simultaneously. Adversarial nodes are assumed to have knowledge of local network topology and routing behavior, enabling them to coordinate attacks with neighboring compromised nodes. They can inject false data, manipulate sensed values, replay previously captured packets, and selectively drop or forward data to influence network performance. However, attackers are not assumed to have global network knowledge or the ability to break cryptographic primitives used for authentication. The attacker is also

assumed to behave strategically and adaptively, modifying attack intensity and timing to evade detection. This includes injecting malinformation at rates comparable to legitimate traffic and adjusting data values to remain within expected ranges. These assumptions reflect practical attack scenarios observed in real-world sensor deployments and ensure that the proposed security framework is evaluated under realistic and challenging conditions.

7 VERIFICATION AND DATA AGGREGATION FOR WSN MALINFORMATION DATA DETECTION

The Data Aggregation and Authentication (DAA) protocol to provide safeguards against hacked sensor nodes, ensure confidentiality, and identify bogus data. Some sensor nodes are selected to act as data aggregators in the DAA approach, and the nodes that are involved in the forwarding process are called forwarding nodes. Some nodes in the vicinity of the data aggregator, known as monitoring nodes in WSN, are responsible for detecting any injected incorrect data that may have been obtained during data aggregation. Pair mates may subsequently confirm the data by evaluating Message Authentication Codes (MACs) for data aggregation. Data aggregators may then take use of the DAA's data secrecy services to transfer data to one another. The sensor nodes certify data integrity on encrypted data instead of plain data, which helps to preserve the secret data transfer between the two sequential data aggregators. Using the DAA protocol, data is instantly deleted when authentication fails at the node transmitting in order to prevent resource loss, such as battery power and bandwidth, caused by bogus data injection.

7.1 Choosing Aggregator Monitoring Nodes

Secure data aggregation from the network was quickly identified by all neighbouring nodes in the DAA protocol. By skillfully selecting monitoring nodes, the data aggregator's neighbour was able to accomplish data aggregation and compute subMACs of the aggregated data using the DAA protocol. By using the Monitoring Node Selection (MNS) algorithm, which safeguards the compromised data aggregator while impacting the chosen monitoring node, the DAA protocol is able to pick the monitoring nodes. Each data aggregator assigns indices to nearby nodes in a certain sequence, and the goal of the MNS algorithm is to choose which nodes should be watching those nodes. Additionally, in order to assess the index by applying the modulus operation to a set of randomly generated integers supplied by nearby nodes, the MNS algorithm is crucial. When indices at one node are comparable to those at another node, we say that the two nodes are watching each other. Consequently, the aggregator of data and

all nearby nodes work together to choose monitoring nodes, mitigating the effect of a hacked node on the network.

7.2 Connecting Sensor Nodes in Pairs

The forwarding nodes that connect the current data aggregator to the forwarding data aggregator are an integral part of the DAA method. There is a fixed interval for each data aggregator's outgoing route to the base station. Sending the pair mate discovery message to the neighbouring node list is how the forward data aggregator introduces the monitoring and forwarding nodes. Along with the present data aggregator's key, the forward data aggregator incorporates the MAC algorithm of nearby nodes into its own list. Upon receiving the message, the present data aggregator generates the IDs for the nodes that are forwarding the message and those that are neighbouring it. Consequently, the DAA method effectively identifies the erroneous data by using data aggregators and the nodes next to them when the data is being sent via the network.

7.3 Detection of Malinformation Data using Secure Data Aggregation

With the DAA method in mind, we examine the SDFC algorithm in light of its ability to provide safe data aggregation, Malinformation data detection, and data confidentiality. A hacked node in the SDFC algorithm may inject fake data via data forwarding or data aggregation. Always encrypting sent data and implementing data authentication over encrypted data are two measures used to ensure data confidentiality. The six-step SDFC algorithm is used in the DAA approach. At the outset, data aggregators and the nodes immediately around them are vital for investigating data authentication in the event that the aggregator receives data. Next, for independent data evaluation, the monitoring nodes and data aggregator are both very beneficial. In order to estimate the subMAC for both the encrypted and plain data, each monitoring node is required. Following this, the data aggregator will create two Full-size MACs (FMACs): one for encrypted data and one for plain data. It does this by combining these subMACs from its monitoring nodes. Additionally, the neighbouring node verifies the data integrity of plain data, and the forwarding node verifies the data integrity of encrypted data. The DAA method reduces communication cost when transmitting data by identifying any injected bogus data via compromised nodes using the SDFC algorithm. However, in order to improve the efficiency and security of the network, not every sensor node can enable the DAA protocol.

CONCLUSION

Malinformation attacks are an extremely serious menace to the dependability, performance and the life of Wireless Sensor Networks, especially when hacked nodes conspire to provide synchronized bogus information. The existing node-based and probabilistic security mechanisms are not enough to counter such group-based attacks because they do not capture group-based malicious behavior and they are also resource-heavy. The importance of group-injected malinformation attacks and their negative effects on data integrity, bandwidth usage, energy use, and network throughput are highlighted in this paper. The research emphasizes the use of a collaborative and group-conscious detection as it offers a crucial protection approach to multipath WSN settings through Bandwidth-Optimal Group-Injected Data Filtration (BO-GIDF). The combination of group-based filtering with secure data aggregation and authentication systems will allow preventing the dissemination of malicious data at an early stage, which will save essential network resources and allow preventing the spread of malicious data. This can not only increase security but also increases lifespan of network and increases scalability. Finally, malinformation attacks in the WSNs can only be dealt with through a paradigm shift shift in that individual node-based defenses are no longer applicable; instead, the collaborative, behavior-based filtering systems must be implemented. Group-based malinformation filtering is an appropriate future of constructing secure, efficient, and trustful wireless sensor networks that can be effectively used in unwelcoming and resource-critical conditions.

References

1. Alzahrani, M., Idris, M. Y., Ghaleb, F. A., & Budiarto, R. (2022). An improved robust misbehavior detection scheme for vehicular ad hoc network. *IEEE Access*, *10*, 111241-111253.

2. Ghaleb, F. A., Maarof, M. A., Zainal, A., Al-Rimy, B. A. S., Saeed, F., & Al-Hadhrami, T. (2019). Hybrid and multifaceted context-aware misbehavior detection model for vehicular ad hoc network. *IEEE Access*, *7*, 159119-159140.

3. Gheyas, I., Asghar, M. R., Schneider, S., & Woodward, A. (2025). Establishing Trust in Crowdsourced Data. *arXiv preprint arXiv:2511.03016*.

4. Jalajakshi, v., an, d. m., ghasemi, e., rafiei, v., ranjbaran, g., handrizal, t., ... & khalid, a. e. (2023). Prediction Of Sensor Devices Failure in Unmanned Aerial Vehicles Using

Kalman Filter & Particle Filter. *Journal of Theoretical and Applied Information Technology*, *101*(18).

5. Balakrishnan, C., Vijayalakshmi, E., & Vinayagasundaram, B. (2016, February). An enhanced iterative filtering technique for data aggregation in WSN. In *2016 International Conference on Information Communication and Embedded Systems (ICICES)* (pp. 1-6). IEEE.

6. Ghaleb, F. A., Zainal, A., Rassam, M. A., & Mohammed, F. (2017, November). An effective misbehavior detection model using artificial neural network for vehicular ad hoc network applications. In *2017 IEEE conference on application, information and network security (AINS)* (pp. 13-18). IEEE.

7. Nedungadi, P., Veena, G., Tang, K. Y., Menon, R. R., & Raman, R. (2025). AI techniques and applications for online social networks and media: Insights from BERTopic modeling. *IEEE Access*.

8. Chettri, L., & Bera, R. (2019). A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems. *IEEE Internet of Things journal*, *7*(1), 16-32.

9. Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*, 100031.

10. Singhal, M., Kumarswamy, N., Kinhekar, S., & Nilizadeh, S. (2021). The prevalence of cybersecurity misinformation on social media: Case studies on phishing reports and zoom's threats. *arXiv preprint arXiv:2110.12296*.

11. Zaidan, D. T. (2021). Analyzing Attacking methods on Wi-Fi wireless networks pertaining (WEP, WPA-WPA2) security protocols. *Periodicals of Engineering and Natural Sciences (PEN)*, *9*(4), 1093-1101.

12. Aldwairi, M., & Tawalbeh, L. A. (2020). Security techniques for intelligent spam sensing and anomaly detection in online social platforms. *International Journal of Electrical and Computer Engineering*, *10*(1), 275.

13. Yang, F., Abedin, M. Z., Qiao, Y., & Ye, L. (2024). Towards trustworthy governance of AI-generated content (AIGC): a blockchain-driven regulatory framework for secure digital ecosystems. *IEEE Transactions on Engineering Management*.

14. Pogorelov, K., Schroeder, D. T., Filkuková, P., Brenner, S., & Langguth, J. (2021, October). Wico text: a labeled dataset of conspiracy theory and 5g-corona misinformation tweets. In Proceedings of the 2021 workshop on open challenges in online social networks (pp. 21-25).

15. Olawole, E. T., Akande, D. O., Adeyemo, Z. K., Ojo, F. K., & Ojo, S. I. (2024). Effect of Modulation Domain Coupled KalmanSpectral Filter on Speech Enhancement over Wireless Voiced Communication System. Nigerian journal of technological development, 21(3), 20-28.