Journal of Advances in Science and Technology
Vol.20, Issue No. 2 September-2023, ISSN 2230-9659

A Bandwidth-Optimal Group-Injected Data Filtering and ElGamal-Based Authentication Framework for Secure 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) place a premium on efficient use of resources and safety. Particularly in multipath sensor network routing, studies have concentrated on reducing resource consumption while increasing security. False information is a major problem since it makes it harder to aggregate and authenticate data, which in turn increases the need for bandwidth and battery life. In response, we have built a bandwidth-optimal group-injected data filtering system to improve network performance by decreasing packet-transferred malinformation. In addition, a framework for network authentication has been put in place to strengthen protection against these types of injections. In addition to promoting improved security in multipath data transmission, this also guarantees safer data transfer between nodes and efficiently controls resource utilization. The bandwidth efficient approach employs a data aggregation algorithm to identify malicious information injections, with the goal of lowering energy consumption and network overheads in WSN. To improve the security of wireless sensor networks (WSNS) and reduce the impact of group-injected misinformation, this study presents the BO-GIDF architectural framework. In order to reduce bandwidth consumption, the framework finds all of the neighbors who are spreading false information using a collaborative neighbor selection method that is based on groups. Moreover, it uses an associative filtering approach to save processing time and enhance packet throughput through efficient sink identification. The authors also provide a system called network authenticated based on Elgamal cryptography (NAEC) to improve network privacy and security by strengthening authentication against malinformation injection using asymmetric key encryption. By identifying and isolating hostile actors, the NAEC framework speeds up processing and guarantees high interoperability security via an implicit approved certificate rule that prevents malinformation injection on dynamic pathways.

Keyword: Malinformation, BO-GIDF, NAEC, WSN

1. INTRODUCTION

Wireless Sensor Networks (WSNs) represent a specialized class of distributed networks composed of a large number of low-power sensor nodes that cooperatively monitor physical or environmental conditions such as temperature, pressure, humidity, vibration, or motion. These sensor nodes are typically deployed in large-scale, often unattended environments and

communicate sensed information to a sink or base station through multi-hop wireless transmission. Due to their ability to operate autonomously and provide real-time data from inaccessible or hazardous environments, WSNs have become an essential enabling technology for applications including environmental monitoring, healthcare systems, industrial automation, military surveillance, disaster management, and smart infrastructure. A defining characteristic of WSNs lies in their severe resource constraints. Sensor nodes are equipped with limited computational capability, restricted memory, constrained communication bandwidth, and finite battery energy that is often non-replaceable once deployed. Unlike conventional wireless networks, where devices benefit from continuous power supply and high processing capacity, WSN nodes must carefully balance sensing accuracy, communication efficiency, and network lifetime. As communication activities consume the largest proportion of energy in sensor nodes, minimizing unnecessary transmissions is critical for sustaining long-term network operation. These constraints profoundly influence network design choices and significantly complicate the implementation of robust security mechanisms. Another fundamental attribute of WSNs is their cooperative and data-centric communication paradigm. Rather than supporting end-user communication, WSNs focus on collecting, aggregating, and transmitting sensor-generated data to a central sink. Intermediate nodes participate in routing and aggregation processes, forwarding data generated by other nodes without having complete knowledge of the data's origin. While this collaborative architecture enhances scalability and efficiency, it also introduces significant security vulnerabilities, as compromised nodes can actively participate in network operations and inject malicious content without raising immediate suspicion. Security concerns in WSNs are considerably more complex than those in traditional networks. The open wireless medium exposes transmitted data to interception, replay, and manipulation attacks, while the unattended nature of sensor deployments makes physical capture and compromise of nodes a realistic threat. Once compromised, a sensor node becomes an insider attacker capable of generating syntactically valid and semantically plausible data that can propagate through the network undetected. Such attacks directly undermine the integrity and trustworthiness of sensed information, which is particularly dangerous in mission-critical applications where decisions rely heavily on accurate sensor data.

Among the various security threats targeting WSNs, malinformation injection has emerged as one of the most damaging and difficult to detect. In this context, malinformation refers to deliberately manipulated or fabricated sensor data introduced by compromised nodes with the

intent to mislead data aggregation, disrupt network performance, or exhaust critical network resources. Unlike accidental faults or environmental noise, malinformation is intentional, adaptive, and often designed to mimic legitimate sensing behavior. As a result, traditional validation methods based on fixed thresholds or statistical outlier detection frequently fail to identify such malicious data. The challenge is further exacerbated in multipath routing environments, which are commonly used in WSNs to enhance reliability and fault tolerance. While multipath routing allows data to reach the sink through multiple alternative routes, it also increases the attack surface by enabling malinformation to propagate simultaneously across different paths. Consequently, false or manipulated data may be repeatedly forwarded, processed, and aggregated, leading to excessive bandwidth consumption, accelerated energy depletion, increased transmission delays, and premature network failure. In such scenarios, malinformation attacks function not only as data integrity threats but also as resource exhaustion mechanisms. Conventional security solutions for WSNs predominantly rely on cryptographic authentication, probabilistic filtering, or node-level trust evaluation. Although cryptographic techniques provide confidentiality and authentication, they are often computationally expensive and insufficient against insider attackers who possess valid credentials. Similarly, probabilistic and node-centric filtering approaches tend to perform poorly when malicious nodes operate in coordinated groups. Coordinated or group-injected malinformation exploits spatial and temporal correlations among compromised nodes, enabling attackers to evade detection mechanisms that assume independent or randomly distributed faults. These limitations highlight the urgent need for security strategies that move beyond isolated node verification and incorporate collaborative, behavior-aware analysis.

2. REVIEW LITERATURE

Haibo Wu (2023) This research offers a distributed set-membership filtering method utilizing a trust dynamic combination technique for target tracking issues in wireless sensor networks affected by malicious assaults. The algorithm employs a prediction-correction recursive updating framework akin to Kalman filtering. It incorporates a clustering fusion phase of data received from other nodes between the prediction and measurement correction update phases. This clustering fusion phase utilizes K-means to categorize data from trusted and untrusted nodes, with the target state being updated through the amalgamation of the trusted data set, thereby enhancing resilience against diverse malicious network attacks. Simulation findings indicate that, in comparison to the conventional distributed set-membership filtering approach,

the suggested technique has superior target tracking efficacy against severe network assaults, including random attacks, fake data injection, replay attacks, and hybrid attacks.

Michael Hooper (2016) asserts that commercially available Wi-Fi-based unmanned aerial vehicles (UAVs) are susceptible to fundamental security breaches, executable by novice to intermediate hackers. This is achieved by illustrating that the conventional ARDiscovery Connection procedure and the Wi-Fi access point utilized in the Parrot Bebop UAV are vulnerable, enabling a remote assailant to interrupt the UAV's flying capabilities during operation. We assert that these vulnerabilities are pervasive in Wi-Fi-dependent Parrot UAVs. Our methodology monitored the standard operation (i.e., ARDiscovery Connection process via Wi-Fi) of the Parrot Bebop UAV. Subsequently, we employed a fuzzing technique to ascertain that the Parrot Bebop UAV is susceptible to fundamental denial of service (DoS) and buffer overflow attacks during its ARDiscovery Connection process. The exploitation of these vulnerabilities may lead to the catastrophic and instantaneous incapacitation of the UAV's rotors during flight. Furthermore, we identified that the Parrot Bebop UAV is susceptible to a fundamental ARP (Address Resolution Protocol) Cache Poisoning attack, which may sever the connection with the primary mobile device user and, in most instances, compel the UAV to land or return to its origin.

Althaf Marsoof (2022) asserts that online service providers and governments have progressively depended on Artificial Intelligence ('AI') to manage internet content. In many areas, the law has encouraged, if not mandated, service providers to implement mechanisms for detecting, tracking, and eliminating problematic information, including terrorist propaganda. As a result, service providers are compelled to employ AI for the moderation of online material. Nonetheless, content-filtering AI systems have constraints that impact their precision and clarity. These constraints provide the potential for valid information to be eliminated while bad stuff persists online. This conclusion might jeopardize human well-being and the fulfillment of our human rights. Given these problems, we contend that the design and implementation of content-filtering AI systems necessitate regulation.

Hongyang Du (2023) states that Generative AI (GAI) models are progressing swiftly, including diverse applications such as intelligent networks and mobile AI-generated content (AIGC) services. Despite their myriad applications and promise, such models present prospects for new security issues. This study analyzes the problems and possibilities presented by Generative Artificial Intelligence (GAI) in the security of intelligent network AIGC

services, including the formulation of security rules and its dual role as both a "spear" for prospective assaults and a "shield" inside various defence systems. Initially, we provide a thorough examination of the GAI ecosystem, emphasizing its applications and the methodologies that support these innovations, particularly big language and diffusion models. Subsequently, we examine the dynamic interaction between GAI's offensive and defensive functions, emphasizing two principal kinds of possible GAI-related attacks and their corresponding defence tactics inside wireless networks.

Shiyou Xu (2022) The rapid progress in deepfake generation technology has jeopardized the credibility of digital media, posing significant concerns to privacy and security through the creation of deepfake videos. This study hypothesizes that the integration of sophisticated algorithms with blockchain technology would significantly improve the accuracy and security of deepfake detection systems. A unique framework for identifying deepfake combinations was developed by integrating DDO-AGNN with blockchain technology for federated learning. The current model utilizes a comprehensive dataset that encompasses several deepfake films, which were standardized by min-max normalization during pre-processing. The DDO-AGNN method was executed in Python and enhanced by DDO for superior feature extraction and classification. Blockchain technology was utilized for federated learning, guaranteeing privacy-preserving collaborative model training across several nodes.

3. RESEARCH METHODOLOGY

This study proposes an integrated security framework Bandwidth-Optimal Group-Injected Data Filtering (BO-GIDF), Network Authentication based on ElGamal Cryptography (NAEC). The BO-GIDF component employs a collaborative group-based neighbor identification strategy to detect and isolate nodes involved in malinformation injection before data aggregation occurs. By filtering malicious packets at an early stage, the framework significantly reduces unnecessary bandwidth usage and improves data transmission efficiency. The NAEC module strengthens network authentication through a lightweight asymmetric encryption mechanism based on ElGamal cryptography. This approach enhances security while minimizing computational overhead, enabling faster authentication and improved packet throughput. The design of the Bandwidth-Optimal Group-Injected Data Filtering (BO-GIDF) framework is guided by four fundamental principles derived from the identified threat model and network constraints. First, group-based detection is prioritized over individual node verification. Since malinformation attacks often exhibit coordinated behavior, BO-GIDF

evaluates data consistency at the neighbor-group level, enabling early identification of collusive malicious activity that would otherwise evade node-centric detection. To improve the authentication strategy on sensor networks and prevent Malinformation data injection in WSN, an effective framework is presented, which is named Network Authenticated based on Elgamal Cryptography (NAEC). Furthermore, the ElGamal encryption system is an asymmetric key encryption technique that was developed to prevent fake data insertion utilizing the NAEC architecture. From this, it is clear that the encrypted data is effectively blocking any malicious actors from injecting fake data into data packets used for communication between sensor nodes. This, in turn, uses the Diffie-Hellman key exchange paradigm to identify the malevolent actors in the WSN. Finally, in order to maintain the network's high level of interoperability with improved efficiency, the Implicit Authorized Certificate Rule was designed.

4. DATA ANALYSIS

4.1 Securing Wireless Sensor Networks with Bandwidth Optimal Group Injection Data Filtering

This section compares the proposed Bandwidth Optimal Group Injected Data Filtering (BO-GIDF) framework with existing methods, such as the Bandwidth Efficient Cooperative Authentication (BECAN) scheme and the Data Aggregation and Authentication (DAA) protocol. The former was developed by Rongxing Lu et al. (2012), while the latter was created by Suat Ozdemir and Hasan Çam (2010). Results analyze the values in tables and graphs, as well as the following metrics, and are used to measure the experimental parameters using the suggested BO-GIDF framework.

Quantification of Data Transfer Rate

According to the BO-GIDF paradigm, the amount of data transported during a certain time period is the definition of bandwidth usage in WSN. Bits per second (bps) is the unit of measurement for bandwidth utilization. The mathematical representation of the bandwidth use is shown below.

$$B = Number\ of\ nodes * Data\ Transmitted\ Time(ms) \quad \textbf{(1)}$$

The bandwidth usage, denoted as 'B' in equation (1), is assessed with regard to the number of nodes and data transmission with respect to the given time. If the amount of bandwidth used is reduced, then the approach is deemed more efficient.

Table 1 Data Table for Bandwidth Usage

No. of nodes	Bandwidth Consumption (bps)		
	Proposed BO-GIDF	Existing BECAN	Existing DAA
10	810	965	1285
20	1585	1853	2381
30	2335	2850	3541
40	3045	3700	4713
50	3952	4680	5916
60	4732	5421	7032
70	5532	6300	8000
80	6200	7192	9120
90	6987	7947	10023
100	7643	8963	10893

Table 1 shows the current systems, including the BECAN scheme by Rongxing Lu et al. (2012) and the DAA protocol by Suat Ozdemir and Hasan Çam (2010), as well as the proposed BO-GIDF framework and its relationship to the number of nodes in a WSN. The experimental goal involves varying the number of nodes from 10 to 100. Table 1 demonstrates that all methods see an increase in bandwidth use as the number of nodes increases. In contrast to the status quo, the suggested BO-GIDF structure drastically cuts down on bandwidth use. The proposed BO-GIDF framework is used to characterize the bandwidth usage in WSN in Figure 1. The present system, which includes the BECAN scheme by Rongxing Lu et al. (2012) and the DAA

protocol by Suat Ozdemir and Hasan Çam (2010), is compared with this. Figure 4.1 clearly shows that the suggested BO-GIDF architecture uses less bandwidth than the current approaches. This is because the sensor node's mobility may be tracked using data gathered from nearby nodes via the mobile compromised node, leading to a decrease in bandwidth usage and improved efficiency.

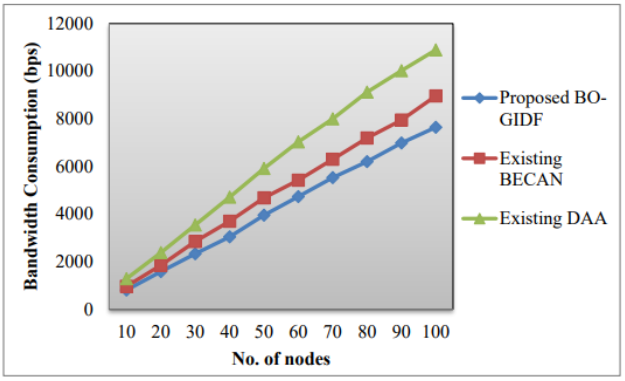

Figure 1 Consumption of bandwidth quantified

Hence, according Rongxing Lu et al. (2012) and the suggested BO-GIDF framework reduces bandwidth usage by 15% compared to the current BECAN scheme and by 33% compared to the existing DAA protocol, respectively.

Evaluation of the Time Required to Send a Packet

A packet's transmission time is the total amount of time it takes to send a packet—header included—over a network at a certain speed. Milliseconds (ms) are the standard units of measurement for packet transmission time. A mathematical expression for the time it takes for a packet to be sent is.

$$PT_{time} = Packet\ Size * H_{size} * \frac{1}{speed} \quad \textbf{(2)}$$

The time it takes for a packet to be sent in a sensor network is represented by the symbol '$PTtime$' in equation (2). The method becomes much more efficient if the time it takes to transmit packets is decreased.

Table 2 Data Table for Time of Packet Transmission

Packet size (bytes)	Packet Transmission Time (ms)		
	Proposed BO-GIDF	Existing BECAN	Existing DAA
400	3.5	4.2	5.2
800	3.9	4.6	5.4
1200	4.3	5.1	5.8
1600	4.5	5.3	6
2000	4	4.8	5.5
2400	3.7	4.5	5.1
2800	3.5	4.2	4.75
3200	3.6	4.4	4.9
3600	3.8	4.6	5.1
4000	4	4.8	5.3

Table 2 displays the time it takes for packets to be sent in WSN using the proposed BO-GIDF framework, in relation to their size. This is compared to current systems, such as the BECAN scheme and the DAA protocol. During the testing process, the packet size is adjusted between 400 and 4000. Table 2 shows that when the packet size increases, the transmission time increases for all techniques. When compared to other techniques, the suggested BO-GIDF architecture offers superior performance in terms of decreasing packet transmission time.

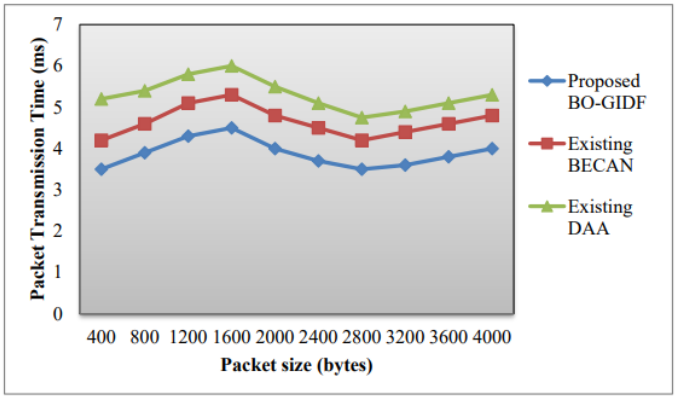

Figure 2 Temporary evaluation of data packet transfer

Figure 2 is a comparison of the current system, comprising the BECAN scheme and the DAA protocol by with the packet transmission time utilizing the proposed BO-GIDF framework in WSN. Figure 2 shows that, in comparison to previous techniques, the suggested BO-GIDF architecture significantly reduced the time it takes for packets to be sent. In order to reduce the time-efficient sink detection algorithm's workload, it compares the frequency of time events in WSNs across nearby nodes at regular intervals. As a result, the packet is optimized for transmission to the sink node after passing through many routers. Therefore, the suggested BO-GIDF framework shortens packet transmission time by 17% compared to the current BECAN scheme (Rongxing Lu et al., 2012) and by 27% compared to the DAA protocol (Suat Ozdemir, 2010; Hasan Çam, 2010).

4.2 Elgamal Cryptography Is Utilized for Network Authentication in Wireless Sensor Networks (Wsn)

The effectiveness of the Network Authenticated based on ElGamal Cryptography (NAEC) framework is evaluated by contrasting it with current methods, such as the Robust Data Aggregation method developed by and the Game theoretical approach. After that, in order to provide better network result analysis, the values of the tables and graphs are evaluated using the performance of the suggested NAEC framework.

Quantification of the Injection of Malinformation Data

In order to assess the NAEC framework's incorrect data injection rate, the packet delivery ratio is used. The percentage of the number of data packets that successfully reach their destination nodes from their source nodes is called the Malinformation data detection rate. The rate of

fraudulent data injection is expressed as a percentage. Here is the mathematical calculation for the incorrect data injection rate.

$$FDI = \left(\frac{Successful\ delivery\ of\ data\ packets}{DP}\right) * 100 \quad \textbf{(3)}$$

In equation (3), the variable 'FDI' stands for the Malinformation data injection rate, which is determined by the quantity of data packets 'DP'. A more efficient approach is one with a greater Malinformation injection rate.

Table 3 Table for the Rate of Malinformation Data Injection

No. of Data Packets	Malinformation Data Injection Rate (%)		
	Proposed NAEC	Existing Game Theoretical Approach	Existing Robust Data Aggregation
10	66.39	49.81	43.67
20	70.65	53.22	47.43
30	68.23	51.18	45.32
40	72.41	55.15	49.16
50	73.55	56.47	50.25
60	70.25	53.82	47.57
70	73.88	56.82	50.88
80	76.43	59.42	53.25
90	79.57	62.65	56.65
100	82.34	65.42	59.41

Comparing the suggested NAEC framework in WSN with current systems, such as the Game theoretical approach and the Robust Data Aggregation technique Table 3 illustrates the Malinformation data injection rate as a function of the number of data packets. For the sake of

experimentation, the number of data packets used as input is adjusted between 10 and 100. According to the statistics in the table, the rate of fake data injection rose for all techniques as the quantity of data packets grew. In contrast to other approaches, the suggested NAEC framework significantly improves the data input rate in the evaluation.

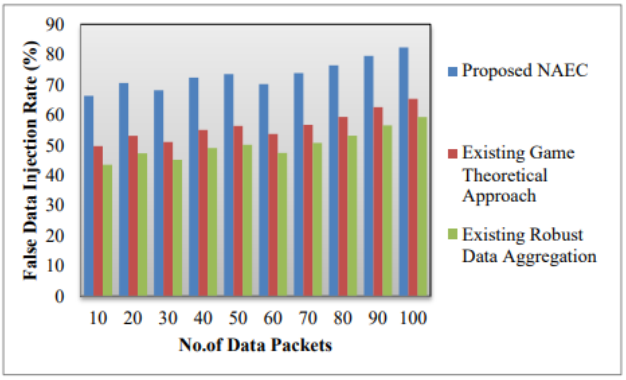

Figure 3 Quantification of the Injection of Malinformation Data

When compared to current systems, such as the Robust Data Aggregation technique and the Game theoretical approach Figure 3 shows the Malinformation data injection rate for the proposed NAEC framework in WSN. In comparison to current approaches, the Malinformation data injection rate is substantially increased by the proposed NAEC architecture (figure 3). Because of the multiplicative ELGamal encryption technique, which helps with the secure distributed storage and transmission of data packets in WSN, the Malinformation data injection rate is improved. In the NAEC architecture, the asymmetric key encryption technique keeps the network system running smoothly while data packets are sent, which improves the rate of Malinformation data injection. Consequently, after comparing the new NAEC framework to the current Game theoretical approach and the existing Robust Data Aggregation technique the Malinformation data injection rate in WSN is improved by 30% and 46%, respectively.

Measure of Security

Using the NAEC architecture, WSN security measures the sum of all data packets delivered to the sink node minus the sum of all data packets that were not received. Percentage is the unit of measurement for the security. Here is an assessment of the mathematical model of security:

$$S = Packetss - Packetsnr \quad \textbf{(4)}$$

The security that is assessed in relation to the data packets transmitted ('$oadketyy$') and those that were not received ($Padketynr$) at the sink node is denoted by 'S' in equation (4). When the level of security in WSN is increased, the process becomes much more efficient.

Table 4 Security Tabulation

No. of Data Packets	Security (%)		
	Proposed NAEC	**Existing Game Theoretical Approach**	**Existing Robust Data Aggregation**
10	65	50	45
20	68	53	48
30	71	56	51
40	73	58	53
50	73	58	53
60	76	61	56
70	79	64	59
80	81	66	61
90	83	68	63
100	85	70	65

The proposed NAEC framework and two existing systems, the Game theoretical and the Robust Data Aggregation technique are shown in Table 4, which shows the security dependent on the quantity of data packets in the network. In order to run the test, the number of data packets is changed from 10 to 100. The security of all the strategies in table 4 is enhanced as the quantity of data packets increases. In contrast to these preexisting approaches, the suggested NAEC framework outperforms them all by increasing the security rate.

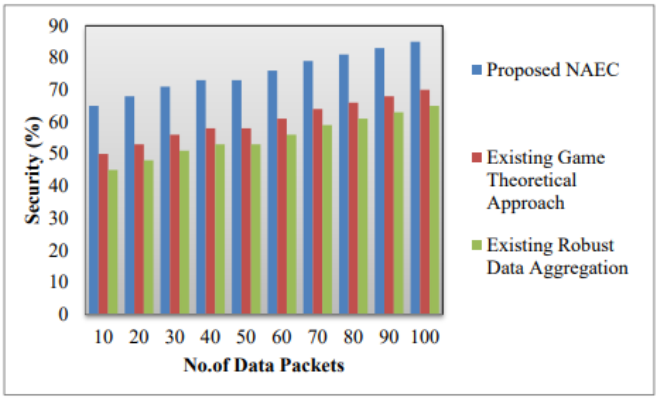

Figure 4 Security Measure

Figure 4 describes the security in WSN for proposed NAEC framework and is compared with existing system including Game theoretical approach and Robust Data Aggregation method From figure 6, the proposed NAEC framework is comparatively improves the security rate when compared to existing methods. The homomorphic mapping function employs encrypted data with private key structure which easily isolate the malicious adversaries from data packets in NAEC framework. Such that, the data packets are avoided during data packet transfer between the source and destination nodes through the sink which resulting in improves the security in WSN. Hence, the rate of security is improved using the proposed NAEC framework in the network by 25% when compared to existing Game theoretical approach by Nicola Basilico et al. (2014) and 37% when compared to existing Robust Data Aggregation method by Mohsen Rezvani et al. (2015) respectively.

CONCLUSION

Primarily, a technique called Localized Bandwidth Optimal Group Injected Data Filtering (BO-GIDF) is suggested for flooding WSNs with fabricated data. To minimize bandwidth usage in WSNs and detect bogus data injection, the BO-GIDF approach introduces a Group based Collaborative Neighbour Selection mechanism. To improve packet transmission and security while doing efficient packet forwarding, the suggested BO-GIDF technique employs a time-efficient sink detection mechanism. By identifying groups of intentionally manipulated data during data packet transmission in WSN, the associative filtering method helps to reduce processing time. For optimally filtering out the misleading data, the suggested BO-GIDF approach employs a verification mechanism. So, the suggested BO-GIDF approach makes WSN networks more secure. The next step in improving the authentication strategy in WSN is to propose the Network Authenticated based on ElGamal Cryptography (NAEC) approach.

The ElGamal encryption system prevents unauthorized access to the network by using an asymmetric key encryption technique. By using the suggested NAEC approach, the ElGamal encryption system improves the privacy level while maintaining the network's security. To detect hostile actors in various forms and cut them off from the network, the Diffie-Hellman key exchange paradigm is used. The suggested NAEC technique reduces processing time by preserving the authentication rules on the sensor network.In order to keep the network's high level of interoperability secure and to prevent the insertion of fake data on dynamic pathways, the Implicit Authorized Certificate Rule was also designed. As a result, WSNs are better protected against fake data injection using the suggested NAEC approach.

References

1. Wu, H., Zhu, H., Li, X., & Amuri, M. J. V. (2023). Trust-based distributed set-membership filtering for target tracking under network attacks. *IEEE Access*, *11*, 84468-84474.

2. Hooper, M., Tian, Y., Zhou, R., Cao, B., Lauf, A. P., Watkins, L., ... & Alexis, W. (2016, November). Securing commercial WiFi-based UAVs from common security attacks. In *MILCOM 2016-2016 IEEE Military Communications Conference* (pp. 1213-1218). IEEE.

3. Marsoof, A., Luco, A., Tan, H., & Joty, S. (2023). Content-filtering AI systems–limitations, challenges and regulatory approaches. *Information & Communications Technology Law*, *32*(1), 64-101.

4. Mah, P. M., Skalna, I., & Pelech-Pilichowski, T. (2022, May). AI-Based Facial-Age Detection and IoT for Enhanced Data Security in Social Media. In *Proceedings of the AAAI Symposium Series* (Vol. 5, No. 1, pp. 242-249).

5. Bahja, M., & Safdar, G. A. (2020). Unlink the link between COVID-19 and 5G networks: an NLP and SNA based approach. *Ieee Access*, *8*, 209127-209137.

6. Du, H., Niyato, D., Kang, J., Xiong, Z., Lam, K. Y., Fang, Y., & Li, Y. (2023). Spear or shield: Leveraging generative AI to tackle security threats of intelligent network services. *arXiv preprint arXiv:2306.02384*.

7. Xu, S., Yang, X., & Xie, Z. (2022). The future of misinformation control: integrating advanced algorithms and Blockchain for effective Deepfake detection. *Peer-to-Peer Networking and Applications*, *18*(4), 244.

8. Kudari, R., & Koduru, S. R. (2021). The study of Mobile cloud computing: Design, Uses, and Security in Covid 19 time. *Int. J. of Aquatic Science*, *12*(2), 2115-2124.

9. Gerts, D., Shelley, C. D., Parikh, N., Pitts, T., Watson Ross, C., Fairchild, G., ... & Daughton, A. R. (2021). "Thought I'd share first" and other conspiracy theory tweets from the COVID-19 infodemic: Exploratory study. *JMIR public health and surveillance*, *7*(4), e26527.

10. Janavičiūtė, A., Liutkevičius, A., & Morkevičius, N. (2022). Toward the Implementation of Text-Based Web Page Classification and Filtering Solution for Low-Resource Home Routers Using a Machine Learning Approach. *Electronics*, *14*(16), 3280.

11. Wani, M. A., ELAffendi, M., Shakil, K. A., Abuhaimed, I. M., Nayyar, A., Hussain, A., & Abd El-Latif, A. A. (2023). Toxic fake news detection and classification for combating COVID-19 misinformation. *IEEE Transactions on Computational Social Systems*, *11*(4), 5101-5118.

12. Rojas, N., Boettcher, N., Játiva, P. P., & Sánchez, I. (2022). Technical Evaluation of Android Parental Control Tools and PDNS Filtering Services: The Chilean Context. *IEEE Access*.

13. Raza, S., Qureshi, R., Lotif, M., Chadha, A., Pandya, D., & Emmanouilidis, C. (2022). Just as humans need vaccines, so do models: Model immunization to combat falsehoods. *arXiv preprint arXiv:2505.17870*.

14. Maulana, A., & Langguth, J. (2023,). Using gnns for misinformation spreader detection via assortativity-aware node label classification in Twitter networks. In *2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS)* (pp. 1-8). IEEE.

15. Yang, H., Li, T., Yan, J., & Elvira, V. (2021). Hierarchical average fusion with GM-PHD filters against FDI and DoS attacks. *IEEE Signal Processing Letters*, *31*, 934-938.