Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Investigating Security, Congestion Control, And Lifetime Enhancement In Wireless Sensor Networks With Various Procedures

S Sivaranjini[1], P.V Ravindranath[2]

[1] *School of Computer Studies, RVS College of Arts & Science, Sulur, Coimbatore, India*
*E-Mail: sivaranjiniooty@gmail.com **
[2] *School of Computer Studies, RVS College of Arts & Science, Sulur, Coimbatore, India*
E-Mail: ravindranath@rvsgroup.com

The development of sophisticated technology known as wireless sensor networks (WSNs) has made remote sensing and monitoring possible in a range of applications. This research paper offers a thorough analysis of WSNs with a focus on Wireless Sensor Networks (WSNs) that rely heavily on security and congestion control to ensure network reliability and longevity. The core concepts of WSNs, design considerations, deployment, and major difficulties encountered in setting up and maintaining WSNs are all covered in this paper. Black hole, gray hole, flooding, and scheduling attacks are also present in WSNs. When there is a lot of data traffic in one area of the network, packet loss, latency, and reduced network efficiency result in congestion. Several strategies and techniques have been developed to improve the lifetime of a WSN, which refers to the amount of time a network can operate on its limited power resources. To promote further breakthroughs in this quickly developing subject, the goal of this study is to give researchers an in-depth understanding of WSNs, their applications, and the difficulties and security, congestion, and lifetime enhancement issues associated with them.

Keywords: Wireless Sensor Networks, Secure Routing, Congestion Control, Delay, Lifetime Enhancement.

1. INTRODUCTION

Small, autonomous sensor node networks with wireless communication capabilities are known as wireless sensor networks (WSNs). To monitor and gather information regarding physical phenomena. Such as temperature, humidity, light, sound, pressure, and more, these nodes are often placed in a variety of surroundings. Environmental monitoring, industrial automation, healthcare, agriculture, and military surveillance is just a few of the many uses for WSNs [1].

The following are some essential traits and elements of wireless sensor networks:
Sensor nodes are network components that sense surroundings and gather data, consisting of sensors, radio transceivers, memory, microcontroller, and power supply.
Wireless Communication: Sensor nodes in WSNs use Zigbee, Wi-Fi, Bluetooth, and LoRa wireless technologies for data communication with a centralized controller or sink node.

Data Aggregation: Sensor nodes perform local processing and data aggregation to reduce network congestion and energy consumption, with network topologies like star, tree, mesh, and ad-hoc determining application and deployment needs.
Energy Efficiency: Energy efficiency is crucial in Wireless Sensor Networks (WSNs), enhancing node longevity through strategies like duty cycling, data compression, and low-power modes.
Routing Protocols: WSNs use routing protocols like LEACH and AODV for efficient data transport while ensuring data integrity, confidentiality, and network availability through encryption, authentication, and intrusion detection mechanisms.
Scalability: Depending on the application, WSNs can expand to incorporate hundreds or thousands of sensor nodes. Effective network management and routing techniques enable scalability.
Fault Tolerance: WSNs frequently need to be resilient to node failures and network interruptions due to the dynamic nature of the settings in which they are deployed. To improve fault tolerance, redundant systems, and self-healing techniques are employed.
Applications: Wireless sensor networks (WSNs) are used for real-time data collection in various industries, including environmental monitoring, industrial automation, healthcare, and agriculture, enhancing productivity, security, and resource management.

1.1 Security Attacks in Wireless Sensor Networks [2]

The dynamic topology of Wireless Sensor Networks (WSNs) allows hostile nodes to exploit its vulnerability, causing numerous security errors and obstructing network traffic.

A. Gray-hole Attack:
The Gray Hole attack is a common WSN routing mechanism that uses a legitimate path to broadcast fake route information. Its primary goal is to intercept packets, discarding all attempts. Identifying the attack involves packet change and packet drop, making it difficult to discern due to various node behaviors.

B. Black-hole Attack:
The primary objective of black-hole attacks is to increase severe network routing technique congestion. An adversary node discards forwarding every packet it receives during a black hole attack. Such an attack no longer allows access to packets. Retransmission causes more widespread network congestion than usual.

C. Sink-hole Attack:
In a sinkhole attack, the attacker tries to attack every network node. As a result, other nodes trust this node and use it to transfer their data. Typically, it uses fictitious resource information to draw on other nodes. After a successful attack, the attacker modifies, spoofs, and forges the received packets.

D. Wormhole Attack:
By tricking a node into thinking there is only one hop between them and the target, an attacker can transfer a packet to a wormhole, enabling the node to drop big data packets or access unauthorized network services. This technique is known as a wormhole attack.

E. Sybil Attack:
This attack interrupts dependable packet transmission by having one node give multiple identities to the other sensors in the established network. It is among the biggest issues when

a user joins a P2P network. It takes over the network, forges several identities, and controls the network as a whole.

F. Denial of Service Attack:

The attacker fills the line of communication with erroneous or redundant traffic to stop it. Genuine users may not be able to discover the information or take the necessary steps as a result of this assault since they are unable to access resources.

- **Modification Attack**

In an attack of this nature, the attacker modifies the routing messages. The quality of the network's packets may be in danger as a result of these adjustments. This will cause network traffic to increase, resulting in DoS attacks. Different types of misbehavior can be carried out with this attack.

- **Rushing Attack**

Rushing attacks enclose sneaky nodes during network discovery by causing faster route requests (RREQs) to nearby nodes. This allows attackers to change packets and add inaccurate hop counts to the routing database, potentially affecting the attacker's success.

- **Sleep Deprivation**

The attacker aims to keep the target node occupied by overloading the network with routing traffic and sleep deprivation attacks. They repeatedly send fictitious requests, causing the node to exhaust its computational capacity and impact genuine network requests.

- **Location Disclosure**

The location disclosure attack exploits mobile networks' secrecy by screening nodes, identifying intermediate nodes, and learning network topology, with the primary goal of acquiring and using other node locations.

- **Routing Table Poisoning**

A route poisoning attack involves an attacker altering the routing table's information to carry out various attacks, creating malicious nodes, altering the network's legitimate messages, generating incorrect entries, and corrupting erroneous information. This can lead to the rejection of valid packets with lower series variety.

- **Route Fabrication**

The goal of this attack is to access network packets without authorization and make them vanish while transactions are in progress. It uses conventional routing rules to alter routing messages, sending packets to malicious or nonexistent nodes. The attack typically involves denial of service (DoS) and flooding, causing packets to be delayed and bandwidth to be wasted. The attack involves sending packets continuously to the target node, dealing with fake packets, and damaging the network's infrastructure.

- **Routing Table Overflow**

Attacks on routing tables' buffering generate fake traffic, dangerous communication, and duplicates. They alter packets, forward them to inexistent nodes, and defeat the buffer, causing the table to run out of space.

- **Impersonation Attack**

The current WSN network lacks authentication, allowing attackers to perform spoofing, flooding, and other attacks by disguising themselves as another node. Spoofing involves a hostile node misrepresenting its network authentication, impacting routing in ad hoc networks. Misbehavior threats involve unauthorized behavior causing unintended harm to different

nodes, such as violating MAC protocol to gain an unfair advantage. Researchers have identified various defense, defending, and protection tactics surveys have provided the latest methods to address network security problems.

1.2 Congestion Control in Wireless Sensor Network [3]

Congestion control in Wireless Sensor Networks (WSNs) is critical to ensuring efficient and reliable communication in these resource-constrained environments. Wireless Sensor Networks (WSNs) are often comprised of an extensive number of small, low-power sensors that gather and send data wirelessly. Congestion can occur when there is an excessive amount of data traffic, limited bandwidth, or limited energy resources.

Here are some approaches to congestion control in WSNs that are commonly used:

A. **Adaptive Data Rate Control:** Sensors can utilize adaptive data rate control to adjust transmission rates based on network conditions, detecting congestion and subsequently lowering them to enhance network efficiency.
B. **Routing Protocols:** Routing protocols, like AODV, DSR, and OLSR, aid in network congestion control by adjusting to network changes and avoiding congested routes.
C. **Priority-Based Traffic:** Congestion can be reduced by prioritizing different types of traffic. Critical data can be prioritized, ensuring timely delivery even in congested scenarios.
D. **Traffic Management:** Controlling the amount and timing of data transmission can aid in congestion reduction. To reduce collisions and congestion, back off mechanisms such as exponential back off or randomization can be used**.**
E. **Cross-Layer Design:** Cross-layer design optimizes communication across physical, MAC, and network layers, reducing congestion and enabling intelligent decision-making at higher levels by utilizing lower-level information.
F. **Energy Efficient Congestion Control:** Because energy efficiency is critical in WSNs, congestion control mechanisms should take node energy consumption into account. To manage congestion while conserving energy, techniques such as duty cycling and sleep scheduling can be used.
G. **Load Balancing:** By distributing traffic evenly among sensor nodes, you can avoid the overuse of specific nodes and thus reduce congestion. Load-balancing algorithms can be used to accomplish this.
H. **Feedback Mechanism:** Sensors can use feedback mechanisms to adjust their behavior in response to network conditions. This feedback, which can come from the base station or neighboring nodes, assists sensors in adapting to changing congestion levels.
I. **Congestion Detection:** It is critical to implement congestion detection mechanisms. Nodes should be able to detect congestion and respond appropriately. Packet loss, queuing delays, and buffer overflow are all indicators of congestion.

1.3 Life Time Enhancement in Wireless Sensor Networks [4]

Since lifetime improvement directly affects the overall effectiveness and performance of Wireless Sensor Networks (WSNs), it is a crucial objective. To monitor and gather data in challenging or remote conditions, WSNs are frequently made of a large number of battery-

powered sensor nodes. Extending the network's life ensures that it can continue to function effectively for an extended period.

Here are some strategies for extending the life of WSNs

A. Energy Efficient Protocols: WSNs use energy-efficient communication protocols like LEACH and TEEN to reduce energy consumption during data transmission, increasing network lifetime through data aggregation and routing techniques.

B. Data Aggregation: Sensor nodes can compress and combine data before delivering it to the base station. Data aggregation at the source node reduces the amount of data transmitted, saving energy and extending the node's lifetime.

C. Sleep-Wake Scheduling: When sensor nodes are not actively sensing or transmitting data, they can be put into low-power sleep mode. They wake up at regular intervals to complete their tasks. Sleep-wake schedules that are synchronized among nodes can save energy by avoiding idle listening and frequent wake-ups.

D. Duty Cycling: Duty cycling entails periodically turning on and off the radio. Nodes can save energy during idle periods and extend their operational lifetime by carefully selecting duty cycles**.**

E. Topology Control: Energy can be saved by adjusting the network topology. Nodes, for example, can adjust their transmission power to effectively communicate with neighboring nodes, reducing energy consumption.

F. Data Storage and In-Network Processing: Nodes can process and store data locally instead of sending it all to the base station. This reduces the need for frequent communication while also conserving energy.

G. Energy-Efficient Hardware: For sensor nodes, using energy-efficient components and low-power microcontrollers can significantly increase their lifetime. Power management techniques such as dynamic voltage and frequency scaling can also be used.

H. Renewable Energy Sources: Sensor nodes' lifespans may be increased in some situations by including renewable energy sources, such as solar panels or energy harvesting systems, which can assist in replenishing the nodes' energy over time.

I. Adaptive Algorithm: Energy consumption can be reduced by implementing adaptive algorithms that can adjust parameters and behaviors based on network conditions and energy levels.

J. Fault Tolerance: Implementing fault-tolerant mechanisms can aid in dealing with node failures and ensuring that the network remains operational even when some nodes are inoperable.

K. Network Deployment and Maintenance: Proper deployment planning and maintenance can help ensure that nodes are optimally placed and in good working order, reducing energy waste.

2. LITERATURE REVIEW

The distinctive characteristics of WSNs, such as their lack of a stable server, lack of a centralized administrative authority, and sparse resource availability in WSN nodes, may exacerbate existing network security vulnerabilities. Throughout a node's existence in the network, it can screen various kinds of unacceptable behavior.

The author [5] (2023) discusses the various applications of WSNs in fields such as environmental monitoring, healthcare, agriculture, and surveillance. The goal of this paper is to provide researchers and practitioners with a thorough understanding of WSNs, their applications, and the challenges they face, thereby fostering further advancements in this rapidly evolving field. The Wireless Sensor Network, or WSN, is a relatively new technology that has the potential to have a wide range of useful uses in the not-too-distant future, both for the general public and for the military. The combination of sensor technologies, computing power, and wireless communication makes it a profitable opportunity that will likely be explored in large quantities in the future.

The paper proposes an Improved Defensive Routing Mechanism (IDRM) and Enhanced Security Model to protect sensor networks from multiple threats (2022) [6]. It evaluates WSNs' broad assaults and secure paths for node security and routing operations, outperforming existing models in terms of security and efficiency. The proposed model outperforms existing models in terms of transmission delay, packet delivery rate, routing overhead, and throughput, making it more useful in evaluation. Strict security policies may increase system load and decrease performance, but these issues can be addressed in the future.

The authors in [7] (2023) proposed a routing against malicious nodes using mobile agents with authentication in each network region and evaluated trust values for each node to detect black hole attacks and protect nodes from various attacks. The network growth increases the complexity of managing mobile agents for authentication, which may have an impact on scalability when additional nodes and agents are added. This issue may be solved in the future.

In the paper [8] (2023), the authors proposed Traditional intrusion detection systems (IDS) are becoming less effective as malicious attempts become more intelligent, frequent, and complicated. Among the greatest common sorts of assaults that harm WSNs is denial of service (DOS). As a result, this paper examines related works that focus on detecting DoS attacks in WSNs. For the purpose of identifying four different kinds of DoS attacks on Wireless Sensor Networks (WSNs), DOS has created deep learning-based intrusion detection systems. Four models were tested, with the CNN model achieving the best performance at 98.79%. CNNs in wireless sensor networks (WSNs) can significantly drain battery-powered devices, potentially reducing network lifespan or requiring regular replacement. Future solutions may address this issue.

The author has offered attacks such as Detect Black Hole, Flooding, and Selective Forwarding (2023) [9]. Random Forest, Decision Tree, Naive Bayes, Logistic Regression, and as well as eight distinct deep learning models Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), CNN-LSTM, LSTM-CNN, CNN-GRU, and GRU-CNN packets across have been used as cluster heads (CH). Good trained on a specialized dataset for WSNs. It has a higher percentage of accuracy compared to classical detection methods. However, node behaviors are not analyzed to prevent possible future attacks.

The authors proposed that one of the most difficult difficulties in wireless sensor networks (WSN) is secure data transmission (2023) [10]. Wormhole node attackers can misbehave in transmission, leading to wormhole-attacked pathways. This work presents a wormhole attack detection approach and optimal path selection strategy using an Ad hoc on-demand Multipath Distance Vector (AOMDV) routing protocol. The source node determines the wormhole-

attacked path. AOMDV's on-demand nature may lead to performance issues, such as longer pathways or less efficient resource use, which may be resolved later.

The author (2023) suggests routing that solves security concerns while minimizing energy consumption, latency, and perfecting-aware Data Replication (PDR) errors and increasing network lifetime [11]. Ant colony networking methods address multi-objective networking problems in sensor networks, focusing on energy consumption and prolonging network lifespan. This routing approach improves energy consumption, PDR, and lifespan, and improves safety rate using a network simulator. The proposed multi-objective routing solution, based on ACOs, minimizes safety threats in Wireless Sensor Network (WSN) information transfer. It assesses nodes' energy, distance, and trust to find the shortest path, enhancing nodes with the most remaining energy for continuous transmission and improved supply security. In the future, the ACO algorithm may prevent vulnerability to security risks such as routing mechanisms or attacks on pheromone paths.

In another study (2020) [12], the author described sensor nodes as especially vulnerable to malicious attacks due to the growing size of wireless sensor networks, the restricted resources of sensor nodes, and the uncertainty of the layout environment. The most frequent attack types, security methods, and trust-based routing protocol security mechanisms are defined in wireless sensor networks. Several types of secure routing methods based on trusted algorithms have been studied and compared. Trust-based routing techniques often require additional expenses for authentication, verification, and trust relationship upholding, potentially causing lower network performance and higher latency, which could be addressed in the future.

This paper introduces SACC-AHP (2022), a novel congestion control method for clustered wireless sensor networks (WSN) [13]. It detects malicious nodes and selects cluster heads using a dynamic belief-based model and multi-criteria decision-making, improving performance, security, and packet delivery and enabling future distributed intrusion detection. WSNs often operate with limited resources such as limited battery power, memory, and processing capabilities. Applying congestion control mechanisms can prevent over-utilization of these scarce resources, affecting the overall performance and lifetime of nodes in the future.

The author (2022) proposed the SACC-AHP technique, which is extended to SACC-FAHP (security-aware congestion control with fuzzy AHP) [14]. Because subjective judgment greatly limits the AHP approach. Basic AHP's capacity to make decisions has increased due to the fuzzy logic approach's failure to take human judgments' ambiguity into account. The same environment for simulation was used to assess both methods. The simulation results show that SACC-FAHP outperforms SACC-AHP. Fuzzy logic-based systems may not always provide transparency in decision-making, making it challenging to comprehend safety outcomes or congestion control strategies, which could be addressed in the future.

The author proposes an angle-based forwarding technique for underwater wireless sensor networks to address congestion, localization, and traffic prioritization issues (2022) [15]. The technique uses hard and soft phases to track energy and buffer status, reducing trafficking. The model's dispatch rate, power efficiency, and long-term viability are compared with current techniques using an NS-3 simulator. Fuzzy logic-based systems may not always provide transparency in decision-making, making it challenging to comprehend safety outcomes or congestion control strategies, which could be addressed in the future.

This study introduces a priority-based rate regulation system using weighted load measures, utilizing a DRED algorithm for service differentiation (2023) [16]. It improves performance with FDNN and adds traffic estimate and diversion techniques. The method also uses a modified additive increase decrease algorithm to reduce congestion and uses an ECA strategy to distribute resources dynamically. Over-reliance on high-value tasks or activities can lead to neglect of other important components, which can hurt overall performance. As a result, a consistent vision of the future can be developed to prioritize specific actions that improve overall performance.

This study offers a novel implementation of TCP-Enewreno over 5G networks, utilizing dynamic bandwidth adjustment and bandwidth estimate to achieve outstanding performance (2023) [17]. If packet losses decrease the congestion window, it increases the transfer rate, which enhances transmission performance in wireless networks. Throughput, loss of packets, and delay are all improved by TCP-Enewreno in simulations compared to previous implementations. A module called TCP-Enewreno is developed in NS-2. TCP-Enewreno variations may not evenly distribute bandwidth among users or apps, potentially affecting user experience on networks with different congestion levels or diverse applications. This can be resolved later.

Hybrid optimum machine learning algorithms are proposed in the study (2023) [18] for secure localization and routing threat detection in wireless sensor networks. It intends to use CICIDS2017 and UNSW standard datasets to determine optimal sensor spacing and location, addressing challenges in estimating unknown nodes and preventing routing attacks. Hybrid models that involve multiple methods can be challenging to explain decision-making processes or reasoning, and future problems in sophisticated applications that require openness can be prevented.

In order to extend the network lifetime by reducing node energy consumption, this study suggests a fuzzy neural network-based clustering with a dolphin swarm optimization routing and congestion control (FNDSCC) scheme (2022) [19]. The technique uses a deep fuzzy neural network model and improved dolphin swarm optimization for energy-efficient cluster head selection. The model's performance has been experimentally validated, in contrast to traditional techniques such as GEC, HPSO, ABC, and RCRT. To expand on this research, hybrid deep learning approaches can be used. Hybrid models, involving multiple methods, can be challenging to explain decision-making processes, openness in sophisticated applications, and debugging and maintaining systems can be used in the future.

The author proposed that WSNs, which are tiny sensor nodes, can sense, process, and transmit data; however, extending their lifespan is costly and difficult in 2023 [20]. Routing protocols that use less energy can ensure reliable data transmission. Control constraints and battery power can have an impact on network longevity. Increased power Node of Influence. The combination of Heterogeneous Path and ONND techniques boosts network node efficiency. The IPENCHP protocol enhances cloud resource management network lifetime by improving energy communication within clusters. Simulation results show it outperforms in terms of throughput, latency, energy consumption, and efficiency. This method may not be able to adjust to abrupt spikes in traffic or dynamically changing network circumstances, which could cause congestion or inefficiency. It may be changed in the future.

The Grey Wolf Optimization Routing Protocol (GWORP), which has been improved with a unique routing mechanism that finds the statistically best path, is introduced in this paper (2023) [21]. Path discovery time can be reduced in half and balanced energy consumption across WSN nodes can be ensured by allowing the finding and reuse of the best path from the source to the destination. GWORP performs better than PSORP (Particle Swarm Optimization Routing Protocol) in terms of energy usage and from beginning to end latency. The results showed that GWORP might potentially extend network longevity by 73% when compared to PSORP. This research does not provide a specific network lifetime. In intricate and diverse network environments, GWO's resilience might be compromised, which could impair its capacity to adjust to various traffic patterns or topologies. This can be fixed in the future.

The Ant Colony Optimization with Genetic Algorithm (ACO-GA) approach is proposed to maximize the number of connected covers (MNCC) (2022) [22]. It converts the problem's search space into a construction graph, reallocating redundantly connected covers to outline non-dominated solutions. The ACO-GNCC approach has proven effective in terms of network lifetime, lower packet loss ratios, and less energy consumption. The system is extended to a real-time WSN model in future work.

The study proposes (2023) [23] a fuzzy logic-based energy-efficient receiver-initiated routing protocol for non-hierarchical wireless sensor networks. The protocol uses multiple hops and fuzzy logic to choose the best path for improved QoS. Simulation results show that the EADQR protocol outperforms other QoS-required protocols in terms of network lifetime expectancy, throughput, and packet delivery ratio while minimizing latency. It also outperforms proactive and reactive routing protocols, extending network lifetime while minimizing energy consumption. Since fuzzy logic-based routing involves exchanging complex information or making decisions together, the presence of increased communication overhead can be addressed in the future.

This study explores an Enhanced based Immune Clonal Selection (EnICS) algorithm for fully connected Wireless Sensor Networks (WSNs) (2019) [24]. The algorithm transmits data via unique routes, ensuring network lifetime is dependent on sensor node battery levels. The EnICS algorithm ensures network connectivity and combined sensing coverage by determining the maximum number of disjoint connected covers. It uses a hypermutation operator, antibody, heuristic data, and local search CSA to improve search efficiency. The EnICS approach is effective in terms of network lifetime, success ratio, packet loss ratio, and energy consumption.

This research paper focuses on energy-efficient target coverage in High-Wave Networks (HWSNs) by applying the Trapezoidal Fuzzy Membership Genetic Algorithm (TFMGA) to the MDCCKC problem (2017) [25]. The TFMGA-MDCCKC algorithm prolongs network lifetime and conserves energy, introducing sensor priority. Simulation results show the proposed approach outperforms other methods regarding Packet Delivery Ratio, energy efficiency, and network lifetime maximization.

3. **CONCLUSION**

The shortcomings of current security features in WSN are explored in this survey using these studies and abstracts. Congestion control mechanisms and lifetime optimization are also explored here to ensure the security of wireless sensor networks. It is heterogeneous, ensures

that nodes cannot advertise routing information that does not conflict with information gathered from other nodes, and provides many useful guarantees, including many promises not provided by secure WSN protocols. In the future, basic WSN security functions can be implemented in WSN protocols, increasing the reliability of current protocols and procedures while reducing their cost. Distributed intrusion detection systems for WSNs can be developed, which improves the reliability of trust estimation while increasing WSN security using less energy and improving performance, security, packet delivery, and lifetime.

REFERENCES

[1] M Asharani & H R Roopashree," A Survey Paper: An Energy and Secure Aware Routing Protocol for Wireless Sensor Network", SN Computer Science, volume 4, Article number: 219 -Springer, 2023.

[2] Saleh Ali Albelwi," An Intrusion Detection System for Identifying Simultaneous Attacks using Multi-Task Learning and Deep learning", International Conference on Computing and Information Technology (ICCIT) Jan. 25 - 27, FCIT/UT/KSA,2022.

[3] J Shene S, S Emmanuel WR, VK Stephen K," Review on energy conservation and Congestion mechanism in mobile WSN: taxonomy, software programs, challenges, and future trends". Springer, 2023

[4] A Hassan, A Anter, M Kayed**,** "A Survey on extending the lifetime of Wireless Sensor Networks in real-time applications", Springer , 2021.

[5] Mr. Sachin Santu Shende," International Journal of Computational Research A Review on Wireless Sensor Network: Its Application and Challenges", Engineering and Science, 2023.

[6] R. Sabitha1, C. Gokul Prasad2 and S. Karthik1," Enhanced Security with Improved Defensive Routing Mechanism in Wireless Sensor Networks", Computer Systems Science & Engineering, 2023.

[7] Humaira Ashraf; Fizza Khan; Uswa Ihsan; Fatima Al-Quayed; N.Z. Jhanjhi; Mamoona Humayun, "MABPD: Mobile Agent-Based Prevention and Black Hole Attack Detection in Wireless Sensor Networks", International Conference on Business Analytics for Technology ieeexplore.ieee.org, 2023.

[8] S Salmi, Loughner, "Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor networks", Journal of Big Data – Springer, 2023.

[9] Murat Dener, Celil Okur, Samed Al, and Abdullah Orman, "A New Dataset for Attacks Detection in Wireless Sensor Networks", IEEE Internet of Things …, ieeexplore.ieee.org, 2023.

[10] N Tamilarasi, SG Santhi. "Detection of wormhole attack and secure path selection in wireless sensor network", Wireless Personal Communications volume 114, Springer, 2020.

[11] B Ravi Chandra, Ajay Roy, and Somnath Chakraborty, Krishan Kumar, "Ant Colony Transmission Method Parallel Deployment for Wireless Sensor Network Optimization in a Multiobjective Routing Protocol", Researchsquare.com, 2023.

[12] Junyao He, Feng Xu, "Research on Trust-Based Secure Routing in Wireless Sensor Networks", Journal of Physics: Conference Series 1486 -022052, 2020.

[13] Divya Pandey∗and Vandana Kushwaha," The use of Analytical Hierarchy Process in sensor-based networks for security-aware congestion control", Research Gate -NHM, 18(1): 244–274, 2022.

[14] Vandana Kushwaha, Divya Pandey,"Security Aware Congestion Management Using Fuzzy Analytical Hierarchal Process for Wireless Sensor Networks", Research Gate, 2023.

[15] S. Sandhiyaa and C. Gomathy," Efficient Routing Protocol with Localization Based Priority and congestion Control for UWSN", Computers, Materials & Continua, 2023

[16] Dr.V.Monisha, "An Improved Mwsn Efficiency by Hybrid Traffic Aware Prescriptive Congestion Avoidance and Reducing Energy Utilization Using Fdnn Approach", Published/ publié in Res Militaris (resmilitaris.net), vol.13, n°2, January Issue , 2023.

[17] Mohamed Sayed Farag, Hatem Ahmed Abd Elkader,"Improving the TCP Newreno Congestion Avoidance Algorithm on 5G Networks", Research Gate, 2023.

[18] Gebrekiros Gebreyesus Gebremariam a,b, J. Panda b, S. Indu b, " Secure localization techniques in wireless sensor networks against routing attacks based on hybrid machine learning models", Alexandria Engineering Journal 82–100-Elsevier, 2023.

[19] P. Suman PRAKASH1, D. KAVITHA2, P. Chenna REDDY3," Multi-Objective Approach to Improve Network Lifetime and Congestion Control Routing for Wireless Sensor Networks", Institute of Fundamental Technological Research PAS, 2022.

[20] Vignesh Prasanna Natarajan[1], S. N. Chandra Shekhar[2], R. Krishna Kumar[3], A," Improved Power Effective Node Combined Heterogeneous Path Protocol for Enhance Network Lifetime Based on Cloud Resource Management in WSN", ISSN:2147-6799-ijisae, 2023.

[21] Baida'a Abdul Qader Khudor1, Dheyaa Mezaal Hussein2, Yousif Abdulwahab Kheerallah3," Lifetime Maximization Using Grey Wolf Optimization Routing Protocol with Statistical Technique in WSNs",Research Gate, 2023.

[22] P.V.Ravindranath*, "Ant Colony Optimization with Genetic Algorithm (ACO-GA) Approach for Network Lifetime Maximization in Heterogeneous Wireless Sensor Networks (HWSNs)", Indian Journal of Natural Sciences- Vol.12 / Issue 70 / February, 2022.

[23] Mohamed Najmus Saqhib 1, and Lakshmikanth S," A Non-hierarchical Multipath Routing Protocol Using Fuzzy Logic for Optimal Network Lifetime in Wireless Sensor Network". Journal of Communications, vol.18, no. 8, August, 2023.

[24] Dr.P.V.Ravindranath, "Enhanced Immune Clonal Selection (Enics) Algorithm For Network Lifetime Maximization In Heterogeneous Wireless Sensor Networks", International Journal of Research and Analytical Reviews (IJRAR) www.ijrar.org- Volume 6, Issue 2, June 2019.

[25] P.V. Ravindranath, "A Trapezoidal Fuzzy Membership Genetic Algorithm (TFMGA) for Energy and Network Lifetime Maximization under Coverage Constrained Problems in Heterogeneous Wireless Sensor Networks", International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 5 Issue: 3, 2017.