ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 15, Issue 3, 2021

Enhancing Efficiency and Security in Distributed Routing for Wireless Sensor Networks

[1]CHIKATI ARAVIND KUMAR
Reg. No.: NU/PR/PHD/18/183
Department of Computer Science and Engineering
NIILM UNIVERSITY,
Kaithal, Haryana, India.

[2]Dr.Sandeep Chahal
Associate Professor
Computer Science and Engineering
NIILM UNIVERSITY,
Kaithal, Haryana, India.

ABSTRACT

Wireless Sensor Networks (WSNs) comprise compact, lightweight sensor nodes that are deployed in a highly distributed and often arbitrary fashion. As technological advancements continue to accelerate the evolution of the Internet of Things (IoT), WSNs are increasingly confronted with challenges, particularly in the domains of security and energy efficiency. Ensuring secure and reliable communication is critical to maintaining the operational longevity and performance of these networks. Among the most pressing concerns is energy consumption at the node level, which directly influences the overall lifespan of the network. Therefore, the development of secure, energy-efficient data transmission protocols is imperative. To address these challenges, various security mechanisms have emerged in recent years, including key management, trust management, access control, and intrusion detection systems. Building on these advancements, this research introduces three novel secure routing algorithms aimed at enhancing communication reliability and energy efficiency in WSNs:

1. **Cluster-Based Secured Geographic Routing using Master-Slave Approach (CGRA-MSA)**
2. **Fuzzy-based Distributed Self-organized Secured G-Cast Routing Protocol (S-GCRP)**
3. **Trust and Fuzzy Cluster-Based Energy Efficient Routing Algorithm (TFCEERA)**

The first proposed algorithm, TFCEERA, presents an innovative trust-based routing framework that utilizes a Gaussian membership function to evaluate and categorize nodes according to their trust levels. Nodes with high trust scores are selected to act as cluster heads, taking part in secure routing processes. The algorithm also considers residual energy and energy consumption during the cluster head selection phase. This strategy enhances the LEACH protocol by integrating trust metrics into its core operation. Additionally, fuzzy logic is applied to enable the formation of non-uniform clusters and optimize routing decisions, thereby improving both energy efficiency and communication security. The second algorithm, S-GCRP, introduces a fuzzy logic-based, self-organizing, and distributed secure routing protocol designed to support dynamic and resilient communication. It leverages the Self-Organized Network (SON) concept to allow nodes to autonomously form and reconfigure

clusters. Each node computes a dynamic weight based on energy status and monitors neighboring nodes to support energy-aware routing. By clustering nodes effectively, the protocol minimizes energy expenditure and ensures load balancing. Cluster heads maintain up-to-date routing information, and secure communication is reinforced through fuzzy logic-driven key vault generation. This ensures the authenticity of data exchanges and enhances overall energy efficiency.

The third approach, CGRA-MSA, addresses the limitations posed by obstacles and isolated nodes in traditional geographic routing models. It employs a novel Master-Slave architecture supported by k-hop neighbor relationships and virtual coordinate mapping to improve communication in complex environments. In this configuration, a single master node can manage communication with multiple slave nodes, enhancing connectivity and conserving energy. The protocol ensures that isolated nodes are incorporated into the routing path through nearby cluster heads, thereby improving network robustness. This method enhances performance by reducing energy consumption, latency, and computational load, while increasing packet delivery ratios and mitigating node isolation issues. Simulation results validate the effectiveness of the proposed routing algorithms. The outcomes demonstrate high packet delivery ratios, reduced energy consumption, lower latency, minimal communication overhead, and strong security—all achieved with low computational complexity. These improvements collectively contribute to extending the overall network lifetime and ensuring more robust, efficient, and secure wireless sensor network operations.

Introduction

Wireless Sensor Networks (WSNs) are becoming increasingly vital in domains such as industrial automation, healthcare, and environmental monitoring. Despite their broad applicability, WSNs face critical challenges due to their distributed architecture, limited energy and processing capabilities, and vulnerability to security threats. Efficient and secure routing remains a key requirement to ensure reliable network performance under such constraints. Traditional routing protocols like LEACH (Low-Energy Adaptive Clustering Hierarchy) aim to reduce energy consumption through clustering but still encounter issues such as control overhead and limited network lifetime. These challenges necessitate both routing optimization and integrated security mechanisms.

Machine Learning and Predictive Routing

Recent advancements in machine learning have introduced predictive routing approaches to enhance efficiency in WSNs. These algorithms analyze real-time and historical network data to forecast traffic patterns and identify energy-efficient transmission routes. Reinforcement learning, in particular, enables nodes to autonomously select optimal paths based on feedback from their environment. This decentralized learning mechanism enhances responsiveness and adaptability in dynamic conditions, reducing reliance on central control systems.

Security Integration in Routing Protocols

Security is critical for WSNs, especially when deployed in sensitive or hostile environments. Routing protocols must incorporate mechanisms that ensure data integrity, confidentiality, and authentication. Cryptographic techniques such as Digital Signatures and Public Key Infrastructure (PKI) help verify the authenticity of transmitted data and prevent unauthorized access. Protocols like Secure Multipath Routing (SMR) and Secure Hierarchical Routing Protocol (SHARP)

ISSN 2454-9940
www.ijasem.org
Vol 15, Issue 3, 2021

are designed to defend against common attacks such as eavesdropping, data tampering, and replay attacks.

Encryption Protocols for Secure Data Transmission

Robust encryption is fundamental for secure data transmission in WSNs. Symmetric encryption algorithms like AES offer strong security with minimal computational load, making them well-suited for sensor nodes. Asymmetric algorithms like RSA provide enhanced security features but are resource-intensive, limiting their use in constrained environments. Lightweight encryption methods such as Speck and Tiny Encryption Algorithm (TEA) offer a practical balance between security and efficiency. Secure key management—through techniques such as dynamic key exchange, key pre-distribution, and secure key agreement—is essential for maintaining confidentiality. When combined with secure routing and authentication, these mechanisms enhance data integrity and communication reliability.

Load Balancing for Optimized Resource Use

Efficient load balancing is necessary to prevent congestion, reduce latency, and ensure even energy usage across the network. Techniques like Weighted Round-Robin (WRR) and Least Connections dynamically distribute traffic based on node availability and capacity. Integrating security with load balancing further safeguards data integrity while maintaining performance. Additionally, anomaly detection mechanisms can monitor irregular behaviors and respond to potential threats, increasing the network's robustness.

Adaptive Routing in Dynamic Topologies

In dynamic environments with node mobility or fluctuating traffic, adaptive routing protocols offer flexibility and resilience. Algorithms such as Ant Colony Optimization (ACO) and Genetic Algorithms (GA) adjust routing paths based on factors like energy reserves, connectivity, and node distance. These strategies minimize energy consumption and latency while maintaining connectivity. Incorporating trust-based mechanisms into adaptive routing enhances reliability, as nodes evaluate the trustworthiness of neighbors and avoid potentially malicious routes.

Intrusion Detection for Network Security

Intrusion Detection Systems (IDS) play a vital role in safeguarding WSNs from internal and external threats. Signature-based IDS can detect known attack patterns, while anomaly-based IDS identify deviations from normal behavior. A hybrid approach combining both methods offers comprehensive threat detection. To be effective in WSNs, IDS solutions must be lightweight and scalable. Distributed and adaptive IDS frameworks help minimize overhead while ensuring timely responses to emerging threats.

Energy-Efficient Routing for Network Longevity

Prolonging the operational lifespan of WSNs hinges on energy-efficient routing. Protocols such as Directed Diffusion and Energy-Efficient Clustering (EEC) reduce energy waste by optimizing data aggregation and communication paths. SPIN (Sensor Protocols for Information via Negotiation) further conserves energy through meta-data negotiation, reducing redundant transmissions. Secure routing

ISSN 2454-9940
www.ijasem.org
Vol 15, Issue 3, 2021

schemes like SEER integrate energy-aware designs with cryptographic techniques to ensure that energy savings do not compromise security.

Multi-Path Routing for Reliability

Multi-path routing enhances network reliability and fault tolerance by establishing multiple routes between source and destination. This redundancy mitigates the effects of node failures and network disruptions. Path selection is often based on factors such as energy consumption, link quality, and traffic load. Security in multi-path routing is reinforced through encryption, digital signatures, and authentication. Combining load balancing with predictive models based on machine learning can improve throughput and enable proactive rerouting, increasing overall network resilience.

Quality of Service (QoS) Optimization

Quality of Service (QoS) is essential for aligning WSN performance with specific application requirements, including latency, bandwidth, and reliability. While protocols like LEACH prioritize energy efficiency, they may fall short in delivering consistent QoS. Machine learning enhances QoS management by enabling dynamic resource allocation tailored to application demands. QoS-aware protocols optimize energy use without sacrificing performance. Hierarchical routing structures further refine QoS by grouping nodes based on capability and tailoring routing strategies accordingly.

Trust-Based Routing for Enhanced Security

Trust-based routing models improve network integrity by assessing and scoring the reliability of nodes based on historical behavior. These models influence routing decisions by prioritizing trusted nodes for data forwarding, thereby reducing the risk of malicious activity. Trust evaluation also enables detection and isolation of compromised nodes. When integrated with adaptive routing and encryption, trust-based models form a comprehensive security framework that supports efficient, secure, and resilient data communication in WSNs.

LITERATURE REVIEW

- **Huang et al. (2010):** ECC with hidden generation point defends against man-in-the-middle attacks using a multi-agent system.
- **Yeh et al. (2011):** ECC-based mutual authentication protocol enhances WSN security and efficiency.
- **Yongsheng et al. (2012):** ECC-based digital signature protocol for efficient and secure broadcast authentication.
- **Li et al. (2013):** Proposed a lightweight ECC-based protocol that reduces delay and improves user identity protection.
- **Nam et al. (2014):** SUA-WSN combines authenticated key exchange and user anonymity using ECC.
- **Vinayagam et al. (2014):** Sybil attack detection via IP-token verification; low cost and fast.
- **Wang et al. (2014):** Analyzed flaws in existing smart card mutual authentication; emphasized need for secure two-factor authentication in HWSNs.
- **Rathore et al. (2015):** Proposed a BAN-logic verified secure mutual authentication protocol, resistant to various threats.
- **Nikooghadam et al. (2016):** Developed a secure key exchange protocol resistant to offline password attacks.

ISSN 2454-9940
www.ijasem.org
Vol 15, Issue 3, 2021

- **YaHan Park et al. (2016):** Combined ECC and biometrics to prevent guessing attacks and improve authentication.
- **Amin et al. (2016):** Token-based mutual authentication system validated via Scyther, showing high security.
- **Challa et al. (2017):** Three-factor user authentication system with biometric revocation and secure smart card integration for WHSNs.
- **Xie et al. (2017):** Anonymous two-factor AKE protocol with dynamic ID, smart card revocation, and low bandwidth.
- **Athmani et al. (2017):** Lightweight key exchange protocol offering resistance to many attacks, verified by AVISPA.
- **Jain et al. (2017):** ECDH-based mutual authentication system with session keys, validated via Scyther tool.
- **Mao et al. (2011):** FL and AACO-based clustering optimize CH selection and inter-cluster routing, improving energy efficiency.
- **Lee et al. (2012):** Fuzzy logic for CH selection to optimize network lifetime in WSNs using LEACH-ERE.
- **Ahamad et al. (2016):** Fuzzy-based CH selection using residual energy and distance to BS, with multi-hop communication.
- **Song Ju (2012):** Simplified ECC with hash chain and symmetric encryption for reduced complexity and risk.
- **Ganesh et al. (2011):** Hybrid encryption scheme combining symmetric/asymmetric methods for robust security.
- **Saqib et al. (2016):** TinyECC implementation improves TinyOS security for WSNs using ECC-based modules.
- **Teguig et al. (2017):** Optimized ECC key management via reduced scalar multiplication, tested on Tmote Sky.
- **Li et al. (2017):** ECC-based protocol for Industrial IoT, resistant to many attacks with high communication efficiency.
- **Alabrah et al. (2012):** Cookie-based TTOHC protocol enhances web session security with lower overhead.
- **Alabrah et al. (2014):** Hash chain protocol improves WSN authentication efficiency and reduces battery consumption.
- **Patil Sanketa et al. (2014):** ENABLE protocol enhances energy efficiency and security over HBQ using ECC.
- **Liao et al. (2014):** ECC-based RFID authentication protocol ensures mutual authentication and performance efficiency.
- **Gajjar et al. (2015):** FAMACRO uses ACO-based CH selection and routing for heat zone avoidance and efficient communication.
- **Nayak et al. (2017):** Proposed a Type-2 Fuzzy Logic (T2FL) clustering method that effectively handles uncertainty and outperforms traditional fuzzy logic models, enhancing network scalability and node lifespan.
- **Wu et al. (2018):** Introduced a lightweight, secure authentication protocol for wireless medical sensor networks, validated using ProVerif and NS-3 simulations.
- **Ahlawat et al. (2018):** Developed a secure key management mechanism (HCKPP) that reduces node capture risks using a peer impact factor and compromise probability model.
- **Mazinani et al. (2018):** Presented FMCR-CT, a clustering and multihop routing method that reduces CH selection frequency and energy consumption, extending network life.

ISSN 2454-9940
www.ijasem.org
Vol 15, Issue 3, 2021

- **Sood et al. (2018):** Proposed a fuzzy logic-based clustering technique with super cluster heads and mobile stations, outperforming LEACH in NS-2 simulations.
- **Du et al. (2019):** Designed a certificateless aggregate signature (CLAS) scheme for secure data aggregation in healthcare WSNs, supporting real-time, low-cost communication.
- Soni **et al. (2019):** Offered a three-factor mutual authentication system for patient monitoring, resilient against major attacks, verified through AVISPA and BAN logic.
- • Selvakumar **et al. (2019):** Used adaptive intrusion detection with biased datasets to improve classification accuracy and reduce false alarms.
- **Sert et al. (2019):** Enhanced fuzzy routing with CLONALG-M, optimizing output membership functions and improving performance in WSNs.
- **Shafik et al. (2020):** Proposed a mobile sink placement strategy using fuzzy logic and expert systems, increasing network lifetime and optimizing data collection.
- **Kausik et al. (2020):** Applied fuzzy inference to optimize DCH selection based on PDR and other network metrics, improving energy efficiency.
- **Mohamed et al. (2020):** Introduced a fuzzy logic algorithm with COA for optimal CH selection, achieving better energy conservation and network performance.
- **Ch et al. (2020):** Developed an energy-efficient data acquisition method using mobile aggregators and CH selection, reducing transmission energy.
- **Lata et al. (2020):** Proposed LEACH–FC protocol with fuzzy-based vice-CH selection, improving energy distribution and WSN reliability.
- **Bensaid et al. (2020):** Applied fuzzy C-means clustering (FCM) for IoT-based WSNs, improving cluster formation and extending network life by 50%.
- **Verma et al. (2020):** Developed FLEC protocol using average energy for CH selection, outperforming LEACH and DEEC in simulations.
- **Kushwaha et al. (2020):** Used fuzzy probabilistic C-means clustering to enhance performance and stability in applications like healthcare and surveillance.
- **Maryem et al. (2020):** Proposed a fuzzy system-based clustering protocol that improves CH selection and overall WSN efficiency.
- **Manikandan et al. (2020):** Integrated VCH-PSO and EFLM for optimal sensor coverage and extended network life, suitable for both static and dynamic WSNs

ACTIVE TRUST AND FUZZY LOGIC BASED ENERGY AWARE ROUTING ALGORITHMS

The Trust and Fuzzy Cluster-based Energy-Efficient Routing Algorithm (TFCEERA) presents a secure and energy-aware routing strategy for wireless sensor networks (WSNs), integrating active trust modeling with fuzzy logic. Unlike traditional passive trust approaches, TFCEERA dynamically evaluates trust based on real-time node behavior, including mobility, energy consumption, packet delivery success, and network participation. Initially, all nodes and links are assigned a default trust value of 0.5, which adjusts over time depending on transmission outcomes. To handle uncertainty in trust evaluations, TFCEERA

ISSN 2454-9940
www.ijasem.org
Vol 15, Issue 3, 2021

uses Gaussian membership functions within a fuzzy logic system. Trust-related metrics such as residual energy, node mobility, reliability, and distance to the cluster head are categorized into fuzzy sets (low, medium, high). These parameters are processed through 81 fuzzy rules to produce trust levels ranging from "lowest" to "best." The system architecture includes several key components: a trust manager for calculating and updating trust values, a fuzzy rule engine for reasoning under uncertainty, a clustering module that forms clusters based on energy and trust, and a secure routing module that ensures robust communication. Clusters are formed with consideration of both energy availability and node trustworthiness, and periodic re-clustering allows adaptability to network topology changes. TFCEERA also includes security mechanisms to detect and mitigate blackhole and denial of service (DoS) attacks. By analyzing abnormal transmission behavior, the system isolates and removes malicious nodes, thereby enhancing network resilience. The system model assumes 50 mobile sensor nodes deployed over a 200m × 200m area, and RSA-based encryption is used to ensure secure communication. Simulations conducted in NS-2 using realistic parameters (such as 0.5 J initial energy, 4000-bit packet size, and 1 Mbps bandwidth) show that TFCEERA significantly outperforms conventional protocols such as LEACH, LEACH with fuzzy logic, and LEACH with active trust.

Performance improvements include:

- First node death delayed (Graph 3.3): TFCEERA extends network life by applying fuzzy logic and energy-aware trust computation.
- 4% lower end-to-end delay (Graph 3.4): Pre-evaluated trust enables efficient routing and reduces retransmissions.
- Improved network lifetime (Graph 3.5): Sensor nodes remain active for more rounds due to efficient energy use.
- Higher network stability (Graph 3.6): Consistent, trust-weighted routing paths improve reliability.
- Last node survival prolonged (Graph 3.7): TFCEERA sustains the network over more operational cycles.
- Slightly higher initial energy consumption (Graph 3.8): This reduces over time as unnecessary transmissions are avoided.
- Enhanced detection of DoS and blackhole attacks (Graphs 3.9 and 3.10): Precise trust scoring improves detection accuracy.
- Higher packet delivery ratio (Graph 3.11): Trust-based routing increases transmission reliability.

FUZZY BASED DISTRIBUTED SELF-ORGANIZED SECURED G-CAST ROUTING PROTOCOL

The fuzzy-based distributed self-organized secured G-Cast routing protocol (S-GCRP) offers a secure, energy-efficient, and adaptive routing solution for wireless sensor networks (WSNs). These networks are typically composed of spatially distributed sensor nodes with limited energy resources. Traditional static clustering techniques are often ineffective in dynamic environments due to frequent changes in node status, mobility, and network topology.

To address these challenges, S-GCRP adopts a self-organizing network (SON) approach that enables the dynamic formation and reorganization of clusters. Cluster formation is based on key parameters such as node density, residual

ISSN 2454-9940
www.ijasem.org
Vol 15, Issue 3, 2021

energy, and distance. Each sensor node calculates a score using these factors and broadcasts it to neighboring nodes. The node with the highest score is elected as the cluster head. Cluster heads are responsible for aggregating data from their member nodes and forwarding it to G-Cast nodes.

G-Cast nodes are high-energy, computationally capable nodes strategically placed within the WSN. The network area is divided into quadrants, with each quadrant containing at least one G-Cast node to ensure even distribution of communication load. These G-Cast nodes relay data from cluster heads to the sink, while also performing additional roles such as data processing and enforcing security mechanisms.

S-GCRP ensures secure and efficient data transmission through the integration of fuzzy logic. Routing decisions are made by evaluating parameters such as transmission energy, data type, and node status. In the event that a G-Cast node is compromised, fuzzy logic helps identify and isolate the malicious node to prevent further damage. The protocol also utilizes a fuzzy vault scheme for secure key generation and management, allowing only authenticated nodes to access and transmit data.

S-GCRP operates in two distinct phases. The first phase involves dynamic cluster formation and reorganization based on the SON model. Re-clustering is triggered by events such as node failure, mobility, or significant signal variation, reducing the overhead of maintaining clusters and improving adaptability. In the second phase, secure routing between cluster heads and G-Cast nodes is managed using fuzzy logic. The size of each cluster is adjusted based on its proximity to a G-Cast node—clusters farther away have larger radii, while denser areas use smaller clusters to optimize energy consumption.

The routing process includes fuzzification of input parameters, rule-based inference to determine the best routing paths, and defuzzification to select the appropriate transmission level. At the receiving end, G-Cast nodes authenticate packets using public and private key verification. Only verified data is forwarded to the sink, ensuring secure end-to-end communication.

Simulation results using OMNeT++ and MATLAB demonstrate that S-GCRP outperforms conventional protocols such as DSBCA and ORLEACH in several aspects, including packet delivery rate, hop count, number of clusters, control overhead, and security. The protocol shows improved performance in hostile environments by effectively detecting insider threats, reducing false rejection rates, and improving network lifetime by up to 20 percent. Additionally, it maintains high data delivery rates and low latency while ensuring balanced traffic distribution and energy efficiency.

S-GCRP provides a robust, scalable, and secure routing framework for dynamic and resource-constrained WSNs. Its combination of self-organized clustering and fuzzy logic-based secure routing makes it well-suited for real-time applications, particularly in sensitive or hostile operating conditions.

CLUSTER AND GEOGRAPHIC BASED MASTER SLAVE APPROACH FOR ENERGY EFFICIENT ROUTING

This study introduces a novel Cluster-Based Geographic Routing Algorithm (CGRA) designed to enhance energy efficiency and packet delivery in wireless sensor networks (WSNs). The proposed

ISSN 2454-9940
www.ijasem.org
Vol 15, Issue 3, 2021

method leverages geographic routing, which enables packet forwarding based on node locations rather than traditional routing tables. It employs a master-slave architecture, where cluster heads (masters) manage routing operations, and cluster members (slaves) are responsible solely for data collection.

System Architecture

The CGRA system architecture comprises sensor nodes, clustering modules, a decision manager, an energy manager, a routing module, and a base station. The architecture combines geographical routing principles with master-slave-based clustering. Node evaluation is conducted using parameters such as residual energy, distance from other nodes, and assigned weights. The decision manager determines the optimal routing path by analyzing these metrics.

Proposed Algorithm: CGRA

Sensor nodes are positioned using a Cartesian coordinate system, and Euclidean distance is employed for cluster formation. The selection of cluster heads is based on three primary criteria:

- Proximity to the sink and cluster members
- High residual energy levels
- Low node mobility

Energy consumption is modeled using Heinzelman's energy model, which accounts for both transmission and reception energy costs.

Obstacle Handling and Virtual Circle Mechanism

To mitigate packet loss caused by physical obstacles, CGRA incorporates a 360-degree geographic forwarding technique using dummy packets to detect blocked paths. When an obstacle is detected, nodes establish a virtual circle around the blockage to reroute data efficiently and reduce the need for retransmissions.

Enhanced CGRA with Master-Slave Architecture (CGRA-MSA)

The CGRA-MSA is an improved version of the original CGRA algorithm. It introduces several enhancements:

- Incorporates isolated nodes into clusters as slave members
- Designates cluster heads with awareness of k-hop neighbors
- Allows high-energy isolated nodes to assume the role of cluster head when necessary

These improvements reduce node isolation, enhance packet delivery success, and distribute energy consumption more evenly across the network.

Simulation Results

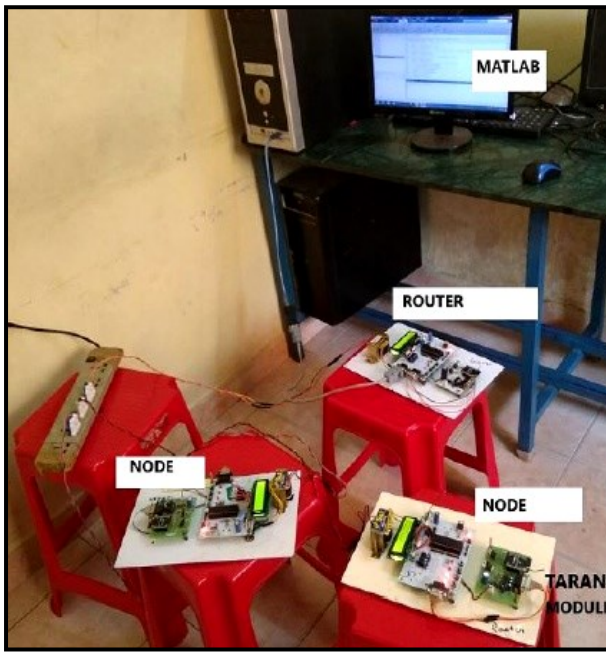
Simulation experiments demonstrate that CGRA-MSA outperforms existing routing protocols such as LEACH, LEACH with fuzzy logic, and REAC-IN. The results highlight:

- A 4 to 6 percent increase in network throughput
- Lower energy consumption and reduced end-to-end delay
- Improved packet delivery ratio
- Extended network lifetime

ISSN 2454-9940
www.ijasem.org
Vol 15, Issue 3, 2021

Hardware Implementation

A hardware prototype was developed using a ZigBee-based system integrated with PIC microcontrollers. Both stationary and mobile nodes exhibited faster decision-making and lower power consumption when operating under the CGRA-MSA protocol, confirming its practical applicability.



CGRA-MSA presents a robust routing solution for WSNs, effectively addressing challenges such as local minima and node isolation. By combining geographic routing with a master-slave architecture and k-hop neighbor awareness, it enhances network scalability, energy efficiency, data delivery reliability, and operational longevity. These characteristics make it well-suited for dynamic and energy-constrained wireless sensor environments.

Conclusion

1. TFCEERA enhances both security and energy efficiency in wireless sensor networks by integrating fuzzy logic with an active trust model. It significantly extends network lifetime, improves stability, and effectively identifies malicious nodes such as blackholes.
2. S-GCRP presents a self-organizing, fuzzy-based secure G-Cast routing protocol. It incorporates fuzzy key management to enable secure communication, adapts dynamically to network topology changes, and achieves efficient load balancing with minimal computational overhead.
3. CGRA-MSA merges geographic routing with a master-slave framework. It effectively addresses obstacles through virtual coordinate mapping and integrates isolated nodes into clusters, leading to improved packet delivery ratio, reduced latency, and balanced energy consumption.

Simulation results confirm that all three approaches outperform existing protocols like LEACH, DSBCA, and ORLEACH in terms of packet delivery efficiency, energy consumption, latency, and overall network lifetime.

This thesis introduces three innovative routing algorithms for Wireless Sensor Networks (WSNs): TFCEERA, S-GCRP, and CGRA-MSA, each designed to enhance network efficiency, security, and reliability. TFCEERA utilizes fuzzy logic for trust-based routing, aiming to establish reliable communication by actively assessing node behavior. When evaluated against existing protocols such as LEACH, LEACH with fuzzy logic, and PWDGR, TFCEERA demonstrates a 6% improvement in network lifetime, a 28% reduction in end-to-end delay, and a 4% increase in overall network stability. S-GCRP proposes a secure routing mechanism based on self-organized G-Cast clustering, incorporating fuzzy key management for robust authentication and secure data transmission. Compared to

ISSN 2454-9940
www.ijasem.org
Vol 15, Issue 3, 2021

protocols like DSBCA and ORLEACH, S-GCRP achieves 15–20% energy savings while reducing routing overhead by 40%. Meanwhile, CGRA-MSA focuses on energy-efficient geographic routing using a master-slave architecture and virtual coordinate mapping, particularly effective in managing isolated nodes and navigating obstacles. It improves network lifetime by 5%, reduces delay by 35%, and enhances the packet delivery ratio (PDR) by 8% over traditional approaches such as LEACH and LEACH with fuzzy logic. Collectively, these three protocols offer significant advancements in addressing the core challenges of WSNs, including secure communication, load balancing, and energy conservation.

Future Work

- Investigate the use of fuzzy rough sets to enhance decision-making in routing protocols.
- Develop advanced clustering strategies and optimize geographic routing techniques for dynamic WSN environments.
- Design robust and secure data aggregation mechanisms to support holistic processing in sensor networks.
- Extend and evaluate the proposed models in diverse network scenarios, including the Internet of Things (IoT), vehicular ad hoc networks (VANETs), and cognitive radio networks.
- Explore trust-based frameworks for real-time monitoring, data prediction, and anomaly detection in wireless sensor applications.

Reference

1. Ahmed & Hussain (2011) – Energy-efficient routing for mobile sensor networks. *IWCMC Conf.*
2. Ali et al. (2017) – Secure region-based geographic routing. *PLoS ONE.*
3. Anju et al. (2014) – Load-balanced clustering in WSN. *IJRCCT.*
4. Ankit & Ketan (2014) – Cluster head election in WSNs. *IEEE Sensors J.*
5. Ari et al. (2015) – Power-efficient routing using swarm intelligence. *J. Netw. Comput. Appl.*
6. Hart & Martinez (2006) – Environmental sensor networks. *Earth Sci. Rev.*
7. Heinzelman et al. (2000) – LEACH protocol. *HICSS.*
8. Heinzelman et al. (2002) – Protocol architecture for microsensor networks. *IEEE Trans.*
9. Hiren et al. (2016) – E2R2 routing for mobile WSNs. *IEEE Sys. J.*
10. Ibriq & Mahgoub (2006) – Secure hierarchical routing. *IEEE Conf.*
11. Jiang et al. (2012) – Unequal clustering protocol. *J. Softw.*
12. Johnson & Maltz (1996) – Dynamic source routing. *Mobile Computing.*
13. Jothi et al. (2016) – Data gathering and routing in MWSNs. *Asian J. IT.*
14. Juan et al. (2015) – Opportunistic routing in WSN. *IEEE Trans. Ind. Inform.*
15. Junfeng et al. (2015) – Pair-wise directional routing. *IEEE IoT J.*
16. Kulothungan et al. (2011) – Fault-tolerant routing. *Int. J. Soft Comput.*
17. Leu et al. (2015) – Energy-efficient clustering for isolated nodes. *IEEE Commun. Lett.*
18. Li et al. (2011) – Geographic hole-bypassing. *IET Commun.*
19. Li et al. (2000) – Scalable location service. *MobiCom.*
20. Lindsey & Raghavendra (2002) – PEGASIS protocol. *IEEE Aero Conf.*
21. Li et al. (2010) – Trust-based multipath routing. *IET Inf. Sec.*

22. Logambigai & Kannan (2015/2016) – Fuzzy unequal clustering. *Wireless Networks.*
23. Manjeswar & Agrawal (2001/2002) – TEEN & APTEEN protocols. *IEEE IPDPS.*
24. Mhatre & Rosenberg (2004) – Homogeneous vs. heterogeneous clusters. *IEEE ICC.*
25. Mohammad & Jalali (2017) – Sugeno fuzzy clustering. *Eng. Appl. AI.*
26. Muhammad & Tae (2016) – Fuzzy adaptive verification. *Ad Hoc Netw.*
27. Padmalaya & Anurag (2016) – Fuzzy-based clustering. *IEEE Sensors J.*
28. Perkins & Royer (1999) – AODV routing. *IEEE Workshop.*
29. Rifa-Pous & Herrera (2011) – Fair and secure clustering. *Wireless Pers. Commun.*
30. Romer et al. (2002) – Middleware challenges. *ACM SIGMOBILE.*
31. Selvi et al. (2016) – Fuzzy temporal routing. *ACM Conf.*
32. Siavoshi et al. (2016) – Geo multilayer clustering. *IET WSN.*
33. Singh & Hussain (2010) – Hierarchical secure routing. *IJASUC.*
34. Sohraby et al. (2007) – WSN tech & protocols. *John Wiley.*
35. Song et al. (2007) – Secure position-based routing. *Ad Hoc Netw.*
36. Son et al. (2003) – IGF protocol. *Univ. Virginia Tech. Rep.*
37. Tarhani et al. (2014) – SEECH protocol. *IEEE Sensors J.*
38. Thangaramya et al. (2017) – Spectral graph clustering. *IEEE Conf.*
39. Wang et al. (2012) – Secure cluster formation. *IJDSN.*
40. Wu et al. (2008) – Secure routing improvements. *IEEE Conf.*
41. Yang Min Lee (2017) – Node classification via DL. *Ad Hoc Netw.*
42. Yassein et al. (2009) – V-LEACH protocol. *IJDCTA.*
43. Ying et al. (2013) – Load-balanced distributed clustering. *IEEE Sensors J.*
44. Younis & Sonia (2004) – HEED protocol. *IEEE Trans. Mob. Comput.*
45. Yuxin et al. (2016) – Active Trust routing. *IEEE Trans. Inf. Forensics.*
46. Zeynab et al. (2016) – Swarm fuzzy routing. *Expert Syst. Appl.*
47. Zhang et al. (2013) – Secure geographic routing. *PLoS ONE.*
48. Zhang et al. (2013) – Secure sensor data transmission. *VLSI & Embedded Sys.*
49. Zhang & Xu (2008) – Secure on-demand routing. *IEEE Conf.*
50. Zhao et al. (2014) – Tree-based energy routing. *IEEE Trans. Nucl. Sci.*
51. Zhao et al. (2012) – Hybrid key management. *WSN J.*
52. Zhong et al. (2014) – Secure clustering & routing. *ISPAA Conf.*
53. Ahamad & Kumar (2016) – Region clustering with fuzzy logic. *RTEICT.*
54. Ahlawat & Dave (2018) – Attack-based key management. *Procedia Comp. Sci.*
55. Ahmed et al. (2012) – Internal attack taxonomy. *Int. Sci. Res.*
56. Alabrah & Bassiouni (2012/2014) – Hash chain & auth. schemes. *IEEE GLOBECOM/WCNC.*
57. Alanazi et al. (2010) – Crypto comparison (DES/3DES/AES). *J. Comput.*
58. Alcaraz et al. (2012) – Key management in WSNs. *Comput. & Security.*
59. Amin & Biswas (2016) – Secure key agreement. *Ad Hoc Netw.*
60. Athmani et al. (2017) – Dynamic auth. in WSNs. *FGCS.*
61. Ahmed et al. (2012) – Taxonomy of internal attacks. *Int. Sci. Res. Innov.*
62. Alabrah & Bassiouni (2012) – One-way hash protocol. *IEEE GLOBECOM.*

63. Alabrah & Bassiouni (2014) – Auth scheme for WSNs. *IEEE WCNC.*
64. Alanazi et al. (2010) – Crypto comparison (DES, 3DES, AES). *J. Comput.*
65. Alcaraz et al. (2012) – Key management scheme selection. *Comput. & Security.*
66. Amin & Biswas (2016) – Lightweight secure key scheme. *Ad Hoc Netw.*
67. Athmani et al. (2017) – Dynamic authentication in WSNs. *FGCS.*
68. Badetia & Hussain (2017) – Node authentication mechanism. *IEEE I2CT.*
69. Bensaid et al. (2020) – Fuzzy C-means clustering. *IEEE IWCMC.*
70. Ch & Budyal (2020) – Energy-efficient EM & fuzzy logic. *SPIN.*
71. Challa et al. (2018) – ECC-based authentication in healthcare. *Comput. Electr. Eng.*
72. Choi et al. (2014) – ECC-based secure WSN protocol. *Sensors.*
73. Dahiya et al. (2015) – Modeling energy-efficient sensor nodes. *JIE (India).*
74. Das et al. (2012) – Password-based user auth. *J. Netw. Comput. Appl.*
75. Fouchal et al. (2013) – DoS prevention using clustering. *Int. J. Commun. Syst.*
76. Gajjar et al. (2015) – Fuzzy-Ant Colony MAC-routing. *Procedia Comp. Sci.*
77. Ganesh et al. (2011) – AES-ECC hybrid security. *IEEE ICRTIT.*
78. Guo & Deng (2011) – ECC + Lagrange key system. *IET Commun.*
79. Huang et al. (2010) – Man-in-middle defense using ECC. *IEEE NSS.*
80. Jain & Hussain (2017) – Lightweight auth. protocol. *IEEE ICECCT.*
81. Ju (2012) – Lightweight ECC key protocol. *IEEE ICAD.*
82. Kaushik & Gupta (2020) – AI-based fuzzy clustering. *IEEE SCEECS.*
83. Kushwaha & Jadon (2020) – Fuzzy C-means WSN perf. boost. *IEEE CSNT.*
84. Lata et al. (2020) – Fuzzy clustering for reliability. *IEEE Access.*
85. Lee & Cheng (2012) – Fuzzy clustering with energy prediction. *IEEE Sensors J.*
86. Li et al. (2014) – Hop-by-hop privacy and auth. *IEEE TPDS.*
87. Li et al. (2013) – Secure key mgmt in WBANs. *ACM Trans. Sensor Netw.*
88. Li et al. (2018) – ECC-based secure auth. for IIoT. *IEEE Ind. Inform.*
89. Li et al. (2013) – Lightweight identity-based auth. *IEEE ICSPCC.*
90. Liao & Hsiao (2014) – ECC-based RFID auth. *Ad Hoc Netw.*
91. Manikandan et al. (2020) – PSO + fuzzy for clustering. *IEEE ICCIT.*
92. Mao & Zhao (2011) – Unequal fuzzy clustering + ACO. *J. CUPT.*
93. Maryem et al. (2020) – Fuzzy logic routing survey. *IEEE ISCV.*
94. Mazinani et al. (2018) – FMCR-CT routing with threshold. *Alexandria Eng. J.*
95. Mohamed et al. (2020) – Coyote opt. with fuzzy logic. *IEEE Access.*
96. Mohanty (2010) – Energy-efficient routing & QoS eval. *M.Tech Thesis.*
97. Nam et al. (2014) – ECC secure auth. for WSNs. *Sensors.*
98. Nayak & Vathasavai (2017) – Type-2 fuzzy clustering. *IEEE Sensors J.*
99. Nikooghadam et al. (2016) – Lightweight anonymous auth. *Multimed. Tools Appl.*
100. Pandey & Tripathi (2010) – WSN security survey. *IJCA.*
101. Park & Park (2016) – Three-factor ECC auth. *Sensors.*
102. Patil et al. (2014) – ECC-based protocol comparison. *IEEE ICACACT.*

103. Potlapally et al. (2006) – Crypto energy consumption study. *IEEE TMC.*
104. Priyanka & Manpreet (2018) – Fuzzy clustering for lifetime. *SSRG IJEC.*
105. Rathore & Hussain (2015) – Token-based WSN auth. *Springer Conf.*
106. Saqib & Iqbal (2016) – ECC-based security. *IEEE ICACA.*
107. Sharma & Ghose (2010) – WSN security threats overview. *IJCA.*
108. Shim et al. (2013) – Identity-based broadcast scheme. *Ad Hoc Netw.*
109. Singh et al. (2010) – Homogeneous energy-efficient clustering. *IJWMN.*
110. Soni et al. (2018) – Three-factor auth. for patient monitoring. *Comp. Methods Biomed.*
111. Stallings (2013) – Cryptography textbook. *Pearson.*
112. Sumathi & Vidhyapriya (2012) – Cognitive radio security survey. *IEEE ISDA.*
113. Teguig et al. (2017) – ECC-based auth. in WSN. *IEEE GCCCE.*
114. Verma et al. (2020) – Fuzzy clustering for mobile sinks. *IEEE Sensors J.*
115. Vinayagam & Parthasarathy (2014) – Token-based IP assignment. *IEEE ICSEMR.*
116. Shafik et al. (2020) – Mobile fuzzy sink WSN protocol. *IEEE CFIS.*
117. Wang & Wang (2014) – Security of two-factor auth. *Ad Hoc Netw.*
118. Wu et al. (2018) – Secure healthcare auth. scheme. *FGCS.*
119. Xie et al. (2017) – ID-based two-factor auth. *IEEE TIFS.*
120. Xue et al. (2013) – Temporal-credential auth. scheme. *J. Netw. Comput. Appl.*
121. Yang et al. (2008) – SDAP data aggregation protocol. *ACM TISSEC.*
122. Yasmin et al. (2010) – ID-based auth. framework. *IEEE CIT.*
123. Yeh et al. (2011) – ECC-based secured protocol. *Sensors.*
124. Liu et al. (2012) – Signature amortization for broadcast. *IEEE Trans. Wireless Commun.*
125. Zhang et al. (2014) – Forward-aware energy-balanced routing. *IEEE Ind. Inform.*
126. Zhu et al. (2012) – Coverage & connectivity in WSN. *Elsevier JNCA.*
127.