ENERGY EFFICIENT RELIABLE COMMUNICATION IN PRESENCE OF COMPROMISED NODES IN A WIRELESS SENSOR NETWORK

A report submitted during 2023 to the University of Hyderabad in partial fulfillment of the award of a Ph.D. degree in Computer Science

by

VASAVI JUNAPUDI

School of Computer and Information Sciences
University of Hyderabad
(P.O.) Central University Campus
Hyderabad-500 046, India
December, 2023

CERTIFICATE

This is to certify that the thesis entitled **"Energy Efficient Reliable Communication in presence of compromised nodes in a Wireless Sensor Network"** submitted by **Vasavi Junapudi** bearing **Reg. No. 12MCPC09** in partial fulfilment of the requirements for award of **Doctor of Philosophy** in **Computer Science** is a bonafide work carried out by him under my supervision and guidance.

This thesis is free from plagiarism and has not been submitted previously in part or in full to this or any other university or institution for award of any degree or diploma. The student has the following publications before submission of the thesis for adjudication and has produced evidence for the same.

1. Vasavi, J., Udgata, S.K. (2018) 'Lifetime maximization of wireless sensor network-swith multiple sinks using multiple paths and variable communication range', International Journal of Sensor Networks (IJSNet), Vol.26, No. 3, pp.no. 200–211, 2018. IJSNET.2018.090142 Inderscience Publishers.

2. Junapudi, V., Udgata, S.K. (2019). 'Extended Lifetime and Reliable Data Transmission in Wireless Sensor Networks with Multiple Sinks'. In: Satapathy, S., Bhateja, V., Das, S. (eds) Smart Intelligent Computing and Applications . Smart Innovation, Systems and Technologies, vol 105. Springer, Singapore. https://doi.org/10.1007/978-981-13-1927-3-10

3. Vasavi, J., Udgata, S.K. (2023). 'Reliable Data Delivery in Wireless Sensor Networks with Multiple Sinks and Optimal Routing'. In the proceedings of International conference of Machine Learning, IoT and Big Data, Odisha 2023

4. Vasavi, Junapudi, and Siba K. Udgata. "Trust-based Compromised node identification and enhancement of network lifetime using alternate path in a wireless sensor network", accepted in 8^{th} International Conference on Information System Design & Intelligent Applications. Dubai: Springer Nature, 2024 accepted for presentation and publication

Further, the student has passed the following courses towards fulfilment of coursework requirement for Ph.D.

Course Code	Name	Credits	Pass/Fail
CS 801	Data Structures and Algorithms	4	PASS
CS 803	Operating Systems and programming	4	PASS
CS 828	Mobile Computing	4	PASS
CS 829	Trends in Soft Computing	4	PASS

Prof. Siba K. Udgata

Supervisor,

School of Computer and

Information Sciences,

University of Hyderabad

Prof. Atul Negi

Dean,

School of Computer and

Information Sciences,

University of Hyderabad

DECLARATION

I, **Vasavi Junapudi**, hereby declare that this thesis entitled **"Energy Efficient Reliable Communication in presence of compromised nodes in a Wireless Sensor Network"** submitted by me under the guidance and supervision of **Prof. Siba K. Udgata**, School of Computer and Information Sciences, University of Hyderabad, is a bonafide research work. I also declare that it has not been submitted previously in part or in full to this University or any other University or Institution for the award of any degree or diploma. A report on plagiarism statistics from the University Librarian is enclosed.

Date: 22-12-2023

Vasavi Junapudi

Regd.No. **12MCPC09**

ACKNOWLEDGMENTS

I take this opportunity to thank the people who helped me in completing my Ph.D. First and foremost I am grateful to my supervisor Prof. Siba Kumar Udgata for his constant supervision and encouragement. He has been a person of positive energy and made me energetic in each interaction I had with him. His appreciation and positive comments always helped me in making my ways better.

I am thankful to my Doctoral Review Committee members, Prof. Alok Singh and Prof. Chakravarthy Bhagvati for their reviews and timely comments during meetings. Their deep insights have helped me understand the problems well and generate solutions.

I am grateful to the Dean of SCIS, Prof. Atul Negi for facilitating top-notch infrastructure facilities and fostering a conducive environment in the laboratory. I thank all the SCIS faculty who have encouraged me directly or indirectly throughout my association with them. I am thankful to the office staff for helping me through all the administrative procedures during my Ph.D. tenure.

My Ph.D. would not have been possible without the support of my family- my husband Mr. Niranjan Surepogu, my children Nirvaan Surepogu and Veronica Surepogu. I admire the sacrifices made by them when I was busy with my work. I sincerely express my gratitude to my parents, Mr. Sundara Singh Junapudi and Mrs. Suseela Junapudi, for their unwavering support and constant motivation throughout my PhD journey. Their encouragement has been a source of inspiration, especially during challenging times when I faced time constraints

due to my job responsibilities. They have consistently been my driving force in pursuing and completing my doctoral work.

My acknowledgments would not be complete without appreciating my friend Mrs. Deepthi Kalavala, who has been a constant motivation in my rough times during Ph.D. Her care, concern and timely advice have given me immense strength while doing my thesis.

Additionally, I am grateful for the collaborative atmosphere created by my labmates, Shekhar, Charan, Ali and Bindu Sri have contributed significantly to maintaining a motivational and peaceful setting in our research space. Their collective efforts have played a crucial role in enhancing the overall research experience, and I truly appreciate the support and resources provided that have positively impacted our academic endeavors.

This thesis is dedicated to my family members and my friends, who have been the sources of motivation for me in every walk of life. It is because of their consistent support and encouragement that I could accomplish this task.

ABSTRACT

Wireless Sensor Networks are spatially distributed sets of sensor nodes over a region by randomly deploying dedicated sensors to monitor different physical conditions. The sensed data is transmitted as data packets to the central base station or sink. WSN is also used to collect the data from a remote region where a human can't reach to deploy or to maintain after deployment. Upon sensing the data, a sensor node transmits this information to the sink for processing.

This work has focused on a few important challenges concerning the WSN. As limited resources characterize the sensor nodes in terms of computational power, memory, storage, and energy, optimum utilization of energy is inevitable for the network to perform satisfactorily for a long time. This thesis proposes different methodologies for enhancing network lifetime (NL) regarding the number of messages successfully delivered to the sink node in the presence of multiple sinks, hot spot nodes, unreliable intermediate nodes, and compromised (untrustworthy) nodes. At first, we implement a Clustering Algorithm for Sink Selection (CASS) wherein multiple sinks are present to improve the network lifetime. In the Wireless Sensor Network set-up, the selection of one sink for data delivery is determined based on shift rate. During the experimentation, it is observed that the network lifetime can not be improved substantially due to the creation of hot spot nodes. Hot spots are those nodes that use most of their energy to forward the data packets to the sink nodes. To overcome this phenomenon, we propose and implement an Alternate Path protocol to avoid the hot spot nodes during the data transmission. This intuitive approach can preserve the remaining

energy in the hot spot nodes and help enhance the network lifetime. With an assumption that nodes can dynamically adjust their communication range by varying the transmitting power, we propose an Adjusting/Increased communication range (ICR) based method to communicate directly with the sink bypassing the hot spot nodes and in the absence of the alternate path. The sensor nodes often do not behave reliably due to buffer overflow, noisy communication channels, memory constraints, inadequate computational power, etc. These unreliable nodes may only be able to forward the data packets successfully depending on the processing demand. We consider the presence of unreliable nodes in the network. We relaxed the assumption that every node can forward the data packets to the next sensor node or sink if it has enough residual energy. We implemented the two earlier methods, namely Alternate Path and Increased Communication Range, to deal with unreliable nodes and, in the presence of hot spot nodes, to enhance the packet delivery ratio as a primary objective and network lifetime as a secondary objective.

As sensor nodes are deployed in the open, there is a chance of the node being compromised. Sometimes, even the communication link is compromised due to different security attacks. The compromised nodes and links can be identified using a trust-based framework. We propose a hybrid trust computation model using direct and indirect trust mechanisms to identify the compromised nodes and links. We then propose a method to segregate the compromised node or link in the network, recompute the alternate path routing, and implement increased communication range as and when required to increase the packet delivery ratio. We have carried out extensive simulations and found that our proposed models can enhance the reliability and lifetime of the WSN using multiple sinks in the presence of hot spot nodes, unreliable nodes, compromised nodes, and compromised links.

Table of Contents

List of Tables

List of Figures

Abbreviations

WSN	Wireless Sensor Network
CBM	condition-based maintenance
NL	lifetime of a network
SN	Source Node
DN	Destination Node
ED	Energy Dissipation
URNode	Un-Reliable Node
percUR	percentage of unreliability
CH	Cluster Head
EAUDC	Energy-Aware Unequal Data Clustering
BS	Base station
GFTCRA	Grid-based Fault Tolerant Clustering and Routing Algorithms
MWSN	Mobile Wireless Sensor Network
ARBIC	Adjustable Range-Based Immune hierarchy Clustering protocol
PDR	packet delivery ratio
AP	Alternate Path
ICR	Adjustable/Increased Communication Range
CASS	Cluster Algorithm for Sink Selection
SWIA	stop-and-wait implicit acknowledgement
DFRF	Directed Flood-Routing Framework

iACK Implicit Acknowledgement

eACK, NACK explicit Acknowledgment

ACK acknowledgement

RTMC Reliable Transport with Memory Consideration

RBC Reliable Bursty Convergecast

ERTP Energy-efficient and Reliable Transport Protocol

LPL Low Power Listening

TRCCIT Tunable Reliability with Congestion Control for Information Transport

HACK Hybrid Acknowledgment

RMST Reliable Multi-Segment Transport

PSFQ Pump Slowly Fetch Quickly

IoT Internet of Things

UR unreliability

CASS-C Reliable data delivery using AP routing to current sink

CASS-A Reliable data delivery using AP routing to any sink

CASS-C-ICR Reliable data delivery using AP routing to current sink with ICR

CASS-A-ICR Reliable data delivery using AP routing to any sink with ICR

CASS-C-HS Reliable data delivery with hotspot nodes using AP routing to current sink

CASS-A-HS Reliable data delivery and hotspot nodes using AP routing to any sink

CASS-C-HS-ICR Reliable data delivery with hotspot nodes using AP routing to current sink with ICR

CASS-A-HS-ICR Reliable data delivery with hotspot nodes using AP routing to any sink with ICR

CASS-C-HS-Relay-Sink Reliable data delivery with hotspot nodes using AP routing to current sink, rerouting from Intermediate or relay node to Sink

CASS-A-HS-Relay-Sink Reliable data delivery and hotspot nodes using AP routing to any sink, rerouting from Intermediate or relay node to Sink

CASS-C-HS-ICR-Relay-Sink Reliable data delivery with hotspot nodes using AP routing to current sink with ICR, rerouting from Intermediate or relay node to Sink

CASS-A-HS-ICR-Relay-Sink Reliable data delivery with hotspot nodes using AP routing to any sink with ICR, rerouting from Intermediate or relay node to Sink

BER Bit error rate

CN compromised node

CL compromised link

MCU microcontroller unit

SNR Signal-to-Noise Ratio

BER Bit Error Rate

D-S Dempster–Shaffer's

RFSN Reputation-based Framework for Sensor Networks

TERP Trust and Energy-aware Routing protocol

MAC Message Authentication Code

CHAPTER 1

Introduction

A WSN is spatially distributed over a region by randomly deploying dedicated sensors to monitor the physical conditions such as temperature, humidity, pressure, vibration, and motion. A sensor works based on the battery energy and communicates with other nodes with limited wireless communication media such as radio transceivers, infrared, and optical media [1]. The sensed data is transmitted as data packets to the central control (also called base station or sink, which we refer to as Sink throughout the writing). A sensor node could behave both as a data originator and data router due to its limited communication range. An end user collects the data received by the sink node for analysis and depending on that makes application-specific decisions.In the context of an event monitoring application, sensors play a crucial role by transmitting data to designated sink nodes upon detecting specific events of interest. The sink node, equipped with a continuous power source, serves a multifaceted purpose. It establishes communication with end-users through diverse channels, including direct connections, the Internet, satellite, or organization-established secure wireless links. This enables the organization to actively monitor the sink, facilitating the sending of tasks, examination of gathered data, and assessment of the overall network status.

WSN is mainly used to collect the data from a remote region where a human can't reach to deploy or to maintain or to collect the data after deployment. In such cases, a typical way of deploying the sensor nodes is to drop them using an airplane [2]. Once these sensors reach the region, they are for the most part self-sustaining. The sensor nodes within the network carry out fundamental tasks, operating within the constraints of a finite power source and a limited communication radio range. Upon collecting data, a sensor transmits

this information back to the sink for processing. Depending on the communication range, a sensor either can reach the sink by a single-hop or use a multi-hop to deliver the sensed data to the sink [3, 4]. Every sensor node broadcasts a Hello message to the nodes in the network. Using these control messages, every sensor will come to know the neighbor nodes of itself. Similarly, a sink node floods a control message to all the sensor nodes in the network to identify the possible route information to reach a sensor node in a bi-directional way. All this network setup should be done before a sensor sends its first sensed data. This makes a WSN self-organized without human intervention.

Every sensor sends the sensed data to the sink either periodic or non-periodic based on the requirement mentioned by the end user. Similarly, data transmission is defined as either delivering all data packets for analysis or sending enough data to identify an event. This will continue till the last sensor node dies making the network non-functional. A NL of a WSN can be defined as the number of messages transmitted to sink till the last node exhausts its energy or the first node starts exhausting its complete energy. Any sensor node should notify the base station or sink before it gets depleting to make the network more fault-tolerant. This notification mechanism helps the network to re-organize the network for non-interrupted data delivery and also ensures reliability in delivering a message irrespective of fault node (dead nodes).

1.1 Application of WSN

WSNs have garnered considerable attention in various real-time applications owing to their adaptability and ability to address diverse challenges across different domains. Their self-organization capability allows them to resist dynamic changes, making them suitable for applications such as military operations, environmental monitoring, and structural health monitoring [1, 2, 5, 6, 7, 8, 9, 10, 11].

In military applications, WSNs play a crucial role in command, control, communications,

computing, intelligence, battlefield surveillance, reconnaissance, and targeting systems.

In area monitoring, sensor nodes are strategically deployed across a region to monitor specific phenomena. Upon detecting the monitored event (e.g., heat, pressure), the sensors report the information to base stations, which then take appropriate actions.

Transportation benefits from WSNs by collecting real-time traffic information for transportation models and providing drivers with alerts about congestion and traffic issues.

In health applications, WSNs contribute to interfaces for the disabled, integrated patient monitoring, diagnostics, drug administration in hospitals, telemonitoring of human physiological data, and tracking and monitoring doctors or patients within a hospital setting.

Environmental Sensor Networks cover a broad range of applications in earth science research, including monitoring volcanoes, oceans, glaciers, forests, etc. Specific areas include air pollution monitoring, forest fire detection, greenhouse monitoring, landslide detection, and more.

In structural monitoring, WSNs are employed to monitor movements within buildings and infrastructure, such as bridges, flyovers, embankments, and tunnels. This capability allows engineering practices to remotely monitor assets without the need for costly site visits.

Industrial monitoring benefits from WSNs in machinery condition-based maintenance (CBM)condition-based maintenance (CBM), offering significant cost savings and enabling new functionalities compared to traditional wired systems, where sensor installations are often limited by wiring costs.

In the agricultural sector, wireless networks relieve farmers from the maintenance of wiring in challenging environments. Automation in irrigation, facilitated by WSNs, leads to more efficient water use and reduced waste.

1.2 Challenges in WSN

Deploying sensor networks presents numerous challenges, encompassing those encountered in wireless ad hoc networks. Within sensor networks, nodes communicate through wireless and struggle with connection loss, devoid of a fixed infrastructure. A distinct challenge lies in the limited, often non-renewable energy supply of sensor nodes. To optimize the network's lifespan, protocols must be meticulously crafted with the primary goal of efficiently managing energy resources from the outset [1, 11]. The design issues of WSNs are extensively examined in the literature, as evidenced by studies such as [1, 11, 12, 13, 14]. Additionally, various simulation and testing platforms for routing protocols in WSNs are explored in works like [11, 15]. Delving into the individual design issues will provide a more in-depth understanding of the intricacies involved.

Fault Tolerance: Sensor nodes, often deployed in hazardous environments, face vulnerabilities leading to failures caused by hardware issues, physical damage, or energy depletion. Node failures in sensor networks are expected to surpass those in wired or infrastructure-based wireless networks. Effective protocols must swiftly detect failures, demonstrating robustness in managing a substantial number of failures while sustaining overall network functionality. This is particularly critical in routing protocol design, which must ensure the availability of alternate paths for packet rerouting to address diverse fault tolerance requirements in different deployment environments.

Scalability: Sensor networks exhibit varying scales, ranging from a few nodes to potentially several hundred thousand, with deployment density fluctuating accordingly. High-resolution data collection scenarios may result in node densities where a single node has thousands of neighbors within its transmission range. Protocols in sensor networks must exhibit scalability to accommodate these varying levels, maintaining optimal performance as the network size and density fluctuate.

Production Costs: In various deployment models where sensor nodes are treated as

disposable devices, the competitiveness of sensor networks against traditional information-gathering methods hinges on the ability to produce individual sensor nodes at an exceptionally low cost. Ideally, the envisioned price for a sensor node should be below $1, emphasizing the importance of cost-effective design and manufacturing processes.

Hardware Constraints: Each sensor node must possess a sensing unit, processing unit, transmission unit, and power supply at a minimum. Additional functionalities, such as built-in sensors or localization systems, introduce extra costs, increased power consumption, and larger physical size. Striking a balance between additional functionality, cost, and low-power requirements is crucial in hardware design for sensor nodes.

Sensor Network Topology: While WSNs have evolved, they remain constrained in terms of energy, computing power, memory, and communication capabilities. Energy consumption is particularly crucial, leading to the development of numerous algorithms, techniques, and protocols to save energy and extend the network's lifespan. Topology maintenance is a key focus in research to reduce energy consumption in WSNs.

Transmission Media: Communication between sensor nodes typically employs radio communication in the ISM bands. However, some sensor networks use optical or infrared communication, with the latter offering advantages such as robustness and virtually interference-free operation.

Power Consumption: Challenges in sensor networks revolve around limited power resources, where node size dictates battery capacity. Careful consideration of efficient energy use in software and hardware design is necessary. For instance, data compression may reduce the energy used for radio transmission but introduce additional energy consumption for computation and/or filtering. Energy policies vary based on applications, with some allowing the turning off of a subset of nodes to conserve energy, while others require all nodes to operate simultaneously.

Reliable Data Delivery: In WSNs, where all sensor nodes forward data towards the sink, congestion around the sink is a concern. Packet loss can occur due to congestion,

transmission errors, collisions, interference, node failure, or other unforeseeable reasons such as unable to meet the processing demands due to the limited memory, communication range, and battery power. This limitation results in delays and packet drops within the network making the sensor node as Unreliable. The constrained computational and memory resources of sensor nodes compromise their ability to efficiently handle the processing requirements, leading to potential disruptions, latency, and data loss in the WSN. Addressing these constraints is crucial for enhancing the overall performance and reliability of the network.

Moreover, the limited range of sensor nodes necessitates data to traverse a significant number of hops, creating numerous potential entry points for errors and contributing to packet loss. To ensure successful monitoring of the environment, it is imperative that critical data collected by sensor nodes reaches the sink reliably. This entails the need to recover lost data. Given the inherently error-prone nature of wireless links, ensuring a dependable transfer of data from resource-constrained sensor nodes to the sink remains a significant challenge in the realm of WSNs [16].

1.3 Motivation

With the limited resources of a sensor node and the impracticality of replacing or recharging the batteries, there is a need to build energy-efficient communication protocols to extend the NL while minimizing the communication cost. By deploying sensors in regions where humans cannot reach and also in harsh weather conditions, the protocols must ensure reliable data delivery with unpredictable behavior of nodes due to the network topology and limited resources such as communication channels, small memory, and buffer size. The end user demands data integrity in real-time applications such as battlefield monitoring. As the sensor nodes are often susceptible to tampering, trust mechanisms are needed to ensure data confidentiality in the presence of rouge nodes. The proposed methods should be scalable to support the real-time environment and applications in terms of lifetime, reliability, and data

security. These are the most expected things from the end user's perspective in real-time applications.

1.4 Objectives of the Thesis

General Objective: Enhancing a NL and reliable communication of a WSN in the presence of compromised nodes.

Specific Objectives:

- To enhance the NL in terms of the total number of messages delivered to the sinks by deploying multiple sinks while reducing the maintenance cost
- To enhance the NL while dealing with hot spot sensor nodes
- To delay the early energy depletion of hot spot nodes to make the network more functional
- To enhance the NL using an adjustable communication range
- To ensure reliable data delivery in the presence of UnReliable Nodes (URNodes) with different percentages of unreliability
- To enhance the NL of a WSN with reliable data delivery in the presence of URNodes
- To find the compromised nodes in a WSN using a trust mechanism
- To optimize the NL with trusted nodes and mechanisms to identify both compromised links and compromised nodes

1.5 Background

1.5.1 Energy consumption issues in WSN

The longevity of a sensor network is predominantly determined by its energy consumption, given that sensor nodes are typically battery-operated. Optimizing energy usage in sensor networks is a complex task, as it involves not only reducing energy consumption but also extending the overall network lifespan. Achieving optimization requires a comprehensive integration of energy awareness into the design and operation aspects at every level, encompassing individual nodes, groups of communicating nodes, and the entire network as a whole [2, 11].

A typical sensor node comprises four subsystems [2, 11]:

- Computing subsystem: This includes a microprocessor microcontroller unit (MCU) responsible for sensor control and communication protocol implementation. MCUs operate under various power management modes, and their energy consumption levels in each mode must be carefully considered for assessing battery life.

- Communication subsystem: Featuring a short-range radio for communication with neighboring nodes and the external environment. Proper power management involves completely shutting down the radio when not transmitting or receiving, rather than placing it in Idle mode, to conserve power.

- Sensing subsystem: Comprising sensors, actuators, and connections to the external world. Energy consumption can be minimized by using low-power components and optimizing power usage without compromising performance unnecessarily.

- Power supply subsystem: Involving a battery that supplies power to the node. Managing the amount of power drawn from the battery is crucial to extending its lifespan.

Lowering current draw or implementing intermittent power shutdowns can significantly enhance battery life.

Various protocols and algorithms worldwide have been explored to minimize the overall energy consumption of sensor networks. Designing an energy-aware operating system, application layer, and network protocols is pivotal in substantially increasing the lifetime of a sensor network. These protocols and algorithms need to consider the hardware specifics and leverage special features of microprocessors and transceivers to minimize energy consumption at the sensor node level. This may lead to customized solutions for different sensor node designs, resulting in diverse collaborative algorithms within the WSN domain based on the types of deployed sensor nodes.

1.5.2 Energy consumption issues in WSN

Various techniques for maximizing NL are documented in the literature. Each technique may adopt a distinct NL definition and objective function, with variations based on the application, specific objectives, and the considered network topology. Key techniques for improving NL in WSNs include sleep-wake scheduling, routing, clustering, the mobility of relays and sinks, optimization of coverage and connectivity, optimal deployment, data gathering, network coding, and data correlation [17].

In the realm of WSNs, employing sleep-wake mode-based scheduling proves highly advantageous for extending the NL, particularly in scenarios where packets arrive sporadically. Researchers have developed various optimal solutions and algorithms to maximize NL while addressing specific constraints and objectives. [18**?**] applies a sleep-wake mode scheduling for packet-forwarding to nearest base station with packet delay constraint, [19] used back bone scheduling for balancing energy dissipation, [20] ensuring throughput and Signal-to-Interference-plus-Noise- Ratio (SINR), [21] considers coverage, clustering and routing as constraints.

Routing decisions are crucial for achieving NL. Constructing lifetime-aware routes is essential for NL maximization, utilizing dynamic routes created by sensors with maximum residual battery charge. This strategy, employed during transmissions from Source Node (SN) to Destination Node (DN), balances overall Energy Dissipation (ED) and extends NL. Balancing traffic routing across the WSN is necessary to prevent rapid depletion of specific sensors' batteries, directly impacting NL. Optimizing routes is pivotal, offering the potential to exploit the remaining active sensors' battery energy and further extend NL.

[22, 23] used opportunistic routing with sleep-wake scheduling to enhance the NL and compared with conventional optimal routing showing 29% and 284% enhancement respectively. [24**?**] proposes a cross-layer approach by a sleep-wake scheduling with MAC layer routing by adjusting network traffic and reducing power dissipation through sleep scheduling. [25] designed a conservative method with a sensor on-off scheduling scheme for specific sensor activation only when necessary.

1.5.3 Reliable data delivery in WSNs

The traffic dynamics in Wireless Sensor Networks (WSNs) create congestion around the sink, as all sensor nodes forward their sensed data in that direction. This congestion, combined with transmission errors, packet collisions, interference, node failures (due to energy depletion), and other unforeseen factors, leads to packet loss. Additionally, the limited range of sensor nodes necessitates data to traverse numerous hops, introducing multiple points for potential errors and packet loss. Ensuring the reliable delivery of critical data from resource-constrained sensor nodes to the sink is essential for successful environmental monitoring. Overcoming the challenges posed by error-prone wireless links remains a significant concern in the field of WSNs, as highlighted by Mahmood et al. (2015) [16].

1.5.4 Security issues in WSNs

Security considerations in sensor networks are contingent upon identifying the assets requiring protection. In the works of [11, 26], four fundamental security goals for sensor networks are elucidated: Confidentiality, Integrity, Authentication, and Availability. An additional security goal freshness is introduced in [11, 27]. Confidentiality ensures that messages remain hidden from passive attackers, safeguarding communication privacy within sensor networks. Integrity guarantees that messages remain untampered during transmission over the network. Authentication verifies the origin of messages, ensuring their reliability. Availability assesses whether nodes can utilize resources and if the network is accessible for message transmission. An additional requirement, Freshness, ensures that the receiver receives recent and untampered data, crucial in scenarios involving shared keys, where stale data could be exploited in replay attacks during key refreshing and propagation [11, 28]. Incorporating timestamps in data packets is a mechanism to achieve freshness.

Building on these foundational security goals, potential security attacks in sensor networks are identified in [11, 29]. Routing loop attacks target information exchanged between nodes, generating false error messages that alter and replay routing information, influencing network traffic and node-to-node latency. Selective forwarding attacks involve malicious nodes dropping specific messages instead of forwarding all, deceiving neighboring nodes about shorter routes and retaining energy levels. Sinkhole attacks attract traffic to compromised nodes, potentially positioned closer to the base station, making them susceptible due to the centralized traffic flow in sensor networks. Sybil attacks involve nodes creating multiple illegitimate identities, impacting routing algorithms and topology maintenance. Geographic routing is exploited in Sybil attacks, where a node appears simultaneously in multiple locations. Wormhole attacks, occurring closer to the base station, disrupt traffic by tunneling messages over a low-latency link and creating a sinkhole. Hello flood attacks use broadcasted messages with stronger transmission power, posing as base station messages,

leading nodes to waste energy in responding. Denial-of-service (DoS) attacks manifest in physical-level disruptions such as radio jamming, network protocol interference, and battery exhaustion. A specific form of DoS attack, targeting a sensor node's power supply, is explored in [11, 30], capable of drastically reducing sensor lifetime and causing severe network impacts.

1.6 WSN NL enhancement using multiple sinks

Energy efficiency plays a crucial role in the functionality of WSNs. Implementing appropriate techniques can enhance the network's overall data throughput while simultaneously reducing operational costs. Efficiently managing the lifespan of sensor nodes in a WSN is a significant challenge, particularly for nodes in close proximity to the sink node. These nodes tend to expend more energy due to the higher volume of messages they transmit, primarily for routing purposes, compared to other nodes in the network.

This energy imbalance results in a shortened lifespan for these sensor nodes, creating dead spots within the network. Dead spots, in turn, can lead to the sink node becoming isolated from various parts of the network, particularly when the dying node lacks viable backups for reconnection. To address these challenges in WSNs, a solution involves the deployment of multiple sink nodes across the sensor field. This approach aims to extend the network's utilization to its maximum capacity, even as sensor nodes experience energy depletion, interference from nearby objects, or mechanical failures.

Introducing multiple sink nodes allows for seamless switching between them, enabling the network to adapt as sensor nodes experience energy depletion or other issues. This dynamic switching ensures optimal network coverage, especially when the initial sink node becomes non-viable or cannot efficiently service the network.

Cluster Algorithm for Sink Selection (CASS) is a technique to extend the life of the network. Sink switching can happen in three ways.

1. which the sink node if network coverage drops below the defined shift rate (say 85%).

2. Optimize the network by consistently selecting the sink node with a good network reach.

3. Determine the optimal network utilization by combining the highest percentage of coverage with areas of highest node density.

1.6.1 Sink node setup

The central point of the network, the sink node, plays a pivotal role in data gathering. Its responsibility is to establish a network infrastructure where sensor nodes can create routes and links to efficiently transmit data back to the sink.

The sink initiates this process by flooding the network with a setup message. This message is propagated to each sensor node within the network. Upon receiving the setup message, each node contacts the sink, providing information about the path the setup message took to reach them. Through this process, the sink node establishes a tree structure with itself as the root, effectively knowing how to communicate with every node within range of at least one other node capable of reaching the sink (see Figure 1.1).

Subsequently, the sink node assumes the role of data aggregator, conducting any necessary calculations and forwarding the data to designated contacts, whether within an organization or globally via its Internet connection. In the event of a sensor node's demise, the sink is notified beforehand and updates the network tree, eliminating any branches that are no longer viable. If a replacement node is chosen by the active sensors surrounding the failing node, the new node sends its ID as a replacement, and the sink reinstates the removed branches, attaching them to the new sensor node.

To address potential network losses, if a certain percentage of the network remains unrecovered within a specified number of cycles, the sink node initiates a test to determine if it meets the shift sink network life ratio. If this ratio is not met, the sink continues

its operations until the criteria are fulfilled. Upon reaching the designated ratio, the sink implements CASS. Following the execution of CASS, the sink evaluates the maximum network reach as a criterion to decide whether to shift to another sink or remain with the current one.

1.6.2 Cluster Algorithm for Sink Selection (CASS)

The CASS algorithm, designed to select the sink node offering the maximum exposure to significant portions of the network, operates in three key steps, focusing on clusters of sensor nodes, each containing a minimum of three nodes. The initial step involves determining clusters using the tree view generated by the sink during the setup phase (Figure 1.1). As CASS traverses down the tree, it identifies parents with at least two children (Figure 1.2).

In the second step, the algorithm consolidates clusters whose parent is a child of another cluster, merging them into a single entity 1.3). The third step evaluates whether a cluster has sufficient access to another cluster, defined by having at least two pathways or links to another cluster 1.5). A pathway is established if a cluster contains a sensor with a child, neighbor, or parent in the comparing branch of the tree, qualifying as one pathway. If a cluster has two pathways, they are combined into one cluster (Figure **??**).

Once clusters are established, the algorithm calculates the reach of each cluster by assigning a weight based on its size. This weight guides sink selection toward larger clusters, which offer better re-routing capabilities and fewer sink shifts in the long run. Additionally, the algorithm considers the number of children a particular sink has, using it as a smaller weighted value. This accounts for the potential access to various parts of the network without necessitating a sink shift. Finally, sensors not included in any cluster contribute as a single point to the reach total. The sink with the highest reach total becomes the next active sink for the network.

Network Reach:

I = current sink

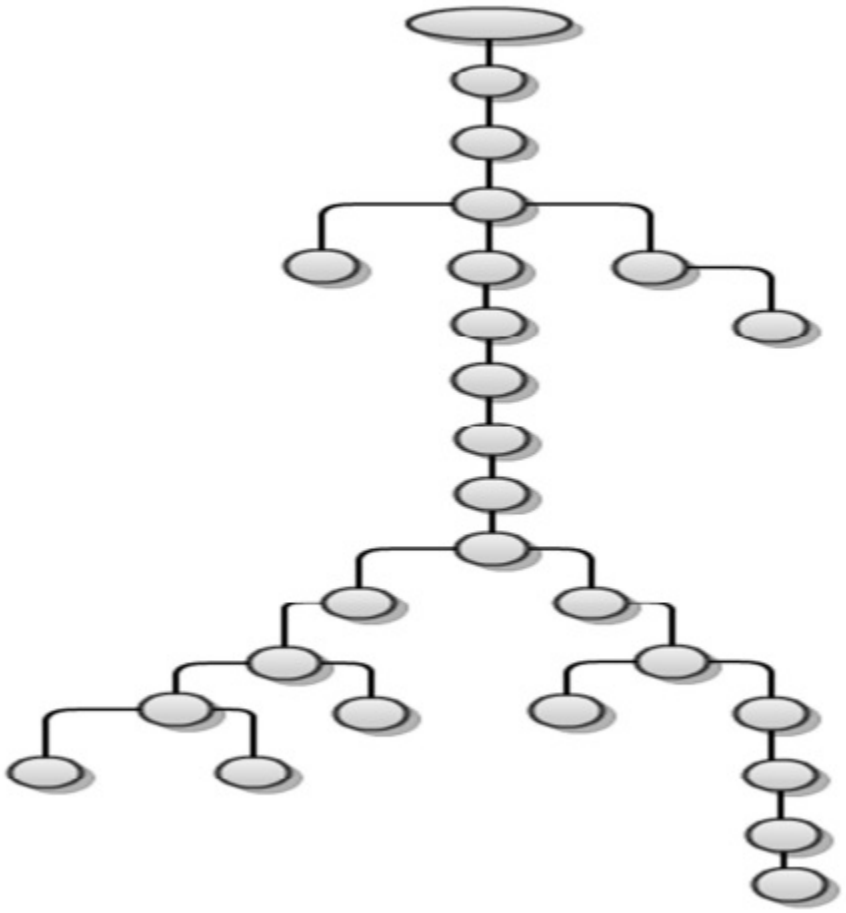

Figure 1.1: Sink setup phase

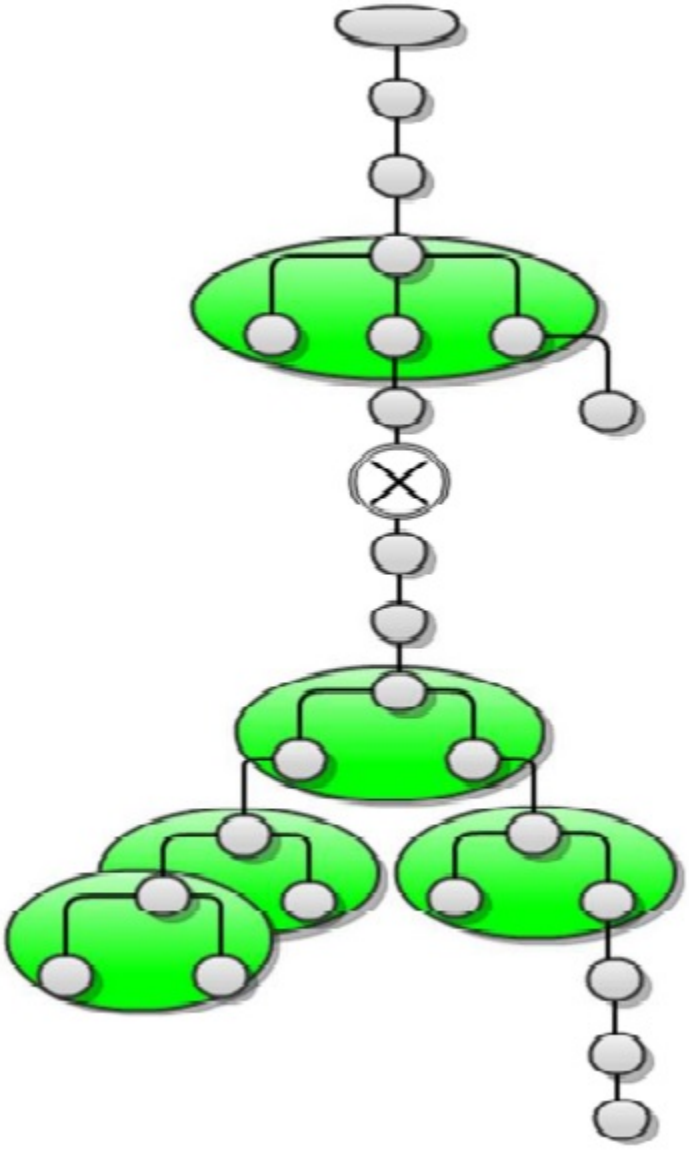

Figure 1.2: Cluster formation phase- step1

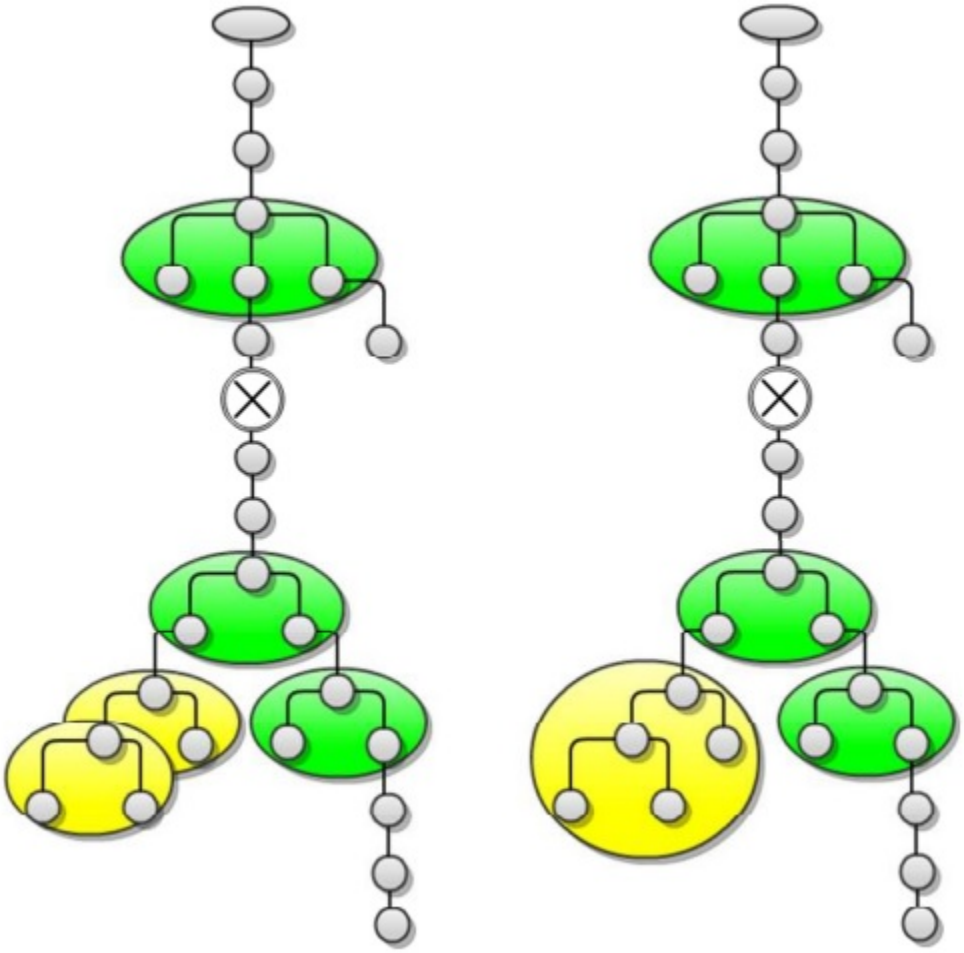

Figure 1.3: Cluster formation phase- step2

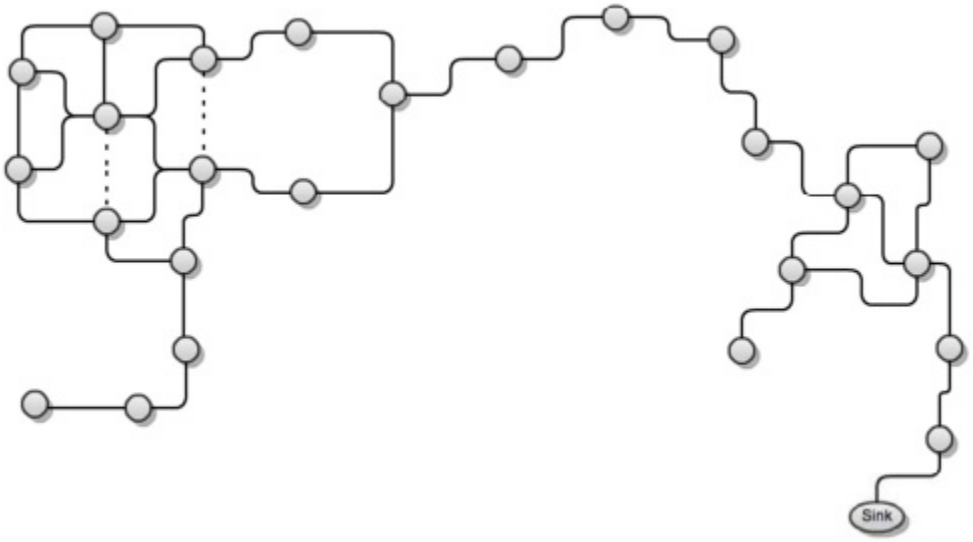

Figure 1.4: Top view of a WSN

CR(I) = No. of nodes contained in clusters reachable by I

CN(I) = No. of child nodes of I

SN(I) = No. of single nodes (not in a cluster) reachable by I

Formula:

$$NetworkReach = CR(I) * 1.33 + CN(I) * 1.2 + SN(I)$$

Example:

Sink 1 will yield a reach value of 4*1.33 + 1*1.2 + 4 = 10.52

Sink 2 will yield a reach value of 8*1.33 + 3*1.33 + 1*1.2 + 5 = 20.83

Sink 2 can be of any single node on the lower half of the network view (Figure 1.4).

Throughout the thesis, CASS algorithm is used to select a new sink based on the network reach of all the sinks when the current sink reaches the defined shift rate. Mainly, to minimize the maintenance cost which arises due to the multiple sink deployment to enhance the WSN.

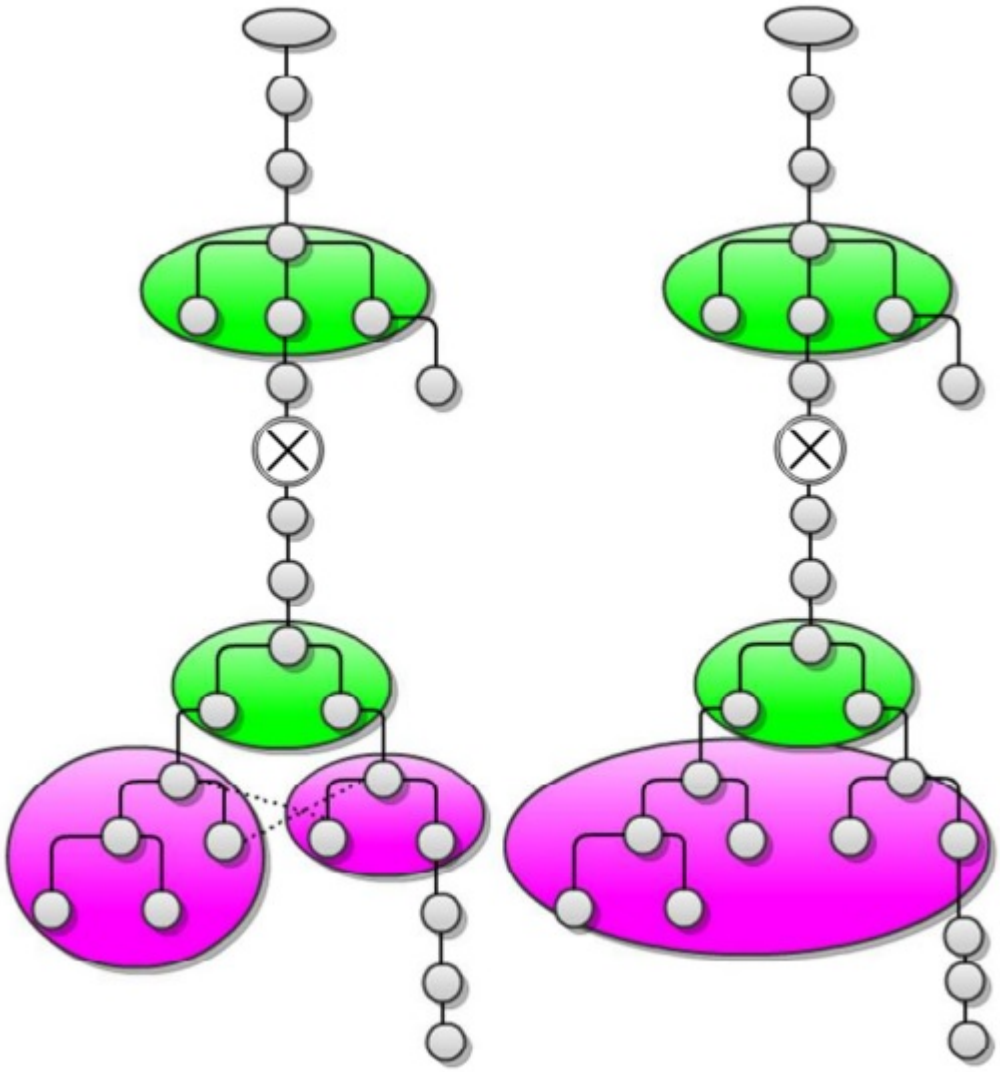

Figure 1.5: Cluster formation phase - step3

1.7 Major Research Contributions

1.7.1 Contribution 1

Maximizing the NL in a WSN for maintaining crucial events and parameters is an important research area. In the proposed work, the total number of messages delivered successfully to all sinks is the metric to measure the NL of a WSN. Deploying multiple sinks in the network handles the load-balancing of the data to prolong the NL. Deploying multiple sinks with increased sensor nodes in the target region increases the maintenance cost required to manage the sinks. This issue is handled well by the CASS algorithm in [31] by activating a single sink. CASS mainly works based on the network reach of each sink, which is calculated based on the cluster formation, size of the cluster, and reachability of an individual node to every sink.

Usually, the energy of the neighbors of the sink drains quickly, as they are often involved in data forwarding. The network becomes less functional or completely non-functional based on the energy-exhausted hot spots. Similarly, many such nodes participate recursively in data transmission in a network as a relay node is crucial to prolong the NL. Such nodes are also considered hot spot nodes. Sometimes, the neighbors of the sinks are left with residual energy to continue the network functioning, but the energy of crucial hot spot nodes gets drained, which demotes the NL. So, the hot spot nodes should be handled carefully, along with energy-efficient routing. One of the alternatives with homogeneous nodes in the network is to delay the energy exhaustion of the mentioned type of hot spot nodes, which internally improves the NL. The proposed routing algorithm is to reroute the data message using an AP approach. The main objective of the work is to enhance the NL with energy-efficient routing and delay the early depletion of the hot spot nodes' energy by selecting the shortest path among the explored routing paths.

ICR is another good alternative to increase the NL. When the network becomes non-

functional with the defined communication range, then the system will increase the communication range to establish a network with the leftover sensor nodes and its residual energy to make the WSN functional by five units every time until the node left with residual energy but unable to establish a network.

1.7.2 Contribution 2

In a WSN, difficult to predict the message drop by a sensor node during data transmission. The reasons can be deploying the sensor nodes in harsh weather conditions, congestion in a specific area, or unavailability of limited sources like memory and buffer size depending on the processing demands. The message drop can happen due to the limited resources of a sensor node such as communication channels, small memory, processing capability, and buffer size affects the reliability of data delivery. Due to this, the sensor node makes an unsuccessful forwarding leads to message dropping which affects the reliable data delivery and NL and also increases the congestion in the network by re-transmitting the data to ensure reliability. Instead of dropping a message, the system looks for an alternative mechanism with load-balancing while minimizing the traffic congestion, drop rate, with improvement in reliable data delivery and the NL of a WSN.

AP routing is modified in such a way that re-routing should not by often to deliver a single message. The AP routing algorithm should select a reliable node for rerouting with less hop count to sink and more residual energy to initiate data re-routing. To improve the reliable data delivery, the AP routing can reroute the message to an inactive sink for that instance. With this the energy of the relay nodes is saved for future operations like sensing, processing, and transmitting the data. However, the unreliable behavior caused by the internal system issues persists for a short time. It allows the node to forward the data successfully. If a node always shows unreliable behavior throughout the data transmission.

Handling the message drop by URNodes is crucial to maintain the network performance, even if the unreliability is short. ICR is another alternative to improve the reliability in

delivering data at the cost of reduced NL. ICR helps to skip the URNode by a defined number of hops to transmit the data. By ICR the energy consumption increases, with increase in communication range, which reduces the overall NL with 99% of reliable data delivery.

1.7.3 Contribution 3

Enhancing the NL while dealing with hot spot nodes in the presence of URNodes with variable percentage of unreliability (percUR) is a challenging task in a WSN. AP reroutes the messages while avoiding the hotspot nodes and URNodes. Energy exhaustion of Hot spot nodes makes the network less functional by small chunks of a WSN which reduces the connectivity to the sink from network nodes. Due to the connectivity issue, the WSN yields less amount of NL. Similarly URNodes with a probability of dropping a message within the defined percUR also reduces the NL. when a system with URNodes and unaddressed hot spot nodes issue then the NL of a WSN yields a lesser number of messages tp get delivered.

In both issues, the common thing is reduced NL due to the disconnection raised by hot spots and message drops by URNode. The sensed data packet is unable to reach the sink because the data packets were unable to avoid the hotspot nodes and URNode. AP is an algorithm that looks at finding an optimal alternate path that can avoid both hot spots and URNodes. Delaying the premature death of hot spots by rerouting and avoiding the URNode when it is dropping a message by looking at alternate path gives a feasible improvement in enhancing the NL.

When dealing with hot spots nodes AP should look at an alternate path with a high residual energy node as the next hop node. When dealing with URNode the AP make sure to minimize the frequent re-routing before the message reaches the sink. In both cases, AP should act according to the issue addressed at that instance.

1.7.4 Contribution 4

Based on the application, WSN with sensor nodes deployed in the target region is difficult to access or attend the deployed area or sensor. It leads to security attacks by tampering with the node and making it behave in a way that compromises its regular duties, such as dropping messages during data transmission and tampering with the privacy and confidentiality of the sending data. Maintaining confidentiality and data integrity is more important in real-time applications such as battlefield monitoring, health care, electrical grids, air and water quality monitoring, industrial automation, traffic monitoring, etc. The existence of a tampered or a CN in a WSN has significant risks such as data integrity and trustworthiness, manipulating routing information which misleads the routing decisions, denial of service (disturbing the normal functioning by overloading the network with malicious traffic which leads to message drop), by engaging the nodes in activities that results in excessive energy consumption leading to premature depletion of the node's energy, eavesdropping.

Identifying a CN in a WSN is challenging while differentiating the message drop by a rouge node from a message drop of temporary URNode. Measuring the trust between two nodes helps the system identify the rough nodes. Measuring the trust between two nodes can be either by direct interaction or based on recommendations received from the neighbor nodes which are referred to as direct and indirect trust. Indirect helps identify the actual rouge nodes based on the indirect trust value and the with percUR. Identification and detaching the CN from a WSN greatly enhances the NL, and ensures reliable data delivery. Using the trust mechanism in dealing with security attacks with reliable data delivery promises an improved NL.

1.7.5 Thesis Organization

The rest of the thesis organization is as follows. In Chapter 2, the research delves into the enhancement of NL through the deployment of multiple sinks, addressing hot spots using AP routing, and ICR. Chapter 3 shifts focus to reliable data delivery, emphasizing in NL improvement in WSN amidst the presence of unreliable nodes URNodes with varying percentages of accuracy percUR. Additionally, Chapter 4 concentrates on mitigating hot spots, ensuring reliability and extending NL in the presence of URNodes. Chapter 5 explores a trust mechanism to detect compromised nodes and links in a WSN, contributing to both reliability and prolonged NL. The thesis conclusion and future scope are discussed in Chapter 6.

CHAPTER 2

Lifetime enhancement using Optimal Alternate Path routing and Increasing Communication Range

2.1 Introduction

A WSN is a special wireless network comprising numerous tiny, energy-efficient sensor nodes equipped with sensors, microprocessors, and wireless communication capabilities. These nodes collaboratively collect, process, and transmit data from their surrounding environment, forming a self-organizing wireless infrastructure. WSNs are utilized in diverse applications, such as environmental monitoring, industrial automation, healthcare, and more, where they enable real-time data acquisition and contribute to the Internet of Things (IoT) by providing valuable insights for decision-making and control purposes [1].

In a WSN, the small sensor nodes function as both data generators and relay nodes within the network. Each node comprises sensors, a microprocessor, and a transceiver. These nodes leverage a diverse range of sensors for seamless integration, enabling the capture of data from various physical phenomena.Equipped with onboard microprocessors, sensor nodes in this system can perform complex tasks beyond the transmission of observed data. The transceiver enables wireless communication related to the observed phenomena. Although these sensor nodes are typically stationary, powered by batteries of limited

capacity, the network topology experiences dynamic changes due to power management. To conserve energy, nodes frequently disable their transceivers, temporarily disconnecting from the network. Navigating this dynamic environment presents a significant challenge in maintaining connectivity while minimizing energy consumption. Despite this challenge, the energy-efficient operations of WSNs result in notably long lifetimes, surpassing systems relying on conventional batteries, as emphasized by [32].

Sensor nodes primarily employ radio frequency for communication among themselves. However, the reach of radio frequency signals is constrained. In situations where the network encompasses a substantial area, a single hop might be insufficient for all sensor nodes to directly transmit data to the sink. Applications like battlefield surveillance, animal monitoring, noise level measurement, vehicle tracking, environmental monitoring, weather reporting, and habitat monitoring require coverage over extensive regions [33, 34, 35]. In such scenarios, the limited range of a radio signal impedes sensor nodes from reaching the sink in a single hop. Consequently, each sensor node relies on its neighboring nodes to relay data to the sink. This iterative process continues until the transmitted message successfully reaches the sink, constituting a mechanism known as multi-hop routing.

Sensor node energy will be consumed more in communication rather than sensing and processing the data [33]. To deliver a message, along with the node that initiated data transmission, the relay nodes are also involved in delivering the data by forwarding it. So, for the sensed data to be delivered, many nodes contribute their energy in delivering the data message/packet to the sink. In sensitive applications such as battlefield applications, underwater applications, volcanic eruption, and many other applications where the human can't reach the sensor to recharge the battery or replace the sensor. As mentioned earlier sensor is an energy-constrained device, and the optimal usage of the sensor energy is very important to make the network functional for a longer period. Efficient energy management is a primary concern in WSNs due to the limited power resources of sensor nodes.

In delivering the data message to the sink, the neighbors of the sink nodes play a major

role as relay nodes. Without the neighbor nodes of the sink, no sensor be able to deliver the sensed data alone with the limited communication range. The neighbors of the sink can be addressed as hot spots of the network. Along with the neighbors of the sinks, a few other nodes will play a major role in transmitting the data from one end to the sink. Without such nodes, even if the sink neighbors are alive the sent message can't be delivered to the sink. Such bridge nodes are as important as sink neighbors and are also considered hot spots of the network as they play a vital role in data forwarding. Once such bridge hot spot energy is exhausted the network becomes isolated chunks though the nodes have a good amount of residual energy. Slowly the network system becomes less functional and ends as non-functional [31, 33]. Over ninety percent (90%) of the energy of the whole network remains unutilized if the lifetime of the network is dropped out due to the hot spot issues [36]. To enhance the functioning of the network, along with routing optimization, keeping the hot spots and bridge nodes without draining the energy is more important while utilizing the available resources. By the time the network completely turns non-functional, many of the nodes are left with a considerable amount of residual energy which turns out to be unused forever.

In such situations, by adjusting the communication range of the sensors, the network can turn into functional which increases the network lifetime in terms of packet delivery ratio. Paying more energy to deliver the message on a non-functional network won't be a waste of energy.

2.2 Literature survey

In the past years, significant research efforts have been dedicated to enhancing the network lifetime of wireless sensor networks. Various strategies have been explored, such as deploying multiple sinks, dividing the network into clusters with efficient routing mechanisms, strategically positioning sinks for optimal data collection, and fine-tuning energy

consumption through scheduling during data transmission. Additionally, aggregating data before forwarding it to the sink and using mobile sinks for data collection have been investigated. Each of these approaches aims to extend the network lifetime, employing distinct methods tailored to minimize energy consumption, balance communication loads, and ultimately ensure a prolonged and sustainable operational lifespan for the network. Through innovative and multifaceted approaches, researchers strive to address the unique challenges of energy management and data handling in wireless sensor networks, contributing to a more efficient and enduring network infrastructure.

Minimizing the hop count is a promising and convincing alternative to optimize energy consumption in wireless sensor networks, ultimately enhancing network efficiency and longevity. By reducing the number of hops required for data transmission, we can alleviate the energy burden on relay nodes, thereby mitigating the risk of energy depletion in hot spots and extending the overall network lifespan.

There are various approaches to achieving hop count minimization, and one effective method is through optimal routing [33]. By carefully planning the paths that data takes from sensor nodes to sinks, we can ensure the shortest possible hop count, thus minimizing energy expenditure at each relay point.

Another promising strategy involves deploying multiple sinks [33] strategically throughout the network. This approach allows sensed data to reach a sink with fewer intermediate relay nodes, optimizing the hop count. When multiple sinks are deployed, sensor nodes have the flexibility to send messages to their nearest sink, further reducing the hops needed to reach a sink and conserve energy.

Moreover, deploying multiple sinks offers an additional advantage: in the event that the neighboring sink is inaccessible due to node failure or energy depletion, a sensor node can redirect its data to the next nearest sink, however with a slightly increased hop count. This dynamic adaptation enables efficient energy utilization across the network, ensuring reliable data transmission even when certain areas experience node failures.

The interconnected nature of these sinks, along with their robust external connections, guarantees seamless delivery of sensed data to the end-user. This not only optimizes energy usage but also minimizes network congestion, reducing the occurrence of message dropping due to traffic and enhancing the timeliness of packet delivery. In summary, by focusing on hop count minimization and deploying multiple sinks strategically, we can maximize energy efficiency, prolong network lifespan, and improve overall network performance.

The First Order Radio Model (FORM) is a common communication model used in wireless sensor networks (WSNs). In this model, sensors utilize a simple representation of radio communication to transmit data to other nodes in the network. However, this communication model has a limitation: if multiple sensors attempt to send data simultaneously over the same communication channel, collisions can occur. These collisions result in data loss, necessitating re-transmission of the data. The act of re-transmitting the same data multiple times consumes additional energy, which not only impacts the network's lifetime but also increases latency in data collection.

Efficient data collection is a critical objective in wireless sensor networks (WSNs). A delay in data collection can have a significant effect. In [37], a comprehensive strategy is presented to address this concern by focusing on reducing data collection latency and improving packet delivery within the WSN. This strategy encompasses two key components: an approximation algorithm and a heuristic algorithm, each with its approach to enhance data transmission efficiency. The primary objective of this approach is to minimize the time required for sensor nodes to relay their sensed data to a central data collection point, often referred to as the sink. This is achieved by deploying multiple sinks in the region.

The approximation algorithm is designed to address data collection latency, particularly in scenarios where finding an exact, optimal solution is computationally challenging or time-prohibitive. This algorithm schedules when and how sensor nodes should transmit their collected data to the sink.

Furthermore, the strategy introduces a heuristic algorithm utilizing a greedy breadth-first

search approach to facilitate data transmission. Heuristic algorithms aim to find reasonably good solutions quickly, although they do not guarantee optimality. This heuristic algorithm is tailored to the task of transmitting data from the sensor nodes to the sink.

An important aspect of this approach is the scheduling component, which is designed by analyzing network flow within various time units. This involves a thorough examination of how data moves through the network over different time intervals, enabling informed decision-making regarding when and how data should be transmitted.

Finally, the scheduling approach, informed by the study of network flow over time units, outperforms the heuristic method significantly, achieving a latency reduction of up to 60%. This suggests that the scheduling strategy based on network flow analysis is notably more effective in minimizing data collection latency compared to the heuristic method, presenting a promising solution to enhance the efficiency of data transmission within the described wireless sensor network in [37].

In [38], a strategy involving the deployment of multiple sinks is discussed to minimize the distance between the data source (sensors) and the sink, similar to the approach in a Single Sink WSN. By strategically using multiple sinks and allowing sensors to transmit data to the nearest sink, not only is energy utilization optimized, but the overall NL is also extended.

The authors propose the use of a logical graph model to create a virtual sink representation when employing multiple sinks. This virtual sink model facilitates the adaptation of existing routing and querying protocols initially designed for single sink sensor networks. This adaptation ensures efficient utilization of the multiple sink deployment.

Moreover, the authors suggest that this model can lead to substantial energy savings in a d-dimensional sensor region with randomly deployed k sinks and n sensors. The expected energy savings are believed to be proportional to $k^{\frac{1}{d}}$, indicating a promising approach to improve energy efficiency and overall network performance in wireless sensor networks with multiple sink deployments as compared to traditional single sink configurations.

In [39], the authors proposed a particle swarm optimization-based algorithm for routing and clustering to improve the network lifetime in wireless sensor networks. Their approach involves both routing and clustering algorithms designed to optimize energy consumption and prolong the network's operational life.

The routing algorithm utilizes a particle encoding scheme within a multi-objective optimization framework. The objective function aims to minimize both the number of hops and the distance between cluster heads, which have an inverse relationship. Reducing the distance between cluster heads increases the number of hops to reach the sink, and vice versa. To resolve this inherent conflict, the authors employ a weighted sum approach.

Additionally, the clustering algorithm emphasizes energy conservation through load balancing to extend the network's lifetime. The authors present their findings using various metrics, including the number of rounds, mean lifetime, standard deviation, time until the first gateway node depletes its energy, and the count of inactive sensor nodes.

Cluster heads in this context are assumed to be equipped with GPS and play a critical role in data aggregation and forwarding, which are energy-intensive tasks. To address the issue of cluster head energy depletion impacting network lifetime, the authors propose equipping cluster heads with a larger communication range and more energy, effectively creating a hybrid network. Deploying multiple sinks in optimal locations is a hot spot strategy to enhance the network lifetime and overall performance of a wireless sensor network (WSN). The placement of sinks directly impacts the efficiency of data collection, energy consumption, and message delivery within the network. If sinks are placed too closely to each other, resembling a single sink scenario, it defeats the purpose of deploying multiple sinks. When neighbor nodes of a sink exhaust their energy, it can significantly impact message delivery and the network as a whole. Therefore, optimal sink placement is vital to ensure a balanced distribution of the workload and to mitigate the risk of localized energy depletion.

In addressing this concern, [40] proposed an improved sink placement strategy aimed at

reducing communication overhead, ultimately leading to a more efficient network with an extended lifetime. By optimizing sink placement, the communication distance and workload on each sink can be better managed, contributing to improved energy utilization and network longevity.

Furthermore, in [41], a mathematical global algorithm was introduced to maximize the benefits of deploying multiple sinks by identifying optimal sink deployment locations. Although this approach provides an ideal solution, it relies on complete location information of the WSN, which can be challenging to obtain in real-time applications. The authors recognized the difficulty in obtaining precise location information, especially in scenarios where sensor nodes are deployed remotely or in inaccessible locations.

To overcome this challenge, [42] proposed an alternative iterative 1-hop algorithm to find optimal sink locations based on the location of neighboring nodes and approximations for distant nodes. The one-hop algorithm produces nearly identical optimal sink locations compared to the global algorithm, taking into account sink locations and information from their neighboring nodes. Additionally, the authors suggested a 1-hop relocation algorithm to adjust sink placement when a sink becomes isolated due to neighboring node failures.

In summary, optimal sink placement is critical for network lifetime enhancement, and various strategies and algorithms have been proposed to achieve this by considering communication efficiency, energy conservation, and the dynamic nature of WSNs. These approaches strive to strike a balance between accurate sink placement and practical implementation, taking into account the challenges associated with obtaining real-time location information in large-scale, dynamic wireless sensor networks.

In [43], an improved corona (multi-layered) model is introduced to analyze sensors with adaptable transmission ranges in a WSN utilizing circular multi-hop deployment, represented as concentric coronas. The objective is to optimize the network lifetime by determining suitable transmission ranges for sensors within each corona, taking into account the specific deployment pattern.

The key insight revolves around adjusting the transmission ranges of sensors at various levels (coronas) to achieve an optimal network lifetime. Determining the optimal transmission ranges for sensors across all coronas poses a multi-objective optimization problem (MOP) recognized for its NP-hard complexity.

To tackle this challenge, the authors propose both centralized and distributed algorithms for assigning transmission ranges to sensors within each corona. These algorithms aim to optimize network lifetime under different node distribution scenarios, be it uniform or non-uniform. The centralized algorithm offers a centralized decision-making approach to determine transmission ranges, while the distributed algorithm decentralizes this process for increased efficiency and scalability.

By leveraging this corona model and the associated transmission range assignment algorithms, the study seeks to improve the operational lifespan of WSNs by strategically adjusting transmission ranges at different layers of the network, thereby enhancing energy efficiency and overall network performance.

In the study by [44], the focus is on maximizing the lifespan of a wireless sensor network through a distributed and adaptive data propagation algorithm. The algorithm aims to balance energy utilization among individual sensors while optimizing message flow throughout the network. This is achieved by allowing each sensor node to make a decision on message propagation based on its remaining energy and potential function.

The key aspect of this algorithm is the flexibility for a sensor node to choose how to propagate a message: either to one of its immediate neighbors or directly to the base station. The decision is influenced by the potential function, which takes into account the node's remaining energy. By adapting message propagation based on energy considerations, the algorithm seeks to extend the overall network lifespan.

In the context of the discussed literature, the emphasis is on maximizing network lifetime by deploying multiple sinks, and sensor nodes have the option to send data to any of the nearest sinks. This strategy is geared toward efficient energy utilization and the maximization

of network lifetime, as mentioned previously.

The challenges associated with managing multiple sinks have grown with increased complexity, particularly in synchronizing data for aggregation. Data fusion introduces latency concerns, while redundancy issues arise, leading to conflicting information from different sinks. Maintaining wake-up schedules becomes hot spot for ensuring data integrity and reliability. Additionally, the cost of providing infrastructure to support multiple sinks adds another layer of complexity to the overall data management process. These factors collectively contribute to the intricate task of navigating and optimizing the management of diverse data sources.

However, an important consideration is that, in all the cases discussed, all the sinks are assumed to be active at all times. This continuous activity of all sinks can result in increased maintenance costs. To address this, future research and practical implementations may explore strategies for optimizing sink activity, such as dynamic sink activation based on network conditions or using energy-efficient sleep and wake-up schedules for sinks to reduce operational costs while maintaining network effectiveness.

In [31], the authors proposed a strategy to reduce maintenance costs in wireless sensor networks (WSNs) by allowing only one sink to function at a time, similar to a single sink network. This concept involves shifting the active sink based on a defined shift rate, providing more efficiency in network management and cost reduction.

The determination of the new sink is grounded in calculating the network reach for each potential sink, employing the CASS. This algorithm incorporates two essential factors: the highest percentage of network coverage and regions with the highest node density within the network. By considering both coverage and node density, the aim is to optimize the utilization of the network.

In the proposed strategy, the shift of the sink occurs when a specific percentage of the network is lost due to energy depletion in hotspot nodes, such as neighbor nodes of the sink or other connecting nodes in the network. This dynamic sink shifting helps in

redistributing the load and maintaining effective communication, thus extending the overall network lifetime and reducing maintenance costs.

Overall, this approach aims to strike a balance between optimal network performance and the associated maintenance costs by intelligently managing sink shifting and reducing energy wastage in critical network nodes.

The enhancement of network lifetime is addressed in various ways across the cited papers, each proposing unique strategies to optimize energy utilization and prolong the network's operational life. These strategies encompass enabling the operation of a single sink at a time, creating logical graphs with solitary virtual sinks, coordinating data collection schedules, and strategically deploying or redeploying sinks.

However, one common theme is the importance of considering hot spot nodes, especially those acting as connecting nodes between sensors and sinks. These nodes play a vital role in relaying data from sensors to sinks or between clusters in the network. In some papers, such as [39], cluster heads are given special consideration, having more communication range and energy compared to regular sensor nodes. This strategic allocation of resources helps in extending the network lifetime by efficiently managing communication and ensuring data transmission to sinks.

Addressing these hot spot nodes is indeed crucial in designing effective strategies to maximize the network lifetime, as their energy levels and efficiency directly impact the overall network performance and longevity. Balancing and optimizing the energy usage of these connecting nodes is essential for achieving a more sustainable and efficient wireless sensor network.

Actually, mobile sinks in wireless sensor networks (WSNs) present a promising solution to minimize energy consumption, prolong network lifetime, and reduce the hot spots issue by dynamically moving to collect data. However, a major challenge associated with mobile sinks is ensuring that sensor nodes are promptly updated about the sink's new location to facilitate efficient data transmission [45].

In addressing this challenge, one common approach is flooding the new sink location to the sensor nodes [46]. Flooding involves broadcasting information about the sink's updated position to all nodes in the network. While flooding is a straightforward method to disseminate information, it increases traffic flow, potentially leading to congestion and message drops within the network.

The challenge lies in finding a balance between timely dissemination of sink location updates and minimizing the adverse effects of increased traffic and congestion. Researchers continue to explore and develop more efficient and optimized techniques to disseminate sink location information without causing excessive traffic burden. These may include more targeted or localized dissemination strategies, leveraging network structures or algorithms that can intelligently route this information to relevant nodes, or employing data-centric approaches to update nodes selectively based on data relevance.

Efficient dissemination of sink location updates is a crucial aspect of utilizing mobile sinks effectively in WSNs. Addressing this challenge ensures that the benefits of mobile sinks, such as reduced energy consumption and improved network lifetime, are realized without compromising the network's performance due to excessive traffic and congestion.

Paper [47], presents the EAERP (Evolutionary Algorithm based Energy-Efficient Routing Protocol) for forming clustered wireless sensor nodes. The primary goal of this approach is to distribute energy consumption evenly across the network to enhance its sustainability and longevity by strategically selecting Cluster Heads Cluster Head (CH)s and Non-CH sensors to join the nearby CHs to form clusters. Clustering helps in efficient data aggregation and routing within the network.

However, the paper highlights several challenges, including the possibility of CHs having insufficient energy levels to perform their assigned tasks effectively and uneven energy consumption within the network, leading to sub-optimal cluster formation and negatively impacting the network's sustainability.

This non-optimized cluster formation can result in some nodes, including CHs, depleting

their energy resources quickly, while others remain underutilized. These disparities can lead to the emergence of hot spots in the network. The method may not result in optimalCH selection and cluster formation. As a consequence, the WSN may struggle to operate efficiently for an extended duration.

Addressing these issues in cluster formation, CH selection and energy balancing is crucial for enhancing the longevity and efficiency of wireless sensor networks. Further research and improvements are needed to define the optimized cluster formation, dynamic CH selection, energy-aware routing to extend the network's lifetime, load balancing techniques to evenly distribute the data traffic among CHs and developing fault-tolerant mechanisms that can adapt to the failure of CHs or other nodes can help in maintaining the network operation even in the presence of node failures while mitigating the formation of hot-spots.

The paper [48], introduces a technique called EAUDC, which stands for Energy-Aware Unequal Data Clustering, designed to address energy efficiency in wireless sensor networks WSNs. It focuses on selecting Cluster Heads CHs unequally. The CH selection is based on the average leftover energy of the nodes in the nearby CHs and adaptive rivalry ranges which is important for optimizing the network's performance. The Energy-Aware Unequal Data Clustering (EAUDC) discusses the estimation of unequal competition ranges for CHs. These ranges are used to determine how far a CH can effectively communicate with its Base station (BS) while considering the energy constraints. The estimation of unequal competition ranges is based on two factors, namely the distance between a sensor node and the BS and residual energy level of nodes. Nodes with higher residual energy may be assigned larger competition ranges. These two factors are taken into account jointly using a weighted factor. However, the paper does not specify the criteria or method for selecting the weighted factor. The selection of this factor could significantly impact the behavior of the algorithm and network performance. Researchers implementing the EAUDC approach may need to experiment with different weight values to optimize their network's performance.

In [49], authors address the issue of energy consumption imbalance and the emergence

of hot spots in the network by designing the CHs in WSNs with unequal cluster sizes based on their distance to the sink as a key factor. The CHs that are closer to the sink have fewer member sensors, and CHs that are farther from the sink accommodate more member sensors. By allocating fewer sensors toCHs close to the sink, theseCHs are expected to consume less energy since they handle a smaller amount of data traffic and have a shorter transmission distance to the sink. Conversely,CHs farther from the sink can handle a larger number of sensors but may consume more energy due to greater data aggregation and longer transmission distances. This way the approach deals with the energy balancing across the network and prevents hot spots from forming which can lead to network instability and reduced network lifetime. By mitigating hot spots and optimizing energy consumption, this approach aims to improve the sustainability and longevity of the WSN. It helps ensure that the network can operate efficiently for a longer duration.

The work presented in [50] tackles the challenges of the hot spot problem, fault tolerance, and load balancing in an integrated approach. The proposed Grid-based Fault Tolerant Clustering and Routing Algorithms (GFTCRA) operate in a distributed manner, relying solely on local information. This approach effectively addresses routing issues without the need for re-clustering when a Cluster Head (CH) becomes inactive.

Addressing the hot-spot problem in WSN is crucial, where nodes close to the sink experience faster energy depletion due to increased communication, potentially leading to network isolation. In [51] paper proposes a solution by employing an integrated MAC and routing protocol that organizes the network into tiers. Additionally, a quantification algorithm is introduced to determine the optimal number of nodes in each tier, effectively mitigating the hot-spot problem and enhancing the overall network lifetime. Although the proposed solution involves a trade-off between the number of sensor nodes in each tier and the overall WSN lifetime, the decreasing cost of sensor nodes makes this trade-off more feasible.

To mitigate the formation of energy holes in a sensor network, a strategic deployment

strategy involves allowing a non-uniform distribution of sensor nodes by incrementally increasing their density around the base station. This approach prevents accelerated energy depletion in proximity to the base station and effectively addresses the energy hole problem. Alternatively, if sensor nodes are equipped with adjustable transmission power, such as employing a shorter range for nodes near the base station and a longer range for those farther away, the occurrence of energy holes can also be minimized, as suggested in [52].

The algorithm proposed in [52] introduces a Dynamic Transmission Range Adjustment (DTA) mechanism, enabling sensor nodes to adapt their transmission range based on their residual energy, thereby promoting balanced energy consumption. The network's operation is organized into rounds, during which sensor nodes employ the DTA algorithm to dynamically adjust their transmission range according to their remaining energy levels, effectively distributing energy consumption more evenly across all nodes.

In [53], the authors demonstrated that uniform and homogeneous deployment of nodes in a network inevitably leads to uneven energy consumption. To address this, they introduced a nonuniform node density approach, deploying more nodes in areas with higher energy consumption. The proposed strategy aims for nearly balanced energy depletion by increasing the number of nodes in geometric progression from outer coronas to inner ones, excluding the outermost corona, in a circular multi-hop Wireless Sensor Network (WSN). This approach involves dividing the sensor field into concentric coronas or rings around the sink, coupled with q-Switch Routing.

Similarly, in [54], the authors explored nonuniform node distribution, focusing on energy consumption in data transmission and asserting the possibility of achieving balanced energy depletion. Introducing more nodes in the sensor field offers advantages such as improved connectivity and higher reliability. However, this comes at a cost, and [55] follows a similar strategy. Nevertheless, an excess of nodes introduces challenges such as wireless interference, data conflicts, and redundancy, as highlighted in the literature.

Adjusting communication distances based on node proximity to the sink is a practical

strategy to manage energy consumption. In [52], a dynamic algorithm is introduced, allowing sensor nodes to vary their transmission range according to residual energy and distance to the sink. A similar approach is employed in [56], particularly suitable for small networks.

The use of mobile sink nodes is another effective tactic, as studied in [57], which identifies that moving the sink along the network's periphery mitigates energy hole problems. Additionally, [58] suggests that employing a mobile node as a sink maximizes lifetime, albeit with increased routing algorithm complexity.

Data aggregation is a valuable technique to reduce the volume of data relayed to the sink, thereby minimizing energy expenditure in nodes near the sink and alleviating energy-hole issues. In [59], an energy-balanced data gathering protocol is proposed to address energy consumption balancing problems, with similar strategies employed in [59]. However, it's worth noting that this approach may not be suitable when preserving the fidelity of collected data is crucial.

Traditionally, wireless sensor network research has predominantly centered on homogeneous sensor nodes. However, contemporary studies are increasingly concentrating on heterogeneous sensor networks, where sensor nodes exhibit dissimilar energy characteristics.

A notable consideration in heterogeneous sensor networks is nonuniform initial energy distribution. In scenarios where node density remains constant, assigning varied initial energy levels to nodes based on their proximity to the sink becomes a crucial strategy. In [60], researchers implement this approach by allocating different initial energy levels to nodes according to their distance from the sink. Notably, the energy levels are constrained within predefined limits to ensure a controlled and effective energy distribution across the network. This tactic aims to extend the lifespan of nodes near the sink, preventing premature energy depletion and enhancing the overall performance of the heterogeneous sensor network.

Mobile Wireless Sensor Network (MWSN)s present a unique set of challenges compared to their stationary counterparts due to their dynamic topology. The complexity of

routing increases, and existing clustering protocols for Wireless Sensor Networks (WSNs) often encounter limitations related to connectivity, energy efficiency, fault tolerance, load balancing, and mobility adaptation. In response to these challenges, Sabor (2018) introduces the Adjustable Range-Based Immune hierarchy Clustering protocol (ARBIC) tailored for Mobile Wireless Sensor Networks (MWSNs). ARBIC supports mobility and effectively transmits sensory data to the base station over an extended period. The protocol reduces overhead packets and computational time by initiating the clustering process only when the residual energy of any cluster head falls below a predefined threshold.

In [61], a topology control algorithm is proposed for constructing a virtual backbone in wireless sensor networks to maintain network connectivity. The Power-CDS (P-CDS) mechanism is introduced to schedule active and backup sensor nodes in the backbone, enhancing fault tolerance by adjusting transmission ranges when node failures are detected.

To enhance the accuracy of event detection in wireless sensor networks, [62] proposes a scheme that leverages adjustable sensing and transmission radius for sensors. The system initially deploys with 1-coverage, optimizing resource utilization. Upon event detection, the scheme dynamically transitions to k-coverage to improve accuracy and robustness. The adjustable sensing model, achieved through power adjustment, is formulated as an optimization problem. The objective is to identify the optimal sensor set, adjusting sensing and transmission radius to achieve the desired coverage degree. The optimization minimizes a cost function considering energy consumption and achievable detection accuracy. This approach not only ensures efficient resource utilization but also enhances the reliability and accuracy of event detection.

Following extensive involvement of hot spots as relay nodes in data forwarding, the energy of the hot spots depletes rapidly, leading to node depletion. An increase in dead nodes in the network renders it isolated or less functional, particularly when crucial relay nodes die early in the network's lifespan. This impacts the packet delivery ratio (PDR), a metric used to gauge network lifetime. Various alternatives have been explored above to

enhance network lifetime in response to these challenges.

2.3 Problem Definition

2.3.1 Network Model

In this wireless sensor network scenario, uniform initial energy is assumed for all sensor nodes, while sinks are considered to have infinite energy and can communicate both within the network and externally. All nodes possess the same communication range, and energy consumption for both sending and receiving is determined by the distance between nodes.

The network is modeled as a graph $G(V, E)$, where V is the set of all sensor nodes denoted as N, and the base stations or sink nodes denoted as S deployed in the network, i.e., $V = N \cup S$. An edge $(u, v) \in E$ exists if and only if the two nodes are within each other's communication range.

For each node to each sink, multiple paths $P_1, P_2, \ldots, P_k$ are assumed, where k is a positive integer ($k \geq 1$). If a source node v and a sink S_i are not in direct communication range, multi-path routing allows the source v to transmit data to the designated sink S_i by following a path such as $v, \ldots, n_i, \ldots, S_i$, where $i \in N - \{v\}$ and $S_i \in S$. Multiple such paths are available for nodes to transmit data to sinks.

To optimize energy consumption, the source node selects the shortest path among the possible alternatives when transmitting data to a sink. The goal is to minimize the energy expended in sending and receiving data. Consideration of a graph with six nodes (A, B, C, D, E, and F) is illustrated using an adjacency matrix, with the choice of alternate paths being depicted based on the given matrix.

$$M = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Certainly, considering the adjacency matrix and identifying the possible paths from node A to sink F based on the provided information:

Paths from A to F: $P1 : A \rightarrow B \rightarrow C \rightarrow E \rightarrow D \rightarrow F$

$P2 : A \rightarrow B \rightarrow D \rightarrow F$

$P3 : A \rightarrow C \rightarrow E \rightarrow D \rightarrow F$

$P4 : A \rightarrow C \rightarrow B \rightarrow D \rightarrow F$

These paths are determined by following the ”1” values in the adjacency matrix, representing the existence of edges between corresponding nodes.

The concept of choosing the shortest path for data transmission in a Wireless Sensor Network (WSN is similar to the example where node A selects the second path (P2) as the shortest path to send data to sink F.

In the context of WSNs, the issue of hot spot nodes arises, particularly when a common intermediate node (e.g., node C) is heavily utilized by multiple source nodes (e.g., V_i, V_j, V_k). This can lead to the premature depletion of node C’s energy, potentially causing sub-networks to become isolated or reducing the number of nodes that can communicate with the sink. Such nodes are also referred to as hot spot nodes, along with the sink neighbors.

Cut vertices, or cut points, in a WSN are nodes whose removal disconnects the graph, leading to vulnerabilities in network connectivity. Referred to as isolated networks, these scenarios occur when sub-graphs become disconnected. In earlier research, allowing nodes to die necessitated network reorganization and the discovery of new paths, incurring

increased costs due to frequent changes.

Recent research has explored the deployment of multiple sinks to extend network lifetime. In [31], the authors propose a method to reduce sink maintenance costs by enabling a single sink to be active at a time. This unique sink activation approach maintains the network's characteristics similar to a WSN with a single sink, while benefiting from the extended network lifetime achieved through multiple sink deployment. Sink selection is performed using CASS, and the shift rate is considered a crucial criterion for activating sinks.

The shift rate is defined based on the number of sensors that can connect to the sink at different time instances. For example, if a sink S can be reached by p sensors in a network of n sensors at time t_i, and after some time at t_j ($i < j$), q sensors can connect to the sink ($q \leq p$), the shift rate is determined by this change in connectivity over time. This strategy helps in efficiently managing sink activation and optimizing network lifetime.

$$\text{Shift rate}_{T_n} = \frac{(\text{Number of nodes connected to sink})_{t_j}}{(\text{Number of nodes connected to sink})_{t_0}}$$

This approach, aims to prevent hot spot nodes from dying prematurely in the network, which is achieved by setting a threshold on the energy usage of sensors before participating in data transmission or acting as intermediate nodes in communication.

As previously mentioned, each node in the network may have multiple paths to reach the sink. The source node selects the shortest path for data transmission, and the remaining paths might be utilized after a network reorganization when certain nodes (hot spot nodes) cease to function. In this approach, by delaying the occurrence of hot spot nodes dying prematurely, thus increasing the chances of finding new paths to the sink.

To achieve this, set a threshold on energy usage, and before allowing intermediate nodes to participate in communication, check if all nodes in the shortest path satisfy this threshold. If they do, the source sends data using the shortest path; otherwise, we explore alternate paths. If the next shortest paths have the same hop count, we choose the one with neighbors having higher residual energy. The alternate path is used to send data instead of the earlier

path, and this process continues till no node is unable to reach any of the sink with the defined threshold value. In such case reduce the threshold to half of its current value. This optimal Alternate path routing continues until the threshold reaches to 10% of the initial energy.

This approach ensures that hot spot nodes are not allowed to die prematurely, enhancing the network. To further extend the network lifetime, especially when network isolation occurs due to dead connecting nodes, introducing adjustable communication or increasing transmission range (ICR). By ICR of sensors and sinks, nodes can find new neighbors within the expanded range. ICR with AP routing continues until no nodes have enough energy to communicate with the current communication range. Although increasing the transmission range may initially require more energy for communication, we optimize its usage by adjusting the range only when establishing connections is not possible. This strategy allows us to utilize the remaining energy efficiently, extending the network lifetime and enabling the transmission of additional messages.

2.3.2 Energy model

The model proposed by [42] addresses radio characteristics, encompassing energy dissipation during both transmitting and receiving modes. This model quantifies the energy expenditure when transmitting a $k-bit$ message over a distance d. The energy dissipation for transmission (E_{Tx}) is given by:

$$\begin{aligned} E_{Tx}(k,d) &= E_{Tx-elec}(k) + E_{Tx-amp}(k,d) \\ E_{Tx}(k,d) &= E_{elec} * k + E_{amp} * k * d^2 \end{aligned} \tag{2.1}$$

Similarly, the energy dissipation for reception (E_{Rx}) is given by:

$$E_{Rx}(k) = E_{Rx-elec}(k) = E_{elec} * k \tag{2.2}$$

The parameters are defined as

$$E_{Tx-elec} = E_{Rx-elec} = E_{elec} = 50nJ/bit$$

Transmit Amplifier $(E_{amp}) = 100pJ/bit/m^2$

In the simulation, a symmetric radio channel is assumed, meaning the energy consumption to transmit data from node A to node B is the same as from node B to node A. Additionally, nodes periodically sense data from the environment. In the beginning of the ICR algorithm, some nodes may be unable to communicate with the sink due to the absence of hot spot nodes acting as routers. To address this, we adjust the communication range of nodes to contact the sink using more energy. The transmission range is increased by five units iteratively, searching for connecting nodes to reach the sink. This enables the utilization of residual energy in nodes to send more messages either by establishing connections with an increased communication range, avoiding connectors/hot spot nodes, or by direct contact with the sink.

The algorithm is heuristic and leverages the existing communication and energy consumption models. It opportunistically uses the energy consumption at each node, especially at hot spot nodes, in a distributed manner to maximize the use of energy and extend the lifetime of the network.

2.3.3 Network lifetime

In the literature, the evaluation of network lifetime in wireless sensor networks involves various metrics, as outlined in studies such as [17, 39]. Some of the commonly used metrics include:

1. the time until the first node dies
2. the time until the last node dies

3. the time until a desired percentage of nodes die
   In some scenarios

4. period until the entire region covered

5. N-of-N means the time duration until the first gateway dies

6. K-of-N means the time duration until K gateways out of N are alive

7. m-in-K of N means the time duration until all m supporting gateways, and overall a minimum of K gateways are alive

8. In [63], along with the old definitions, they defined the total number of messages received by the sink as a lifetime of the network.

In our work, the objective is to maximize the NL until no node can communicate with the sink, achieved either through a multi-hop approach or by adjusting the communication range (ICR). As long as nodes can send data to the sink, we consider the network to be live and capable of collecting sensed data.

Traditionally, in WSN, the first set of gateways tends to exhaust their energy, leading to reduced network connectivity. However, in our approach, we prevent hot spot nodes from dying at the initial stage by actively seeking APs. Consequently, no node dies until a specified threshold is reached, allowing sensors to continue sending data to the sink. As long as nodes maintain communication with the sink, network connectivity persists, and the NL is extended. In our scenario, the total number of messages received by the sink serves as a suitable metric to define NL.

2.4 Methodology

2.4.1 Enhancing WSN lifetime by sending the data through Alternate path (AP)

Algorithm 1 outlines the procedure for enhancing the network lifetime of a wireless sensor network by selecting alternative paths, ensuring that nodes live as long as possible.

Several assumptions are made for the construction of WSN:

1. Nodes (sensors and sinks) are randomly deployed, with each sensor capable of communicating with at least one sink.
2. Homogeneous sensor nodes are considered, with predefined initial energy.
3. Sinks have infinite energy and can communicate with other sinks and the external world.
4. Nodes identify their neighbors based on Euclidean distance by broadcasting a Hello packet.
    - If $dist(u, v)$ fall under the given communication range then node u and v are neighbors to each other
    - otherwise they are not neighbors and communication can be established only by using multi-hopping.
5. The above information is used to identify all possible paths from a source to the current sink.
6. Sinks broadcast setup messages to determine paths from each sensor to the sink.
7. The source has the option to select the shortest path among all possible paths to minimize energy consumption during data transmission.

The network model, energy model, definition of NL, and the assumptions applied in a (WSN) are consistently utilized throughout the thesis. These aspects may be adapted or modified as necessary based on the specific work discussed in the thesis.

A tree is constructed with the sink as the root, considering the source as the child nodes. The number of nodes reachable to the sink that satisfy the energy threshold T_E is determined, representing 100% of nodes capable of connecting to the sink. Initially, the shift rate of every sink is 100%. As the network continues data transmission, the number of nodes connected to the sink satisfying T_E decreases, leading to a reduction in the shift rate from 100% to $x\%$, where $x < 100$.

Data transmission begins from each source, and the energy consumption for transmitting and trans-receiving data is calculated based on the formula in [42], considering a given communication range. The algorithm implements periodic-driven application properties, where all nodes periodically send collected data to the sink. Each node starts sending data messages one by one, constituting a single turn. These turns continue until no node connects to any of the sinks.

Algorithm 2 outlines the procedure for sending data messages from source to sinks based on the energy threshold T_E. Before transmitting data from the source to the sink, it is ensured that the residual energy of all hops satisfies T_E. If the source does not have sufficient energy, the next node in line is allowed to send. If any intermediate node fails to meet T_E, the algorithm explores all multiple paths from the source to the sink. The algorithm selects the alternate path with the shortest distance and all hops satisfying T_E. This AP routing continues until either a node with residual energy less than T_E is found or no node can communicate with the sink with the given T_E.

If a node with residual energy less than T_E is identified, the algorithm determines the number of nodes that can connect to the sink satisfying T_E. Based on this count, the shift rate is calculated.

If the calculated shift rate meets the predefined criteria or no node can establish comm

Algorithm 1: Enhancing network lifetime by Alternate Path

Input: Initial Energy of Sensor E_S, Shift Rate, Number of Sensors n, Number of Sinks m, Energy_Threshold T_E = 50% of E_S , Energy required to act as a Source E_T, Energy required to act as Intermediate Node E_{TR}, Commn_Range, Initial Sink S_1, $tot\_msgs = 0$, lower_bound=10% of E_S

Output: Total number of messages received by all sinks tot_msgs

Randomly deploy all nodes (sinks, sensors) ensuring that they can be connected to at least any one of the sink;

repeat

- Find the neighbors of all nodes in the network;
- Find the shortest path from all nodes to initial sink;
- Construct a tree by considering the selected sink as root node;
- calculate the shift rate of the selected sink $Current\_shift\_rate$;
- `/* shift rate is defined as the percentage of nodes connected at` t_n `and` t_0 `*/`
- **if** $current\_shift\_rate \geq shift\_rate$ **then**
  - **if** $T_E > lower\_bound$ **then**
    - count the number of nodes connected to the sink and satisfying the T_E;
    - $(no\_of\_msgs, less\_threshold, no\_more\_sending) = send\_msg\_threshold()$;
    - $tot\_msgs \mathrel{+}= no\_of\_msgs$;
    - **if** $less\_threshold$ *is true* **then**
      - recalculate the $current\_shift\_rate$;
    - **if** $no\_more\_sending$ *is true* **then**
      - calculate the network reach of all sinks. pick the sink with more connected nodes satisfying the threshold as the next active sink;
      - goto step 2;
  - **if** $T_E \leq lower\_bound$ **then**
    - count the number of nodes connected to the sink;
    - $(no\_of\_msgs, redefine\_network\_cond) = send\_msg()$;
    - $tot\_msgs \mathrel{+}= no\_of\_msgs$;
    - **if** $redefine\_network\_cond$ *is true* **then**
      - calculate the network reach of all sinks by considering the reorganized network;
      - pick the sink with more network reach as the next active sink;
      - goto step 2;

until *network reach of all sinks become 1*;

if *no node is able to send the message to all the sink with* T_E **then**

- $T_E = T_E/2$;

Algorithm 2: Message sending based on the energy threshold (*function send_msg_threshold*)

Input: Initial Energy of Sensor E_S, source, path, neighbors, Residual_Energy[], Number of Sensors n, Number of Sinks m, Energy required to act as a Source E_T, Energy required to act as Intermediate Node E_{TR}, Current_sink S_i

Output: Number of messages received by sink $sent\_msg$, $dead\_node\_cond$

```
if Residual_Energy(source) > T_E then
    if path exist from source to sink then
        if all hops residual energy > T_E then
            send message to sink;
            reflect the energy consumption in the respective hops;
            if Residual_Energy(hop_node) ≤ T_E then
                less_threshold ← TRUE;
                break;
        else
            [path_exist] ← find_possible_paths
             (src, sink_neigh, path, neigh);
            if path_exist is true then
                send the message to sink;
                reflect the energy consumption in the respective hops;
                if Residual_Energy(hop_node) ≤ T_E then
                    less_threshold ← TRUE;
                    break;
            else
                move to next source to send the message;
    else
        move to next source to send the message;
else
    move to next source to send the message;
```

nication with the current sink, the CASS is triggered to choose a new sink; otherwise, the current sink continues to be active. This cycle repeats with the new sink, and the shift rate is redefined based on the assumed conditions. The new sink is selected by considering the sink with a greater network reach, as per the updated definition.

$$\text{Shift rate}_{T_n} = \frac{(\text{Number of nodes connected to sink satisfying } T_E)_{T_n}}{(\text{Number of nodes connected to sink satisfying } T_E)_{T_0}}$$

Algorithm 3: Message sending allowing nodes to die ($function\ send\_msg$) }

Input: Initial Energy of Sensor E_S, source, path, neighbors, Residual_Energy[], Number of Sensors n, Number of Sinks m, Energy required to act as Intermediate Node E_{TR}, Current_sink S_i
Output: Number of messages received by sink $sent\_msg$, $redefine\_network\_cond$

```
if path exist from source to sink then
    send message to sink;
    reflect the energy consumption in the respective hops;
    if Residual_Energy(hop_node) ≤ E_T then
        redefine_network_cond ← TRUE;
        break;
    if Residual_Energy(hop_node) ≤ E_TR then
        redefine_network_cond ← TRUE;
        break;
else
    move to next source to send the message;
```

When no node can reach all the sinks with the considered T_E, reset T_E to half of its current value. Begin selecting the sink with more nodes satisfying T_E. This process persists until the threshold reaches the lower bound, i.e., 10% of the initial energy of the sensor.

Exploring multiple paths to identify an alternate path entails avoiding nodes with residual energy less than T_E for forwarding the data message. By keeping these nodes alive using the threshold, the energy of other nodes can be utilized to transmit the data message. Once the threshold $T_E \leq$ lower_bound is reached, there is no further means to prolong the lifetime of the hot spot nodes.

Algorithm 3 details the procedure for network reorganization and the continuation of the message-sending process. When the hot spot nodes inevitably begin to die, and a dead node is encountered, it signals the time to reorganize the network and recommence the data message transmission. During this process, the calculation of the shift rate and the sink shift are performed based solely on the shift rate in the Cluster Algorithm for Sink Selection (CASS). If all nodes are unable to communicate with the sink, the network reach of all sinks becomes 1, and the network lifetime cannot be further extended. Utilizing the residual

energy of other nodes to follow alternate paths delays the premature death of hot spot nodes, minimizes the need for reorganizations, and prolongs the network lifetime (NL).

The algorithm demonstrates a significant utilization of residual energy in comparison to CASS. When applying the algorithm and making the network more dense with a sensor-to-sink ratio of 100/4, 200/6, and 300/8, the results show improvements of 12.58%, 49.8%, and 67.6%, respectively, over CASS.

Following the utilization of residual energy from nodes to transmit data, numerous nodes retain a significant amount of energy, which often goes to waste due to a lack of connecting nodes to the sink. Referencing papers such as [43, 64] and the IRIS data sheet, where each sensor node may have a different transmission level for data communication, it is observed that such transmissions can draw more current from the battery. Rather than allowing the energy of these nodes to remain unused, the algorithm introduces ICR, aiming to harness this untapped energy and further extend the network lifetime.

2.4.2 Increasing the network lifetime using ICR

Each sensor node is initially deployed with a specified communication range denoted as x units in a designated region. This implies that a node can establish communication with all other nodes within a distance of x units. Following a designated period, denoted as T_i, the sensors in the network are expected to adjust their communication range from x units to $x + y$ units, where y is a constant. This adjustment is based on the energy consumption procedure implemented by the sensors, with the assumption that the sensors will utilize energy from their batteries to send and receive data depending on the distance between the sender and receiver nodes. In the context of WSN, energy consumption is proportional to the distance between the transmitting and receiving nodes. Nodes endowed with the capability to adapt their transceivers to variable distances are referred to as nodes with an increased communication range.

To implement a WSN with a variable communication range, it is assumed that the

sensors are equipped with adjustable transceivers capable of sending data even when the distance exceeds the originally defined communication range at the time of deployment. The proposed AP algorithm with CASS based sink selection is applied on a WSN until no more messages can be sent to any of the sinks from any source node. In this scenario, the sensors are allowed to increase their communication range by y units to send additional messages from sources to any of the sinks by re-organizing the network with new communication range. This helps in extending NL) by transmitting more messages. After ICR, the AP with CASS algorithm continues with data transmission. This process continues until no nodes can communicate with ICR. ICR continues until no node is left with enough energy to establish a network with the revised communication range.

The procedure is described step by step in algorithm 4.

Algorithm 4: Enhancing the network lifetime by Variable Communication Range

Output: Number of messages received by sink
repeat
    Increase the existing communication range by 5 units;
    Run the algorithm Enhancing the network lifetime by Alternate Path;
until *no node have enough energy to communicate*;

2.5 Experimental Setup & Results

In this section, exploring the experimental setup and performance analysis of the proposed methodologies alongside CASS [31]. The key performance metric under evaluation is the network lifetime, quantified in terms of transmitted messages.

- *Network Life Time:* Number of messages received by all the sinks until no more communication established between the nodes

The experimental setup is consistent throughout the thesis, incorporating additional input parameters specific to the addressed problems.

A Wireless Sensor Network was simulated using MATLAB, deploying sensors and sinks randomly. The simulation assumes that all sinks possess infinite energy for communication with the outer world and the nodes within the network. AfterA lower deployment, the neighbors of all nodes (sensors and sinks) are identified based on communication range and Euclidean distance between nodes.

Following the determination of node neighbors, a sink is selected, and message transmission begins using the proposed AP routing. In this simulation, the network lifetime is gauged by the number of messages received by all sinks. An increase in the message count signifies the improvement of the network lifetime. Experiments were conducted on various data sets with different network sizes. The input data details are presented in Table 2.1.

Grid Size	100 X 100
Initial Energy of Sensors	100 Joules
Communication Range	15 units
Shift Rate	90% - 45%
Number of Sensors	100, 200, 300
Number of Sinks	4, 6, 8
Lower bound of Energy Threshold	10% of the Initial Energy

Table 2.1: Input Data Information

The number of sinks was increased in the improved sensor configurations, and subsequently, variable communication ranges were applied for each combination of sensors and sinks to observe the network lifetime.

The algorithm was tested with a communication range set at 15 units. The results presented in Figure 2.1 offer a comparative analysis of CASS, AP routing, and AP routing with ICR over a 100-node network with 4 sinks. The experiments were conducted across 30 test cases, revealing that AP routing and AP routing with ICR exhibited an improvement of 12.4% and 37.9% over CASS respectively. However, in some test cases, AP routing showed nearly the same NL as CASS, attributed to the network topology formed by the random deployment of sensor nodes and sinks. The introduction of ICR in conjunction with AP

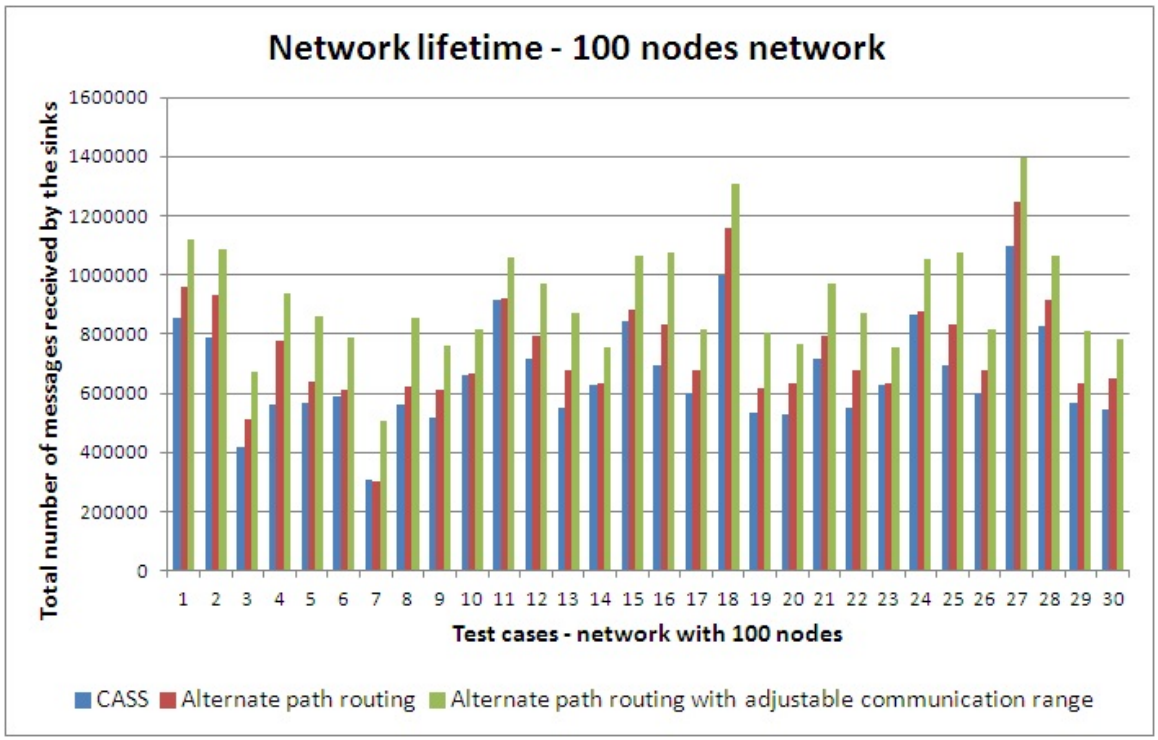

Figure 2.1: Comparison of NL on CASS, AP, and ICR over a 100 node network

routing demonstrated significant improvement in all test cases. Notably, ICR was applied to the network after the energy depletion of hot spot nodes, eliminating the side effects of random deployment.

The experiments were extended to include 200 and 300 sensor nodes deployed in a 100 x 100 grid, featuring 6 and 8 sinks, respectively. The results are illustrated in Figures 2.2 and 2.3. In Table 2.2, it is evident that AP routing and AP routing with ICR exhibited improvements of 49.8% and 72.2% in the case of 200 nodes with 6 sinks, and 67.6% and 87% for 300 nodes with 8 sinks. Figure 2.4 provides a comparative analysis between CASS, AP routing, and AP routing with ICR as the network density increases in terms of sensor nodes and sink nodes.

In all the cases, the Alternate path approach has shown a considerable improvement of 12.5% over CASS. Later the experiments were done on the same data set by decreasing communication range to 10 units and 7 units. The results are shown in Table 2.3. When we study the table, by decreasing the communication range, the network lifetime also

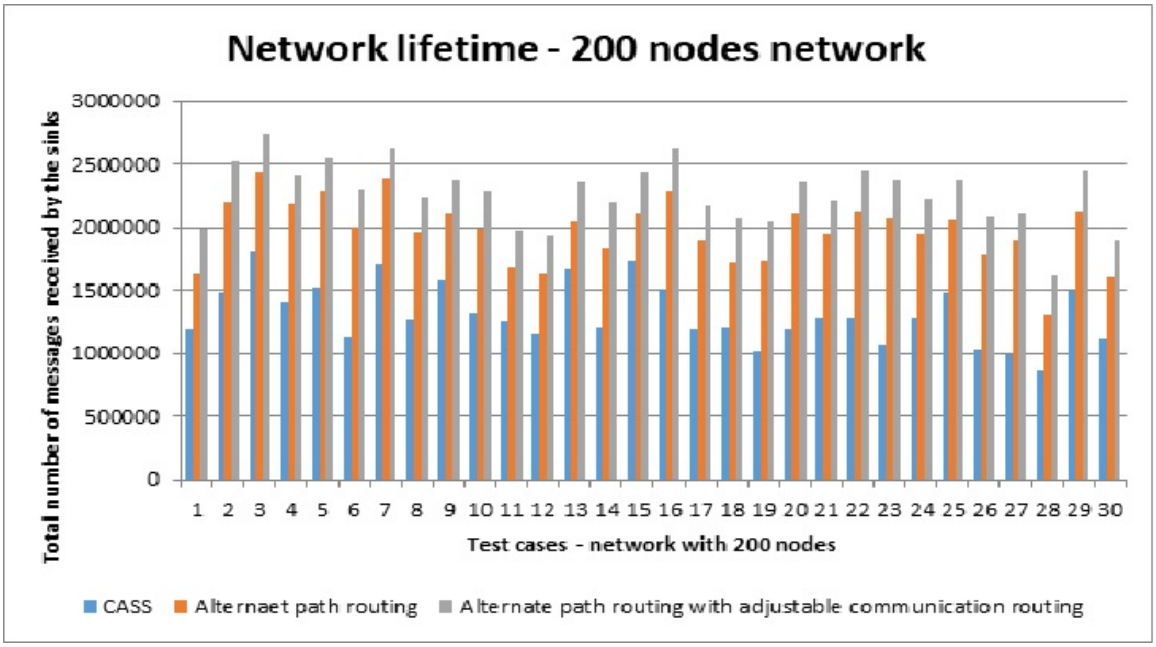

Figure 2.2: Comparison of NL on CASS, AP, and ICR over a 200 node network

Number of sensor nodes	CASS	AP	AP with ICR	% of improvement of AP over CASS	% of improvement of AP with ICR over CASS
100 nodes	664680	746868	916579.5	12.5	37.9
200 nodes	1315358	1970261.5	2265113.7	49.8	72
300 nodes	2141116.7	3587780.8	4003358.7	67.6	87

Table 2.2: Average of NL on all variation with increased sensor nodes

gradually decreases and the improvement comes down from 14.47% to 4.90% and 3.03% in a 200-sensor node network. We can observe from the percentages that by reducing the communication by five units only, the improvement rate suddenly dropped from 14.47% to 4.90% on a 200-sensor node network.

Increasing the network density and maintaining a transmission range of 15 units across 5 test cases resulted in an improvement rate of up to 19.08% compared to CASS. However, when the communication range was changed to 10 units and 7 units, the network lifetime began to decrease to 14.00% and 2.96%, respectively. These results emphasize the impact of not considering a feasible communication range, particularly in a dense WSN. Given this

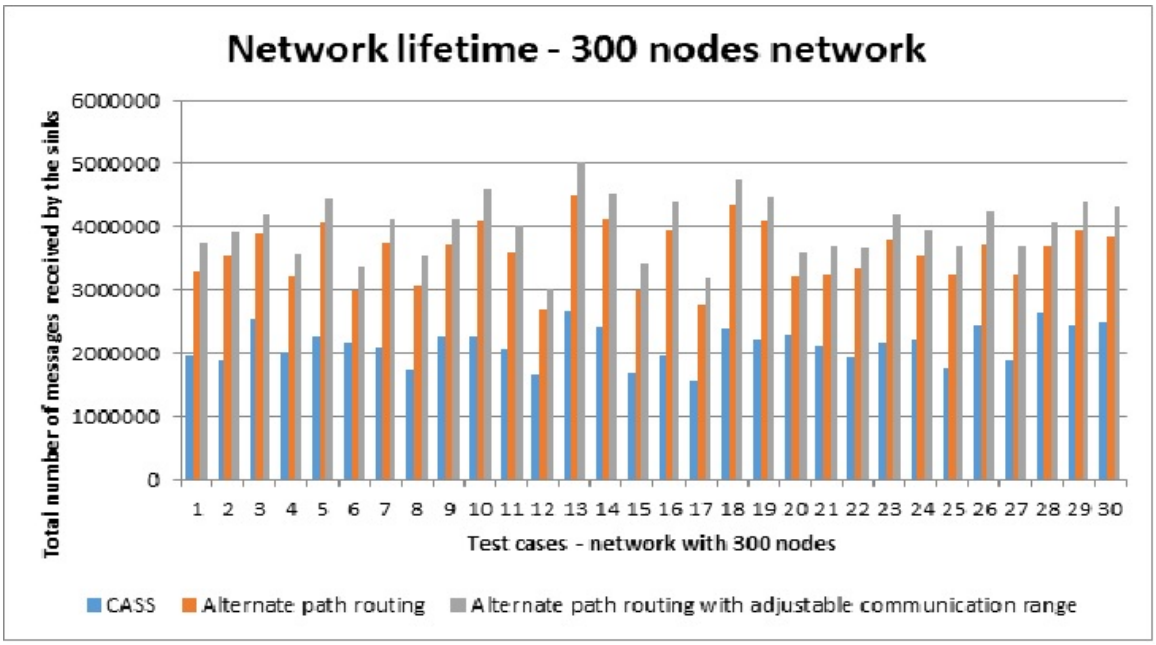

Figure 2.3: Comparison of NL on CASS, AP, and ICR over a 300 node network

observation, subsequent experiments continued with a communication range of 15 units, deemed a feasible value.

No. of Test Cases	No. of Sensors / Sinks	Commn. Range	Avg. Inc. of Alternate Path over CASS
5	100 / 4	15	8.75
5	200 / 6	7	3.03
5	200 / 6	10	4.90
5	200 / 6	15	14.47
5	300 / 8	7	2.96
5	300 / 8	10	14.00
5	300 / 8	15	19.18

Table 2.3: Study of finding a feasible communication range based on CASS and AP

Experiments were conducted on all test cases by varying the shift rate from 90%, 85%, ..., 45%. Results for 20 test cases on a 100-sensor network are presented in Figure 2.5. Upon observation, no significant change in NL was noted for each test case with varying shift rates, indicating that, for a 100-sensor network, the shift rate does not have a substantial impact on network lifetime. Similarly, AP and AP with ICR were tested on 20 cases with

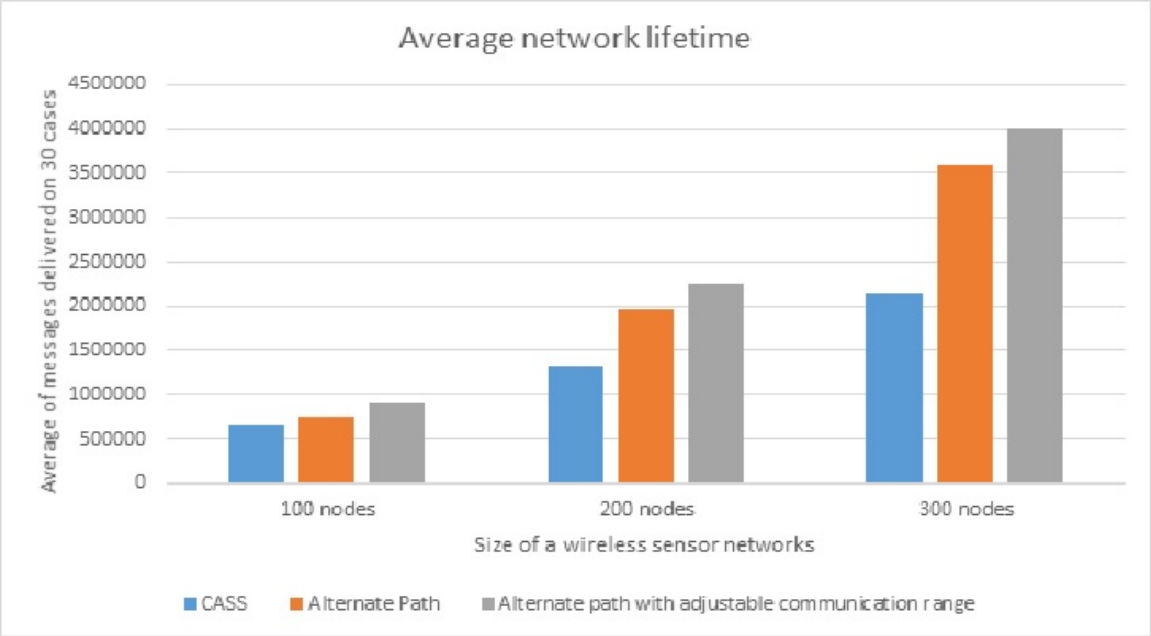

Figure 2.4: Average study of all approaches on a WSN making it denser

variable shift rates, and the results are illustrated in Figure 2.6 and Figure 2.7, respectively, with minimal differences in NL.

The experiments were extended to 200-sensor and 300-sensor networks with varying shift rates. One test case result from a dense network is presented here, showcasing the results obtained using CASS, AP routing, and AP routing with ICR in Figure 2.8 and Figure 2.9, respectively. The outcomes suggest that the shift rate does not exert a significant influence on NL.

2.6 Summary

This chapter outlines an approach to maximize the utilization of residual energy in WSNs for enhancing NL. The strategy involves employing the AP routing from source to sink to prolong the lifespan of hot spot nodes and dynamically adjusting the communication range ICR opportunistically. By doing so, all nodes, including hot spot nodes, are allowed to operate until the residual energy of nodes in the network reaches a lower bound. This

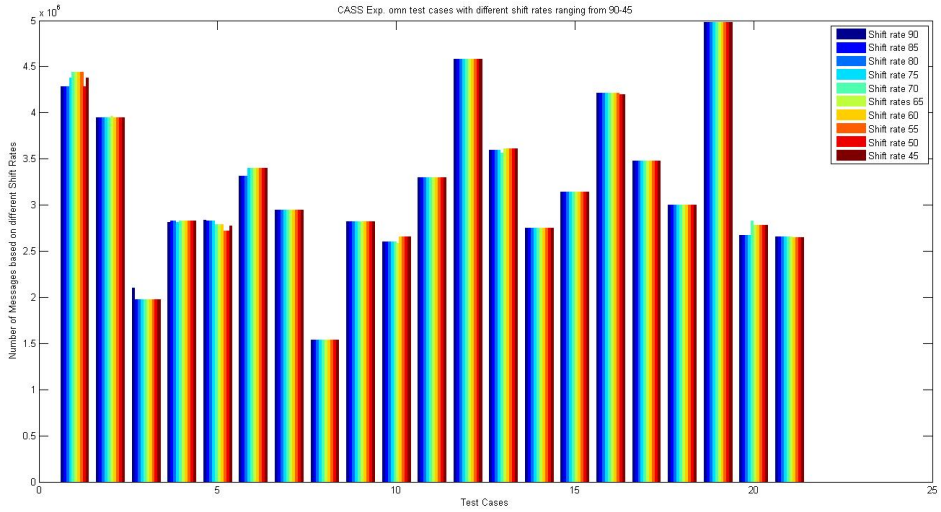

Figure 2.5: Varying shift rate from 90% - 45% on CASS - 100 node network

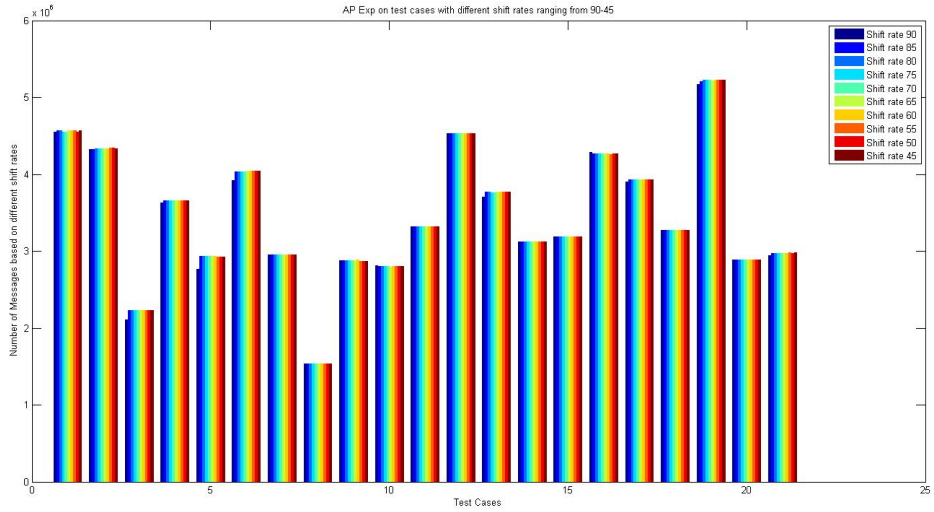

Figure 2.6: Varying shift rate from 90% - 45% on AP - 100 node network

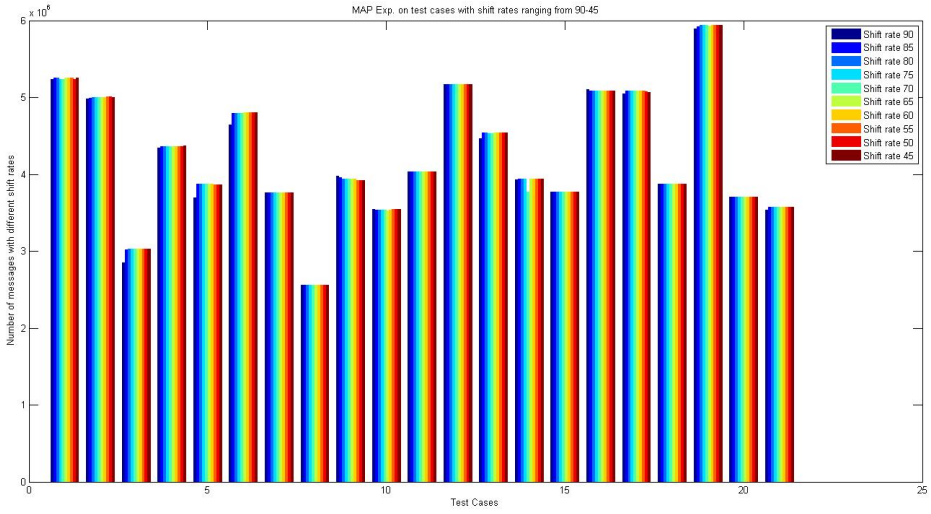

Figure 2.7: Varying shift rate from 90% - 45% on AP routing with ICR - 100 node network

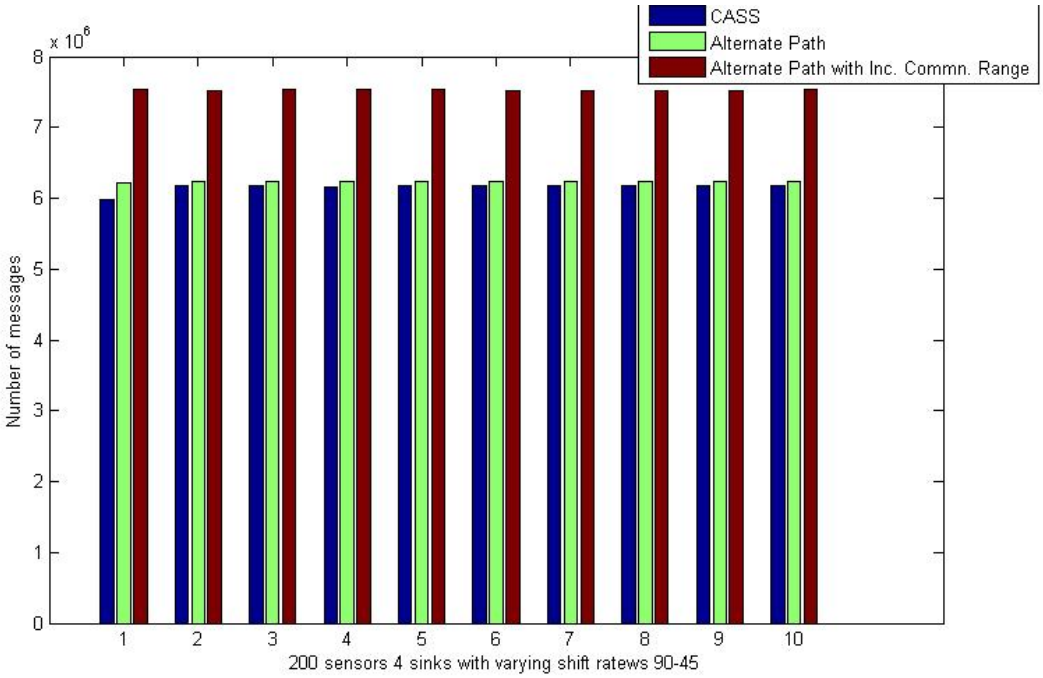

Figure 2.8: Varying shift rate from 90% - 45% on all approaches - 200 node network

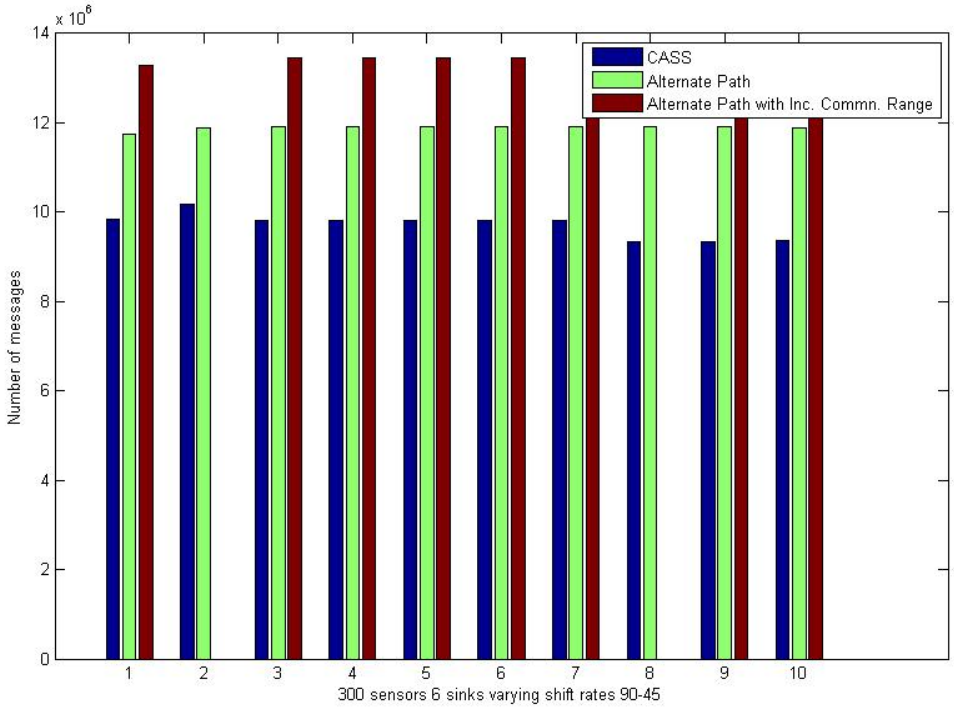

Figure 2.9: Varying shift rate from 90% - 45% on all approaches - 300 node network

methodology restricts the energy usage of hot spot nodes, enabling the network to transmit more messages with an increased Packet Delivery Ratio (PDR) compared to CASS.

AP routing proves effective in improving NL, particularly in dense WSNs. The combination of AP routing and the use of ICR contributes to extending the NL by leveraging the remaining energy of nodes. This approach demonstrates superior performance over both AP routing and CASS. Moreover, the paper emphasizes the advantage of AP routing in exploring available paths and rerouting data messages, thereby delaying the premature death of hot spot nodes and reducing frequent path updates associated with reorganization.

Simulation results indicate that AP routing yields promising outcomes, especially in denser network configurations. When the network is no longer connected to any sink, dynamically adjusting the communication range (ICR) ensures that the residual energy of remaining nodes is effectively utilized to further enhance NL compared to AP routing and CASS. In conclusion, the variable shift rates are observed to have no significant impact on

NL in the context of the proposed schemes.

However, identifying the residual energy of all relay nodes at the initial data transmission stage by a source node will require more control message communications. It thus will increase the traffic in the network. All these require more energy to communicate via control messages, but still, this information helps us successfully deliver more messages than usual.

CHAPTER 3

Reliable Data Delivery and Lifetime Enhancement in a Wireless Sensor Network

3.1 Introduction

WSNs have emerged as the preferred solution for developing and implementing advanced monitoring and control systems, as highlighted in previous works [1, 7]. The deployment of numerous cost-effective sensors has become feasible, enabling extensive monitoring across diverse terrains such as the Earth's surface, underwater realms, and the atmosphere [65]. A key advantage of sensor networks lies in their ability to extend computational capabilities to physically inaccessible environments, offering a means to operate in hostile, challenging, or ecologically sensitive areas where human presence is impractical [66, 67].

Sensor networks have the potential to operate continuously in remote habitats, providing valuable data about the environment and facilitating data transmission to end-users [8]. At the core of WSNs are the sensor nodes—devices equipped with sensing, computation, and communication capabilities. These sensor nodes, tailored to monitor various phenomena such as temperature, light, motion, pressure, and humidity based on application requirements, play a central role in collecting and processing data [68].

The processing module within a sensor node performs computations on both locally

sensed data and information received from neighboring sensors. Simultaneously, the communication module facilitates the exchange of data packets among adjacent nodes, forming a network that provides coverage over expansive environments [1, 68]. Given that individual sensors offer limited information, the collaborative efforts of a sensor network become essential for comprehensive coverage across large-scale environments. These sensor nodes are responsible for continuously collecting data from the surrounding environment and transmitting it to the sink node. In typical scenarios, numerous sensor nodes, ranging from a few tens to thousands, are strategically deployed across a designated area of interest. Through wireless communication, these nodes autonomously organize into a network, fostering collaboration to achieve a shared objective [7].

The sensor nodes operate by sensing data from their respective environments and autonomously sharing this information within the network. The sink node, positioned to receive data from all the distributed sensor nodes, plays a crucial role in processing the collected data before forwarding it to the end user. This collaborative and self-organizing nature of WSNs enables efficient data collection and dissemination across the network, contributing to the accomplishment of common tasks [7].

The traffic dynamics within WSNs pose challenges, particularly near the sink, as all sensor nodes transmit their sensed data in its direction. This congestion around the sink can lead to packet loss, exacerbated by factors such as transmission errors, collisions, interference, node failures due to energy depletion, and unforeseeable issues due to limited resources which unable to handle the processing demands [69]. Additionally, the limited range of sensor nodes may necessitate data to traverse numerous hops, introducing multiple points for potential errors and packet loss.

Ensuring the dependable transmission of vital data from sensor nodes to the sink is essential for the success of environmental monitoring. The necessity for data recovery arises from the occurrence of packet loss caused by a variety of factors. The ongoing challenge in WSNs lies in addressing the inherent unreliability of wireless links, coupled with the

limitations imposed by resource constraints in sensor nodes. The pursuit of a reliable data transfer mechanism from sensors to the sink continues to be a central focus in the continuous development of WSN technologies.

In resource-constrained Wireless Sensor Networks (WSNs), ensuring both energy efficiency and reliable data transport is vital for optimal performance in monitoring and control systems. The primary strategies employed to enhance reliability in WSNs include re-transmission and redundancy. While traditional research has primarily focused on re-transmission-based reliability, which involves recovering lost data packets through retransmission, this approach can lead to increased transmission overhead, energy depletion, network congestion, and compromised data reliability.

Redundancy-based reliability in data transmission involves using coding schemes to recover lost or corrupted bits within a packet, minimizing transmission overhead by correcting only affected bits. Both retransmission and redundancy can be applied on a hop-by-hop or an end-to-end basis. In the hop-by-hop method, intermediate nodes handle re-transmission or redundancy, reducing the memory load on source and relay nodes. Conversely, the end-to-end approach limits these processes to the source and destination nodes, potentially leading to memory scarcity and operational issues for the source node. Additionally, determining the required data quantity introduces packet-level and event-level reliability concepts. Packet-level reliability ensures all packets from relevant sensor nodes reach the sink, while event-level reliability focuses on providing sufficient information about a specific event.

Acknowledgments are commonly used in multi-hop WSNs to achieve re-transmission-based reliability, with explicit Acknowledgment (eACK, NACK) and Implicit Acknowledgement (iACK) mechanisms. While eACK, NACK involve special control messages, iACKs exploit the broadcast nature of the wireless channel, reducing transmission overhead.

In summary, the choice between re-transmission and redundancy, as well as between end-to-end and hop-by-hop mechanisms, depends on the specific requirements of the application and the nature of the WSN.

3.1.1 Definitions

1. Reliable Node: A node is considered reliable when it consistently forwards all received data packets from other relay nodes without dropping any messages. The percUR of a reliable node is 0.

2. Unreliable Node (URNode): A node with varying probabilities of forwarding data packets. If a node is unable to handle demands from other nodes due to limited processing and memory resources, it may drop received messages. A node exhibiting dropping probability due to resource constraints is referred to as a URNode.

3. Probability of Unreliability (percUR):This parameter signifies the probability of unreliability exhibited by a URNode and is considered within the range of 10 to 50 with a difference of 10. For an instance, considering 20% as the percUR for a set of URNodes then every URNode has a probability of dropping a message at most 20 times out of 100 times.

4. Network Lifetime (NL): In a Wireless Sensor Network (WSN), NL is quantified by the messages received by the sink nodes.

5. Message Drop: An URNode engages in message dropping when it receives unmanageable demands for data forwarding from other relay nodes, leading to the non-delivery of data messages or packets based on the defined percUR.

3.2 Literature survey

In [70], a Directed Flood-Routing Framework (DFRF) is introduced for WSNs, providing a foundation for the modeling and rapid development of application-specific routing protocols based on directed flooding. This framework utilizes flood-routing protocols, which are probabilistic methods that exert best-effort routing for data packets.

The presented approach integrates SWIA (Selective Wireless Information Assurance) as a dependable packet recovery mechanism in Wireless Sensor Networks (WSNs). SWIA employs iACK (implicit acknowledgment), where a transmitting node monitors the channel after sending a packet to verify if the receiver has subsequently forwarded the packet towards the destination. The utilization of iACK in SWIA provides a significant advantage by avoiding additional packet overhead. However, in cases where the sender does not receive any acknowledgment (ACK), the packet is considered lost, and for reliability, each lost packet undergoes re-transmission. This continual re-transmission of packets exacerbates challenges related to channel contention and network congestion. Furthermore, the framework supports automatic data packet aggregation and facilitates in-network data packet filtering and modification.

In [69], Reliable Transport with Memory Consideration (RTMC) protocol is introduced as a transport layer protocol specifically tailored for sensor nodes with limited memory. Functioning with both hop-by-hop re-transmission and congestion control, RTMC ensures smooth and reliable data transport. To tackle memory overflow concerns, packet headers are enriched with memory information, which is shared among neighboring nodes. The source node transmits data segments until the relay node's memory is full, and reliability is upheld by holding forwarded segments at the sender until acknowledgment is received. The protocol aims to optimize channel resources, facilitating the delivery of all segments to the sink with low transport time and minimal memory cost. While validated on real test beds, scalability poses a challenge for RTMC, potentially impacting performance in scenarios with a large number of nodes and dynamic topologies. The increased storage requirements per hop raise concerns about memory overflow, leading to packet loss and compromising reliability.

The Reliable Bursty Convergecast (RBC) protocol, presented in [71], aims to improve channel utilization in bursty convergecast within multi-hop WSN. It employs a window-less block acknowledgment scheme, ensuring continuous packet forwarding by utilizing an

adaptive timer mechanism for re-transmission timeouts. The protocol replicates acknowledgments for packets to alleviate channel contention caused by re-transmissions in large bursts of packets destined for the sink from various locations. However, the introduction of priority schemes for transmission scheduling raises concerns about potential indefinite waiting for lower-priority packets in the queue, leading to increased latency and unnecessary queue occupancy. While RBC demonstrates enhanced reliability compared to stop-and-wait implicit acknowledgement (SWIA), there is a lack of validation regarding its energy consumption, a critical aspect in the context of WSNs.

In [72], the Energy-efficient and Reliable Transport Protocol (ERTP) is proposed with a focus on energy constraints in WSNs. ERTP, a link-oriented packet reliability protocol, addresses energy efficiency and loss recovery at each hop, offering statistical reliability based on the quantity of received data packets at the sink. Leveraging the SWIA mechanism for packet recovery, ERTP employs a re-transmission timeout estimation mechanism dynamically reducing re-transmissions to conserve energy. Unlike RBC, ERTP has been validated with a low transmission rate and minimal congestion, contributing to improved overall performance. The protocol utilizes a Low Power Listening (LPL) MAC protocol for iACKs, reducing overhearing and subsequent packet loss. While some issues persist, ERTP demonstrates superior performance in scalability, energy efficiency, and reliability compared to other schemes in the same category.

In [73], the Tunable Reliability with Congestion Control for Information Transport (TRCCIT) is introduced as a protocol aiming to deliver reliable data transmission in diverse network conditions and application scenarios. The protocol employs a localized Hybrid Acknowledgment (HACK) mechanism and a timer management system. HACK combines iACK and eACK, NACKs, primarily utilizing iACKs, while allowing the next hop neighbor to send an eACK, NACK to the sender to prevent unnecessary re-transmissions. The adaptive re-transmission timeout mechanism is based on buffer occupancy, maintaining a balance between incoming and outgoing messages at each node. TRCCIT not only offers improved

reliability compared to RBC but also addresses key issues such as timeliness, adaptive timers, HACK, and energy efficiency under dynamic network conditions.

The Reliable Multi-Segment Transport (RMST), introduced in [74], proposes a sink-centric link-oriented packet reliability scheme based on eACK, NACKs. RMST provides caching and non-caching modes, deciding whether to store data segments for re-transmission. It utilizes selective eACK, NACKs, and timer-based mechanisms for loss detection. While suitable for WSNs dealing with large-sized data transfers like images, RMST only performs fragmentation/assembly at the source and destination, leading to potential delivery order issues. This may contribute to increased channel contention and in-network congestion due to a growing number of fragments. Additionally, RMST does not address the possibility of eACK, NACK implosion, where downstream nodes issue a chain of eACK, NACK requests in non-caching mode for detected gaps within transmitted fragments.

In addressing the downstream reliability of control messages and sensor software updates from the sink to sensors, [75, 76] propose hop-by-hop mechanisms known as Pump Slowly Fetch Quickly (PSFQ) and GARUDA, respectively. These mechanisms aim to disseminate control messages or software code segments downstream with reliability, utilizing re-transmission for loss detection and data recovery. PSFQ employs a strategy of pacing data at a slow speed (”pump slowly”) from the source node, allowing nodes experiencing data loss to aggressively fetch missing segments from their local immediate neighbors (”fetch quickly”). The pump operation consistently broadcasts code segments, while the fetch operation commences when intermediate nodes detect a gap in sequence numbers. PSFQ, however, requires all nodes to cache received packets, making it less suitable for memory-constrained sensor nodes. It is better suited for infrequent node reprogramming scenarios rather than continuous operations.

In the GARUDA protocol proposed in [76], designed for downstream reliability, the objective is to ensure the reliable delivery of query-metadata and control codes to the down-stream nodes. GARUDA designates certain nodes in the network as core nodes responsible

for re-transmitting lost packets, utilizing an Availability Map (A-map) to avoid unnecessary re-transmission requests. However, GARUDA introduces an additional core construction stage, potentially causing high latency in large sensor networks. The reliability guarantee is limited to the transfer of the first packet, making it less efficient for main functions in environmental sensing scenarios. Similar to PSFQ, GARUDA may be considered overkill if used for primary tasks in environmental sensing due to the associated complexities and potential latency issues.

This section has explored several schemes that target packet-level reliability through link-oriented methods for recovering lost packets. Link-oriented approaches have demonstrated greater reliability, time efficiency, and energy efficiency compared to connection-oriented schemes, as loss recovery occurs at each hop rather than at the end nodes. A common challenge in both categories, focusing on packet-level reliability, is the insistence on ensuring the safe delivery of every packet to its destination. While each scheme achieves this requirement in a unique way tailored to specific applications, it is essential to recognize that many WSN applications can tolerate a certain degree of packet loss. Allowing for some level of packet loss not only conserves the limited energy of sensors but also enhances overall system reliability.

In the context of WSN, a sensor node is considered ”dumb” when it can sense its surroundings but faces communication limitations due to reduced range caused by adverse environmental effects. This temporary behavior may lead to node isolation during unfavorable conditions, with reconnection occurring when the environment becomes favorable again. In [77], the impact of dumb nodes in stationary WSNs is explored. While an energy-efficient WSN typically achieves complete network coverage with a sufficient number of activated sensor nodes, the presence of dumb nodes introduces wasteful power consumption, diminishing NL. This behavior negatively affects the performance of WSN applications, leading to a degradation in network performance, as demonstrated in the findings presented in [77].

In [78], the focus is on achieving energy-efficient and reliable data delivery in WSN. Packet loss, a common issue in networks, hampers reliable data transmission rates, necessitating re-transmissions to improve reliability. However, an increase in re-transmissions leads to higher energy consumption and packet delivery delays. The paper presents a Routing mechanism for WSNs based on Learning Automata. This approach utilizes learning automata to calculate the selection probability of the next node in a routing path, taking into account the node's score, link quality, and previous selection probability. Additionally, the paper introduces an energy-efficient and reliable routing mechanism that combines learning automata with the A-star search algorithm. This integrated approach determines optimal routing paths by considering factors such as residual energy, link quality, free buffer space, and distance. Simulation results demonstrate the algorithm's effectiveness in reducing energy consumption, data delivery delay, and data transmissions, thereby enhancing overall NL.

The integration of technologies in the Internet of Things (IoT), such as WSN, edge computing, and cloud computing, addresses applications like environmental monitoring and disaster surveillance. However, IoT devices face challenges with limited resources like battery, communication bandwidth, and processing capacities. Load balancing, fault tolerance, and energy and memory efficiency are crucial concerns for data dissemination in IoT networks. In addressing these issues, [79] proposes a cross-layer optimization approach, integrating data-centric storage into distributed data storage mechanisms. The Collaborative Memory and Energy Management heuristic, solved using a genetic algorithm, outperforms existing approaches in various IoT scenarios by enhancing memory and energy efficiency while supporting load balancing.

In a WSN utilizing multi-hop routing over error-prone wireless channels, conventional approaches keep all nodes awake, leading to increased energy consumption. However, [80] introduces a sleeping multi-path routing approach that selects a minimal number of disjoint paths to meet reliability requirements. This strategy puts the rest of the network to sleep,

prolonging the NL while achieving a trade-off between reliability and energy efficiency.

In [81], the deployment problem of heterogeneous WSNs is addressed as it is one of the effective way to increase NL and reliability.

3.3 System Model

3.3.1 Assumptions

- All sensor nodes equipped with iACK technique with re-transmission reliability using hop-by-hop at packet level
- Considering a random set of nodes as URNodes
- percUR is predefined for a given set of URNodes and network handles the URNodes not to drop the message beyond the defined percUR
- the URNode is dropping the message due to the limitations on processing and memory like a dumb node discussed in section 3.2
- The NL is defined as the total number of messages delivered by all the sinks until no node is unable to communicate with any of the sinks, as discussed in [16, 82]. Additional details can be found in Section 2.3.3.

3.3.2 Network model

In the deployment of sensor nodes and sink nodes within the target region, sink nodes initiate a hello message broadcast to identify reachable nodes and establish a wireless sensor network. The network is modeled as a graph $G(V, E)$, where V represents the set of sensor nodes (N) and sink nodes (S). Multi-hop communication is essential for data transmission, given the large deployment area and limited communication range of individual sensor

nodes. Each source node determines multiple paths to reach the sink, selecting the shortest path for energy efficiency. The CASS approach then activates a sink in the network. A random set of Unreliable Nodes (URNodes) with a predefined probability of unreliability (percUR) is considered, and the network manages URNodes to prevent excessive message dropping. For a comprehensive understanding of the network model, please consult Section 2.3.1.

3.3.3 Energy model

The energy model for radio characteristics, encompassing energy consumption in transmitting and receiving models for sending a k-bit message over a distance d using the radio model, is expounded in [42, 82]. In our simulation scenarios, we made specific assumptions, including the symmetry of the radio channel, where the energy consumption for transmitting data from node A to node B is equivalent to that from node B to node A. Additionally, it was assumed that nodes within the network transmit sensed data periodically to the sink, as discussed in [82]. For a more detailed explanation of the Energy model, please refer to Section 2.3.2.

3.3.4 Reliability model

At the initial stage of network setup, a subset of nodes is randomly selected as URNodes with a predefined percUR.

1. Percentage of URNodes: The number of URNodes is determined based on the network density, i.e., the total number of nodes deployed in the network. The URNodes constitute 5%, 10%, 15%, 20%, and 25% of the deployed sensors, varying in increments of 5%. For example, if x% of the deployed sensor nodes in a region are designated as URNodes, the number of URNodes increases proportionally with the network density. For instance, if 15% of the nodes are designated as URNodes in

a network with 100 nodes, then the number of URNodes will be 15 nodes. In a network with n nodes, and x% of URNodes then the formula to determine the count of URNodes is $(n * x)/100$.

2. Percentage of Unreliability: This parameter defines the probability of a message being dropped by an URNode. For example, if a node UN_i is identified as an URNode with a percUR of 40, it implies that, on average, UN_i is permitted to drop a message up to 40 times out of 100. The probability of message drop by an URNode is unpredictable, as it depends on the availability of resources at the time of message forwarding.

3.3.5 Adjustable Communication Range

Adjusting the communication range is crucial for addressing the challenge of reliability in data transmission caused by URNodes. In addition to enhancing the NL, this adjustment aims to reduce message drops resulting from the dropping tendency of URNodes. Nodes dynamically modify their communication range to bypass URNodes and reach the next non-URNode effectively. This not only improves the NL but also mitigates the drop rate caused by URNodes. Previous studies, such as [3, 52, 83], have highlighted that adjusting the communication range can prolong the network's lifetime and alleviate the energy drain in hot spot nodes. While this adjustment may slightly reduce the number of messages initiated towards a sink, it contributes to delaying energy hole formation, thereby enhancing overall network reliability.

3.4 Proposed method:

After establishing the network through Hello messages for neighbor identification and control messages from the sink to establish the path, one of the sinks is selected as the active sink. This choice is made based on the assumption that all sinks have good network

reach in the initial phase. The sink with the smallest ID is considered as the initial active sink. Initially, the sink broadcasts the set of URNode ID's to all sensor nodes, and each node maintains a list of URNodes present in the network. Given that each URNode has a probability of dropping a message, every sensor node permits the inclusion of URNodes in the path routing.

The AP approach, outlined in Algorithm 5, is executed without considering the percUR of the relay node. All sensor nodes begin sending their sensed data to the sink, assuming that all relay nodes behave reliably during data transmission. In the routing path, if an URNode (denoted as v) encounters and drops a message due to resource unavailability, the node u preceding URNode v identifies the message drop using the iACK mechanism. Subsequently, node u initiates the AP routing algorithm. The neighbor nodes of u (excluding v) report the hop count to reach the active sink and their residual energy. Node u then selects the shortest path among the listed alternatives to reroute the message. In case multiple neighbor nodes have the same hop count, u prioritizes the one with higher residual energy. Before updating the new path over the old path, node u ensures that the neighbor node does not belong to the set of URNodes to minimize the number of re-routings. If no such neighbor node exists under the specified conditions, node u allows the message to drop. Otherwise, u selects an optimal path as per the AP algorithm to reroute the message. This process continues until either the sink receives the message or it is dropped by an intermediate node.

If node u fails to find an AP, it has several alternatives to handle the data message, depending on the capacity and availability of the sender node. In the given condition, u can choose any of the following options:

- Drop the message if buffer space is unavailable.
- Retain the message for aggregation if space is available.
- If the application is not time-sensitive, defer the message for later resending.

When node u is evaluating alternative neighbors to reroute a data message, it may

encounter a situation where it has an inactive sink node as a direct neighbor. From the perspective of the sink, node u is a direct neighbor (as described in the hot spot node concept in Chapter 2), as outlined in Algorithm 6. When comparing the energy consumption of rerouting a data packet to the active sink versus rerouting it to an immediate inactive sink, the optimal solution is to reroute the packet to any sink, considering that all sinks are interconnected. Rerouting to any sink offers an optimal solution for the network, extending its NL compared to rerouting to the active sink alone. In this scenario, the inactive sink needs to be temporarily activated to receive the data packet from node u, optimizing energy consumption while improving NL and reducing the drop rate.

Similarly, when prioritizing reliability over NL enhancement, the approach involves adjusting the communication range to skip URNode when re-routing is not possible. This variation emphasizes reliability at the expense of compromised NL and is presented in Algorithm 7. In this approach, the ICR operates by skipping a specified number of hops. For instance, if the system allows skipping at most 1 hop, then node u adjusts its communication range to reach the next hop by bypassing URNode v. If within the hop skip count, the next hop continues to drop the message, and no AP is found for re-routing, and the hop skip count exceeds the specified limit, then node u drops the message. By skipping one hop, the node ensures reliability more than rerouting to the active/current sink. The application of ICR results in a drastic decrease in the energy depletion of relay nodes, allowing the sensor node to function for a shorter time based on residual energy.

Applying the ICR variation in AP routing to the current sink and any sink ensures improved reliable data delivery compared to the reliability achieved in the two variants discussed in Algorithm 5 and 6.

Algorithm 5: Reliability model with Alternate path routing to active sink

Input: URNodes[],perc_unreliability,path[],AP[][],neigh[][], intermediate nodes u, v
// Node u sending the data packet to relay node v **Output:** AP-R[] ,drop_UR
//Reliable transmission of data packet with Alternate Path re-routing to currents sink
// h_i sends the data to h_j and watches h_j
if *Relay node* v *is a URNode* **then**
    if v *forwards the message* **then**
        update energy;
        discard the local copy from sender node u;
    else
        look for AP;
        if *AP found* **then**
            update the previous path with the AP;
        else
            Drop the message;
            drop_UR=drop_UR+1;

Algorithm 6: Reliability model with Alternate path routing to any sink

Input: active sink S_i, inactive sink S_j, neigh[][], intermediate node u
Output: AP-R[]
//Reliable transmission of data packet with Alternate Path re-routing to any sink
// Active sink - S_i and Inactive sinks - S_j **if** *neighbor of* u *is* S_j **then**
    temporary activation of S_j;
    reroute the data packet to S_j;
    update the energy consumption of node u;
    Increment the successful message delivery;
    Reactivate the previous active sink S_i;

Algorithm 7: Reliability model with optimal routing AP with ICR

```
Input: neigh[][], intermediate nodes u, v, hop skip
Output: AP-R[]
//Reliable transmission of data packet with Alternate Path re-routing with ICR
// h_i sends the data to h_j and watches h_j
if Relay node v is a URNode then
    if v forwards the message then
        update energy;
        discard the local copy from sender node u;
    else
        look for AP;
        if AP found then
            update the previous path with the AP;
        else
            Adjust the communication range to skip v and reach the next relay node
             of v say p if p is a URNode then
                if p not forwarding the message then
                    if AP not found then
                        if ICR upto the mentioned number of hop skips then
                            Drop the message;
                            drop_UR=drop_UR+1;
```

These algorithms continue until the network reach of sinks becomes 1, indicating that either the nodes do not have enough residual energy to communicate with the sink or the network has divided into multiple isolated chunks that cannot be connected due to energy depletion of hot spot nodes.

The network shifts the sinks using CASS to minimize the maintenance cost, and sink shifts occur according to the defined shift rate.

3.5 Experimental Results:

The experiments were conducted using MATLAB on networks of variable sizes deployed in a 100X100 grid. The simulations were initiated with a randomly selected set of unreliable nodes. All nodes, excluding the declared ones, as well as sink nodes, were considered to be reliable. A total of 30 test cases were conducted, progressively increasing the number

of sensor nodes and sink nodes deployed in the region. The data sets from Chapter 2 were utilized, and the reliability model was applied with different percentages of URNodes and percUR. Input parameter details are provided in Table 3.1.

Grid Size	100 X 100
Initial Energy of Sensors	10 Joules
Number of Sensors	100, 200, 300
Number of Sinks	4, 6, 8
Communication Range	15 units
Shift Rate	90%
Unreliable nodes	5% - 25% on total deployed sensor nodes with interval 5
Percentage of Unreliability	10% - 50% of the sensor nodes with interval 10
Number of iterations	25

Table 3.1: Input Data Information

The experiments were conducted using networks consisting of 100 sensors with 4 sinks, 200 sensors with 6 sinks, and 300 sensors with 8 sinks. Unreliable nodes were introduced at varying percentages, specifically 5%, 10%, 15%, 20%, and 25% of the total number of sensor nodes, with unreliability percentages set at 10%, 20%, 30%, 40%, and 50%.

Figure 3.1 to Figure 3.3 shows how the performance is impacted in the presence of URNodes. In the mentioned figures the performance of a WSN is measured with the output parameters total number of messages initiated by the sensors to send to the sink nodes, the number of messages received by the sinks altogether and the number of messages dropped in the network due to the URNodes. Experiments has done on 100 nodes, 200 nodes, and 300 nodes with multiple sinks as BS. With the increased number of URNodes and probability of dropping a message is 100% increases the number of messages initiated by the sensor nodes. When a sensor node tries to forward its sensed data through the relay nodes and on the occurrence of an URNode the messages get dropped which leaves the battery of relay nodes unused. With that remaining energy, the sensors could sense the environment and try to deliver a message to the sink. Like this, the messages initiated by the sensors increase with the increase in URNodes count.

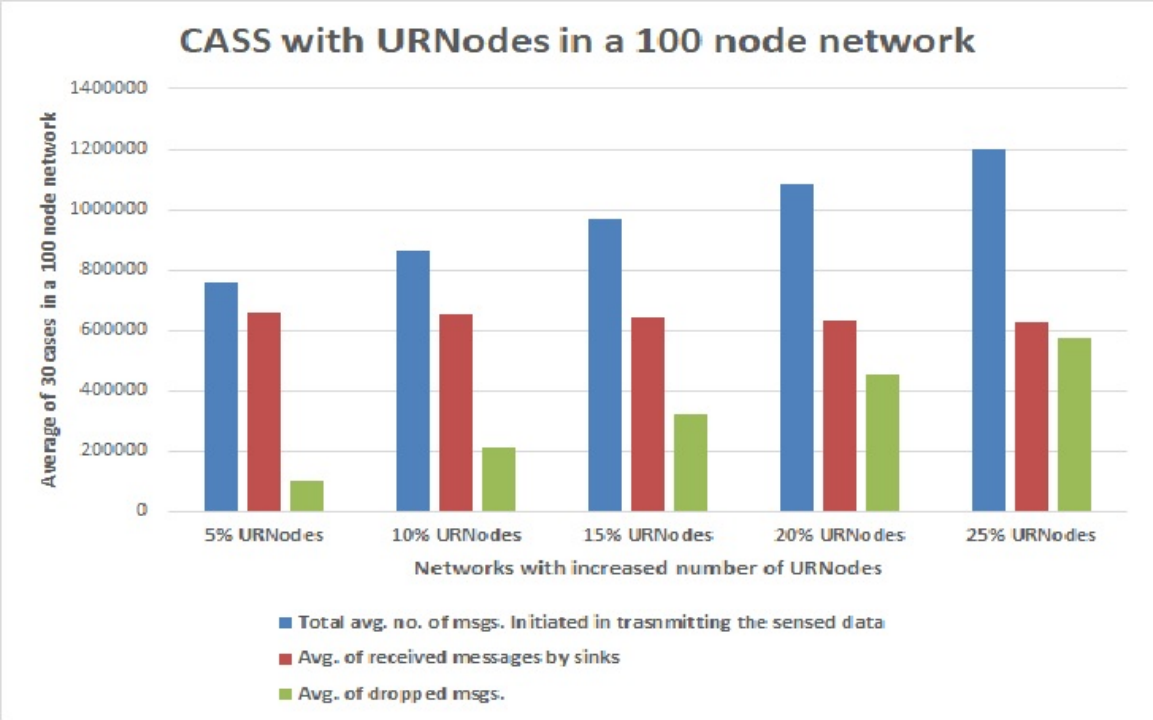

Figure 3.1: Performance of a network on a 100 node network with variable URNodes

Due to URNodes dropping tendency, the messages delivered to the sink are reducing with an increase in message drop count. This is experimented on a WSN by increasing the density from 100 nodes to 200 nodes and 300 nodes. Figure 3.2 and 3.3 show the worse condition of a WSN in the presence of URNodes while increasing in number. Studying dropped message parameters in 200 node and 300 node WSN the parameter increases more than half of the initiated messages with raise in URNodes. Figure 3.4, 3.5, and 3.6 gives a comparison study on 100 nodes, 200 nodes and 300 nodes taking the average of each parameter on 30 cases.

Experiments are done on 100 nodes, 200 nodes, and 300 nodes with a modified AP routing to ensure reliable data delivery on 30 cases for 25 iterations on each. Each case runs for one combination of URNodes with all combinations of percUR. Figure 3.7 shows the average of all output parameters in all possible combinations of URNodes and percUR. In figure 3.7, the first set of bar indicates the average of 30 cases for 25 iterations each with 5% URNodes and 10%, 20%, 30%, 40%, and 50% for the output parameter the total number

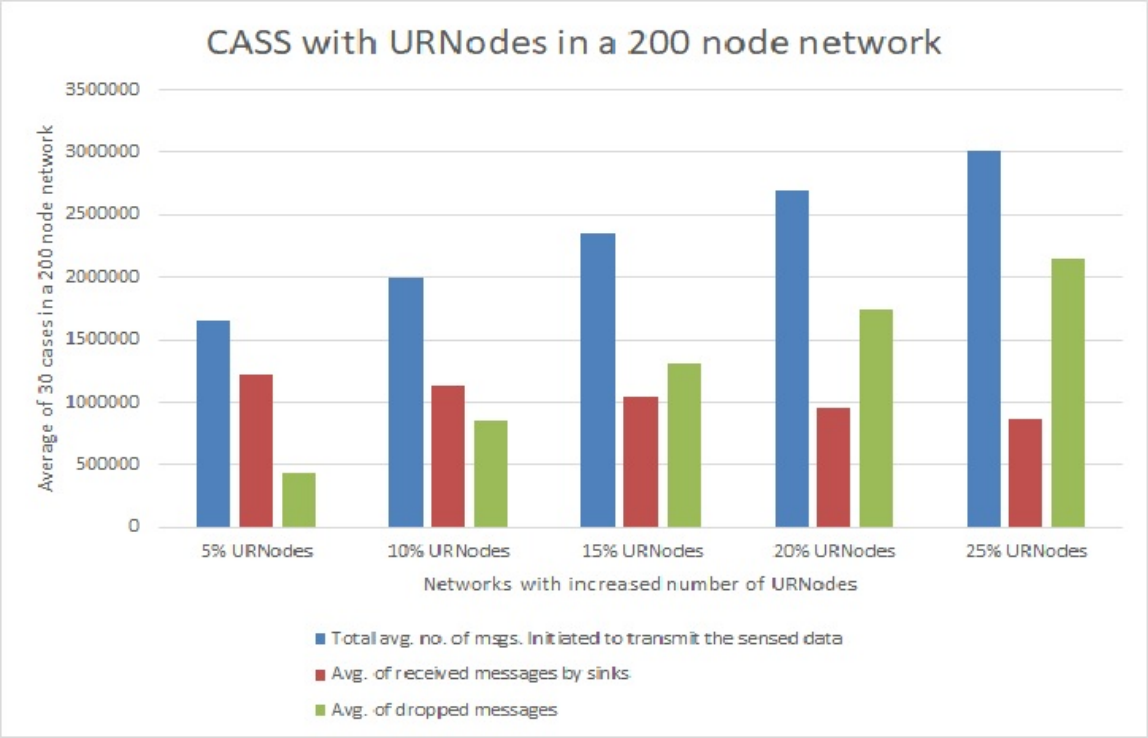

Figure 3.2: Performance of a network on a 100 node network with variable URNodes

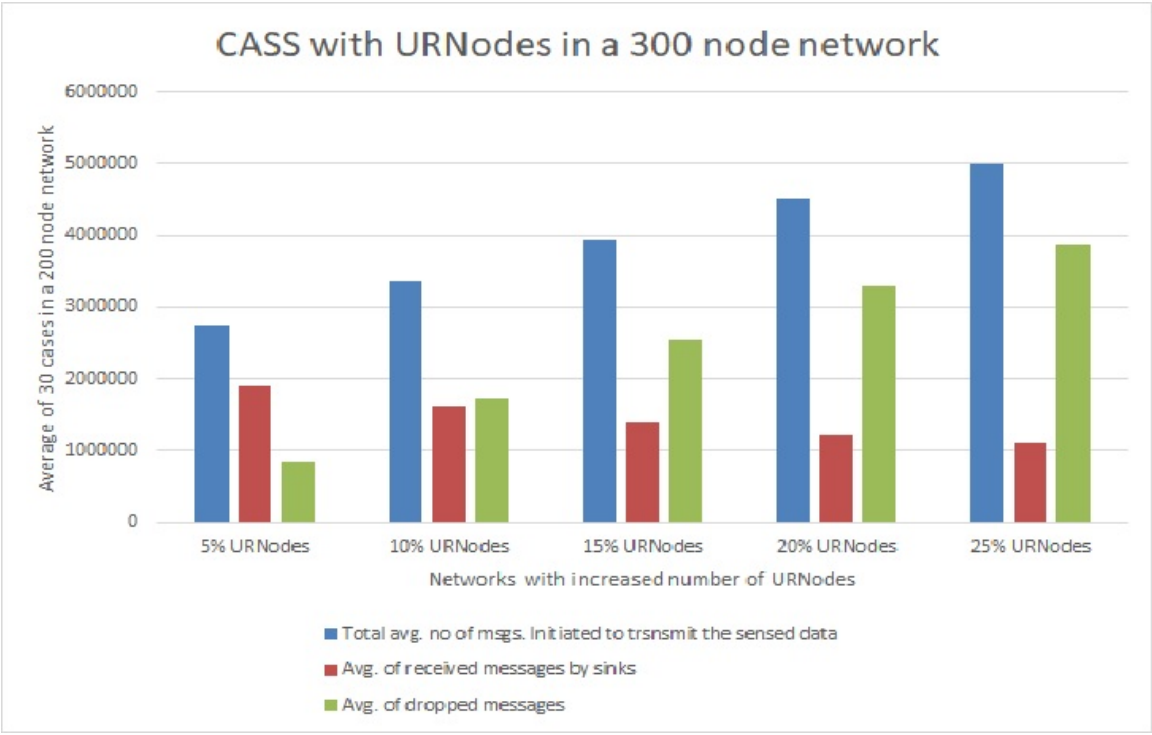

Figure 3.3: Performance of a network on a 100 node network with variable URNodes

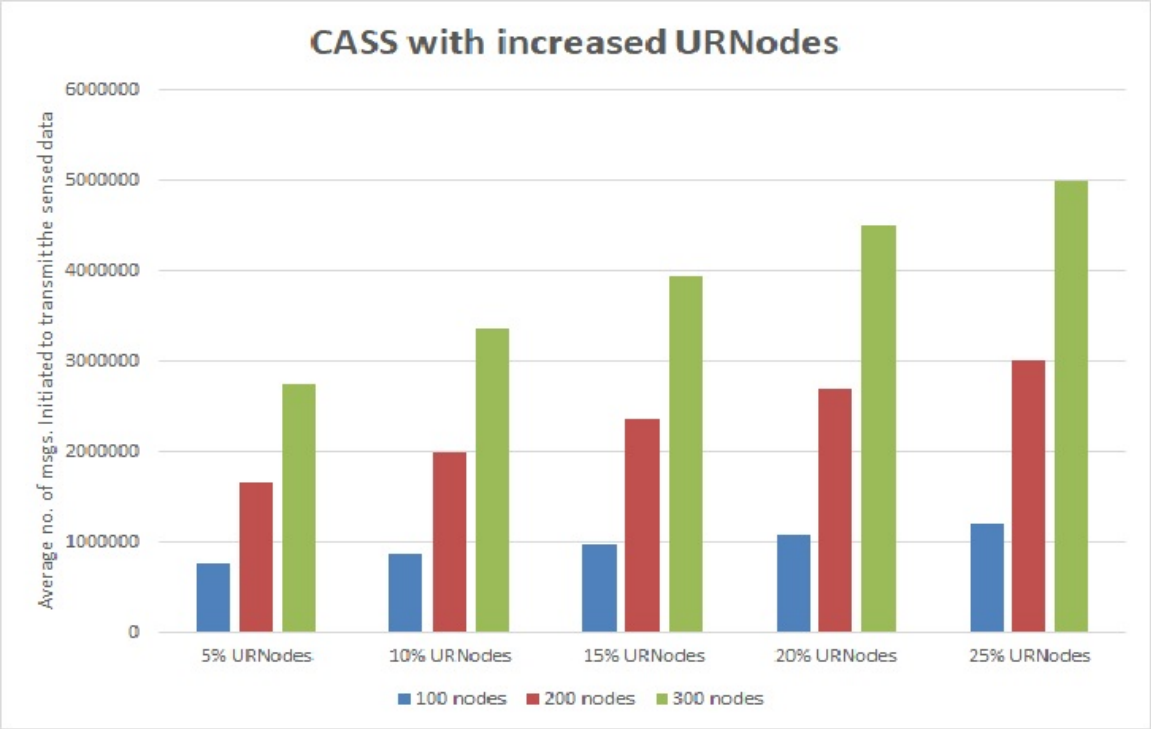

Figure 3.4: Performance of a network on a 100 node network with variable URNodes

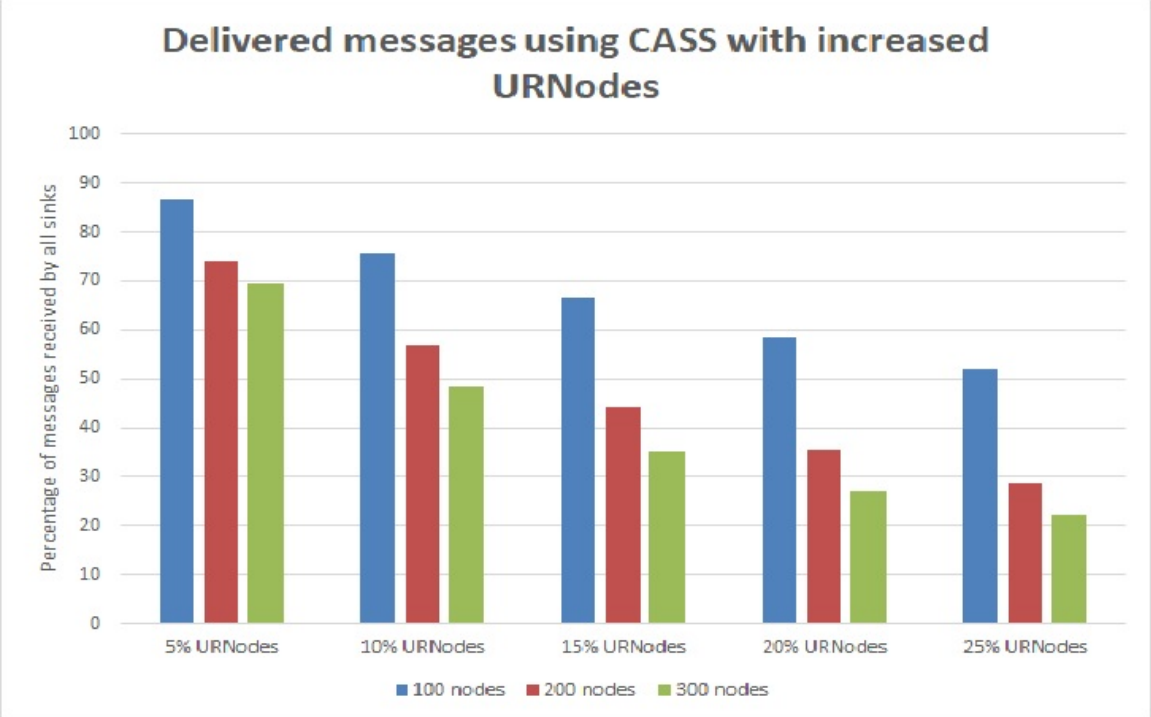

Figure 3.5: Performance of a network on a 100 node network with variable URNodes

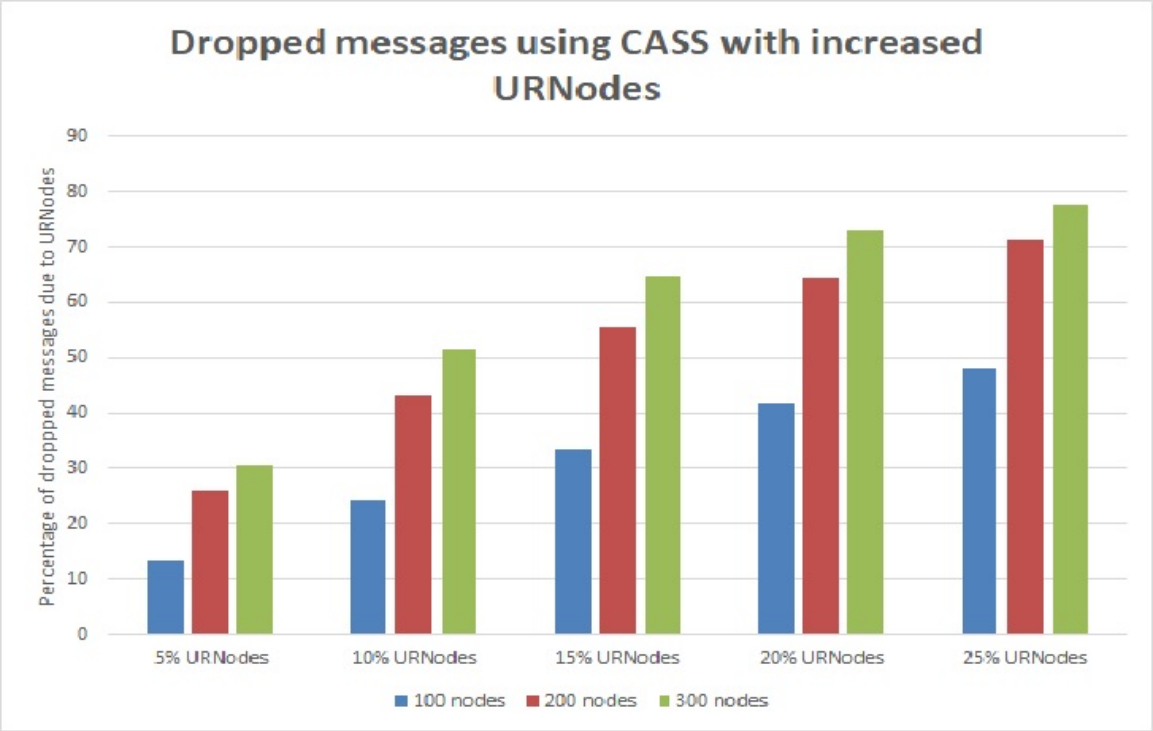

Figure 3.6: Performance of a network on a 100 node network with variable URNodes

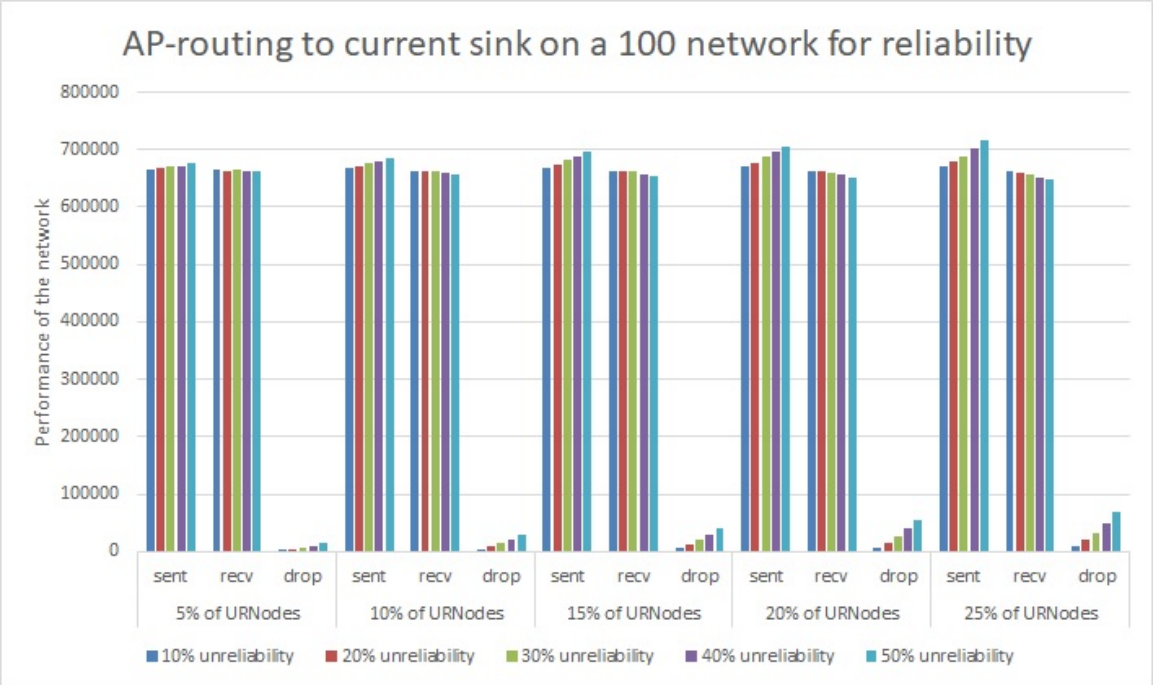

Figure 3.7: Performance of a network on a 100 node network with variable URNodes

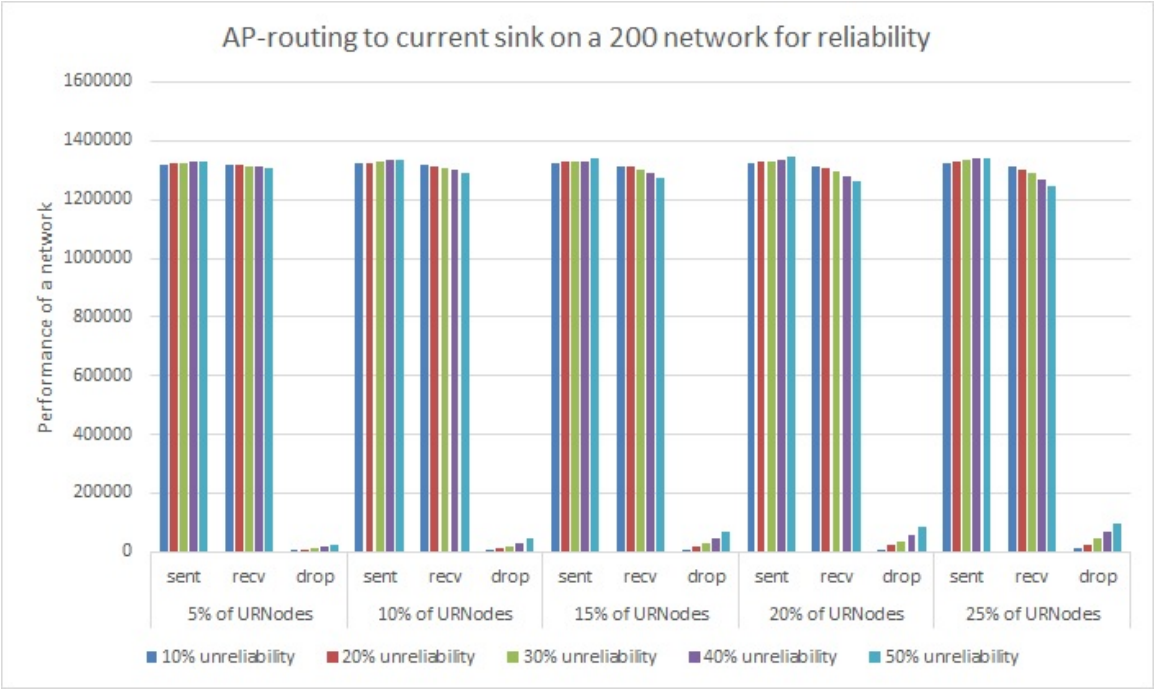

Figure 3.8: Performance of a network on a 200 node network with variable URNodes

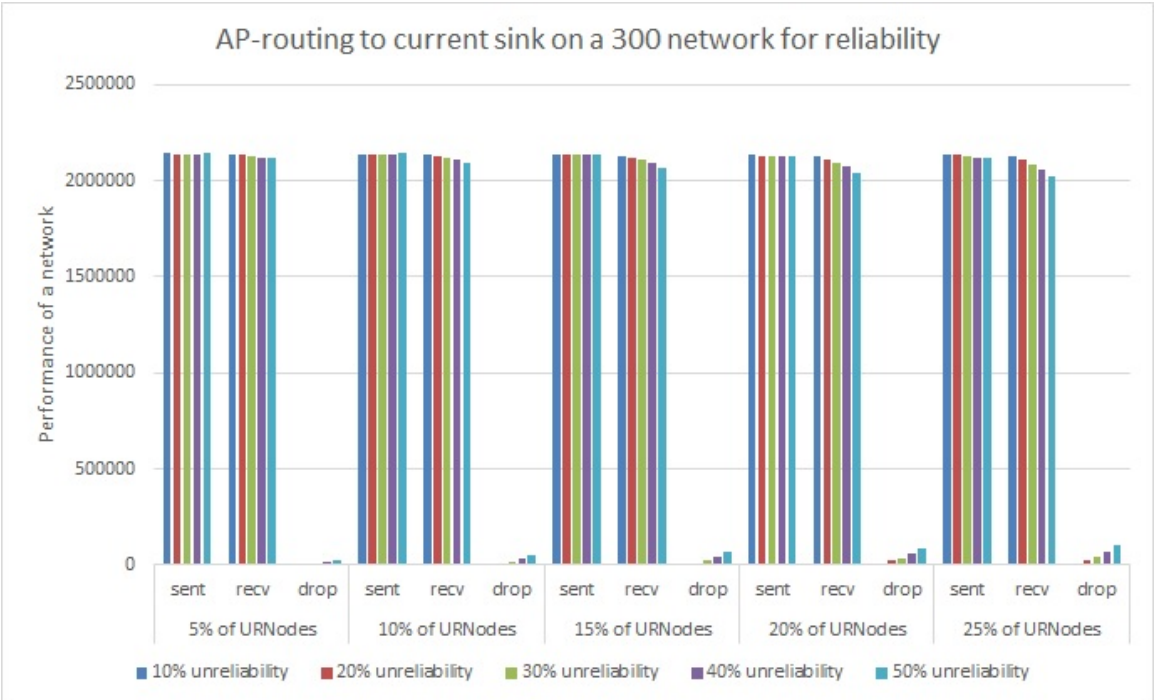

Figure 3.9: Performance of a network on a 300 node network with variable URNodes

of messages initiated to send by all sensors. The next two sets of bars indicate the average of the total received messages by sinks and the average of total messages dropped by relay nodes respectively on 30 cases with 25 iterations each on a 100-node network. This set of output parameters are continued to present with 10% of URNodes, 15% of URNodes, ..., 25% of URNodes with interval 5. With the increase in percUR the message drop gradually increases. In figure 3.7 the extreme set in the right end shows the raise in message drop with an increase in URNodes to 25% and percUR to 50%.

Observing figure 3.8, and 3.9 message drop is reduced with an increase in the density of sensor nodes. With an increased density in the network region, the AP routing algorithm explores more paths to reroute. This makes the AP routing show a remarkable improvement in reliable data delivery in terms of total messages delivered to the sink and reduction of message drop on a dense network with more number of URNodes and with high percUR.

Method	Number of Nodes	% of received messages	% of drop messages
CASS-R-Current			
	100	99.7 - 90.5	0.3 - 9.5
	200	99.8 - 92.7	0.2 - 7.3
	300	99.9 - 95.3	0.1 - 4.7
CASS-R-Any			
	100	99.8 - 94.6	0.2 - 5.4
	200	99.9 - 97.3	0.2 - 2.7
	300	99.96 - 98.6	0.03 - 1.4
CASS-R-C-ICR Hop skip 1			
	100	99.9 - 99.6	0 - 0.4
	200	99.9 - 99.6	0 - 0.4
	300	99.9 - 99.7	0 - 0.3
CASS-R-A-ICR Hop skip 1			
	100	99.9 - 99.91	0 - 0.1
	200	99.9 - 99.91	0 - 0.1
	300	99.9 - 99.95	0 - 0.04

Table 3.2: Summarized Results of CASS with all variations to re-route a message

Table 3.2 presents the percentage of received messages on average of 30 cases for 25 iterations on 100 nodes, 200 nodes, and 300 nodes WSN. In this table, a range is given for the percentage of received messages and message drops by taking the average percentage of

both parameters considering all possible combinations of URNodes and percUR. From this table, the NL measuring in messages received by all sinks, the ICR has shown almost close to 100% reliable data delivery for the initiated data messages. AP routing to any sink also improved the percentage of PDR when comparing with AP routing to any sink. In particular, the performance of AP routing to any sink is worth mentioning with 200 and 300 nodes WSN with 25% of URNodes and 50% of percUR.

3.6 Summary

This chapter focuses on the reliable data delivery issue, considering various percentages of URNodes and percUR. To maintain the NL of a WSN deploying multiple sinks in the network and minimize the maintenance cost of multiple sinks deployment, CASS comes with single sink activation at a time. Sink shift happens when an active sink loses its connectivity with other nodes of the network, and based on the network reach CASS chooses the next active sink. Considering three variations of re-routing to ensure the reliable data delivery with prolonged NL in the presence of a defined set of URNodes with different percUR. Variation 1 rerouting to the Current active sink outperforms the network with URNode where on encountering of a URNode the network drops the message and to recover the data packet applying re-transmission increases the congestion in the network and also wasting energy of sensor node by re-transmitting the data. Instead of dropping a message and re-transmitting the data to ensure reliable data delivery with increased congestion in the network and energy consumption of sensor nodes, AP routing re-route the data using shortest AP considering energy consumption. By re-routing the data the PDR increases with decreased drop rate. The variation 2- rerouting to any sink also helps the sensor node to efficiently utilization of energy by re-routing the data packet to the nearest idle sink instead of taking energy energy-consuming path to the current sink. Including ICR ensures 99.9% of reliable data delivery at the cost of reduced initiated messages to send a message.

While ensuring reliable data delivery with enhanced network lifetime in the presence of URNodes, the system neglected the hot spot nodes issue which highly impacts the NL of a WSN by making the WSN into small isolated chunks.

CHAPTER 4

Lifetime Enhancement and Reliable data transmission in presence of unreliable and hotspot nodes

4.1 Introduction

WSN is a network with several sensor nodes to get the data by sensing and sending to a sink for analyzing the data to take decisions by an end user [7, 8, 68]. The sensor node is constrained with a limited battery source and communication range to send the data. Sensor acts as data collector as well as data router [1, 7, 68]. Some sensors are involved in data transmission recurrently to forward it towards a sink. The energy of such nodes depletes quickly and makes them die prematurely. These hot spot nodes generally refer to the neighbor nodes of the sink as they act as data routers for nodes far from the sink rather than a data collector. Like these, there are other nodes, that keep the network connected. Such crucial connecting nodes drain their energy prematurely like hot spot nodes (sink neighbors) then the network divides into isolated chunks making the network less functional.

Neighbors of the sink node and connecting nodes both are important to prolong the NL of a WSN, which continues to be referred to as hot spot nodes. These hot spots are dealt with in Chapter 2 using AP routing to reroute the data packet by avoiding the hotspot node based on its residual energy. To enhance the NL, ICR plays a vital role when a network

becomes completely non-functional.

Reliable data delivery is one more major concern to deal with in a WSN as many of the applications demand to deploy a WSN in a remote area with harsh weather conditions where the deployment or maintenance can't be managed by a human directly [66, 67, 69]. Applications such as underwater applications, and battlefield applications demand reliable data delivery [1, 7, 65]. In Chapter 3, the algorithm works on reliable data delivery with enhanced network lifetime using a modified AP routing in the presence of URNodes while considering various probabilities of dropping a message by an URNode. AP routing helps to re-route the data packet if the URNode encountered in a routing path and drops the message due to heavy demand of processing [69]. From the literature survey, the proposed methods and protocols mainly focus on recovering the data after data loss by using re-transmission. Re-transmission increases the congestion in the network due to multiple re-transmissions. This re-transmission increases the message drop, re-transmitting the dropped data, and increasing congestion in the traffic with an increased number of sensor node deployments. One major side-effect of re-transmission is the wastage of limited resources of sensor nodes which decreases the NL of WSN.

Addressing hot spot nodes, and URNodes with different probability of message drop while enhancing the NL is a multi-objective challenge in WSN.

4.2 Literature survey

Reducing the hop count stands out as a compelling and effective strategy to optimize energy consumption in wireless sensor networks, ultimately enhancing overall network efficiency and longevity. The idea is that by minimizing the number of hops needed for data transmission, the energy burden on relay nodes can be alleviated, thereby reducing the risk of energy depletion in hotspots and extending the overall lifespan of the network. A viable alternative is to minimize the hop count, which in turn minimizes the energy consumption

of relay nodes, mitigating the risk of energy exhaustion in hotspots and improving the network's overall lifespan.

Introducing mobile sinks is another promising approach to minimize energy consumption and extend the network's lifetime. Mobile sinks help alleviate the creation of hotspots by moving around the network to collect data. However, a significant challenge in implementing mobile sinks is ensuring the rapid update of the sink's new location to the sensor nodes, enabling timely transmission of sensed data [45]. One effective option to achieve this is flooding [46] the new sink location. However, this can lead to increased traffic flow, congestion, message drops, and other issues.

In a different approach presented in [49], the authors designed the Cluster Heads (CH) with unequal sizes based on their distance to the sink. The CH farther from the sink has more sensors as members, while the CH closer to the sink has fewer members, resulting in lower energy consumption for the CH near the sink. This approach helps balance hotspots, preventing early exhaustion of energy in the network.

The above survey presents efficient routing and designing unequal size CH's helps in mitigating hot spot nodes early depletion problem. Here the simulations are done on homogeneous network nodes where a formation cluster is not an optimal solution to delay the premature death of hot spots of any kind. So finding optimal routing to avoid premature energy exhaustion of hot spots is an adaptable feasible method to mitigate hot spots as well as to prolong the NL.

The integration of technologies within the Internet of Things (IoT), such as Wireless Sensor Networks (WSN), edge computing, and cloud computing, addresses various applications such as environmental monitoring and disaster surveillance. However, IoT devices encounter challenges due to limited resources such as battery life, communication bandwidth, and processing capacities. Key concerns for data dissemination in IoT networks include load balancing, fault tolerance, as well as energy and memory efficiency.

To tackle these issues, [79] proposes a cross-layer optimization approach that incor-

porates data-centric storage into distributed data storage mechanisms. The Collaborative Memory and Energy Management heuristic, solved using a genetic algorithm, surpasses existing methods in diverse IoT scenarios by improving memory and energy efficiency while ensuring load balancing.

In the context of WSN employing multi-hop routing over error-prone wireless channels, traditional approaches keep all nodes active, leading to increased energy consumption. However, [80] introduces a sleeping multi-path routing approach that selects a minimal number of disjoint paths to meet reliability requirements. This strategy allows the remainder of the network to enter sleep mode, extending the Network Lifetime (NL) while achieving a balance between reliability and energy efficiency.

As mentioned in section 4.1, re-transmission of the data packet is not a feasible solution when comes to a denser network. Sleep-wake mechanism for multi-path routing helps the WSN to route the data to multiple sinks using different pathways by allowing the sink to sleep and wake based on the shift rate and network reach calculated by CASS. Proposed AP routing to re-route the data, handles both problems efficiently by balancing the load on the network and prolonging the life of hotspots with reliable data delivery and increased NL.

4.3 Proposed method:

System model assumptions, network model, energy model, reliability model, and ICR are considered in Chapter 2 and Chapter 3. Proposed AP re-routing is re-defined in the combination of hotspot nodes and reliability to enhance the NL of a WSN.

Presenting two variations of AP re-routing. One re-routing from source to sink which consumes energy for transmitting the control messages with acknowledgement (ACK) mentioning the residual energy of the relay nodes. This earlier analysis ensures reliable data delivery at the cost of energy spent for control message transmission. Another variant reduces the cost spent for the control message by re-routing the message from the previous

node of the hot spot node to sink. With this variation reliable data delivery comes to a volatile state. If the node looking for AP is unable to find a AP for re-routing then the message is either to be dropped or should be maintained in its internal buffer by locking the memory slot it delivers it. Every variant has its benefits with drawbacks.

The main aim of this work is it enhance the NL while minimizing the message drop. The message drops due to hot spot or URNode. But focusing on prolonged NL, minimizing the message drop is required and also for reliable data delivery.

Algorithm 10 details about the AP re-routing from sender to sink node to avoid the hot spot if the residual energy of the hot spot node falls below the threshold value. In the algorithm 10 refers h_i as a sending node which is the predecessor of hot spot h_j. The source won't take the responsibility of delivering the data packet. The sender node will take responsibility like a hop-by-hop method of ensuring reliable data delivery by using AP re-routing. If h_i is unable to find a feasible AP then the drops the message. In this scenario the successful delivery of a message on encounter of a hot spot node is uncertain.

But the Algorithm 2 in Chapter 2 ensures the reliable data delivery of sensed information. In this algorithm, if the source couldn't come up with an optimal AP then managing its own data is not a tough task for a source node. It can process its own data by using other alternatives such as data aggregation or data fusion to deliver the data with a recent update which improves the accuracy of the sensed data. For instance, WSN works for an event-based application where it expects enough messages to identify an event. The sensor nodes other than the source node can sense the common region to predict the event occurrence. The chances are low for misidentifying the event based on the received data.

As mentioned earlier in Chapter 1, the network collects the data periodically. Even if the source fails to send the data the other nodes can come with sensed data which is similar

to source sensed data.

In a multi-objective problem, the network prioritizes one objective over another. Here, dealing with hot spot nodes, URNodes with NL enhancement. Enhancing the NL is the

Algorithm 8: Alternate Path routing from sender to sink to avoid hot spot

```
Input: threshold,path[],AP[][],neigh[][], sender h_i, relay_node h_j
Output: AP-R[] ,drop_HS,drop_UR
if Residual_Energy(source) ≥ T_E then
    if path exists from source to sink then
        h_i check the threshold condition against the residual energy of h_j;
        if h_j is satisfying threshold then
            forward the message to h_j;
            update energy;
            discard the copy from h_i internal buffer;
        else
            look for shortest AP;
            if AP found then
                update the path[ ] with the new hop information;
            else
                Increment the dropping count due to unavailable AP to avoid hot
                  spot;
                drop_HS=drop_HS+1;
            end
        end
    else
        move to the next node;
    end
else
    move to the next node;
end
```

ultimate goal of this work with hot spot nodes and URNodes. In this work, after NL, the hot spot nodes problem is given priority over URNodes, because after observing the results from The Chapters 2 and 3, the existence of hot spot nodes plays a major role to maintain the network connectivity to prolong the NL. When all nodes fail to reach the sink within the specified threshold, the threshold is halved. This iterative process continues until the energy threshold reaches 10% of the initial energy. Subsequently, the network permits the hot spot to utilize its remaining energy.

Algorithm 9: Reliability model and hot spot nodes

```
Input: URNodes[],perc_unreliability,path[],AP[][],neigh[][], sender h_i, relay_node
       h_j
Output: AP-R[] ,drop_UR, drop_HS
//Reliable transmission of data packet with rerouting to shortest AP with hot spots
if Relay node h_j satisfies the threshold then
    Watch h_j behaviour as relay node
    if h_J is reliable (means the message is forwarding then
        update energy;
        discard the local copy from sender node h_i;
    else
        look for AP;
        if AP found then
            update the previous path with the AP;
        else
            Drop the message;
            drop_UR=drop_UR+1;
else
    Look for AP to avoid the hop spot;
    if AP found then
        update the previous path with AP;
    else
        Drop the message to keep the hop spot alive;
        drop_HS=drop_HS+1;
```

The Algorithm 9 is explains how to deal when the unreliable node is encountered and behaves as an unreliable node. But before reaching the state to know the reliability of a node, the Algorithm 8 checks whether the node satisfies the threshold condition to delay the energy exhaustion of a hot spot node. Based on that, if AP is not found the dropping will

Grid Size	100 X 100
Initial Energy of Sensors	10 Joules
Number of Sensors	100, 200, 300
Number of Sinks	4, 6, 8
Communication Range	15 units
Shift Rate	90%
Lower bound of Energy Threshold	10% of the Initial Energy
Unreliable nodes	5% - 25% on total deployed sensor nodes
Percentage of Unreliability	10% - 50% of the sensor nodes

Table 4.1: Input Data Information

be counted in their respective drop variable. When AP is looking by an URNode then the AP must clear the threshold condition then the probability of a node needs to be checked to ensure the hot spot nodes extended life with minimal re-routing to deliver a message.

The variations apply in Chapter 3 to re-route a message to any sink and ICR to ensure the reliability is also extended to this work.

4.4 Experimental Results:

The experiments were conducted in MATLAB using networks of variable sizes deployed in a 100x100 grid. The simulation initiates with a randomly selected set of unreliable nodes, and all nodes, except those in the designated set, including sink nodes, are assumed to be reliable. Thirty test cases of varying densities were examined, with different datasets generated by increasing the number of sinks relative to network density. Detailed parameter information is presented in Table 4.1. The experiments were performed on networks comprising 100 sensors with 4 sinks, 200 sensors with 6 sinks, and 300 sensors with 8 sinks. The URNodes ranged from 5% to 25% in increments of 5% of the total number of sensor nodes and from 10% to 50% in increments of 10 as percUR.

Presenting short forms of the variations used in this chapter, all variations using CASS for sink shifting, using AP to reroute the data on the occurrence of a URNode for reliable

Short form	Routing for reliability
CASS-C	current sink
CASS-A	any sink
CASS-C-ICR	current sink with ICR
CASS-A-ICR	any sink with ICR
Hot spot issue - Rerouting from Source to Sink	
CASS-C-HS	current sink
CASS-A-HS	any sink
CASS-C-HS-ICR	current sink with ICR
CASS-A-HS-ICR	any sink with ICR
Hot spot issue - Rerouting from the intermediate relay node to Sink	
CASS-C-HS-Relay-Sink	current sink
CASS-A-HS-Relay-Sink	any sink
CASS-C-HS-ICR-Relay-Sink	current sink with ICR
CASS-A-HS-ICR-Relay-Sink	any sink with ICR

Table 4.2: Abbreviations of variants in AP routing

data delivery. This is common for all variations and is shown in Table 4.2. Additional to addressing hotspot node issues by rerouting either from source to sink or from relay node to sink.

From Table 4.3 to 4.5 shows the NL received by two variations CASS-C and CASS-C-HS, and Table 4.6 presents the NL in percentage by taking the average of 30 cases in 100, 200, and 300 nodes in a WSN for all combinations of input parameters URNode and percUR on variations CASS-C, CASS-C-HS, Reliable data delivery using AP routing to any sink (CASS-A), Reliable data delivery and hotspot nodes using AP routing to any sink (CASS-A-HS), Reliable data delivery using AP routing to current sink with ICR (CASS-C-ICR), Reliable data delivery with hotspot nodes using AP routing to current sink with ICR (CASS-C-HS-ICR), Reliable data delivery using AP routing to any sink with ICR (CASS-A-ICR), and Reliable data delivery with hotspot nodes using AP routing to any sink with ICR (CASS-A-HS-ICR).

A comparative study between CASS-C and CASS-C-HS on NL is for 100 nodes, 200 nodes, and 300 nodes WSNs are presented from Table 4.3 to 4.5. On observing the performance of CASS-C-HS, dealing the hot spot problem along with URNode is beneficial

		Percentage of URNodes				
percUR	Title of the variation	5%	10%	15%	20%	25%
10% UR	CASS-C	99.7	99.5	99.2	98.9	98.6
	CASS-C-HS	99.9	99.7	99.5	99.4	99.2
20% UR	CASS-C	99.4	98.7	98.2	97.6	97.0
	CASS-C-HS	99.7	99.3	99.0	98.6	98.3
30% UR	CASS-C	99.0	98.0	97.1	96.0	95.2
	CASS-C-HS	99.4	98.8	98.3	97.8	97.2
40% UR	CASS-C	98.5	97.0	95.7	94.2	92.9
	CASS-C-HS	99.1	98.2	97.4	96.6	95.8
50% UR	CASS-C	97.9	95.9	94.0	92.1	90.5
	CASS-C-HS	98.7	97.6	96.3	95.1	93.8

Table 4.3: Comparison of received messages on a 100 node WSN in CASS-C and CASS-C-HS

when the network density increases and also the number of URNodes with highest percUR. Looking into the table 4.3 when 25% URNode exists in the network with increased percUR the improvement ranges from 0.6% to 3.3% in a 100 node network. Considering 200, and 300 nodes the improvement ranges 0.9% to 5.7%, and 0.4% to 4% respectively when comparing with CASS-C. Table 4.4 gives a range for NL for the mentioned variants. When we study the results the CASS-C-HS gives a prolonged NL than CASS-C. Dealing the multi-objective problem in a WSN considering hotspots, URNode with NL enhancement using AP routing addresses well by showing the improvement in NL and minimizing message drop.

The variants rerouting to any sink and ICR to skip a node has shown improvement over CASS-C. Also, when addressing the hotspot problem the NL the improvement is more visible even a WSN consists of more number of URNode with a high probability of message drop. Inclusion of ICR in the variants helps the network to deliver the messages almost cent percent. The message drop is negligible as the majority of the applications can tolerate dropping.

Table 4.7 presents the summarized results of both variants' rerouting from Source to sink and from the relay node to sink to mitigate hotspots problem in WSN. Rerouting

		Percentage of URNodes				
percUR	Title of the variation	5%	10%	15%	20%	25%
10% UR	CASS-C	99.8	99.6	99.4	99.3	99.1
	CASS-C-HS	100.0	99.9	99.9	99.9	99.8
20% UR	CASS-C	99.6	99.2	98.8	98.4	98.0
	CASS-C-HS	99.9	99.8	99.8	99.7	99.6
30% UR	CASS-C	99.2	98.5	97.9	97.2	96.7
	CASS-C-HS	99.9	99.7	99.6	99.5	99.3
40% UR	CASS-C	98.8	97.7	96.7	95.8	95.0
	CASS-C-HS	99.8	99.6	99.3	99.1	99.0
50% UR	CASS-C	98.2	96.5	95.1	93.8	92.7
	CASS-C-HS	99.6	99.3	99.0	98.7	98.4

Table 4.4: Comparison of received messages on a 200 node WSN in CASS-C and CASS-C-HS

		Percentage of URNodes				
percUR	Title of the variation	5%	10%	15%	20%	25%
10% UR	CASS-C	99.9	99.8	99.7	99.6	99.5
	CASS-C-HS	100.0	100.0	99.9	99.9	99.9
20% UR	CASS-C	99.7	99.5	99.3	99.0	98.8
	CASS-C-HS	100.0	99.9	99.9	99.9	99.8
30% UR	CASS-C	99.5	99.1	98.7	98.3	97.9
	CASS-C-HS	99.9	99.9	99.8	99.8	99.7
40% UR	CASS-C	99.2	98.6	97.9	97.3	96.8
	CASS-C-HS	99.9	99.8	99.7	99.6	99.5
50% UR	CASS-C	98.8	97.7	96.8	96.0	95.3
	CASS-C-HS	99.8	99.6	99.5	99.4	99.3

Table 4.5: Comparison of received messages on a 300 node WSN in CASS-C and CASS-C-HS

No. of nodes	Method	Range of NL in percentage	perc. of message drop
100	CASS-C	99.7-90.5	0.3-9.5
	CASS-C-HS	99.9-93.8	0.1-6.2
	CASS-A	99.8-94.6	0.2-5.4
	CASS-A-HS	99.9-97.8	0.1-2.2
	CASS-C-ICR	99.9-99.6	0-0.4
	CASS-C-HS-ICR	99.9-99.7	0-0.3
	CASS-A-ICR	99.9-99.91	0-0.1
	CASS-A-HS-ICR	99.9-99.9	0-0.1
200	CASS-C	99.8-92.7	0.2-7.3
	CASS-C-HS	99.9-98.4	0.03-1.6
	CASS-A	99.9-97.3	0.2-2.7
	CASS-A-HS	99.9-99.6	0-0.4
	CASS-C-ICR	99.9-99.6	0-0.4
	CASS-C-HS-ICR	99.9-99.9	0-0.1
	CASS-A-ICR	99.9-99.91	0-0.1
	CASS-A-HS-ICR	99.9-99.9	0-0
300	CASS-C	99.9-95.3	0.1-4.7
	CASS-C-HS	99.9-99.3	0.01-0.7
	CASS-A	99.9-98.6	0.03-1.4
	CASS-A-HS	99.9-99.8	0-0.2
	CASS-C-ICR	99.9-99.7	0-0.3
	CASS-C-HS-ICR	99.9-99.9	0-0.1
	CASS-A-ICR	99.9-99.95	0-0.04
	CASS-A-HS-ICR	100-99.9	0-0

Table 4.6: NL in percentage for all variation with possible input combinations

from source to sink when a node with below threshold encounters has prolonged NL than the variant rerouting from intermediate relay node to sink on variants of reliable routing listed here Reliable data delivery with hotspot nodes using AP routing to current sink, rerouting from Intermediate or relay node to Sink (CASS-C-HS-Relay-Sink), Reliable data delivery and hotspot nodes using AP routing to any sink, rerouting from Intermediate or relay node to Sink (CASS-A-HS-Relay-Sink), Reliable data delivery with hotspot nodes using AP routing to current sink with ICR, rerouting from Intermediate or relay node to Sink (CASS-C-HS-ICR-Relay-Sink), and Reliable data delivery with hotspot nodes using AP routing to any sink with ICR, rerouting from Intermediate or relay node to Sink (CASS-A-HS-ICR-Relay-Sink).

By observing Table 4.7, the rerouting from the intermediate relay node to sink for mitigating hotspots is unable to extend the NL than the routing from Source to sink. Comparing the NL of rerouting from the relay node to sink, the rerouting to any sink (for ensuring reliability) is improving than rerouting to the current sink. But increasing the density with respect to URNodes with high drop rate, the network behaves very abruptly in delivering the message as the nodes couldn't find an AP to reroute or even find after the URNodes probability of dropping a message is the influence factors to define NL. Looking at the percentage of message drop range the dropping due to hotspots and URNode together increase the drop rate. As mentioned earlier the message drop influences the NL. Though rerouting from the relay node to sink minimizes the cost incurred by control message in routing from source to sink to know the residual energy before initiating data transmission, that saved battery power is not effectively used because of dropping probability of URNode and looking for AP when triggering hotspot. Rerouting from the relay node to the sink doesn't promise reliable data delivery which impacts the NL.

Applying ICR, the node starts spending more energy when the paths are not available during the occurrence of hotspots and URNodes, which depletes the energy of sensor nodes by minimizing the messages initiated by the sink. But with ICR, reliable data delivery is

No. of nodes	Method	Range of NL in percentage	Range of message drop in percentage
100	CASS-C-HS	99.9-93.8	0.1-6.6
	CASS-C-HS-Relay-Sink	95.4 - 88	4.6 - 12
	CASS-A-HS	99.9-97.8	0.1-2.2
	CASS-A-HS-Relay-Sink	95.6 - 81.6	4.4 - 18.4
	CASS-C-HS-ICR	99.9-99.7	0-0.3
	CASS-C-HS-ICR-Relay-Sink	95.6 - 95.2	4.4-8.4
	CASS-A-HS-ICR	99.9-99.9	0-0.1
	CASS-A-HS-ICR-Relay-Sink	98 - 97.9	2 - 2.1
200	CASS-C-HS	99.9-98.4	0.03-1.6
	CASS-C-HS-Relay-Sink	90.9 - 87.9	9 - 12.1
	CASS-A-HS	99.9-99.6	0-0.4
	CASS-A-HS-Relay-Sink	95.5-90.6	4.5 - 28.5
	CASS-C-HS-ICR	99.9-99.9	0-0.1
	CASS-C-HS-ICR-Relay-Sink	91 - 90.6	9 - 9.4
	CASS-A-HS-ICR	99.9-99.9	0-0
	CASS-A-HS-ICR-Relay-Sink	98.3 - 98.3	1.7 - 1.8
300	CASS-C-HS	99.9-99.3	0.01-0.7
	CASS-C-HS-Relay-Sink	88.6 - 86.1	11.4 - 14
	CASS-A-HS	99.9-99.8	0-0.2
	CASS-A-HS-Relay-Sink	96.4 - 73.4	3.6 - 26.6
	CASS-C-HS-ICR	99.9-99.9	0-0.1
	CASS-C-HS-ICR-Relay-Sink	88.7 - 88.3	11.3 - 11.7
	CASS-A-HS-ICR	100-99.9	0-0
	CASS-A-HS-ICR-Relay-Sink	98.6 - 98.6	1.4 - 1.4

Table 4.7: Comparison study between the variants to address hotspots issue

ensured but not more than routing from source to sink while delaying the premature death of hotspots.

4.5 Summary

After analyzing and understanding the results, giving priority to hot spot nodes over URNodes improves the number of messages delivered to the sinks altogether and also rerouting from Source to sink making the network more reliable for data delivery. The advantage of rerouting from source to sink to deal with hot spots problem is observed when more URNodes with high percUR the lifetime enhances from 2% to 6% approximately. With the improved NL dealing hot spots along with URNodes is beneficial when the rerouting starts from the Source node. Increasing the sensor nodes density in the deploying region the AP routing works efficiently even with increased percUR. ICR helps in improving the NL in terms of messages received by sinks together. Message drop and message delivery influence NL directly and inversely proportional to each other to enhance the NL. Minimization of message drop improves the PDR and vice versa.

To mitigate hotspots, routing from source to sink delays the premature death of the hotspots. However, it takes energy for control messages to know the residual energy of all involving relay nodes prior to the data transmission. To avoid energy consumption, we came up with a variant rerouting the data packet from the relay node after encountering the hotspot. With this re-routing the variants save the energy consumption for control messages, but, the energy is not well utilized due to the hotspots and URNodes. With the hotspots, the AP routing comes with a new path without ensuring the data delivery due to again re-occurrence of hotspots or URNodes. The routing from the source-sink is more beneficial in the presence of URNode as it handles the hotspots better than re-routing from the relay node.

ICR is always an optimal solution to enhance the NL with a reduction in messages to initiate due to more consumption of energy due to adjusting the communication range.

Irrespective of the variant the algorithm with ICR increases the NL when compared to rerouting either to the current sink or any sink.

CHAPTER 5

Trust-based Identification of Compromised Nodes and Improved Reliable Data Communication

5.1 Introduction

WSNs are equipped with less expensive, tiny, self-organized, and effective functioning sensors. The sensor is a battery-based device to senses and communicates with other nodes. It uses a radio channel for data transmission which itself constrained with limited communication range. It makes the sensors rely on other nodes for data transmission which consumes more energy of relay nodes in forwarding the data than sensing. In the target region, after deploying the sensors, due to the above-mentioned limitations, the battery (energy) has to be utilized efficiently to continue the network functioning [1].

To enhance the NL, deploying multiple sinks is one of the alternatives, and sensed data can be sent to any of the sinks. Deploying multiple sinks increases the maintenance cost and this is well addressed in [2] using the CASS by activating a single sink at a time. CASS uses the cluster size as a key factor in selecting a new sink during the sink shifting [2].

But in CASS, the hot spots (neighbor nodes of the sink and other relay nodes that play a vital role in transmitting the data in the whole network) energy drains quickly, and the

network is no longer functional even though the network has sensor nodes with sufficient residual energy. This issue is handled effectively in [5] by using alternate paths to reroute the data by using other nodes' residual energy. By doing so, the NL not only increases by 8.75% but also handles the hot spots issue efficiently.

Unattended sensors can be easily tampered with and make the node malfunction. Applications like battlefield surveillance strongly recommend reliable data delivery without losing or tampering with the data not even in partial [6]. The existing security mechanisms are not suitable for WSNs due to their constrained resources. In this paper, a Trust mechanism has been proposed based on the node behavior during data transmission. In the initial setup of the network, every sensor node is considered to be trustworthy in a moderate state, and its value is either increased or decreased based on the successful or unsuccessful data transmission of the message respectively. The trust model works based on direct and indirect trust to identify the CNs and compromised link (CL)s. A Direct trust between any two nodes is the value counted based on the interactions that happen between them during data transmission. The Indirect trust value is calculated based on the influence of the neighbor nodes of sending nodes during their data transmission with relay nodes. The trust values are considered in the range of [-1, 1] where -1 indicates complete non-trustworthy node, 1 indicates full trust, and 0 is moderate trust [84].

In the proposed approach indirect trust plays a vital role in identifying the CLs and also identifies the CN if the total number of CLs of a faulty node exceeds the pre-defined threshold value. The unreliable communication link between two sensor nodes is defined as the unreliable behavior of the relay node shown towards a sending node only. If the relay node drops a message instead of forwarding it to its next node, it shows the unreliable behavior of the relay node [85]. The reasons for unreliable behavior can be congestion in the network, memory buffer overflow, and sometimes node tampering to disturb the network functionality. The first two reasons exist temporarily for a short period, but this behavior of a tampered node continues by taking the unreliability as an advantage. A CN's behavior

affects the network performance parameters such as reliable data delivery, and the NL. Identifying and excluding the faulty node is crucial for reliable data delivery, and enhancing the network functioning [85, 86, 87].

Combining the alternate path approach and the trust mechanism with CASS ensures reliable data delivery, and NL enhancement. These combinations help the network to identify and remove faulty links and rouge nodes with the help of indirect trust.

5.2 Background

A Wireless Sensor Network (WSN) comprises distributed sensor nodes that collaboratively monitor physical and environmental conditions. These nodes, with limited communication capabilities, computational power, and memory, are deployed in the environment to detect events and report to the cluster head or base station [1]. Due to their wireless nature, these nodes are vulnerable to various attacks. Consequently, the establishment of a trust framework addressing security, reliability, privacy, robustness, authentication, and authorization in WSNs is crucial. In this context, trust refers to the level of assurance or confidence one node can have in another within the network [84]. The trust values in a WSN range from -1 to +1, where -1 denotes complete untrustworthiness, 0 represents moderate or acceptable trust, and +1 indicates complete trustworthiness.

In the context of WSNs, trust is defined as the ”combined characteristics model for providing security, reliability, privacy concerning mobility.” The establishment and evaluation of trust in a WSN facilitate secure and reliable communication among nodes or networks based on their trust values. Assessing the trustworthiness of nodes in the network addresses challenges related to secure routing, ensures dedicated paths for packet transmission, and assists in the selection of a secure mobility model. Determining trust values is particularly critical in challenging and military environments where sensor nodes are deployed. The evaluation of trustworthiness between nodes is essential for establishing secure communica-

tion [86]. The challenges associated with ensuring security and dependable communication within a sensor network are explored through the lens of trust evaluation.

The trust initialization process starts either at the construction of a network or when a node enters a network. In establishing trust within a WSN, three distinct approaches can be employed. The first approach involves considering all nodes as trustworthy, providing a rapid method for trust establishment but carrying the risk of assigning higher trust values to potentially malicious nodes. This approach is practical for non-critical network deployments, such as temperature monitoring. The second approach treats all nodes as untrustworthy, resulting in a slower trust-building process but offering high robustness. This method is suitable for critical mission networks, especially in scenarios like battlefield deployments. The third approach considers all nodes as neutral, placing them in a middle ground between trustworthiness and untrustworthiness, offering a balanced perspective compared to the other methods.

5.2.1 TRUST PARAMETERS AND METRICS

The calculation of a node's trust value in a Wireless Sensor Network is influenced by various parameters and metrics, including transmission range (the distance a node can send packets), packet loss (indicating malicious data packet losses), energy consumption (for mobility and data fusion), latency (average time for data packets to reach destinations), optimal path/path quality (ratio of hops in the optimal path to actual path), node positions/spots, hop count (number of nodes traversed by a packet), Signal-to-Noise Ratio (SNR), and Bit Error Rate (BER). These factors collectively contribute to the trustworthiness assessment of a node within the network.

5.2.2 Trust properties

Given properties help to model the trust efficiently [87].

1. Subjectivity of Trust: Trust is subjective, influenced by the observations and evidence available to a node in a specific situation.

2. Link to Risk: Trust is closely linked to risk; there is typically no reason to trust if no risk is involved.

3. Intransitivity of Trust: Trust relationships are not necessarily transitive. If node A trusts node B and node B trusts node C, it doesn't automatically imply that node A trusts node C. Trust can be indirect in such cases.

4. Dynamic Nature of Trust: Trust is dynamic and can change over time based on new evidence or experiences. It may increase or decrease over time.

5. Asymmetry in Trust: Trust between two nodes does not have to be mutual or symmetric. Nodes may have different levels of trust in each other.

6. Reflexivity of Trust: Every node inherently trusts itself; trust is reflexive in nature.

5.2.3 Trust model and attributes

In a WSN, the trust value of a node, as described in [88], is contingent on security, mobility, and reliability attributes. The security model within the trust framework assesses a node's trust value based on the implementation of a secure routing protocol and packet encryption for routing. A high trust value is assigned when these security measures are employed, contrasting with a trust value of zero in their absence. The mobility model in the trust framework is influenced by a secured mobility model, awarding a node a high trust value when it ensures secured mobility and minimal energy consumption during mobility. Conversely, the trust value in the mobility model is set to zero in the absence of these features. In the reliability model, a node achieves a high trust value when it incorporates data fusion techniques for packets with lower energy consumption [89].

5.2.4 Trust Calculation

The quantification of trust in a network, as discussed in [86], can be expressed as a continuous variable within the range of -1 to +1 or categorized using labels such as low, medium, high, and very high trust. When a node receives a communication request, it follows a two-step process to calculate the trust value of the requesting node, aiming to establish trusted communication. The first step involves determining the node's trust value by assessing past interactions and recommendations from neighboring nodes, resulting in the calculation of the indirect trust value. If the initial trust value is considered sufficient, the node proceeds with communication tasks. However, if the initial trust value is deemed insufficient, the node initiates the second step, involving the calculation of the direct trust value [86].

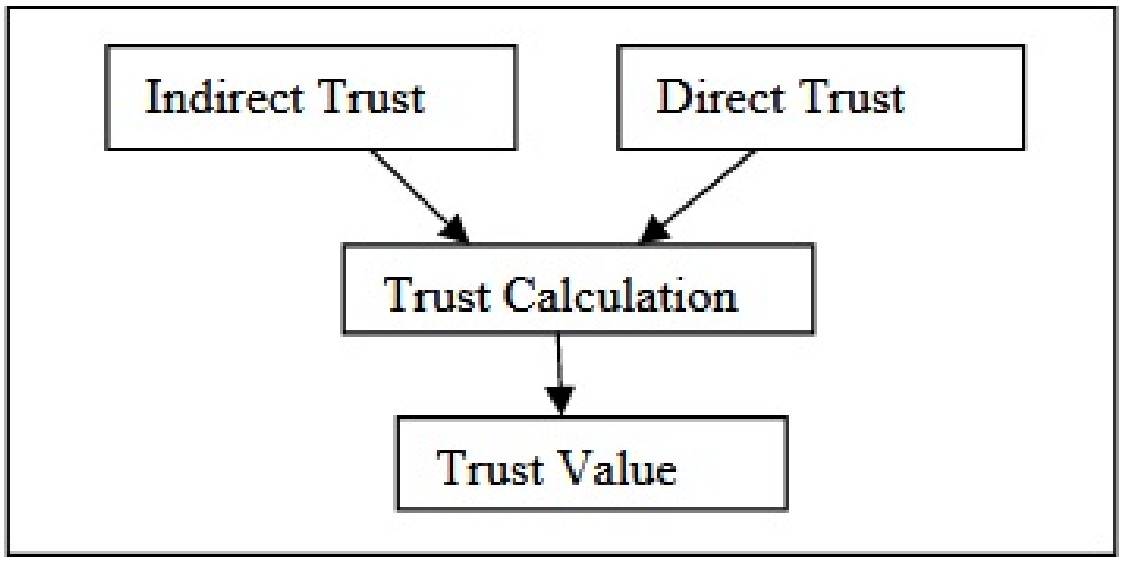

Figure 5.1: Trust calculation

The direct trust calculation involves assessing three models: the node's security model, mobility model, and reliability model. If the trust value from the security model is deemed sufficient, communication is initiated; otherwise, the evaluation extends successively to the mobility model and then the reliability model. If none of these individual trust values meet

the criteria, the node calculates the total trust by combining the indirect and direct trust values. If the overall trust value falls below the threshold, the communication request is rejected. The accompanying table delineates potential trust values and their corresponding implications for communication.

5.2.5 Types of attacks

WSNs find applications in various domains, including military, environmental monitoring, traffic management, and surveillance. These networks aim to sense the environment and relay information to a base station. However, the inherent vulnerability of sensor nodes, which are often left unattended and lack tamper resistance, makes WSNs susceptible to internal attacks. Traditional cryptographic mechanisms are limited in addressing these internal threats due to the independent nature of sensor nodes and the absence of a centralized authentication server.

Several types of internal attacks pose challenges to WSN security, including packet modification attacks, on-off attacks, bad-mouthing attacks, and collusion attacks.

- Packet Modification Attacks: Malicious nodes alter the content they receive before forwarding it to the next node.
- On-Off Attacks: A malicious node alternates between good and bad behavior intentionally, making it challenging to detect this alternating behavior.
- Bad-Mouthing and Collusion Attacks: These attacks exploit indirect trust computation methods that use recommendations from neighbors. In a bad-mouthing attack, a malicious node provides false recommendations to decrease the trust of a target node. Collusion attacks involve nodes forming a group to artificially boost mutual trust values, presenting themselves as legitimate nodes.

While existing trust-based approaches in WSNs show promise, some models struggle to identify abrupt changes in node behavior and promptly recognize behavioral alterations.

Trust models often rely on direct observations of a node's behavior and the sharing of these assessments as recommendations with neighbors to establish trust. Despite the challenges, trust models have demonstrated effectiveness against internal attacks.

5.3 Literature survey

WSN) face security challenges in open environments, such as node compromise. Traditional encryption methods encounter difficulties when key security is uncertain. [90] propose a cooperative security mechanism where trustworthy nodes collaboratively identify malicious nodes through inter-node voting based on observed behavior. This approach provides a robust solution for securing WSN in open environments, addressing key security concerns. Another study by [91] introduces a trust mechanism evaluating communication and data trust. Effective against various attacks, it employs direct and indirect trust assessments, demonstrating its robustness. [92] utilize direct observations and recommendations in a trust management scheme, yet it lacks differentiation between recommendations, making it susceptible to attacks. To counter bad-mouthing attacks, [93] introduce Reputation-based Framework for Sensor Networks (RFSN), propagating only positive reputation, mitigating negative collaboration. Trust and Energy-aware Routing protocol (TERP) by [94] focuses on communication trust, utilizing a weighted average of trust, residual energy, and hop count for route establishment.

In WSNs, ensuring data integrity is crucial. [95] validate data consistency by comparing a node's data with redundant data from neighbors, considering factors like location and energy. [96] leverage correlations among sensor readings to establish a correlation network for trust assessment, acknowledging its complexity. [97] propose a comprehensive model incorporating communication, data, and energy trust, facing challenges in practicality and computation. [98] introduce a group trust management scheme, assessing trust for the entire group, but it poses challenges in detecting malicious nodes if a cluster head is compromised.

Energy efficiency is a key concern in WSN protocol design. [99] present ADP, an adaptive energy-efficient approach that dynamically adjusts sleep and wake-up cycles based on a cost function, effectively enhancing energy efficiency while minimizing reporting latency under varying traffic loads.

In [100], the authors proposed a two-hop relay node communication to deliver the data packet from a source node. A sensor node selects a relay node based on the RESR criterion which includes residual energy, security (trust) value, and relay probability to meet the destination node. The neighbor node with high probability will be considered as a relay node by the source node. With this approach, the relay node has been chosen based on RESR criteria which helps the network to increase the lifetime. Though the routing algorithm considers the initiator node, destination node, and transmission range which acts as inputs with RESR criteria, it is highly difficult to deal with dense networks with mixed security issues [101].

In [102], the authors present a lightweight, fully-distributed model to enable the detection and recovery from network-level attacks particularly at tampering with the message security issue. It is a self-reference trust model where the node listens to its neighbor's behavior and analyses the network traffic at different time intervals. By overhearing, the message-sending node builds a profile on the relay nodes and makes a decision in message transmitting. During a network attack, if the nodes observe a big difference in two consecutive time intervals then the node will decide to collaborate with its neighborhood and avoid the affected region by changing its communication routing pattern.

[103] proposes a weighted trust approach, where each node, including the sensing node, cluster head, and relay node is assigned a trust value based on their behavior. The cluster head aggregates the collected data from sensing nodes and forwards it to a relay node to deliver it to the sink. The trust value is decreased if the node shows faulty behavior. If the trust value falls below the threshold, then the node is identified as a malicious node. The authors consider two scenarios, one with a single cluster head with no grid structure and the

other with multiple cluster heads with a non-overlapping grid and the results have shown that the approach works well with the second scenario.

5.4 System model

5.4.1 Assumptions

- sink nodes S with infinite energy and can communicate with the end user / outer world and with each other for the benefit of the network functioning
- In the initial setup no faulty node is deployed
- Every sensor node is equipped with an implicit acknowledge (iACK) to monitor/overhear its neighboring node's behavior [85].
- every node ensures the hop-to-hop reliability [85]
- all nodes are considered to be unreliable up to a predefined value during data transmission of a message [85]
- Lifetime of a network is defined to be the total number of messages received by the sinks altogether [5, 85]

5.4.2 Network model

The network is modeled as a graph $G(V, E)$, where V is the set of all sensor nodes say N, and the base stations/sink nodes S i.e. $V = N \cup S$. The sensor nodes and sink nodes are dropped randomly in the target region. As soon as the sensor node hits the region, it sends a hello message to know its neighbors and the sink sends a setup message to every node to know the shortest path to reach it for efficient use of energy. This shortest path is referred to as the initial path in further explanation.

After the network setup phase, the CASS algorithm is used to find the network reach of all the sinks. In the initial phase of the network, all nodes are in good condition in terms of energy and trust. So any sink can be set to active in the beginning. When the nodes start to drain their energy and the network is reorganized based on the shift rate, then CASS is more efficient in choosing the next active sink. Mainly CASS identifies the sink based on

- the number of nodes in cluster reachable by a sink
- direct neighbor nodes of the sink and
- nodes reachable by the sink but not in a cluster

The network reach is calculated based on the above three factors and gives more weight to the cluster size.

An energy model is considered to calculate the energy consumption in transmitting and receiving a $k-bit$ message to a distance d based on radio characteristics assuming that the energy consumption between node U to node V is symmetric. [2, 5, 42, 85].

5.4.3 Trust model

On successful data forwarding from node U to node V, node U complements node V by increasing the trust between them, and on message drop node U punishes node V by decreasing the trust between them. The trust model considers two kinds of trust, Direct and Indirect trust. Direct trust is the value obtained from past interactions between U and V and Indirect trust gets from the recommendations of neighbor U on node V. In this paper, trust value ranges from [-1,1] [84] and moderate trust of a node is indicated by 0.

If the trust between sending node U and relay node V is in the acceptable range i.e., $trust(u, v) \geq 0$ then the relay node will receive the message from sender U. Otherwise, the sender U looks for an alternate path using other neighbor nodes of it. The neighbor node with maximum residual energy and minimal hop count among all possible paths to reroute

the data will be considered as an alternate path and the message will be en-routed using an updated routing path.

If direct trust is not enough to consider node V as a relay node then node U gets recommendations from common neighbor nodes of both U and V to decide node V. But, if node V is behaving like a compromised behavior with U then the indirect trust value is not very helpful in routing the data. So, the proposed approach considers indirect trust only in identifying the faulty paths and faulty nodes.

5.4.4 Identifying the Fault Nodes

In this work, the nodes are considered URNodes due to internal system issues. However, some nodes are turned into malicious nodes and do denial of service attacks by not forwarding the data to the next node though it received the message correctly and has enough energy, and buffer space to handle and can be scheduled to forward the data. Such nodes are to be identified [90, 102, 103] to ascertain network efficiency along with reliable data delivery.

Indirect trust value and percUR of a node are the two key parameters in finding the CL and node. Sender node U considers the indirect trust, and if V is not reliable though the trust between them is moderate or above and V showing reliable behavior with other nodes and V is showing unreliable behavior in the defined range then node U considers the link with V as compromised after monitoring its behavior for a specific time interval. If node V behaves well during the monitoring period then node U proceeds with V as a relay node for data transmission. Showing the unreliable behavior with a defined range of neighbors of V and disconnecting the communication link with node V node V is considered to be a fault node and will be discarded from the network by announcing the same by broadcasting a notification to the entire network.

5.5 Proposed Algorithms

In the initial network phase, the nodes are randomly deployed in the target region with limited energy sensors. All sensor nodes are assumed to be in good condition at the time of deployment and equipped with the iACK technique to monitor other nodes. Trust between the neighboring nodes is considered to be moderate i.e., starting with 0 trust value. The trust value is either incremented or decremented based on the behavior shown by node V at the time of data transmission. Multiple sinks are deployed in the network assuming with infinite power supply and able to deliver the data to the end user. Using the CASS approach the sink selection process will be continued when the sink meets the defined shift rate. Meanwhile, the other sinks are in a passive state.

Algorithm 10 explains how a sender h_u considers the next node h_v to count for data forwarding. If no alternate path (AP) is found then the message drop be counted in drop_UR and presented in Algorithm 12. When node h_v shows unreliable behavior the h_u has to know the reason behind this kind of behavior due to the vulnerable nature of sensors while ensuring reliability. At this point h_u starts monitoring h_v behavior collaborating with other common neighbors and the overall behavior of h_v during data forwarding and presented in Algorithm 11. It will take a count of the total common neighbors and the number of neighbors

with satisfying trust. It gets compared with the defined percentage of neighbor's trust. Similarly by watching h_v behavior the h_u comes to know the unreliable nature shown by h_v is within the range. This routine will continue till the monitoring period completes or the h_v starts behaving reliably with h_u. During the monitoring time if h_v behaves reliably with h_u, then h_u considers that h_v has shown unreliability due to internal system issues. On completion of the monitoring period, if h_u comes to know the h_v is behaving well with all other nodes in the network then h_u removes h_v from its neighborhood as it showing fault behavior only with h_u. h_v shows unreliable behavior with other neighbors

Algorithm 10: Trust Computation

Input: initial_path[],trust[][],AP[][],neigh[][], sender h_u, relay_node h_v
Output: AP-R[] ,drop_trust, drop_AP
forwards the data message from h_u to h_v;
if $trust[h_u][h_v] < 0$ **then**
    if h_v *is reliable* **then**
        increment $trust[h_u][h_v]$;
        discard the copy from h_u internal buffer;
        update the residual energy;
    else
        decrement $trust[h_u][h_v]$;
        monitor node h_v;
        look for the shortest AP to the sink;
        if *AP found* **then**
            update the path[];
        else
            update drop_AP;
            //Dropped message count for no AP found
        end
    end
else
    look for the shortest AP to the sink;
    if *AP found* **then**
        update the path[];
    else
        update drop_trust; //Dropped message count for no AP found
    end
end

Algorithm 11: Monitoring a node

Input: perc_unreliability, neigh[][], sender h_u, relay_node h_v, perc_neigh_trust, perc_neigh_count_relayNode
Output: $neigh[h_u][h_v]$
forwards the data message from h_u to h_v;
if $trust[h_u][h_v]$ ¿ *0 and* h_v *is behaving unreliable* **then**
    monitor h_v;
    find the common neighbors of h_u and h_v;
    count the neighbors with $trust \geq 0$;
    calculate the percentage of Neigh. Trust say X;
    if $X \geq perc\_neigh\_trust$ **then**
        neigh_trust=1;
    end
    check the percUR of h_v during data transmission say Y;
    if $Y \leq perc\_unreliability$ **then**
        UR_range=1;
        //within the defined unreliability (UR) range
    end
    $z = (neigh\_trust + UR\_range)/2$;
end

Algorithm 12: Reliability model

Input: initial_path[], perc_unreliability, AP[][],neigh[][], sender h_u, relay_node h_v
Output: AP-R[] ,drop_AP
//Reliable transmission of a data packet with rerouting to shortest AP
forwards the data message from h_u to h_v;
if h_v *behaves as reliable* **then**
    discard the copy from h_u internal buffer;
    update the residual energy;
else
    look for the shortest AP to the sink;
    if *AP found* **then**
        update the path[];
    end
    update drop_AP;
    //Dropped message count for no AP found
end

or beyond the defined percentage of UR then all neighbor nodes also start disconnecting the neighborhood relation with h_v. If this count reaches the defined parameter percentage $perc\_neigh\_count\_relayNode$ declared in Algorithm 11 then the network will declare h_v as fault node and remove it from the network. This process will continue till the network reaches the shift rate. CASS will come into the picture to select the next active sink based on the network reachability. This model continues till no node is unable to reach any of the sinks.

Algorithm 12 helps h_u to find an alternate path to active sink. Some neighbor nodes of h_u can be a neighbors of any passive sink node which can directly receive the data without looking for an alternate path to the current sink. As the sinks are connected which is mentioned in section 3.1, the proposed approach is taking advantage of it.

Based on that either h_u considers the h_v as a relay node or will look for an alternate path to deliver the message to sink. Sometimes the node may not behave reliably due to traffic congestion and other internal system issues and drops the message. In such cases to ensure reliability, h_i takes the responsibility as it follows hop-to-hop transmission and forwards the data to the neighbor with high residual energy and shortest path among all possible paths generated by other neighbors.

5.5.1 The advantages of the proposed model

1. the Alternate path to the current sink is not considered so saving the energy of relay nodes

2. Drop can be avoided if an alternate path not found to the active sink

3. increases the number of messages delivered to sink which makes the NL enhancement

Grid Size	100 X 100
Initial Energy of Sensors	10 Joules
Number of Sensors	100, 200, 300
Number of Sinks	4, 6, 8
Communication Range	15 units
Shift Rate	90%
percUR	10% - 50%
Percentage of common neighbors trust	50% - 90%
Percentage of h_v neighbor count	50% - 80%

Table 5.1: Input Data Information

5.6 Experimental Results

The experiments were done in MATLAB with 100,200 and 300-node networks deployed in a 100X100 grid with 4, 6, and 8 sinks respectively. The simulation starts with trust between all neighbor nodes is 0 assuming all deployed sensors work well. Experiments have been done on 30 test cases with different percentages of unreliability 10, 20, 30, 40, and 50. It allows the sensor nodes to behave unreliablely due to internal system issues up to a defined range.

If a network is defined with 20% of allowed unreliability, it means the node is allowed to behave unreliable at most 20% during data transmission. If the range exceeds then the node needs to be monitored for its fault behavior by collaborating with other neighbor nodes. The percentage of common neighbors trust ranges from 50, 60, 70, 80 and 90. It gives support to h_v to declare it as a non-faulty node based on the trust considered by common neighbors of h_u and h_v. If the percentage of common neighbor's trust is defined as 70% means at least 70% of the common neighbor nodes should have good trust on h_v. These criteria help to identify CLs. This factor is more beneficial when a

more dense network is considered as the probability of having more neighbors is high as well and the percentage of common neighbor's trust also increases. The last key factor

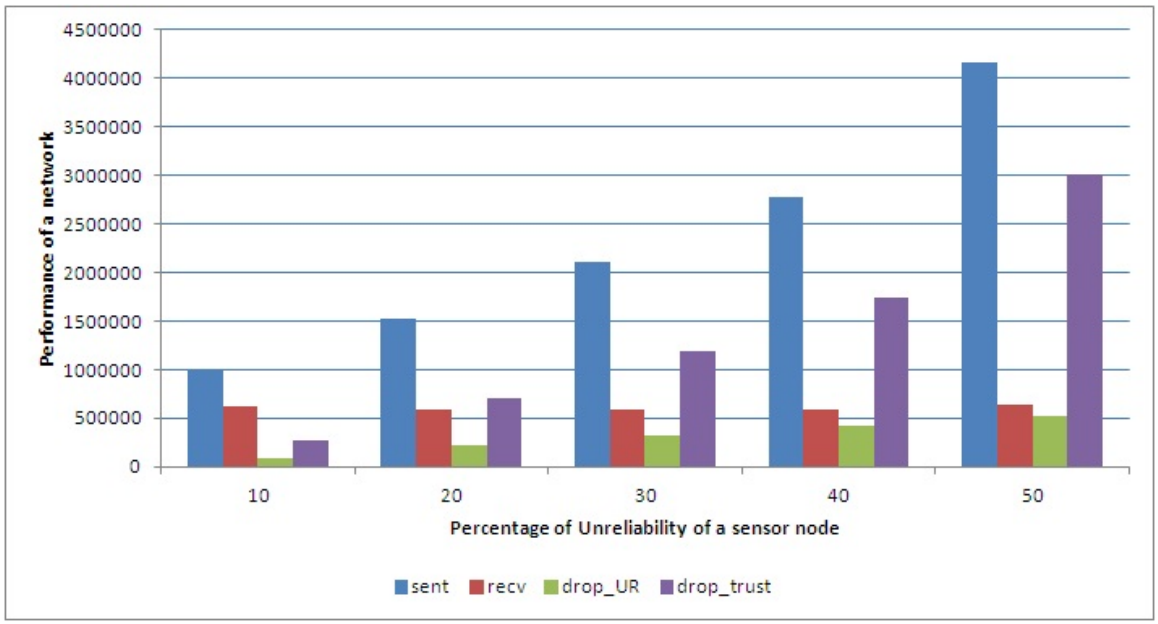

Figure 5.2: 100 node network - unidentified CN

to identify a fault node is the percentage of the neighbors of h_v who disconnected the neighborhood relation with h_v. These values range from 50, 60, 70 and 80. If 80% of neighboring nodes of h_v disconnected the neighbor link with h_v clears that the h_v is doing a security attack on the network. Detailed parameter information is provided in Table 5.1.

Presenting the performance comparison between the approaches where there is no method followed to identify the CNs (it is referred to as simple CASS and after identifying and removing the CNs from the network (referred to as CASS-CN). The performance is measured in terms of the number of messages delivered to the sink altogether and the message drop due to the internal issues mentioned earlier and the trust between the nodes falling below the moderate level and not being able to find an alternate path in both cases.

Fig. 5.2 shows the results of simple CASS on a 100-node network where no trust mechanism is used to identify the CNs. As the graph shows the messages initiated to sent are high, but the messages received by the sinks is only 63.5% and dropping due to CNs (drop_CN) is 26.5% and the remaining 9.9% dropping due to the nodes 10% unreliable behavior. With the increase of unreliable behavior of the node (drop_UR), the CNs take advantage of it to drop the messages and affect the network performance in terms of

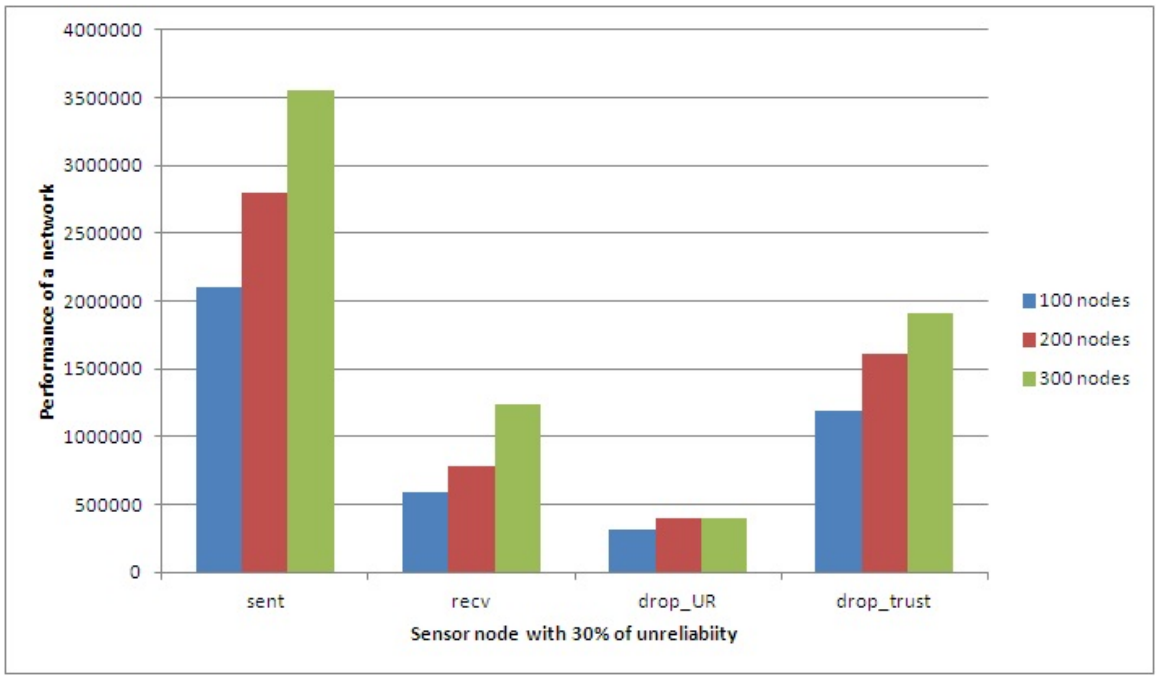

Figure 5.3: On dense network - unidentified CN

delivering the messages to the sink.

Fig. 5.3 shows the effect of unattended CNs in a network with 200 and 300 nodes. The graph presents that in a 300-node network, the drop_CN is value is more than 50% of the sent messages which addresses the importance of detecting and eliminating the CNs from the network. The proposed model helps in identifying the CNs and improves the network performance by 96.8% to 99.1% concerning an increased percUR in a 100-node network. Message drop due to CNs is reduced from 26.5% to 0.1% in a 100-node network with 10% of unreliability. With the increase in the percUR, the drop_CN varies from 0.1% to 0.5%.

Fig. 5.4 shows the performance of a 100 node with 20% of unreliability and varying the other two key parameters to identify the CNs. In all variations, the network performance has improved over the simple CASS giving a great message delivery to the sink with reduced drop rate. Fig. 5.5 shows a performance measure on an increased network size with 20% of unreliability. With increased sensor nodes the sender node finds more alternate paths to reroute which helps in improving the NL in terms of received messages by all sinks together. We computed the average of all desired output parameters for different unreliable

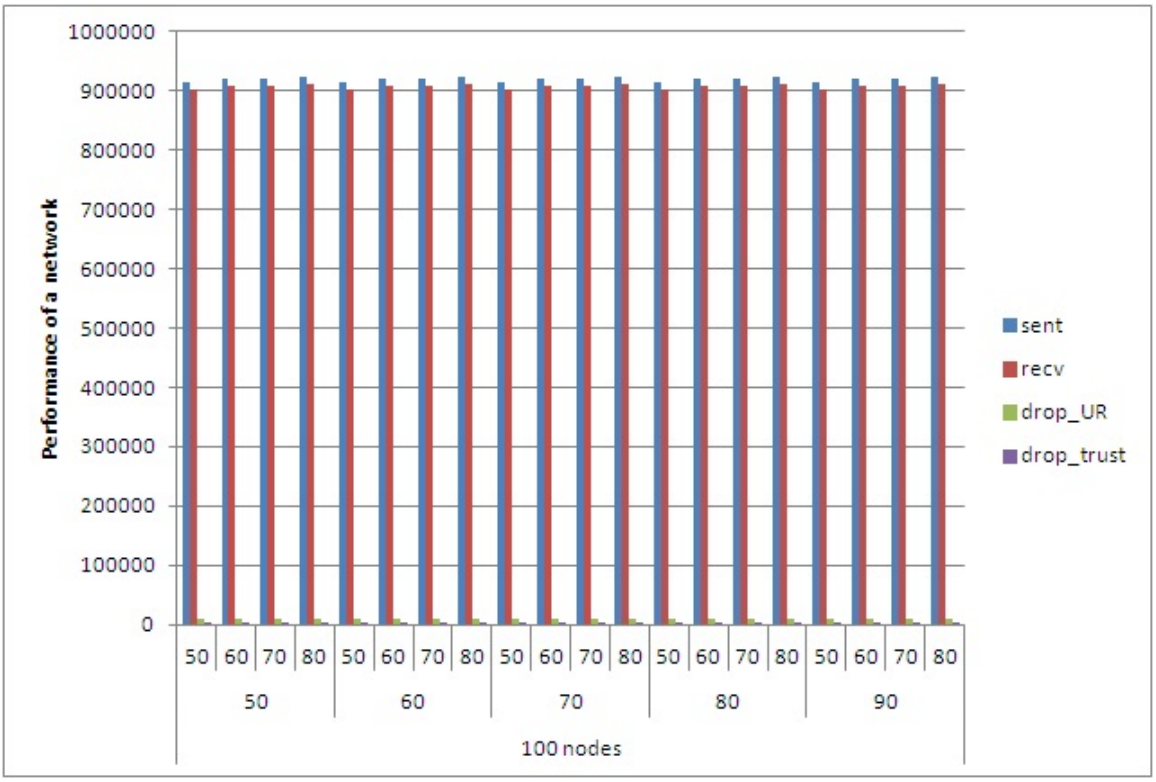

Figure 5.4: CASS with CN detection mechanism on 100 node network with 20% of UR

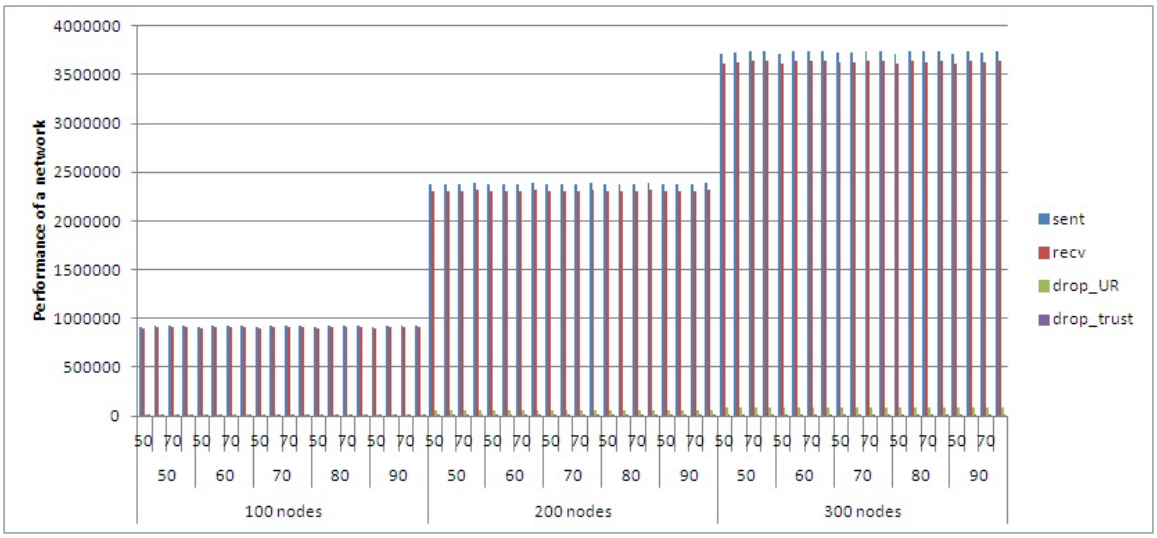

Figure 5.5: acCASS with CN detection mechanism on dense networks

No.of nodes	percUR	Sent	% Received	% Drop_UR	% Drop_CN
100	10	874193	96.8	3	0.1
	20	919357	98.7	1.1	0.2
	30	925358	99.05	0.6	0.3
	40	927517	99.3	0.5	0.4
	50	928676	99.1	0.5	0.5
200	10	1661550	94.9	4.9	0.2
	20	2379435	97	2.7	0.3
	30	2542094	97.4	2	0.7
	40	2600051	96.7	1.9	1.3
	50	2660945	95.9	2	2.1
300	10	2478669	96.8	2.9	0.3
	20	3731511	97.3	2.4	0.3
	30	4304410	97.7	1.8	0.5
	40	4403682	96.2	2.3	1.5
	50	4560848	93.3	3.5	3.2

Table 5.2: Performance of CASS with CN detection mechanism and rerouting to active sink

percentages of total nodes. The results are tabulated in Table. 5.2.

The graphs and results presented for a rerouting mechanism to the active sink. While looking for an alternate path, some nodes are encountered in such a way that the node itself is a direct neighbor to other inactive sinks at that instance. By taking advantage of it and the sinks are interconnected to each other irrespective of the active sink, we simulated rerouting to any sink. Rerouting to any sink increased the delivery ratio in the range of [0.1%, 3.2%] than the alternate path to the current sink for an increased percentage of the unreliability of a sensor node.

5.7 Summary

Sensor nodes are easily adaptable in the deployed region and also easily attacked by intruders. Handling the CNs is a major task in achieving a reliable and long-lasting network. This paper describes to what extent the CNs impact the NL and also proposes an algorithm to detect and detach them from the network based on the two key parameters common neighbor trust (NT) and neighbor count (NC) of a monitoring node. The proposed method took the

help of an alternate path to ensure reliable data delivery in the presence of CNs and nodes with unreliable behavior. The paper presents two variations to reroute the data message to the currently active sink and any sink irrespective of the active sink. Both variations have experimented with different combinations of unreliable behavior of the sensor node, NC and NT, and shown a considerable network life enhancement with minimal drop in the presence of unreliable behavior and CNs.

CHAPTER 6

Conclusions and Future Scope

6.1 Conclusions

In this work, we have focused on an important challenge the WSN encountered. As discussed, the sensor nodes are characterized by limited computational power, memory, storage, and energy resources. Optimizing energy utilization is inevitable for the network to perform satisfactorily for a long time. This thesis attempted and proposed different methodologies for enhancing NL in terms of the number of messages successfully delivered to the sink node in the presence of multiple sinks, hot spots, unreliable intermediate nodes, and compromised (untrustworthy) nodes. In the first contributions, we discussed the improvement of the NL by implementing a CASS wherein we implemented multiple sinks in the WSN set-up and selected one sink for data delivery based on shift rate. We experimented with different shift rates and node densities in the sensing region. During the experimentation, it was observed that the NL could not be improved substantially due to the evolution of hot spots. Hot spots are those nodes that use most of their energy to forward the data packets to the sink nodes and usually the one-hop neighbors of the sink node. In addition, due to the typical topology of the network, a few hot spots are distributed within the network. Thus, we proposed and implemented AP finding and routing method to avoid the hot spots during the data transmission. This approach will preserve the remaining energy in the hot spots and help enhance the NL. We experimented with defining the hot spots with different percentages of remaining energy and measured the improvement in the NL. On

average there is an improvement of 12.5% to 67.6% in the overall NL of the WSN with 100 nodes to 300 nodes. During the experimentation, we found that even if we choose an alternate path, some nodes still have enough residual energy to communicate to the sink by adjusting the communication range. With an assumption that nodes can dynamically adjust their communication range by increasing the transmitting power, **we proposed an acICR based method to communicate directly with the sink bypassing the hot spots and in the absence of the alternate path.** This also yielded almost 37.9% to 87% improvement in the overall NL with an increased number of sensors. For ICR, we increased the transmitting power based on the standard energy model.

The sensor nodes often do not behave reliably due to buffer overflow, noisy communication channels, memory constraints, inadequate computational power, etc. These unreliable nodes may only be able to forward the data packets successfully sometimes. We consider the presence of unreliable nodes in the network. We relaxed the assumption that every node can forward the data packets to the next sensor node or sink if it has enough residual energy. For experimentation, we consider different percentages of unreliable nodes and the percentage of times they behave in an unreliable manner. We also implemented the principle of the AP and ICR approach here to enhance the lifetime. **We observed an increase of more than 10% in the packet delivery ratio of the network in the presence of 5% to 25% unreliable nodes and a varying percentage of unreliable behavior from 10% to 50%**. This proposed model also considers the presence of hot spots in the network, as discussed earlier.

As sensor nodes are deployed in the open and are accessible, the node may be compromised. Sometimes, even the communication link is compromised due to different security attacks. One of our research objectives was to identify the compromised node and compromised link and increase the PDR in the presence of those. In this work, we proposed a model to identify the compromised nodes and links using a trust mechanism. **We considered both direct**

trust and indirect trust to identify the CN, CL. By calculating the percUR the approach can determine the CN precisely. Successful packet forwarding/ delivery was considered a crucial parameter for trust computation. We have considered various hyperparameters like different threshold values for trust computation, and other means to find the compromised links. We modified the proposed AP and ICR to adapt to the trust-based data routing. We have conducted extensive simulations and found that, on average, our proposed model can increase the packet delivery ratio by 20% while considering trust to identify compromised nodes and links.

6.2 Future Scope

While experimenting and also during a recent literature survey, we identified some potential future scope of the work done in this thesis.

- We have implemented shortest path methods to find the alternate path with the residual energy as the edge weight. In the future, we propose to consider the traffic in that link as weight, in addition to the residual energy, for computing the shortest path.
- The message drop probability of an URNode in a WSN largely depends on the data traffic received by the node, the sensing/ sampling frequency, etc. In the future, we plan to monitor the sensor nodes for the incoming traffic, sampling rate, etc., and try to predict the probability of unreliability instead of assuming.
- We have considered only direct and indirect trust for computing the overall trust of a sensor node. However, more trust models can be considered for computing the trust and evaluating the performance.
- In the future, we also plan to deploy a small sensor network to induce various unreliable factors in real networks and observe the performance of our proposed models.

This will help us deploy the model in real networks and improve their lifetime and reliability in compromised nodes and links.

REFERENCES

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[2] A. Bharathidasan and V. A. S. Ponduru, "Sensor networks: An overview," in *IEEE INFOCOM*, vol. 4, Citeseer, 2002.

[3] X. Liu, "A novel transmission range adjustment strategy for energy hole avoiding in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 67, pp. 43–52, 2016.

[4] M. Haghpanahi, M. Kalantari, and M. Shayman, "Topology control in large-scale wireless sensor networks: Between information source and sink," *Ad Hoc Networks*, vol. 11, no. 3, pp. 975–990, 2013.

[5] J. Polastre, R. Szewczyk, A. Mainwaring, D. Culler, and J. Anderson, "Analysis of wireless sensor networks for habitat monitoring," *Wireless sensor networks*, pp. 399–423, 2004.

[6] N. Xu, "A survey of sensor network applications," *IEEE communications magazine*, vol. 40, no. 8, pp. 102–114, 2002.

[7] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[8] A. Boukerche and S. Nikoletseas, "Protocols for data propagation in wireless sensor networks," *Wireless communications systems and networks*, pp. 23–51, 2004.

[9] K. Sohraby, D. Minoli, and T. Znati, *Wireless sensor networks: technology, protocols, and applications*. John wiley & sons, 2007.

[10] C. Buratti, A. Conti, D. Dardari, and R. Verdone, "An overview on wireless sensor networks technology and evolution," *Sensors*, vol. 9, no. 9, pp. 6869–6896, 2009.

[11] M. A. Matin and M. Islam, "Overview of wireless sensor network," *Wireless sensor networks-technology and protocols*, vol. 1, no. 3, 2012.

[12] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad hoc networks*, vol. 3, no. 3, pp. 325–349, 2005.

[13] O. Younis and S. Fahmy, "Heed: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Transactions on mobile computing*, vol. 3, no. 4, pp. 366–379, 2004.

[14] J. Pan, Y. T. Hou, L. Cai, Y. Shi, and S. X. Shen, "Topology control for wireless sensor networks," in *Proceedings of the 9th annual international conference on Mobile computing and networking*, pp. 286–299, 2003.

[15] X. Zeng, R. Bagrodia, and M. Gerla, "Glomosim: a library for parallel simulation of large-scale wireless networks," in *Proceedings of the twelfth workshop on Parallel and distributed simulation*, pp. 154–161, 1998.

[16] M. A. Mahmood, W. K. Seah, and I. Welch, "Reliability in wireless sensor networks: A survey and challenges ahead," *Computer networks*, vol. 79, pp. 166–187, 2015.

[17] H. Yetgin, K. T. K. Cheung, M. El-Hajjar, and L. H. Hanzo, "A survey of network lifetime maximization techniques in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 828–854, 2017.

[18] J. Kim, X. Lin, N. B. Shroff, and P. Sinha, "Minimizing delay and maximizing lifetime for wireless sensor networks with anycast," *IEEE/ACM Transactions on networking*, vol. 18, no. 2, pp. 515–528, 2009.

[19] Y. Zhao, J. Wu, F. Li, and S. Lu, "On maximizing the lifetime of wireless sensor networks using virtual backbone scheduling," *IEEE transactions on parallel and distributed systems*, vol. 23, no. 8, pp. 1528–1535, 2011.

[20] J.-H. Jeon, H.-J. Byun, and J.-T. Lim, "Joint contention and sleep control for lifetime maximization in wireless sensor networks," *IEEE Communications Letters*, vol. 17, no. 2, pp. 269–272, 2013.

[21] A. Chamam and S. Pierre, "On the planning of wireless sensor networks: Energy-efficient clustering under the joint routing and coverage constraint," *IEEE Transactions on Mobile Computing*, vol. 8, no. 8, pp. 1077–1086, 2009.

[22] F. Liu, C.-Y. Tsui, and Y. J. Zhang, "Joint routing and sleep scheduling for lifetime maximization of wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 9, no. 7, pp. 2258–2267, 2010.

[23] C.-C. Hsu, M.-S. Kuo, S.-C. Wang, and C.-F. Chou, "Joint design of asynchronous sleep-wake scheduling and opportunistic routing in wireless sensor networks," *IEEE Transactions on Computers*, vol. 63, no. 7, pp. 1840–1846, 2012.

[24] L. Van Hoesel, T. Nieberg, J. Wu, and P. J. Havinga, "Prolonging the lifetime of wireless sensor networks by cross-layer interaction," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 78–86, 2004.

[25] M. L. Sichitiu, "Cross-layer scheduling for power efficiency in wireless sensor networks," in *IEEE INFOCOM 2004*, vol. 3, pp. 1740–1750, IEEE, 2004.

[26] T. Zia and A. Zomaya, "Security issues in wireless sensor networks," in *2006 International Conference on Systems and Networks Communications (ICSNC'06)*, pp. 40–40, IEEE, 2006.

[27] S. Sharma and S. K. Jena, "A survey on secure hierarchical routing protocols in wireless sensor networks," in *Proceedings of the 2011 international conference on communication, computing & security*, pp. 146–151, 2011.

[28] J. Sen, "A survey on wireless sensor network security," *arXiv preprint arXiv:1011.1529*, 2010.

[29] J. Undercoffer, S. Avancha, A. Joshi, and J. Pinkston, "Security for sensor networks," in *CADIP Research Symposium*, pp. 25–26, Baltimore, 2002.

[30] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network mac protocols," *IEEE transactions on vehicular technology*, vol. 58, no. 1, pp. 367–380, 2008.

[31] C. Boler, S. Yenduri, W. Ding, L. Perkins, and J. Harris, "To shift or not to shift: Maximizing the efficiency of a wireless sensor network.," *(Vol 1, No 1, 2011) International Journal of Networked Computing and Advanced Information*, pp. 66–73, 2011.

[32] C. S. Raghavendra, K. M. Sivalingam, and T. Znati, *Wireless sensor networks*. Springer, 2006.

[33] J. J. Lotf, S. Hossein, and N. Ghazan, "Overview on wireless sensor networks," *Journal of Basic and Applied Scientific Research*, vol. 11, no. 1, pp. 2811–2816, 2011.

[34] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, "Wireless sensor networks for habitat monitoring," in *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, pp. 88–97, 2002.

[35] Q. Wang and I. Balasingham, "Wireless sensor networks-an introduction," *Wireless sensor networks: application-centric design*, pp. 1–14, 2010.

[36] O. I. Khalaf, C. A. T. Romero, S. Hassan, and M. T. Iqbal, "Mitigating hotspot issues in heterogeneous wireless sensor networks," *Journal of Sensors*, vol. 2022, pp. 1–14, 2022.

[37] S. Chen, M. Coolbeth, H. Dinh, Y.-A. Kim, and B. Wang, "Data collection with multiple sinks in wireless sensor networks.," *WASA*, vol. 9, pp. 284–294, 2009.

[38] A. Das and D. Dutta, "Data acquisition in multiple-sink sensor networks," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 9, no. 3, pp. 82–85, 2005.

[39] P. Kuila and P. K. Jana, "Energy efficient clustering and routing algorithms for wireless sensor networks: Particle swarm optimization approach," *Engineering Applications of Artificial Intelligence*, vol. 33, pp. 127–140, 2014.

[40] W. Y. Poe and J. B. Schmitt, "Self-organized sink placement in large-scale wireless sensor networks," in *2009 IEEE International Symposium on Modeling, Analysis & Simulation of Computer and Telecommunication Systems*, pp. 1–3, IEEE, 2009.

[41] Z. Vincze, R. Vida, and A. Vidacs, "Deploying multiple sinks in multi-hop wireless sensor networks," in *IEEE international conference on pervasive services*, pp. 55–63, IEEE, 2007.

[42] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, pp. 10 pp. vol.2–, 2000.

[43] C. Song, M. Liu, J. Cao, Y. Zheng, H. Gong, and G. Chen, "Maximizing network lifetime based on transmission range adjustment in wireless sensor networks," *Computer Communications*, vol. 32, no. 11, pp. 1316–1325, 2009.

[44] A. Jarry, P. Leone, O. Powell, and J. Rolim, "An optimal data propagation algorithm for maximizing the lifespan of sensor networks," in *Distributed Computing in Sensor Systems: Second IEEE International Conference, DCOSS 2006, San Francisco, CA, USA, June 18-20, 2006. Proceedings 2*, pp. 405–421, Springer, 2006.

[45] S. Maurya, V. K. Jain, and D. R. Chowdhury, "Delay aware energy efficient reliable routing for data transmission in heterogeneous mobile sink wireless sensor network," *Journal of Network and Computer Applications*, vol. 144, pp. 118–137, 2019.

[46] F. Ye, G. Zhong, S. Lu, and L. Zhang, "Gradient broadcast: A robust data delivery protocol for large scale sensor networks," *Wireless Networks*, vol. 11, pp. 285–298, 2005.

[47] E. A. Khalil and A. A. Bara'a, "Energy-aware evolutionary routing protocol for dynamic clustering of wireless sensor networks," *Swarm and Evolutionary Computation*, vol. 1, no. 4, pp. 195–203, 2011.

[48] J. Yu, Y. Qi, G. Wang, Q. Guo, X. Gu, *et al.*, "An energy-aware distributed unequal clustering protocol for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 7, no. 1, p. 202145, 2011.

[49] D. Jain, P. K. Shukla, and S. Varma, "Energy efficient architecture for mitigating the hot-spot problem in wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–18, 2022.

[50] S. Jannu and P. K. Jana, "A grid based clustering and routing algorithm for solving hot spot problem in wireless sensor networks," *Wireless Networks*, vol. 22, pp. 1901–1916, 2016.

[51] R. Balamurali and K. Kathiravan, "Mitigating hot spot problems in wireless sensor networks using tier-based quantification algorithm," *Cybernetics and Information Technologies*, vol. 16, no. 1, pp. 73–79, 2016.

[52] V. Tran-Quang and T. Miyoshi, "A transmission range adjustment algorithm to avoid energy holes in wireless sensor networks," in *8th Asia-Pacific Symposium on Information and Telecommunication Technologies*, pp. 1–6, IEEE, 2010.

[53] X. Wu, G. Chen, and S. K. Das, "Avoiding energy holes in wireless sensor networks with nonuniform node distribution," *IEEE Transactions on parallel and distributed systems*, vol. 19, no. 5, pp. 710–720, 2008.

[54] S. Olariu and I. Stojmenovic, "Design guidelines for maximizing lifetime and avoiding energy holes in sensor networks with uniform distribution and uniform reporting," in *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications*, pp. 1–12, Citeseer, 2006.

[55] J. Jia, J. Chen, X. Wang, and L. Zhao, "Energy-balanced density control to avoid energy hole for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 8, no. 1, p. 812013, 2012.

[56] Z. Zhi-wen, L. An-Feng, C. Zhi-gang, W. Xian-you, and L. Jun, "Improved analysis of energy hole for wireless sensor networks," in *2009 WRI International Conference on Communications and Mobile Computing*, vol. 1, pp. 533–537, IEEE, 2009.

[57] J. Luo and J.-P. Hubaux, "Joint mobility and routing for lifetime elongation in wireless sensor networks," in *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, vol. 3, pp. 1735–1746, IEEE, 2005.

[58] W. Wang, V. Srinivasan, and K.-C. Chua, "Using mobile relays to prolong the lifetime of wireless sensor networks," in *Proceedings of the 11th annual international conference on Mobile computing and networking*, pp. 270–283, 2005.

[59] H. Zhang and H. Shen, "Balancing energy consumption to maximize network lifetime in data-gathering sensor networks," *IEEE Transactions on parallel and distributed systems*, vol. 20, no. 10, pp. 1526–1539, 2008.

[60] M. L. Sichitiu and R. Dutta, "Benefits of multiple battery levels for the lifetime of large wireless sensor networks," in *NETWORKING 2005. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems: 4th International IFIP-TC6 Networking Conference, Waterloo, Canada, May 2-6, 2005. Proceedings 4*, pp. 1440–1444, Springer, 2005.

[61] C.-W. Chen, K.-F. Ssu, and H. C. Jiau, "Fault-tolerant topology control with adjustable transmission ranges in wireless sensor networks," in *13th Pacific Rim International Symposium on Dependable Computing (PRDC 2007)*, pp. 131–138, IEEE, 2007.

[62] K. M. Alam, J. Kamruzzaman, G. Karmakar, and M. Murshed, "Dynamic adjustment of sensing range for event coverage in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 46, pp. 139–153, 2014.

[63] M. Azharuddin and P. K. Jana, "Particle swarm optimization for maximizing lifetime of wireless sensor networks," *Computers & Electrical Engineering*, vol. 51, pp. 26–42, 2016.

[64] M. Cardei, J. Wu, M. Lu, and M. O. Pervaiz, "Maximum network lifetime in wireless sensor networks with adjustable sensing ranges," in *WiMob'2005), IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, 2005.*, vol. 3, pp. 438–445, IEEE, 2005.

[65] S. Nikoletseas, "Models and algorithms for wireless sensor networks (smart dust)," in *SOFSEM 2006: Theory and Practice of Computer Science: 32nd Conference on Current Trends in Theory and Practice of Computer Science, Merin, Czech Republic, January 21-27, 2006. Proceedings 32*, pp. 64–83, Springer, 2006.

[66] S. Nikoletseas and J. D. Rolim, *Theoretical aspects of distributed computing in sensor networks*. Springer, 2011.

[67] R. Szewczyk, A. Mainwaring, J. Polastre, J. Anderson, and D. Culler, "An analysis of a large scale habitat monitoring application," in *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pp. 214–226, 2004.

[68] X. Tang and J. Xu, "Extending network lifetime for precision-constrained data aggregation in wireless sensor networks.," in *INFOCOM*, pp. 1–12, Citeseer, 2006.

[69] H. Zhou, X. Guan, and C. Wu, "Reliable transport with memory consideration in wireless sensor networks," in *2008 IEEE International Conference on Communications*, pp. 2819–2824, IEEE, 2008.

[70] M. Maroti, "Directed flood-routing framework for wireless sensor networks," in *Middleware 2004: ACM/IFIP/USENIX International Middleware Conference, Toronto, Canada, October 18-22, 2004. Proceedings 5*, pp. 99–114, Springer, 2004.

[71] H. Zhang, A. Arora, Y.-r. Choi, and M. G. Gouda, "Reliable bursty convergecast in wireless sensor networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, pp. 266–276, 2005.

[72] T. Le, W. Hu, P. Corke, and S. Jha, "Ertp: Energy-efficient and reliable transport protocol for data streaming in wireless sensor networks," *Computer Communications*, vol. 32, no. 7-10, pp. 1154–1171, 2009.

[73] F. K. Shaikh, A. Khelil, A. Ali, and N. Suri, "Trccit: tunable reliability with congestion control for information transport in wireless sensor networks," in *2010 The 5th Annual ICST Wireless Internet Conference (WICON)*, pp. 1–9, IEEE, 2010.

[74] F. Stann and J. Heidemann, "Rmst: Reliable data transport in sensor networks," in *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.*, pp. 102–112, IEEE, 2003.

[75] C.-Y. Wan, A. T. Campbell, and L. Krishnamurthy, "Pump-slowly, fetch-quickly (psfq): a reliable transport protocol for sensor networks," *IEEE Journal on selected areas in Communications*, vol. 23, no. 4, pp. 862–872, 2005.

[76] S.-J. Park, R. Vedantham, R. Sivakumar, and I. F. Akyildiz, "Garuda: Achieving effective reliability for downstream communication in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 7, no. 2, pp. 214–230, 2007.

[77] S. Misra, P. Kar, A. Roy, and M. S. Obaidat, "Existence of dumb nodes in stationary wireless sensor networks," *Journal of Systems and Software*, vol. 91, pp. 135–146, 2014.

[78] S. Gudla and N. R. Kuda, "Learning automata based energy efficient and reliable data delivery routing mechanism in wireless sensor networks," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 8, pp. 5759–5765, 2022.

[79] P. Hejazi and G. Ferrari, "A novel approach for energy-and memory-efficient data loss prevention to support internet of things networks," *International Journal of Distributed Sensor Networks*, vol. 16, no. 6, p. 1550147720929823, 2020.

[80] O. Yang and W. Heinzelman, "Sleeping multipath routing: a trade-off between reliability and lifetime in wireless sensor networks," in *2011 IEEE Global Telecommunications Conference-GLOBECOM 2011*, pp. 1–5, IEEE, 2011.

[81] L. Yu, N. Wang, W. Zhang, and C. Zheng, "Deploying a heterogeneous wireless sensor network," in *2007 International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 2588–2591, IEEE, 2007.

[82] J. Vasavi and S. K. Udgata, "Lifetime maximisation of wireless sensor networks with multiple sinks using multiple paths and variable communication range," *International Journal of Sensor Networks*, vol. 26, no. 3, pp. 200–211, 2018.

[83] E. Zhao, B. Yi, H. Li, and J. Yao, "Transmission range adjustment in wsns based on dynamic programming algorithm," in *2006 International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1–4, IEEE, 2006.

[84] N. Karthik and V. S. Dhulipala, "Trust calculation in wireless sensor networks," in *2011 3rd International Conference on Electronics Computer Technology*, vol. 4, pp. 376–380, IEEE, 2011.

[85] V. Junapudi and S. K. Udgata, "Reliable data delivery in wireless sensor networks with multiple sinks and optimal routing," in *International Conference on Machine Learning, IoT and Big Data*, pp. 607–619, Springer, 2023.

[86] A. A. Pirzada and C. McDonald, "Establishing trust in pure ad-hoc networks," in *Proceedings of the 27th Australasian conference on Computer science-Volume 26*, pp. 47–54, Citeseer, 2004.

[87] M. Momani, S. Challa, and K. Aboura, "Modelling trust in wireless sensor networks from the sensor reliability prospective," *Innovative algorithms and techniques in automation, industrial electronics and telecommunications*, pp. 317–321, 2007.

[88] V. S. Dhulipala, B. V. Prabha, and R. Chandrasekaran, "Trust worthy architecture for mobile ad hoc network environment," in *Information Processing and Management: International Conference on Recent Trends in Business Administration and Information Processing, BAIP 2010, Trivandrum, Kerala, India, March 26-27, 2010. Proceedings*, pp. 557–560, Springer, 2010.

[89] W. Zhang, S. K. Das, and Y. Liu, "A trust based framework for secure data aggregation in wireless sensor networks," in *2006 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks*, vol. 1, pp. 60–69, IEEE, 2006.

[90] Y. Kimura, E. Nii, and Y. Takizawa, "Cooperative detection for falsification and isolation of malicious nodes through inter-node vote for wireless sensor networks in open environments," in *2019 Global Information Infrastructure and Networking Symposium (GIIS)*, pp. 1–3, IEEE, 2019.

[91] V. B. Reddy, S. Venkataraman, and A. Negi, "Communication and data trust for wireless sensor networks using d–s theory," *IEEE Sensors Journal*, vol. 17, no. 12, pp. 3921–3929, 2017.

[92] S. Ravindranath, G. Srikanth, and K. Swetha, "Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning," in *International Conference on Recent Innovations in Engineering & Technology ICRIET*, vol. 23, 2015.

[93] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 4, no. 3, pp. 1–37, 2008.

[94] A. Ahmed, K. A. Bakar, M. I. Channa, K. Haseeb, and A. W. Khan, "Terp: A trust and energy aware routing protocol for wireless sensor network," *IEEE Sensors Journal*, vol. 15, no. 12, pp. 6962–6972, 2015.

[95] J. Hur, Y. Lee, H. Yoon, D. Choi, and S. Jin, "Trust evaluation model for wireless sensor networks," in *The 7th International Conference on Advanced Communication Technology, 2005, ICACT 2005.*, vol. 1, pp. 491–496, IEEE, 2005.

[96] X.-Y. Xiao, W.-C. Peng, C.-C. Hung, and W.-C. Lee, "Using sensorranks for in-network detection of faulty readings in wireless sensor networks," in *Proceedings of the 6th ACM international workshop on Data engineering for wireless and mobile access*, pp. 1–8, 2007.

[97] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An efficient distributed trust model for wireless sensor networks," *IEEE transactions on parallel and distributed systems*, vol. 26, no. 5, pp. 1228–1237, 2014.

[98] R. A. Shaikh, H. Jameel, S. Lee, S. Rajput, and Y. J. Song, "Trust management problem in distributed wireless sensor networks," in *12th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA'06)*, pp. 411–414, IEEE, 2006.

[99] A. Attiah, M. F. Amjad, O. Nakhila, and C. Zou, "Adp: An adaptive feedback approach for energy-efficient wireless sensor networks," in *2016 International Conference on Computing, Networking and Communications (ICNC)*, pp. 1–7, IEEE, 2016.

[100] N. Achyutha Prasad and C. Guruprakash, "A two hop relay battery aware mote scheme for energy redeemable and network lifespan improvement in wsn," *International Journal of Engineering and Advanced Technology*, vol. 9, pp. 4785–4791, 2019.

[101] H. Chaitra, G. Manjula, M. Shabaz, A. B. Martinez-Valencia, K. Vikhyath, S. Verma, J. L. Arias-Gonzáles, *et al.*, "Delay optimization and energy balancing algorithm for improving network lifetime in fixed wireless sensor networks," *Physical Communication*, vol. 58, p. 102038, 2023.

[102] I. Tomić, P.-Y. Chen, M. J. Breza, and J. A. McCann, "Antilizer: run time self-healing security for wireless sensor networks," in *Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pp. 107–116, 2018.

[103] B. Jaint, V. Singh, L. K. Tanwar, S. Indu, and N. Pandey, "An efficient weighted trust method for malicious node detection in clustered wireless sensor networks," in *2018 2nd IEEE International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES)*, pp. 1183–1187, IEEE, 2018.

Energy Efficient Reliable Communication in presence of compromised nodes in a Wireless Sensor Network

by vasavi Junapudi

Submission date: 22-Dec-2023 05:01PM (UTC+0530)
Submission ID: 2264056749
File name: Vasavi_Junapudi.pdf (2.39M)
Word count: 33095
Character count: 174545

22/12/2023
Prof. Siba K. Udgata
Professor
School Of Computer & Information Sciences
University of Hyderabad
Hyderabad, India.

Energy Efficient Reliable Communication in presence of compromised nodes in a Wireless Sensor Network

ORIGINALITY REPORT

19%	7%	18%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

Similarity from her own paper = 6+3 = 9%.
Overall similarity = 19-6-3 = 10%.
Sudgata 22/12/23

PRIMARY SOURCES

1	Junapudi Vasavi, Siba K. Udgata. "Lifetime maximisation of wireless sensor networks with multiple sinks using multiple paths and variable communication range", International Journal of Sensor Networks, 2018 Publication	6%
2	Vasavi Junapudi, Siba K. Udgata. "Chapter 52 Reliable Data Delivery in Wireless Sensor Networks with Multiple Sinks and Optimal Routing", Springer Science and Business Media LLC, 2024 Publication	3%
3	Mahmood, Muhammad Adeel, Winston K.G. Seah, and Ian Welch. "Reliability in wireless sensor networks: A survey and challenges ahead", Computer Networks, 2015. Publication	1%
4	www.intechopen.com Internet Source	1%
5	aquila.usm.edu	

Sudgata 22/12/2023

Prof. Siba K. Udgata
Professor
School Of Computer & Information Sciences
University of Hyderabad
Hyderabad, India.

	Internet Source	1%
6	researcharchive.vuw.ac.nz Internet Source	1%
7	Karthik, N., and V. R. Sarma Dhulipala. "Trust calculation in wireless sensor networks", 2011 3rd International Conference on Electronics Computer Technology, 2011. Publication	1%
8	vdoc.pub Internet Source	1%
9	Submitted to University of Alabama Student Paper	<1%
10	"Smart Intelligent Computing and Applications", Springer Science and Business Media LLC, 2019 Publication	<1%
11	findthatstream.com Internet Source	<1%
12	repository.ju.edu.et Internet Source	<1%
13	"Nature Inspired Computing for Wireless Sensor Networks", Springer Science and Business Media LLC, 2020 Publication	<1%

14	Vijender Busi Reddy, Sarma Venkataraman, Atul Negi. "Communication and Data Trust for Wireless Sensor Networks Using D–S Theory", IEEE Sensors Journal, 2017 Publication	<1 %
15	"Theoretical Aspects of Distributed Computing in Sensor Networks", Springer Nature, 2011 Publication	<1 %
16	www.researchgate.net Internet Source	<1 %
17	Meicheng Liu, Jie Zhang, Ming Lyu, Yuming Bo. "A novel solution for energy hole of Wireless Sensor Network", Proceedings of the 33rd Chinese Control Conference, 2014 Publication	<1 %
18	Submitted to Coventry University Student Paper	<1 %
19	Pooya Hejazi, Gianluigi Ferrari. "A novel approach for energy- and memory-efficient data loss prevention to support Internet of Things networks", International Journal of Distributed Sensor Networks, 2020 Publication	<1 %
20	www.openaccessrepository.it Internet Source	<1 %

21	"Wireless Sensor Networks and Applications", Springer Science and Business Media LLC, 2008 Publication	<1 %
22	www.inderscience.com Internet Source	<1 %
23	"Advances in Networks and Communications", Springer Science and Business Media LLC, 2011 Publication	<1 %
24	opus.lib.uts.edu.au Internet Source	<1 %
25	"Algorithms and Protocols for Wireless Sensor Networks", Wiley, 2008 Publication	<1 %
26	Halil Yetgin, Kent Tsz Kan Cheung, Mohammed El-Hajjar, Lajos Hanzo. "A Survey of Network Lifetime Maximization Techniques in Wireless Sensor Networks", IEEE Communications Surveys & Tutorials, 2017 Publication	<1 %
27	Submitted to Kwame Nkrumah University of Science and Technology Student Paper	<1 %
28	mts.intechopen.com Internet Source	<1 %

29	Sateesh Gudla, Nageswara Rao Kuda. "Learning automata based energy efficient and reliable data delivery routing mechanism in wireless sensor networks", Journal of King Saud University - Computer and Information Sciences, 2021 Publication	<1 %
30	"Inventive Computation Technologies", Springer Science and Business Media LLC, 2020 Publication	<1 %
31	Athota Kavitha, Vijender Busi Reddy, Ninni Singh, Vinit Kumar Gunjan et al. "Security in IoT Mesh Networks Based on Trust Similarity", IEEE Access, 2022 Publication	<1 %
32	Submitted to University of Malaya Student Paper	<1 %
33	Sudip Misra, Pushpendu Kar, Arijit Roy, Mohammad S. Obaidat. "Existence of dumb nodes in stationary wireless sensor networks", Journal of Systems and Software, 2014 Publication	<1 %
34	Aubin Jarry. "An Optimal Data Propagation Algorithm for Maximizing the Lifespan of	<1 %

Sensor Networks", Lecture Notes in Computer Science, 2006
Publication

35	Submitted to Universidad Politécnica de Cartagena Student Paper	<1 %
36	webthesis.biblio.polito.it Internet Source	<1 %
37	Bi, Y.. "DAR: An energy-balanced data-gathering scheme for wireless sensor networks", Computer Communications, 20071015 Publication	<1 %
38	Chao Song, Ming Liu, Jiannong Cao, Yuan Zheng, Haigang Gong, Guihai Chen. "Maximizing network lifetime based on transmission range adjustment in wireless sensor networks", Computer Communications, 2009 Publication	<1 %
39	Yang, Ou, and Wendi Heinzelman. "An adaptive sensor sleeping solution based on sleeping multipath routing and duty-cycled MAC protocols", ACM Transactions on Sensor Networks, 2013. Publication	<1 %

40	Tarique, M.. "Minimum energy hierarchical dynamic source routing for Mobile Ad Hoc Networks", Ad Hoc Networks, 200908 Publication	<1 %
41	Bhavnesh Jaint, Vishwamitra Singh, Lalit Kumar Tanwar, S. Indu, Neeta Pandey. "An Efficient Weighted Trust Method for Malicious Node Detection in Clustered Wireless Sensor Networks", 2018 2nd IEEE International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES), 2018 Publication	<1 %
42	J. Hill, D.B. Johnson. "Directed Flood-Routing Framework for Wireless Sensor Networks", 'Springer Science and Business Media LLC', 2004 Internet Source	<1 %
43	K. Thanigaivelu, K. Murugan. "K-level based transmission range scheme to alleviate energy hole problem in WSN", Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology, 2012 Publication	<1 %
44	Meenalochani Manickam, Hemavathi N, Sudha S.. "Performance Analysis of Iterative Linear Regression Based Clustering in	<1 %

Wireless Sensor Networks", IET Science, Measurement & Technology, 2019
Publication

45	Zhiqi Li, Weidong Fang, Chunsheng Zhu, Zhiwei Gao, Wuxiong Zhang. "AI-enabled Trust in Distributed Networks", IEEE Access, 2023 Publication	<1 %
46	Deyu Lin, Quan Wang, Weidong Min, Jianfeng Xu, Zhiqiang Zhang. "A Survey on Energy-Efficient Strategies in Static Wireless Sensor Networks", ACM Transactions on Sensor Networks, 2021 Publication	<1 %
47	Srikanth Jannu, Prasanta K. Jana. "A grid based clustering and routing algorithm for solving hot spot problem in wireless sensor networks", Wireless Networks, 2015 Publication	<1 %
48	us98highlands.com Internet Source	<1 %
49	Springer Series in Bio-/Neuroinformatics, 2015. Publication	<1 %
50	ijsrcseit.com Internet Source	<1 %
51	onlinelibrary.wiley.com	

	Internet Source	<1%
52	"Algorithms and Protocols for Wireless and Mobile Ad Hoc Networks", Wiley, 2008 Publication	<1%
53	K. Thanigaivelu. "Grid-based clustering with dual cluster heads to alleviate energy hole problem for non-uniform node distribution in wireless sensor networks", International Journal of Mobile Network Design and Innovation, 2012 Publication	<1%
54	Mohamed Khalil Watfa. "Wireless Sensor Networks, Making a Difference Tomorrow", Lecture Notes in Computer Science, 2007 Publication	<1%
55	Tarik Yardibi. "A distributed activity scheduling algorithm for wireless sensor networks with partial coverage", Wireless Networks, 08/01/2008 Publication	<1%
56	Zhang Haifeng. "An implementation of wireless sensor network for detection of runaway trains", 2011 Academic International Symposium on Optoelectronics and Microelectronics Technology, 10/2011 Publication	<1%

57	Adnan Ahmed, Kamalrulnizam AbuBakar, Muhammad Ibrahim Channa, Khalid Haseeb, Abdul Waheed Khan. "A trust aware routing protocol for energy constrained wireless sensor network", Telecommunication Systems, 2015 Publication	<1 %
58	Communications in Computer and Information Science, 2011. Publication	<1 %
59	Submitted to Higher Education Commission Pakistan Student Paper	<1 %
60	Xiaobing Wu. "", IEEE Transactions on Parallel and Distributed Systems, 5/2008 Publication	<1 %
61	Yoon, Seokhoon, Abul K. Azad, Hoon Oh, and Sunghwan Kim. "AURP: An AUV-Aided Underwater Routing Protocol for Underwater Acoustic Sensor Networks", Sensors, 2012. Publication	<1 %
62	nozdr.ru Internet Source	<1 %
63	repositorio.unicamp.br Internet Source	<1 %
64	A. Meena Kowshalya, M. L. Valarmathi. "Trust Management in the Social Internet of Things",	<1 %

	Wireless Personal Communications, 2017 Publication	
65	Lecture Notes in Computer Science, 2015. Publication	<1 %
66	Submitted to University of East London Student Paper	<1 %
67	V. R. Sarma Dhulipala, N. Karthik, RM. Chandrasekaran. "A Novel Heuristic Approach Based Trust Worthy Architecture for Wireless Sensor Networks", Wireless Personal Communications, 2012 Publication	<1 %
68	Communications in Computer and Information Science, 2012. Publication	<1 %
69	Submitted to PSG Institute of Management Coimbatore Student Paper	<1 %

Exclude quotes	On	Exclude matches	< 14 words
Exclude bibliography	On		