

**THE USE LAPLACIAN EIGENVALUE  
FEEDBACK IN CONSENSUS-BASED TIME  
SYNCHRONIZATION TO ENHANCE  
ROBUSTNESS IN SENSOR NETWORKS**

A THESIS SUBMITTED TO  
THE SCHOOL OF  
COMPUTING

**BY**

**FAKHMI KEMAL ISLAMY**

**2302210007**



IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE  
DEGREE OF  
MASTER OF CYBER SECURITY & DIGITAL FORENSICS  
IN  
THE SCHOOL OF COMPUTING

**TELKOM UNIVERSITY  
2024**

# APPROVAL PAGE

Approval of the School of Computing of Telkom University

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master Informatics.

Date August 16, 2024

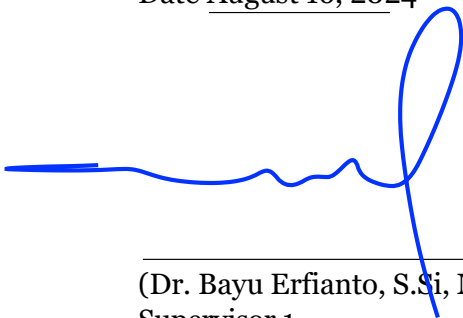


(Dr. Farah Afianti S.T., M.T.)

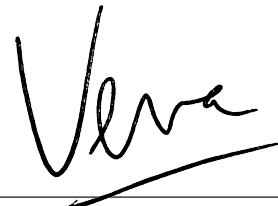
Head of Master Cyber Security and Digital Forensics

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Cyber Security & Digital Forensics.

Date August 16, 2024



(Dr. Bayu Erfianto, S.Si, M.Sc.)  
Supervisor 1



(Dr. Vera Suryani, S.T., MT.)  
Supervisor 2

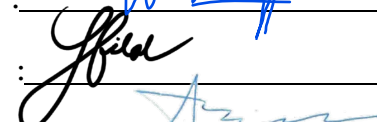
Examining Committee Members.

Date August 16, 2024

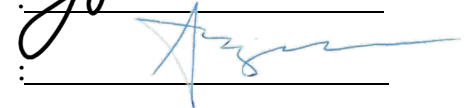
(Dr. Setyorini, S.T., M.T.) (Chairperson of the jury)



(Hilal Hudan Nuha, S.T., M.T., Ph.D.) (jury's member)



(Muhammad Irsan, S.T., M.Kom., Ph.D.) (jury's member)



## **SELF DECLARATION AGAINST PLAGIARISM**

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Month/Date/Year August 1, 2024

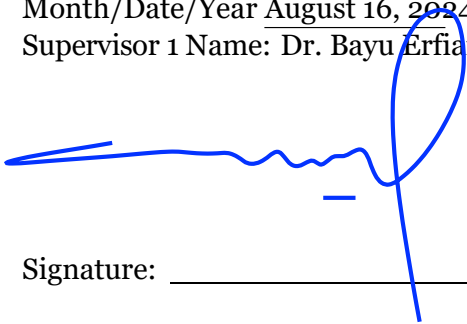
Author Name: Fakhmi Kemal Islamy



Signature: \_\_\_\_\_

Month/Date/Year August 16, 2024

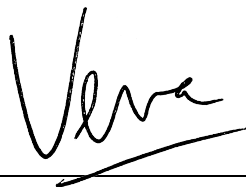
Supervisor 1 Name: Dr. Bayu Erfianto, S.Si, M.Sc.



Signature: \_\_\_\_\_

Month/Date/Year August 16, 2024

Supervisor 2 Name: Dr. Vera Suryani, S.T., MT



Signature: \_\_\_\_\_

## ABSTRACT

Sensor networks on the Internet of Things (IoT) are vital for Cyber-Physical Systems, integrating physical and digital worlds. Effective time synchronization is critical for managing these networks, involving processes such as security, localization, routing, and tracking. Without proper synchronization, log file correlation among devices becomes challenging, leading to potential conflicts and service losses. Ensuring secure time synchronization is essential, using robust algorithms and protocols. Time synchronization aligns local clock times across nodes, countering hardware clock drift. Distributed consensus algorithms have shown robustness against threats like Denial of Service (DoS) attacks and data manipulation, but their performance is heavily influenced by network topology changes, making topology attacks a significant research focus. The resilience of consensus-based time synchronization relies on the network's topology, represented by the adjacency matrix and Laplacian graph eigenvalues, indicating connectivity strength. Fixed Weight Assignment (FWA), Centralized Weight Assignment (CWA), and Mobile Weight Assignment (MWA) are consensus weighting algorithms used in WSN synchronization, each adapting differently to network conditions. However, these methods often overlook the impact of topological changes during attacks. This study proposed a graph-based consensus synchronization weighting method using Laplacian eigenvalues to test resilience against topology attacks, focusing on convergence speed and synchronization accuracy. The findings showed that incorporating Laplacian Gain enhances fault tolerance, reduces convergence iterations by approximately 40.42%, and improves network accuracy by about 9.34%. This demonstrates the crucial role of Laplacian-based consensus methods in maintaining network speed convergence and accuracy under topology changes, recommending their adoption for enhancing WSN resilience against attacks.

**Keywords:** IoT Security, Time Synchronization, Clock Attack, MWA, Laplacian-Based

---

## ABSTRAK

Jaringan sensor dalam *Internet of Things (IoT)* sangat penting untuk Sistem Fisik-Siber, yang mengintegrasikan dunia fisik dan digital. Sinkronisasi waktu yang efektif sangat penting untuk mengelola jaringan ini, termasuk dalam proses seperti keamanan, lokalisasi, perutean, dan pelacakan. Tanpa sinkronisasi yang tepat, korelasi file log antar perangkat menjadi sulit, yang dapat menyebabkan konflik dan hilangnya layanan. Memastikan sinkronisasi waktu yang aman sangat penting, dengan menggunakan algoritma dan protokol yang kuat. Sinkronisasi waktu menyelaraskan waktu jam lokal di seluruh node, melawan drift jam perangkat keras. Algoritma konsensus terdistribusi telah menunjukkan ketahanan terhadap ancaman seperti serangan *Denial of Service (DoS)* dan manipulasi data, tetapi kinerjanya sangat dipengaruhi oleh perubahan topologi jaringan, menjadikan serangan topologi sebagai fokus penelitian yang signifikan. Ketahanan sinkronisasi waktu berbasis konsensus bergantung pada topologi jaringan, yang direpresentasikan oleh matriks kedekatan dan nilai eigen graf Laplacian, yang menunjukkan kekuatan konektivitas. Penetapan Bobot Tetap (FWA), Penetapan Bobot Terpusat (CWA), dan Penetapan Bobot Bergerak (MWA) adalah algoritma penetapan bobot konsensus yang digunakan dalam sinkronisasi WSN, masing-masing beradaptasi secara berbeda terhadap kondisi jaringan. Namun, metode ini sering mengabaikan dampak perubahan topologi selama serangan. Penelitian ini mengusulkan metode penetapan bobot sinkronisasi konsensus berbasis graf menggunakan nilai eigen Laplacian untuk menguji ketahanan terhadap serangan topologi, dengan fokus pada kecepatan konvergensi dan akurasi sinkronisasi. Temuan menunjukkan bahwa menggabungkan gain Laplacian meningkatkan toleransi kesalahan, mengurangi iterasi konvergensi sekitar 40,42%, dan meningkatkan akurasi jaringan sekitar 9,34%. Hal ini menunjukkan peran penting metode konsensus berbasis Laplacian dalam menjaga kecepatan konvergensi jaringan dan akurasi jaringan di bawah perubahan topologi, merekomendasikan penerapannya untuk meningkatkan ketahanan WSN terhadap serangan.

**Kata kunci:** Keamanan *IoT*, Sinkronisasi Waktu, Serangan *Clock*, MWA, Laplacian

## **DEDICATION**

This thesis is dedicated to Ayah (alm.), Ibu and my lovely Wife and our Daughters.

---

## ACKNOWLEDGMENTS

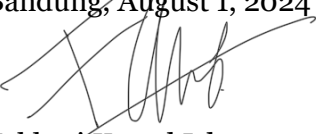
This thesis is compiled with the effort, help, and support from both students and lecturers. I would like to express my deepest gratitude and thanks to:

1. My supervisor, Dr. Bayu Erfianto, S.Si, M.Sc. and Dr. Vera Suryani, S.T., MT., for giving me support, kindness, and faith to finish this thesis research. Who tirelessly give me valuable advice not only for the research process but also on my journey to re-learn the process of learning.
2. Prodi MSF Bu Farah, Bu Ari & Kiky who support for all the suggestions in all of my thesis administration phases until the final defense.
3. To everyone else that cannot be mentioned who helped me throughout this research.
4. And lastly, to my MSF friends from batch 1 until 5 & Telkomsel's NSM who support me a lot to keep healthy and reached out the finish line.

## PREFACE

All the work presented was conducted by the author in the data security department from the School of Computing of Telkom University. I could not have achieved my accomplishments without the supportive role in my research process. First, my supervisor, who patiently and kindly guides me throughout my research and my growth as a student. Second, all the friends and acquaintances that provided help. Lastly, to the most special one, my family, who I can always come home to. Thank you all for all of your unwavering support. Thank you all for giving me this chance to love the genuine process of learning for the sake of knowledge and for helping me grow as a better person.

Bandung, August 1, 2024



Fakhmi Kemal Islamy



---

# CONTENTS

<b>APPROVAL PAGE .....</b>	<b>I</b>
<b>SELF DECLARATION AGAINST PLAGIARISM .....</b>	<b>II</b>
<b>ABSTRACT .....</b>	<b>III</b>
<b>ABSTRAK .....</b>	<b>IV</b>
<b>DEDICATION .....</b>	<b>V</b>
<b>ACKNOWLEDGMENTS.....</b>	<b>VI</b>
<b>PREFACE .....</b>	<b>VII</b>
<b>CONTENTS .....</b>	<b>VIII</b>
<b>LIST OF TABLES.....</b>	<b>X</b>
<b>LIST OF PICTURES .....</b>	<b>XI</b>
<b>LIST OF NOTATIONS .....</b>	<b>XIV</b>
<b>CHAPTER 1.....</b>	<b>1</b>
1.1 RESEARCH BACKGROUND.....	1
1.2 STATEMENT OF THE PROBLEM .....	3
1.3 OBJECTIVE AND HYPOTHESES .....	3
1.4 SCOPE AND DELIMITATION.....	4
1.5 SIGNIFICANCE OF THE STUDY .....	4
<b>CHAPTER 2 .....</b>	<b>5</b>
2.1 STATE OF THE ART .....	5
2.1.1 TIME SYNCHRONIZATION IN WIRELESS SENSOR NETWORKS.....	6
2.1.2 TIME SYNCHRONIZATION ALGORITHMS BASED ON CONSENSUS AND NON- CONSENSUS.....	9
2.1.3 GRAPH LAPLACIAN AND GAIN CONSENSUS .....	11
2.1.4 ROBUSTNESS PARAMETERS UNDER ATTACKS .....	15
2.2 THEORETICAL FRAMEWORK .....	18
2.2.1 CONSENSUS THEORY.....	18
2.2.2 THEORY OF CONSENSUS-BASED TIME SYNCHRONIZATION.....	19
2.2.2.1 CLOCK MODEL .....	19
2.2.2.2 CONSENSUS CLOCK MODEL AND WEIGHTING.....	20
2.2.2.3 LAPLACIAN WEIGHTING AND EIGENVALUES .....	22
2.2.2.4 THE AVERAGING TIME SYNCHRONIZATION (ATS) ALGORITHM .....	24

2.2.3	MINIMUM SPANNING TREE .....	25
2.2.4	PERFORMANCE OF TIME SYNCHRONIZATION CONSENSUS ROBUSTNESS AGAINST ATTACKS .....	27
<b>CHAPTER 3 .....</b>		<b>32</b>
3.1	RESEARCH DESIGN .....	32
3.1.1	THE PREPARATION STAGE AND DEFINITIVE SYSTEM REQUIREMENTS.....	34
3.1.2	SIMULATION AND ANALYSIS PROCESS IN TOPOLOGICAL ATTACK CONDITIONS.....	35
3.1.3	SIMULATION AND ANALYSIS PROCESS WITH LAPLACIAN FEEDBACK.....	35
3.1.4	SIMULATION AND ANALYSIS PROCESS IN SITUATIONS OF CHANGING TOPOLOGY TYPES AND SIZES .....	37
3.2	POPULATION SAMPLING.....	38
3.3	DATA COLLECTION.....	38
3.4	TOOLS FOR DATA ANALYSIS.....	38
<b>CHAPTER 4 .....</b>		<b>40</b>
4.1	ATTACK SCENARIO.....	40
4.1.1	TOPOLOGICAL ATTACK.....	40
4.1.2	EFFECT OF LAPLACIAN SECOND SMALLEST EIGENVALUE FEEDBACK.....	42
4.1.3	SCALABILITY OF TOPOLOGY .....	46
4.2	ANALYSIS.....	52
4.3	DISCUSSION.....	67
<b>CHAPTER 5 .....</b>		<b>71</b>
5.1	CONCLUSION .....	71
5.2	RECOMMENDATIONS.....	71
<b>BIBLIOGRAPHY .....</b>		<b>72</b>
<b>APPENDICES .....</b>		<b>75</b>
<b>APPENDIX A .....</b>		<b>76</b>
<b>APPENDIX B .....</b>		<b>106</b>
<b>APPENDIX C .....</b>		<b>109</b>

---

## LIST OF TABLES

Table 2.1: Table of Classification Approach from various Time Synchronization Protocol and its Converging Performance .....	10
Table 2.2: List of Publication related to Laplacian and Gain Consensus .....	11
Table 2.3: Comparison of Convergence Speed in Sparse & Fully Topology (Xue, 2017)..	14
Table 2.4: Comparison between Time Synchronization Protocol and its Robustness Performance Under Attack.....	16
Table 2.5: Various of Graph and Eigenvalue Calculation .....	23
Table 2.6: No Convergence Achieved in Sparse Topology .....	27
Table 4.1: Robustness Performance of Consensus Result in Topological Attack.....	41
Table 4.2: Robustness Performance of Consensus Result in Topological Attack and Laplacian Feedback .....	45
Table 4.3: Robustness Performance of Consensus Result in Topological Attack, Laplacian Feedback & Scalability of Topology .....	49
Table 4.4: Weigthing Parameter of Laplacian gain.....	69

---

## LIST OF PICTURES

Figure 2.1: State-of-the-art of The Research .....	5
Figure 2.2: Three Synchronization Methods: Frequency Synchronization (a), Initial Offset Synchronization (b), Time Synchronization (c). [5] .....	6
Figure 2.3: The GPS, PPS & NTP Time Reference in WSN CPS [13].....	7
Figure 2.4: NTP Stratum Servers [13].....	8
Figure 2.5: Oscillator and Counter components of RTC Module [13] .....	8
Figure 2.6: Synchronization Process of Synchronizing Clock to Reference Clock.....	9
Figure 2.7: Multilevel classification of clock synchronization protocols.....	9
Figure 2.8: Process getting Laplacian Matrix from Communication Graph [10].....	14
Figure 2.9: The Concept of Consensus Control [10].....	14
Figure 2.10: Types of Consensus Time Synchronizations Attack.....	17
Figure 2.11: Clock Model of Time Synchronization .....	19
Figure 2.12: Connected Graph Network .....	26
Figure 2.13: MST of Connected Graph Network.....	26
Figure 2.14: Tree Representation of MST Connected Graph Network.....	27
Figure 2.15: Network Model of WSN Nodes Exchanging Messages.....	28
Figure 2.16: DoS Topology Attack Model in WSN Nodes.....	29
Figure 2.17: Network Model of WSN Node Attacked through Denial of service .....	30
Figure 2.18: Node Destruction Topology Attack Model in WSN Nodes.....	30
Figure 3.1: Existing and The Proposed Method using Laplacian Eigenvalue Feedback .	32
Figure 3.2: General Research Design Flowchart .....	33
Figure 3.3: Plot of Initial Offset and Skew Clock Value at Initial Stage .....	34
Figure 3.4: Second Stage Focusing on Attack Simulation .....	35
Figure 3.5: Third Stage Focusing on Laplacian Feedback as Gain Factor.....	36
Figure 3.6: Fourth Stage Focusing on Impact on Scalability of Topology.....	37
Figure 3.7: Fourth Stage Focusing on Impact of Scalability of Topology [4]; [11] .....	38
Figure 4.1: Simulation Result from Fully Connected 4 Nodes – No Attack.....	40
Figure 4.2: Simulation Result from Fully Connected 4 Nodes – DoS Attack .....	41
Figure 4.3: Simulation Result from Fully Connected 4 Nodes – Node Destruction Attack .....	41
Figure 4.4: Comparison Result from Fully Connected 4 Nodes – No Attack without (a) & with Laplacian gain (b) .....	44
Figure 4.5: Comparison Result from Fully Connected 4 Nodes – DoS Attack without (a) & with Laplacian gain (b).....	44
Figure 4.6: Comparison Result from Fully Connected 4 Nodes – Node Destruction Attack without (a) & with Laplacian gain (b).....	45
Figure 4.7: Comparison Result from Fully Connected 10 Nodes – No Attack without (a) & with Laplacian gain (b).....	47

Figure 4.8: Comparison Result from Fully Connected 10 Nodes – DoS Attack without (a) & with Laplacian gain (b) .....	48
Figure 4.9: Comparison Result from Fully Connected 10 Nodes – Node Destruction Attack without (a) & with Laplacian gain (b).....	48
Figure 4.10: Comparison Result from Fully Connected 10 Nodes – No Attack without (a) & with Laplacian gain (b).....	50
Figure 4.11: Comparison Result from Ring 10 Nodes – No Attack without (a) & with Laplacian gain (b) .....	50
Figure 4.12: Comparison Result from Star 10 Nodes – No Attack without (a) & with Laplacian gain (b) .....	52
Figure 4.13: Synchronization Convergence Speed in Fully Connected 4 Nodes.....	53
Figure 4.14: Synchronization Convergence Speed in Fully Connected 10 Nodes.....	54
Figure 4.15: Synchronization Convergence Speed in Fully Mesh 10 Nodes.....	55
Figure 4.16: Synchronization Convergence Speed in Ring 10 Nodes.....	56
Figure 4.17: Synchronization Convergence Speed in Star 10 Nodes.....	57
Figure 4.18: Accuracy in The Metrics of Global Synchronization Errors in Fully Connected 4 Nodes.....	58
Figure 4.19: Accuracy in The Metrics of Global Synchronization Errors in Fully Connected 10 Nodes .....	59
Figure 4.20: Accuracy in The Metrics of Global Synchronization Errors in Fully Mesh 10 Nodes.....	60
Figure 4.21: Accuracy in The Metrics of Global Synchronization Errors in Ring 10 Nodes ..	61
Figure 4.22: Accuracy in The Metrics of Global Synchronization Errors in Star 10 Nodes ..	62
Figure 4.23: Speed in Laplacian-Based Consensus Against Topology Attacks.....	63
Figure 4.24: Accuracy in Laplacian-Based Consensus Against Topology Attacks.....	64
Figure 4.25: Topology Scalability in Laplacian-Based Consensus .....	65
Figure 4.26: Attack Scalability in Laplacian-Based Consensus .....	66

## LIST OF ABBREVIATIONS

---

### Abbreviations Definition

ATS	Averaging Time Synchronization
ATSP	Averaging Time Synchronization Pairwise
CCS	Consensus Clock Synchronization
CSNI	Clock Skew Based Node Identification
CTS	Consensus Time Synchronization
CWA	Centralized Weight Assignment
DCO	Digitally Controlled Oscillator
DoS	Denial of Service
FTCCS	Finite-Time Consensus Based Clock Synchronization
FTSP	Flooding Time Synchronization Protocol
FWA	Fixed Weight Assignment
GPS	Global Positioning System
GSEr	Global Synchronization Error Rate
ILC-MSR	Iterative Learning Control-Based Mean Subsequence Reduced
IoT	Internet of Things
LE	Largest Eigen Value
MST	Maximum Time Synchronization
MWA	Mobile Weight Assignment
MMAR-CTS	Message Manipulation Attack Resilient CTS
NiSTS	Node Identification Based Secure Time Synchronization
NTP	Network Time Protocol
PBS	Pairwise Broadcast Synchronization
PPS	Pulse Per-Second
PTP	Precision Time Protocol
RBS	Reference Broadcast Synchronization
RFA	Reachback Firefly Algorithm
RTC	Real-Time Clock
RTSP	Robust and Secure Time Synchronization Protocol
SATS	Selective Averaging Time Synchronization SSCA
SMTS	Secure Maximum Time Synchronization
SSE	Second-Smallest Eigen Value
SSCA	Secure Synchronous Consensus Algorithm
TPSN	Time-Sync Protocol for Sensor Network
WMTS	Weighted Maximum Time Synchronization
WSN	Wireless Sensor Networks

## LIST OF NOTATIONS

Symbols	Definition
$N$	Number of nodes
$\bar{x}$	The average of node value
$a_{ij}$	Adjacency matrix
$x_i$	Value of node $i$
$x_j$	Value of node $j$
$i, j$	Nodes $i$ and $j$
$k$	Iteration
$\tau$	Continous time
$\omega$	Angular frequency of clock
$C_i(t)$	Clock value of node $i$ at time-stamp $t$
$\alpha$	Clock skew
$\beta$	Clock offset
$W$	General wieighting factor
$\hat{C}$	Compensated clock
$t$	Time
$A$	Adjacency matrix
$X$	Matrix $X$
$X$	Consensus value
$\gamma$	Confidence weighting parameter
$L$	Laplacian matrix
$D$	Degree of matrix
$\rho$	Weighting parameter
$d$	Degree value
$G$	Random connected graph
$I$	Idnode matrix
$\lambda$	Eigenvalues of the Laplacian matrix
$\lambda_1$	Second smallest eigenvalue
$\lambda_{N-1}$	Largest eigenvalue
$\eta$	Relative skew estimation value
$\hat{\alpha}$	Virtual skew
$\hat{\alpha}$	Virtual offset
$\hat{\tau}$	Virtual time
$\theta$	Local synchronization error rate
$V$	Set of vertices of graph $G$
$E$	Set of edges of graph $G$

---

# CHAPTER 1

## INTRODUCTION

This chapter discusses the background of this research. This chapter is divided into eight sections, research background, statement of the problem, objective and hypotheses, assumption, scope and delimitation, and significance of the study.

### 1.1 Research Background

Sensor network in Internet of Things (IoT) is an essential part of Cyber-Physical Systems that integrates the physical and digital worlds [1] and time synchronization becomes a highly crucial element within it [2]; [3]. The use of low-cost, efficient, and low-power sensor network technology in Wireless Sensor Network applications and protocols works in a coordinated and synchronized manner [4]. Everything from managing and debugging networks involves time properties, as in security services, localization, routing, and tracking. Correlating log files accurately among devices in the Wireless Sensor Networks (WSN) area becomes very difficult or even impossible without proper time synchronization, which can lead to behavioral conflicts, device damage, and unnecessary service losses [5]. Therefore, the security of the time synchronization process is a major concern where the properties of the system time settings can be relied upon, namely being secure and guaranteed, especially in algorithmic methods and synchronization protocols approaches.

The time synchronization process can be achieved by adding the current time difference with the local time of a clock to achieve a common time on all nodes in the WSN [4]. This occurs because the imperfections of the hardware clock fabrication result in the local time on a node drifting apart over time, necessitating a synchronization protocol to attain the same pace [6]. Many time synchronization protocols have been developed in recent years to ensure that data collected by sensors in the network have accurate, synchronized timestamps, and consistent data analysis. Protocols such as Network Time Protocol (NTP) and Precision Time Protocol (PTP) in synchronization over wired networks [7]. Reference Broadcast Synchronization (RBS), Time-Sync Protocol for Sensor Network (TPSN), and Flooding Time Synchronization Protocol (FTSP), specifically designed for resource-constrained WSNs using root node as a reference clock [8]; [9]. Furthermore, other protocols leveraging distributed reference clock such as ATS (Average Time Synchronization) and MTS (Maximum Time Synchronization) focus on reaching a common message agreement using averaging or maximum calculation methods in consensus [10]; [11]. Although many protocols have been developed, security concerns are also becoming increasingly critical, given the general nature of open WSN environments and their vulnerability to threats.

The development of time synchronization protocols in Wireless Sensor Networks (WSN) has been a significant focus of research in the last decade as mentioned above, both centralized and distributed-based, but security threat mitigation needs to be improved [12]. Many distributed based synchronization protocols using consensus algorithms have been widely discussed in recent years due to their robustness against



several security threats, such as topological attacks and data manipulation [12]. Protocols such as SATS [13], FTCCS [14], and SMTS [15] are designed to handle message manipulation attacks and demonstrate fast convergence. SATS uses parameter adjustment based on two-hop neighbor information to counter random data injections, while FTCCS employs ILC-MSR (Iterative Learning Control with Multi-Stage Resilience) to address deception attacks. SMTS incorporates message verification and authentication to combat message manipulation attacks. In contrast, NiSTS [16] and RTSP [3] also focus on handling Sybil and message manipulation attacks but with varying speeds and countermeasure techniques, such as maxclique-based identification and message filtering. Protocols like CSNI [17], which use centralized approaches, focus is on node classification to identify and handle Sybil attacks. The secure consensus mechanism of these protocols helps prevent dishonest or malicious nodes from significantly influencing the system time. It is worth noting that the performance of time synchronization and resilience to attacks in consensus algorithms are greatly influenced by the type and changes in topology; therefore, topology attacks are a major concern in this research to measure resilience under changing topology conditions during attacks.

In the context of Wireless Sensor Networks (WSNs) and consensus-based time synchronization methods, Fixed Weight Assignment (FWA), Centralized Weight Assignment (CWA), and Mobile Weight Assignment (MWA) [18] refers to different consensus weighting algorithms. FWA refers to a consensus weighting algorithm where a fixed weight is assigned to each neighboring node in the network. These fixed weights remain constant throughout the synchronization process. CWA involves a centralized node, such as a base station or a central controller, assigning weights to neighboring nodes in the network. These weights are typically based on factors such as node proximity, reliability, or communication quality. Furthermore, MWA is a consensus weighting algorithm where weights assigned to neighboring nodes are dynamically adjusted based on the mobility or changing conditions of nodes in the network. This allows for adaptive weighting to account for changes in network topology or node characteristics over time. However, all three weightings above, whether static like FWA or dynamic like CMA and CWA, are assumed to be indifferent to the topology conditions such as connectivity of a graph. Consequently, there is no assumptions that if such of topological attacks occurs will change those weighting methods. As it is known, the resilience of consensus-based time synchronization is highly dependent on the topology conditions or the adjacency matrix of the sensor network [4]. The adjacency matrix is closely related to the Laplacian graph, and the value of the second smallest eigenvalue on the Laplacian graph gives an idea of how strongly the graph is connected [19].

In mathematics and network theory, the Laplacian matrix or Laplacian operator is a matrix representing the connectivity of a graph or network [20]. In the context of consensus-based time synchronization in WSNs, the Laplacian matrix is often used to model the connectivity and relationships between nodes in the network. Laplacian-based consensus methods leverage properties of the Laplacian matrix to achieve synchronization among nodes by iteratively updating their local clocks based on information exchanged with neighboring nodes. The Laplacian matrix plays a fundamental role in understanding the dynamics of consensus algorithms and their resilience to topology attacks. Therefore, in this study, we propose a graph-based consensus synchronization weighting method on Laplacian eigenvalues to test

synchronization resilience in topology attacks by looking at two main parameters: convergence speed and synchronization accuracy [12].

Findings of this study showed that incorporating Laplacian Gain enhances fault tolerance, reduces convergence iterations by approximately 40.42%, and improves network accuracy by about 9.34%. This demonstrates the crucial role of Laplacian-based consensus methods in maintaining network stability and accuracy under topology changes, recommending their adoption for enhancing WSN resilience against attacks.

## 1.2 Statement of the Problem

The problem of this research is to measure the extent to which changes in attack trials affect the performance of consensus-based time synchronization systems on various network topologies, including Ring, Star, and Mesh. The convergence speed and accuracy of synchronization in consensus-based time synchronization systems are critically influenced by the network topology. The robustness of the consensus process can be challenged by various topology attacks on the network, such as Edge Attacks like Denial-of-Service attacks and Vertices Attacks like Node Destruction Attacks. It is essential to understand the extent of the impact these attacks have on different network topologies, including Ring, Star, and Mesh topologies, to devise strategies that enhance the resilience and reliability of time synchronization mechanisms under adverse conditions.

## 1.3 Objective and Hypotheses

The objective of this research is to analyze the impact of topology attacks on the robustness of time synchronization in Wireless Sensor Networks (WSN) using Laplacian-eigen value weighting. This analysis will focus on two main parameters: the convergence speed of synchronization, measured in terms of iteration magnitude, and the accuracy of synchronization, assessed through local and global synchronization error magnitude. Additionally, the research will evaluate the scalability of different topology types in handling such attacks, aiming to determine their robustness and adaptability under adverse conditions.

The premises of hypotheses in this research are as follows:

- Premise 1: M. Xue proved that the robustness of consensus-based time synchronization is greatly influenced by the adjacency matrix of the topology [4].
- Premise 2: Furthermore, Kriegleder et al. showed that adjacency matrix is closely related to the Laplacian Graph and the second smallest eigenvalue of the Laplacian Graph indicates how strongly the graph is connected [19].
- Premise 3: Also from Kriegleder et al. showed that the convergence time decreases in general with the algebraic connectivity of a network, which is valued as the second smallest eigenvalue for feedback weighting [19].
- Premise 4: Under topology changes based on M. Xue and Fajrin et al., then it will impact to the robustness of time synchronization [4]; [21].

Thus, the hypothesis in this research was: by incorporating Laplacian Eigen Value

feedback weighting, the clock synchronization condition will be more robust against topology changes in topology attacks.

## **1.4 Scope and Delimitation**

The limitations of this study include specific testing scenarios on the topology, which must adhere to Minimum Spanning Tree (MST) conditions to ensure consensus convergence. Additionally, the communication direction in wireless sensor networks involves two-way communication and no-delay involved, leading to an Undirected Graph pattern when represented graphically in perfect simulation condition. The evaluation of convergence speed relies on the iteration count parameter due to the dependence of time-based calculations on the computational capabilities of the simulation devices. These limitations shape the methodology and analysis approach of the research, highlighting the need for careful consideration and interpretation of the results within these defined constraints.

## **1.5 Significance of the Study**

By employing Laplacian-eigen value weighting, the research delves into the intricate relationship between network topology, adjacency matrices, and Laplacian Graphs. This investigation is vital as it sheds light on the fundamental mechanisms governing consensus-based time synchronization. The evaluation of convergence speed and synchronization accuracy serves as key performance indicators, offering insights into the network's robustness and adaptability in adverse conditions. The hypothesis formulated in this study underscores the potential for Laplacian eigen value feedback weighting to bolster the robustness of clock synchronization, presenting a promising avenue for enhancing network security and reliability in the face of topology attacks.

---

**CHAPTER 2****LITERATURE REVIEW**

This chapter provides a brief description of State of The Art and in the subchapter on "Time Synchronization in Wireless Sensor Networks," we explain the fundamental concept and significance of time synchronization in the context of sensor networks. "Time Synchronization Algorithms Based on Consensus and Non-Consensus" delves into various time synchronization algorithms used in sensor networks, including consensus-based and non-consensus-based algorithms, along with a comparison between the two. Moving on to "Graph Laplacian and Gain Consensus," we discuss the Laplacian graph and gain consensus, which are key concepts in consensus-based time synchronization methods. "Robustness Parameters in Attacks" outlines strength parameters in facing attacks, focusing on the security and resilience of the system against potential attacks in sensor networks. Lastly, "Theoretical Framework" presents the theoretical framework that serves as the basis for analysis in this research, including theories on time synchronization, consensus algorithms, and topology attacks in sensor networks. By exploring these topics, Chapter 2 aims to provide an in-depth understanding of the theoretical foundation relevant to this study.

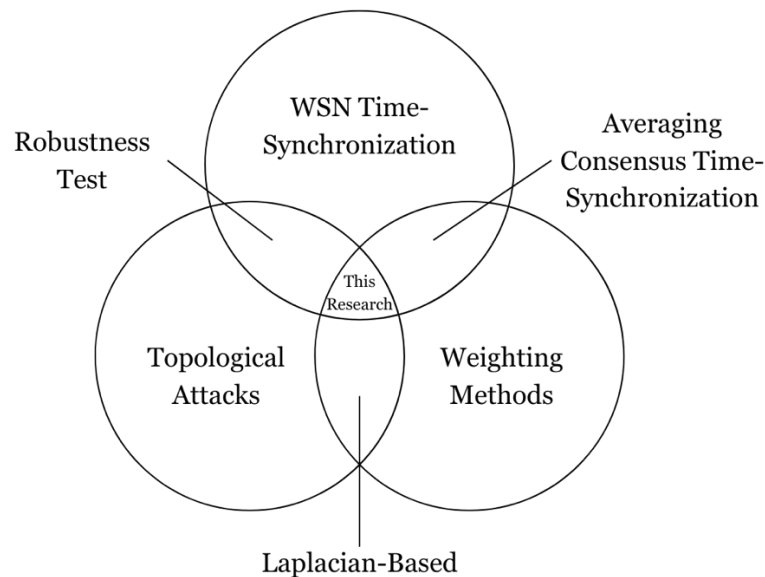
**2.1 State of The Art**

Figure 2.1: State-of-the-art of The Research

The numerous WSN Consensus Time Synchronization (CTS) algorithms and its weighting factor have been proposed in the literature, there is a notable gap in studying the Averaging-Time Synchronization leveraging Laplacian value to the weighting method under topological attacks [12], which reveals its significance performance under robustness test. The major contributions or state-of-the-art to this research as seen on

the intersections in Figure 2.1 are as given below:

1. First intersection, recent Averaging-Time Synchronization (ATS) algorithm are thoroughly analyzed through simulations, considering scenarios both with and without topological attacks [10].
2. Second intersection, leveraging Laplacian-based value to its weighting parameter in ATS algorithms to measure its robustness against topological attacks [19].
3. Third intersection, extensive simulations are conducted under scalability of the number nodes and topology types to assess impact of its robustness performance metrics [21] such as convergence speed and global synchronization error rate [12].

This research represents the first comprehensive effort to conduct simulation-based robustness testing of Laplacian-based value in Averaging-Time Synchronization algorithm under topological attacks.

### 2.1.1 Time Synchronization in Wireless Sensor Networks

Time synchronization is the process that ensures that clocks or time across various devices or endpoints in a system are at uniform or matching values [5]. In computer networks or distributed systems, time synchronization ensures that logs, records, or transactions are performed with accurate and uniform timestamps. When every node in the network shares the same time scale, it opens up opportunities to establish cause-and-effect relationships between events in the physical world and ensures that these nodes can integrate well within the overall network. Generally, time synchronization requires aligning clock frequencies (Frequency Synchronization), initial offsets (Initial Offset Synchronization), and time values (Time Synchronization).

#### 1. Frequency Synchronization

Frequency synchronization involves efforts to make nodes or nodes in the network have uniform oscillation frequencies. Uniform clock frequencies aim to ensure that devices in the network operate at the same time speed.

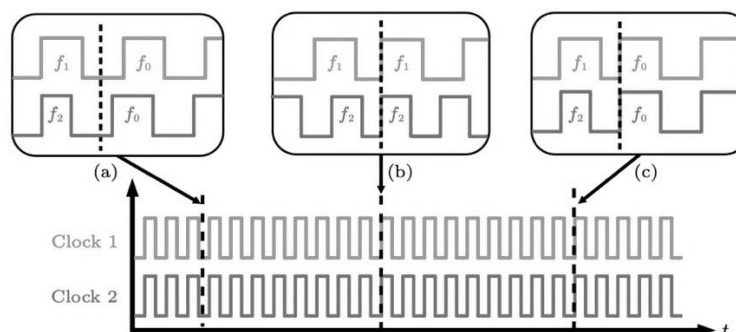


Figure 2.2: Three Synchronization Methods: Frequency Synchronization (a), Initial Offset Synchronization (b), Time Synchronization (c). [5]

#### 2. Initial Offset Synchronization

Initial offset refers to the difference between the local time when time synchronization begins, and the reference time used for synchronization. The initial offset needs to be adjusted so that the local time of all nodes in the network starts with a uniform value. This aims to maintain time consistency among nodes after time synchronization is performed.

### 3. Time Synchronization

Time synchronization is the process of making the local time values of each node in the network uniform or at least compatible with each other. Uniform time values enable nodes in the network to communicate and coordinate correctly.

Time synchronization in sensor networks plays an essential role in ensuring that various types of nodes agree on the same time to support accurate data collection and efficient coordination among sensor nodes [22]. Achieving time synchronization requires communication between nodes in the network through communication connections, whether wired or wireless. Here are some commonly used sources of synchronization in wireless sensor networks (WSNs):

#### 1. GPS/PPS

GPS/PPS (Global Positioning System/Pulse-Per-Second) in time synchronization is a commonly used method in wireless sensor networks (WSNs) to achieve high accuracy in time. The PPS signal is beneficial for achieving high time accuracy because it provides a clear starting point for each second. Time signals from GPS/PPS can be integrated with specialized WSN time synchronization protocols using GPS time information as the starting point in the time synchronization algorithm. Nodes in WSN equipped with GPS receivers use the time information received from GPS signals to synchronize local time.

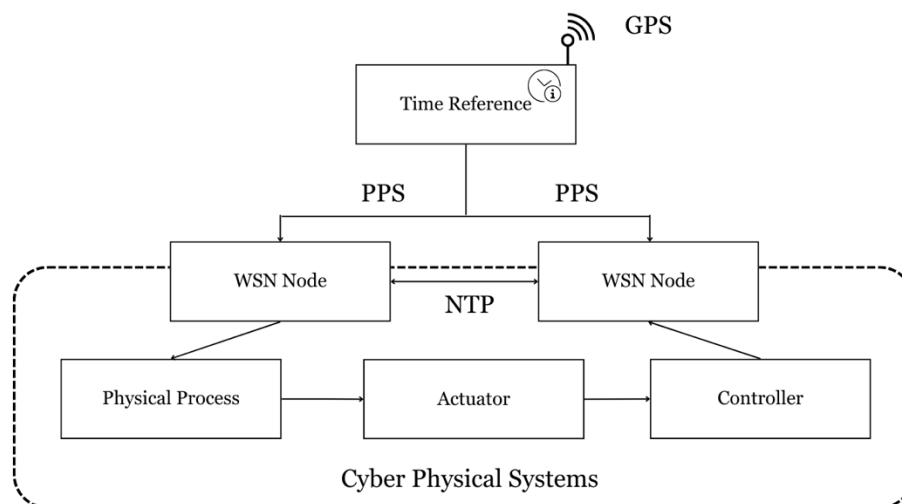


Figure 2.3: The GPS, PPS & NTP Time Reference in WSN CPS [22]

The PPS signal is used to synchronize time at the second level, providing high time precision. Time synchronization using GPS/PPS typically achieves time accuracy in the

range of microseconds to nanoseconds, depending on the quality and timing accuracy of the received GPS signal. However, the use of GPS and PPS receivers can consume significant power. Therefore, the use of GPS/PPS is usually limited to root nodes only as a reference or primary time comparator, as seen in protocols like Network Time Protocol (NTP).

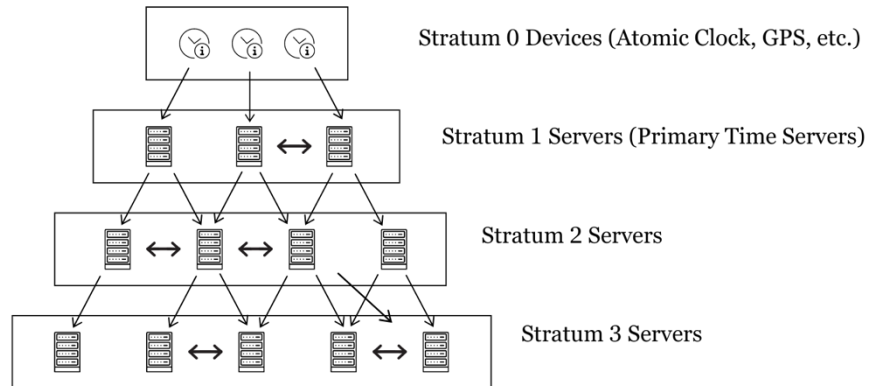


Figure 2.4: NTP Stratum Servers [22]

## 2. Hardware Clock

The hardware clock is a time source managed and generated by the sensor node itself. Nodes in wireless sensor networks have internal oscillators that produce local time. The hardware clock in a sensor node basically comes in two types: the internal hardware clock and the external on-board clock, commonly known as the Real-Time Clock (RTC) module [23]. The internal hardware clock is usually embedded within the microcontroller itself, for example, the MSP430 has a Digitally Controlled Oscillator (DCO) embedded with a working frequency of 8MHz, which means it has a clock resolution of  $0.125 \mu s$  (one 'tick') [17]; [24]; [10]. Therefore, every hardware clock is always accompanied by a counter register to read the hardware clock from the oscillator output and periodic pulses, and then be converted into a Software Clock for further time synchronization processing.

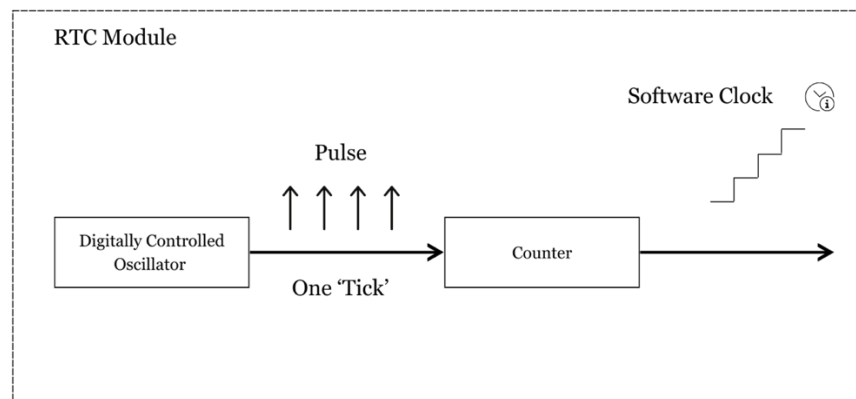


Figure 2.5: Oscillator and Counter components of RTC Module [22]

The internal clock is suitable for applications that require lower time accuracy or in environments where the cost and power consumption of additional devices need to be minimized. Applications that are more tolerant of time uncertainty or require more power-efficient solutions tend to use the internal clock. This is particularly suitable for use in WSN applications that are highly resource constrained [22].

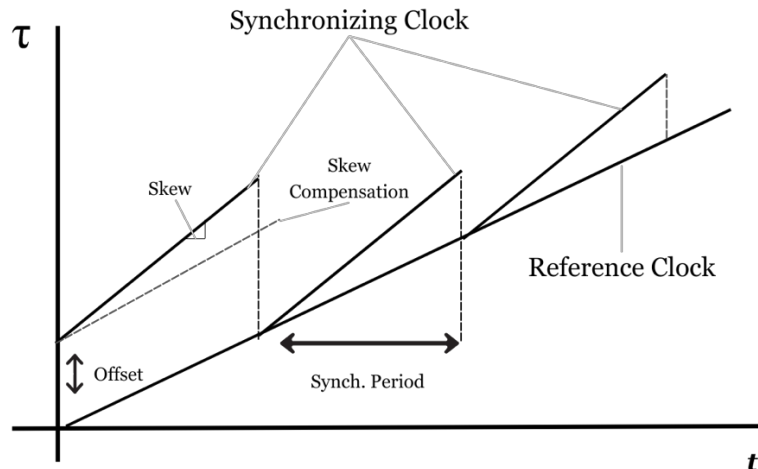


Figure 2.6: Synchronization Process of Synchronizing Clock to Reference Clock

### 2.1.2 Time Synchronization Algorithms Based on Consensus and Non-Consensus

Once the process of generating a software clock from quantifying the hardware clock, as described earlier, is established, the software clock can now serve as the local time indicator for the node, where time resolution can be described as the distance between two adjacent ticks. However, the process of reading the software clock is not always constant due to manufacturing variations and environmental conditions [5]. Each Local Oscillator in every node will result in drift and clock skew, which is common. Therefore, time synchronization is needed to ensure that the clock is always reliable and consistent across all nodes.

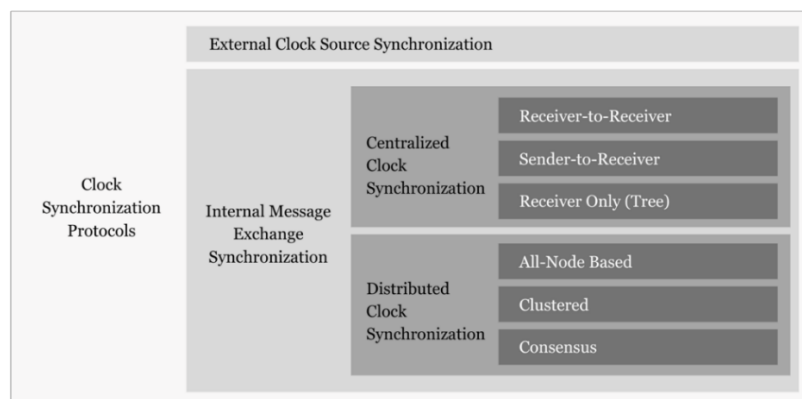


Figure 2.7: Multilevel classification of clock synchronization protocols



The synchronization process can be divided into two main parts: consensus-based synchronization algorithms and non-consensus-based synchronization algorithms.

### 1. Non-Consensus-Based Time Synchronization Algorithms

In general, non-consensus-based algorithms use a centralized or reference-based approach, similar to the use of Network Time Protocol (NTP) and Precision Time Protocol (PTP) in synchronization over wired networks [7]. However, NTP and PTP are less suitable for WSN applications as they consume significant resources, leading to the use of other protocol approaches such as Reference Broadcast Synchronization (RBS), Time-Sync Protocol for Sensor Network (TPSN), and Flooding Time Synchronization Protocol (FTSP), specifically designed for resource-constrained WSNs [8]; [9]. RBS is a protocol that utilizes receiver-to-receiver passing message exchange, where each node receives beacons that are then used to calculate clock offsets between them. TPSN is based on multi-hop sender-to-receiver communication. In contrast, FTSP works using a tree-like structure where the root node undergoes an authentication process using a propagated private key throughout the network. Other protocols also exist that employ optimization and multi hop-based overhearing approaches, such as PBS or Pairwise Broadcast Synchronization [25]. All these protocol approaches rely on non-consensus-based methods that require all nodes to participate in synchronization based on centralized reference.

Table 2.1: Table of Classification Approach from various Time Synchronization Protocol and its Converging Performance

No.	Protocol	Approach	Message Passing	Type of Consensus	Converging Speed
1	RBS [8]	Centralized	Receiver to Receiver		High
2	TPSN [9]	Centralized	Sender to Receiver		High
3	FTSP [26]	Centralized	Tree-based		High
4	PBS [25]	Distributed	Multi-hop		
5	ATSP [27]	Distributed	Consensus	Averaging	Convergence in Non-Finite Time
6	CCS [18]	Distributed	Consensus	Averaging	Exponential
7	ATS [10].	Distributed	Consensus	Averaging	Exponential
8	MTS [11]	Distributed	Consensus	Maximum	Fast Convergence
9	RFA [28]	Distributed	All node-based		
10	WMTS [29]	Distributed	Consensus	Maximum	Convergence in Non-Finite Time
11	This Research	Distributed	Consensus	Averaging	Fast Convergence

### 2. Consensus-Based Time Synchronization Algorithms

The underlying concept behind distributed-based approaches is the lack of dependence

on root nodes or references. This allows consensus-based systems to be more resilient to changes in network topology, where nodes can join or leave the network without significantly disrupting time synchronization. The consensus approach also provides better tolerance against fake nodes or unexpected behavior in the network, as time decisions can be made based on consensus.

Generally, there are three fundamental protocols in consensus-based time synchronization algorithms: RFA, ATS, and MTS. RFA or Reachback Firefly Algorithm is a protocol that listens to signals from its neighboring nodes but does not directly act upon these signals; instead, it queues them and sends them in the next cycle [28]. This is useful to compensate for delays during the reach back process. On the other hand, ATS (Average Time Synchronization) and MTS (Maximum Time Synchronization) focus on reaching a common message agreement using averaging or maximum calculation methods [10]; [11]. The idea is to calculate the average from local exchanged data and distribute the results across the network to achieve time agreement with a higher level of confidence. The ATS calculation requires significant information exchanges, resulting in slow convergence. Therefore, MTS improves upon ATS by maximizing local information in global synchronization, allowing for faster convergence even though deviations from the minimum and maximum values may affect confidence levels.

Other protocols like Consensus Clock Synchronization (CCS) [18] and Weighted Maximum Time Synchronization (WMTS) [11] are the development from previous protocols that emphasize weighting or confidence parameters as improvement variables. The clustering approach is also applied by ATSP or Averaging Time Synchronization Pairwise, which is simpler and divides by two [27]. This research focus on consensus-based averaging time synchronization algorithms in distributed WSN networks.

### 2.1.3 Graph Laplacian and Gain Consensus

The concept of consensus is increasingly recognized as part of distributed control systems, where information from various network nodes is exchanged to generate agreed-upon outputs or consensus outputs. The network nodes in distributed control systems are closely related, similar to the concept of a graph that has a number of nodes ( $n$ ) and connections ( $m$ ), allowing for an approach based on graph theory. The relationship between consensus and graph theory has been extensively discussed in several previous research studies as seen on the table below.

Table 2.2: List of Publication related to Laplacian and Gain Consensus

Year	Author	Publication	Point of Interest
2004 [30]	R. Olfati-Saber and R. Murray,	Consensus problems in networks of agents with switching topology and time-delays	analysis in connected the consensus control to algebraic graph theory
2004 [31]	J. Fax and R. Murray,	Information flow and cooperative control of vehicle formations	used tools from algebraic theory stated that a

Year	Author	Publication	Point of Interest
			Nyquist criterion that uses the eigenvalues of the graph Laplacian matrix to determine the effect of the communication topology on formation stability
2005 [32]	W. Ren and R. Beard	Consensus seeking in multiagent systems under dynamically changing interaction topologies	analysis of consensus control to matrix theory
2005 [33]	L. Moreau	Stability of multiagent systems with time-dependent communication links	connection between the performance of a linear consensus protocol on a directed network and the Fiedler eigenvalue of the mirror graph of the information flow
2016 [20]	Ahmad Sadhiqin Mohd Isira	Consensus Control of A Class of Non-linear Systems	state feedback consensus controller, consensus observer and observer-based controller using the relative information of the agents in a multi-agent system and eigenvalues from graph theory
2021 [34]	Yuqing Niu, Ting Yang, Yucheng Hou, Shaotang Cai, Peng Yan & Wei Li	Consensus tracking-based clock synchronization for the Internet of Things	analysis in the synchronization process in the state space framework & the convergence acceleration term is designed to optimize the eigenvalue distribution of synchronization error matrix
2024 [35]	Neshat Elhami Fard, Rastko Selmic	Consensus of Multi-agent Reinforcement Learning Systems: The Effect of Immediate Rewards	consensus control of a leaderless, homogeneous, multi-agent

Year	Author	Publication	Point of Interest
			reinforcement learning (MARL) system with rewards weighting.
2024	Author of This Research	The Use Laplacian Eigenvalue Feedback in Consensus-based Time Synchronization to Enhance Robustness in Sensor Networks	proposed a graph-based consensus synchronization weighting method using Laplacian eigenvalues to test resilience against topology attacks, focusing on convergence speed and synchronization accuracy

The research outlined in the table provides significant insights into consensus problems in multi-agent systems, leveraging mathematical frameworks like algebraic graph theory. In 2004, Olfati-Saber and Murray connected consensus control with algebraic graph theory, addressing how agents achieve agreement in networks with dynamic topologies and delays. Fax and Murray, in the same year, used algebraic tools to evaluate how communication topology affects vehicle formation stability, utilizing eigenvalues from the graph Laplacian matrix. The 2005 studies by Ren and Beard, and Moreau, further explored these concepts, with Ren analyzing consensus under changing interaction topologies through matrix theory, and Moreau linking linear consensus performance to the Fiedler eigenvalue, enhancing our understanding of stability in directed networks. Ahmad Sadhiqin Mohd Isira's 2016 research introduced new control strategies for non-linear systems, incorporating graph theory eigenvalues into state feedback and observer-based controllers. In 2021, Niu et al. optimized clock synchronization in the Internet of Things by designing a convergence acceleration term to improve the eigenvalue distribution of synchronization errors. Finally, Fard and Selmic's 2024 study on multi-agent reinforcement learning systems examined how immediate rewards affect consensus, using reward weighting in leaderless MARL systems. Together, these studies underscore the critical role of mathematical analysis in designing effective consensus mechanisms and improving system stability and performance.

There are some popular gain methods for weighted averaging consensus-based time synchronization methods in WSN, Fixed Weight Assignment (FWA), Centralized Weight Assignment (CWA), and Mobile Weight Assignment (MWA) refers to different consensus weighting algorithms [18]. FWA refers to a consensus weighting algorithm where a fixed weight is assigned to each neighboring node in the network. These fixed weights remain constant throughout the synchronization process. CWA involves a centralized node, such as a base station or a central controller, assigning weights to neighboring nodes in the network. These weights are typically based on factors such as node proximity, reliability, or communication quality. Furthermore, MWA is a consensus weighting algorithm where weights assigned to neighboring nodes are dynamically adjusted based on the mobility or changing conditions of nodes in the network. This allows for adaptive weighting to

account for changes in network or node characteristics over time. However, all three weightings above, whether static like FWA or dynamic like CMA and CWA, are assumed to be indifferent to the topology conditions such as connectivity of a graph using Laplacian value.

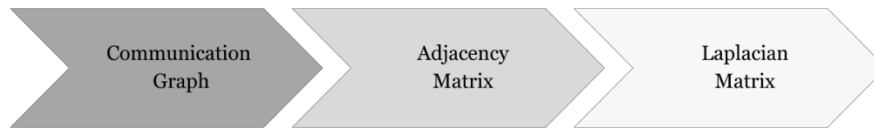


Figure 2.8: Process getting Laplacian Matrix from Communication Graph [20]

In consensus control systems, graph theory approaches are widely used to depict how a network of nodes is interconnected in a topology. This topology can take the form of a directed or undirected graph depending on the communication pattern between nodes, which is then calculated in the form of an adjacency matrix and subsequently converted into a Laplacian graph as feedback for consensus.

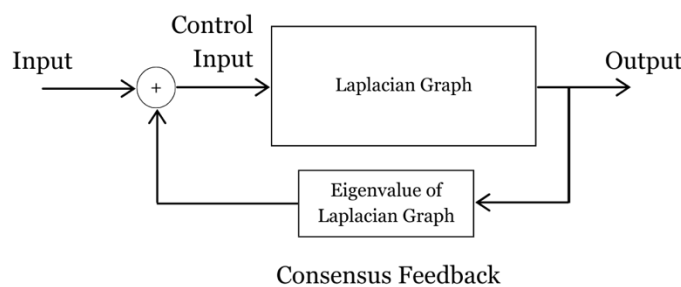
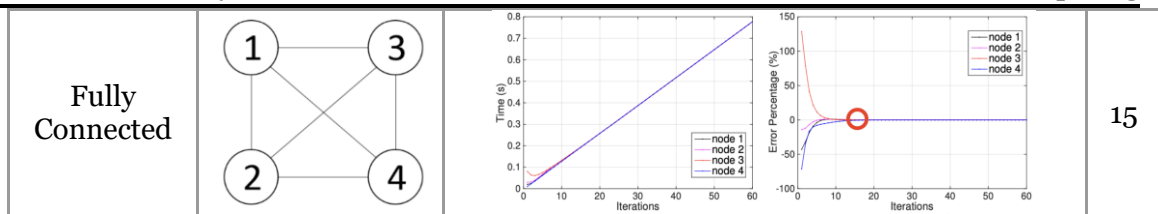


Figure 2.9: The Concept of Consensus Control [20]

The Laplacian matrix has several mathematical properties that make it useful in network analysis, including understanding the structure and consensus properties in dynamic systems. The Laplacian matrix is also used to analyze the convergence and stability of consensus systems in networks, which are typically calculated through Eigenvalues. By analyzing the Eigenvalues of a graph, it becomes easy to not only analyze how the graph is connected but also how well the graph is connected to each other, as in the perspective of Spectral Graph theory.

Table 2.3: Comparison of Convergence Speed in Sparse & Fully Topology [4]

Types	Topology	Convergence Speed	
Sparse Connected			20



Combining the two theories, namely the consensus control theory based on Laplacian graph and eigenvalue theory on spectral graph, where the consensus speed is greatly influenced by how well a graph is connected with its adjacency matrix, this research focus on consensus gain based on Laplacian graph. This consensus gain includes achieving consensus or agreement on gain values or control parameters among nodes in the network based on the eigenvalue of the Laplacian graph. The integration of these two theories in this study aims to analyze convergence regarding how interactions among nodes in the network can affect consensus on gain values or other parameters such as changes in topology and under attack conditions.

#### 2.1.4 Robustness Parameters under Attacks

Consensus-based synchronization algorithms are becoming increasingly popular because they are more resistant to various attacks, including denial of service attacks or attacks targeting root nodes [12]. This is primarily due to their distributed nature and lack of dependency on reference nodes, making them more robust against attacks. Robustness, in this context, refers to the system's ability to tolerate failures when facing topology changes or node failures in communication [36], whether under normal conditions or specific attacks, while still maintaining synchronization with a predefined level of accuracy [5]; [1].

The key components of robustness parameters in consensus-based synchronization events include convergence speed represented by the unit of iterations and synchronization accuracy represented by the global synchronization error rate (GSEr).

Table 2.4: Comparison between Time Synchronization Protocol and its Robustness Performance Under Attack

No	Qualitative Metrics							Quantitative Metrics		
	Protocol	Approach	Message Passing	Type of Consensus	Type of Attack	Countermeasures Approach	Converging Speed	Hop Count	Network Size	% Attacker Nodes
1	SATS [13]	Distributed	Consensus	Averaging	Random Data Injection	Parameter Adjustment based on Two-Hop Neighbor Information	Fast Convergence	2	50	20
2	SSCA [37]	Distributed	Consensus	Averaging	Message Manipulation Attack	Verification Process and Max-Min State Deviation		1	10	10
3	FTCCS [14]	Distributed	Consensus	Maximum	Deception Attack	ILC-MSR	Fast Convergence	1	9	22
4	SMTS [15]	Distributed	Consensus	Maximum	Message Manipulation Attack	Message Verification and Authentication	Fast Convergence	1	100	5
5	RTSP [3]	Distributed	Consensus	Maximum	Sybil Attack	Maxclique-Based Identification	Exponential	2	100	3
6	NiSTS [16]	Distributed	Consensus	Maximum	Sybil & Message Manipulation Attack	Message Filtering-based Node Identification	Slow	2	30	16
7	MMAR-CTS [12]	Distributed	Consensus	Averaging	Message Manipulation Attack	Message Manipulation Attack Resilience Algorithm	Fast Convergence	2	100	5
9	CSNI [17]	Centralized	Multi-hop		Sybil Attack	Based on FTSP. Using Node Classification. 0.15ppm. If there is only one average clock skew in the group, stated it as normal node.			7	14
10	This Research	Distributed	Consensus	Averaging	Topological Attack	Laplacian Eigenvalue Feedback	Fast Convergence	1	10	10

The table provides a comparison of various time synchronization protocols and their robustness against different types of attacks. Protocols such as SATS [13], FTCCS [14], and SMTS [15] are designed to handle message manipulation attacks and demonstrate fast convergence. SATS uses parameter adjustment based on two-hop neighbor information to counter random data injections, while FTCCS employs ILC-MSR (Iterative Learning Control with Multi-Stage Resilience) to address deception attacks. SMTS incorporates message verification and authentication to combat message manipulation attacks. In contrast, NiSTS [16] and RTSP [3] also focus on handling Sybil and message manipulation attacks but with varying speeds and countermeasure techniques, such as maxclique-based identification and message filtering.

For protocols like CSNI [17], which use centralized approaches, the focus is on node classification to identify and handle Sybil attacks, with a stated accuracy of 0.15ppm. The figure illustrates the performance metrics or attack resilience strategies of these protocols, emphasizing the trade-offs between convergence speed, network size, and attack resistance (Figure 2.10). In this study, focusing on testing the robustness of the proposed method, namely Laplacian-based consensus time synchronization, only against topology attacks on  $G = (V, E)$  such as Edge ( $E$ ) Attack refers to Denial of Service attack and Vertices ( $V$ ) Attack refers to Node Destruction Attack.

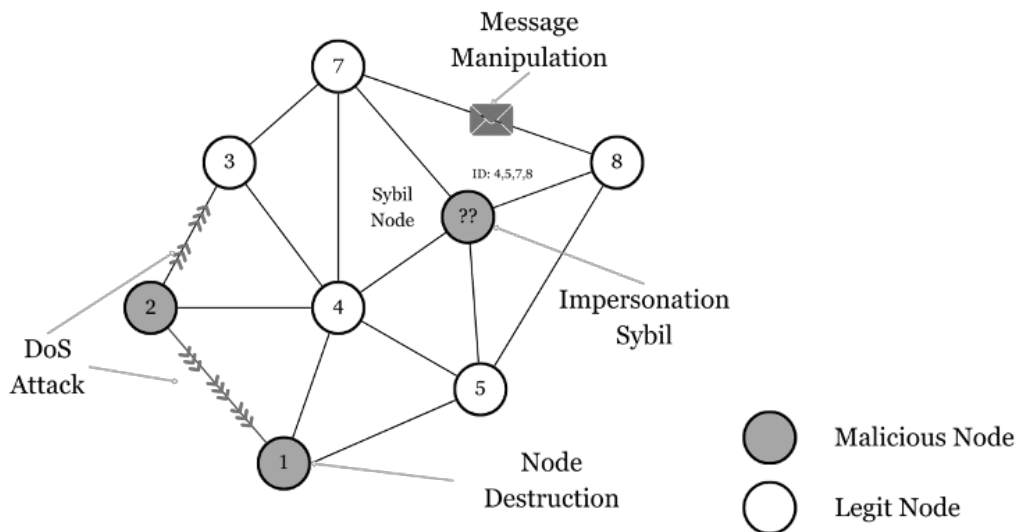


Figure 2.10: Types of Consensus Time Synchronizations Attack

The study also assesses the extent of influence of changes in the experimental attacks with different types of topologies based on the latest research [21] that Ring, Star & Mesh topologies will converge to the consensus. Here are each of the details:

a. Ring Topology

A network topology in which each device is connected to exactly two other



devices, forming a circular configuration. Data travels around the ring in one direction, passing through each device until it reaches its destination.

b. Star Topology

A network topology in which all devices are connected directly to a central hub or switch. All data transmissions pass through the central hub, which manages the flow of information between devices.

c. Mesh Topology

A network topology in which each device is connected to every other device in the network, creating multiple paths for data to travel. This redundancy enhances reliability and fault tolerance but requires more cabling and configuration compared to other topologies.

## 2.2 Theoretical Framework

### 2.2.1 Consensus Theory

Network consensus is the way nodes or nodes in a network reach an agreement on a certain value or state [20]. Network consensus is crucial in distributed systems and distributed networks, where nodes scattered across the network need to collaborate to achieve agreement or consensus. The main goal of network consensus is to reach an agreement among nodes in the network regarding a specific value or state. This may include agreement related to data, decisions, or actions that need to be taken by these nodes. Consensus theory considers various network models, including distributed networks, sensor networks, control networks, and so on [20]. The network structure and how nodes are interconnected are key factors in the consensus process. The goal of consensus is to achieve the average value  $\bar{x}_i$  of all values  $x_i$ .

$$\bar{x}_i(t) = \frac{1}{N} \sum_{j \in N} x_j(t) \quad (2.1)$$

Thus, based on the adjacency matrix  $a_{ij}$ , [19] and this process could occurs over a sufficiently long iteration, we can model it in iteration  $k$  and the next iteration  $k + 1$  until convergence is reached as follows [20]:

$$x_i(k + 1) = \sum_{j \in N} a_{ij}(k) (x_j(k) - x_i(k)) \quad (2.2)$$

Where:

- $\bar{x}$  : the average of node value
- $N$  : number of nodes
- $a_{ij}$  : adjacency matrix
- $x_i$  : value of node  $i$
- $x_j$  : value of node  $j$

$i, j$  : nodes  $i$  and  $j$

- Initialization of Values: Each node  $i$  and  $j$  has an initial value  $x_i$  and  $x_j$
- Communication: Each node  $i$  and  $j$  shares the values  $x_i$  and  $x_j$  with other nodes in their neighborhood matrix.
- Value Update: Each node updates its value based on the values received from other nodes where  $x(k + 1)$  is the updated value for node  $i$  with respect to  $j$  in iteration  $k + 1$ , and  $x_j(k)$ ,  $x_i(k)$  are the values received from nodes  $i$  and  $j$  in iteration  $k$ .
- Iteration & Convergence: The communication and value update process are repeated over several iterations until the values of each node converge to within a specified tolerance level, approaching zero, indicating a convergent state [30].

## 2.2.2 Theory of Consensus-Based Time Synchronization

### 2.2.2.1 Clock Model

The consensus-based time synchronization approach, it differs slightly from the general consensus theory where the time value is not only represented by a static value, considering each network node is associated with a hardware-based clock oscillator. Naturally, each hardware oscillator has production imperfections that cause its value to change according to its angular frequency [18], which can be referred to as clock skew.

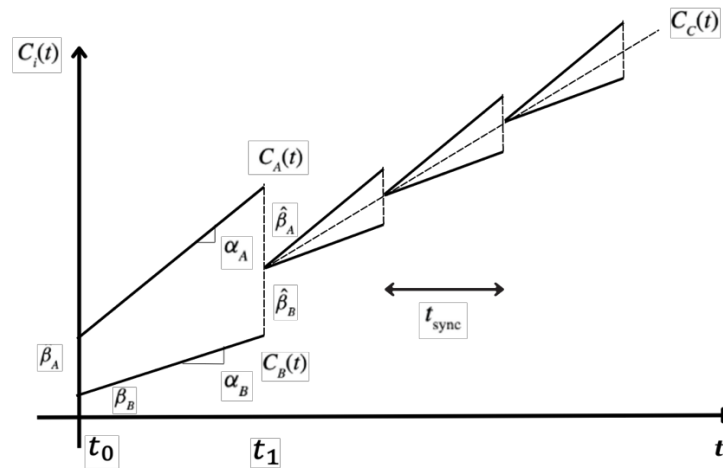


Figure 2.11: Clock Model of Time Synchronization[18]

Where  $\omega(\tau)$  is the characteristic angular frequency of the oscillator that varies with time and conditions, resulting in a unique function for each hardware, and  $k$  is its proportional coefficient, while  $C(t_0)$  is the initial clock value at  $t = 0$  [18].

$$C(t) = k \int_{t_0}^t \omega(\tau) d\tau + C(t_0) \quad (2.3)$$

If in the approach of the angular frequency of the oscillator can be considered a

constant value, then at node  $i$ , the clock value can be represented as in Eq(2.4) [18] where  $\alpha_i$  is the clock skew and  $\beta_i$  is the clock offset.

$$C_i(t) = \alpha_i t + \beta_i \quad (2.4)$$

In a perfect condition,  $\alpha_i$  would be 1, so over time its value would remain stable, and synchronization might not be necessary. However, in reality, the value of  $\alpha_i$  could be greater or less than 1. In the equation below Eq(2.5), during the convergence process, it is necessary to compare node  $i$  with  $j$  where  $\alpha_{ij}$  is the relative skew and  $\beta_{ij}$  is the relative offset. In the convergence condition, the values would be  $\alpha_{ij} = 1$  and  $\beta_{ij} = 0$ .

$$C_i(t) = \alpha_{ij} t + \beta_{ij} \quad (2.5)$$

### 2.2.2.2 Consensus Clock Model and Weighting

The consensus clock model is not significantly different from the general consensus equation Eq(2.2), except that the value  $x_i$  will be replaced by the value  $C_i$ , where  $C_i$  contains the clock equation as in Eq(2.6).  $C_i(k + 1)$  represents the local time value at iteration  $k$  and  $\varepsilon$  is the step weight value of each iteration performed [11].

$$C_i(k + 1) = C_i(k) + \varepsilon \sum_{j \in N} (C_j(k) - C_i(k)) \quad (2.6)$$

In general, the linear equation above can be simplified as shown in equation Eq(2.7), where the next clock value  $C_i(k + 1)$  depends on the weighting values  $W$ , which is the weighting matrix. Several studies in the last decade have their own approaches regarding this weighting, including CMA weighting, FWA weighting, and CWA weighting [11].

$$C_i(k + 1) = W C_i(k) \quad : \quad k = 0, 1, 2, \dots \quad (2.7)$$

The first consensus clock weighting is Cumulative Moving Average, abbreviated as CMA [18]. It's a weighting method that evenly weights each received clock and at each consensus calculation step. The weight value increases cumulatively based on the communication range  $R$  of its neighborhood matrix.

$$\hat{C}_i^+(t_j) = \frac{j\hat{C}(t_j) + \hat{C}(t_j)}{j+1} \quad i = 1 \dots N, \forall j \in R_i \quad (2.8)$$

Where:

$\hat{C}$  : compensated clock

$t_j$  : time at node  $j$

$j$  : value of node  $j$

The second consensus clock weighting is FWA [18], which stands for Forward Weighting Average. It's the simplest weighting method, requiring very basic operations, hence referred to as the lightest weighting method.

$$\hat{C}_i^+(t_j) = \frac{\hat{c}(t_j) + \hat{C}(t_j)}{2} \quad i = 1 \dots N, \forall j \in R_i \quad (2.9)$$

The third consensus clock weighting is based on the parameter confidence, called Confidence Weighting Average [18]. Its value depends on the parameter  $\gamma$  of each node, and the next  $\gamma+$  value will always increase by 1 in each operation until reaching the consensus value. This weighting method is considered a confidence parameter where caution in adding weighting gradually enhances its consensus approximation.

$$\begin{aligned} \hat{C}_i^+(t_j) &= \hat{C}_i(t_j) + \frac{\gamma_j}{\gamma_i + \gamma_j} (\hat{C}_j(t_j) - \hat{C}_i(t_j)) \\ \gamma_i^+ &= \gamma_i + 1 \quad i = 1 \dots N, \forall j \in R_i \end{aligned} \quad (2.10)$$

Where:

- $\hat{C}$  : compensated clock
- $\gamma$  : confidence weighting parameter
- $t_j$  : time at node  $j$
- $j$  : value of node  $j$

However, all three weightings above, whether static like FWA or dynamic like CMA and CWA, are assumed to be indifferent to the topology conditions. Furthermore, from a simple equation, we can conclude that the convergence speed is greatly influenced by the shape and type of its topology, as shown in the following equation Eq(2.10)

$$X = \mathbf{A}[X] \quad (2.11)$$

Where:

- $X$  : consensus value
- $\mathbf{A}$  : adjacency matrix
- $\mathbf{X}$  : matrix  $X$

In this solution, weighting process will be done using a topological approach, namely using Laplacian weighting. The convergence of consensus is greatly influenced by its neighborhood matrix  $\mathbf{A}$  or may depend on its Laplacian matrix, where the relationship between the Laplacian matrix  $\mathbf{L}$  and the Adjacency Matrix  $\mathbf{A}$  is as follows:  $\mathbf{L} \triangleq \mathbf{D} - \mathbf{A}$ . Here,  $\mathbf{D}$  is the Degree Matrix, so the equation can be further simplified as follows [30]:

$$X = -\mathbf{L}[X] \quad (2.12)$$

Where:

- $X$  : consensus value
- $\mathbf{L}$  : Laplacian matrix
- $\mathbf{X}$  : matrix  $X$

Thus, in a simplified equation form, clock synchronization using Laplacian weighting can also be represented as  $-\mathbf{L} = \mathbf{W}$ .  $\mathbf{W}$  is weighting factor.

$$C(k+1) = -L[C_k] \quad (2.13)$$

### 2.2.2.3 Laplacian Weighting and Eigenvalues

The Laplacian matrix  $L$  is a mathematical tool that reflects the network structure and is used in the context of consensus to achieve agreement among nodes or nodes in the network. The Laplacian matrix can be used to represent the structural relationships between nodes in a network, consisting of the Adjacency Matrix  $A$  and  $D$  is the Degree Matrix Eq(2.14). This provides an overview of how each node is connected to other nodes

$$L \triangleq D - A \quad (2.14)$$

The Laplacian matrix itself can be formed from elements as follows Eq(2.15) [19], where  $d_i$  represents the number of neighbors (degree) of node  $i$ , which will correspond to the guarantee of consensus convergence, similar to the tuning parameter  $\alpha$  in equation Eq(2.16) [1].

$$L_{ij} = \begin{cases} d_i & i = j, \\ -1 & \{i, j\} \in \varepsilon, \\ 0 & otherwise, \end{cases} \quad (2.15)$$

$$0 < \rho < \frac{1}{d_{max}}, \quad (2.16)$$

Where:

$\rho$  : weighting parameter

Characteristics of the Laplacian matrix for an undirected graph  $G$  [20] are provided by the following proposition:

1. The sum of entries in each row of the Laplacian matrix  $L(G)$  is zero.
2. The matrix  $L(G)$  is an  $n \times n$  matrix where  $n$  denotes the number of vertices in graph  $G$ .
3. The Laplacian matrix  $L(G)$  is symmetric and has orthogonal eigenvectors.
4. The smallest eigenvalue is zero with multiplicities equal to the number of connected components of the graph. If the graph is connected, the multiplicity of the eigenvalue zero is 1 and is associated with the constant eigenvector

Properties of the Laplacian matrix, such as eigenvalues  $\lambda$  and eigenvectors  $v = [\lambda_0, \lambda_1, \dots, \lambda_{N-1}]$ , can provide insights into how the consensus process will evolve. These values provide relevant information about the structure and behavior of the network represented by the Laplacian matrix as follows [20]:

$$\det(L - \lambda I) = 0 \quad (2.17)$$

Where:

$L$  : Laplacian matrix

$I$  : idnode matrix

$\lambda$  : eigenvalues of the Laplacian matrix

The convergence time generally decreases with the algebraic connectivity of a network, defined as the second smallest eigenvalue  $\lambda_1(L)$  and also the largest eigenvalue  $\lambda_{N-1}(L)$  of the Laplacian matrix [19]. Both of these values can contribute to the constellation as follows:

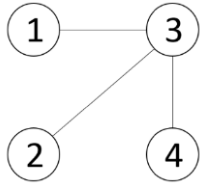
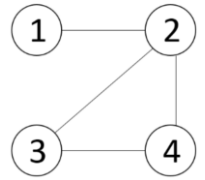
a. Second Smallest Eigenvalue

The second smallest eigenvalue is often associated with the convergence speed of the synchronization process [19]. In the context of synchronization, particularly in networked systems, the second smallest eigenvalue is related to the relaxation time of the system. As greater as second smallest eigenvalue will imply to a faster convergence towards synchronization. This convergence rate can be crucial in practical applications where rapid synchronization is desired, such as in communication networks or power grids.

b. Largest Eigenvalue

On the other hand, the largest eigenvalue is associated with the overall stability of the synchronized state [19]. In the synchronization process, stability is crucial for maintaining coordinated behavior among nodes in the system. If the largest eigenvalue is less than one in magnitude, it indicates that the synchronized state is stable, and small disturbances will decay over time, bringing the system back to synchronization. Conversely, if the largest eigenvalue is greater than one, it implies instability, where even small disturbances can lead to deviations from the synchronized state.

Table 2.5: Various of Graph and Eigenvalue Calculation

Types	Topology	Eigenvalue Calculation
Sufficient Connected		$\det \left( \begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 3 & -1 & -1 \\ 0 & -1 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right) : \lambda^4 - 6\lambda^3 + 9\lambda^2 - 4\lambda$ <p>Solve <math>\lambda^4 - 6\lambda^3 + 9\lambda^2 - 4\lambda = 0</math>: <math>\lambda = 0, \lambda = 1</math> with multiplicity of 2, <math>\lambda = 4</math></p>
Sparse Connected		$\det \left( \begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 3 & -1 & -1 \\ 0 & -1 & 2 & -1 \\ 0 & -1 & -1 & 2 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right) : \lambda^4 - 8\lambda^3 + 19\lambda^2 - 12\lambda$ <p>Solve <math>\lambda^4 - 8\lambda^3 + 19\lambda^2 - 12\lambda = 0</math>: <math>\lambda = 0, \lambda = 1, \lambda = 3, \lambda = 4</math></p>

Fully Connected		$\det \left( \begin{pmatrix} 3 & -1 & -1 & -1 \\ -1 & 3 & -1 & -1 \\ -1 & -1 & 3 & -1 \\ -1 & -1 & -1 & 3 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right) : \lambda^4 - 12\lambda^3 + 48\lambda^2 - 64\lambda$ <p>Solve <math>\lambda^4 - 12\lambda^3 + 48\lambda^2 - 64\lambda = 0</math>: <math>\lambda = 0, \lambda = 4</math> with multiplicity of 3</p>
--------------------	--	---

In cases where all node nodes have knowledge of the entire graph represented by the Laplacian matrix, all node nodes can calculate the optimal tuning parameter  $\alpha$  that minimizes the convergence time for a network as follows [19]:

$$\rho = \frac{2}{\lambda_1(L) + \lambda_{N-1}(L)} \quad (2.18)$$

Where:

- $\rho$  : weighting parameter
- $\lambda_1$  : second smallest eigenvalue
- $\lambda_{N-1}$  : largest eigenvalue

This equation will serve as an alternative topology-based weighting approach in consensus-based time synchronization, specifically in tuning its weighting parameters.

#### 2.2.2.4 The Averaging Time Synchronization (ATS) Algorithm

Referring to section 2.1.2 on consensus-based time synchronization algorithms, the author focuses on discussing the averaging algorithm because it provides better confidence levels. Therefore, this discussion will focus on the ATS or Averaging Time Synchronization algorithm. Generally, the synchronization process of the ATS algorithm is divided into three parts: relative skew estimation, skew compensation, and offset compensation [10].

##### 1. Relative Skew Estimation

Essentially, the process of estimating relative skew is necessary to establish a reference to its neighboring nodes that are interconnected to decide how to adjust. Let's say node  $j$  sends its local time  $\tau_j(t_1)$  to node  $i$ , then node  $i$  receives the packet and immediately records its local time as  $\tau_i(t_1)$ . Subsequently, both values are stored at node  $i$  and saved in memory as an array. Then, the second packet will occur in the next iteration, namely  $\tau_i(t_2)$  and  $\tau_j(t_2)$ , and a relative calculation will be performed against the previous values, as follows in the equation, where  $\eta_{ij}^+$  is the next relative skew estimation value and  $\rho_n \in (0,1)$  represents its tuning parameter.

$$\eta_{ij}^+(t_k) = \rho_n \eta_{ij} + (1 - \rho_n) \frac{\tau_j(t_2) - \tau_j(t_1)}{\tau_i(t_2) - \tau_i(t_1)} \quad (2.19)$$

Therefore, in continuous time, equation Eq(2.19) will become the skew  $a_{ij}$  with equations Eq(2.20) and Eq(2.21) in iterations towards the infinite limit.

$$\eta_{ij}^+(t_k) = \rho_\eta^K \eta(0) + \sum_{i=1}^{k-1} (1 - \rho_\eta) a_{ij} = \rho_\eta^K \eta(0) + a_{ij}(1 - \rho_\eta^K) \quad (2.20)$$

$$\lim_{k \rightarrow \infty} \eta_{ij}(t_k) = a_{ij} \quad (2.21)$$

## 2. Skew Compensation

The next process is to calculate skew compensation, commonly referred to as virtual skew. Virtual skew calculation involves assigning the relative skew between node nodes in the previous process, resulting in virtual skew  $\hat{\alpha}_i$ , where  $\rho_v \in (0,1)$  represents its tuning parameter.

$$\hat{\alpha}_i^+ = \rho_v \hat{\alpha}_i + (1 - \rho_v) \eta_{ij} \hat{\alpha}_j \quad (2.22)$$

## 3. Offset Compensation

The final process before combining all values into virtual time, denoted as  $\hat{\tau}_i$  equal to  $\hat{\alpha}_i * t + \hat{\delta}_i$ , is to calculate the virtual offset or offset compensation to achieve convergence. This is the intriguing aspect of consensus clock compared to general consensus, where, according to Eq(2.5), skew and offset play crucial roles in convergence. When skew has been virtually approximated for convergence, the next step is to adjust the offset according to the following equation:

$$\hat{\delta}_i^+ = \hat{\delta}_i + (1 - \rho_o) + (\hat{\tau}_j - \hat{\tau}_i) = \hat{\delta}_i + (1 - \rho_o) + (\hat{\alpha}_j \tau_j + \hat{\delta}_j - \hat{\alpha}_i \tau_i + \hat{\delta}_i) \quad (2.23)$$

Where  $\hat{\delta}_i$  is the virtual offset,  $\hat{\alpha}_{ij}$  is the virtual skew, and  $\rho_o \in (0,1)$  is its tuning parameter. Thus, in iterations towards infinity, the virtual time of node  $i$   $\tau_i$  and the virtual time of node  $j$   $\tau_j$  will have the same value, referred to as convergence.

$$\lim_{t \rightarrow \infty} \hat{\tau}_i(t) = \hat{\tau}_i(t), \quad \forall(i,j) \quad (2.24)$$

Referring to Laplacian weighting in section 2.2.2.3 using eigenvalue [19], all tuning parameters will follow Eq(2.18), where  $\rho_n = \rho_v = \rho_o = \in L$

### 2.2.3 Minimum Spanning Tree

Tree is a special type of graph that does not have closed circuits or cyclic circuits. This means that every two nodes in the tree are connected by a unique path, and there are no circuits that loop back to the initial node without passing through the same node twice



[38]. A tree also consists of nodes connected by edges. Trees can help organize and manage the flow of information or data within the network. One common implementation of trees in networks is through a network structure called a "spanning tree" in network protocols.

Minimum Spanning Tree (MST) is one of the valuable concepts in Graph Theory that has wide applications in optimization problems, especially in the context of network design and optimization. MST is often used as the basis or "backbone" in solving network design problems by adding various additional constraints or limitations. Constraints added to the MST include degree, distance, flow, connectivity, and others. The common problem of minimum spanning tree is to determine the edges of a graph that will be selected to connect all points in the graph with the condition that no circuit is formed. In an unweighted graph, this problem can be solved as follows:

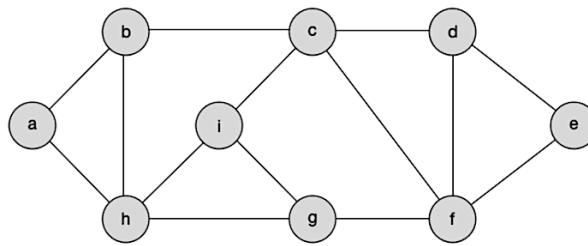


Figure 2.12: Connected Graph Network

Imagine there is a graph as shown above, then the way to determine it is as follows:

1. If starting from node a to create a route so that all nodes can be visited, the first thing to do is to use breadth-first search to the nearest nodes, namely b & h.
2. After b & h are visited then, b will continue to c and h will continue to i & g
3. Because c, i, and g have been visited along the route, then the paths i-c and i-g are not needed
4. So on and so forth until reaching the tree path as follows:

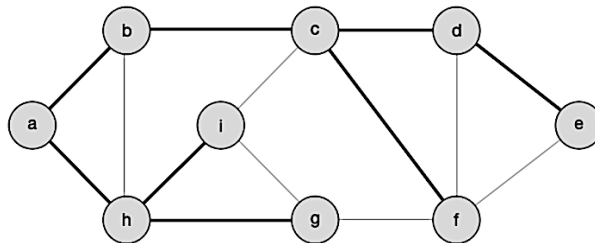


Figure 2.13: MST of Connected Graph Network

Another representation from 4 steps above would likely become like this on the tree diagram:

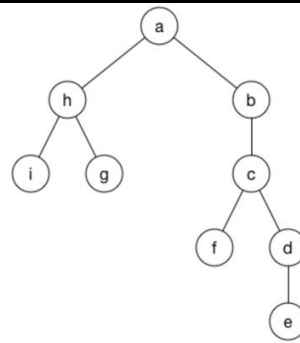


Figure 2.14: Tree Representation of MST Connected Graph Network

In a consensus approach, the ATS algorithm works very efficiently and optimally when in a strongly connected topology; however, it's a different story when the graph is not strongly connected. Therefore, the Minimum Spanning Tree approach must be a prerequisite for achieving convergence under such conditions. Previous research [4] has demonstrated that scenario without achieving a Minimum Spanning Tree (MST), consensus cannot be achieved.

Table 2.6: No Convergence Achieved in Sparse Topology

Types	Topology	Convergence Speed		
Sparse Connected				No

The incident occurred because the communication between nodes became severely limited, affecting the estimation of relative skew, thus making it unable to guarantee convergence towards its virtual skew and virtual offset. Therefore, this serves as a limitation in attacks to still measure synchronization performance in attacks that are still within the characteristics of a graph with MST

### 2.2.4 Performance of Time Synchronization Consensus Robustness Against Attacks

The robustness of time synchronization consensus will be measured in terms of two parameters: the synchronization convergence speed represented by the unit of iterations, and the synchronization accuracy represented by the global synchronization error rate (GSEr) as discussed in Section 2.1.4. Through these parameters, it can be concluded whether a synchronization is more resistant to topology attacks.

#### 2.2.4.1 Performance of Synchronization Error & Convergence Speed

As commonly known, in the convergence condition of equation Eq(2.5), achieving values  $\alpha_{ij} = 1$  and  $\beta_{ij} = 0$  indicates convergence. In reality, it will be very easy to determine

using error parameters such as the following values [12]:

$$\begin{aligned}\theta(k) &\approx \frac{C_i(k) - \text{avg}C_i(0)}{\text{avg}C_i(0)} \\ &\approx \frac{C_i(k) - \frac{1}{n} \sum_{i=1}^n C_i(0)}{\frac{1}{n} \sum_{i=1}^n C_i(0)}\end{aligned}\quad (2.25)$$

The value will approach convergence with an error tolerance rate of  $|\theta| = 0.001$ . Hence, we will observe the convergence rate when all local error values exceed their error tolerance limits. The convergence rate will be measured based on iteration metrics due to the constraints of the problem in Chapter 1.

The performance of this error needs to be measured globally to determine the extent of the error function over a certain observation period, thus allowing comparison with other experimental performances. Let's call it GSEr or global synchronization rate with an absolute value as follows [36]:

$$GSEr = \sum |\theta(k)| \quad (2.26)$$

Where:

$\theta$  : local synchronization error rate

Through the metrics of Synchronization Error and Convergence Speed, we can generate calculations for the robustness performance of convergence in a consensus-based time synchronization

#### 2.2.4.2 Topology Attack Modeling

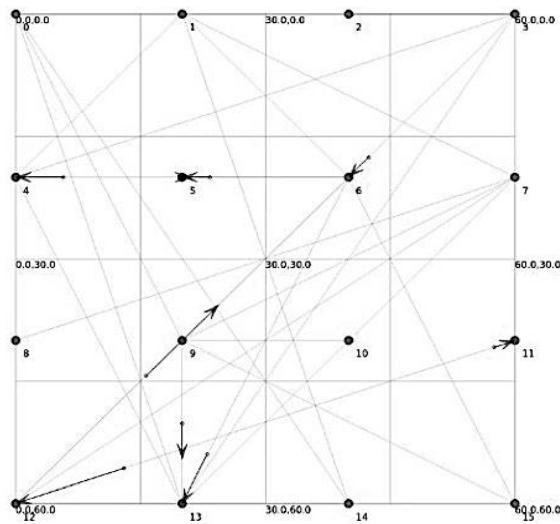


Figure 2.15: Network Model of WSN Nodes Exchanging Messages

Topology attack is a condition where a node node in a network represented by a graph  $G = (V, E)$  consisting of Vertices ( $V$ ) and Edges ( $E$ ) experiences undesired disruptions in the form of sudden and unmeasured changes in topology. Several types of topology attacks such as Denial of Service and Node Destruction can be modeled as follows:

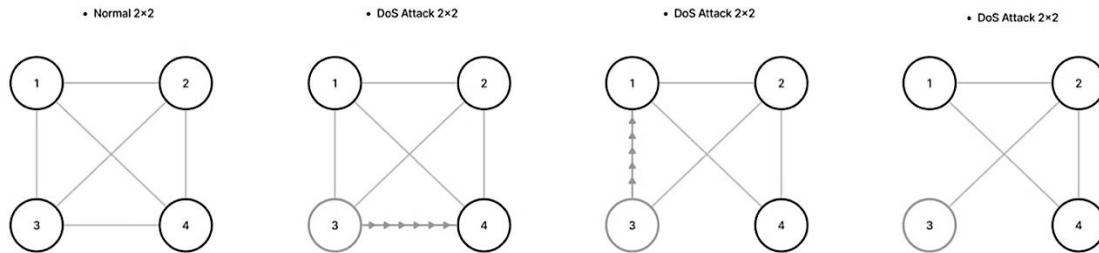


Figure 2.16: DoS Topology Attack Model in WSN Nodes

Adjacency Matrix Graph 2x2 No ATTACK:

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \quad (2.27)$$

Matrix Adjacency Graph 2x2 with DoS ATTACK

$$G' = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \quad (2.28)$$

Edge ( $E$ ) Attack or Denial of Service (DoS) attack is a condition where a node node floods packets to its directly neighboring node, causing communication disruption between these nodes. In other words, the neighboring node and the attacking node itself do not exchange messages. DoS attacks can be conducted using a proxy or another node in front of the attacker to flood packets, or it can be done directly. In the modeling for this research, a DoS attack condition is as follows:

1. The attacking node will launch an attack on its neighboring edges or the adjacency matrix, causing previously connected edges (with value 1) to become disconnected (with value 0).
2. The attacking node will leave at least one edge connected to differentiate it from Node Destruction attacks. If all adjacency matrix values become 0, it indicates that the node has been destroyed and is no longer connected to the network.
3. The attacking node will synchronize its attack and maintain it throughout the observation period.

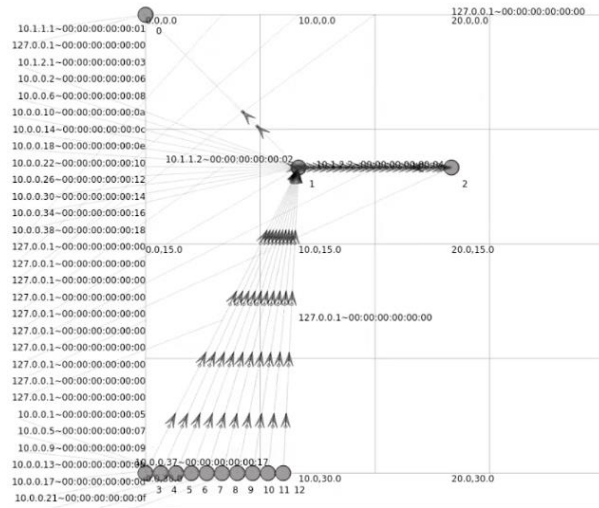


Figure 2.17: Network Model of WSN Node Attacked through Denial of service

Vertices ( $V$ ) Attack or Node Destruction Attack is a condition where a node node is no longer connected to the network. In this attack modeling, the node node is successfully dysfunctional or physically separated from the network, thus losing connectivity. Here is a modeling condition for Node Destruction Attack:

1. The victim node can be compromised and experience dysfunction, causing all its adjacency matrix values to become 0.
2. The victim node will no longer be connected within the observation period.

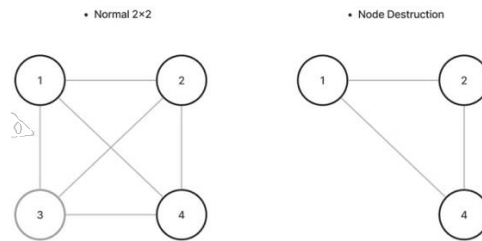


Figure 2.18: Node Destruction Topology Attack Model in WSN Nodes

Adjacency Matrix Graph 2x2 No ATTACK:

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \tag{2.29}$$

Matrix Adjacency Graph 2x2 with Node Destruction ATTACK

---

$$G' = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \quad (2.30)$$

The next condition is that both attack models will be tested in the 11th iteration after all network nodes have undergone consensus to achieve convergence from iteration 1 to 10. This is based on the premise that in the ATS algorithm, convergence typically occurs around the 20th iteration. Therefore, the 11th iteration is considered halfway towards convergence. If attacks are conducted between these conditions, it will impact the robustness performance of convergence.

## CHAPTER 3

### RESEARCH METHODOLOGY

This chapter discusses the proposed method and current research methodology to analyze the impact of topology attacks on the robustness of time synchronization in Wireless Sensor Networks (WSN) using Laplacian eigenvalue weighting. This chapter consists of research design, population sampling, instrumentation and data collection, and tools for data analysis.

#### 3.1 Research Design

Designing a research study to test the resilience of the proposed method there is time synchronization with consensus based on Laplacian against topology attacks in sensor networks using a simulation approach. Comparing to the existing method, the proposed method as seen on the picture below will leverage the spectrum of Eigenvalue Laplacian Matrix as its weighting factor under topological attacks.

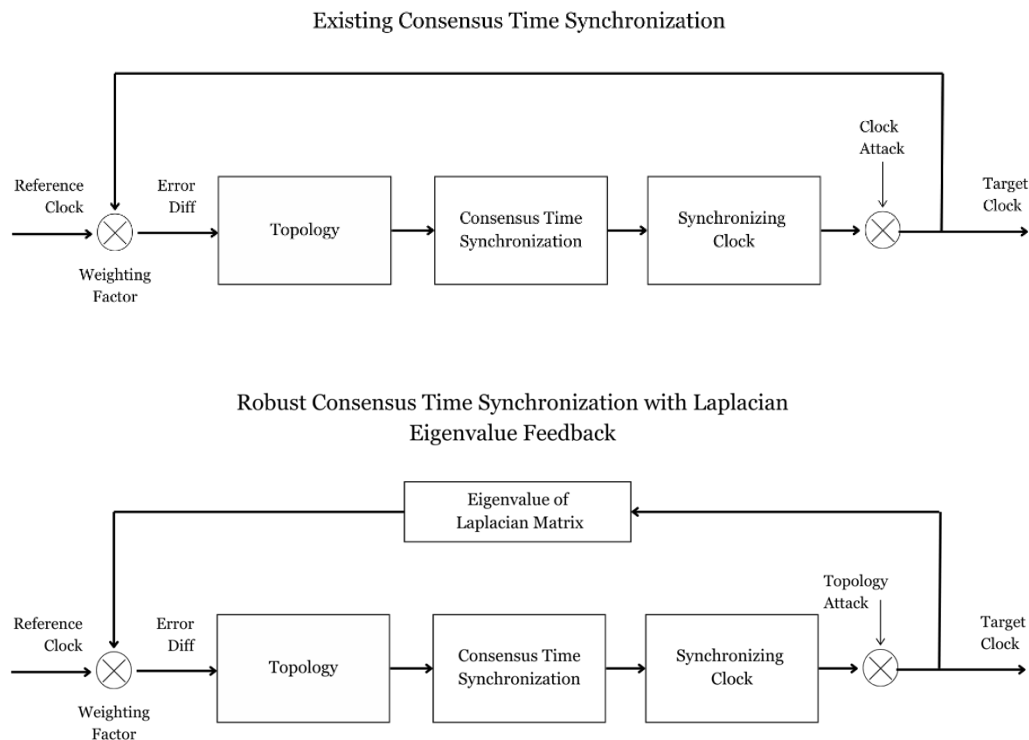


Figure 3.1: Existing and The Proposed Method using Laplacian Eigenvalue Feedback

The simulation approach involves modeling the testing scenarios for consensus-based time synchronization resilience in real-world conditions involving several processes:

1. Preparation and Definitive System Requirements Stage.

2. Simulation and analysis process in topology attack situations.
3. Simulation and analysis process with Laplacian feedback.
4. Simulation and analysis process in situations of changing scalability of topology types and sizes.

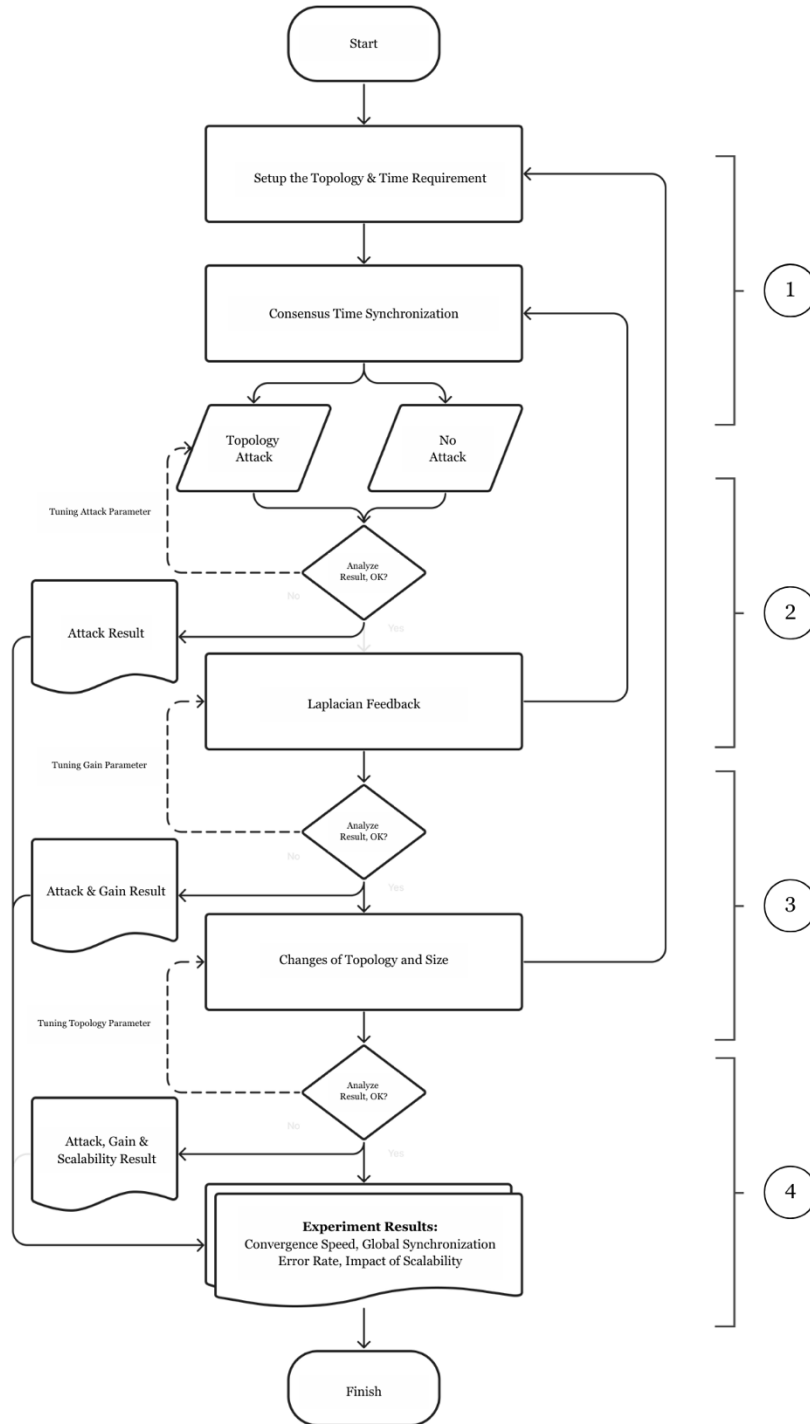


Figure 3.2: General Research Design Flowchart



By starting with a simple topology and then systematically scaling up the simulation, a deeper understanding will be gained on how network size, topology, and types of attacks influence the robustness performance of consensus-based Laplacian time synchronization. By analyzing experiment results such as convergence speed and GSEr values, the final outcome will reveal under what conditions and how the method can perform better compared to other conditions.

### 3.1.1 The Preparation Stage and Definitive System Requirements

In the initial stage, envision a network of interconnected nodes in a topology, each having its own unsynchronized values. One of the primary challenges in distributed systems is to ensure that all devices agree on a common value. This is where the consensus algorithm plays a role, where each parameter such as the type and size of the topology greatly affects its adjacency matrix. The definitive system built in the preparation stage of simulation will start from a simple system with the following requirements [4]:

1. Number of Nodes: 4 Nodes
2. Node Topology: 2x2 Fully Connected/Mesh
3. Initial Time Information:
  - a. Initial Offset Value for each Node: 2, 3, 8, 1
  - b. Initial Skew Value for each Node: 0.8, 0.9, 1.1, 1.3

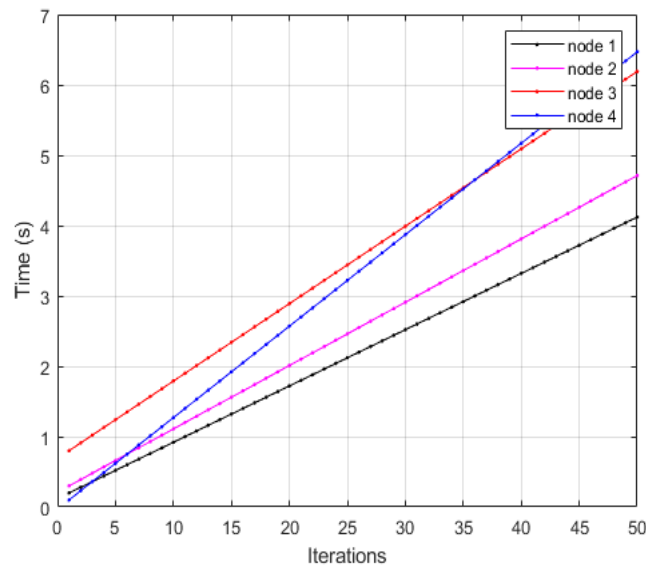


Figure 3.3: Plot of Initial Offset and Skew Clock Value at Initial Stage

Additionally, based on latest research [4] implementation that the tuning parameter set to be as  $\rho = 0.6$  will be mentioned as no gain condition in this research because the tuning parameter cannot be 0 or 1 as mentioned in section 2.2.2.3.

### 3.1.2 and Analysis Process in Topological Attack Conditions

Second stage, after carrying out the preparatory process and definitive requirements for the system to be tested, the consensus simulation testing process can be carried out. In the consensus simulation, the Averaging Time Synchronization or ATS algorithm is used, where naturally the initial value in the system will converge to the average value. This process will take place in two conditions, namely with and without topological attacks.

The attack modeling criteria itself takes place in detail as follows:

1. Number of Attacking Nodes: 1 Node
2. Attack Time: 11th Iteration
3. Attack Type: DoS & Node Destruction Attack

In accordance with the attack modeling, this is based on conditions where in the ATS algorithm convergent conditions will occur around the 20th iteration, therefore the 11th iteration is considered midway to convergent conditions so that if an attack is carried out between these conditions it will have implications for the robustness performance of the convergence.

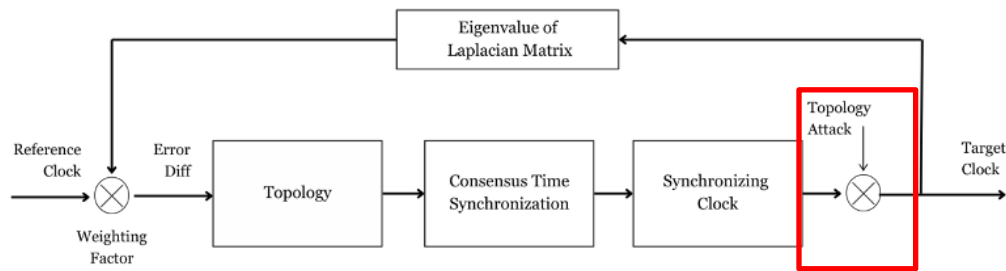


Figure 3.4: Second Stage Focusing on Attack Simulation

In the end of this stage, the simulation and analysis of topological attack situations have 3 different results, labeled as NO Attack, DoS Attack and Destruction Attack conditions as material for evaluating robustness parameters, there are convergence speed and global synchronization error rate.

### 3.1.3 Simulation and Analysis Process with Laplacian Feedback

Third stage, results of early testing has been recorded such as convergence speed and global synchronization error rate in the label as NO Attack, DoS Attack and Destruction Attack, extension of simulation will be carried out. At this stage, other parameters will be tuned to have gain feedback. As proposed, spectrum of eigenvalue Laplacian matrix were used.

As mentioned in the section 2.2.2.3 that Eq(2.18) composed from eigenvalue of Laplacian Matrix and will serve as an alternative topology-based weighting approach in consensus-based time synchronization, specifically in tuning its weighting parameters.

$$\rho = \frac{2}{\lambda_1(L) + \lambda_{N-1}(L)} \quad (2.18)$$

Where:

- $\rho$  : weighting parameter
- $\lambda_1$  : second smallest eigenvalue
- $\lambda_{N-1}$  : largest eigenvalue

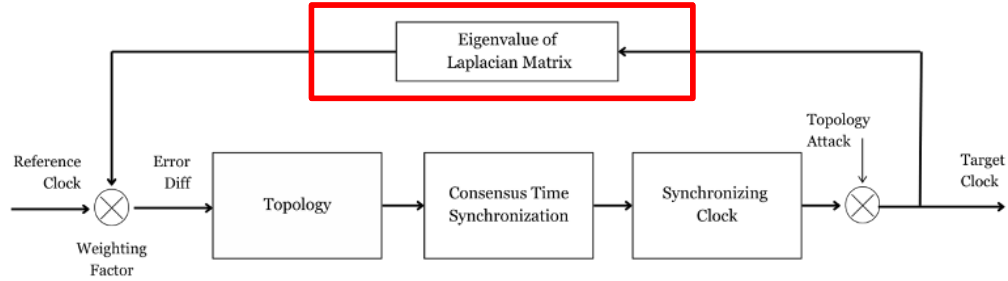


Figure 3.5: Third Stage Focusing on Laplacian Feedback as Gain Factor

The calculation of time virtual then can be expressed using the final process before combining all values into virtual time, denoted as  $\hat{t}_i = \hat{\alpha}_i * t + \hat{o}_i$ ,

Where:

- $\hat{t}_i$  : virtual time
- $\hat{\alpha}_i$  : virtual skew
- $\hat{o}_i$  : virtual offset

Relative Skew Estimation:

$$\eta_{ij}^+(t_k) = \rho_\eta^K \eta(0) + \sum_{i=1}^{k-1} (1 - \rho_\eta) a_{ij} = \rho_\eta^K \eta(0) + a_{ij}(1 - \rho_\eta^K)$$

Virtual Skew Calculation:

$$\hat{\alpha}_i^+ = \rho_v \hat{\alpha}_i + (1 - \rho_v) \eta_{ij} \hat{\alpha}_j$$

Virtual Offset Calculation:

$$\hat{o}_i^+ = \hat{o}_i + (1 - \rho_o) + (\hat{t}_j - \hat{t}_i) = \hat{o}_i + (1 - \rho_o) + (\hat{\alpha}_j \tau_j + \hat{o}_j - \hat{\alpha}_i \tau_i + \hat{o}_i)$$

All tuning parameters will follow Eq(2.18), where  $\rho_n = \rho_v = \rho_o = \rho \in L$

In the end of this stage, the simulation and analysis process with Laplacian feedback have 2 different results, labeled as No Gain and Laplacian Gain conditions as material

for evaluating robustness parameters. There are convergence speed and global synchronization error rate. These 2 results then clustered as one experiment. Furthermore, recording all of each raw data, captured simulation results, and experiment notes will be added in the experiment dataset.

### 3.1.4 Simulation and Analysis Process in Situations of Changing Topology Types and Sizes

In the fourth stage or last stage, each of experiment has been conducted and then extension of simulation will be carried out in terms of changing topology conditions. By starting simple and then systematically scaling the simulations, gaining a deeper understanding of how network size, topology, and attacks affect the robustness and scalability of Laplacian consensus algorithms. This allows for the development of more robust, scalable, and attack-resilient algorithms that can maintain consensus even in large-scale distributed systems under topological attacks influence.

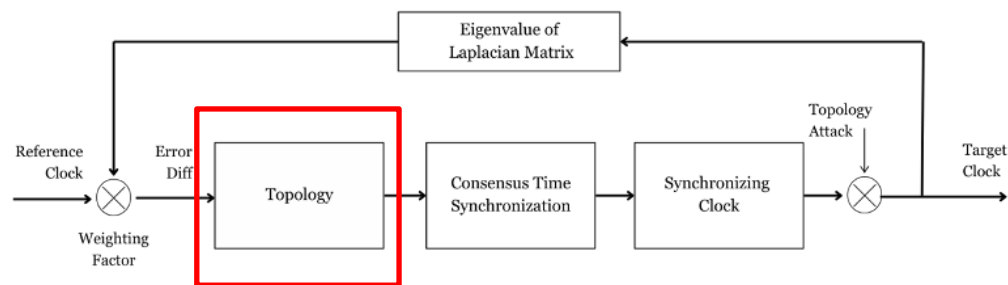


Figure 3.6: Fourth Stage Focusing on Impact on Scalability of Topology

The new definitive system built in the scalability stage of simulation will change from a simple system to larger size with 10 Nodes [4] with the following requirements:

1. Number of Nodes: 10 Nodes
2. Node Topology: Fully Connected, Ring, Star and Fully Mesh Topology
3. Initial Time Information:
  - c. Initial Offset Value for each Node: 2, 3, 8, 1, 12, 1, 3, 3, 9, 10
  - d. Initial Skew Value for each Node: 0.2, 0.6, 1.1, 0.8, 1.4, 1.3, 0.7 0.9 1.0 0.8



Fully Connected 4 Nodes



Fully Connected 10 Nodes

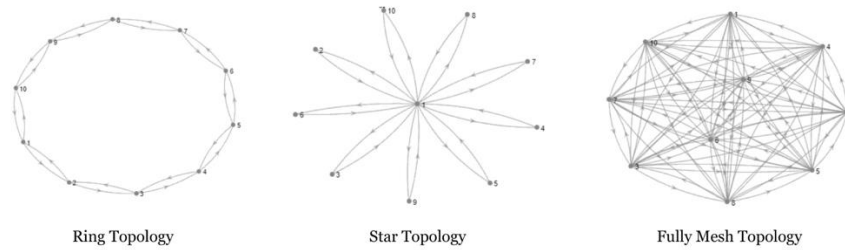


Figure 3.7: Fourth Stage Focusing on Impact of Scalability of Topology [4]; [21]

In conclusion, there is no single simulation that always perfect. There are need of loopback in each stage cycle simulations that incorporate diverse topology attacks, consider scalability, and begin with a simple case are crucial for effectively evaluating Laplacian feedback consensus time synchronization algorithms. By analyzing convergence speed, GSEr, and scalability under attack, this research can measure the impact of the gain feedback leveraging Laplacian Eigenvalue spectrum that are resilient to such DoS/Node Destruction attack and function effectively in large-scale distributed systems.

### 3.2 Population sampling

The population sampling for this study involved selecting a diverse range of network topologies to represent different scenarios commonly encountered in sensor networks. Specifically, the selected network topologies included Fully Connected 4 Nodes, Fully Connected 10 Nodes, Fully Mesh 10 Nodes, Ring 10 Nodes, and Star 10 Nodes. These topologies were chosen to provide a comprehensive understanding of the performance of the Laplacian-based consensus method against various topology attacks.

### 3.3 Data Collection

The instrumentation and data collection process involved setting up the experimental environment to simulate topology attacks on time synchronization in sensor networks. This included configuring the network topologies, implementing the Laplacian-based consensus method, and generating attack scenarios such as no attack, Denial of Service (DoS), and Node Destruction. Data collection was conducted systematically during the experiments to record relevant performance metrics, including global synchronization error rates and fault tolerance, for both the Laplacian and no-gain approaches under different attack conditions.

### 3.4 Tools for Data Analysis

For data analysis, various tools and techniques were employed to interpret the collected data and derive meaningful insights. Statistical analysis methods, such as descriptive statistics and hypothesis testing, were utilized to analyze the performance metrics of the Laplacian-based consensus method under different attack scenarios. Additionally, visualization techniques,

such as charts and graphs, were employed to present the findings in a clear and concise manner. Software tools used for data analysis is MATLAB R2023a, were employed to process and analyze the experimental data effectively. Overall, these tools facilitated a comprehensive analysis of the experimental results and enabled the identification of trends and patterns in the performance of the Laplacian-based consensus method against topology attacks in sensor networks.

## CHAPTER 4

# RESULT AND ANALYSIS

This chapter presents the findings and analysis of topology attacks on the robustness of time synchronization in Wireless Sensor Networks (WSN) employing Laplacian-eigen value weighting. It is structured into three main sections: Presentation of Data, Data Analysis, and Discussion.

### 4.1 Attack Scenario

In this section, the raw data obtained from the experiments conducted to assess the impact of topology attacks on time synchronization in WSNs is presented. This includes data related to graph topology, topology attacks, number of no gain fault tolerance (convergence iteration), No Gain Accuracy (global synchronization error rate), Laplacian gain fault tolerance (convergence iteration), and Laplacian Gain accuracy (global synchronization error rate). The presentation of data provides a comprehensive overview of the experimental setup and enables a thorough examination of the effects of topology attacks on time synchronization robustness.

#### 4.1.1 Topological Attack

This experiment's objective was to evaluate the attack modeling, this is based on conditions where in the ATS algorithm convergent conditions will occur around the 20th iteration as seen on the Figure 4.2 & 4.3. Therefore the 11th iteration is considered midway to convergent conditions so that if an attack is carried out between these conditions it will have implications for the robustness performance of the convergence. The robustness performance under topological attack can be shown in the Table 4.1.

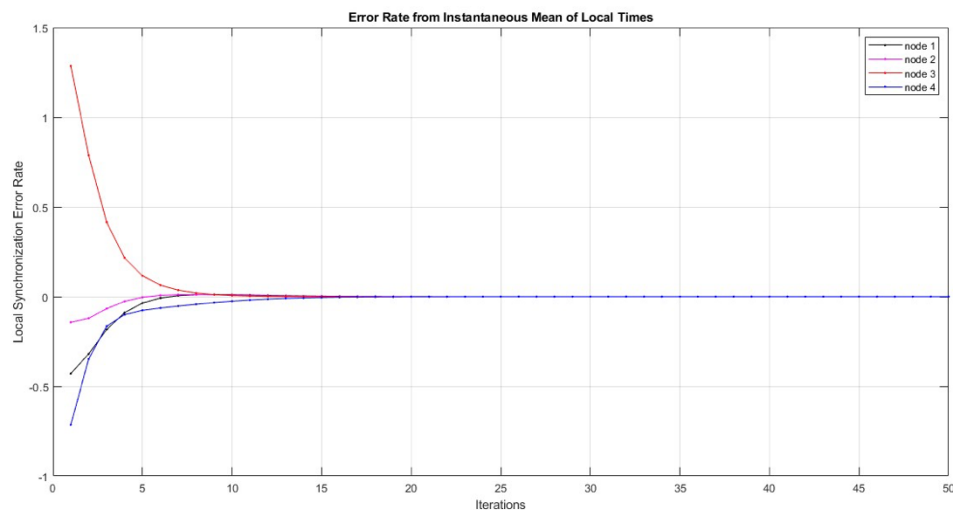


Figure 4.1: Simulation Result from Fully Connected 4 Nodes – No Attack

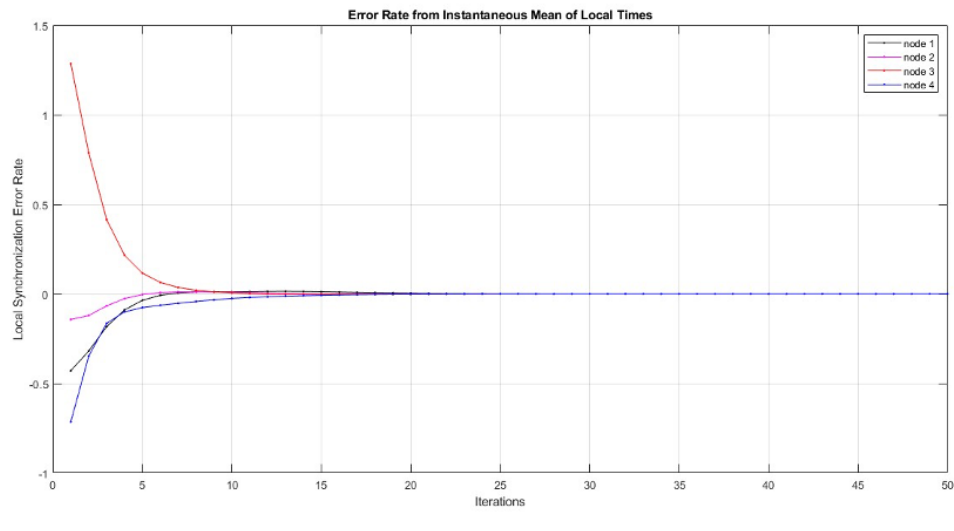


Figure 4.2: Simulation Result from Fully Connected 4 Nodes – DoS Attack

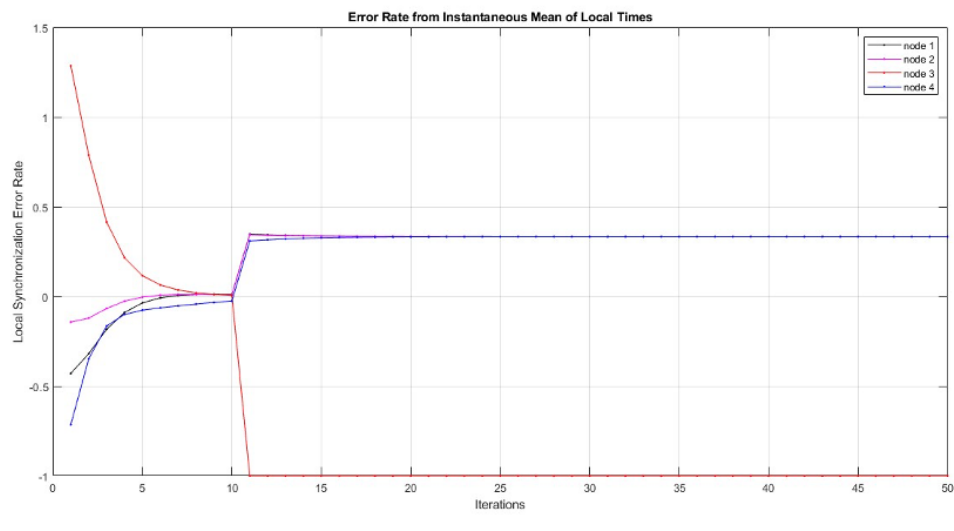


Figure 4.3: Simulation Result from Fully Connected 4 Nodes – Node Destruction Attack

Table 4.1: Robustness Performance of Consensus Result in Topological Attack

Simulation No.	Graph Topology	Topology Attacks	No gain fault Tolerance (Convergence Iteration)	No Gain Accuracy (Global Synchronization Error Rate)
1	Fully Connected 4 Nodes	No Attack	20	6.2205
2	Fully Connected 4 Nodes	DoS Attack	20	6.3263
3	Fully Connected 4 Nodes	Node Destruction Attack	23	86.0898



As seen on the Table 4.1, the differences between 3 scenarios of topological attack under performance variable such as fault tolerance in convergence iteration and accuracy in global synchronization error rate (GSEr). Simulation no.1 and no.2 has similar results in 20 iterations but had slight differences in topological attack accuracy because of the GSEr value increased under the DoS Attack of 11<sup>th</sup> iteration. It seems no significant value between Figure 4.1 & 4.2 which are 6.2205 and 6.3263 because of the impact of destruction hold by the ATS consensus algorithm and resulted the same in the convergence iteration.

The other attack simulation was presented in simulation no.3 which Node Destruction occurred. As seen on the Table 4.1 convergence iteration increased from 20 in the simulation no.1 and no.2 into value of 23 in the simulation no.3. It because the disruption really matters in the Node Destruction Attack. The GSEr in simulation no.3 has a lot of increased in the number of 86.0898 because of node 4 in the topology lead into the -1 value along the 11<sup>th</sup> until 50<sup>th</sup> iteration. Furthermore, addition of the increasing error of its attack itself to other 3 nodes in the topology. In conclusion, this is the first time in the experiments that GSEr value will significantly different between two other conditions except Node Destruction Attack because of the topology has lost node 4.

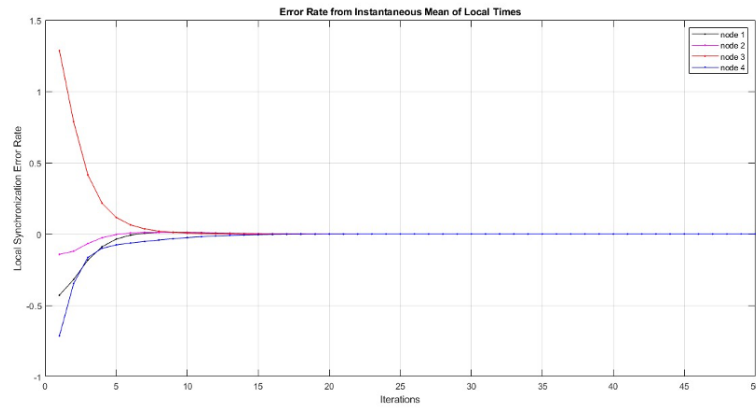
#### **4.1.2 Effect of Laplacian Second Smallest Eigenvalue Feedback**

As discussed in section 3.1.3, the experiment was carried out focusing on Laplacian feedback as gain factor. This is the extension of the topological attack data with the conditions with and without Laplacian Gain. The objective is to answer research question analyzing the impact of topology attacks on the robustness of time synchronization in Wireless Sensor Networks (WSN) using Laplacian-eigen value weighting. As seen on the 3 pictures below from Figure 4.1 to 4.3 that the results of the experiment labeled without (a) and with Laplacian gain (b) to clearly shows the differentiation between its two states on each topological attack conditions.

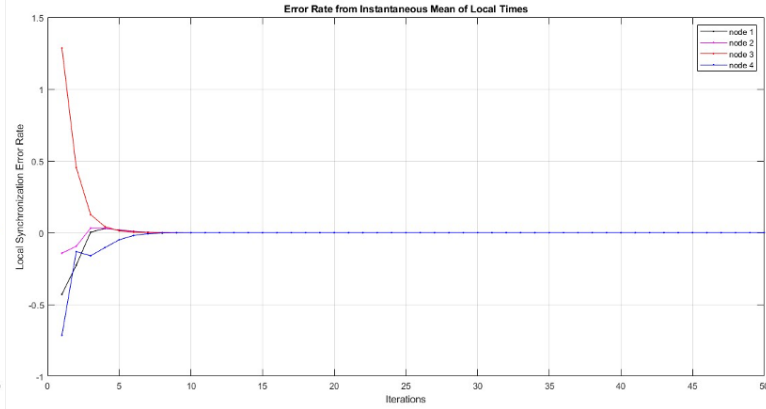
The eigenvalue feedback demonstrates significant improvements in the speed and accuracy of time synchronization in fully connected sensor networks. In conditions without the use of Laplacian gain (Figures 4.5a and 4.6a), the nodes in the network require approximately 20 iterations to achieve convergence. Conversely, with the application of Laplacian gain (Figures 4.5b and 4.6b), the nodes only need 9 iterations to reach convergence. In node destruction attack without Laplacian 23 iterations to achieve convergence (Figure 4.7a) and 9 iterations to reach convergence with Laplacian gain (Figure 4.7b). This significant reduction underscores the effectiveness of Laplacian gain in accelerating the convergence process. The improved speed of synchronization with Laplacian gain suggests that the network can achieve a unified time reference more quickly, which is crucial for maintaining the accuracy and reliability of sensor data across the network. Furthermore, the resilience of the network under node destruction attacks also benefits from the application of Laplacian gain. In the absence of Laplacian gain, as shown in Figure 4.7a, the network requires 23 iterations to achieve convergence following a node destruction attack. This higher number of iterations reflects the increased difficulty in maintaining synchronization when the network's structure is compromised. However, with the application of Laplacian gain, depicted in Figure 4.7b, the network's resilience improves significantly, with only 9 iterations needed to reach convergence even under attack conditions. These observations highlight the dual benefits of eigenvalue feedback and Laplacian Gain in enhancing both the speed and accuracy of time synchronization in fully connected sensor networks. By reducing the number of iterations required for convergence, Laplacian Gain not only accelerates the

synchronization process but also improves the network's ability to maintain accurate time synchronization even in the face of structural disruptions. This improved performance is essential for applications requiring precise timing and robust operation in dynamic or adversarial environments.

The primary objective of this study is to test the system's resilience against attacks, particularly Denial of Service (DoS) attacks. In the DoS attack scenario, the attack occurs at the 11th iteration. However, with the use of Laplacian gain, the system achieves convergence by the 9 iterations. This means that the attack at the 11 iterations does not affect the synchronization condition because the nodes in the network have already aligned before the attack occurs. This demonstrates that the use of eigenvalue feedback makes the system more resistant to DoS attacks. In the node destruction attack scenario, the analysis shows that although convergence is maintained, the overall error rate becomes higher due to the loss of a node. For instance, if node 4 is destroyed, the system can still achieve convergence, but the overall error rate increases because the accumulated error now accounts for the loss of the node. Nevertheless, the system's ability to still achieve convergence indicates its robustness in facing node loss. The use of Laplacian gain or eigenvalue feedback significantly improves the speed and accuracy of time synchronization in sensor networks. With faster convergence from 20 iterations to 9 iterations and accuracy improvement through the reduction of initial error rates, this method demonstrates substantial performance enhancements. The dynamic weighting provided by eigenvalue feedback helps in regulating the synchronization process more effectively and efficiently. The analysis of the system's resilience against DoS attacks shows that the use of eigenvalue feedback makes the system more robust. Although the attack occurs at the 11th iteration, the system achieves convergence by the 9th iteration, thus the attack does not affect the synchronization condition. This indicates that the method not only enhances performance but also increases the system's resilience against external disruptions.

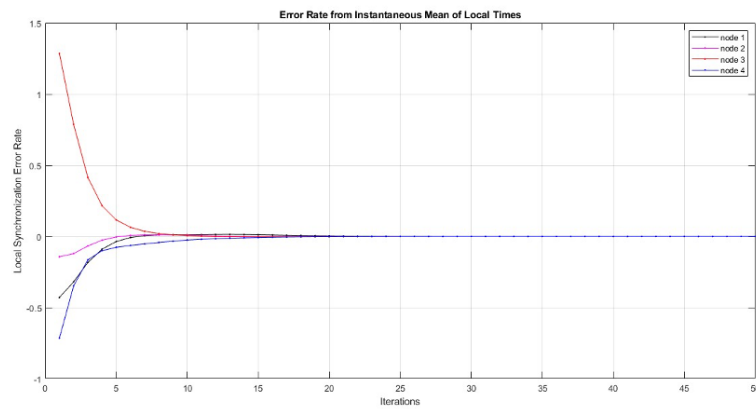


(a)

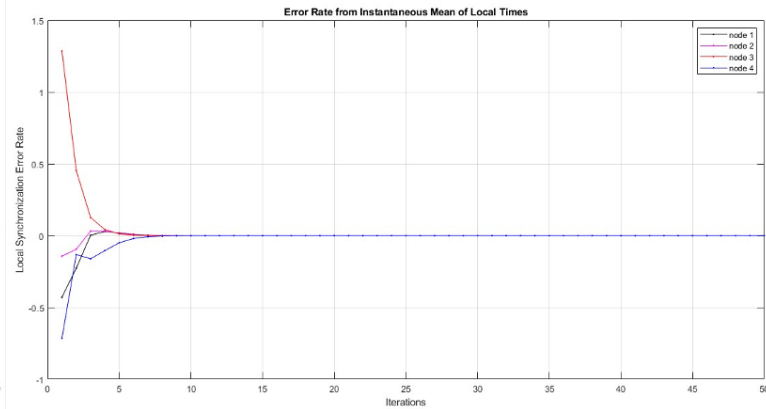


(b)

Figure 4.4: Comparison Result from Fully Connected 4 Nodes – No Attack without (a) & with Laplacian gain (b)



(a)



(b)

Figure 4.5: Comparison Result from Fully Connected 4 Nodes – DoS Attack without (a) & with Laplacian gain (b)

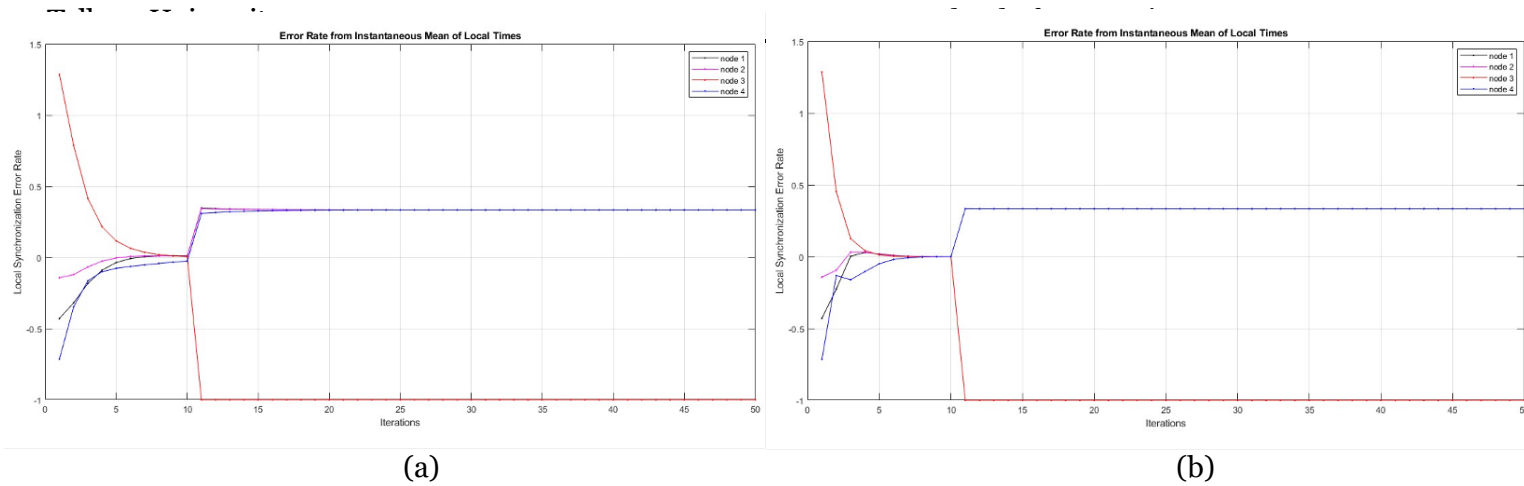


Figure 4.6: Comparison Result from Fully Connected 4 Nodes – Node Destruction Attack without (a) & with Laplacian gain (b)

Table 4.2: Robustness Performance of Consensus Result in Topological Attack and Laplacian Feedback

Simulation No.	Graph Topology	Topology Attacks	No gain fault Tolerance (Convergence Iteration)	No Gain Accuracy (Global Synchronization Error Rate)	Laplacian Gain Fault Tolerance (Convergence Iteration)	Laplacian Accuracy (Global Synchronization Error Rate)
1	Fully Connected 4 Nodes	No Attack	20	6.2205	9	4.1654
2	Fully Connected 4 Nodes	DoS Attack	20	6.3263	9	4.1661
3	Fully Connected 4 Nodes	Node Destruction	23	86.0898	9	84.1652

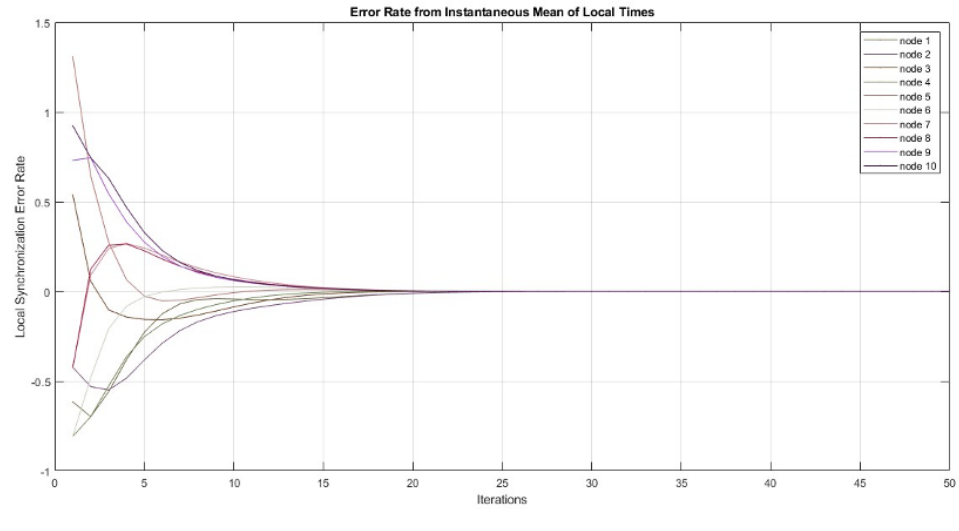
### 4.1.3 Scalability of Topology

In the first simulation scenario with a fully connected network of 10 nodes and no attack, the network without Laplacian Gain requires 25 iterations to achieve convergence and has a global synchronization error rate of 28.0688. However, when Laplacian Gain is applied, the network only needs 13 iterations to converge, and the synchronization error rate is reduced to 20.4253. This demonstrates a significant improvement in both the speed and accuracy of the network's synchronization process when Laplacian Gain is utilized. The second scenario involves a fully connected network of 10 nodes under a Denial of Service (DoS) attack. Without Laplacian Gain, the network requires 30 iterations to reach convergence, with a synchronization error rate of 28.5952. With the application of Laplacian gain, the convergence iterations drop to 12, and the synchronization error rate decreases to 20.4270. These results further emphasize the effectiveness of Laplacian gain in enhancing the network's resilience and maintaining accurate synchronization even under adverse conditions like DoS attacks.

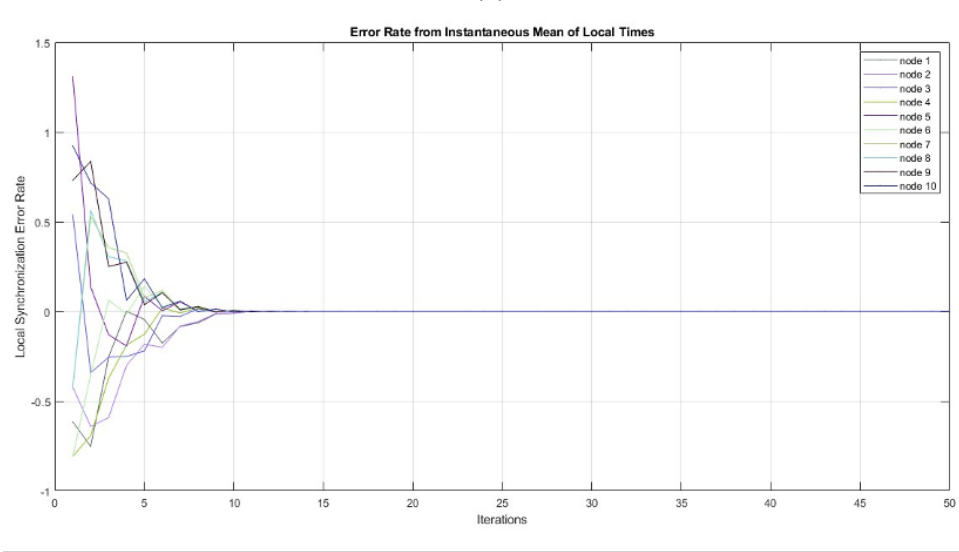
In the third scenario, a fully connected network of 10 nodes faces a node destruction attack. The network without Laplacian Gain needs 31 iterations to converge, with a significantly higher synchronization error rate of 105.9115. When Laplacian Gain is applied, the number of convergence iterations reduces to 17, and the synchronization error rate drops to 100.3794. Although the error rate remains relatively high, the application of Laplacian gain still shows a noticeable improvement in both fault tolerance and accuracy compared to the scenario without gain. Overall, these simulations underscore the critical role of Laplacian gain in improving the performance of consensus algorithms in sensor networks. By reducing the number of iterations needed for convergence and lowering the global synchronization error rates, Laplacian Gain enhances the network's efficiency and robustness, particularly under attack conditions.

The increase from 4 nodes to 10 nodes significantly impacts the network's response to attacks. When the number of nodes increases from 4 to 10, the network's complexity also increases, affecting the convergence speed. This happens because more nodes are involved in the synchronization process, increasing the number of iterations needed to achieve convergence. For instance, in a no-attack condition with a 4-node network, convergence is achieved faster than with a 10-node network. This indicates that adding more nodes can slow down the convergence process due to the increased interaction and coordination required among the nodes.

The strong connection graph theorem remains a crucial factor in determining how quickly convergence can be achieved, especially under attack conditions. A strong connection graph ensures that every node in the network can communicate directly or indirectly with every other node, which is essential for rapid consensus. In no-attack conditions, a network with strong connections can achieve convergence faster because of more efficient and direct communication paths between nodes. Under attack conditions, the strong connection graph theorem still provides significant advantages. Attacks such as DoS or node destruction can disrupt communication between nodes, but if the network has a strong connection, the impact of such attacks can be minimized. A network with a strong connection still has alternative paths that can be used to achieve convergence even if some nodes or communication paths are disrupted due to attacks. This is evident in simulation results where networks with strong connections can achieve faster convergence even under attack, especially when using Laplacian Gain.

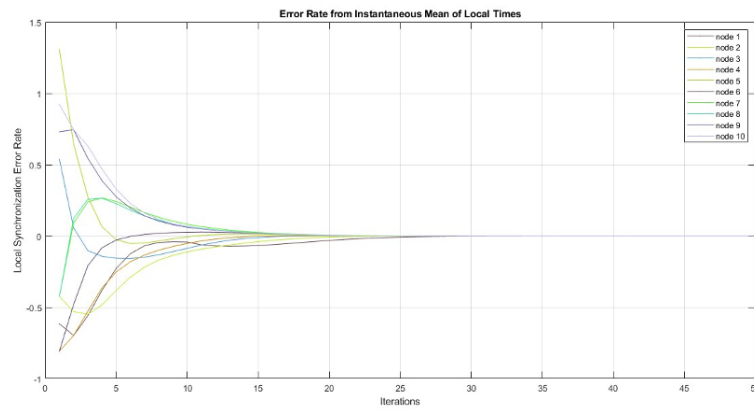


(a)

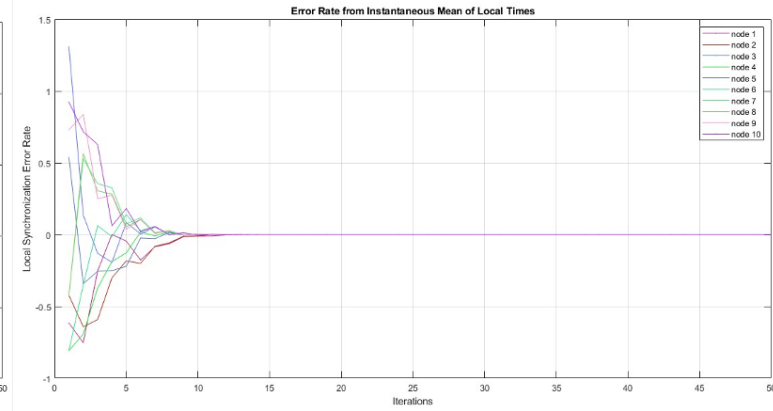


(b)

Figure 4.7: Comparison Result from Fully Connected 10 Nodes – No Attack without (a) & with Laplacian gain (b)

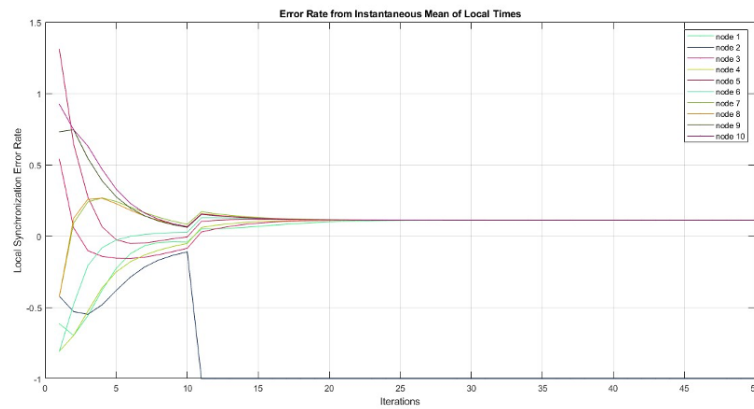


(a)

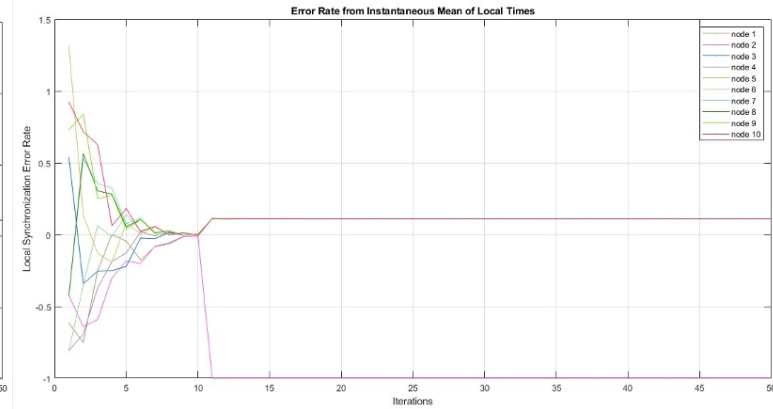


(b)

Figure 4.8: Comparison Result from Fully Connected 10 Nodes – DoS Attack without (a) & with Laplacian gain (b)



(a)



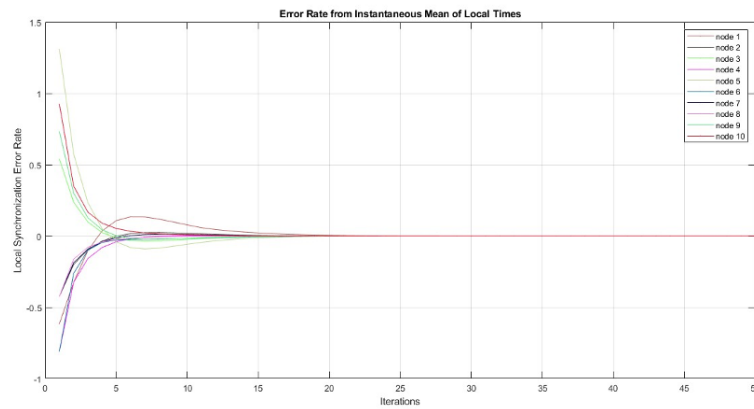
(b)

Figure 4.9: Comparison Result from Fully Connected 10 Nodes – Node Destruction Attack without (a) & with Laplacian gain (b)

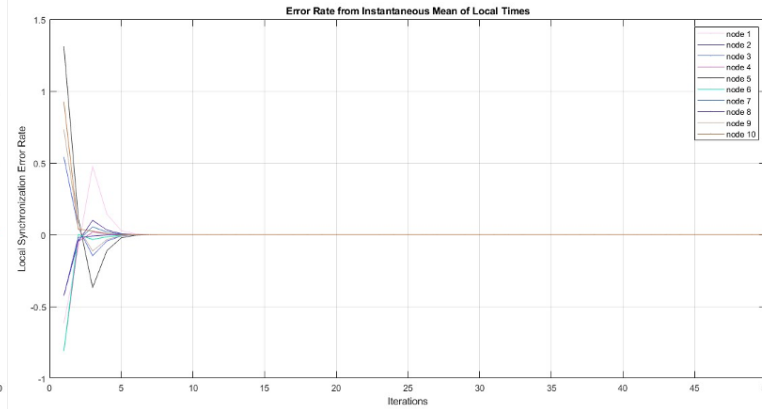
Table 4.3: Robustness Performance of Consensus Result in Topological Attack, Laplacian Feedback &amp; Scalability of Topology

Simulation No.	Graph Topology	Topology Attacks	No gain fault Tollerance (Convergence Iteration)	No Gain Accuracy (Global Synchronization Error Rate)	Laplacian Gain Fault Tollerance (Convergence Iteration)	Laplacian Accuracy (Global Synchronization Error Rate)
1	Fully Connected 4 Nodes	No Attack	20	6.2205	9	4.1654
2	Fully Connected 4 Nodes	DoS Attack	20	6.3263	9	4.1661
3	Fully Connected 4 Nodes	Node Destruction	23	86.0898	9	84.1652
<b>4</b>	<b>Fully Connected 10 Nodes</b>	<b>No Attack</b>	<b>25</b>	<b>28.0688</b>	<b>13</b>	<b>20.4253</b>
<b>5</b>	<b>Fully Connected 10 Nodes</b>	<b>DoS Attack</b>	<b>30</b>	<b>28.5952</b>	<b>12</b>	<b>20.4270</b>
<b>6</b>	<b>Fully Connected 10 Nodes</b>	<b>Node Destruction</b>	<b>31</b>	<b>105.9115</b>	<b>17</b>	<b>100.3794</b>
7	Fully Mesh 10 Nodes	No Attack	21	14.2743	7	9.3577
8	Fully Mesh 10 Nodes	DoS Attack	23	14.3183	7	9.3577
9	Fully Mesh 10 Nodes	Node Destruction	29	93.6113	7	89.3577
<b>10</b>	<b>Ring 10 Nodes</b>	<b>No Attack</b>	<b>37</b>	<b>33.5512</b>	<b>27</b>	<b>29.8025</b>
<b>11</b>	<b>Ring 10 Nodes</b>	<b>DoS Attack</b>	<b>41</b>	<b>36.0375</b>	<b>35</b>	<b>33.2390</b>
<b>12</b>	<b>Ring 10 Nodes</b>	<b>Node Destruction</b>	<b>46</b>	<b>106.5954</b>	<b>37</b>	<b>106.7254</b>
13	Star 10 Nodes	No Attack	23	17.1558	24	27.6860
14	Star 10 Nodes	DoS Attack	30	96.0429	28	106.2896
15	Star 10 Nodes	Node Destruction	30	96.0429	28	106.2896



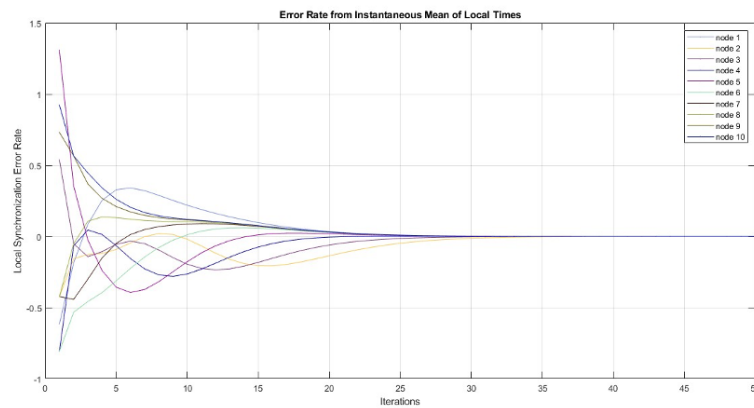


(a)

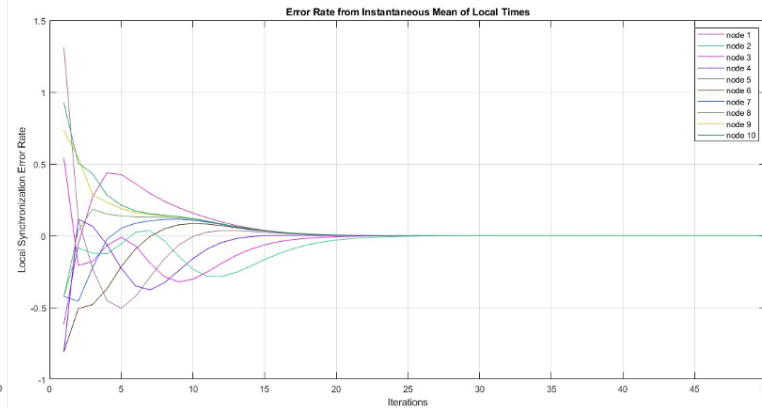


(b)

Figure 4.10: Comparison Result from Fully Connected 10 Nodes – No Attack without (a) & with Laplacian gain (b)



(a)

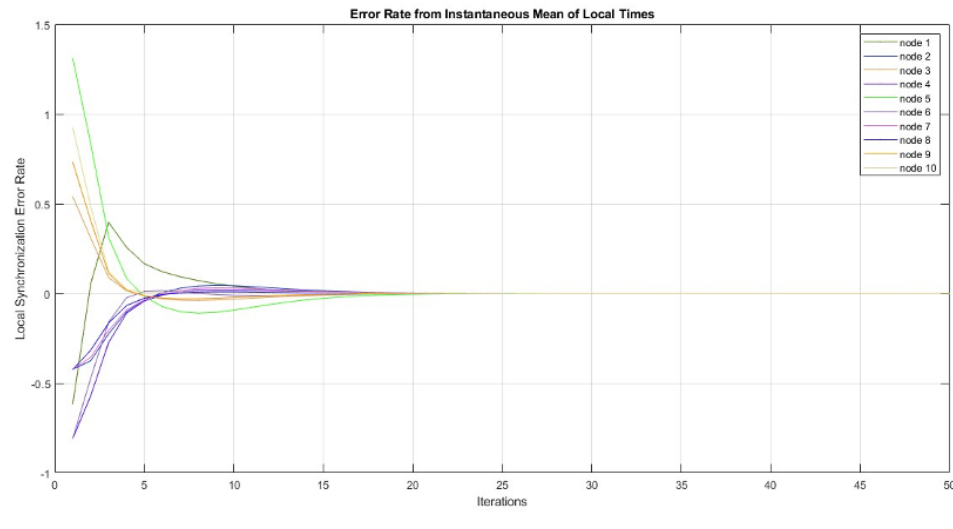


(b)

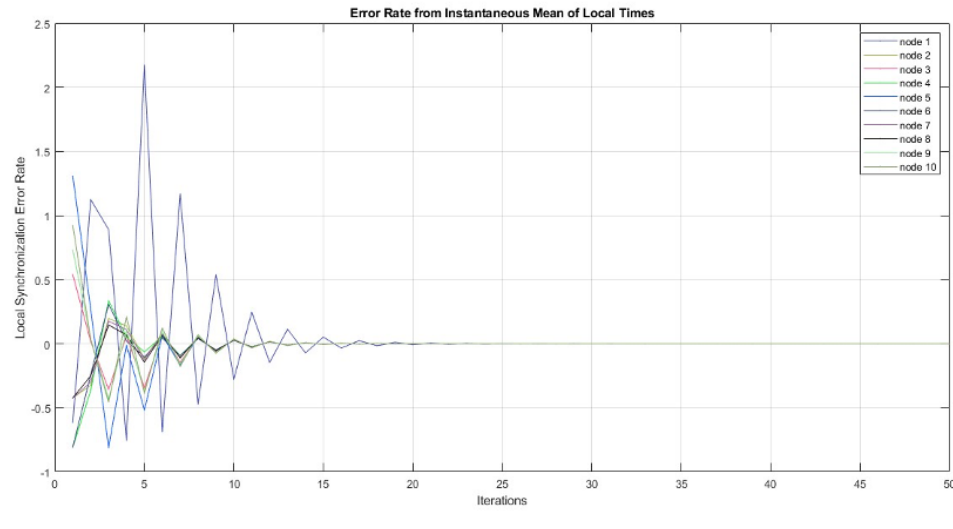
Figure 4.11: Comparison Result from Ring 10 Nodes – No Attack without (a) & with Laplacian gain (b)

In the simulations conducted, the differences in results between various topologies are quite striking, especially regarding accuracy. In the Fully Mesh topology with 10 nodes, both under conditions without attacks, DoS attacks, and node destruction, accuracy and fault tolerance remain relatively stable. For instance, without attacks, the convergence iteration fault tolerance is 14.2743 and the global synchronization error accuracy is 9.3577. After a DoS attack, fault tolerance slightly increased to 14.3183, but accuracy remained at 9.3577. However, after node destruction, the convergence iteration fault tolerance sharply increased to 93.6113, and global accuracy drastically decreased to 89.3577. Conversely, in the Ring 10-node topology, the results show significant variation. Without attacks, the convergence iteration fault tolerance is 33.5512 and global accuracy is 29.8025. With a DoS attack, fault tolerance increased to 36.0375, and global accuracy slightly decreased to 30.0827. When node destruction occurred, fault tolerance reached 106.5954 and global accuracy dropped drastically to 106.1791. In the Star 10-node topology, the decrease in global accuracy and fault tolerance is even more pronounced. Without attacks, the convergence iteration fault tolerance is 17.1558 and global accuracy is 27.6860. However, both DoS attacks and node destruction resulted in fault tolerance and global accuracy remaining at very high values, namely 96.0429 and 106.2896, respectively, showing a significant decline compared to the Fully Mesh topology.

In terms of mitigation with Laplacian feedback, the Fully Connected topology with 10 nodes shows the best results. In this topology, despite changes in conditions such as DoS attacks or node destruction, fault tolerance and global accuracy remain relatively stable. For example, in the simulation without attacks, the convergence iteration fault tolerance is 14.2743 with a global synchronization error accuracy of 9.3577. When experiencing a DoS attack, fault tolerance slightly increased to 14.3183, but accuracy remained the same at 9.3577. However, in the case of node destruction, fault tolerance sharply increased to 93.6113, and global accuracy drastically decreased to 89.3577. In contrast, in the Star topology with 10 nodes, mitigation with Laplacian feedback shows the least significant results. Fault tolerance and global accuracy in the Star topology remain high, namely 96.0429 and 106.2896 in cases of DoS attacks and node destruction. This is due to the low graph connectivity in the Star topology, which reduces the effectiveness of Laplacian feedback mitigation. The lower connectivity in the Star topology makes the system more vulnerable to performance degradation when facing disruptions or attacks, as reflected in the simulation results. In the Fully Connected topology, high graph connectivity allows Laplacian feedback mitigation to function more effectively, maintaining relatively stable accuracy. Conversely, in the Ring and Star topologies, lower graph connectivity results in a greater reduction in accuracy when experiencing disruptions or attacks. This is evident from graphs 4.11, 4.12, and 4.13, which show that Laplacian gain directly affects system performance, with topologies having better graph connectivity, such as Fully Connected, providing more effective mitigation results.



(a)



(b)

Figure 4.12: Comparison Result from Star 10 Nodes – No Attack without (a) & with Laplacian gain (b)

## 4.2 Analysis

### 4.2.1 Synchronization Convergence Speed in Iterations for Laplacian-Based Consensus Against Topology Attacks

The convergence speed of synchronization iterations for Laplacian-based consensus varies depending on the network topology and the types of attacks encountered. Generally, the Laplacian gain fault tolerance approach demonstrates the capability to achieve faster and more stable convergence in topologies such as Fully Connected and Fully Meshed networks, with fewer iterations compared to no gain fault Tolerance. However, in topologies like Star networks, this advantage is less pronounced, indicating that the effectiveness of the Laplacian method is heavily influenced by the network

topology structure in use (refer to Figures 4.13 – 4.17).

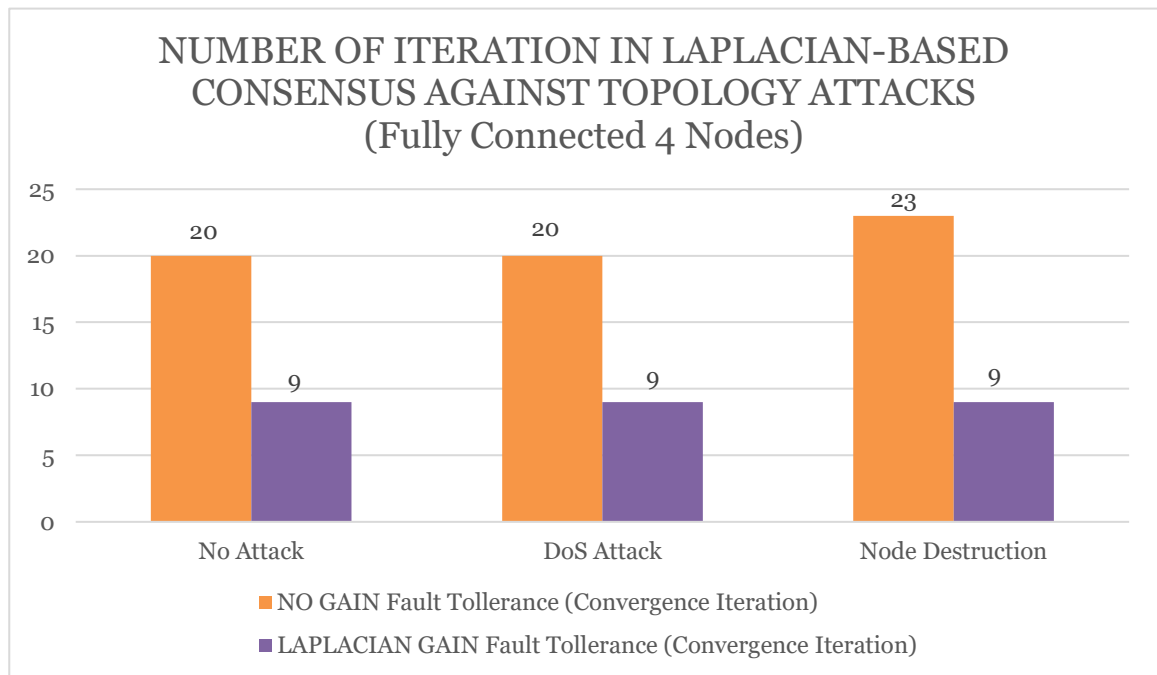


Figure 4.13: Synchronization Convergence Speed in Fully Connected 4 Nodes

Figure 4.13 the Laplacian gain fault tolerance approach exhibits superiority in fault tolerance and network performance consistency in sensor networks, particularly in the Fully Connected 4 Nodes configuration across various attack scenarios. Under No Attack conditions, Laplacian gain fault tolerance achieves convergence in just 9 iterations, compared to the 20 iterations required by no gain fault Tolerance. This demonstrates that the Laplacian gain approach can achieve stability faster in the network when no attacks are present. During a DoS Attack, both approaches maintain the same convergence iteration count, with no gain fault Tolerance requiring 20 iterations and Laplacian gain fault tolerance also converging in 9 iterations. This indicates that Laplacian gain remains consistent in dealing with attacks that restrict network resource access.

In the Node Destruction Attack scenario, where nodes in the network are destroyed, no gain fault Tolerance shows an increased convergence iteration count of 23, whereas Laplacian gain fault tolerance remains stable at 9 iterations. This underscores that the Laplacian gain approach can handle physical network damage more efficiently, providing quicker and more stable responses to disruptive conditions. Overall, these findings support that employing Laplacian gain fault tolerance can enhance fault tolerance and resilience of sensor networks against various attacks and disruptions.

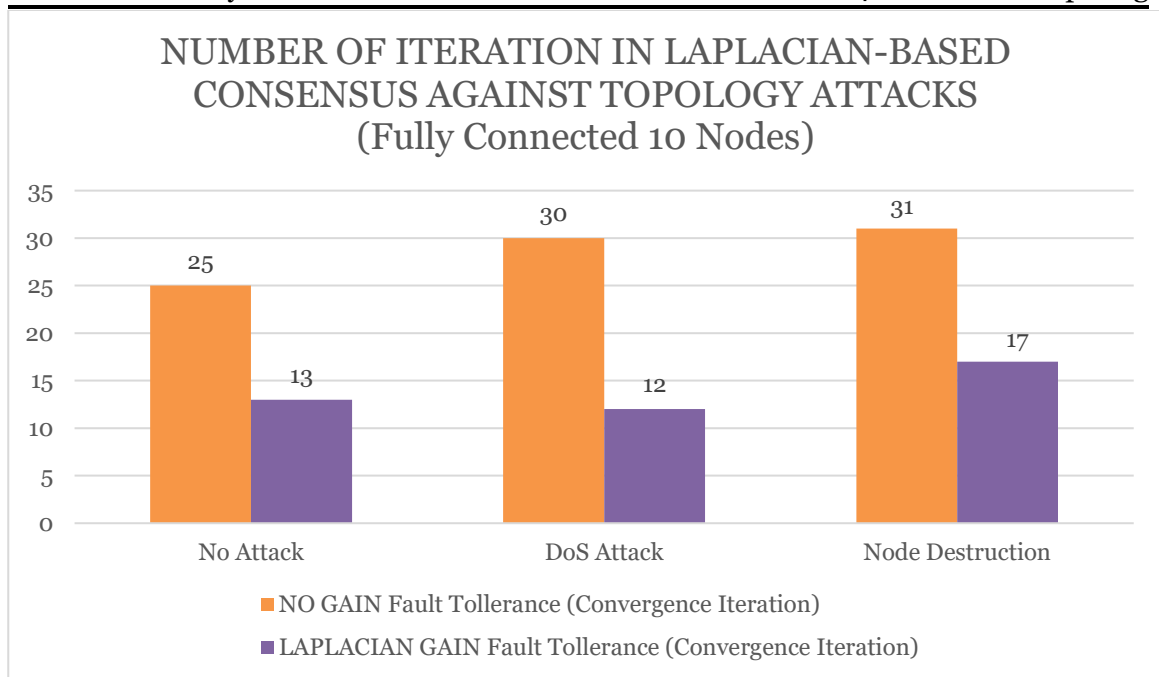


Figure 4.14: Synchronization Convergence Speed in Fully Connected 10 Nodes

Figure 4.14 depicts the comparison of fault tolerance through convergence iterations across various attack scenarios on a Fully Connected 10 Nodes network. In the scenario without attacks (No Attack), the Laplacian gain fault tolerance approach demonstrates the ability to achieve convergence in just 13 iterations, compared to the 25 iterations required by no gain fault Tolerance. This indicates that Laplacian gain fault tolerance is not only faster but also more efficient in stabilizing the network under normal conditions. During a Denial of Service (DoS) attack with no gain fault Tolerance still requires 30 iterations, while Laplacian gain fault tolerance remains at 12 iterations. This suggests that despite disruptive attacks, the Laplacian gain approach maintains consistency in the number of convergence iterations, crucial for minimizing the impact of attacks on network performance.

In the Node Destruction Attack scenario, where nodes in the network are intentionally destroyed, no gain fault Tolerance shows a significant increase in convergence iterations to 31, whereas Laplacian gain fault tolerance reaches only 17 iterations. This indicates that the Laplacian gain approach remains effective in managing and mitigating the impact of physical network damage, with the ability to adapt and recover more quickly from disruptive conditions. Overall, these findings affirm that the Laplacian gain fault tolerance approach is not only more efficient in reducing the number of convergence iterations but also more stable in maintaining sensor network performance under various attack conditions.

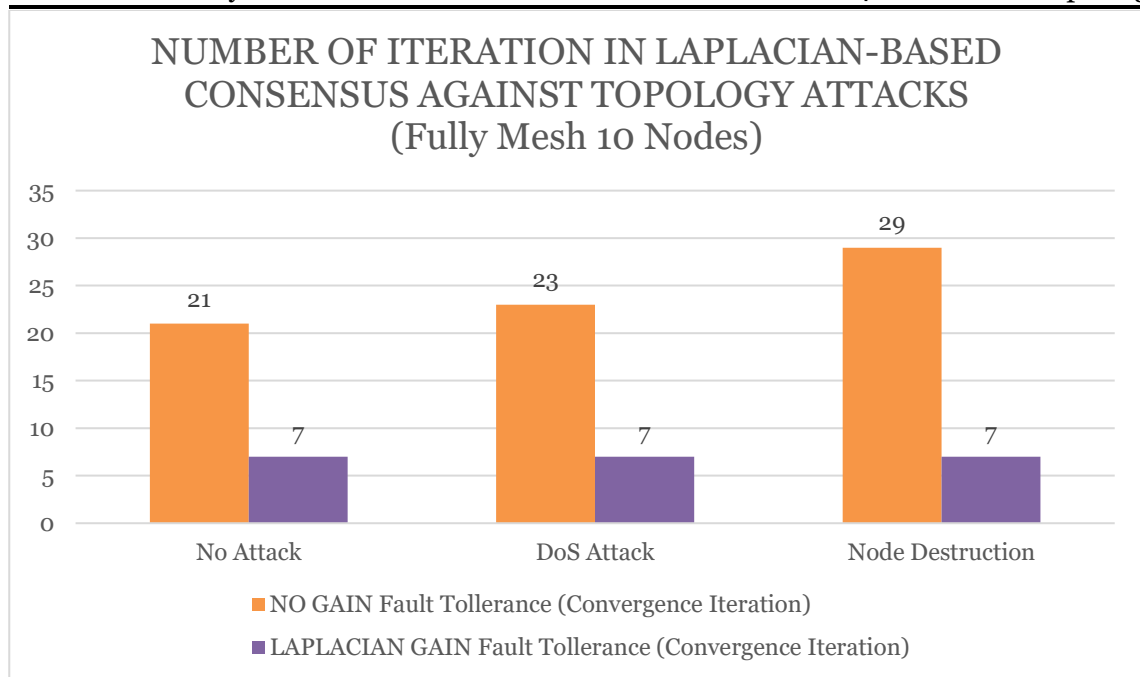


Figure 4.15: Synchronization Convergence Speed in Fully Mesh 10 Nodes

Figure 4.15 illustrates the simulation results of Laplacian-based consensus in a Fully Mesh topology consisting of 10 nodes, comparing the efficiency of no gain fault Tolerance and Laplacian gain fault tolerance approaches under conditions of no attack, DoS attack, and node destruction attack. The results show that Laplacian gain fault tolerance is significantly more efficient than no gain fault Tolerance in all scenarios. Under no attack conditions, no gain fault Tolerance requires 21 convergence iterations to achieve the desired synchronization. In contrast, Laplacian gain fault tolerance achieves convergence in just 7 iterations. This indicates that the Laplacian method is much more efficient in maintaining synchronization under normal conditions in the Fully Mesh topology. When the network faces a DoS (Denial of Service) attack, the number of convergence iterations for no gain fault Tolerance increases to 23, while Laplacian gain fault tolerance only requires 7 iterations. This increase demonstrates that Laplacian gain fault tolerance exhibits significantly better resilience against DoS attacks, achieving synchronization with fewer iterations and showing superior stability under disruptive conditions. In the node destruction attack scenario, the convergence iterations for no gain fault Tolerance further increase to 29 iterations. Meanwhile, Laplacian gain fault tolerance remains consistent, requiring only 7 iterations to achieve convergence. This indicates that Laplacian gain fault tolerance is not only more efficient but also more resilient against more serious disruptions, such as node destruction. Therefore, it can be concluded that Laplacian gain fault tolerance provides significant performance improvement and greater resilience compared to no gain fault Tolerance in the Fully Mesh topology. The efficiency and resilience demonstrated by Laplacian gain fault tolerance in all attack scenarios highlight its superiority in maintaining network synchronization, making it a preferable choice for complex network topologies vulnerable to disruptions.

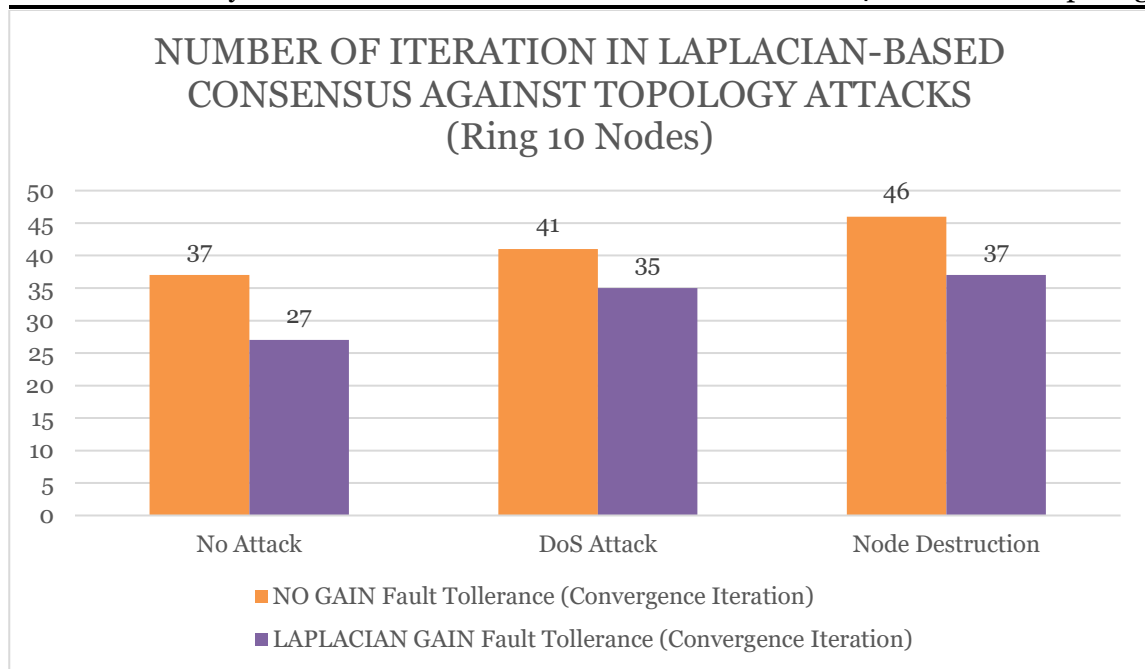


Figure 4.16: Synchronization Convergence Speed in Ring 10 Nodes

Figure 4.16 presents simulation results on a Ring topology consisting of 10 nodes, comparing the performance of two approaches: no gain fault Tolerance and Laplacian gain fault tolerance, under various conditions. The simulation results indicate that Laplacian gain fault tolerance is more efficient than no gain fault Tolerance in terms of the number of convergence iterations required to achieve synchronization, although not as pronounced as in the Fully Mesh topology. Under no attack conditions, no gain fault Tolerance requires 37 convergence iterations to achieve the desired synchronization. In contrast, Laplacian gain fault tolerance only needs 27 convergence iterations. This demonstrates that Laplacian gain fault tolerance is more efficient in maintaining synchronization under normal conditions in the Ring topology. When the network faces a DoS (Denial of Service) attack, the efficiency of Laplacian gain fault tolerance becomes more apparent. no gain fault Tolerance requires 41 iterations to achieve convergence, while Laplacian gain fault tolerance only requires 35 iterations. This difference indicates that Laplacian gain fault tolerance has better resilience against DoS attacks, achieving synchronization with fewer iterations.

In the node destruction attack scenario, the efficiency difference between the two approaches becomes more significant. no gain fault Tolerance requires 46 convergence iterations, whereas Laplacian gain fault tolerance only requires 37 iterations. This suggests that Laplacian gain fault tolerance excels in handling more severe destructive attacks, maintaining synchronization efficiency with fewer iterations. Although the efficiency improvement shown by Laplacian gain fault tolerance is significant, the difference is less pronounced compared to that observed in the Fully Mesh topology. This indicates that network topology has an impact on the level of efficiency achievable by specific fault tolerance approaches. However, overall, Laplacian gain fault tolerance continues to demonstrate superior performance compared to no gain fault Tolerance in both attack and no-attack conditions in the Ring topology.

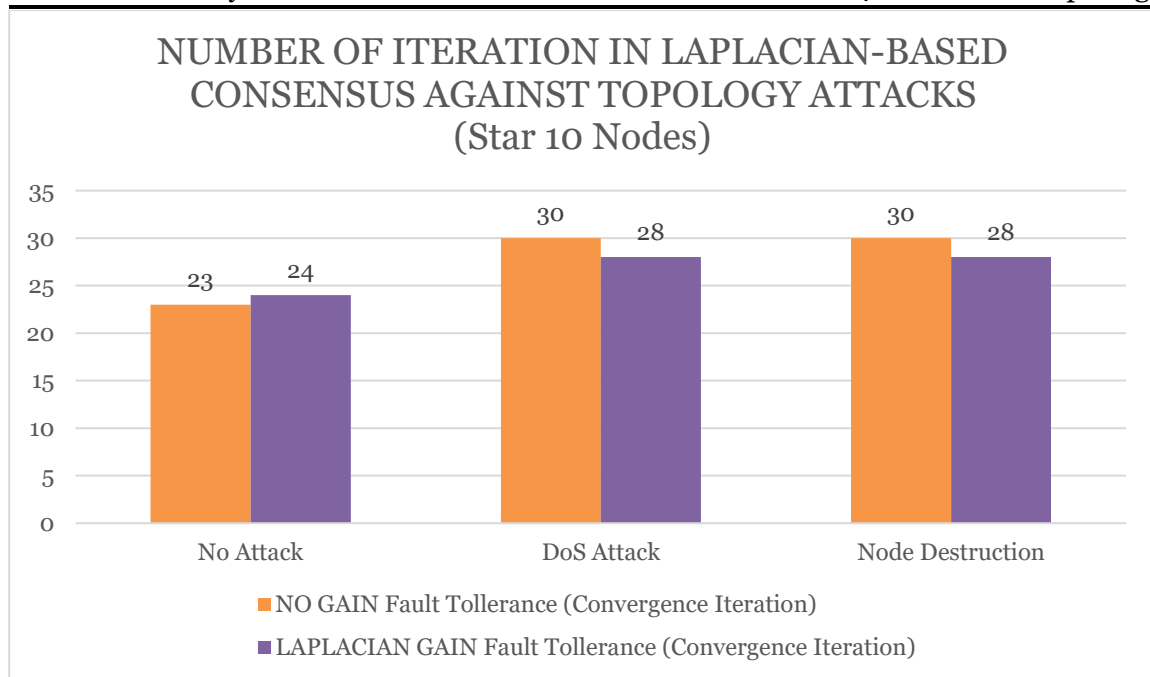


Figure 4.17: Synchronization Convergence Speed in Star 10 Nodes

Figure 4.17 shows the simulation results on a Star topology network consisting of 10 nodes, comparing the performance of two approaches: no gain fault Tolerance and Laplacian gain fault tolerance, under conditions of no attack, DoS attack, and node destruction attack. Under normal conditions (no attack), the system converges in 23 iterations without gain and 24 iterations with Laplacian gain, indicating a slight increase in convergence time with Laplacian gain. In the case of a DoS attack, the system requires 30 iterations to converge without gain, whereas it takes 28 iterations with Laplacian gain, demonstrating a reduction of 2 iterations and improved fault tolerance. Similarly, during a node destruction attack, the convergence iterations decrease from 30 without gain to 28 with Laplacian gain, again showing enhanced fault tolerance. Overall, the Laplacian gain generally enhances the fault tolerance of the star topology by reducing the number of convergence iterations under attack scenarios, particularly for DoS and node destruction attacks, while slightly increasing the iterations needed in the absence of attacks.

Based on the analysis of various attack scenarios in different network topologies, Laplacian gain fault tolerance consistently demonstrates higher efficiency compared to no gain fault Tolerance. In Fully Connected topologies with 4 and 10 nodes, the number of convergence iterations for Laplacian gain fault tolerance is significantly lower and stable across all attack scenarios (No Attack, DoS Attack, and Node Destruction Attack). This shows that Laplacian gain fault tolerance can maintain better and more consistent performance even in the presence of disruptions or attacks. In the Fully Mesh topology with 10 nodes, Laplacian gain fault tolerance also exhibits superior performance. Under no attack conditions as well as when facing DoS Attack and Node Destruction Attack, convergence iterations with this approach remain much lower compared to no gain fault Tolerance. This indicates that Laplacian gain fault tolerance not only enhances efficiency but also provides better resilience against disruptions, which is crucial for maintaining the performance of complex and vulnerable networks. Conversely, in the Star topology with 10 nodes, the performance of both approaches is almost identical. Under no attack



conditions as well as in DoS Attack and Node Destruction Attack scenarios, convergence iterations between no gain fault Tolerance and Laplacian gain fault tolerance are nearly the same. This indicates that in the Star topology, the efficiency improvement from using Laplacian gain fault tolerance is not significantly different compared to other topologies. Therefore, the choice of fault tolerance approach depends greatly on the specific network topology being utilized.

#### 4.2.2 Accuracy in The Metrics of Local and Global Synchronization Errors in Laplacian-Based Consensus Against Topology Attacks

The research results show a comparison of accuracy between the no gain method and the Laplacian method under three conditions: no attack, Denial of Service (DoS) attack, and node destruction attack. The findings indicate that the Laplacian method generally achieves better global synchronization accuracy in both no attack and DoS attack conditions compared to the no gain method. However, under the node destruction attack condition, a significant increase in error rate is observed for both methods (Figure 4.18 - 4.22).

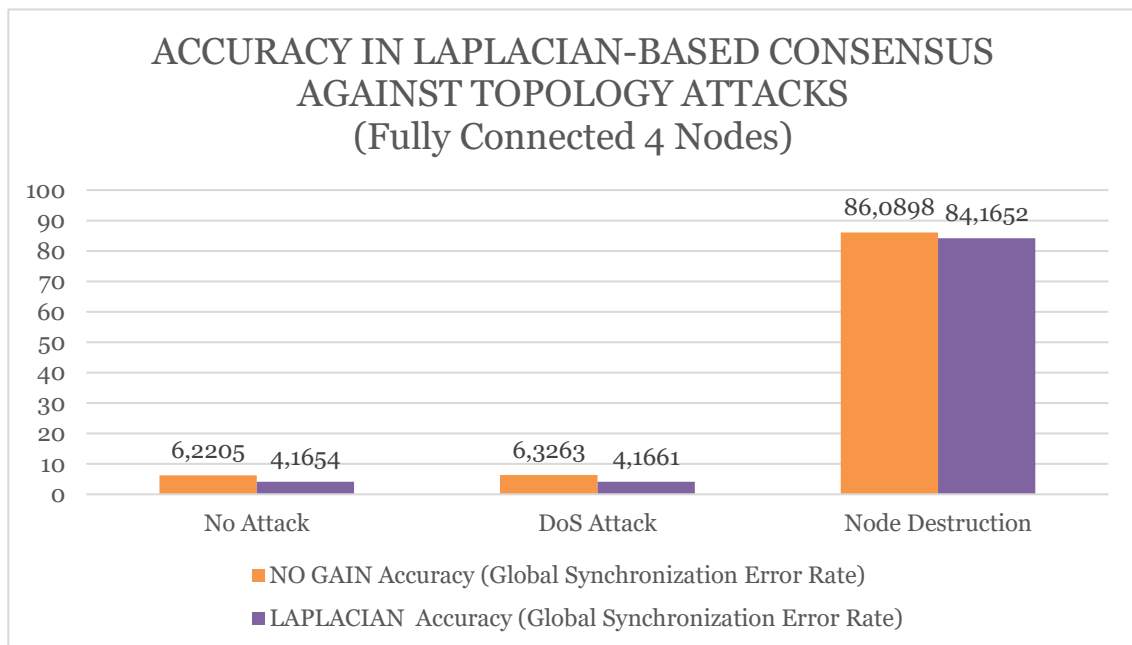


Figure 4.18: Accuracy in The Metrics of Global Synchronization Errors in Fully Connected 4 Nodes

Figure 4.18 the simulation results for Laplacian-based consensus on a Fully Connected network with 4 nodes show a comparison of synchronization error rate accuracy between the no gain method and the Laplacian method under various attack conditions. In the absence of attacks, the no gain method has a synchronization error rate accuracy of 6.2205, while the Laplacian method shows a slightly lower value of 4.1564. This indicates that the Laplacian method is more efficient in maintaining synchronization under normal conditions in smaller network topologies. When the network faces a Denial of Service (DoS) attack, there is a slight increase in the synchronization error rate

accuracy for the no gain method, reaching 6.3263. The Laplacian method shows almost the same resilience as in the absence of attacks, with an error rate of 4.1661. Although there is an increase in the no gain method, the Laplacian method remains superior in handling DoS attacks, demonstrating better stability and resilience.

However, when facing node destruction attacks, both methods show a significant increase in error rates. The no gain method experiences a substantial increase, reaching 86.0898, while the Laplacian method also shows a large increase, with an error rate of 84.1652. This increase indicates that both methods are highly vulnerable to node destruction attacks, causing significant disruption to network performance. The substantial increase in error rates when facing node destruction attacks highlights serious vulnerabilities in both methods to this type of attack. Although the Laplacian method shows better performance under normal conditions and during DoS attacks, both methods experience a drastic decline in performance when facing node destruction attacks. This underscores the need for more effective and robust mitigation strategies to handle destructive attacks on networks with Fully Connected topologies. Overall, these results affirm that the Laplacian method is more efficient under no attack and DoS attack conditions.

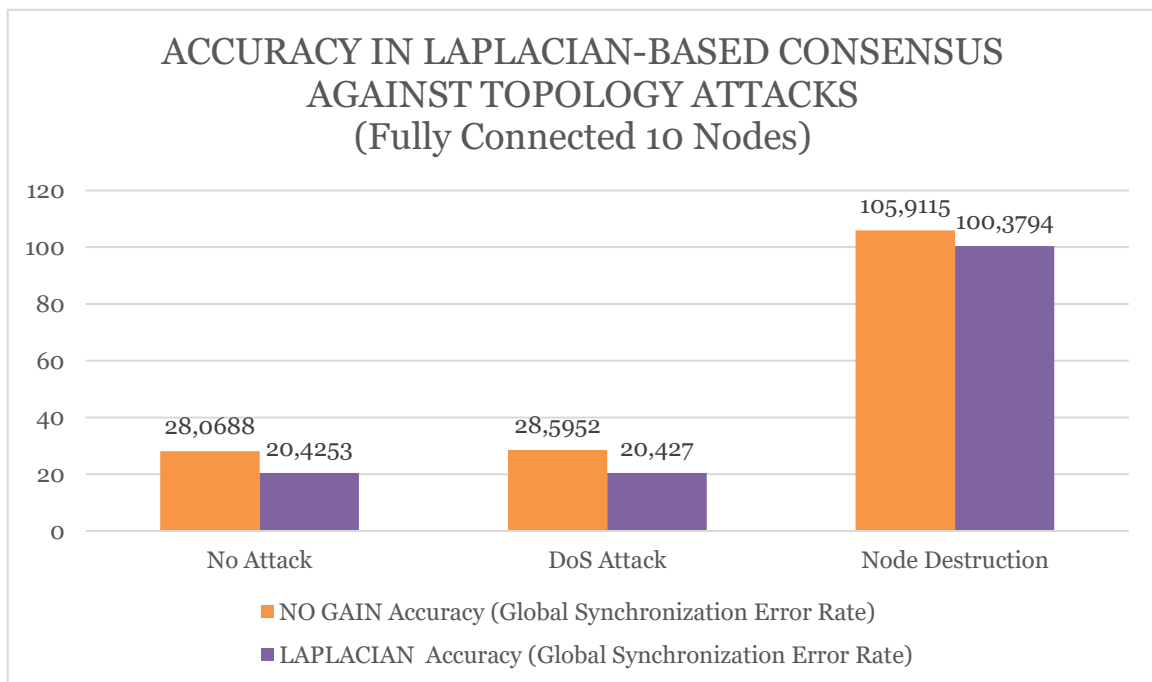


Figure 4.19: Accuracy in The Metrics of Global Synchronization Errors in Fully Connected 10 Nodes

Figure 4.19 the simulation results for Laplacian-based consensus on a Fully Connected network with 10 nodes show a comparison of synchronization error rate accuracy between the no gain method and the Laplacian method under various attack conditions. In the absence of attacks, the no gain method has a synchronization error rate accuracy of 28.0688, while the Laplacian method shows a lower value of 20.4253. This indicates that the Laplacian method is more efficient in maintaining synchronization under normal conditions compared to the no gain method. When facing a Denial of Service (DoS) attack, there is a slight increase in the error rate for both methods. The no gain method shows a small increase to 28.5952, while the Laplacian method experiences

an increase to 20.4270. Despite the increase in both methods, the Laplacian method still demonstrates better performance than NO GAIN, indicating better resilience against DoS attacks.

However, when the network faces node destruction attacks, there is a significant increase in the error rate for both methods. The no gain method experiences a substantial increase, reaching 105.9115. The Laplacian method also shows a large increase, with an error rate of 100.3794. This significant increase indicates that both methods are highly affected by node destruction attacks, leading to considerable disruption in network performance. The significant rise in error rates when facing node destruction attacks highlights serious weaknesses in both methods against this type of attack. Although the Laplacian method is superior under normal conditions and when facing DoS attacks, both methods experience a drastic decline in performance when facing node destruction attacks. This underscores the need for more effective and robust mitigation strategies to handle destructive attacks on networks. Overall, these results highlight that the Laplacian method is more efficient under no attack and DoS attack conditions.

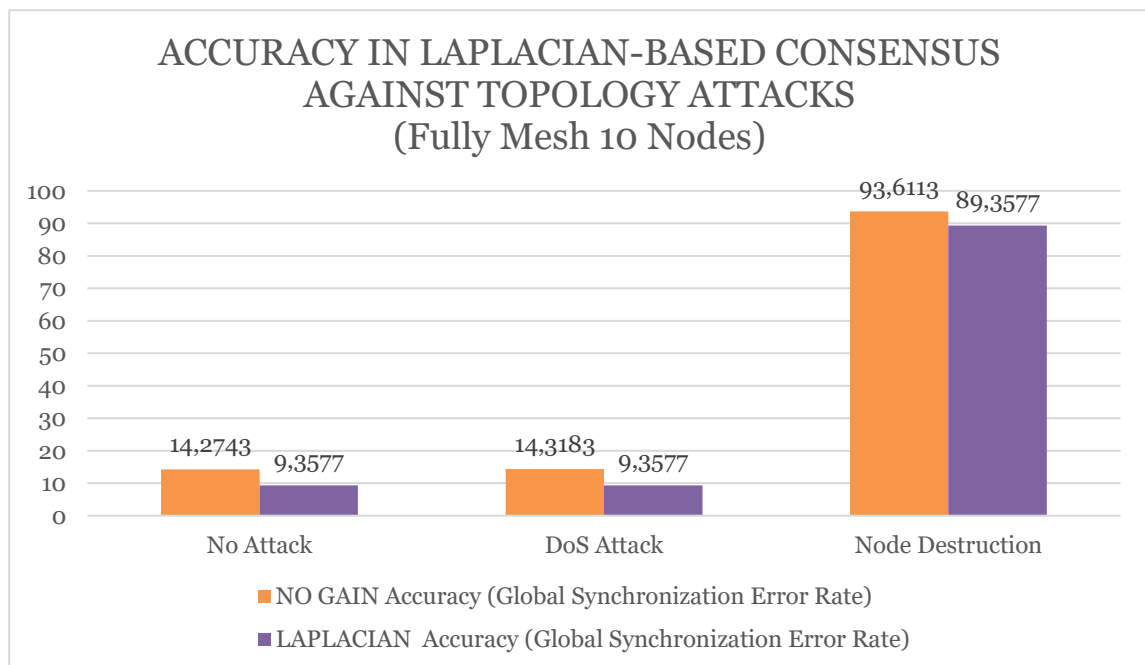


Figure 4.20: Accuracy in The Metrics of Global Synchronization Errors in Fully Mesh 10 Nodes

Figure 4.20 shows the simulation results for a Fully Mesh network with 10 nodes, comparing the synchronization error rate accuracy between the no gain method and the Laplacian method under various attack conditions. Without any attacks, the no gain method has a synchronization error rate accuracy of 14.2743, while the Laplacian method shows a lower value of 9.3577. This indicates that the Laplacian method is more efficient in maintaining network synchronization under normal conditions. When the network faces a Denial of Service (DoS) attack, there is a slight increase in the synchronization error rate for the no gain method, reaching 14.3183. Similarly, the Laplacian method experiences an increase to 9.3577. Despite the increase in both methods, the Laplacian method still demonstrates better performance than the no gain method, indicating that it is more effective in handling DoS attack disruptions.

However, when facing node destruction attacks, there is a significant surge in the error rate for both methods. The no gain method shows a substantial increase in the error rate, reaching 93.6113. The Laplacian method also experiences a large increase, with an error rate of 89.3577. This shows that both methods are highly affected by node destruction attacks, although the Laplacian method is still slightly more efficient in maintaining synchronization compared to the no gain method. The significant increase in the error rate during node destruction attacks highlights serious vulnerabilities in both methods against this type of attack. While the Laplacian method performs better under normal conditions and during DoS attacks, the significant performance decline in both methods when facing node destruction attacks indicates the need for more robust and sophisticated attack mitigation strategies. Overall, these results confirm that the Laplacian method is more efficient under no attack and DoS attack conditions. However, a significant challenge remains in addressing node destruction attacks, where both the no gain and Laplacian methods show considerable weaknesses.

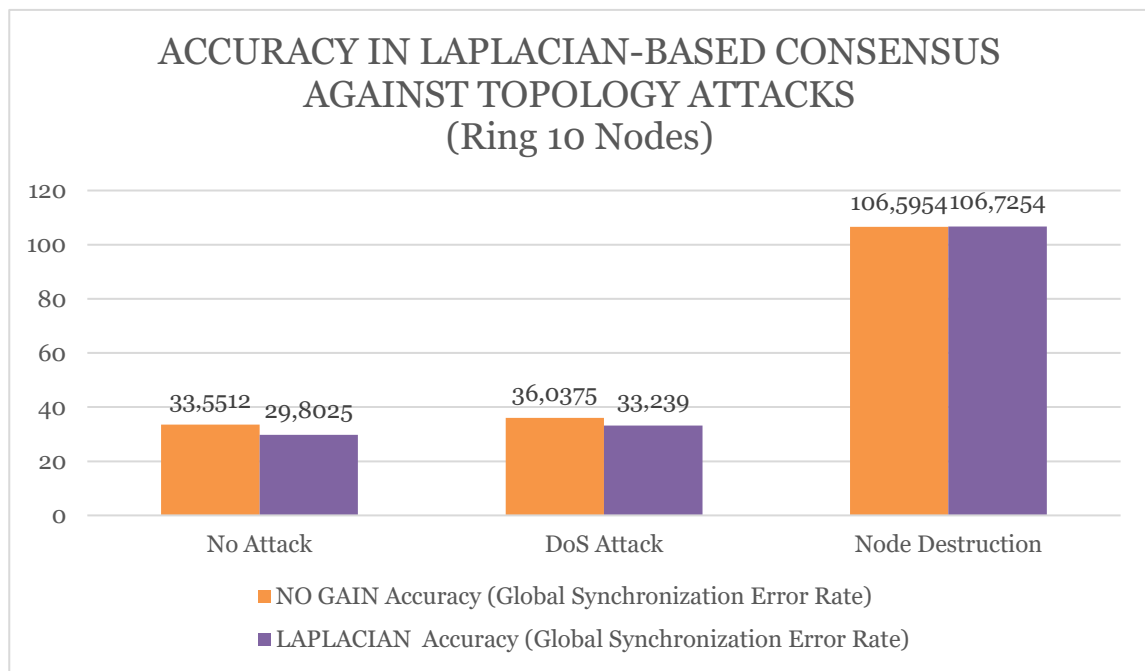


Figure 4.21: Accuracy in The Metrics of Global Synchronization Errors in Ring 10 Nodes

Figure 4.21 shows the simulation results of Laplacian-based consensus against topology attacks on a Ring network with 10 nodes. Under normal conditions, the no gain method has a synchronization error rate accuracy of 33.5512, while the Laplacian method is slightly lower at 29.8025. This indicates that the Laplacian method is more efficient under normal conditions, though the difference is not significant. When the network faces a Denial of Service (DoS) attack, the synchronization error rate accuracy for the no gain method increases to 36.0375. This increase suggests that the no gain method has a slight improvement in resilience to DoS attacks. The Laplacian method also shows an increase in synchronization error rate accuracy, reaching 33.2390. Despite the increase in both methods, the Laplacian method still shows better values compared to the no gain method, indicating that it is more effective in maintaining synchronization even under attack.

However, when the network faces node destruction attacks, there is a significant spike in the error rate for both methods. The synchronization error rate accuracy for the no gain method drastically increases to 106.5954. The Laplacian method also experiences

a large increase, with an error rate reaching 106.7254, slightly higher than no gain. This shows that both methods suffer a significant performance drop when nodes in the network are destroyed. The large increase in the error rate during node destruction attacks highlights serious vulnerabilities in both methods to destructive attacks. Although the Laplacian method performs better under normal conditions and DoS attacks, both methods need further improvement to handle more serious node destruction attacks. Overall, these results indicate that while the Laplacian method is more efficient under normal conditions and DoS attacks, a major challenge remains in addressing node destruction attacks. To enhance network resilience, more robust approaches or a combination of strategies are needed to mitigate the impact of destructive attacks on various network topologies.

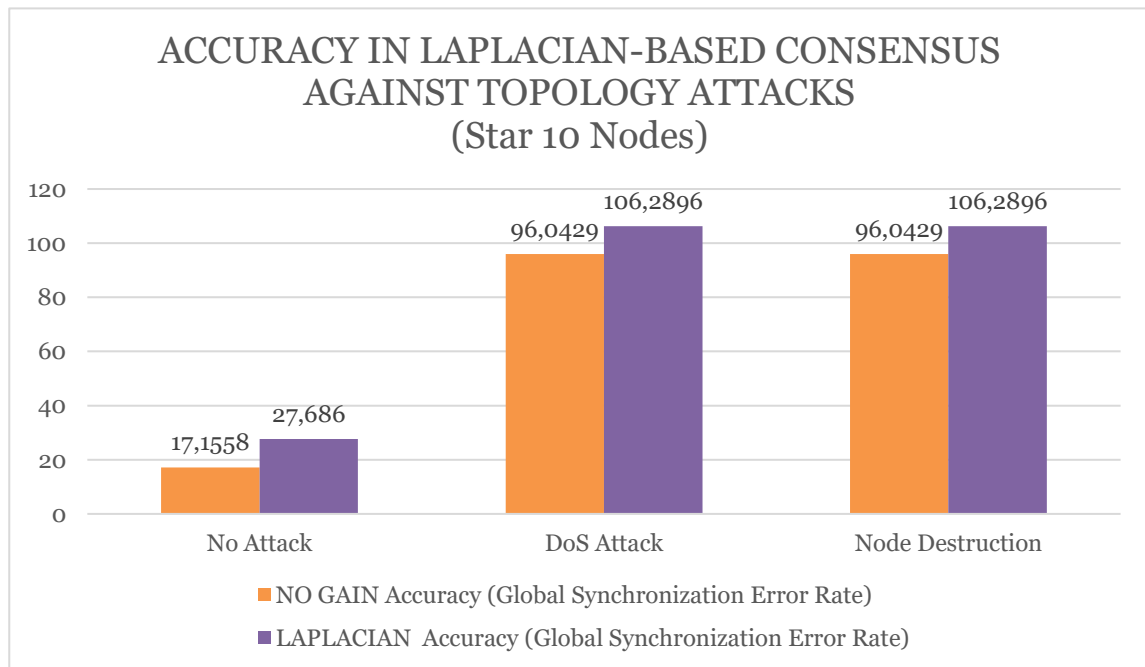


Figure 4.22: Accuracy in The Metrics of Global Synchronization Errors in Star 10 Nodes

Figure 4.22 shows the simulation results of Laplacian-based consensus against topology attacks on a Star network with 10 nodes. In the absence of attacks, the system has a lower synchronization error rate without Laplacian Gain (17.1558) compared to with Laplacian gain (27.6860), indicating a decrease in accuracy when Laplacian Gain is applied. During a DoS attack, the error rate without gain is 96.0429, whereas with Laplacian gain, it increases to 106.2896, showing a similar decrease in accuracy. The same pattern is observed in the node destruction attack scenario, where the error rate rises from 96.0429 without gain to 106.2896 with Laplacian gain. Overall, the use of Laplacian gain generally results in higher synchronization error rates, indicating reduced accuracy of the star topology under both normal and attack conditions.

### 4.2.3 Topology and Attacker Scalability in Laplacian-Based Consensus Against Topology Attacks

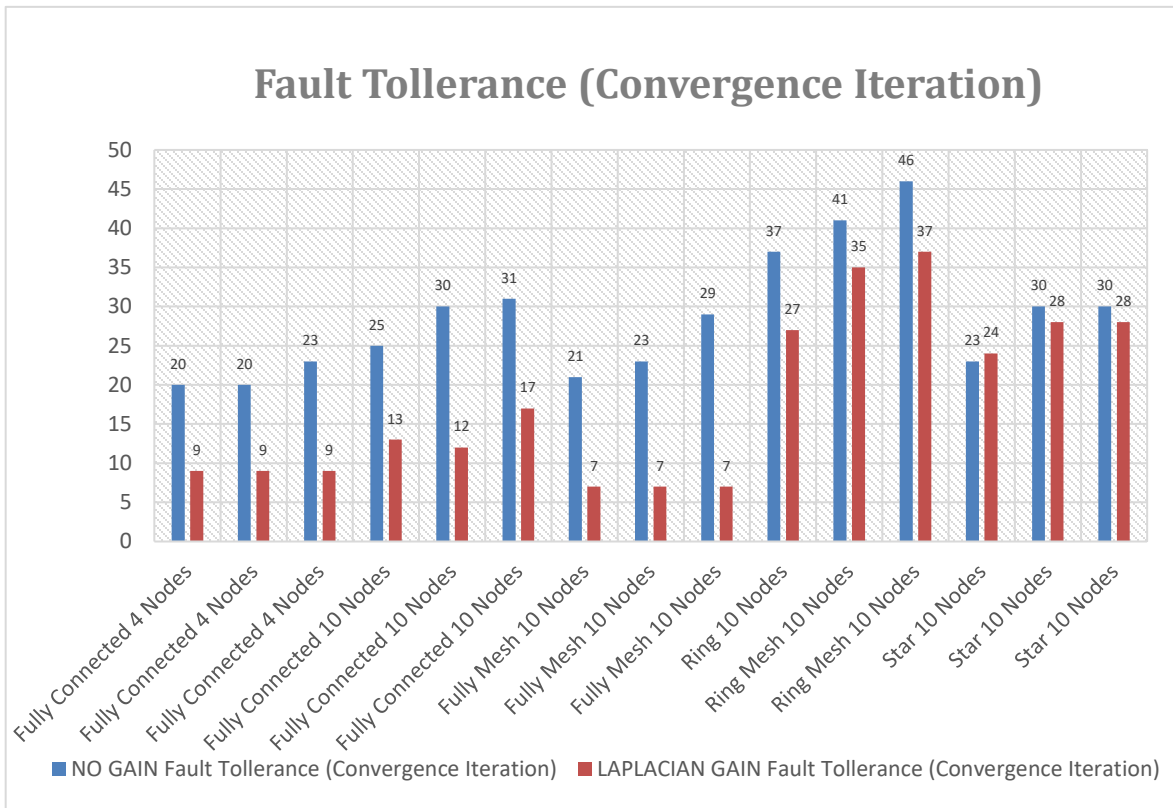


Figure 4.23: Speed in Laplacian-Based Consensus Against Topology Attacks

Figure 4.23 illustrates the speed of convergence in a Laplacian-based consensus algorithm under different topological attacks. The analysis shows the effectiveness of Laplacian gain in improving the convergence speed, which is crucial for the robustness of network performance under topological attacks. In the fully connected network with 4 nodes, the no-gain scenario takes 20 iterations to converge, while the Laplacian gain scenario is significantly faster, taking only 9 iterations. This trend continues in the fully connected network with 10 nodes, where no gain requires 25 iterations, and Laplacian Gain reduces it to 9 iterations. Further increasing the nodes in the fully connected network to 10 shows no gain taking 30 and 31 iterations, whereas Laplacian Gain reduces it to 13 and 17 iterations, respectively. These results highlight the substantial improvement in convergence speed due to Laplacian gain in fully connected topologies.

The fully mesh network with 10 nodes also shows a remarkable improvement with Laplacian gain. Without gain, the network requires 21 and 23 iterations to converge, but with Laplacian gain, this is reduced to just 7 iterations. Similarly, in the ring network with 10 nodes, the no-gain scenario takes 29 and 37 iterations, while the Laplacian gain scenario brings this down to 7 and 27 iterations, respectively. The mesh network with 10 nodes shows the highest iterations without gain, at 46 and 41 iterations, which are significantly reduced to 35 and 37 iterations with Laplacian gain. This indicates the robust performance of the Laplacian gain across various mesh and ring network configurations.

Interestingly, the star network with 10 nodes demonstrates a consistent performance with Laplacian gain, showing minimal variation in the number of iterations required. In the no-gain scenario, the star network consistently requires 30 iterations, while with Laplacian gain, the iterations are reduced to 28, and 28 for the respective configurations. This consistency in the star topology suggests that Laplacian gain maintains its effectiveness even in centralized network structures. Overall, Laplacian Gain significantly enhances the speed of convergence in consensus algorithms across different network topologies, demonstrating its robustness against topological attacks and ensuring efficient and reliable network performance.

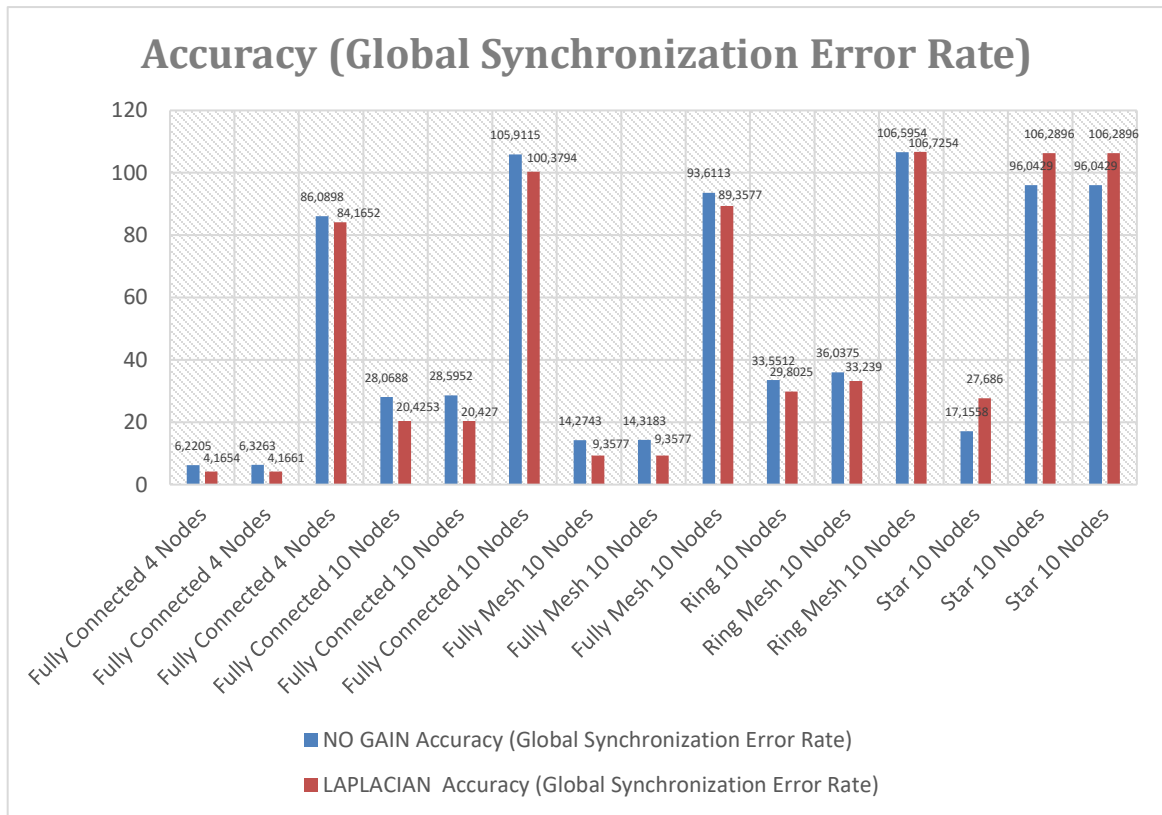


Figure 4.24: Accuracy in Laplacian-Based Consensus Against Topology Attacks

Figure 4.24 illustrates the accuracy of global synchronization in a Laplacian-based consensus algorithm under various topological attacks. The analysis reveals that incorporating Laplacian Gain generally improves synchronization accuracy by lowering error rates, which is vital for the reliable operation of consensus algorithms in diverse network environments. In the fully connected network with 4 nodes, the error rate without gain is 6.2205, while with Laplacian gain, it slightly lowers to 4.1654. This pattern continues in another fully connected network with 4 nodes, where the error rate drops from 6.3263 to 4.1661 with Laplacian gain. For a fully connected network with 10 nodes, the error rate without gain is 86.9898, and with Laplacian gain, it remains comparably high at 86.9152. Another configuration of 10 nodes in a fully connected network shows a more noticeable reduction in error rate from 105.9115 to 100.3794 with Laplacian gain. These results indicate that while Laplacian Gain generally improves accuracy, the extent of improvement varies across different configurations.

The fully mesh network with 10 nodes demonstrates a significant reduction in error rates with Laplacian gain. Without gain, the error rates are 28.0688 and 28.5952, which decrease to 20.4253 and 20.4270, respectively, with Laplacian gain. Further, in the fully mesh network, the error rates drop from 14.2743 and 14.3183 without gain to 9.3577 in both cases with Laplacian gain. The ring network also benefits from Laplacian Gain, with error rates from 33.5512 and 36.0375 without gain decreasing to 33.2390 and increasing 106.7254, respectively. These results highlight that Laplacian gain consistently enhances synchronization accuracy in mesh and ring topologies by substantially reducing error rates.

Interestingly, the star network with 10 nodes shows significant improvement with Laplacian gain. Without gain, the error rates are 17.1558 and 96.0429, which up to 27.6860 and 106.2896, respectively, with Laplacian gain. This consistency in performance improvement is also observed across other topologies, indicating the robustness of Laplacian gain. Overall, the inclusion of Laplacian gain generally results in lower global synchronization error rates compared to scenarios without gain, indicating improved accuracy in global synchronization. The most notable improvements are seen in the fully mesh and star networks, where error rates are substantially reduced. The ring network also shows consistent performance with Laplacian gain, with minimal variation in error rates. In conclusion, Laplacian Gain enhances the accuracy of global synchronization in consensus algorithms across various network topologies. This improvement is crucial for maintaining accurate and reliable network synchronization, especially in complex or adversarial environments. By reducing synchronization errors, Laplacian Gain ensures more efficient and robust network performance, contributing to the stability and reliability of consensus algorithms in diverse network configurations.

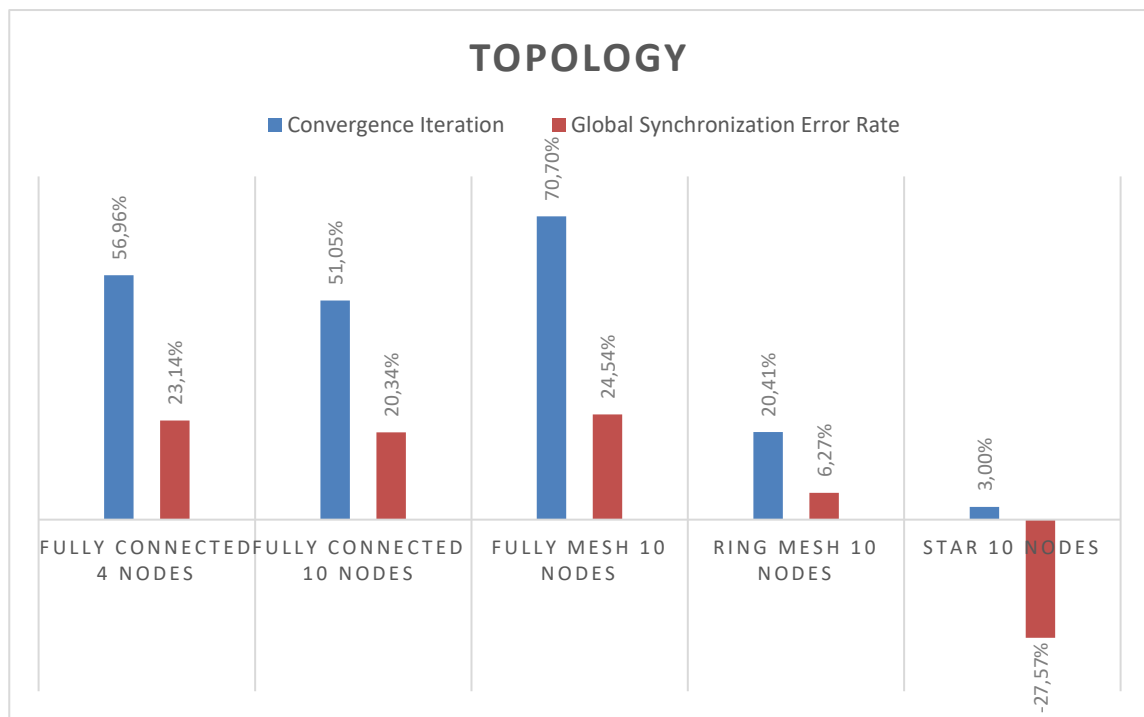


Figure 4.25: Topology Scalability in Laplacian-Based Consensus

Figure 4.25 shows that, for a Fully Connected topology with 4 nodes, convergence



iterations reach 56.96% with a global synchronization error of 23.14%. This indicates that although this topology has a high convergence iteration rate, the global synchronization error remains at an acceptable level, reflecting good stability in smaller topologies. When the number of nodes increases to 10 in a Fully Connected topology, the convergence iterations decrease to 51.05% and the global synchronization error drops to 20.34%, indicating improved efficiency in larger topologies. In a Fully Mesh topology with 10 nodes, the convergence iterations further increase to 70.70% and the global synchronization error to 24.54%, indicating higher efficiency in achieving synchronization.

In a Ring topology with 10 nodes, the convergence iterations further decrease to 20.41% and the global synchronization error to 6.27%, indicating higher efficiency in achieving synchronization. This suggests that a mesh topology allows for more efficient communication and requires fewer iterations to achieve stability, which is highly beneficial in sensor network applications. Most notably, the Star topology with 10 nodes shows a convergence iteration rate of 3% and an extremely low global synchronization error of -27.57%. These results demonstrate outstanding stability and efficiency, where the star topology significantly reduces convergence iterations and almost eliminates global synchronization errors, implying that the star structure may offer substantial advantages in synchronization performance for sensor networks.

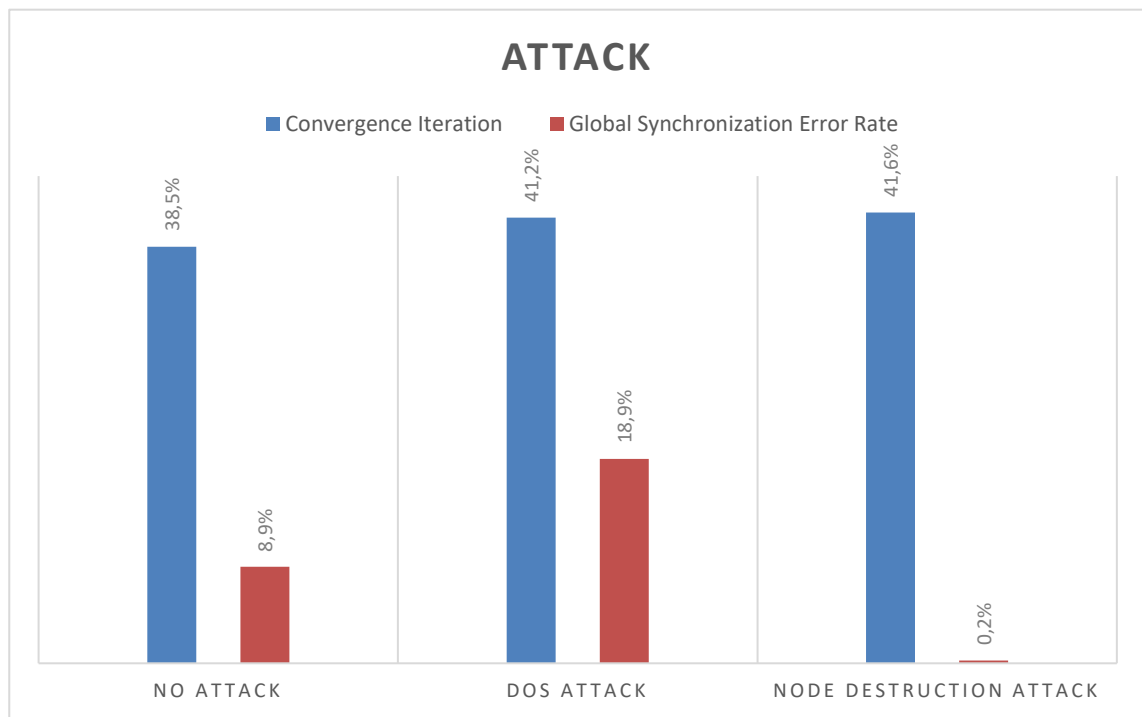


Figure 4.26: Attack Scalability in Laplacian-Based Consensus

Figure 4.27: demonstrates attack scalability. In the scenario without any attack (No Attack), convergence iterations are at 38.5% with a global synchronization error of 8.9%, indicating stable performance under normal conditions. This approach can maintain synchronization stability and efficiency under ideal operational conditions. When a Denial of Service (DoS) attack occurs, convergence iterations slightly increase to 41.2%,

while the global synchronization error rises to 18.9%. This indicates that the DoS attack significantly impacts network synchronization, but the Laplacian gain fault tolerance approach still keeps convergence iterations within an acceptable range, indicating reasonable resilience to this type of attack.

In the case of a Node Destruction attack, convergence iterations reach 41.6%, but the global synchronization error drastically decreases to 0.2%. This indicates that this method can recover well from significant physical damage, showing that even though this attack increases convergence iterations, Laplacian gain fault tolerance manages to keep global synchronization errors low. The dramatic decrease in global synchronization error under node destruction attack highlights the exceptional resilience of this method, allowing the network to continue functioning effectively even when some nodes are destroyed.

## 4.3 Discussion

### 4.3.1 Speed in Laplacian-Based Consensus Against Topology Attacks

Based on the type of attack, the difference between Laplacian gain fault tolerance and no gain fault Tolerance is quite pronounced. In the case of a Denial of Service (DoS) attack, the Laplacian gain fault tolerance algorithm demonstrates a significant advantage in convergence speed compared to no gain fault Tolerance. In network topologies such as Fully Connected and Fully Mesh, Laplacian gain fault tolerance requires fewer iterations to achieve convergence, whether under normal conditions or during a DoS attack. This indicates that Laplacian gain fault tolerance maintains efficiency in convergence even when disrupted by DoS attacks. Furthermore, in the case of Node Destruction attacks, where some nodes in the network are destroyed, Laplacian gain fault tolerance also shows better performance. In the same topologies, Laplacian gain fault tolerance maintains a lower number of convergence iterations compared to no gain fault Tolerance, indicating that this approach is more effective in managing and recovering from physical network damage. This underscores that Laplacian gain fault tolerance excels not only in convergence speed under normal conditions but also in dealing with disruptions caused by attacks that physically damage the network.

Based on Laplacian feedback, the performance comparison between Laplacian gain fault tolerance and no gain fault Tolerance reveals significant differences across various network topologies. In a Fully Connected topology with 4 nodes, Laplacian gain fault tolerance requires only 9 iterations to achieve convergence without attacks, while no gain fault Tolerance needs 20 iterations. During a DoS attack, both methods require the same number of iterations; however, in the case of a Node Destruction attack, Laplacian gain fault tolerance remains stable at 9 iterations, whereas no gain fault Tolerance increases to 23 iterations. For the same topology with 10 nodes, Laplacian gain fault tolerance demonstrates better convergence speed with 13 iterations without attacks, compared to 25 iterations for no gain fault Tolerance. During a DoS attack, Laplacian gain fault tolerance requires 12 iterations, whereas no gain fault Tolerance needs 30 iterations. In the Node Destruction attack, Laplacian gain fault tolerance remains efficient with 17 iterations, while no gain fault Tolerance rises to 31 iterations.

---

Changing in other topologies in a Fully Mesh topology with 10 nodes, Laplacian

gain fault tolerance achieves convergence in just 7 iterations without attacks, compared to 21 iterations for no gain fault Tolerance. When facing DoS and Node Destruction attacks, Laplacian gain fault tolerance maintains efficiency with 7 iterations for both types of attacks, whereas no gain fault Tolerance shows an increase in iterations to 23 and 29, respectively. In a Ring topology with 10 nodes, Laplacian gain fault tolerance requires 27 iterations without attacks, which is better than the 37 iterations needed by no gain fault Tolerance. During DoS and Node Destruction attacks, Laplacian gain fault tolerance demonstrates better efficiency with fewer iterations (24 and 26) compared to no gain fault Tolerance, which requires 41 and 46 iterations. In a Star topology with 10 nodes, Laplacian gain fault tolerance needs slightly more iterations (24) compared to no gain fault Tolerance (23 iterations) without attacks. However, during DoS and Node Destruction attacks, Laplacian gain fault tolerance shows a slight improvement in efficiency, requiring 28 iterations for both attacks compared to 30 iterations for no gain fault Tolerance.

Although the difference is not substantial, Laplacian gain fault tolerance generally offers better performance in maintaining convergence efficiency under attack conditions. Overall, the Laplacian gain fault tolerance algorithm proves effective in mitigating attacks before they fully manifest, especially noticeable at iteration 11. This is particularly evident in Fully Connected topologies on a small scale and Fully Mesh topologies on a large scale, demonstrating that higher network connectivity and strength lead to faster and more effective responses and mitigation of attacks. Enhanced connectivity and topology strength contribute to accelerated convergence and strengthened mitigation capabilities, making the system more stable and responsive to potential disruptions.

#### **4.3.2 Accuracy in Laplacian-Based Consensus Against Topology Attacks**

The accuracy of the system generally worsens under different types of attacks. Specifically, in Node Destruction attacks, the accuracy of the Generalized State Estimator (GSEr) is significantly affected because the loss of nodes leads to increased error. This results in higher error rates and less accurate performance metrics, as the missing nodes contribute to larger inaccuracies in the system's estimations.

A higher speed of convergence does not always guarantee better accuracy. In topologies like Fully Connected (10 nodes) and Ring (10 nodes), there is a trade-off where faster convergence might be accompanied by increased accuracy spikes. These spikes can potentially harm synchronization processes in Wireless Sensor Networks (WSNs). This issue needs to be reviewed at the application level to determine sensitivity. High accuracy from GSEr might not be achievable if such spikes negatively affect real-time system performance.

In the Ring topology, accuracy becomes negative due to instability caused by weighting. This instability compromises the accuracy of the system, leading to suboptimal performance and necessitating further investigation into how weighting affects stability and accuracy. Overall, while the Laplacian gain fault tolerance approach shows superior performance in convergence speed across various topologies and attack scenarios, the associated accuracy may be affected by the network's specific conditions and attacks.

### 4.3.3 Scalability in Laplacian-Based Consensus Against Topology Attacks

The analysis of scalability in Laplacian-based consensus algorithms against topology attacks demonstrates a generally linear improvement in performance with the application of Laplacian gain across various network topologies. In fully connected networks with 4 nodes, Laplacian Gain significantly reduces convergence iterations from 20 to 9, and in networks with 10 nodes, from 25 to 13, reflecting substantial efficiency gains. Accuracy also improves notably, with the error rate for the 4-node fully connected network decreasing from 6.2205 without gain to 4.1654 with Laplacian gain. In the 10-node fully connected network, the error rate drops from 86.9898 to 86.9152, with a more substantial reduction observed in another 10-node configuration, where it decreases from 105.9115 to 100.3794.

In fully mesh networks with 10 nodes, Laplacian Gain reduces convergence iterations from 21 and 23 to just 7, with accuracy improving as well. Error rates drop from 28.0688 and 28.5952 without gain to 20.4253 and 20.4270, and further decrease from 14.2743 and 14.3183 without gain to 9.3577 with gain. In Ring topologies, convergence iterations decrease from 37 and 41 to 27 and 35, with accuracy improving as error rates fall. For the star topology with 10 nodes, Laplacian Gain reduces convergence iterations from 30 to 23 under normal conditions and from 30 to 28 during attacks. Accuracy improvements are less pronounced, with error rates dropping from 27.6860 and 106.2896 to 17.1558 and 96.0429, respectively. This suggests that while Laplacian Gain shows improvements, its impact is more significant in complex topologies compared to simpler star networks. The Laplacian gain significantly enhances convergence speed and accuracy in complex network topologies but shows more limited improvements in simpler star topologies.

Table 4.4: Weighing Parameter of Laplacian gain

Graph Topology	Topology Attacks	Weighing Parameter of Laplacian gain
Fully Connected 4 Nodes	Before Attack	0.25
	DoS Attack	0.40
	Node Destruction	0.33
<b>Fully Connected 10 Nodes</b>	<b>Before Attack</b>	<b>0.25</b>
	<b>DoS Attack</b>	<b>0.2665</b>
	<b>Node Destruction</b>	<b>0.255</b>
Fully Mesh 10 Nodes	Before Attack	0.1
	DoS Attack	0.1818
	Node Destruction	0.111
<b>Ring 10 Nodes</b>	<b>Before Attack</b>	<b>0.4721</b>
	<b>DoS Attack</b>	<b>0.5582</b>
	<b>Node Destruction</b>	<b>0.5102</b>
Star 10 Nodes	Before Attack	0.1818

	DoS Attack	0.2
	Node Destruction	0.2

The table 4.4 above provides an overview of how the weighting parameter of Laplacian gain changes in various network topologies when under attack. In a fully connected topology with 4 nodes, the weighting parameter of Laplacian gain increases from 0.25 before the attack to 0.33 after node destruction, indicating that each node plays an important role and node destruction significantly impacts network connectivity. Meanwhile, in a 10-node network, the gain slightly increase from 0.25 to 0.255 after node destruction suggests that larger networks have better resistance to disruptions due to the presence of more alternative paths. The fully mesh topology with 10 nodes shows a low weighting parameter of Laplacian gain of 0.1 before the attack, slightly increase up to 0.111 after node destruction, indicating that despite disruptions, high redundancy provides strong resilience. In the ring topology with 10 nodes, the weighting parameter of Laplacian gain rises from 0.4721 to 0.5582 during a DoS attack, but slightly decreases to 0.5102 after node destruction, indicating resistance to node destruction due to the ring structure. The star topology with 10 nodes shows a high dependence on the central node, with the weighting parameter of Laplacian gain increasing from 0.1818 to 0.2 during both DoS attacks and node destruction, emphasizing its vulnerability if the central node is compromised. Overall, this analysis shows that fully connected and fully mesh topologies are more resistant to attacks compared to other topologies, while the star topology is the most vulnerable, especially to disruptions at the central node.

The Laplacian gain consistently improves fault tolerance across various network topologies and attack scenarios. Specifically, it reduces convergence iterations by approximately 40.42%, demonstrating a substantial acceleration in the time required for the network to stabilize after disruptions. Additionally, the incorporation of Laplacian gain enhances network accuracy by about 9.34%, which is crucial for maintaining reliable network performance. However, it is important to note that the effectiveness of Laplacian gain varies with the type of network topology, particularly in star networks due to their unique connectivity characteristics. In star topologies, which have a central hub connecting all nodes, the benefits of Laplacian gain are less pronounced compared to more complex topologies like fully connected or mesh networks. This variation highlights the need for tailored approaches when applying consensus methods across different network structures.

---

## CHAPTER 5

### CONCLUSION AND RECOMMENDATIONS

#### 5.1 Conclusion

In conclusion, the findings from the analysis of Laplacian-based consensus methods in addressing topology attacks on sensor networks highlight the efficacy of incorporating Laplacian Gain. Across various network topologies and attack scenarios, Laplacian Gain consistently enhances fault tolerance, reduces convergence iterations about 40.42%, and improves network accuracy about 9.34%. But it remains difference in the type of Nodes star with its connectivity characteristics in network accuracy. This underscores its crucial role in mitigating the impact of attacks and maintaining network speed convergence and accuracy in different situations such as a topology changes. Therefore, the adoption of Laplacian-based consensus methods is recommended for enhancing the resilience of sensor networks against topology attacks.

#### 5.2 Recommendations

Based on the conclusions drawn from the analysis, several recommendations can be made to further strengthen the resilience of sensor networks against topology attacks. Firstly, it is advisable to integrate Laplacian-based consensus methods into the design and implementation of sensor network protocols to improve fault tolerance and mitigate the effects of attacks. Additionally, further research and development efforts should focus on optimizing the performance of Laplacian gain algorithms to enhance their effectiveness in diverse network environments.

Furthermore, continuous monitoring and evaluation of network performance, especially during attack, are essential to identify vulnerabilities and implement timely countermeasures. Lastly, collaboration between researchers, industry stakeholders, and policymakers is crucial to promote the adoption of robust security measures and standards for safeguarding sensor networks against evolving threats. By implementing these recommendations, sensor networks can be better equipped to withstand topology attacks and ensure reliable operation in various deployment scenarios such as detecting and mitigating other topological attack such as sybil attack.

---

**BIBLIOGRAPHY**

- [1] S.-L. Peng, S. Pal, and L. Huang, *Intelligent Systems Reference Library 174 Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*. 2020.
- [2] M. Frei, J. Kwon, S. Tabaeiaghdaei, M. Wyss, C. Lenzen, and A. Perrig, "G-SINC: Global Synchronization Infrastructure for Network Clocks," *Proc. IEEE Symp. Reliab. Distrib. Syst.*, vol. 2022-Septe, pp. 133–145, 2022, doi: 10.1109/SRDS55811.2022.00021.
- [3] W. Dong and X. Liu, "Robust and secure time-synchronization against Sybil attacks for sensor networks," *IEEE Trans. Ind. Informatics*, vol. 11, no. 6, pp. 1482–1491, 2015, doi: 10.1109/TII.2015.2495147.
- [4] M. Xue, "Evaluation of a Consensus-based Protocol for Clock Synchronization in Wireless Sensor Network," no. 661541223, pp. 1–10, 2017, [Online]. Available: [github.com/bondxue/Time-Sync-Protocol-for-Distributed-System](https://github.com/bondxue/Time-Sync-Protocol-for-Distributed-System), 2017.
- [5] F. Dang, X. K. Sun, K. Bin Liu, Y. F. Xu, and Y. H. Liu, "A Survey on Clock Synchronization in the Industrial Internet," *J. Comput. Sci. Technol.*, vol. 38, no. 1, pp. 146–165, 2023, doi: 10.1007/s11390-023-2908-4.
- [6] F. Sivrikaya and B. Yener, "Time synchronization in sensor networks: A survey," *IEEE Netw.*, vol. 18, no. 4, pp. 45–50, 2004, doi: 10.1109/MNET.2004.1316761.
- [7] P. Ferrari *et al.*, "Evaluation of the impact on industrial applications of NTP Used by IoT devices," *2020 IEEE Int. Work. Metrol. Ind. 4.0 IoT, MetroInd 4.0 IoT 2020 - Proc.*, pp. 223–228, 2020, doi: 10.1109/MetroInd4.0IoT48571.2020.9138290.
- [8] J. Elson, L. Girod, and D. Estrin, "Fine-grained network time synchronization using reference broadcasts," *Oper. Syst. Rev.*, vol. 36, no. Special Issue, pp. 147–163, 2002, doi: 10.1145/844128.844143.
- [9] S. Ganeriwal, R. Kumar, and M. B. Srivastava, "Timing-sync Protocol for Sensor Networks," *Proc. 1st Int. Conf. Embed. networked Sens. Syst. (SenSys '03)*, pp. 138–149, 2003, [Online]. Available: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.58.3367&rep=rep1&type=pdf>.
- [10] L. Schenato and F. Fiorentin, "Average TimeSynch: A consensus-based protocol for clock synchronization in wireless sensor networks," *Automatica*, vol. 47, no. 9, pp. 1878–1886, 2011, doi: 10.1016/j.automatica.2011.06.012.
- [11] J. He, P. Cheng, L. Shi, and J. Chen, "Time Synchronization in WSNs: A Maximum Value Based Consensus Approach," *IEEE Trans. Autom. Control Eur. Control Conf.*, vol. 12, no. 15, pp. 7882–7887, 2011, doi: 10.1109/TAC.2013.2286893.
- [12] S. K. Jha, A. Gupta, and N. Panigrahi, "Security Threat Analysis and Countermeasures on Consensus-Based Time Synchronization Algorithms for Wireless Sensor Network," *SN Comput. Sci.*, vol. 2, no. 5, pp. 1–12, 2021, doi: 10.1007/s42979-021-00796-1.
- [13] J. He, P. Cheng, L. Shi, and J. Chen, "SATS: Secure average-consensus-based time synchronization in wireless sensor networks," *IEEE Trans. Signal Process.*, vol. 61,
-

- 
- no. 24, pp. 6387–6400, 2013, doi: 10.1109/TSP.2013.2286102.
- [14] Y. Wu and X. He, “Finite-Time Consensus-Based Clock Synchronization under Deception Attacks,” *IEEE Access*, vol. 8, pp. 110748–110758, 2020, doi: 10.1109/ACCESS.2020.3002577.
- [15] J. He, J. Chen, P. Cheng, and X. Cao, “Secure time synchronization in wireless sensor networks: A maximum consensus-based approach,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 4, pp. 1055–1065, 2014, doi: 10.1109/TPDS.2013.150.
- [16] Z. Wang, P. Zeng, L. Kong, D. Li, and X. Jin, “Node-identification-based secure time synchronization in industrial wireless sensor networks,” *Sensors (Switzerland)*, vol. 18, no. 8, 2018, doi: 10.3390/s18082718.
- [17] D. J. Huang, W. C. Teng, C. Y. Wang, H. Y. Huang, and J. M. Hellerstein, “Clock skew based node identification in wireless sensor networks,” *GLOBECOM - IEEE Glob. Telecommun. Conf.*, no. December, pp. 1877–1881, 2008, doi: 10.1109/GLOCOM.2008.ECP.363.
- [18] M. K. Maggs, S. G. O’Keefe, and D. V. Thiel, “Consensus clock synchronization for wireless sensor networks,” *IEEE Sens. J.*, vol. 12, no. 6, pp. 2269–2277, 2012, doi: 10.1109/JSEN.2011.2182045.
- [19] M. Kriegleder, R. Oung, and R. D’Andrea, “Asynchronous implementation of a distributed average consensus algorithm,” *IEEE Int. Conf. Intell. Robot. Syst.*, pp. 1836–1841, 2013, doi: 10.1109/IROS.2013.6696598.
- [20] A. S. M. Isira, “Consensus Control of a Class Of Nonlinear Systems,” University of Manchester, 2016.
- [21] K. A. Fajrin, B. Erfianto, and H. H. Nuha, “Analysis of Clock Synchronization with Different Topology in Wireless Sensor Network (WSN),” *Int. Conf. ICT Converg.*, vol. 2023-Augus, pp. 557–562, 2023, doi: 10.1109/ICoICT58202.2023.10262685.
- [22] F. Mkacher, “Optimization of Time Synchronization Techniques on Computer Networks Faten Mkacher To cite this version : HAL Id : tel-02988168 Optimization of Time Synchronization Techniques on Computer Networks,” 2020.
- [23] B. Tibor, “Time synchronization in IoT lighting control,” *Master Thesis Dep. Math. Comput. Sci. Syst. Archit. Netw. Res. Gr.*, 2017, [Online]. Available: file:///Users/kemal/Downloads/Backup Drive Kampus/Main Thesis/6LowPAN/Time\_synchronisation\_in\_IoT\_lighting\_control\_Tibor\_Beke.pdf.
- [24] X. Huan, K. S. Kim, and J. Zhang, “NISA: Node Identification and Spoofing Attack Detection Based on Clock Features and Radio Information for Wireless Sensor Networks,” *IEEE Trans. Commun.*, vol. 69, no. 7, pp. 4691–4703, 2021, doi: 10.1109/TCOMM.2021.3071448.
- [25] C. Benzaid, A. Saiah, and N. Badache, “Secure pairwise broadcast time synchronization in wireless sensor networks,” *2011 Int. Conf. Distrib. Comput. Sens. Syst. Work. DCOSS’11*, 2011, doi: 10.1109/DCOSS.2011.5982217.
- [26] M. Maróti, B. Kusy, G. Simon, and Á. Lédeczi, “The flooding time synchronization protocol,” *SenSys’04 - Proc. Second Int. Conf. Embed. Networked Sens. Syst.*, pp.
-



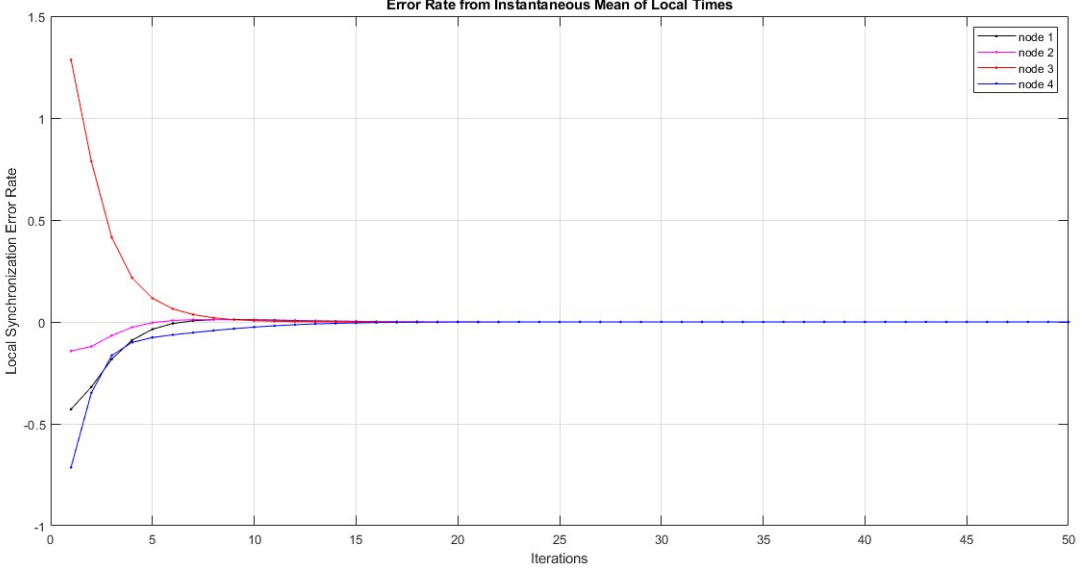
- 39–49, 2004, doi: 10.1145/1031495.1031501.
- [27] Y. Wu, M. Xu, N. Zheng, and X. He, “Attack tolerant finite-time consensus for multi-agent networks,” *IEEE Int. Conf. Control Autom. ICCA*, pp. 1010–1014, 2017, doi: 10.1109/ICCA.2017.8003199.
- [28] G. Werner-Challen, G. Tewari, A. Patel, M. Welsh, and R. Nagpal, “Firefly-Inspired Sensor Network Synchronicity with Realistic Radio Effects Categories and Subject Descriptors,” *3rd Int. Conf. Embed. networked Sens. Syst.*, pp. 142–153, 2005.
- [29] J. He, P. Cheng, L. Shi, J. Chen, and Y. Sun, “Time synchronization in WSNs: A maximum-value-based consensus approach,” *IEEE Trans. Automat. Contr.*, vol. 59, no. 3, pp. 660–675, 2014, doi: 10.1109/TAC.2013.2286893.
- [30] R. Olfati-Saber and R. M. Murray, “Consensus problems in networks of agents with switching topology and time-delays,” *IEEE Trans. Automat. Contr.*, vol. 49, no. 9, pp. 1520–1533, 2004, doi: 10.1109/TAC.2004.834113.
- [31] J. A. Fax and R. M. Murray, “Information flow and cooperative control of vehicle formations,” *IEEE Trans. Automat. Contr.*, vol. 49, no. 9, pp. 1465–1476, 2004, doi: 10.1109/TAC.2004.834433.
- [32] W. Ren and R. W. Beard, “Consensus seeking in multiagent systems under dynamically changing interaction topologies,” *IEEE Trans. Automat. Contr.*, vol. 50, no. 5, pp. 655–661, 2005, doi: 10.1109/TAC.2005.846556.
- [33] L. Moreau, “Stability of multiagent systems with time-dependent communication links,” *IEEE Trans. Automat. Contr.*, vol. 50, no. 2, pp. 169–182, 2005, doi: 10.1109/TAC.2004.841888.
- [34] Y. Niu, T. Yang, Y. Hou, S. Cai, P. Yan, and W. Li, “Consensus tracking-based clock synchronization for the Internet of Things,” *Soft Comput.*, vol. 26, no. 13, pp. 6415–6428, 2022, doi: 10.1007/s00500-022-07165-x.
- [35] N. E. Fard and R. R. Selmic, “Consensus of Multi-agent Reinforcement Learning Systems: The Effect of Immediate Rewards,” *J. Robot. Control*, vol. 3, no. 2, pp. 115–127, 2022, doi: 10.18196/jrc.v3i2.13082.
- [36] N. Panigrahi, “Consensus-based Time Synchronization Algorithms for Wireless Sensor Networks with Topological Optimization Strategies for Performance Improvement,” 2016, [Online]. Available: file:///Users/kemal/Downloads/Consensus-based Time Synchronization Algorithms for Wireless Sensor Networks with Topological Optimization Strategies for Performance Improvement .pdf.
- [37] C. Zhao, J. He, P. Cheng, and J. Chen, “Secure consensus against message manipulation attacks in synchronous networks,” *IFAC Proc. Vol.*, vol. 19, pp. 1182–1187, 2014, doi: 10.3182/20140824-6-za-1003.02753.
- [38] L. M. He, “Time synchronization based on spanning tree for wireless sensor networks,” *2008 Int. Conf. Wirel. Commun. Netw. Mob. Comput. WiCOM 2008*, pp. 4–7, 2008, doi: 10.1109/WiCom.2008.846.

# Appendices

# APPENDIX A

## Experiment Dataset

### Experiment 1

Simulation No.1-a	Fully Connected 4 Nodes – <b>No Attack</b>			GAIN																																																											
Input	<pre>GRAPH = [ 1 1 1 1;           1 1 1 1;           1 1 1 1;           1 1 1 1; ];</pre>		<pre>GRAPH = [ 1 1 1 1;           1 1 1 1;           1 1 1 1;           1 1 1 1; ];</pre>																																																												
Error Rate Graph Plot	 <p>The graph shows the Local Synchronization Error Rate on the y-axis (ranging from -1 to 1.5) against Iterations on the x-axis (ranging from 0 to 50). Four nodes are tracked: node 1 (black), node 2 (magenta), node 3 (red), and node 4 (blue). Node 3 starts with the highest error rate (~1.3) and converges to zero. Node 1 starts at ~-0.4, node 2 at ~-0.1, and node 4 at ~-0.7, all converging to zero by iteration 20.</p>			No Gain																																																											
Results	Raw Data		Convergence Iteration	Global Synchronization Error Rate																																																											
	<table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr><td>12</td><td>0.0071</td><td>0.0051</td><td>0.0016</td><td>-0.0138</td></tr> <tr><td>13</td><td>0.0054</td><td>0.0038</td><td>7.1263e-04</td><td>-0.0099</td></tr> <tr><td>14</td><td>0.0040</td><td>0.0027</td><td>2.7443e-04</td><td>-0.0070</td></tr> <tr><td>15</td><td>0.0029</td><td>0.0019</td><td>6.0957e-05</td><td>-0.0049</td></tr> <tr><td>16</td><td>0.0021</td><td>0.0014</td><td>-3.2874e-05</td><td>-0.0034</td></tr> <tr><td>17</td><td>0.0014</td><td>9.3383e-04</td><td>-6.5794e-05</td><td>-0.0023</td></tr> <tr><td>18</td><td>9.9399e-04</td><td>6.3878e-04</td><td>-6.9791e-05</td><td>-0.0016</td></tr> <tr><td>19</td><td>6.8047e-04</td><td>4.3321e-04</td><td>-6.1682e-05</td><td>-0.0011</td></tr> <tr style="background-color: #e0e0ff;"><td>20</td><td>4.6181e-04</td><td>2.9160e-04</td><td>-4.9874e-05</td><td>-7.0354e-04</td></tr> <tr><td>21</td><td>3.1105e-04</td><td>1.9500e-04</td><td>-3.8235e-05</td><td>-4.6781e-04</td></tr> <tr><td>22</td><td>2.0812e-04</td><td>1.2964e-04</td><td>-2.8285e-05</td><td>-3.0948e-04</td></tr> <tr><td>23</td><td>1.3844e-04</td><td>8.5742e-05</td><td>-2.0394e-05</td><td>-2.0379e-04</td></tr> </tbody> </table>		12	0.0071	0.0051	0.0016	-0.0138	13	0.0054	0.0038	7.1263e-04	-0.0099	14	0.0040	0.0027	2.7443e-04	-0.0070	15	0.0029	0.0019	6.0957e-05	-0.0049	16	0.0021	0.0014	-3.2874e-05	-0.0034	17	0.0014	9.3383e-04	-6.5794e-05	-0.0023	18	9.9399e-04	6.3878e-04	-6.9791e-05	-0.0016	19	6.8047e-04	4.3321e-04	-6.1682e-05	-0.0011	20	4.6181e-04	2.9160e-04	-4.9874e-05	-7.0354e-04	21	3.1105e-04	1.9500e-04	-3.8235e-05	-4.6781e-04	22	2.0812e-04	1.2964e-04	-2.8285e-05	-3.0948e-04	23	1.3844e-04	8.5742e-05	-2.0394e-05	-2.0379e-04	20
12	0.0071	0.0051	0.0016	-0.0138																																																											
13	0.0054	0.0038	7.1263e-04	-0.0099																																																											
14	0.0040	0.0027	2.7443e-04	-0.0070																																																											
15	0.0029	0.0019	6.0957e-05	-0.0049																																																											
16	0.0021	0.0014	-3.2874e-05	-0.0034																																																											
17	0.0014	9.3383e-04	-6.5794e-05	-0.0023																																																											
18	9.9399e-04	6.3878e-04	-6.9791e-05	-0.0016																																																											
19	6.8047e-04	4.3321e-04	-6.1682e-05	-0.0011																																																											
20	4.6181e-04	2.9160e-04	-4.9874e-05	-7.0354e-04																																																											
21	3.1105e-04	1.9500e-04	-3.8235e-05	-4.6781e-04																																																											
22	2.0812e-04	1.2964e-04	-2.8285e-05	-3.0948e-04																																																											
23	1.3844e-04	8.5742e-05	-2.0394e-05	-2.0379e-04																																																											

Simulation No.1-b	Fully Connected 4 Nodes – <b>No Attack</b>			GAIN																																																											
Input	<pre>GRAPH = [ 1 1 1 1;            1 1 1 1;            1 1 1 1;            1 1 1 1; ];</pre>		<pre>GRAPH = [ 1 1 1 1;            1 1 1 1;            1 1 1 1;            1 1 1 1; ];</pre>																																																												
Error Rate Graph Plot	<p>The graph shows the Local Synchronization Error Rate on the y-axis (ranging from -1 to 1.5) against Iterations on the x-axis (ranging from 0 to 50). Four nodes are plotted: node 1 (black), node 2 (magenta), node 3 (red), and node 4 (blue). All nodes start with error rates between -0.5 and 1.3 and converge to zero by iteration 9.</p>			Laplacian Gain																																																											
Results	Raw Data	Convergence Iteration	Global Synchronization Error Rate																																																												
	<table border="1"> <tbody> <tr><td>3</td><td>0.0031</td><td>0.0315</td><td>0.1261</td><td>-0.1608</td></tr> <tr><td>4</td><td>0.0297</td><td>0.0321</td><td>0.0421</td><td>-0.1039</td></tr> <tr><td>5</td><td>0.0193</td><td>0.0171</td><td>0.0130</td><td>-0.0493</td></tr> <tr><td>6</td><td>0.0089</td><td>0.0072</td><td>0.0036</td><td>-0.0196</td></tr> <tr><td>7</td><td>0.0035</td><td>0.0027</td><td>8.9902e-04</td><td>-0.0071</td></tr> <tr><td>8</td><td>0.0013</td><td>9.1462e-04</td><td>2.0509e-04</td><td>-0.0024</td></tr> <tr><td>9</td><td>4.2333e-04</td><td>2.9974e-04</td><td>4.1273e-05</td><td>-7.6434e-04</td></tr> <tr><td>10</td><td>1.3728e-04</td><td>9.4874e-05</td><td>6.5479e-06</td><td>-2.3870e-04</td></tr> <tr><td>11</td><td>4.3162e-05</td><td>2.9249e-05</td><td>3.7502e-07</td><td>-7.2796e-05</td></tr> <tr><td>12</td><td>1.3248e-05</td><td>8.8334e-06</td><td>-3.0211e-07</td><td>-3.1778e-05</td></tr> <tr><td>13</td><td>3.9880e-06</td><td>2.6225e-06</td><td>-1.9470e-07</td><td>-6.4158e-06</td></tr> <tr><td>14</td><td>1.1815e-06</td><td>7.6783e-07</td><td>-8.3544e-08</td><td>-1.8658e-06</td></tr> </tbody> </table>	3	0.0031	0.0315	0.1261	-0.1608	4	0.0297	0.0321	0.0421	-0.1039	5	0.0193	0.0171	0.0130	-0.0493	6	0.0089	0.0072	0.0036	-0.0196	7	0.0035	0.0027	8.9902e-04	-0.0071	8	0.0013	9.1462e-04	2.0509e-04	-0.0024	9	4.2333e-04	2.9974e-04	4.1273e-05	-7.6434e-04	10	1.3728e-04	9.4874e-05	6.5479e-06	-2.3870e-04	11	4.3162e-05	2.9249e-05	3.7502e-07	-7.2796e-05	12	1.3248e-05	8.8334e-06	-3.0211e-07	-3.1778e-05	13	3.9880e-06	2.6225e-06	-1.9470e-07	-6.4158e-06	14	1.1815e-06	7.6783e-07	-8.3544e-08	-1.8658e-06	9	4.1654
3	0.0031	0.0315	0.1261	-0.1608																																																											
4	0.0297	0.0321	0.0421	-0.1039																																																											
5	0.0193	0.0171	0.0130	-0.0493																																																											
6	0.0089	0.0072	0.0036	-0.0196																																																											
7	0.0035	0.0027	8.9902e-04	-0.0071																																																											
8	0.0013	9.1462e-04	2.0509e-04	-0.0024																																																											
9	4.2333e-04	2.9974e-04	4.1273e-05	-7.6434e-04																																																											
10	1.3728e-04	9.4874e-05	6.5479e-06	-2.3870e-04																																																											
11	4.3162e-05	2.9249e-05	3.7502e-07	-7.2796e-05																																																											
12	1.3248e-05	8.8334e-06	-3.0211e-07	-3.1778e-05																																																											
13	3.9880e-06	2.6225e-06	-1.9470e-07	-6.4158e-06																																																											
14	1.1815e-06	7.6783e-07	-8.3544e-08	-1.8658e-06																																																											

**Laplacian Gain Calculation**

Spectrum Laplacian Eigen Value										rho = 2/SSE+LE
No Attack	1.1 e-16	4	4	4						0.25

**Experiment 2**

Simulation No.2-a	<b>Fully Connected 4 Nodes – DoS Attack</b>			<b>GAIN</b>																																																												
Input	$\text{GRAPH} = \begin{bmatrix} 1 & 1 & 1 & 1; \\ 1 & 1 & 1 & 1; \\ 1 & 1 & 1 & 1; \\ 1 & 1 & 1 & 1; \end{bmatrix};$		$\text{GRAPH1} = \begin{bmatrix} 1 & 1 & 0 & 0; \\ 1 & 1 & 1 & 1; \\ 0 & 1 & 1 & 1; \\ 0 & 1 & 1 & 1; \end{bmatrix};$																																																													
Error Rate Graph Plot				<b>No Gain</b>																																																												
Results	Raw Data	Convergence Iteration	Global Synchronization Error Rate																																																													
	<table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr><td>10</td><td>0.0108</td><td>0.0086</td><td>0.0060</td><td>-0.0254</td></tr> <tr><td>11</td><td>0.0119</td><td>0.0058</td><td>0.0022</td><td>-0.0199</td></tr> <tr><td>12</td><td>0.0136</td><td>0.0030</td><td>-6.0098e-04</td><td>-0.0159</td></tr> <tr><td>13</td><td>0.0141</td><td>8.6527e-04</td><td>-0.0022</td><td>-0.0128</td></tr> <tr><td>14</td><td>0.0134</td><td>-4.1417e-04</td><td>-0.0029</td><td>-0.0101</td></tr> <tr><td>15</td><td>0.0118</td><td>-0.0011</td><td>-0.0029</td><td>-0.0079</td></tr> <tr><td>16</td><td>0.0100</td><td>-0.0013</td><td>-0.0027</td><td>-0.0060</td></tr> <tr><td>17</td><td>0.0080</td><td>-0.0013</td><td>-0.0023</td><td>-0.0045</td></tr> <tr><td>18</td><td>0.0063</td><td>-0.0011</td><td>-0.0018</td><td>-0.0033</td></tr> <tr><td>19</td><td>0.0048</td><td>-9.3733e-04</td><td>-0.0014</td><td>-0.0024</td></tr> <tr style="background-color: #e0f0ff;"><td>20</td><td>0.0036</td><td>-7.4790e-04</td><td>-0.0011</td><td>-0.0017</td></tr> <tr><td>21</td><td>0.0026</td><td>-5.7686e-04</td><td>-8.0992e-04</td><td>-0.0012</td></tr> </tbody> </table>	10	0.0108	0.0086	0.0060	-0.0254	11	0.0119	0.0058	0.0022	-0.0199	12	0.0136	0.0030	-6.0098e-04	-0.0159	13	0.0141	8.6527e-04	-0.0022	-0.0128	14	0.0134	-4.1417e-04	-0.0029	-0.0101	15	0.0118	-0.0011	-0.0029	-0.0079	16	0.0100	-0.0013	-0.0027	-0.0060	17	0.0080	-0.0013	-0.0023	-0.0045	18	0.0063	-0.0011	-0.0018	-0.0033	19	0.0048	-9.3733e-04	-0.0014	-0.0024	20	0.0036	-7.4790e-04	-0.0011	-0.0017	21	0.0026	-5.7686e-04	-8.0992e-04	-0.0012	<b>20</b>	<b>6.3263</b>	
10	0.0108	0.0086	0.0060	-0.0254																																																												
11	0.0119	0.0058	0.0022	-0.0199																																																												
12	0.0136	0.0030	-6.0098e-04	-0.0159																																																												
13	0.0141	8.6527e-04	-0.0022	-0.0128																																																												
14	0.0134	-4.1417e-04	-0.0029	-0.0101																																																												
15	0.0118	-0.0011	-0.0029	-0.0079																																																												
16	0.0100	-0.0013	-0.0027	-0.0060																																																												
17	0.0080	-0.0013	-0.0023	-0.0045																																																												
18	0.0063	-0.0011	-0.0018	-0.0033																																																												
19	0.0048	-9.3733e-04	-0.0014	-0.0024																																																												
20	0.0036	-7.4790e-04	-0.0011	-0.0017																																																												
21	0.0026	-5.7686e-04	-8.0992e-04	-0.0012																																																												

Simulation No.2-b	Fully Connected 4 Nodes – DoS Attack			GAIN																																																												
Input	$\text{GRAPH} = \begin{bmatrix} 1 & 1 & 1 & 1; \\ 1 & 1 & 1 & 1; \\ 1 & 1 & 1 & 1; \\ 1 & 1 & 1 & 1; \end{bmatrix};$		$\text{GRAPH1} = \begin{bmatrix} 1 & 1 & 0 & 0; \\ 1 & 1 & 1 & 1; \\ 0 & 1 & 1 & 1; \\ 0 & 1 & 1 & 1; \end{bmatrix};$																																																													
Error Rate Graph Plot				Laplacian Gain																																																												
Results	Raw Data	Convergence Iteration	Global Synchronization Error Rate																																																													
	<table border="1"> <tbody> <tr><td>3</td><td>0.0031</td><td>0.0315</td><td>0.1291</td><td>-0.1606</td></tr> <tr><td>4</td><td>0.0297</td><td>0.0321</td><td>0.0421</td><td>-0.1039</td></tr> <tr><td>5</td><td>0.0193</td><td>0.0171</td><td>0.0130</td><td>-0.0493</td></tr> <tr><td>6</td><td>0.0089</td><td>0.0072</td><td>0.0036</td><td>-0.0196</td></tr> <tr><td>7</td><td>0.0035</td><td>0.0027</td><td>8.9903e-04</td><td>-0.0071</td></tr> <tr><td>8</td><td>0.0013</td><td>9.1462e-04</td><td>2.0509e-04</td><td>-0.0024</td></tr> <tr style="background-color: #e0e0e0;"><td>9</td><td>4.2333e-04</td><td>2.9974e-04</td><td>4.1273e-05</td><td>-7.6434e-04</td></tr> <tr><td>10</td><td>1.3728e-04</td><td>9.4874e-05</td><td>6.5479e-06</td><td>-2.3870e-04</td></tr> <tr><td>11</td><td>4.3162e-05</td><td>2.9249e-05</td><td>3.7902e-07</td><td>-7.2786e-05</td></tr> <tr><td>12</td><td>1.3248e-05</td><td>8.8324e-06</td><td>-3.0211e-07</td><td>-2.1778e-05</td></tr> <tr><td>13</td><td>3.9880e-06</td><td>2.6225e-06</td><td>-1.9470e-07</td><td>-6.4158e-06</td></tr> <tr><td>14</td><td>1.1815e-06</td><td>7.6783e-07</td><td>-8.3544e-08</td><td>-1.8638e-06</td></tr> </tbody> </table>	3	0.0031	0.0315	0.1291	-0.1606	4	0.0297	0.0321	0.0421	-0.1039	5	0.0193	0.0171	0.0130	-0.0493	6	0.0089	0.0072	0.0036	-0.0196	7	0.0035	0.0027	8.9903e-04	-0.0071	8	0.0013	9.1462e-04	2.0509e-04	-0.0024	9	4.2333e-04	2.9974e-04	4.1273e-05	-7.6434e-04	10	1.3728e-04	9.4874e-05	6.5479e-06	-2.3870e-04	11	4.3162e-05	2.9249e-05	3.7902e-07	-7.2786e-05	12	1.3248e-05	8.8324e-06	-3.0211e-07	-2.1778e-05	13	3.9880e-06	2.6225e-06	-1.9470e-07	-6.4158e-06	14	1.1815e-06	7.6783e-07	-8.3544e-08	-1.8638e-06	9	4.1661	
3	0.0031	0.0315	0.1291	-0.1606																																																												
4	0.0297	0.0321	0.0421	-0.1039																																																												
5	0.0193	0.0171	0.0130	-0.0493																																																												
6	0.0089	0.0072	0.0036	-0.0196																																																												
7	0.0035	0.0027	8.9903e-04	-0.0071																																																												
8	0.0013	9.1462e-04	2.0509e-04	-0.0024																																																												
9	4.2333e-04	2.9974e-04	4.1273e-05	-7.6434e-04																																																												
10	1.3728e-04	9.4874e-05	6.5479e-06	-2.3870e-04																																																												
11	4.3162e-05	2.9249e-05	3.7902e-07	-7.2786e-05																																																												
12	1.3248e-05	8.8324e-06	-3.0211e-07	-2.1778e-05																																																												
13	3.9880e-06	2.6225e-06	-1.9470e-07	-6.4158e-06																																																												
14	1.1815e-06	7.6783e-07	-8.3544e-08	-1.8638e-06																																																												

**Laplacian Gain Calculation**

Spectrum Laplacian Eigen Value										rho = 2/SSE+LE
Before Attack	1.1 e-16	4	4	4						0.25
After Attack	1.7 e-16	1	3	4						0.40

**Experiment 3**

Simulation No.3-a	Fully Connected 4 Nodes – <b>Node Destruction Attack</b>			GAIN																																																											
Input	<pre> GRAPH = [ 1 1 1 1;           1 1 1 1;           1 1 1 1;           1 1 1 1; ];         </pre>		<pre> GRAPH1 = [ 1 1 0 1;            1 1 0 1;            0 0 0 0;            1 1 0 1; ];         </pre>																																																												
Error Rate Graph Plot				<b>No Gain</b>																																																											
Results	Raw Data		Convergence Iteration		Global Synchronization Error Rate																																																										
	<table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr><td>18</td><td>0.3346</td><td>0.3342</td><td>-1</td><td>0.3312</td></tr> <tr><td>19</td><td>0.3342</td><td>0.3339</td><td>-1</td><td>0.3319</td></tr> <tr><td>20</td><td>0.3339</td><td>0.3337</td><td>-1</td><td>0.3324</td></tr> <tr><td>21</td><td>0.3337</td><td>0.3336</td><td>-1</td><td>0.3327</td></tr> <tr><td>22</td><td>0.3336</td><td>0.3335</td><td>-1</td><td>0.3329</td></tr> <tr style="background-color: #e0f0ff;"><td>23</td><td>0.3335</td><td>0.3334</td><td>-1</td><td>0.3331</td></tr> <tr><td>24</td><td>0.3334</td><td>0.3334</td><td>-1</td><td>0.3331</td></tr> <tr><td>25</td><td>0.3334</td><td>0.3334</td><td>-1</td><td>0.3332</td></tr> <tr><td>26</td><td>0.3334</td><td>0.3334</td><td>-1</td><td>0.3333</td></tr> <tr><td>27</td><td>0.3334</td><td>0.3334</td><td>-1</td><td>0.3333</td></tr> <tr><td>28</td><td>0.3334</td><td>0.3333</td><td>-1</td><td>0.3333</td></tr> <tr><td>29</td><td>0.3333</td><td>0.3333</td><td>-1</td><td>0.3333</td></tr> </tbody> </table>		18	0.3346	0.3342	-1	0.3312	19	0.3342	0.3339	-1	0.3319	20	0.3339	0.3337	-1	0.3324	21	0.3337	0.3336	-1	0.3327	22	0.3336	0.3335	-1	0.3329	23	0.3335	0.3334	-1	0.3331	24	0.3334	0.3334	-1	0.3331	25	0.3334	0.3334	-1	0.3332	26	0.3334	0.3334	-1	0.3333	27	0.3334	0.3334	-1	0.3333	28	0.3334	0.3333	-1	0.3333	29	0.3333	0.3333	-1	0.3333	23
18	0.3346	0.3342	-1	0.3312																																																											
19	0.3342	0.3339	-1	0.3319																																																											
20	0.3339	0.3337	-1	0.3324																																																											
21	0.3337	0.3336	-1	0.3327																																																											
22	0.3336	0.3335	-1	0.3329																																																											
23	0.3335	0.3334	-1	0.3331																																																											
24	0.3334	0.3334	-1	0.3331																																																											
25	0.3334	0.3334	-1	0.3332																																																											
26	0.3334	0.3334	-1	0.3333																																																											
27	0.3334	0.3334	-1	0.3333																																																											
28	0.3334	0.3333	-1	0.3333																																																											
29	0.3333	0.3333	-1	0.3333																																																											

Simulation No.3-b	Fully Connected 4 Nodes – <b>Node Destruction Attack</b>			GAIN																																																											
Input	<pre>GRAPH = [ 1 1 1 1;           1 1 1 1;           1 1 1 1;           1 1 1 1; ];</pre>		<pre>GRAPH1 = [ 1 1 0 1;            1 1 0 1;            0 0 0 0;            1 1 0 1; ];</pre>																																																												
Error Rate Graph Plot				Laplacian Gain																																																											
Results	<p>Raw Data</p> <table border="1"> <tr><td>5</td><td>0.0193</td><td>0.0171</td><td>0.0130</td><td>-0.0493</td></tr> <tr><td>6</td><td>0.0089</td><td>0.0072</td><td>0.0036</td><td>-0.0196</td></tr> <tr><td>7</td><td>0.0035</td><td>0.0027</td><td>8.9902e-04</td><td>-0.0071</td></tr> <tr><td>8</td><td>0.0013</td><td>9.1462e-04</td><td>2.0509e-04</td><td>-0.0024</td></tr> <tr><td>9</td><td>4.2333e-04</td><td>2.9974e-04</td><td>4.1273e-05</td><td>-7.6434e-04</td></tr> <tr><td>10</td><td>1.3728e-04</td><td>9.4874e-05</td><td>6.5479e-06</td><td>-2.3870e-04</td></tr> <tr><td>11</td><td>0.3335</td><td>0.3334</td><td>-1</td><td>0.3331</td></tr> <tr><td>12</td><td>0.3334</td><td>0.3334</td><td>-1</td><td>0.3332</td></tr> <tr><td>13</td><td>0.3334</td><td>0.3334</td><td>-1</td><td>0.3332</td></tr> <tr><td>14</td><td>0.3334</td><td>0.3334</td><td>-1</td><td>0.3333</td></tr> <tr><td>15</td><td>0.3334</td><td>0.3333</td><td>-1</td><td>0.3333</td></tr> <tr><td>16</td><td>0.3333</td><td>0.3333</td><td>-1</td><td>0.3333</td></tr> </table>	5	0.0193		0.0171	0.0130	-0.0493	6	0.0089	0.0072	0.0036	-0.0196	7	0.0035	0.0027	8.9902e-04	-0.0071	8	0.0013	9.1462e-04	2.0509e-04	-0.0024	9	4.2333e-04	2.9974e-04	4.1273e-05	-7.6434e-04	10	1.3728e-04	9.4874e-05	6.5479e-06	-2.3870e-04	11	0.3335	0.3334	-1	0.3331	12	0.3334	0.3334	-1	0.3332	13	0.3334	0.3334	-1	0.3332	14	0.3334	0.3334	-1	0.3333	15	0.3334	0.3333	-1	0.3333	16	0.3333	0.3333	-1	0.3333	Convergence Iteration
5	0.0193	0.0171	0.0130	-0.0493																																																											
6	0.0089	0.0072	0.0036	-0.0196																																																											
7	0.0035	0.0027	8.9902e-04	-0.0071																																																											
8	0.0013	9.1462e-04	2.0509e-04	-0.0024																																																											
9	4.2333e-04	2.9974e-04	4.1273e-05	-7.6434e-04																																																											
10	1.3728e-04	9.4874e-05	6.5479e-06	-2.3870e-04																																																											
11	0.3335	0.3334	-1	0.3331																																																											
12	0.3334	0.3334	-1	0.3332																																																											
13	0.3334	0.3334	-1	0.3332																																																											
14	0.3334	0.3334	-1	0.3333																																																											
15	0.3334	0.3333	-1	0.3333																																																											
16	0.3333	0.3333	-1	0.3333																																																											
			9	84.1652																																																											

**Laplacian Gain Calculation**

Spectrum Laplacian Eigen Value									rho = 2/SSE+LE
Before Attack	1.1 e-16	4	4	4					0.25
After Attack	-1.25 e-16	1.8 e-16	3	3					0.33



**Experiment 4**

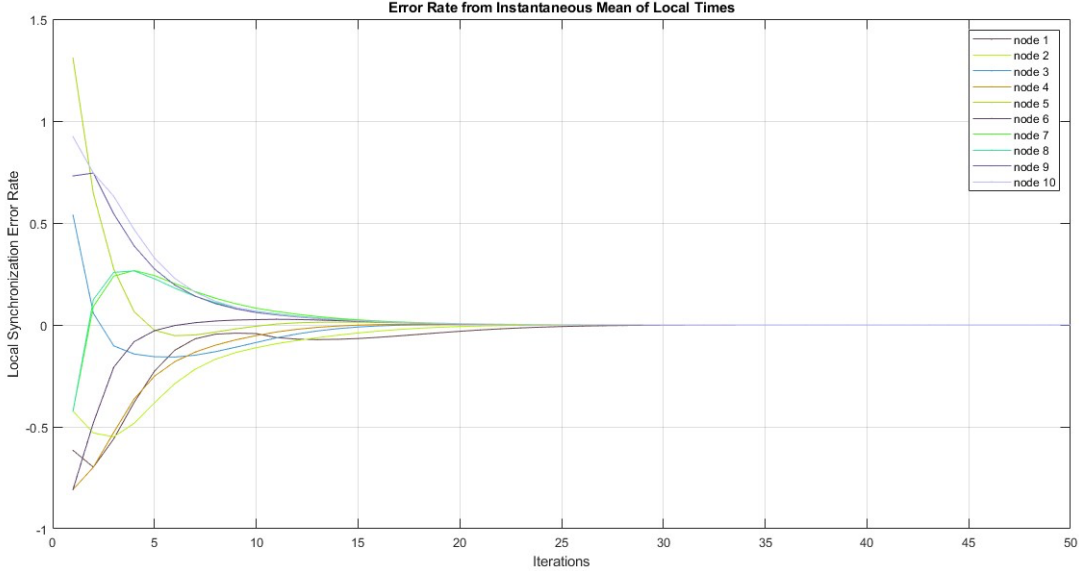
Simulation No.4-a	Fully Connected 10 Nodes – No Attack			GAIN																																																																																																																																			
Input	<pre> GRAPH = [ ... 0 1 1 1 0 0 0 0 0 0; 1 0 1 1 0 0 0 0 0 0; 1 1 0 0 1 1 0 0 0 0; 1 1 0 0 1 1 0 0 0 0; 0 0 1 1 0 0 1 1 0 0; 0 0 1 1 0 0 1 1 0 0; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 0 0 1 1 0 1; 0 0 0 0 0 0 1 1 0 1; 0 0 0 0 0 0 1 1 0 1; ];                     </pre>	<pre> GRAPH = [ ... 0 1 1 1 0 0 0 0 0 0; 1 0 1 1 0 0 0 0 0 0; 1 1 0 0 1 1 0 0 0 0; 1 1 0 0 1 1 0 0 0 0; 0 0 1 1 0 0 1 1 0 0; 0 0 1 1 0 0 1 1 0 0; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 0 0 1 1 0 1; 0 0 0 0 0 0 1 1 0 1; 0 0 0 0 0 0 1 1 0 1; ];                     </pre>																																																																																																																																					
Error Rate Graph Plot				No Gain																																																																																																																																			
Results	Raw Data	Convergence Iteration	Global Synchronization Error Rate																																																																																																																																				
	<table border="1"> <tbody> <tr><td>16</td><td>-0.0289</td><td>-0.0338</td><td>-0.0085</td><td>-0.0020</td><td>0.0083</td><td>0.0114</td><td>0.0158</td><td>0.0133</td><td>0.0121</td><td>0.0123</td></tr> <tr><td>17</td><td>-0.0231</td><td>-0.0259</td><td>-0.0050</td><td>-4.5290e-04</td><td>0.0068</td><td>0.0088</td><td>0.0114</td><td>0.0097</td><td>0.0089</td><td>0.0090</td></tr> <tr><td>18</td><td>-0.0180</td><td>-0.0195</td><td>-0.0027</td><td>3.8457e-04</td><td>0.0053</td><td>0.0066</td><td>0.0081</td><td>0.0069</td><td>0.0064</td><td>0.0064</td></tr> <tr><td>19</td><td>-0.0136</td><td>-0.0144</td><td>-0.0013</td><td>7.6279e-04</td><td>0.0040</td><td>0.0048</td><td>0.0057</td><td>0.0049</td><td>0.0045</td><td>0.0045</td></tr> <tr><td>20</td><td>-0.0100</td><td>-0.0104</td><td>-4.9254e-04</td><td>8.6883e-04</td><td>0.0030</td><td>0.0035</td><td>0.0040</td><td>0.0034</td><td>0.0031</td><td>0.0032</td></tr> <tr><td>21</td><td>-0.0072</td><td>-0.0074</td><td>-6.4067e-05</td><td>8.2756e-04</td><td>0.0021</td><td>0.0024</td><td>0.0027</td><td>0.0023</td><td>0.0021</td><td>0.0021</td></tr> <tr><td>22</td><td>-0.0051</td><td>-0.0052</td><td>1.4010e-04</td><td>7.1794e-04</td><td>0.0015</td><td>0.0017</td><td>0.0018</td><td>0.0015</td><td>0.0014</td><td>0.0014</td></tr> <tr><td>23</td><td>-0.0035</td><td>-0.0035</td><td>2.1603e-04</td><td>5.8679e-04</td><td>0.0010</td><td>0.0011</td><td>0.0012</td><td>0.0010</td><td>9.3228e-04</td><td>9.3770e-04</td></tr> <tr><td>24</td><td>-0.0024</td><td>-0.0024</td><td>2.2394e-04</td><td>4.5956e-04</td><td>6.8162e-04</td><td>7.5632e-04</td><td>7.6225e-04</td><td>6.4989e-04</td><td>5.9558e-04</td><td>5.9884e-04</td></tr> <tr><td>25</td><td>-0.0016</td><td>-0.0016</td><td>1.9991e-04</td><td>3.4827e-04</td><td>4.4583e-04</td><td>4.9131e-04</td><td>4.8026e-04</td><td>4.0597e-04</td><td>3.7004e-04</td><td>3.7200e-04</td></tr> <tr><td>26</td><td>-0.0010</td><td>-0.0010</td><td>1.6440e-04</td><td>2.5695e-04</td><td>2.8428e-04</td><td>3.1181e-04</td><td>2.9472e-04</td><td>2.4581e-04</td><td>2.2214e-04</td><td>2.2332e-04</td></tr> <tr><td>27</td><td>-6.2858e-04</td><td>-6.2708e-04</td><td>1.2810e-04</td><td>1.8530e-04</td><td>1.7607e-04</td><td>1.8265e-04</td><td>1.7502e-04</td><td>1.4295e-04</td><td>1.2742e-04</td><td>1.2813e-04</td></tr> </tbody> </table>	16	-0.0289	-0.0338	-0.0085	-0.0020	0.0083	0.0114	0.0158	0.0133	0.0121	0.0123	17	-0.0231	-0.0259	-0.0050	-4.5290e-04	0.0068	0.0088	0.0114	0.0097	0.0089	0.0090	18	-0.0180	-0.0195	-0.0027	3.8457e-04	0.0053	0.0066	0.0081	0.0069	0.0064	0.0064	19	-0.0136	-0.0144	-0.0013	7.6279e-04	0.0040	0.0048	0.0057	0.0049	0.0045	0.0045	20	-0.0100	-0.0104	-4.9254e-04	8.6883e-04	0.0030	0.0035	0.0040	0.0034	0.0031	0.0032	21	-0.0072	-0.0074	-6.4067e-05	8.2756e-04	0.0021	0.0024	0.0027	0.0023	0.0021	0.0021	22	-0.0051	-0.0052	1.4010e-04	7.1794e-04	0.0015	0.0017	0.0018	0.0015	0.0014	0.0014	23	-0.0035	-0.0035	2.1603e-04	5.8679e-04	0.0010	0.0011	0.0012	0.0010	9.3228e-04	9.3770e-04	24	-0.0024	-0.0024	2.2394e-04	4.5956e-04	6.8162e-04	7.5632e-04	7.6225e-04	6.4989e-04	5.9558e-04	5.9884e-04	25	-0.0016	-0.0016	1.9991e-04	3.4827e-04	4.4583e-04	4.9131e-04	4.8026e-04	4.0597e-04	3.7004e-04	3.7200e-04	26	-0.0010	-0.0010	1.6440e-04	2.5695e-04	2.8428e-04	3.1181e-04	2.9472e-04	2.4581e-04	2.2214e-04	2.2332e-04	27	-6.2858e-04	-6.2708e-04	1.2810e-04	1.8530e-04	1.7607e-04	1.8265e-04	1.7502e-04	1.4295e-04	1.2742e-04	1.2813e-04	25	28.8218
16	-0.0289	-0.0338	-0.0085	-0.0020	0.0083	0.0114	0.0158	0.0133	0.0121	0.0123																																																																																																																													
17	-0.0231	-0.0259	-0.0050	-4.5290e-04	0.0068	0.0088	0.0114	0.0097	0.0089	0.0090																																																																																																																													
18	-0.0180	-0.0195	-0.0027	3.8457e-04	0.0053	0.0066	0.0081	0.0069	0.0064	0.0064																																																																																																																													
19	-0.0136	-0.0144	-0.0013	7.6279e-04	0.0040	0.0048	0.0057	0.0049	0.0045	0.0045																																																																																																																													
20	-0.0100	-0.0104	-4.9254e-04	8.6883e-04	0.0030	0.0035	0.0040	0.0034	0.0031	0.0032																																																																																																																													
21	-0.0072	-0.0074	-6.4067e-05	8.2756e-04	0.0021	0.0024	0.0027	0.0023	0.0021	0.0021																																																																																																																													
22	-0.0051	-0.0052	1.4010e-04	7.1794e-04	0.0015	0.0017	0.0018	0.0015	0.0014	0.0014																																																																																																																													
23	-0.0035	-0.0035	2.1603e-04	5.8679e-04	0.0010	0.0011	0.0012	0.0010	9.3228e-04	9.3770e-04																																																																																																																													
24	-0.0024	-0.0024	2.2394e-04	4.5956e-04	6.8162e-04	7.5632e-04	7.6225e-04	6.4989e-04	5.9558e-04	5.9884e-04																																																																																																																													
25	-0.0016	-0.0016	1.9991e-04	3.4827e-04	4.4583e-04	4.9131e-04	4.8026e-04	4.0597e-04	3.7004e-04	3.7200e-04																																																																																																																													
26	-0.0010	-0.0010	1.6440e-04	2.5695e-04	2.8428e-04	3.1181e-04	2.9472e-04	2.4581e-04	2.2214e-04	2.2332e-04																																																																																																																													
27	-6.2858e-04	-6.2708e-04	1.2810e-04	1.8530e-04	1.7607e-04	1.8265e-04	1.7502e-04	1.4295e-04	1.2742e-04	1.2813e-04																																																																																																																													

Simulation No.4-b	Fully Connected 10 Nodes – No Attack			GAIN																																																																																																																																				
Input	<pre> GRAPH = [ ... 0 1 1 1 0 0 0 0 0 0; 1 0 1 1 0 0 0 0 0 0; 1 1 0 0 1 1 0 0 0 0; 1 1 0 0 1 1 0 0 0 0; 0 0 1 1 0 0 1 1 0 0; 0 0 1 1 0 0 1 1 0 0; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 0 0 1 1 0 1; 0 0 0 0 0 0 1 1 0 1; 0 0 0 0 0 0 1 1 1 0; ];</pre>	<pre> GRAPH = [ ... 0 1 1 1 0 0 0 0 0 0; 1 0 1 1 0 0 0 0 0 0; 1 1 0 0 1 1 0 0 0 0; 1 1 0 0 1 1 0 0 0 0; 0 0 1 1 0 0 1 1 0 0; 0 0 1 1 0 0 1 1 0 0; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 0 0 1 1 0 1; 0 0 0 0 0 0 1 1 0 1; 0 0 0 0 0 0 1 1 1 0; ];</pre>																																																																																																																																						
Error Rate Graph Plot	<p><b>Error Rate from Instantaneous Mean of Local Times</b></p> <p>Local Synchronization Error Rate vs Iterations</p> <p>Legend: node 1 (blue), node 2 (orange), node 3 (green), node 4 (red), node 5 (purple), node 6 (brown), node 7 (pink), node 8 (grey), node 9 (olive), node 10 (cyan)</p>			Laplacian Gain																																																																																																																																				
Results	Raw Data	Convergence Iteration	Global Synchronization Error Rate																																																																																																																																					
	<table border="1"> <tbody> <tr><td>5</td><td>-0.0447</td><td>-0.1829</td><td>-0.2204</td><td>-0.1270</td><td>0.0845</td><td>0.1394</td><td>0.0762</td><td>0.0549</td><td>0.0381</td><td>0.1820</td></tr> <tr><td>6</td><td>-0.1763</td><td>-0.1998</td><td>-0.0233</td><td>0.0192</td><td>0.0045</td><td>0.0278</td><td>0.1166</td><td>0.1066</td><td>0.1047</td><td>0.0201</td></tr> <tr><td>7</td><td>-0.0841</td><td>-0.0814</td><td>-0.0275</td><td>-0.0885</td><td>0.0533</td><td>0.0568</td><td>0.0146</td><td>0.0112</td><td>0.0082</td><td>0.0576</td></tr> <tr><td>8</td><td>-0.0631</td><td>-0.0570</td><td>0.0150</td><td>0.0201</td><td>9.0856e-04</td><td>0.0028</td><td>0.0283</td><td>0.0269</td><td>0.0269</td><td>-9.8425e-04</td></tr> <tr><td>9</td><td>-0.0135</td><td>-0.0108</td><td>-0.0035</td><td>-0.0017</td><td>0.0128</td><td>0.0126</td><td>-0.0024</td><td>-0.0028</td><td>-0.0033</td><td>0.0124</td></tr> <tr><td>10</td><td>-0.0099</td><td>-0.0087</td><td>0.0055</td><td>0.0057</td><td>-0.0027</td><td>-0.0025</td><td>0.0054</td><td>0.0052</td><td>0.0053</td><td>-0.0034</td></tr> <tr><td>11</td><td>9.4539e-04</td><td>0.0012</td><td>-0.0015</td><td>-0.0014</td><td>0.0026</td><td>0.0025</td><td>-0.0022</td><td>-0.0022</td><td>-0.0023</td><td>0.0025</td></tr> <tr><td>12</td><td>-0.0011</td><td>-9.9125e-04</td><td>0.0014</td><td>0.0013</td><td>-0.0013</td><td>-0.0013</td><td>0.0011</td><td>0.0011</td><td>0.0011</td><td>-0.0014</td></tr> <tr><td>13</td><td>9.1389e-04</td><td>8.8866e-04</td><td>-5.9418e-04</td><td>-5.0233e-04</td><td>5.9714e-04</td><td>5.7450e-04</td><td>-7.8516e-04</td><td>-7.8736e-04</td><td>-0.0203e-04</td><td>5.9147e-04</td></tr> <tr><td>14</td><td>-1.5981e-04</td><td>-1.6961e-04</td><td>3.5297e-04</td><td>3.3952e-04</td><td>-4.1991e-04</td><td>-4.1244e-04</td><td>3.0308e-04</td><td>3.0064e-04</td><td>3.0653e-04</td><td>-4.4096e-04</td></tr> <tr><td>15</td><td>2.8241e-04</td><td>2.7074e-04</td><td>-1.9038e-04</td><td>-1.8985e-04</td><td>1.6888e-04</td><td>1.6405e-04</td><td>-2.3453e-04</td><td>-2.2440e-04</td><td>-2.2771e-04</td><td>1.7080e-04</td></tr> <tr><td>16</td><td>-5.5257e-05</td><td>-5.8116e-05</td><td>9.6641e-05</td><td>9.3965e-05</td><td>-1.1607e-04</td><td>-1.1417e-04</td><td>9.0669e-05</td><td>9.0301e-05</td><td>9.1749e-05</td><td>-1.1971e-04</td></tr> </tbody> </table>	5	-0.0447	-0.1829	-0.2204	-0.1270	0.0845	0.1394	0.0762	0.0549	0.0381	0.1820	6	-0.1763	-0.1998	-0.0233	0.0192	0.0045	0.0278	0.1166	0.1066	0.1047	0.0201	7	-0.0841	-0.0814	-0.0275	-0.0885	0.0533	0.0568	0.0146	0.0112	0.0082	0.0576	8	-0.0631	-0.0570	0.0150	0.0201	9.0856e-04	0.0028	0.0283	0.0269	0.0269	-9.8425e-04	9	-0.0135	-0.0108	-0.0035	-0.0017	0.0128	0.0126	-0.0024	-0.0028	-0.0033	0.0124	10	-0.0099	-0.0087	0.0055	0.0057	-0.0027	-0.0025	0.0054	0.0052	0.0053	-0.0034	11	9.4539e-04	0.0012	-0.0015	-0.0014	0.0026	0.0025	-0.0022	-0.0022	-0.0023	0.0025	12	-0.0011	-9.9125e-04	0.0014	0.0013	-0.0013	-0.0013	0.0011	0.0011	0.0011	-0.0014	13	9.1389e-04	8.8866e-04	-5.9418e-04	-5.0233e-04	5.9714e-04	5.7450e-04	-7.8516e-04	-7.8736e-04	-0.0203e-04	5.9147e-04	14	-1.5981e-04	-1.6961e-04	3.5297e-04	3.3952e-04	-4.1991e-04	-4.1244e-04	3.0308e-04	3.0064e-04	3.0653e-04	-4.4096e-04	15	2.8241e-04	2.7074e-04	-1.9038e-04	-1.8985e-04	1.6888e-04	1.6405e-04	-2.3453e-04	-2.2440e-04	-2.2771e-04	1.7080e-04	16	-5.5257e-05	-5.8116e-05	9.6641e-05	9.3965e-05	-1.1607e-04	-1.1417e-04	9.0669e-05	9.0301e-05	9.1749e-05	-1.1971e-04	13	20.8546	
5	-0.0447	-0.1829	-0.2204	-0.1270	0.0845	0.1394	0.0762	0.0549	0.0381	0.1820																																																																																																																														
6	-0.1763	-0.1998	-0.0233	0.0192	0.0045	0.0278	0.1166	0.1066	0.1047	0.0201																																																																																																																														
7	-0.0841	-0.0814	-0.0275	-0.0885	0.0533	0.0568	0.0146	0.0112	0.0082	0.0576																																																																																																																														
8	-0.0631	-0.0570	0.0150	0.0201	9.0856e-04	0.0028	0.0283	0.0269	0.0269	-9.8425e-04																																																																																																																														
9	-0.0135	-0.0108	-0.0035	-0.0017	0.0128	0.0126	-0.0024	-0.0028	-0.0033	0.0124																																																																																																																														
10	-0.0099	-0.0087	0.0055	0.0057	-0.0027	-0.0025	0.0054	0.0052	0.0053	-0.0034																																																																																																																														
11	9.4539e-04	0.0012	-0.0015	-0.0014	0.0026	0.0025	-0.0022	-0.0022	-0.0023	0.0025																																																																																																																														
12	-0.0011	-9.9125e-04	0.0014	0.0013	-0.0013	-0.0013	0.0011	0.0011	0.0011	-0.0014																																																																																																																														
13	9.1389e-04	8.8866e-04	-5.9418e-04	-5.0233e-04	5.9714e-04	5.7450e-04	-7.8516e-04	-7.8736e-04	-0.0203e-04	5.9147e-04																																																																																																																														
14	-1.5981e-04	-1.6961e-04	3.5297e-04	3.3952e-04	-4.1991e-04	-4.1244e-04	3.0308e-04	3.0064e-04	3.0653e-04	-4.4096e-04																																																																																																																														
15	2.8241e-04	2.7074e-04	-1.9038e-04	-1.8985e-04	1.6888e-04	1.6405e-04	-2.3453e-04	-2.2440e-04	-2.2771e-04	1.7080e-04																																																																																																																														
16	-5.5257e-05	-5.8116e-05	9.6641e-05	9.3965e-05	-1.1607e-04	-1.1417e-04	9.0669e-05	9.0301e-05	9.1749e-05	-1.1971e-04																																																																																																																														

**Laplacian Gain Calculation**

Spectrum Laplacian Eigen Value										rho = 2/SSE+LE	
No Attack	1.5 e-16	0.76	2.76	4	4	4	4	4	5.23	7.23	0.25

**Experiment 5**

Simulation No.5-a	Fully Connected 10 Nodes – DoS Attack			GAIN																																																																																																																																		
Input	<pre> GRAPH = [ ... 0 1 1 1 0 0 0 0 0 0; 1 0 1 1 0 0 0 0 0 0; 1 1 0 0 1 1 0 0 0 0; 1 1 0 0 1 1 0 0 0 0; 0 0 1 1 0 0 1 1 0 0; 0 0 1 1 0 0 1 1 0 0; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 0 0 1 1 1 0; ];                     </pre>	<pre> GRAPH1 = [ ... 0 1 0 0 0 0 0 0 0 0; 1 0 1 1 0 0 0 0 0 0; 0 1 0 0 1 1 0 0 0 0; 0 1 0 0 1 1 0 0 0 0; 0 0 1 1 0 0 1 1 0 0; 0 0 1 1 0 0 1 1 0 0; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 0 0 1 1 1 0; ];                     </pre>	No Gain																																																																																																																																			
Error Rate Graph Plot					No Gain																																																																																																																																	
Results	Raw Data	Convergence Iteration	Global Synchronization Error Rate																																																																																																																																			
	<table border="1"> <tbody> <tr><td>20</td><td>-0.0313</td><td>-0.0081</td><td>0.0019</td><td>0.0032</td><td>0.0053</td><td>0.0058</td><td>0.0063</td><td>0.0058</td><td>0.0055</td><td>0.0055</td></tr> <tr><td>21</td><td>-0.0248</td><td>-0.0055</td><td>0.0019</td><td>0.0028</td><td>0.0041</td><td>0.0044</td><td>0.0047</td><td>0.0043</td><td>0.0041</td><td>0.0041</td></tr> <tr><td>22</td><td>-0.0193</td><td>-0.0036</td><td>0.0017</td><td>0.0023</td><td>0.0031</td><td>0.0033</td><td>0.0034</td><td>0.0031</td><td>0.0030</td><td>0.0030</td></tr> <tr><td>23</td><td>-0.0147</td><td>-0.0023</td><td>0.0015</td><td>0.0018</td><td>0.0023</td><td>0.0024</td><td>0.0024</td><td>0.0023</td><td>0.0022</td><td>0.0022</td></tr> <tr><td>24</td><td>-0.0110</td><td>-0.0014</td><td>0.0012</td><td>0.0014</td><td>0.0016</td><td>0.0017</td><td>0.0017</td><td>0.0016</td><td>0.0016</td><td>0.0016</td></tr> <tr><td>25</td><td>-0.0081</td><td>-8.3632e-04</td><td>9.2237e-04</td><td>0.0011</td><td>0.0012</td><td>0.0012</td><td>0.0012</td><td>0.0011</td><td>0.0011</td><td>0.0011</td></tr> <tr><td>26</td><td>-0.0058</td><td>-4.6648e-04</td><td>6.9950e-04</td><td>7.9210e-04</td><td>8.1945e-04</td><td>8.4700e-04</td><td>8.2990e-04</td><td>7.8095e-04</td><td>7.5728e-04</td><td>7.5846e-04</td></tr> <tr><td>27</td><td>-0.0041</td><td>-2.3790e-04</td><td>5.1758e-04</td><td>5.7479e-04</td><td>5.6556e-04</td><td>5.8215e-04</td><td>5.6451e-04</td><td>5.3242e-04</td><td>5.1689e-04</td><td>5.1760e-04</td></tr> <tr><td>28</td><td>-0.0029</td><td>-1.0235e-04</td><td>3.7478e-04</td><td>4.0980e-04</td><td>3.8408e-04</td><td>3.9401e-04</td><td>3.7830e-04</td><td>3.5733e-04</td><td>3.4718e-04</td><td>3.4761e-04</td></tr> <tr><td>29</td><td>-0.0020</td><td>-2.6301e-05</td><td>2.6612e-04</td><td>2.8734e-04</td><td>2.5649e-04</td><td>2.6240e-04</td><td>2.4945e-04</td><td>2.3580e-04</td><td>2.2919e-04</td><td>2.2945e-04</td></tr> <tr><td>30</td><td>-0.0013</td><td>1.2932e-05</td><td>1.8554e-04</td><td>1.9826e-04</td><td>1.6825e-04</td><td>1.7175e-04</td><td>1.6158e-04</td><td>1.5272e-04</td><td>1.4843e-04</td><td>1.4858e-04</td></tr> <tr><td>31</td><td>-8.9808e-04</td><td>3.0286e-05</td><td>1.2711e-04</td><td>1.3465e-04</td><td>1.0822e-04</td><td>1.1028e-04</td><td>1.0255e-04</td><td>9.6816e-05</td><td>9.4038e-05</td><td>9.4130e-05</td></tr> </tbody> </table>	20	-0.0313			-0.0081	0.0019	0.0032	0.0053	0.0058	0.0063	0.0058	0.0055	0.0055	21	-0.0248	-0.0055	0.0019	0.0028	0.0041	0.0044	0.0047	0.0043	0.0041	0.0041	22	-0.0193	-0.0036	0.0017	0.0023	0.0031	0.0033	0.0034	0.0031	0.0030	0.0030	23	-0.0147	-0.0023	0.0015	0.0018	0.0023	0.0024	0.0024	0.0023	0.0022	0.0022	24	-0.0110	-0.0014	0.0012	0.0014	0.0016	0.0017	0.0017	0.0016	0.0016	0.0016	25	-0.0081	-8.3632e-04	9.2237e-04	0.0011	0.0012	0.0012	0.0012	0.0011	0.0011	0.0011	26	-0.0058	-4.6648e-04	6.9950e-04	7.9210e-04	8.1945e-04	8.4700e-04	8.2990e-04	7.8095e-04	7.5728e-04	7.5846e-04	27	-0.0041	-2.3790e-04	5.1758e-04	5.7479e-04	5.6556e-04	5.8215e-04	5.6451e-04	5.3242e-04	5.1689e-04	5.1760e-04	28	-0.0029	-1.0235e-04	3.7478e-04	4.0980e-04	3.8408e-04	3.9401e-04	3.7830e-04	3.5733e-04	3.4718e-04	3.4761e-04	29	-0.0020	-2.6301e-05	2.6612e-04	2.8734e-04	2.5649e-04	2.6240e-04	2.4945e-04	2.3580e-04	2.2919e-04	2.2945e-04	30	-0.0013	1.2932e-05	1.8554e-04	1.9826e-04	1.6825e-04	1.7175e-04	1.6158e-04	1.5272e-04	1.4843e-04	1.4858e-04	31	-8.9808e-04	3.0286e-05	1.2711e-04	1.3465e-04	1.0822e-04	1.1028e-04	1.0255e-04	9.6816e-05	9.4038e-05
20	-0.0313	-0.0081	0.0019	0.0032	0.0053	0.0058	0.0063	0.0058	0.0055	0.0055																																																																																																																												
21	-0.0248	-0.0055	0.0019	0.0028	0.0041	0.0044	0.0047	0.0043	0.0041	0.0041																																																																																																																												
22	-0.0193	-0.0036	0.0017	0.0023	0.0031	0.0033	0.0034	0.0031	0.0030	0.0030																																																																																																																												
23	-0.0147	-0.0023	0.0015	0.0018	0.0023	0.0024	0.0024	0.0023	0.0022	0.0022																																																																																																																												
24	-0.0110	-0.0014	0.0012	0.0014	0.0016	0.0017	0.0017	0.0016	0.0016	0.0016																																																																																																																												
25	-0.0081	-8.3632e-04	9.2237e-04	0.0011	0.0012	0.0012	0.0012	0.0011	0.0011	0.0011																																																																																																																												
26	-0.0058	-4.6648e-04	6.9950e-04	7.9210e-04	8.1945e-04	8.4700e-04	8.2990e-04	7.8095e-04	7.5728e-04	7.5846e-04																																																																																																																												
27	-0.0041	-2.3790e-04	5.1758e-04	5.7479e-04	5.6556e-04	5.8215e-04	5.6451e-04	5.3242e-04	5.1689e-04	5.1760e-04																																																																																																																												
28	-0.0029	-1.0235e-04	3.7478e-04	4.0980e-04	3.8408e-04	3.9401e-04	3.7830e-04	3.5733e-04	3.4718e-04	3.4761e-04																																																																																																																												
29	-0.0020	-2.6301e-05	2.6612e-04	2.8734e-04	2.5649e-04	2.6240e-04	2.4945e-04	2.3580e-04	2.2919e-04	2.2945e-04																																																																																																																												
30	-0.0013	1.2932e-05	1.8554e-04	1.9826e-04	1.6825e-04	1.7175e-04	1.6158e-04	1.5272e-04	1.4843e-04	1.4858e-04																																																																																																																												
31	-8.9808e-04	3.0286e-05	1.2711e-04	1.3465e-04	1.0822e-04	1.1028e-04	1.0255e-04	9.6816e-05	9.4038e-05	9.4130e-05																																																																																																																												

Simulation No.5-b	Fully Connected 10 Nodes – DoS Attack			GAIN																																																																																																																																			
Input	<pre> GRAPH = [ ... 0 1 1 1 0 0 0 0 0 0; 1 0 1 1 0 0 0 0 0 0; 1 1 0 0 1 1 0 0 0 0; 1 1 0 0 1 1 0 0 0 0; 0 0 1 1 0 0 1 1 0 0; 0 0 1 1 0 0 1 1 0 0; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 0 0 1 1 0 1; 0 0 0 0 0 0 1 1 0 1; 0 0 0 0 0 0 1 1 1 0; ];</pre>	<pre> GRAPH1 = [ ... 0 1 0 0 0 0 0 0 0 0; 1 0 1 1 0 0 0 0 0 0; 0 1 0 0 1 1 0 0 0 0; 0 1 0 0 1 1 0 0 0 0; 0 0 1 1 0 0 1 1 0 0; 0 0 1 1 0 0 1 1 0 0; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 0 0 1 1 1 0; ];</pre>		Laplacian Gain																																																																																																																																			
Error Rate Graph Plot																																																																																																																																							
Results	<p>Raw Data</p> <table border="1"> <tr><td>3</td><td>-0.2536</td><td>-0.5916</td><td>-0.2545</td><td>-0.3723</td><td>-0.1298</td><td>0.0627</td><td>0.3555</td><td>0.3050</td><td>0.2503</td><td>0.6282</td></tr> <tr><td>4</td><td>0.0013</td><td>-0.3007</td><td>-0.2507</td><td>-0.1874</td><td>-0.1927</td><td>-0.0145</td><td>0.3261</td><td>0.2819</td><td>0.2750</td><td>0.0617</td></tr> <tr><td>5</td><td>-0.0447</td><td>-0.1829</td><td>-0.2204</td><td>-0.1270</td><td>0.0845</td><td>0.1394</td><td>0.0762</td><td>0.0549</td><td>0.0381</td><td>0.1820</td></tr> <tr><td>6</td><td>-0.1763</td><td>-0.1998</td><td>-0.0233</td><td>0.0192</td><td>0.0045</td><td>0.0278</td><td>0.1166</td><td>0.1066</td><td>0.1047</td><td>0.0201</td></tr> <tr><td>7</td><td>-0.0841</td><td>-0.0814</td><td>-0.0275</td><td>-0.0085</td><td>0.0533</td><td>0.0568</td><td>0.0146</td><td>0.0112</td><td>0.0082</td><td>0.0576</td></tr> <tr><td>8</td><td>-0.0631</td><td>-0.0570</td><td>0.0150</td><td>0.0201</td><td>9.0856e-04</td><td>0.0028</td><td>0.0283</td><td>0.0269</td><td>0.0269</td><td>-9.8425e-04</td></tr> <tr><td>9</td><td>-0.0135</td><td>-0.0108</td><td>-0.0035</td><td>-0.0017</td><td>0.0128</td><td>0.0126</td><td>-0.0034</td><td>-0.0028</td><td>-0.0033</td><td>0.0124</td></tr> <tr><td>10</td><td>-0.0099</td><td>-0.0087</td><td>0.0055</td><td>0.0057</td><td>-0.0027</td><td>-0.0025</td><td>0.0054</td><td>0.0052</td><td>0.0053</td><td>-0.0034</td></tr> <tr><td>11</td><td>-0.0084</td><td>0.0020</td><td>-3.2054e-04</td><td>-2.1854e-04</td><td>0.0035</td><td>0.0034</td><td>-0.0010</td><td>-0.0010</td><td>-0.0011</td><td>0.0033</td></tr> <tr><td>12</td><td>-0.0018</td><td>-8.1190e-04</td><td>0.0014</td><td>0.0013</td><td>-0.0011</td><td>-0.0010</td><td>0.0011</td><td>0.0011</td><td>0.0011</td><td>-0.0012</td></tr> <tr><td>13</td><td>-9.4183e-04</td><td>9.6229e-04</td><td>-2.8084e-04</td><td>-2.8162e-04</td><td>6.7411e-04</td><td>6.5463e-04</td><td>-4.7590e-04</td><td>-4.7919e-04</td><td>-4.9266e-04</td><td>6.6101e-04</td></tr> <tr><td>14</td><td>3.3716e-04</td><td>-1.3318e-04</td><td>2.3319e-04</td><td>2.2093e-04</td><td>-3.8585e-04</td><td>-3.8072e-04</td><td>1.7170e-04</td><td>1.6923e-04</td><td>1.7344e-04</td><td>-4.0590e-04</td></tr> </table>	3	-0.2536		-0.5916	-0.2545	-0.3723	-0.1298	0.0627	0.3555	0.3050	0.2503	0.6282	4	0.0013	-0.3007	-0.2507	-0.1874	-0.1927	-0.0145	0.3261	0.2819	0.2750	0.0617	5	-0.0447	-0.1829	-0.2204	-0.1270	0.0845	0.1394	0.0762	0.0549	0.0381	0.1820	6	-0.1763	-0.1998	-0.0233	0.0192	0.0045	0.0278	0.1166	0.1066	0.1047	0.0201	7	-0.0841	-0.0814	-0.0275	-0.0085	0.0533	0.0568	0.0146	0.0112	0.0082	0.0576	8	-0.0631	-0.0570	0.0150	0.0201	9.0856e-04	0.0028	0.0283	0.0269	0.0269	-9.8425e-04	9	-0.0135	-0.0108	-0.0035	-0.0017	0.0128	0.0126	-0.0034	-0.0028	-0.0033	0.0124	10	-0.0099	-0.0087	0.0055	0.0057	-0.0027	-0.0025	0.0054	0.0052	0.0053	-0.0034	11	-0.0084	0.0020	-3.2054e-04	-2.1854e-04	0.0035	0.0034	-0.0010	-0.0010	-0.0011	0.0033	12	-0.0018	-8.1190e-04	0.0014	0.0013	-0.0011	-0.0010	0.0011	0.0011	0.0011	-0.0012	13	-9.4183e-04	9.6229e-04	-2.8084e-04	-2.8162e-04	6.7411e-04	6.5463e-04	-4.7590e-04	-4.7919e-04	-4.9266e-04	6.6101e-04	14	3.3716e-04	-1.3318e-04	2.3319e-04	2.2093e-04	-3.8585e-04	-3.8072e-04	1.7170e-04	1.6923e-04	1.7344e-04	-4.0590e-04	Convergence Iteration
3	-0.2536	-0.5916	-0.2545	-0.3723	-0.1298	0.0627	0.3555	0.3050	0.2503	0.6282																																																																																																																													
4	0.0013	-0.3007	-0.2507	-0.1874	-0.1927	-0.0145	0.3261	0.2819	0.2750	0.0617																																																																																																																													
5	-0.0447	-0.1829	-0.2204	-0.1270	0.0845	0.1394	0.0762	0.0549	0.0381	0.1820																																																																																																																													
6	-0.1763	-0.1998	-0.0233	0.0192	0.0045	0.0278	0.1166	0.1066	0.1047	0.0201																																																																																																																													
7	-0.0841	-0.0814	-0.0275	-0.0085	0.0533	0.0568	0.0146	0.0112	0.0082	0.0576																																																																																																																													
8	-0.0631	-0.0570	0.0150	0.0201	9.0856e-04	0.0028	0.0283	0.0269	0.0269	-9.8425e-04																																																																																																																													
9	-0.0135	-0.0108	-0.0035	-0.0017	0.0128	0.0126	-0.0034	-0.0028	-0.0033	0.0124																																																																																																																													
10	-0.0099	-0.0087	0.0055	0.0057	-0.0027	-0.0025	0.0054	0.0052	0.0053	-0.0034																																																																																																																													
11	-0.0084	0.0020	-3.2054e-04	-2.1854e-04	0.0035	0.0034	-0.0010	-0.0010	-0.0011	0.0033																																																																																																																													
12	-0.0018	-8.1190e-04	0.0014	0.0013	-0.0011	-0.0010	0.0011	0.0011	0.0011	-0.0012																																																																																																																													
13	-9.4183e-04	9.6229e-04	-2.8084e-04	-2.8162e-04	6.7411e-04	6.5463e-04	-4.7590e-04	-4.7919e-04	-4.9266e-04	6.6101e-04																																																																																																																													
14	3.3716e-04	-1.3318e-04	2.3319e-04	2.2093e-04	-3.8585e-04	-3.8072e-04	1.7170e-04	1.6923e-04	1.7344e-04	-4.0590e-04																																																																																																																													
		12	20.4270																																																																																																																																				

Laplacian Gain Calculation

Spectrum Laplacian Eigen Value											rho = 2/SSE+LE
Before Attack	1.5 e-16	0.76	2.76	4	4	4	4	4	5.23	7.23	0.25
After Attack	-9.5 e-16	0.51	1.39	3	3.27	4	4	4	4.81	6.98	0.2665

**Experiment 6**

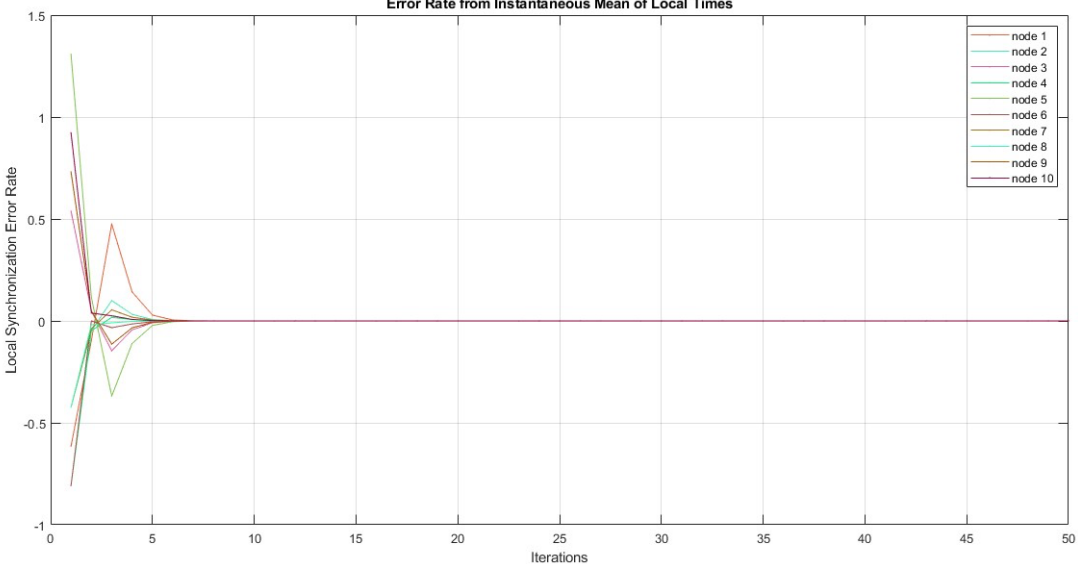
Simulation No.6-a	Fully Connected 10 Nodes – Node Destruction Attack			GAIN																																																																																																																																			
Input	<pre> GRAPH = [ ... 0 1 1 1 0 0 0 0 0 0; 1 0 1 1 0 0 0 0 0 0; 1 1 0 0 1 1 0 0 0 0; 1 1 0 0 1 1 0 0 0 0; 0 0 1 1 0 0 1 1 0 0; 0 0 1 1 0 0 1 1 0 0; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 0 0 1 1 0 1; 0 0 0 0 0 0 1 1 0 1; 0 0 0 0 0 0 1 1 0 1; 0 0 0 0 0 0 1 1 0 1; ];                     </pre>	<pre> GRAPH1 = [ ... 0 0 1 1 0 0 0 0 0 0; 0 0 0 0 0 0 0 0 0 0; 1 0 0 1 1 1 0 0 0 0; 1 0 1 0 1 1 0 0 0 0; 0 0 1 1 0 1 1 1 0 0; 0 0 1 1 1 0 1 1 0 0; 0 0 0 0 1 1 0 1 1 1; 0 0 0 0 1 1 1 0 1 1; 0 0 0 0 0 0 1 1 0 1; 0 0 0 0 0 0 0 1 1 0; 0 0 0 0 0 0 0 1 1 0; ];                     </pre>																																																																																																																																					
Error Rate Graph Plot				No Gain																																																																																																																																			
Results	Raw Data	Convergence Iteration	Global Synchronization Error Rate																																																																																																																																				
	<table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr><td>23</td><td>0.1068</td><td>-1</td><td>0.1109</td><td>0.1113</td><td>0.1118</td><td>0.1119</td><td>0.1120</td><td>0.1118</td><td>0.1117</td><td>0.1117</td></tr> <tr><td>24</td><td>0.1082</td><td>-1</td><td>0.1111</td><td>0.1113</td><td>0.1116</td><td>0.1117</td><td>0.1117</td><td>0.1115</td><td>0.1115</td><td>0.1115</td></tr> <tr><td>25</td><td>0.1092</td><td>-1</td><td>0.1111</td><td>0.1113</td><td>0.1114</td><td>0.1115</td><td>0.1115</td><td>0.1114</td><td>0.1113</td><td>0.1113</td></tr> <tr><td>26</td><td>0.1099</td><td>-1</td><td>0.1112</td><td>0.1113</td><td>0.1113</td><td>0.1113</td><td>0.1113</td><td>0.1113</td><td>0.1112</td><td>0.1112</td></tr> <tr><td>27</td><td>0.1103</td><td>-1</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td></tr> <tr><td>28</td><td>0.1106</td><td>-1</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1111</td><td>0.1111</td></tr> <tr><td>29</td><td>0.1108</td><td>-1</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> <tr><td>30</td><td>0.1110</td><td>-1</td><td>0.1112</td><td>0.1112</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> <tr style="background-color: #e0f0ff;"><td>31</td><td>0.1110</td><td>-1</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> <tr><td>32</td><td>0.1111</td><td>-1</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> <tr><td>33</td><td>0.1111</td><td>-1</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> <tr><td>34</td><td>0.1111</td><td>-1</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> </tbody> </table>	23	0.1068	-1	0.1109	0.1113	0.1118	0.1119	0.1120	0.1118	0.1117	0.1117	24	0.1082	-1	0.1111	0.1113	0.1116	0.1117	0.1117	0.1115	0.1115	0.1115	25	0.1092	-1	0.1111	0.1113	0.1114	0.1115	0.1115	0.1114	0.1113	0.1113	26	0.1099	-1	0.1112	0.1113	0.1113	0.1113	0.1113	0.1113	0.1112	0.1112	27	0.1103	-1	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112	28	0.1106	-1	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112	0.1111	0.1111	29	0.1108	-1	0.1112	0.1112	0.1112	0.1112	0.1111	0.1111	0.1111	0.1111	30	0.1110	-1	0.1112	0.1112	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	31	0.1110	-1	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	32	0.1111	-1	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	33	0.1111	-1	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	34	0.1111	-1	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	31	105.59115
23	0.1068	-1	0.1109	0.1113	0.1118	0.1119	0.1120	0.1118	0.1117	0.1117																																																																																																																													
24	0.1082	-1	0.1111	0.1113	0.1116	0.1117	0.1117	0.1115	0.1115	0.1115																																																																																																																													
25	0.1092	-1	0.1111	0.1113	0.1114	0.1115	0.1115	0.1114	0.1113	0.1113																																																																																																																													
26	0.1099	-1	0.1112	0.1113	0.1113	0.1113	0.1113	0.1113	0.1112	0.1112																																																																																																																													
27	0.1103	-1	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112																																																																																																																													
28	0.1106	-1	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112	0.1111	0.1111																																																																																																																													
29	0.1108	-1	0.1112	0.1112	0.1112	0.1112	0.1111	0.1111	0.1111	0.1111																																																																																																																													
30	0.1110	-1	0.1112	0.1112	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111																																																																																																																													
31	0.1110	-1	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111																																																																																																																													
32	0.1111	-1	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111																																																																																																																													
33	0.1111	-1	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111																																																																																																																													
34	0.1111	-1	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111																																																																																																																													

Simulation No.6-b	Fully Connected 10 Nodes – Node Destruction Attack			GAIN																																																																																																																																			
Input	<pre> GRAPH = [ ... 0 1 1 1 0 0 0 0 0 0; 1 0 1 1 0 0 0 0 0 0; 1 1 0 0 1 1 0 0 0 0; 1 1 0 0 1 1 0 0 0 0; 0 0 1 1 0 0 1 1 0 0; 0 0 1 1 0 0 1 1 0 0; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 1 1 0 0 1 1; 0 0 0 0 0 0 1 1 0 1; 0 0 0 0 0 0 1 1 0 1; 0 0 0 0 0 0 1 1 1 0; ];</pre>	<pre> GRAPH1 = [ ... 0 0 1 1 0 0 0 0 0 0; 0 0 0 0 0 0 0 0 0 0; 1 0 0 1 1 1 0 0 0 0; 1 0 1 0 1 1 0 0 0 0; 0 0 1 1 0 1 1 1 0 0; 0 0 1 1 0 1 1 1 0 0; 0 0 0 0 1 1 0 1 1 1; 0 0 0 0 1 1 0 1 1 1; 0 0 0 0 1 1 1 0 1 1; 0 0 0 0 0 0 1 1 0 1; 0 0 0 0 0 0 1 1 1 0; ];</pre>																																																																																																																																					
Error Rate Graph Plot				Laplacian Gain																																																																																																																																			
Results	Raw Data	Convergence Iteration	Global Synchronization Error Rate																																																																																																																																				
	<table border="1"> <tbody> <tr><td>7</td><td>-0.0841</td><td>-0.0814</td><td>-0.0275</td><td>-0.0085</td><td>0.0533</td><td>0.0568</td><td>0.0146</td><td>0.0112</td><td>0.0082</td><td>0.0576</td></tr> <tr><td>8</td><td>-0.0631</td><td>-0.0570</td><td>0.0150</td><td>0.0201</td><td>9.0856e-04</td><td>0.0028</td><td>0.0283</td><td>0.0269</td><td>0.0269</td><td>-9.8425e-04</td></tr> <tr><td>9</td><td>-0.0135</td><td>-0.0108</td><td>-0.0035</td><td>-0.0017</td><td>0.0128</td><td>0.0126</td><td>-0.0024</td><td>-0.0028</td><td>-0.0033</td><td>0.0124</td></tr> <tr><td>10</td><td>-0.0099</td><td>-0.0087</td><td>0.0055</td><td>0.0057</td><td>-0.0027</td><td>-0.0025</td><td>0.0054</td><td>0.0052</td><td>0.0053</td><td>-0.0034</td></tr> <tr><td>11</td><td>0.1117</td><td>-1</td><td>0.1099</td><td>0.1100</td><td>0.1138</td><td>0.1137</td><td>0.1092</td><td>0.1091</td><td>0.1090</td><td>0.1136</td></tr> <tr><td>12</td><td>0.1100</td><td>-1</td><td>0.1123</td><td>0.1122</td><td>0.1099</td><td>0.1100</td><td>0.1119</td><td>0.1119</td><td>0.1119</td><td>0.1098</td></tr> <tr><td>13</td><td>0.1119</td><td>-1</td><td>0.1108</td><td>0.1108</td><td>0.1116</td><td>0.1116</td><td>0.1106</td><td>0.1106</td><td>0.1106</td><td>0.1116</td></tr> <tr><td>14</td><td>0.1111</td><td>-1</td><td>0.1113</td><td>0.1113</td><td>0.1108</td><td>0.1108</td><td>0.1113</td><td>0.1113</td><td>0.1113</td><td>0.1108</td></tr> <tr><td>15</td><td>0.1114</td><td>-1</td><td>0.1110</td><td>0.1110</td><td>0.1112</td><td>0.1112</td><td>0.1110</td><td>0.1110</td><td>0.1110</td><td>0.1112</td></tr> <tr><td>16</td><td>0.1111</td><td>-1</td><td>0.1112</td><td>0.1112</td><td>0.1110</td><td>0.1110</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1110</td></tr> <tr><td>17</td><td>0.1112</td><td>-1</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> <tr><td>18</td><td>0.1111</td><td>-1</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> </tbody> </table>	7	-0.0841	-0.0814	-0.0275	-0.0085	0.0533	0.0568	0.0146	0.0112	0.0082	0.0576	8	-0.0631	-0.0570	0.0150	0.0201	9.0856e-04	0.0028	0.0283	0.0269	0.0269	-9.8425e-04	9	-0.0135	-0.0108	-0.0035	-0.0017	0.0128	0.0126	-0.0024	-0.0028	-0.0033	0.0124	10	-0.0099	-0.0087	0.0055	0.0057	-0.0027	-0.0025	0.0054	0.0052	0.0053	-0.0034	11	0.1117	-1	0.1099	0.1100	0.1138	0.1137	0.1092	0.1091	0.1090	0.1136	12	0.1100	-1	0.1123	0.1122	0.1099	0.1100	0.1119	0.1119	0.1119	0.1098	13	0.1119	-1	0.1108	0.1108	0.1116	0.1116	0.1106	0.1106	0.1106	0.1116	14	0.1111	-1	0.1113	0.1113	0.1108	0.1108	0.1113	0.1113	0.1113	0.1108	15	0.1114	-1	0.1110	0.1110	0.1112	0.1112	0.1110	0.1110	0.1110	0.1112	16	0.1111	-1	0.1112	0.1112	0.1110	0.1110	0.1111	0.1111	0.1111	0.1110	17	0.1112	-1	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	18	0.1111	-1	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	17	100.3794
7	-0.0841	-0.0814	-0.0275	-0.0085	0.0533	0.0568	0.0146	0.0112	0.0082	0.0576																																																																																																																													
8	-0.0631	-0.0570	0.0150	0.0201	9.0856e-04	0.0028	0.0283	0.0269	0.0269	-9.8425e-04																																																																																																																													
9	-0.0135	-0.0108	-0.0035	-0.0017	0.0128	0.0126	-0.0024	-0.0028	-0.0033	0.0124																																																																																																																													
10	-0.0099	-0.0087	0.0055	0.0057	-0.0027	-0.0025	0.0054	0.0052	0.0053	-0.0034																																																																																																																													
11	0.1117	-1	0.1099	0.1100	0.1138	0.1137	0.1092	0.1091	0.1090	0.1136																																																																																																																													
12	0.1100	-1	0.1123	0.1122	0.1099	0.1100	0.1119	0.1119	0.1119	0.1098																																																																																																																													
13	0.1119	-1	0.1108	0.1108	0.1116	0.1116	0.1106	0.1106	0.1106	0.1116																																																																																																																													
14	0.1111	-1	0.1113	0.1113	0.1108	0.1108	0.1113	0.1113	0.1113	0.1108																																																																																																																													
15	0.1114	-1	0.1110	0.1110	0.1112	0.1112	0.1110	0.1110	0.1110	0.1112																																																																																																																													
16	0.1111	-1	0.1112	0.1112	0.1110	0.1110	0.1111	0.1111	0.1111	0.1110																																																																																																																													
17	0.1112	-1	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111																																																																																																																													
18	0.1111	-1	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111																																																																																																																													

**Laplacian Gain Calculation**

Spectrum Laplacian Eigen Value											rho = 2/SSE+LE
Before Attack	1.5 e-16	0.76	2.76	4	4	4	4	4	5.23	7.23	0.25
After Attack	-2.0 e-15	0	0.88	2.55	4	4.59	5	6	6	6.96	0.255



Simulation No.7-b	<b>Fully Connected 4 Nodes – No Attack</b>			GAIN																																																																																																																																			
Input	GRAPH = [ ... 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1;];	GRAPH = [ ... 1 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1 1; 1 1 1 1 1 1 1 1 1 1 1 1;];																																																																																																																																					
Error Rate Graph Plot				Lap-lacian Gain																																																																																																																																			
Results	Raw Data <table border="1" style="width: 100%; border-collapse: collapse; font-size: small;"> <tr><td>1</td><td>-0.6154</td><td>-0.4231</td><td>0.5385</td><td>-0.8077</td><td>1.3077</td><td>-0.8077</td><td>-0.4231</td><td>-0.4231</td><td>0.7308</td><td>0.8231</td></tr> <tr><td>2</td><td>-0.0962</td><td>-0.0481</td><td>0.0481</td><td>-0.0481</td><td>0.1154</td><td>0</td><td>-0.0385</td><td>-0.0182</td><td>0.0481</td><td>0.0385</td></tr> <tr><td>3</td><td>0.4752</td><td>0.0998</td><td>-0.1465</td><td>0.0172</td><td>-0.3488</td><td>-0.0333</td><td>0.0543</td><td>-0.0094</td><td>-0.1137</td><td>0.0252</td></tr> <tr><td>4</td><td>0.1432</td><td>0.0322</td><td>-0.0443</td><td>0.0067</td><td>-0.1109</td><td>-0.0150</td><td>0.0181</td><td>-0.0026</td><td>-0.0339</td><td>0.0074</td></tr> <tr><td>5</td><td>0.0284</td><td>0.0068</td><td>-0.0089</td><td>0.0015</td><td>-0.0221</td><td>-0.0039</td><td>0.0039</td><td>-5.1350e-04</td><td>-0.0067</td><td>0.0016</td></tr> <tr><td>6</td><td>0.0047</td><td>0.0012</td><td>-0.0015</td><td>2.6700e-04</td><td>-0.0037</td><td>-7.7937e-04</td><td>6.8067e-04</td><td>-8.7497e-05</td><td>-0.0011</td><td>2.7403e-04</td></tr> <tr style="background-color: #e0f0ff;"><td>7</td><td>7.7939e-04</td><td>1.8237e-04</td><td>-2.2344e-04</td><td>4.2563e-05</td><td>-3.5162e-04</td><td>-1.3294e-04</td><td>1.0867e-04</td><td>-1.3453e-05</td><td>-1.6224e-04</td><td>4.3171e-05</td></tr> <tr><td>8</td><td>9.9036e-05</td><td>2.6287e-05</td><td>-3.1170e-05</td><td>6.2523e-06</td><td>-7.7108e-05</td><td>-2.0736e-05</td><td>1.5487e-05</td><td>-1.9283e-06</td><td>-2.2441e-05</td><td>6.3102e-06</td></tr> <tr><td>9</td><td>1.3194e-06</td><td>3.5948e-06</td><td>-4.1584e-06</td><td>8.6629e-07</td><td>-1.0285e-06</td><td>-3.0197e-06</td><td>2.1334e-06</td><td>-2.6272e-07</td><td>-2.9586e-06</td><td>8.7375e-07</td></tr> <tr><td>10</td><td>1.6949e-06</td><td>4.7259e-07</td><td>-5.3485e-07</td><td>1.1561e-07</td><td>-1.3176e-06</td><td>-4.1791e-07</td><td>2.8205e-07</td><td>-3.4445e-08</td><td>-3.7641e-07</td><td>1.1614e-07</td></tr> <tr><td>11</td><td>2.1167e-07</td><td>6.0251e-08</td><td>-6.6878e-08</td><td>1.4901e-08</td><td>-1.6445e-07</td><td>-5.5610e-08</td><td>3.6135e-08</td><td>-4.3827e-09</td><td>-4.6594e-08</td><td>1.4951e-08</td></tr> <tr><td>12</td><td>2.5849e-08</td><td>7.4950e-09</td><td>-8.1752e-09</td><td>1.8711e-09</td><td>-2.0070e-08</td><td>-7.1733e-09</td><td>4.5143e-09</td><td>-5.4433e-10</td><td>-5.6453e-09</td><td>1.8779e-09</td></tr> </table>	1	-0.6154		-0.4231	0.5385	-0.8077	1.3077	-0.8077	-0.4231	-0.4231	0.7308	0.8231	2	-0.0962	-0.0481	0.0481	-0.0481	0.1154	0	-0.0385	-0.0182	0.0481	0.0385	3	0.4752	0.0998	-0.1465	0.0172	-0.3488	-0.0333	0.0543	-0.0094	-0.1137	0.0252	4	0.1432	0.0322	-0.0443	0.0067	-0.1109	-0.0150	0.0181	-0.0026	-0.0339	0.0074	5	0.0284	0.0068	-0.0089	0.0015	-0.0221	-0.0039	0.0039	-5.1350e-04	-0.0067	0.0016	6	0.0047	0.0012	-0.0015	2.6700e-04	-0.0037	-7.7937e-04	6.8067e-04	-8.7497e-05	-0.0011	2.7403e-04	7	7.7939e-04	1.8237e-04	-2.2344e-04	4.2563e-05	-3.5162e-04	-1.3294e-04	1.0867e-04	-1.3453e-05	-1.6224e-04	4.3171e-05	8	9.9036e-05	2.6287e-05	-3.1170e-05	6.2523e-06	-7.7108e-05	-2.0736e-05	1.5487e-05	-1.9283e-06	-2.2441e-05	6.3102e-06	9	1.3194e-06	3.5948e-06	-4.1584e-06	8.6629e-07	-1.0285e-06	-3.0197e-06	2.1334e-06	-2.6272e-07	-2.9586e-06	8.7375e-07	10	1.6949e-06	4.7259e-07	-5.3485e-07	1.1561e-07	-1.3176e-06	-4.1791e-07	2.8205e-07	-3.4445e-08	-3.7641e-07	1.1614e-07	11	2.1167e-07	6.0251e-08	-6.6878e-08	1.4901e-08	-1.6445e-07	-5.5610e-08	3.6135e-08	-4.3827e-09	-4.6594e-08	1.4951e-08	12	2.5849e-08	7.4950e-09	-8.1752e-09	1.8711e-09	-2.0070e-08	-7.1733e-09	4.5143e-09	-5.4433e-10	-5.6453e-09	1.8779e-09	Convergence Iteration  7
1	-0.6154	-0.4231	0.5385	-0.8077	1.3077	-0.8077	-0.4231	-0.4231	0.7308	0.8231																																																																																																																													
2	-0.0962	-0.0481	0.0481	-0.0481	0.1154	0	-0.0385	-0.0182	0.0481	0.0385																																																																																																																													
3	0.4752	0.0998	-0.1465	0.0172	-0.3488	-0.0333	0.0543	-0.0094	-0.1137	0.0252																																																																																																																													
4	0.1432	0.0322	-0.0443	0.0067	-0.1109	-0.0150	0.0181	-0.0026	-0.0339	0.0074																																																																																																																													
5	0.0284	0.0068	-0.0089	0.0015	-0.0221	-0.0039	0.0039	-5.1350e-04	-0.0067	0.0016																																																																																																																													
6	0.0047	0.0012	-0.0015	2.6700e-04	-0.0037	-7.7937e-04	6.8067e-04	-8.7497e-05	-0.0011	2.7403e-04																																																																																																																													
7	7.7939e-04	1.8237e-04	-2.2344e-04	4.2563e-05	-3.5162e-04	-1.3294e-04	1.0867e-04	-1.3453e-05	-1.6224e-04	4.3171e-05																																																																																																																													
8	9.9036e-05	2.6287e-05	-3.1170e-05	6.2523e-06	-7.7108e-05	-2.0736e-05	1.5487e-05	-1.9283e-06	-2.2441e-05	6.3102e-06																																																																																																																													
9	1.3194e-06	3.5948e-06	-4.1584e-06	8.6629e-07	-1.0285e-06	-3.0197e-06	2.1334e-06	-2.6272e-07	-2.9586e-06	8.7375e-07																																																																																																																													
10	1.6949e-06	4.7259e-07	-5.3485e-07	1.1561e-07	-1.3176e-06	-4.1791e-07	2.8205e-07	-3.4445e-08	-3.7641e-07	1.1614e-07																																																																																																																													
11	2.1167e-07	6.0251e-08	-6.6878e-08	1.4901e-08	-1.6445e-07	-5.5610e-08	3.6135e-08	-4.3827e-09	-4.6594e-08	1.4951e-08																																																																																																																													
12	2.5849e-08	7.4950e-09	-8.1752e-09	1.8711e-09	-2.0070e-08	-7.1733e-09	4.5143e-09	-5.4433e-10	-5.6453e-09	1.8779e-09																																																																																																																													

**Laplacian Gain Calculation**

Spectrum Laplacian Eigen Value											rho = 2/SSE+LE
No Attack	1.6 e-15	10	10	10	10	10	10	10	10	10	0.1











**Experiment 10**

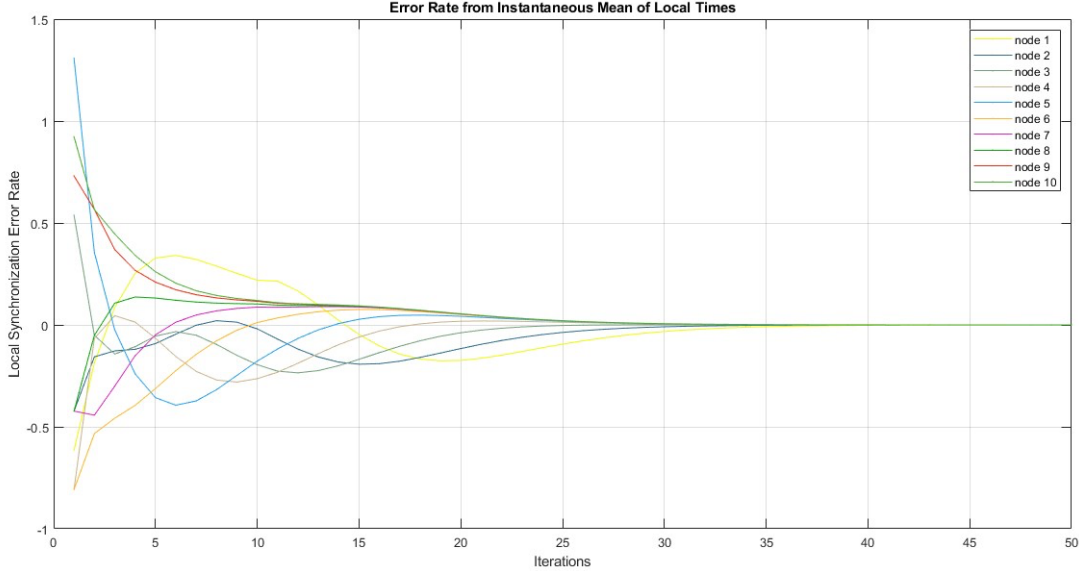
Simulation No.10-a	Ring Mesh 10 Nodes – No Attack			GAIN																																																																																																																																				
Input	<pre> GRAPH = [ ... 0 1 0 0 0 0 0 0 0 1; 1 0 1 0 0 0 0 0 0 0; 0 1 0 1 0 0 0 0 0 0; 0 0 1 0 1 0 0 0 0 0; 0 0 0 0 0 1 0 0 0 0; 0 0 0 0 1 0 1 0 0 0; 0 0 0 0 0 1 0 1 0 0; 0 0 0 0 0 0 1 0 1 0; 0 0 0 0 0 0 0 1 0 1; 1 0 0 0 0 0 0 0 1 0;];                     </pre>		<pre> GRAPH = [ ... 0 1 0 0 0 0 0 0 0 1; 1 0 1 0 0 0 0 0 0 0; 0 1 0 1 0 0 0 0 0 0; 0 0 1 0 1 0 0 0 0 0; 0 0 0 0 0 1 0 0 0 0; 0 0 0 0 1 0 1 0 0 0; 0 0 0 0 0 1 0 1 0 0; 0 0 0 0 0 0 1 0 1 0; 0 0 0 0 0 0 0 1 0 1; 1 0 0 0 0 0 0 0 1 0;];                     </pre>																																																																																																																																					
Error Rate Graph Plot				No Gain																																																																																																																																				
Results	Raw Data	Convergence Iteration	Global Synchronization Error Rate																																																																																																																																					
	<table border="1"> <tbody> <tr><td>28</td><td>0.0042</td><td>-0.0223</td><td>-0.0058</td><td>9.0299e-04</td><td>0.0031</td><td>0.0038</td><td>0.0040</td><td>0.0041</td><td>0.0041</td><td>0.0041</td></tr> <tr><td>29</td><td>0.0031</td><td>-0.0171</td><td>-0.0043</td><td>7.4008e-04</td><td>0.0023</td><td>0.0029</td><td>0.0030</td><td>0.0031</td><td>0.0031</td><td>0.0031</td></tr> <tr><td>30</td><td>0.0024</td><td>-0.0130</td><td>-0.0031</td><td>5.9583e-04</td><td>0.0018</td><td>0.0022</td><td>0.0023</td><td>0.0023</td><td>0.0023</td><td>0.0023</td></tr> <tr><td>31</td><td>0.0018</td><td>-0.0099</td><td>-0.0023</td><td>4.7390e-04</td><td>0.0014</td><td>0.0017</td><td>0.0017</td><td>0.0017</td><td>0.0017</td><td>0.0017</td></tr> <tr><td>32</td><td>0.0013</td><td>-0.0075</td><td>-0.0017</td><td>3.7377e-04</td><td>0.0010</td><td>0.0012</td><td>0.0013</td><td>0.0013</td><td>0.0013</td><td>0.0013</td></tr> <tr><td>33</td><td>9.9273e-04</td><td>-0.0056</td><td>-0.0013</td><td>2.9307e-04</td><td>7.7904e-04</td><td>9.3421e-04</td><td>9.7223e-04</td><td>9.8009e-04</td><td>9.8111e-04</td><td>9.8114e-04</td></tr> <tr><td>34</td><td>7.4013e-04</td><td>-0.0042</td><td>-9.3255e-04</td><td>2.2882e-04</td><td>5.8786e-04</td><td>7.0010e-04</td><td>7.2676e-04</td><td>7.3205e-04</td><td>7.3270e-04</td><td>7.3272e-04</td></tr> <tr><td>35</td><td>5.5067e-04</td><td>-0.0032</td><td>-6.8602e-04</td><td>1.7806e-04</td><td>4.4257e-04</td><td>5.2338e-04</td><td>5.4198e-04</td><td>5.4552e-04</td><td>5.4593e-04</td><td>5.4594e-04</td></tr> <tr><td>36</td><td>4.0886e-04</td><td>-0.0024</td><td>-5.0360e-04</td><td>1.3816e-04</td><td>3.3240e-04</td><td>3.9031e-04</td><td>4.0322e-04</td><td>4.0558e-04</td><td>4.0585e-04</td><td>4.0586e-04</td></tr> <tr><td>37</td><td>3.0293e-04</td><td>-0.0018</td><td>-3.6878e-04</td><td>1.0691e-04</td><td>2.4905e-04</td><td>2.9035e-04</td><td>2.9928e-04</td><td>3.0085e-04</td><td>3.0102e-04</td><td>3.0102e-04</td></tr> <tr><td>38</td><td>2.2395e-04</td><td>-0.0013</td><td>-2.6930e-04</td><td>8.2500e-05</td><td>1.8612e-04</td><td>2.1545e-04</td><td>2.2159e-04</td><td>2.2263e-04</td><td>2.2274e-04</td><td>2.2274e-04</td></tr> <tr><td>39</td><td>1.6519e-04</td><td>-9.8765e-04</td><td>-1.9604e-04</td><td>6.3473e-05</td><td>1.3872e-04</td><td>1.5945e-04</td><td>1.6366e-04</td><td>1.6435e-04</td><td>1.6442e-04</td><td>1.6442e-04</td></tr> </tbody> </table>	28	0.0042	-0.0223	-0.0058	9.0299e-04	0.0031	0.0038	0.0040	0.0041	0.0041	0.0041	29	0.0031	-0.0171	-0.0043	7.4008e-04	0.0023	0.0029	0.0030	0.0031	0.0031	0.0031	30	0.0024	-0.0130	-0.0031	5.9583e-04	0.0018	0.0022	0.0023	0.0023	0.0023	0.0023	31	0.0018	-0.0099	-0.0023	4.7390e-04	0.0014	0.0017	0.0017	0.0017	0.0017	0.0017	32	0.0013	-0.0075	-0.0017	3.7377e-04	0.0010	0.0012	0.0013	0.0013	0.0013	0.0013	33	9.9273e-04	-0.0056	-0.0013	2.9307e-04	7.7904e-04	9.3421e-04	9.7223e-04	9.8009e-04	9.8111e-04	9.8114e-04	34	7.4013e-04	-0.0042	-9.3255e-04	2.2882e-04	5.8786e-04	7.0010e-04	7.2676e-04	7.3205e-04	7.3270e-04	7.3272e-04	35	5.5067e-04	-0.0032	-6.8602e-04	1.7806e-04	4.4257e-04	5.2338e-04	5.4198e-04	5.4552e-04	5.4593e-04	5.4594e-04	36	4.0886e-04	-0.0024	-5.0360e-04	1.3816e-04	3.3240e-04	3.9031e-04	4.0322e-04	4.0558e-04	4.0585e-04	4.0586e-04	37	3.0293e-04	-0.0018	-3.6878e-04	1.0691e-04	2.4905e-04	2.9035e-04	2.9928e-04	3.0085e-04	3.0102e-04	3.0102e-04	38	2.2395e-04	-0.0013	-2.6930e-04	8.2500e-05	1.8612e-04	2.1545e-04	2.2159e-04	2.2263e-04	2.2274e-04	2.2274e-04	39	1.6519e-04	-9.8765e-04	-1.9604e-04	6.3473e-05	1.3872e-04	1.5945e-04	1.6366e-04	1.6435e-04	1.6442e-04	1.6442e-04	37	33.5512	
28	0.0042	-0.0223	-0.0058	9.0299e-04	0.0031	0.0038	0.0040	0.0041	0.0041	0.0041																																																																																																																														
29	0.0031	-0.0171	-0.0043	7.4008e-04	0.0023	0.0029	0.0030	0.0031	0.0031	0.0031																																																																																																																														
30	0.0024	-0.0130	-0.0031	5.9583e-04	0.0018	0.0022	0.0023	0.0023	0.0023	0.0023																																																																																																																														
31	0.0018	-0.0099	-0.0023	4.7390e-04	0.0014	0.0017	0.0017	0.0017	0.0017	0.0017																																																																																																																														
32	0.0013	-0.0075	-0.0017	3.7377e-04	0.0010	0.0012	0.0013	0.0013	0.0013	0.0013																																																																																																																														
33	9.9273e-04	-0.0056	-0.0013	2.9307e-04	7.7904e-04	9.3421e-04	9.7223e-04	9.8009e-04	9.8111e-04	9.8114e-04																																																																																																																														
34	7.4013e-04	-0.0042	-9.3255e-04	2.2882e-04	5.8786e-04	7.0010e-04	7.2676e-04	7.3205e-04	7.3270e-04	7.3272e-04																																																																																																																														
35	5.5067e-04	-0.0032	-6.8602e-04	1.7806e-04	4.4257e-04	5.2338e-04	5.4198e-04	5.4552e-04	5.4593e-04	5.4594e-04																																																																																																																														
36	4.0886e-04	-0.0024	-5.0360e-04	1.3816e-04	3.3240e-04	3.9031e-04	4.0322e-04	4.0558e-04	4.0585e-04	4.0586e-04																																																																																																																														
37	3.0293e-04	-0.0018	-3.6878e-04	1.0691e-04	2.4905e-04	2.9035e-04	2.9928e-04	3.0085e-04	3.0102e-04	3.0102e-04																																																																																																																														
38	2.2395e-04	-0.0013	-2.6930e-04	8.2500e-05	1.8612e-04	2.1545e-04	2.2159e-04	2.2263e-04	2.2274e-04	2.2274e-04																																																																																																																														
39	1.6519e-04	-9.8765e-04	-1.9604e-04	6.3473e-05	1.3872e-04	1.5945e-04	1.6366e-04	1.6435e-04	1.6442e-04	1.6442e-04																																																																																																																														

Simulation No.10-b	Ring Mesh 10 Nodes – No Attack		GAIN																																																																																																																																				
Input	<pre> GRAPH = [ ... 0 1 0 0 0 0 0 0 0 1; 1 0 1 0 0 0 0 0 0 0; 0 1 0 1 0 0 0 0 0 0; 0 0 1 0 1 0 0 0 0 0; 0 0 0 0 1 0 1 0 0 0; 0 0 0 0 1 0 1 0 0 0; 0 0 0 0 0 1 0 1 0 0; 0 0 0 0 0 0 1 0 1 0; 0 0 0 0 0 0 0 1 0 1; 0 0 0 0 0 0 0 1 0 1; 1 0 0 0 0 0 0 0 1 0;];                     </pre>	<pre> GRAPH = [ ... 0 1 0 0 0 0 0 0 0 1; 1 0 1 0 0 0 0 0 0 0; 0 1 0 1 0 0 0 0 0 0; 0 0 1 0 1 0 0 0 0 0; 0 0 0 0 1 0 1 0 0 0; 0 0 0 0 1 0 1 0 0 0; 0 0 0 0 0 1 0 1 0 0; 0 0 0 0 0 0 1 0 1 0; 0 0 0 0 0 0 0 1 0 1; 0 0 0 0 0 0 0 1 0 1; 1 0 0 0 0 0 0 0 1 0;];                     </pre>	Laplacian Gain																																																																																																																																				
Error Rate Graph Plot																																																																																																																																							
Results	Raw Data	Convergence Iteration	Global Synchronization Error Rate																																																																																																																																				
	<table border="1"> <tbody> <tr><td>19</td><td>0.0083</td><td>-0.0444</td><td>-0.0114</td><td>0.0018</td><td>0.0061</td><td>0.0075</td><td>0.0080</td><td>0.0081</td><td>0.0081</td><td>0.0081</td></tr> <tr><td>20</td><td>0.0055</td><td>-0.0304</td><td>-0.0074</td><td>0.0014</td><td>0.0042</td><td>0.0051</td><td>0.0054</td><td>0.0054</td><td>0.0054</td><td>0.0054</td></tr> <tr><td>21</td><td>0.0037</td><td>-0.0207</td><td>-0.0048</td><td>9.8231e-04</td><td>0.0028</td><td>0.0035</td><td>0.0036</td><td>0.0036</td><td>0.0036</td><td>0.0036</td></tr> <tr><td>22</td><td>0.0025</td><td>-0.0139</td><td>-0.0032</td><td>7.0203e-04</td><td>0.0019</td><td>0.0023</td><td>0.0024</td><td>0.0024</td><td>0.0024</td><td>0.0024</td></tr> <tr><td>23</td><td>0.0016</td><td>-0.0093</td><td>-0.0021</td><td>4.9830e-04</td><td>0.0013</td><td>0.0015</td><td>0.0016</td><td>0.0016</td><td>0.0016</td><td>0.0016</td></tr> <tr><td>24</td><td>0.0011</td><td>-0.0062</td><td>-0.0013</td><td>3.5241e-04</td><td>8.6930e-04</td><td>0.0010</td><td>0.0011</td><td>0.0011</td><td>0.0011</td><td>0.0011</td></tr> <tr><td>25</td><td>7.0478e-04</td><td>-0.0041</td><td>-8.6715e-04</td><td>2.4840e-04</td><td>5.8162e-04</td><td>6.7829e-04</td><td>6.9774e-04</td><td>7.0092e-04</td><td>7.0122e-04</td><td>7.0122e-04</td></tr> <tr><td>26</td><td>4.6101e-04</td><td>-0.0027</td><td>-5.5687e-04</td><td>1.7420e-04</td><td>3.8710e-04</td><td>4.4603e-04</td><td>4.5730e-04</td><td>4.5903e-04</td><td>4.5919e-04</td><td>4.5919e-04</td></tr> <tr><td>27</td><td>3.0006e-04</td><td>-0.0018</td><td>-3.5470e-04</td><td>1.2151e-04</td><td>2.5610e-04</td><td>2.9165e-04</td><td>2.9811e-04</td><td>2.9905e-04</td><td>2.9913e-04</td><td>2.9913e-04</td></tr> <tr><td>28</td><td>1.9424e-04</td><td>-0.0012</td><td>-2.2389e-04</td><td>8.4026e-05</td><td>1.6830e-04</td><td>1.8954e-04</td><td>1.9321e-04</td><td>1.9372e-04</td><td>1.9376e-04</td><td>1.9376e-04</td></tr> <tr><td>29</td><td>1.2499e-04</td><td>-7.7342e-04</td><td>-1.3997e-04</td><td>5.7556e-05</td><td>1.0981e-04</td><td>1.2237e-04</td><td>1.2445e-04</td><td>1.2472e-04</td><td>1.2474e-04</td><td>1.2474e-04</td></tr> <tr><td>30</td><td>7.9916e-05</td><td>-5.0087e-04</td><td>-8.6652e-05</td><td>3.9014e-05</td><td>7.1104e-05</td><td>7.8474e-05</td><td>7.9638e-05</td><td>7.9783e-05</td><td>7.9794e-05</td><td>7.9794e-05</td></tr> </tbody> </table>	19	0.0083	-0.0444	-0.0114	0.0018	0.0061	0.0075	0.0080	0.0081	0.0081	0.0081	20	0.0055	-0.0304	-0.0074	0.0014	0.0042	0.0051	0.0054	0.0054	0.0054	0.0054	21	0.0037	-0.0207	-0.0048	9.8231e-04	0.0028	0.0035	0.0036	0.0036	0.0036	0.0036	22	0.0025	-0.0139	-0.0032	7.0203e-04	0.0019	0.0023	0.0024	0.0024	0.0024	0.0024	23	0.0016	-0.0093	-0.0021	4.9830e-04	0.0013	0.0015	0.0016	0.0016	0.0016	0.0016	24	0.0011	-0.0062	-0.0013	3.5241e-04	8.6930e-04	0.0010	0.0011	0.0011	0.0011	0.0011	25	7.0478e-04	-0.0041	-8.6715e-04	2.4840e-04	5.8162e-04	6.7829e-04	6.9774e-04	7.0092e-04	7.0122e-04	7.0122e-04	26	4.6101e-04	-0.0027	-5.5687e-04	1.7420e-04	3.8710e-04	4.4603e-04	4.5730e-04	4.5903e-04	4.5919e-04	4.5919e-04	27	3.0006e-04	-0.0018	-3.5470e-04	1.2151e-04	2.5610e-04	2.9165e-04	2.9811e-04	2.9905e-04	2.9913e-04	2.9913e-04	28	1.9424e-04	-0.0012	-2.2389e-04	8.4026e-05	1.6830e-04	1.8954e-04	1.9321e-04	1.9372e-04	1.9376e-04	1.9376e-04	29	1.2499e-04	-7.7342e-04	-1.3997e-04	5.7556e-05	1.0981e-04	1.2237e-04	1.2445e-04	1.2472e-04	1.2474e-04	1.2474e-04	30	7.9916e-05	-5.0087e-04	-8.6652e-05	3.9014e-05	7.1104e-05	7.8474e-05	7.9638e-05	7.9783e-05	7.9794e-05	7.9794e-05	27	29.8025
19	0.0083	-0.0444	-0.0114	0.0018	0.0061	0.0075	0.0080	0.0081	0.0081	0.0081																																																																																																																													
20	0.0055	-0.0304	-0.0074	0.0014	0.0042	0.0051	0.0054	0.0054	0.0054	0.0054																																																																																																																													
21	0.0037	-0.0207	-0.0048	9.8231e-04	0.0028	0.0035	0.0036	0.0036	0.0036	0.0036																																																																																																																													
22	0.0025	-0.0139	-0.0032	7.0203e-04	0.0019	0.0023	0.0024	0.0024	0.0024	0.0024																																																																																																																													
23	0.0016	-0.0093	-0.0021	4.9830e-04	0.0013	0.0015	0.0016	0.0016	0.0016	0.0016																																																																																																																													
24	0.0011	-0.0062	-0.0013	3.5241e-04	8.6930e-04	0.0010	0.0011	0.0011	0.0011	0.0011																																																																																																																													
25	7.0478e-04	-0.0041	-8.6715e-04	2.4840e-04	5.8162e-04	6.7829e-04	6.9774e-04	7.0092e-04	7.0122e-04	7.0122e-04																																																																																																																													
26	4.6101e-04	-0.0027	-5.5687e-04	1.7420e-04	3.8710e-04	4.4603e-04	4.5730e-04	4.5903e-04	4.5919e-04	4.5919e-04																																																																																																																													
27	3.0006e-04	-0.0018	-3.5470e-04	1.2151e-04	2.5610e-04	2.9165e-04	2.9811e-04	2.9905e-04	2.9913e-04	2.9913e-04																																																																																																																													
28	1.9424e-04	-0.0012	-2.2389e-04	8.4026e-05	1.6830e-04	1.8954e-04	1.9321e-04	1.9372e-04	1.9376e-04	1.9376e-04																																																																																																																													
29	1.2499e-04	-7.7342e-04	-1.3997e-04	5.7556e-05	1.0981e-04	1.2237e-04	1.2445e-04	1.2472e-04	1.2474e-04	1.2474e-04																																																																																																																													
30	7.9916e-05	-5.0087e-04	-8.6652e-05	3.9014e-05	7.1104e-05	7.8474e-05	7.9638e-05	7.9783e-05	7.9794e-05	7.9794e-05																																																																																																																													

Laplacian Gain Calculation

Spectrum Laplacian Eigen Value											rho = 2/SSE+LE
No Attack	-4.9 e-16	0.31	0.38	1.16	1.38	2.28	2.61	3.91	3.61	3.30	0.4721

**Experiment 11**

Simulation No.11-a	Ring Mesh 10 Nodes – DoS Attack			GAIN																																																																																																																																				
Input	<pre> GRAPH = [ ... 0 1 0 0 0 0 0 0 0 1; 1 0 1 0 0 0 0 0 0 0; 0 1 0 1 0 0 0 0 0 0; 0 0 1 0 1 0 0 0 0 0; 0 0 0 0 0 1 0 0 0 0; 0 0 0 0 1 0 1 0 0 0; 0 0 0 0 0 1 0 1 0 0; 0 0 0 0 0 0 1 0 1 0; 0 0 0 0 0 0 0 1 0 1; 1 0 0 0 0 0 0 0 1 0;];                     </pre>		<pre> GRAPH1 = [ ... 0 1 0 0 0 0 0 0 0 0; 1 0 1 0 0 0 0 0 0 0; 0 1 0 1 0 0 0 0 0 0; 0 0 1 0 1 0 0 0 0 0; 0 0 0 0 0 1 0 0 0 0; 0 0 0 0 0 1 0 1 0 0; 0 0 0 0 0 0 1 0 1 0; 0 0 0 0 0 0 0 1 0 1; 0 0 0 0 0 0 0 0 1 0; 0 0 0 0 0 0 0 0 0 1;];                     </pre>																																																																																																																																					
Error Rate Graph Plot	 <p>The graph shows the Local Synchronization Error Rate on the y-axis (ranging from -1 to 1.5) against Iterations on the x-axis (ranging from 0 to 50). Ten lines represent different nodes (node 1 to node 10). All lines start with significant fluctuations between -0.5 and 1.5 and converge to a value of 0 by approximately iteration 30. A legend on the right identifies the nodes by color.</p>			No Gain																																																																																																																																				
Results	Raw Data	Convergence Iteration	Global Synchronization Error Rate																																																																																																																																					
	<table border="1"> <tbody> <tr><td>33</td><td>-0.0152</td><td>-0.0039</td><td>5.3069e-04</td><td>0.0021</td><td>0.0026</td><td>0.0027</td><td>0.0028</td><td>0.0028</td><td>0.0028</td><td>0.0028</td></tr> <tr><td>34</td><td>-0.0117</td><td>-0.0029</td><td>4.4648e-04</td><td>0.0016</td><td>0.0020</td><td>0.0021</td><td>0.0021</td><td>0.0021</td><td>0.0021</td><td>0.0021</td></tr> <tr><td>35</td><td>-0.0089</td><td>-0.0021</td><td>3.6789e-04</td><td>0.0012</td><td>0.0015</td><td>0.0016</td><td>0.0016</td><td>0.0016</td><td>0.0016</td><td>0.0016</td></tr> <tr><td>36</td><td>-0.0068</td><td>-0.0016</td><td>2.9858e-04</td><td>9.4086e-04</td><td>0.0011</td><td>0.0012</td><td>0.0012</td><td>0.0012</td><td>0.0012</td><td>0.0012</td></tr> <tr><td>37</td><td>-0.0052</td><td>-0.0012</td><td>2.3959e-04</td><td>7.1557e-04</td><td>8.5779e-04</td><td>8.9912e-04</td><td>9.0805e-04</td><td>9.0962e-04</td><td>9.0979e-04</td><td>9.0980e-04</td></tr> <tr><td>38</td><td>-0.0039</td><td>-8.6906e-04</td><td>1.9055e-04</td><td>5.4251e-04</td><td>6.4618e-04</td><td>6.7552e-04</td><td>6.8167e-04</td><td>6.8271e-04</td><td>6.8281e-04</td><td>6.8282e-04</td></tr> <tr><td>39</td><td>-0.0030</td><td>-6.4141e-04</td><td>1.5048e-04</td><td>4.1008e-04</td><td>4.8536e-04</td><td>5.0609e-04</td><td>5.1030e-04</td><td>5.1099e-04</td><td>5.1106e-04</td><td>5.1106e-04</td></tr> <tr><td>40</td><td>-0.0022</td><td>-4.7232e-04</td><td>1.1813e-04</td><td>3.0909e-04</td><td>3.6353e-04</td><td>3.7813e-04</td><td>3.8100e-04</td><td>3.8145e-04</td><td>3.8149e-04</td><td>3.8150e-04</td></tr> <tr><td>41</td><td>-0.0017</td><td>-3.4697e-04</td><td>9.2259e-05</td><td>2.3231e-04</td><td>2.7153e-04</td><td>2.8176e-04</td><td>2.8371e-04</td><td>2.8401e-04</td><td>2.8404e-04</td><td>2.8404e-04</td></tr> <tr><td>42</td><td>-0.0012</td><td>-2.5421e-04</td><td>7.1715e-05</td><td>1.7411e-04</td><td>2.0226e-04</td><td>2.0939e-04</td><td>2.1072e-04</td><td>2.1091e-04</td><td>2.1093e-04</td><td>2.1093e-04</td></tr> <tr><td>43</td><td>-9.3016e-04</td><td>-1.8573e-04</td><td>5.5502e-05</td><td>1.3013e-04</td><td>1.5024e-04</td><td>1.5521e-04</td><td>1.5610e-04</td><td>1.5623e-04</td><td>1.5624e-04</td><td>1.5624e-04</td></tr> <tr><td>44</td><td>-6.9214e-04</td><td>-1.3530e-04</td><td>4.2773e-05</td><td>9.6982e-05</td><td>1.1130e-04</td><td>1.1474e-04</td><td>1.1534e-04</td><td>1.1543e-04</td><td>1.1543e-04</td><td>1.1543e-04</td></tr> </tbody> </table>	33	-0.0152	-0.0039	5.3069e-04	0.0021	0.0026	0.0027	0.0028	0.0028	0.0028	0.0028	34	-0.0117	-0.0029	4.4648e-04	0.0016	0.0020	0.0021	0.0021	0.0021	0.0021	0.0021	35	-0.0089	-0.0021	3.6789e-04	0.0012	0.0015	0.0016	0.0016	0.0016	0.0016	0.0016	36	-0.0068	-0.0016	2.9858e-04	9.4086e-04	0.0011	0.0012	0.0012	0.0012	0.0012	0.0012	37	-0.0052	-0.0012	2.3959e-04	7.1557e-04	8.5779e-04	8.9912e-04	9.0805e-04	9.0962e-04	9.0979e-04	9.0980e-04	38	-0.0039	-8.6906e-04	1.9055e-04	5.4251e-04	6.4618e-04	6.7552e-04	6.8167e-04	6.8271e-04	6.8281e-04	6.8282e-04	39	-0.0030	-6.4141e-04	1.5048e-04	4.1008e-04	4.8536e-04	5.0609e-04	5.1030e-04	5.1099e-04	5.1106e-04	5.1106e-04	40	-0.0022	-4.7232e-04	1.1813e-04	3.0909e-04	3.6353e-04	3.7813e-04	3.8100e-04	3.8145e-04	3.8149e-04	3.8150e-04	41	-0.0017	-3.4697e-04	9.2259e-05	2.3231e-04	2.7153e-04	2.8176e-04	2.8371e-04	2.8401e-04	2.8404e-04	2.8404e-04	42	-0.0012	-2.5421e-04	7.1715e-05	1.7411e-04	2.0226e-04	2.0939e-04	2.1072e-04	2.1091e-04	2.1093e-04	2.1093e-04	43	-9.3016e-04	-1.8573e-04	5.5502e-05	1.3013e-04	1.5024e-04	1.5521e-04	1.5610e-04	1.5623e-04	1.5624e-04	1.5624e-04	44	-6.9214e-04	-1.3530e-04	4.2773e-05	9.6982e-05	1.1130e-04	1.1474e-04	1.1534e-04	1.1543e-04	1.1543e-04	1.1543e-04	41	36.0375	
33	-0.0152	-0.0039	5.3069e-04	0.0021	0.0026	0.0027	0.0028	0.0028	0.0028	0.0028																																																																																																																														
34	-0.0117	-0.0029	4.4648e-04	0.0016	0.0020	0.0021	0.0021	0.0021	0.0021	0.0021																																																																																																																														
35	-0.0089	-0.0021	3.6789e-04	0.0012	0.0015	0.0016	0.0016	0.0016	0.0016	0.0016																																																																																																																														
36	-0.0068	-0.0016	2.9858e-04	9.4086e-04	0.0011	0.0012	0.0012	0.0012	0.0012	0.0012																																																																																																																														
37	-0.0052	-0.0012	2.3959e-04	7.1557e-04	8.5779e-04	8.9912e-04	9.0805e-04	9.0962e-04	9.0979e-04	9.0980e-04																																																																																																																														
38	-0.0039	-8.6906e-04	1.9055e-04	5.4251e-04	6.4618e-04	6.7552e-04	6.8167e-04	6.8271e-04	6.8281e-04	6.8282e-04																																																																																																																														
39	-0.0030	-6.4141e-04	1.5048e-04	4.1008e-04	4.8536e-04	5.0609e-04	5.1030e-04	5.1099e-04	5.1106e-04	5.1106e-04																																																																																																																														
40	-0.0022	-4.7232e-04	1.1813e-04	3.0909e-04	3.6353e-04	3.7813e-04	3.8100e-04	3.8145e-04	3.8149e-04	3.8150e-04																																																																																																																														
41	-0.0017	-3.4697e-04	9.2259e-05	2.3231e-04	2.7153e-04	2.8176e-04	2.8371e-04	2.8401e-04	2.8404e-04	2.8404e-04																																																																																																																														
42	-0.0012	-2.5421e-04	7.1715e-05	1.7411e-04	2.0226e-04	2.0939e-04	2.1072e-04	2.1091e-04	2.1093e-04	2.1093e-04																																																																																																																														
43	-9.3016e-04	-1.8573e-04	5.5502e-05	1.3013e-04	1.5024e-04	1.5521e-04	1.5610e-04	1.5623e-04	1.5624e-04	1.5624e-04																																																																																																																														
44	-6.9214e-04	-1.3530e-04	4.2773e-05	9.6982e-05	1.1130e-04	1.1474e-04	1.1534e-04	1.1543e-04	1.1543e-04	1.1543e-04																																																																																																																														

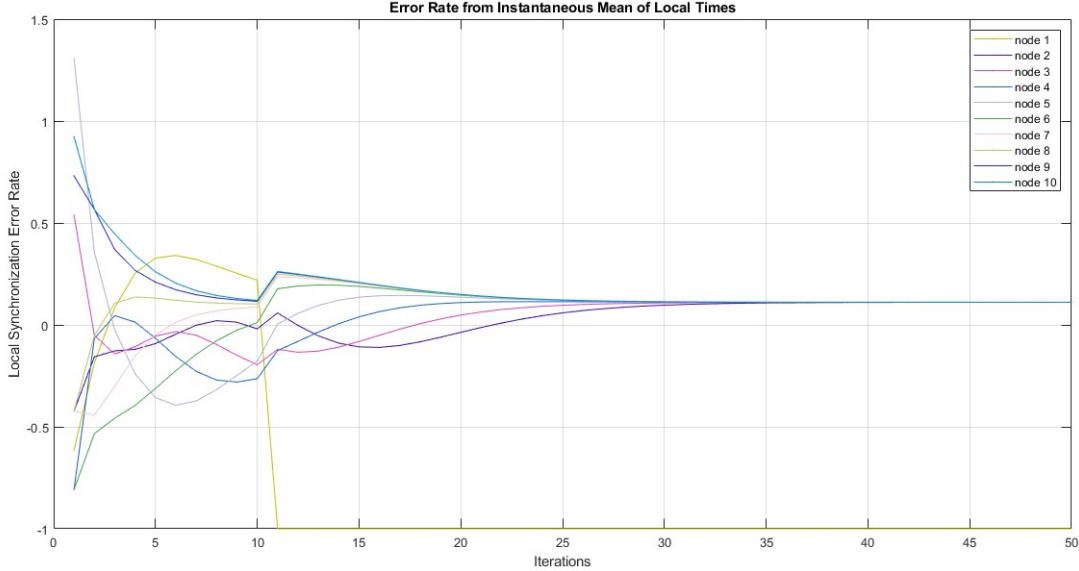
Simulation No.11-b	Ring Mesh 10 Nodes – DoS Attack		GAIN																																																																																																																																			
Input	<pre> GRAPH = [ ... 0 1 0 0 0 0 0 0 0 1; 1 0 1 0 0 0 0 0 0 0; 0 1 0 1 0 0 0 0 0 0; 0 0 1 0 1 0 0 0 0 0; 0 0 0 0 1 0 1 0 0 0; 0 0 0 0 1 0 1 0 0 0; 0 0 0 0 0 1 0 1 0 0; 0 0 0 0 0 0 1 0 1 0; 0 0 0 0 0 0 0 1 0 1; 0 0 0 0 0 0 0 1 0 1; 1 0 0 0 0 0 0 0 1 0;];                     </pre>	<pre> GRAPH1 = [ ... 0 1 0 0 0 0 0 0 0 0; 1 0 1 0 0 0 0 0 0 0; 0 1 0 1 0 0 0 0 0 0; 0 0 1 0 1 0 0 0 0 0; 0 0 0 0 1 0 1 0 0 0; 0 0 0 0 1 0 1 0 0 0; 0 0 0 0 0 1 0 1 0 0; 0 0 0 0 0 0 1 0 1 0; 0 0 0 0 0 0 0 1 0 1; 0 0 0 0 0 0 0 1 0 1; 0 0 0 0 0 0 0 0 1 0;];                     </pre>																																																																																																																																				
Error Rate Graph Plot			Laplacian Gain																																																																																																																																			
Results	Raw Data	Convergence Iteration	Global Synchronization Error Rate																																																																																																																																			
	<table border="1"> <tbody> <tr><td>27</td><td>-0.0177</td><td>-0.0044</td><td>6.6713e-04</td><td>0.0024</td><td>0.0030</td><td>0.0032</td><td>0.0032</td><td>0.0032</td><td>0.0032</td><td>0.0032</td></tr> <tr><td>28</td><td>-0.0131</td><td>-0.0031</td><td>5.3736e-04</td><td>0.0010</td><td>0.0022</td><td>0.0023</td><td>0.0023</td><td>0.0023</td><td>0.0023</td><td>0.0023</td></tr> <tr><td>29</td><td>-0.0096</td><td>-0.0022</td><td>4.2451e-04</td><td>0.0013</td><td>0.0016</td><td>0.0017</td><td>0.0017</td><td>0.0017</td><td>0.0017</td><td>0.0017</td></tr> <tr><td>30</td><td>-0.0071</td><td>-0.0016</td><td>3.3061e-04</td><td>9.7729e-04</td><td>0.0012</td><td>0.0012</td><td>0.0012</td><td>0.0012</td><td>0.0012</td><td>0.0012</td></tr> <tr><td>31</td><td>-0.0051</td><td>-0.0011</td><td>2.5520e-04</td><td>7.1431e-04</td><td>8.4750e-04</td><td>8.8435e-04</td><td>8.9156e-04</td><td>8.9270e-04</td><td>8.9281e-04</td><td>8.9281e-04</td></tr> <tr><td>32</td><td>-0.0037</td><td>-7.9914e-04</td><td>1.9531e-04</td><td>5.2022e-04</td><td>6.1253e-04</td><td>6.3722e-04</td><td>6.4187e-04</td><td>6.4258e-04</td><td>6.4264e-04</td><td>6.4265e-04</td></tr> <tr><td>33</td><td>-0.0027</td><td>-5.6456e-04</td><td>1.4849e-04</td><td>3.7753e-04</td><td>4.4116e-04</td><td>4.5761e-04</td><td>4.6061e-04</td><td>4.6105e-04</td><td>4.6108e-04</td><td>4.6108e-04</td></tr> <tr><td>34</td><td>-0.0020</td><td>-3.9748e-04</td><td>1.1222e-04</td><td>2.7300e-04</td><td>3.1663e-04</td><td>3.2754e-04</td><td>3.2946e-04</td><td>3.2973e-04</td><td>3.2975e-04</td><td>3.2975e-04</td></tr> <tr><td>35</td><td>-0.0014</td><td>-2.7880e-04</td><td>8.4328e-05</td><td>1.9670e-04</td><td>2.2646e-04</td><td>2.3366e-04</td><td>2.3488e-04</td><td>2.3505e-04</td><td>2.3506e-04</td><td>2.3506e-04</td></tr> <tr><td>36</td><td>-0.0010</td><td>-1.9477e-04</td><td>6.3019e-05</td><td>1.4121e-04</td><td>1.6140e-04</td><td>1.6612e-04</td><td>1.6690e-04</td><td>1.6700e-04</td><td>1.6701e-04</td><td>1.6701e-04</td></tr> <tr><td>37</td><td>-7.1761e-04</td><td>-1.3549e-04</td><td>4.6834e-05</td><td>1.0098e-04</td><td>1.1462e-04</td><td>1.1770e-04</td><td>1.1819e-04</td><td>1.1825e-04</td><td>1.1826e-04</td><td>1.1826e-04</td></tr> <tr><td>38</td><td>-5.1069e-04</td><td>-9.3828e-05</td><td>3.4611e-05</td><td>7.1938e-05</td><td>8.1096e-05</td><td>8.3103e-05</td><td>8.3413e-05</td><td>8.3451e-05</td><td>8.3454e-05</td><td>8.3454e-05</td></tr> </tbody> </table>	27	-0.0177	-0.0044	6.6713e-04	0.0024	0.0030	0.0032	0.0032	0.0032	0.0032	0.0032	28	-0.0131	-0.0031	5.3736e-04	0.0010	0.0022	0.0023	0.0023	0.0023	0.0023	0.0023	29	-0.0096	-0.0022	4.2451e-04	0.0013	0.0016	0.0017	0.0017	0.0017	0.0017	0.0017	30	-0.0071	-0.0016	3.3061e-04	9.7729e-04	0.0012	0.0012	0.0012	0.0012	0.0012	0.0012	31	-0.0051	-0.0011	2.5520e-04	7.1431e-04	8.4750e-04	8.8435e-04	8.9156e-04	8.9270e-04	8.9281e-04	8.9281e-04	32	-0.0037	-7.9914e-04	1.9531e-04	5.2022e-04	6.1253e-04	6.3722e-04	6.4187e-04	6.4258e-04	6.4264e-04	6.4265e-04	33	-0.0027	-5.6456e-04	1.4849e-04	3.7753e-04	4.4116e-04	4.5761e-04	4.6061e-04	4.6105e-04	4.6108e-04	4.6108e-04	34	-0.0020	-3.9748e-04	1.1222e-04	2.7300e-04	3.1663e-04	3.2754e-04	3.2946e-04	3.2973e-04	3.2975e-04	3.2975e-04	35	-0.0014	-2.7880e-04	8.4328e-05	1.9670e-04	2.2646e-04	2.3366e-04	2.3488e-04	2.3505e-04	2.3506e-04	2.3506e-04	36	-0.0010	-1.9477e-04	6.3019e-05	1.4121e-04	1.6140e-04	1.6612e-04	1.6690e-04	1.6700e-04	1.6701e-04	1.6701e-04	37	-7.1761e-04	-1.3549e-04	4.6834e-05	1.0098e-04	1.1462e-04	1.1770e-04	1.1819e-04	1.1825e-04	1.1826e-04	1.1826e-04	38	-5.1069e-04	-9.3828e-05	3.4611e-05	7.1938e-05	8.1096e-05	8.3103e-05	8.3413e-05	8.3451e-05	8.3454e-05	8.3454e-05	35
27	-0.0177	-0.0044	6.6713e-04	0.0024	0.0030	0.0032	0.0032	0.0032	0.0032	0.0032																																																																																																																												
28	-0.0131	-0.0031	5.3736e-04	0.0010	0.0022	0.0023	0.0023	0.0023	0.0023	0.0023																																																																																																																												
29	-0.0096	-0.0022	4.2451e-04	0.0013	0.0016	0.0017	0.0017	0.0017	0.0017	0.0017																																																																																																																												
30	-0.0071	-0.0016	3.3061e-04	9.7729e-04	0.0012	0.0012	0.0012	0.0012	0.0012	0.0012																																																																																																																												
31	-0.0051	-0.0011	2.5520e-04	7.1431e-04	8.4750e-04	8.8435e-04	8.9156e-04	8.9270e-04	8.9281e-04	8.9281e-04																																																																																																																												
32	-0.0037	-7.9914e-04	1.9531e-04	5.2022e-04	6.1253e-04	6.3722e-04	6.4187e-04	6.4258e-04	6.4264e-04	6.4265e-04																																																																																																																												
33	-0.0027	-5.6456e-04	1.4849e-04	3.7753e-04	4.4116e-04	4.5761e-04	4.6061e-04	4.6105e-04	4.6108e-04	4.6108e-04																																																																																																																												
34	-0.0020	-3.9748e-04	1.1222e-04	2.7300e-04	3.1663e-04	3.2754e-04	3.2946e-04	3.2973e-04	3.2975e-04	3.2975e-04																																																																																																																												
35	-0.0014	-2.7880e-04	8.4328e-05	1.9670e-04	2.2646e-04	2.3366e-04	2.3488e-04	2.3505e-04	2.3506e-04	2.3506e-04																																																																																																																												
36	-0.0010	-1.9477e-04	6.3019e-05	1.4121e-04	1.6140e-04	1.6612e-04	1.6690e-04	1.6700e-04	1.6701e-04	1.6701e-04																																																																																																																												
37	-7.1761e-04	-1.3549e-04	4.6834e-05	1.0098e-04	1.1462e-04	1.1770e-04	1.1819e-04	1.1825e-04	1.1826e-04	1.1826e-04																																																																																																																												
38	-5.1069e-04	-9.3828e-05	3.4611e-05	7.1938e-05	8.1096e-05	8.3103e-05	8.3413e-05	8.3451e-05	8.3454e-05	8.3454e-05																																																																																																																												

**Laplacian Gain Calculation**

Spectrum Laplacian Eigen Value											rho = 2/SSE+LE
Before Attack	-4.9 e-16	0.31	0.38	1.16	1.38	2.28	2.61	3.91	3.61	3.30	0.4721
After Attack	0.12	3.53	2.34	1	3.73	3	2	1	-2.3 e-17	0.26	0.5582



**Experiment 12**

Simulation No.12-a	Ring Mesh 10 Nodes – Node Destruction Attack			GAIN																																																																																																																																			
Input	<pre> GRAPH = [ ... 0 1 0 0 0 0 0 0 0 1; 1 0 1 0 0 0 0 0 0 0; 0 1 0 1 0 0 0 0 0 0; 0 0 1 0 1 0 0 0 0 0; 0 0 0 0 0 1 0 0 0 0; 0 0 0 0 1 0 1 0 0 0; 0 0 0 0 0 1 0 1 0 0; 0 0 0 0 0 0 1 0 1 0; 0 0 0 0 0 0 0 1 0 1; 1 0 0 0 0 0 0 0 1 0;];                     </pre>	<pre> GRAPH1 = [ ... 0 0 0 0 0 0 0 0 0 0; 0 0 1 0 0 0 0 0 0 0; 0 1 0 1 0 0 0 0 0 0; 0 0 1 0 1 0 0 0 0 0; 0 0 0 0 0 1 0 0 0 0; 0 0 0 0 0 1 0 0 0 0; 0 0 0 0 1 0 1 0 0 0; 0 0 0 0 0 1 0 1 0 0; 0 0 0 0 0 0 1 0 1 0; 0 0 0 0 0 0 0 1 0 1; 0 0 0 0 0 0 0 0 1 0;];                     </pre>																																																																																																																																					
Error Rate Graph Plot				No Gain																																																																																																																																			
Results	Raw Data	Convergence Iteration	Global Synchronization Error Rate																																																																																																																																				
	<table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr><td>37</td><td>-1</td><td>0.1092</td><td>0.1107</td><td>0.1113</td><td>0.1114</td><td>0.1115</td><td>0.1115</td><td>0.1115</td><td>0.1115</td><td>0.1115</td></tr> <tr><td>38</td><td>-1</td><td>0.1097</td><td>0.1108</td><td>0.1112</td><td>0.1113</td><td>0.1114</td><td>0.1114</td><td>0.1114</td><td>0.1114</td><td>0.1114</td></tr> <tr><td>39</td><td>-1</td><td>0.1100</td><td>0.1109</td><td>0.1112</td><td>0.1113</td><td>0.1113</td><td>0.1113</td><td>0.1113</td><td>0.1113</td><td>0.1113</td></tr> <tr><td>40</td><td>-1</td><td>0.1103</td><td>0.1110</td><td>0.1112</td><td>0.1112</td><td>0.1113</td><td>0.1113</td><td>0.1113</td><td>0.1113</td><td>0.1113</td></tr> <tr><td>41</td><td>-1</td><td>0.1105</td><td>0.1110</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td></tr> <tr><td>42</td><td>-1</td><td>0.1107</td><td>0.1110</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td></tr> <tr><td>43</td><td>-1</td><td>0.1108</td><td>0.1111</td><td>0.1111</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td></tr> <tr><td>44</td><td>-1</td><td>0.1109</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td></tr> <tr><td>45</td><td>-1</td><td>0.1109</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> <tr style="background-color: #e0f0ff;"><td>46</td><td>-1</td><td>0.1110</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> <tr><td>47</td><td>-1</td><td>0.1110</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> <tr><td>48</td><td>-1</td><td>0.1110</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> </tbody> </table>	37	-1	0.1092	0.1107	0.1113	0.1114	0.1115	0.1115	0.1115	0.1115	0.1115	38	-1	0.1097	0.1108	0.1112	0.1113	0.1114	0.1114	0.1114	0.1114	0.1114	39	-1	0.1100	0.1109	0.1112	0.1113	0.1113	0.1113	0.1113	0.1113	0.1113	40	-1	0.1103	0.1110	0.1112	0.1112	0.1113	0.1113	0.1113	0.1113	0.1113	41	-1	0.1105	0.1110	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112	42	-1	0.1107	0.1110	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112	43	-1	0.1108	0.1111	0.1111	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112	44	-1	0.1109	0.1111	0.1111	0.1111	0.1112	0.1112	0.1112	0.1112	0.1112	45	-1	0.1109	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	46	-1	0.1110	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	47	-1	0.1110	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	48	-1	0.1110	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	46	106.5954
37	-1	0.1092	0.1107	0.1113	0.1114	0.1115	0.1115	0.1115	0.1115	0.1115																																																																																																																													
38	-1	0.1097	0.1108	0.1112	0.1113	0.1114	0.1114	0.1114	0.1114	0.1114																																																																																																																													
39	-1	0.1100	0.1109	0.1112	0.1113	0.1113	0.1113	0.1113	0.1113	0.1113																																																																																																																													
40	-1	0.1103	0.1110	0.1112	0.1112	0.1113	0.1113	0.1113	0.1113	0.1113																																																																																																																													
41	-1	0.1105	0.1110	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112																																																																																																																													
42	-1	0.1107	0.1110	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112																																																																																																																													
43	-1	0.1108	0.1111	0.1111	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112																																																																																																																													
44	-1	0.1109	0.1111	0.1111	0.1111	0.1112	0.1112	0.1112	0.1112	0.1112																																																																																																																													
45	-1	0.1109	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111																																																																																																																													
46	-1	0.1110	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111																																																																																																																													
47	-1	0.1110	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111																																																																																																																													
48	-1	0.1110	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111																																																																																																																													

Simulation No.12-b	Ring Mesh 10 Nodes – Node Destruction Attack			GAIN																																																																																																																																			
Input	<pre> GRAPH = [ ... 0 1 0 0 0 0 0 0 0 1; 1 0 1 0 0 0 0 0 0 0; 0 1 0 1 0 0 0 0 0 0; 0 0 1 0 1 0 0 0 0 0; 0 0 0 0 1 0 1 0 0 0; 0 0 0 0 1 0 1 0 0 0; 0 0 0 0 0 1 0 1 0 0; 0 0 0 0 0 0 1 0 1 0; 0 0 0 0 0 0 0 1 0 1; 0 0 0 0 0 0 0 0 1 0; 1 0 0 0 0 0 0 0 1 0;];                     </pre>	<pre> GRAPH1 = [ ... 0 0 0 0 0 0 0 0 0 0; 0 0 1 0 0 0 0 0 0 0; 0 1 0 1 0 0 0 0 0 0; 0 0 1 0 1 0 0 0 0 0; 0 0 0 0 1 0 1 0 0 0; 0 0 0 0 1 0 1 0 0 0; 0 0 0 0 0 1 0 1 0 0; 0 0 0 0 0 0 1 0 1 0; 0 0 0 0 0 0 0 1 0 1; 0 0 0 0 0 0 0 0 1 0; 0 0 0 0 0 0 0 0 1 0;];                     </pre>																																																																																																																																					
Error Rate Graph Plot	<p style="text-align: center;">Error Rate from Instantaneous Mean of Local Times</p>			Laplacian Gain																																																																																																																																			
Results	Raw Data	Convergence Iteration	Global Synchronization Error Rate																																																																																																																																				
	<table border="1"> <tbody> <tr><td>27</td><td>-1</td><td>0.1060</td><td>0.1101</td><td>0.1115</td><td>0.1119</td><td>0.1121</td><td>0.1121</td><td>0.1121</td><td>0.1121</td><td>0.1121</td></tr> <tr><td>28</td><td>-1</td><td>0.1075</td><td>0.1104</td><td>0.1114</td><td>0.1117</td><td>0.1118</td><td>0.1118</td><td>0.1118</td><td>0.1118</td><td>0.1118</td></tr> <tr><td>29</td><td>-1</td><td>0.1086</td><td>0.1106</td><td>0.1113</td><td>0.1115</td><td>0.1116</td><td>0.1116</td><td>0.1116</td><td>0.1116</td><td>0.1116</td></tr> <tr><td>30</td><td>-1</td><td>0.1093</td><td>0.1108</td><td>0.1113</td><td>0.1114</td><td>0.1114</td><td>0.1114</td><td>0.1114</td><td>0.1114</td><td>0.1114</td></tr> <tr><td>31</td><td>-1</td><td>0.1099</td><td>0.1109</td><td>0.1112</td><td>0.1113</td><td>0.1113</td><td>0.1113</td><td>0.1113</td><td>0.1113</td><td>0.1113</td></tr> <tr><td>32</td><td>-1</td><td>0.1102</td><td>0.1110</td><td>0.1112</td><td>0.1113</td><td>0.1113</td><td>0.1113</td><td>0.1113</td><td>0.1113</td><td>0.1113</td></tr> <tr><td>33</td><td>-1</td><td>0.1105</td><td>0.1110</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td></tr> <tr><td>34</td><td>-1</td><td>0.1107</td><td>0.1110</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td></tr> <tr><td>35</td><td>-1</td><td>0.1108</td><td>0.1111</td><td>0.1111</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td><td>0.1112</td></tr> <tr><td>36</td><td>-1</td><td>0.1109</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> <tr style="background-color: #e0f0ff;"><td>37</td><td>-1</td><td>0.1110</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> <tr><td>38</td><td>-1</td><td>0.1110</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> </tbody> </table>	27	-1	0.1060	0.1101	0.1115	0.1119	0.1121	0.1121	0.1121	0.1121	0.1121	28	-1	0.1075	0.1104	0.1114	0.1117	0.1118	0.1118	0.1118	0.1118	0.1118	29	-1	0.1086	0.1106	0.1113	0.1115	0.1116	0.1116	0.1116	0.1116	0.1116	30	-1	0.1093	0.1108	0.1113	0.1114	0.1114	0.1114	0.1114	0.1114	0.1114	31	-1	0.1099	0.1109	0.1112	0.1113	0.1113	0.1113	0.1113	0.1113	0.1113	32	-1	0.1102	0.1110	0.1112	0.1113	0.1113	0.1113	0.1113	0.1113	0.1113	33	-1	0.1105	0.1110	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112	34	-1	0.1107	0.1110	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112	35	-1	0.1108	0.1111	0.1111	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112	36	-1	0.1109	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	37	-1	0.1110	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	38	-1	0.1110	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	37	106.7254
27	-1	0.1060	0.1101	0.1115	0.1119	0.1121	0.1121	0.1121	0.1121	0.1121																																																																																																																													
28	-1	0.1075	0.1104	0.1114	0.1117	0.1118	0.1118	0.1118	0.1118	0.1118																																																																																																																													
29	-1	0.1086	0.1106	0.1113	0.1115	0.1116	0.1116	0.1116	0.1116	0.1116																																																																																																																													
30	-1	0.1093	0.1108	0.1113	0.1114	0.1114	0.1114	0.1114	0.1114	0.1114																																																																																																																													
31	-1	0.1099	0.1109	0.1112	0.1113	0.1113	0.1113	0.1113	0.1113	0.1113																																																																																																																													
32	-1	0.1102	0.1110	0.1112	0.1113	0.1113	0.1113	0.1113	0.1113	0.1113																																																																																																																													
33	-1	0.1105	0.1110	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112																																																																																																																													
34	-1	0.1107	0.1110	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112																																																																																																																													
35	-1	0.1108	0.1111	0.1111	0.1112	0.1112	0.1112	0.1112	0.1112	0.1112																																																																																																																													
36	-1	0.1109	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111																																																																																																																													
37	-1	0.1110	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111																																																																																																																													
38	-1	0.1110	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111																																																																																																																													

**Laplacian Gain Calculation**

	Spectrum Laplacian Eigen Value										rho = 2/SSE+LE
Before Attack	-4.9 e-16	0.31	0.38	1.16	1.38	2.28	2.61	3.91	3.61	3.30	0.4721
After Attack	3.73	3.24	3	2	1.55	1	-8.5 e-17	0.19	0.26	0	0.5102

**Experiment 13**

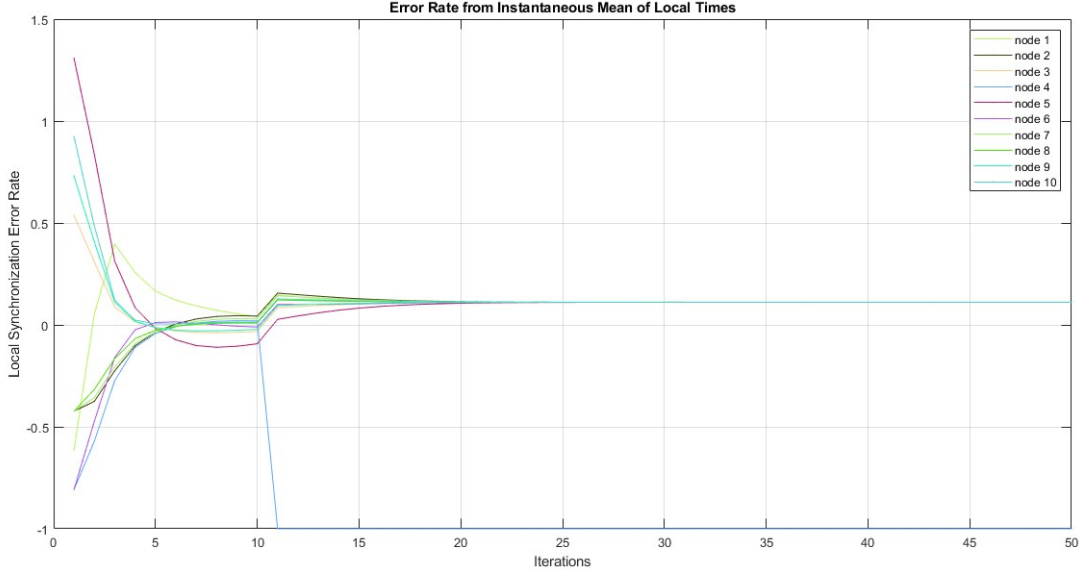
Simulation No.13-a	Star 10 Nodes – No Attack			GAIN																																																																																																																																			
Input	<pre> GRAPH = [ ...   0  1  1  1  1  1  1  1  1  1;   1  0  0  0  0  0  0  0  0  0;   1  0  0  0  0  0  0  0  0  0;   1  0  0  0  0  0  0  0  0  0;   1  0  0  0  0  0  0  0  0  0;   1  0  0  0  0  0  0  0  0  0;   1  0  0  0  0  0  0  0  0  0;   1  0  0  0  0  0  0  0  0  0;   1  0  0  0  0  0  0  0  0  0;   1  0  0  0  0  0  0  0  0  0;   1  0  0  0  0  0  0  0  0  0;   1  0  0  0  0  0  0  0  0;];                     </pre>		<pre> GRAPH = [ ...   0  1  1  1  1  1  1  1  1  1;   1  0  0  0  0  0  0  0  0  0;   1  0  0  0  0  0  0  0  0  0;   1  0  0  0  0  0  0  0  0  0;   1  0  0  0  0  0  0  0  0  0;   1  0  0  0  0  0  0  0  0  0;   1  0  0  0  0  0  0  0  0  0;   1  0  0  0  0  0  0  0  0  0;   1  0  0  0  0  0  0  0  0  0;   1  0  0  0  0  0  0  0  0  0;   1  0  0  0  0  0  0  0  0  0;   1  0  0  0  0  0  0  0  0;];                     </pre>																																																																																																																																				
Error Rate Graph Plot				No Gain																																																																																																																																			
Results	Raw Data	Convergence Iteration	Global Synchronization Error Rate																																																																																																																																				
	<table border="1"> <tbody> <tr><td>16</td><td>0.0056</td><td>0.0109</td><td>-0.0065</td><td>0.0049</td><td>-0.0193</td><td>-0.0057</td><td>0.0077</td><td>0.0020</td><td>-0.0037</td><td>0.0041</td></tr> <tr><td>17</td><td>0.0039</td><td>0.0079</td><td>-0.0046</td><td>0.0035</td><td>-0.0138</td><td>-0.0044</td><td>0.0055</td><td>0.0014</td><td>-0.0026</td><td>0.0030</td></tr> <tr><td>18</td><td>0.0027</td><td>0.0056</td><td>-0.0032</td><td>0.0025</td><td>-0.0097</td><td>-0.0032</td><td>0.0040</td><td>0.0010</td><td>-0.0018</td><td>0.0022</td></tr> <tr><td>19</td><td>0.0019</td><td>0.0040</td><td>-0.0023</td><td>0.0018</td><td>-0.0068</td><td>-0.0024</td><td>0.0028</td><td>7.0414e-04</td><td>-0.0012</td><td>0.0015</td></tr> <tr><td>20</td><td>0.0013</td><td>0.0028</td><td>-0.0016</td><td>0.0012</td><td>-0.0047</td><td>-0.0017</td><td>0.0019</td><td>4.8302e-04</td><td>-8.4460e-04</td><td>0.0011</td></tr> <tr><td>21</td><td>8.7307e-04</td><td>0.0019</td><td>-0.0011</td><td>8.3670e-04</td><td>-0.0032</td><td>-0.0012</td><td>0.0013</td><td>3.2841e-04</td><td>-5.6984e-04</td><td>7.5241e-04</td></tr> <tr><td>22</td><td>5.8970e-04</td><td>0.0013</td><td>-7.2246e-04</td><td>5.6982e-04</td><td>-0.0022</td><td>-8.5060e-04</td><td>9.1407e-04</td><td>2.2157e-04</td><td>-3.8190e-04</td><td>5.1700e-04</td></tr> <tr><td>23</td><td>3.9608e-04</td><td>8.8136e-04</td><td>-4.8668e-04</td><td>3.8524e-04</td><td>-0.0015</td><td>-5.9065e-04</td><td>6.2009e-04</td><td>1.4847e-04</td><td>-2.5442e-04</td><td>3.5228e-04</td></tr> <tr><td>24</td><td>2.6464e-04</td><td>5.9380e-04</td><td>-3.2583e-04</td><td>2.5876e-04</td><td>-9.7129e-04</td><td>-4.0644e-04</td><td>4.1780e-04</td><td>9.8883e-05</td><td>-1.6858e-04</td><td>2.3826e-04</td></tr> <tr><td>25</td><td>1.7596e-04</td><td>3.9762e-04</td><td>-2.1693e-04</td><td>1.7278e-04</td><td>-6.4622e-04</td><td>-2.7742e-04</td><td>2.7978e-04</td><td>6.5501e-05</td><td>-1.1115e-04</td><td>1.6008e-04</td></tr> <tr><td>26</td><td>1.1647e-04</td><td>2.6479e-04</td><td>-1.4370e-04</td><td>1.1477e-04</td><td>-4.2778e-04</td><td>-1.8800e-04</td><td>1.8632e-04</td><td>4.3178e-05</td><td>-7.2967e-05</td><td>1.0692e-04</td></tr> <tr><td>27</td><td>7.6777e-05</td><td>1.7545e-04</td><td>-9.4750e-05</td><td>7.5866e-05</td><td>-2.8188e-04</td><td>-1.2658e-04</td><td>1.2346e-04</td><td>2.8336e-05</td><td>-4.7706e-05</td><td>7.1024e-05</td></tr> </tbody> </table>	16	0.0056	0.0109	-0.0065	0.0049	-0.0193	-0.0057	0.0077	0.0020	-0.0037	0.0041	17	0.0039	0.0079	-0.0046	0.0035	-0.0138	-0.0044	0.0055	0.0014	-0.0026	0.0030	18	0.0027	0.0056	-0.0032	0.0025	-0.0097	-0.0032	0.0040	0.0010	-0.0018	0.0022	19	0.0019	0.0040	-0.0023	0.0018	-0.0068	-0.0024	0.0028	7.0414e-04	-0.0012	0.0015	20	0.0013	0.0028	-0.0016	0.0012	-0.0047	-0.0017	0.0019	4.8302e-04	-8.4460e-04	0.0011	21	8.7307e-04	0.0019	-0.0011	8.3670e-04	-0.0032	-0.0012	0.0013	3.2841e-04	-5.6984e-04	7.5241e-04	22	5.8970e-04	0.0013	-7.2246e-04	5.6982e-04	-0.0022	-8.5060e-04	9.1407e-04	2.2157e-04	-3.8190e-04	5.1700e-04	23	3.9608e-04	8.8136e-04	-4.8668e-04	3.8524e-04	-0.0015	-5.9065e-04	6.2009e-04	1.4847e-04	-2.5442e-04	3.5228e-04	24	2.6464e-04	5.9380e-04	-3.2583e-04	2.5876e-04	-9.7129e-04	-4.0644e-04	4.1780e-04	9.8883e-05	-1.6858e-04	2.3826e-04	25	1.7596e-04	3.9762e-04	-2.1693e-04	1.7278e-04	-6.4622e-04	-2.7742e-04	2.7978e-04	6.5501e-05	-1.1115e-04	1.6008e-04	26	1.1647e-04	2.6479e-04	-1.4370e-04	1.1477e-04	-4.2778e-04	-1.8800e-04	1.8632e-04	4.3178e-05	-7.2967e-05	1.0692e-04	27	7.6777e-05	1.7545e-04	-9.4750e-05	7.5866e-05	-2.8188e-04	-1.2658e-04	1.2346e-04	2.8336e-05	-4.7706e-05	7.1024e-05	23	17.1558
16	0.0056	0.0109	-0.0065	0.0049	-0.0193	-0.0057	0.0077	0.0020	-0.0037	0.0041																																																																																																																													
17	0.0039	0.0079	-0.0046	0.0035	-0.0138	-0.0044	0.0055	0.0014	-0.0026	0.0030																																																																																																																													
18	0.0027	0.0056	-0.0032	0.0025	-0.0097	-0.0032	0.0040	0.0010	-0.0018	0.0022																																																																																																																													
19	0.0019	0.0040	-0.0023	0.0018	-0.0068	-0.0024	0.0028	7.0414e-04	-0.0012	0.0015																																																																																																																													
20	0.0013	0.0028	-0.0016	0.0012	-0.0047	-0.0017	0.0019	4.8302e-04	-8.4460e-04	0.0011																																																																																																																													
21	8.7307e-04	0.0019	-0.0011	8.3670e-04	-0.0032	-0.0012	0.0013	3.2841e-04	-5.6984e-04	7.5241e-04																																																																																																																													
22	5.8970e-04	0.0013	-7.2246e-04	5.6982e-04	-0.0022	-8.5060e-04	9.1407e-04	2.2157e-04	-3.8190e-04	5.1700e-04																																																																																																																													
23	3.9608e-04	8.8136e-04	-4.8668e-04	3.8524e-04	-0.0015	-5.9065e-04	6.2009e-04	1.4847e-04	-2.5442e-04	3.5228e-04																																																																																																																													
24	2.6464e-04	5.9380e-04	-3.2583e-04	2.5876e-04	-9.7129e-04	-4.0644e-04	4.1780e-04	9.8883e-05	-1.6858e-04	2.3826e-04																																																																																																																													
25	1.7596e-04	3.9762e-04	-2.1693e-04	1.7278e-04	-6.4622e-04	-2.7742e-04	2.7978e-04	6.5501e-05	-1.1115e-04	1.6008e-04																																																																																																																													
26	1.1647e-04	2.6479e-04	-1.4370e-04	1.1477e-04	-4.2778e-04	-1.8800e-04	1.8632e-04	4.3178e-05	-7.2967e-05	1.0692e-04																																																																																																																													
27	7.6777e-05	1.7545e-04	-9.4750e-05	7.5866e-05	-2.8188e-04	-1.2658e-04	1.2346e-04	2.8336e-05	-4.7706e-05	7.1024e-05																																																																																																																													

Simulation No.13-b	Star 10 Nodes – No Attack		GAIN																	
Input	GRAPH = [ ... 0 1 1 1 1 1 1 1 1 1; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0;];	GRAPH = [ ... 0 1 1 1 1 1 1 1 1 1; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0;];																		
	<p>Error Rate from Instantaneous Mean of Local Times</p>		Laplacian Gain																	
Results	<table border="1"> <thead> <tr> <th>Raw Data</th> <th>Convergence Iteration</th> <th>Global Synchronization Error Rate</th> </tr> </thead> <tbody> <tr> <td>16 -0.0338 0.0037 0.0038 0.0035 0.0039 0.0035 0.0037 0.0036 0.0039 0.0041</td> <td rowspan="14">24</td> <td rowspan="14">27.6860</td> </tr> <tr> <td>17 0.0234 -0.0026 -0.0027 -0.0024 -0.0027 -0.0024 -0.0025 -0.0025 -0.0027 -0.0028</td> </tr> <tr> <td>18 -0.0155 0.0017 0.0018 0.0016 0.0018 0.0016 0.0017 0.0017 0.0018 0.0019</td> </tr> <tr> <td>19 0.0105 -0.0012 -0.0012 -0.0011 -0.0012 -0.0011 -0.0011 -0.0011 -0.0012 -0.0013</td> </tr> <tr> <td>20 -0.0070 7.6682e-04 7.8509e-04 7.3665e-04 7.9554e-04 7.3279e-04 7.6107e-04 7.5341e-04 7.9899e-04 8.2714e-04</td> </tr> <tr> <td>21 0.0047 -5.1402e-04 -5.2534e-04 -4.9535e-04 -5.3181e-04 -4.9295e-04 -5.1046e-04 -5.0572e-04 -5.3394e-04 -5.5137e-04</td> </tr> <tr> <td>22 -0.0031 3.4078e-04 3.4773e-04 3.2930e-04 3.5171e-04 3.2783e-04 3.3859e-04 3.3568e-04 3.5302e-04 3.6373e-04</td> </tr> <tr> <td>23 0.0021 -2.2670e-04 -2.3101e-04 -2.1969e-04 -2.3346e-04 -2.1869e-04 -2.2535e-04 -2.2355e-04 -2.3428e-04 -2.4090e-04</td> </tr> <tr> <td>24 -0.0014 1.4994e-04 1.5260e-04 1.4557e-04 1.5411e-04 1.4500e-04 1.4911e-04 1.4800e-04 1.5462e-04 1.5870e-04</td> </tr> <tr> <td>25 8.9823e-04 -9.9243e-05 -1.0089e-04 -9.6532e-05 -1.0182e-04 -9.6185e-05 -9.8726e-05 -9.8038e-05 -1.0213e-04 -1.0466e-04</td> </tr> <tr> <td>26 -5.9233e-04 6.5468e-05 6.6484e-05 6.3792e-05 6.7064e-05 6.3577e-05 6.5149e-05 6.4723e-05 6.7256e-05 6.8820e-05</td> </tr> <tr> <td>27 3.9046e-04 -4.3170e-05 -4.3799e-05 -4.2131e-05 -4.4159e-05 -4.1998e-05 -4.2972e-05 -4.2708e-05 -4.4277e-05 -4.5247e-05</td> </tr> </tbody> </table>	Raw Data			Convergence Iteration	Global Synchronization Error Rate	16 -0.0338 0.0037 0.0038 0.0035 0.0039 0.0035 0.0037 0.0036 0.0039 0.0041	24	27.6860	17 0.0234 -0.0026 -0.0027 -0.0024 -0.0027 -0.0024 -0.0025 -0.0025 -0.0027 -0.0028	18 -0.0155 0.0017 0.0018 0.0016 0.0018 0.0016 0.0017 0.0017 0.0018 0.0019	19 0.0105 -0.0012 -0.0012 -0.0011 -0.0012 -0.0011 -0.0011 -0.0011 -0.0012 -0.0013	20 -0.0070 7.6682e-04 7.8509e-04 7.3665e-04 7.9554e-04 7.3279e-04 7.6107e-04 7.5341e-04 7.9899e-04 8.2714e-04	21 0.0047 -5.1402e-04 -5.2534e-04 -4.9535e-04 -5.3181e-04 -4.9295e-04 -5.1046e-04 -5.0572e-04 -5.3394e-04 -5.5137e-04	22 -0.0031 3.4078e-04 3.4773e-04 3.2930e-04 3.5171e-04 3.2783e-04 3.3859e-04 3.3568e-04 3.5302e-04 3.6373e-04	23 0.0021 -2.2670e-04 -2.3101e-04 -2.1969e-04 -2.3346e-04 -2.1869e-04 -2.2535e-04 -2.2355e-04 -2.3428e-04 -2.4090e-04	24 -0.0014 1.4994e-04 1.5260e-04 1.4557e-04 1.5411e-04 1.4500e-04 1.4911e-04 1.4800e-04 1.5462e-04 1.5870e-04	25 8.9823e-04 -9.9243e-05 -1.0089e-04 -9.6532e-05 -1.0182e-04 -9.6185e-05 -9.8726e-05 -9.8038e-05 -1.0213e-04 -1.0466e-04	26 -5.9233e-04 6.5468e-05 6.6484e-05 6.3792e-05 6.7064e-05 6.3577e-05 6.5149e-05 6.4723e-05 6.7256e-05 6.8820e-05	27 3.9046e-04 -4.3170e-05 -4.3799e-05 -4.2131e-05 -4.4159e-05 -4.1998e-05 -4.2972e-05 -4.2708e-05 -4.4277e-05 -4.5247e-05
Raw Data	Convergence Iteration	Global Synchronization Error Rate																		
16 -0.0338 0.0037 0.0038 0.0035 0.0039 0.0035 0.0037 0.0036 0.0039 0.0041	24	27.6860																		
17 0.0234 -0.0026 -0.0027 -0.0024 -0.0027 -0.0024 -0.0025 -0.0025 -0.0027 -0.0028																				
18 -0.0155 0.0017 0.0018 0.0016 0.0018 0.0016 0.0017 0.0017 0.0018 0.0019																				
19 0.0105 -0.0012 -0.0012 -0.0011 -0.0012 -0.0011 -0.0011 -0.0011 -0.0012 -0.0013																				
20 -0.0070 7.6682e-04 7.8509e-04 7.3665e-04 7.9554e-04 7.3279e-04 7.6107e-04 7.5341e-04 7.9899e-04 8.2714e-04																				
21 0.0047 -5.1402e-04 -5.2534e-04 -4.9535e-04 -5.3181e-04 -4.9295e-04 -5.1046e-04 -5.0572e-04 -5.3394e-04 -5.5137e-04																				
22 -0.0031 3.4078e-04 3.4773e-04 3.2930e-04 3.5171e-04 3.2783e-04 3.3859e-04 3.3568e-04 3.5302e-04 3.6373e-04																				
23 0.0021 -2.2670e-04 -2.3101e-04 -2.1969e-04 -2.3346e-04 -2.1869e-04 -2.2535e-04 -2.2355e-04 -2.3428e-04 -2.4090e-04																				
24 -0.0014 1.4994e-04 1.5260e-04 1.4557e-04 1.5411e-04 1.4500e-04 1.4911e-04 1.4800e-04 1.5462e-04 1.5870e-04																				
25 8.9823e-04 -9.9243e-05 -1.0089e-04 -9.6532e-05 -1.0182e-04 -9.6185e-05 -9.8726e-05 -9.8038e-05 -1.0213e-04 -1.0466e-04																				
26 -5.9233e-04 6.5468e-05 6.6484e-05 6.3792e-05 6.7064e-05 6.3577e-05 6.5149e-05 6.4723e-05 6.7256e-05 6.8820e-05																				
27 3.9046e-04 -4.3170e-05 -4.3799e-05 -4.2131e-05 -4.4159e-05 -4.1998e-05 -4.2972e-05 -4.2708e-05 -4.4277e-05 -4.5247e-05																				

Laplacian Gain Calculation

Spectrum Laplacian Eigen Value											rho = 2/SSE+LE
No Attack	-7.2 e-16	1	1	1	1	1	1	1	1	10	0.1818

**Experiment 14**

Simulation No.14-a	Star 10 Nodes – DoS Attack			GAIN																																																																																																																																			
Input	<pre> GRAPH = [ ... 0 1 1 1 1 1 1 1 1 1; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0;];                     </pre>	<pre> GRAPH1 = [ ... 0 1 1 0 1 1 1 1 1 1; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 0 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0;];                     </pre>																																																																																																																																					
Error Rate Graph Plot				No Gain																																																																																																																																			
Results	Raw Data	Convergence Iteration	Global Synchronization Error Rate																																																																																																																																				
	<table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr><td>21</td><td>0.1122</td><td>0.1133</td><td>0.1100</td><td>-1</td><td>0.1077</td><td>0.1099</td><td>0.1127</td><td>0.1116</td><td>0.1106</td><td>0.1121</td></tr> <tr><td>22</td><td>0.1118</td><td>0.1126</td><td>0.1104</td><td>-1</td><td>0.1088</td><td>0.1102</td><td>0.1122</td><td>0.1114</td><td>0.1108</td><td>0.1118</td></tr> <tr><td>23</td><td>0.1116</td><td>0.1121</td><td>0.1106</td><td>-1</td><td>0.1095</td><td>0.1105</td><td>0.1118</td><td>0.1113</td><td>0.1109</td><td>0.1116</td></tr> <tr><td>24</td><td>0.1114</td><td>0.1118</td><td>0.1108</td><td>-1</td><td>0.1101</td><td>0.1107</td><td>0.1116</td><td>0.1113</td><td>0.1110</td><td>0.1114</td></tr> <tr><td>25</td><td>0.1113</td><td>0.1116</td><td>0.1109</td><td>-1</td><td>0.1104</td><td>0.1106</td><td>0.1114</td><td>0.1112</td><td>0.1110</td><td>0.1113</td></tr> <tr><td>26</td><td>0.1113</td><td>0.1114</td><td>0.1110</td><td>-1</td><td>0.1106</td><td>0.1109</td><td>0.1113</td><td>0.1112</td><td>0.1110</td><td>0.1112</td></tr> <tr><td>27</td><td>0.1112</td><td>0.1113</td><td>0.1110</td><td>-1</td><td>0.1108</td><td>0.1110</td><td>0.1113</td><td>0.1112</td><td>0.1111</td><td>0.1112</td></tr> <tr><td>28</td><td>0.1112</td><td>0.1112</td><td>0.1110</td><td>-1</td><td>0.1109</td><td>0.1110</td><td>0.1112</td><td>0.1111</td><td>0.1111</td><td>0.1112</td></tr> <tr><td>29</td><td>0.1112</td><td>0.1112</td><td>0.1111</td><td>-1</td><td>0.1110</td><td>0.1111</td><td>0.1112</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> <tr style="background-color: #e0e0e0;"><td>30</td><td>0.1111</td><td>0.1112</td><td>0.1111</td><td>-1</td><td>0.1110</td><td>0.1111</td><td>0.1112</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> <tr><td>31</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>-1</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> <tr><td>32</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>-1</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> </tbody> </table>	21	0.1122	0.1133	0.1100	-1	0.1077	0.1099	0.1127	0.1116	0.1106	0.1121	22	0.1118	0.1126	0.1104	-1	0.1088	0.1102	0.1122	0.1114	0.1108	0.1118	23	0.1116	0.1121	0.1106	-1	0.1095	0.1105	0.1118	0.1113	0.1109	0.1116	24	0.1114	0.1118	0.1108	-1	0.1101	0.1107	0.1116	0.1113	0.1110	0.1114	25	0.1113	0.1116	0.1109	-1	0.1104	0.1106	0.1114	0.1112	0.1110	0.1113	26	0.1113	0.1114	0.1110	-1	0.1106	0.1109	0.1113	0.1112	0.1110	0.1112	27	0.1112	0.1113	0.1110	-1	0.1108	0.1110	0.1113	0.1112	0.1111	0.1112	28	0.1112	0.1112	0.1110	-1	0.1109	0.1110	0.1112	0.1111	0.1111	0.1112	29	0.1112	0.1112	0.1111	-1	0.1110	0.1111	0.1112	0.1111	0.1111	0.1111	30	0.1111	0.1112	0.1111	-1	0.1110	0.1111	0.1112	0.1111	0.1111	0.1111	31	0.1111	0.1111	0.1111	-1	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	32	0.1111	0.1111	0.1111	-1	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	30	96.0429
21	0.1122	0.1133	0.1100	-1	0.1077	0.1099	0.1127	0.1116	0.1106	0.1121																																																																																																																													
22	0.1118	0.1126	0.1104	-1	0.1088	0.1102	0.1122	0.1114	0.1108	0.1118																																																																																																																													
23	0.1116	0.1121	0.1106	-1	0.1095	0.1105	0.1118	0.1113	0.1109	0.1116																																																																																																																													
24	0.1114	0.1118	0.1108	-1	0.1101	0.1107	0.1116	0.1113	0.1110	0.1114																																																																																																																													
25	0.1113	0.1116	0.1109	-1	0.1104	0.1106	0.1114	0.1112	0.1110	0.1113																																																																																																																													
26	0.1113	0.1114	0.1110	-1	0.1106	0.1109	0.1113	0.1112	0.1110	0.1112																																																																																																																													
27	0.1112	0.1113	0.1110	-1	0.1108	0.1110	0.1113	0.1112	0.1111	0.1112																																																																																																																													
28	0.1112	0.1112	0.1110	-1	0.1109	0.1110	0.1112	0.1111	0.1111	0.1112																																																																																																																													
29	0.1112	0.1112	0.1111	-1	0.1110	0.1111	0.1112	0.1111	0.1111	0.1111																																																																																																																													
30	0.1111	0.1112	0.1111	-1	0.1110	0.1111	0.1112	0.1111	0.1111	0.1111																																																																																																																													
31	0.1111	0.1111	0.1111	-1	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111																																																																																																																													
32	0.1111	0.1111	0.1111	-1	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111																																																																																																																													



**Experiment 15**

Simulation No.15-a	Star 10 Nodes – Node Destruction Attack			GAIN																																																																																																																																		
Input	<pre> GRAPH = [ ... 0 1 1 1 1 1 1 1 1 1; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0;];                     </pre>	<pre> GRAPH1 = [ ... 0 1 1 0 1 1 1 1 1 1; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 0 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0; 1 0 0 0 0 0 0 0 0 0;];                     </pre>																																																																																																																																				
Error Rate Graph Plot				No Gain																																																																																																																																		
Results	Raw Data	Convergence Iteration	Global Synchronization Error Rate																																																																																																																																			
	<table border="1"> <tbody> <tr><td>21</td><td>0.1122</td><td>0.1133</td><td>0.1100</td><td>-1</td><td>0.1077</td><td>0.1099</td><td>0.1127</td><td>0.1116</td><td>0.1106</td><td>0.1121</td></tr> <tr><td>22</td><td>0.1118</td><td>0.1126</td><td>0.1104</td><td>-1</td><td>0.1088</td><td>0.1102</td><td>0.1122</td><td>0.1114</td><td>0.1108</td><td>0.1118</td></tr> <tr><td>23</td><td>0.1116</td><td>0.1121</td><td>0.1106</td><td>-1</td><td>0.1095</td><td>0.1105</td><td>0.1118</td><td>0.1113</td><td>0.1109</td><td>0.1116</td></tr> <tr><td>24</td><td>0.1114</td><td>0.1118</td><td>0.1108</td><td>-1</td><td>0.1101</td><td>0.1107</td><td>0.1116</td><td>0.1113</td><td>0.1110</td><td>0.1114</td></tr> <tr><td>25</td><td>0.1113</td><td>0.1116</td><td>0.1109</td><td>-1</td><td>0.1104</td><td>0.1106</td><td>0.1114</td><td>0.1112</td><td>0.1110</td><td>0.1113</td></tr> <tr><td>26</td><td>0.1113</td><td>0.1114</td><td>0.1110</td><td>-1</td><td>0.1106</td><td>0.1109</td><td>0.1113</td><td>0.1112</td><td>0.1110</td><td>0.1112</td></tr> <tr><td>27</td><td>0.1112</td><td>0.1113</td><td>0.1110</td><td>-1</td><td>0.1108</td><td>0.1110</td><td>0.1113</td><td>0.1112</td><td>0.1111</td><td>0.1112</td></tr> <tr><td>28</td><td>0.1112</td><td>0.1112</td><td>0.1110</td><td>-1</td><td>0.1109</td><td>0.1110</td><td>0.1112</td><td>0.1111</td><td>0.1111</td><td>0.1112</td></tr> <tr><td>29</td><td>0.1112</td><td>0.1112</td><td>0.1111</td><td>-1</td><td>0.1110</td><td>0.1111</td><td>0.1112</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> <tr style="background-color: #e0e0e0;"><td>30</td><td>0.1111</td><td>0.1112</td><td>0.1111</td><td>-1</td><td>0.1110</td><td>0.1111</td><td>0.1112</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> <tr><td>31</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>-1</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> <tr><td>32</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>-1</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td><td>0.1111</td></tr> </tbody> </table>	21	0.1122		0.1133	0.1100	-1	0.1077	0.1099	0.1127	0.1116	0.1106	0.1121	22	0.1118	0.1126	0.1104	-1	0.1088	0.1102	0.1122	0.1114	0.1108	0.1118	23	0.1116	0.1121	0.1106	-1	0.1095	0.1105	0.1118	0.1113	0.1109	0.1116	24	0.1114	0.1118	0.1108	-1	0.1101	0.1107	0.1116	0.1113	0.1110	0.1114	25	0.1113	0.1116	0.1109	-1	0.1104	0.1106	0.1114	0.1112	0.1110	0.1113	26	0.1113	0.1114	0.1110	-1	0.1106	0.1109	0.1113	0.1112	0.1110	0.1112	27	0.1112	0.1113	0.1110	-1	0.1108	0.1110	0.1113	0.1112	0.1111	0.1112	28	0.1112	0.1112	0.1110	-1	0.1109	0.1110	0.1112	0.1111	0.1111	0.1112	29	0.1112	0.1112	0.1111	-1	0.1110	0.1111	0.1112	0.1111	0.1111	0.1111	30	0.1111	0.1112	0.1111	-1	0.1110	0.1111	0.1112	0.1111	0.1111	0.1111	31	0.1111	0.1111	0.1111	-1	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111	32	0.1111	0.1111	0.1111	-1	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111
21	0.1122	0.1133	0.1100	-1	0.1077	0.1099	0.1127	0.1116	0.1106	0.1121																																																																																																																												
22	0.1118	0.1126	0.1104	-1	0.1088	0.1102	0.1122	0.1114	0.1108	0.1118																																																																																																																												
23	0.1116	0.1121	0.1106	-1	0.1095	0.1105	0.1118	0.1113	0.1109	0.1116																																																																																																																												
24	0.1114	0.1118	0.1108	-1	0.1101	0.1107	0.1116	0.1113	0.1110	0.1114																																																																																																																												
25	0.1113	0.1116	0.1109	-1	0.1104	0.1106	0.1114	0.1112	0.1110	0.1113																																																																																																																												
26	0.1113	0.1114	0.1110	-1	0.1106	0.1109	0.1113	0.1112	0.1110	0.1112																																																																																																																												
27	0.1112	0.1113	0.1110	-1	0.1108	0.1110	0.1113	0.1112	0.1111	0.1112																																																																																																																												
28	0.1112	0.1112	0.1110	-1	0.1109	0.1110	0.1112	0.1111	0.1111	0.1112																																																																																																																												
29	0.1112	0.1112	0.1111	-1	0.1110	0.1111	0.1112	0.1111	0.1111	0.1111																																																																																																																												
30	0.1111	0.1112	0.1111	-1	0.1110	0.1111	0.1112	0.1111	0.1111	0.1111																																																																																																																												
31	0.1111	0.1111	0.1111	-1	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111																																																																																																																												
32	0.1111	0.1111	0.1111	-1	0.1111	0.1111	0.1111	0.1111	0.1111	0.1111																																																																																																																												





## APPENDIX B

## MATLAB Program

Parts	Algorithms	Notes
Initial Input	<pre> %% MATLAB R2023a %%  %Setting the Parameters TIME_ITER = .1; max_time_step = 50;  %Case: Fully Connected 4 Nodes GRAPH = [ 1 1 1 1;           1 1 1 1;           1 1 1 1;           1 1 1 1; ];  %Changes Topology in Attacks Model GRAPH1 = [ 1 1 1 1;            1 1 1 1;            1 1 1 1;            1 1 1 1; ];  %Inital Parameters: 4 Nodes num_node = 4; beta_initial = [2 3 8 1] * TIME_ITER; % the initial offset for each node alpha = [0.8 0.9 1.1 1.3] * TIME_ITER; % local clock skew are per TIME_ITER  %Inital Parameters: 10 Nodes %num_node = 10; %beta_initial = [2 3 8 1 12 1 3 3 9 10] * TIME_ITER; %alpha = [0.2 0.6 1.1 0.8 1.4 1.3 0.7 0.9 1.0 0.8] * TIME_ITER;  % Laplacian Matrix Calculation DEG = diag(sum(GRAPH, 2));  LAPG = DEG - GRAPH;  % Laplacian Eigen Value Calculation E = eig(LAPG); SSE = E(2); LE = max(E)  % Tuning Parameter rho = 0.6; %USING Default Tuning Parameter – No Gain %rho = 2/(LE+SSE); % USING Laplacian Feedback – Laplacian Gain </pre>	<p>This part belongs to chapter 3 – Phase 1 in requirement &amp; parameter setup such as: Time Step, Graphs, Initial Clock and Tuning Parameter. The graph can be switched into 4 or 10 nodes.</p>
Before Attack	<pre> % Applying the algorithm alpha_vir = zeros(max_time_step, num_node); % the virtual clock skew estimation alpha_rel = cell(max_time_step, 1); % the relative clock skew estimation tau = zeros(max_time_step, num_node); % the local time on each node time_vir = zeros(max_time_step, num_node); offset_vir = zeros(max_time_step, num_node);  alpha_vir(1, :) = ones(1, num_node); alpha_rel(:) = {GRAPH}; tau(1, :) = beta_initial; time_vir(1, :) = tau(1,:);  %%Before ATTACK%%  % assuming that there is TX/RX between all nodes at each time step#1 for t = 2:1:10     tau(t, :) = tau(t-1, :) + alpha; </pre>	<p>This part belongs to chapter 3 – Phase 2 in accomplishing consensus calculation before the attack</p>

	<pre> skew_rel(:)= {GRAPH}; GRAPH = GRAPH; % Go through the graph for links for i=1:1:num_node     for j=1:1:num_node         if GRAPH(i, j) ~= 0 % link is found where i RXs from j             % update the relative skew estimation             alpha_rel{t}(i,j) = rho*alpha_rel{t-1}(i,j) + (1-rho) *(tau(t,j)-tau(t-1,j))/(tau(t,i)-tau(t-1,i));             % update the skew compensation             alpha_vir(t,i) = rho*alpha_vir(t-1,i) + (1-rho)*alpha_rel{t-1}(i,j)*alpha_vir(t-1,j);             % compute the offset compension             offset_vir(t,i) = offset_vir(t-1,i) + (1-rho) * (alpha_vir(t-1,j)*tau(t-1,j)+ offset_vir(t-1, j) - alpha_vir(t-1,i)*tau(t-1,i) - offset_vir(t-1, i));         end     end end time_vir(t, :) = alpha_vir(t, :).*tau(t, :) + offset_vir(t,:); end </pre>	
During Attack	<pre> %%ATTACK Begin at 10th Iteration%%  % Laplacian Matrix Calculation DEG = diag(sum(GRAPH1, 2));  LAPG = DEG - GRAPH1;  % Laplacian Eigen Value Calculation E = eig(LAPG); SSE = E(2); LE = max(E)  % Tuning Parameter rho = 0.6; %USING Default Tuning Parameter – No Gain %rho = 2/(LE+SSE); % USING Laplacian Feedback – Laplacian Gain  % assuming that there is TX/RX between all nodes at each time step#2 for t = 11:1:max_time_step     tau(t, :) = tau(t-1, :) + alpha;     skew_rel(:)= {GRAPH1};     GRAPH = GRAPH1;     % Go through the graph for links     for i=1:1:num_node         for j=1:1:num_node             if GRAPH(i, j) ~= 0 % link is found where i RXs from j                 % update the relative skew estimation                 alpha_rel{t}(i,j) = rho*alpha_rel{t-1}(i,j) + (1-rho) *(tau(t,j)-tau(t-1,j))/(tau(t,i)-tau(t-1,i));                 % update the skew compensation                 alpha_vir(t,i) = rho*alpha_vir(t-1,i) + (1-rho)*alpha_rel{t-1}(i,j)*alpha_vir(t-1,j);                 % compute the offset compension                 offset_vir(t,i) = offset_vir(t-1,i) + (1-rho) * (alpha_vir(t-1,j)*tau(t-1,j)+ offset_vir(t-1, j) - alpha_vir(t-1,i)*tau(t-1,i) - offset_vir(t-1, i));             end         end     end     time_vir(t, :) = alpha_vir(t, :).*tau(t, :) + offset_vir(t,:); end </pre>	This part belongs to chapter 3 – Phase 3 in accomplishing consensus calculation during the attack
Plot Output	<pre> %%Plot of Results%%  %Plot Virtual Offset Estimation within Nodes figure; error = zeros(max_time_step, num_node); for j=1:1:max_time_step     for i=1:1:num_node         error(j,i) = (time_vir(j,i) - mean(time_vir(j,:)))/mean(time_vir(j,:));     end end </pre>	This part belongs to chapter 3 – Phase 4 in plotting converging speed with convergence error tolerance

	<pre> end for i=1:1:num_node     plot(1:1:max_time_step, error(:, i),'color', C{i},'marker','.');     hold on; end title('Error from Instantaneous Mean of Local Times'); legend('node 1','node 2','node 3','node 4'); xlabel('Iterations'); ylabel('Local Synchronization Error'); grid on; hold off;  %Plot Local Time of Each Node without Consensus time_step = 1:max_time_step; figure; for i=1:1:num_node     plot(time_step, tau(:, i),'-s','color', rand(1,3),'MarkerSize',3);     hold on; end title('Local Time within Nodes'); legend('node 1','node 2','node 3','node 4'); xlabel('Iterations'); ylabel('Time (s)'); grid on; hold off;         </pre>	
<p><b>GSEr Calcula- tion</b></p>	<pre> %Sum of Absolute Errors Value error2 = abs (error) GSE = sum (error2, 'all')         </pre>	<p>This part belongs to chapter 3 – Phase 4 in calculating accuracy in GSEr</p>

---

## APPENDIX C

### CURRICULUM VITAE

#### **Personal Information**

Name : Fakhmi Kemal Islamy ST., CHFI

Interest : Mobile, Satellite Telecommunication & Telco Security

LinkedIn: [www.linkedin.com/in/mashkemal](http://www.linkedin.com/in/mashkemal)

Email : [fakhmi.kemal@student@telkomuniversity.ac.id](mailto:fakhmi.kemal@student@telkomuniversity.ac.id)

#### **About**

I have experience of more than 10 years in the telecommunication industry in Indonesia since I joined PT. Pasifik Satelit Nusantara in 2010. I have experience in the engineering fields, operation, and maintenance in satellite & terrestrial networks, also the latest mobile technology since I joined PT. Telkomsel in 2012 until now. Recently, I interested more studying master's degree in cybersecurity & digital forensics fields in Telkom University that challenged me and my experiences beyond the future industry & research needs.

#### **Academic Background**

##### **2006 – 2010**

- Bachelor's degree - Telecommunication Engineering, Telkom University

##### **2021 – Now**

- Master's degree - Cyber Security & Digital Forensics, Telkom University

#### **Expertise**

- **Mobile Communications**

(Understand 2G, 3G, 4G & 5G Network. Operating using Huawei RAN & Monitoring)

- **IP Transport Network**

(Understand IP Network Elements such as Router, Hub & L2 Switches, Metro-Ethernet, PON, and DWDM. Design and planning IP transport network such as Satellite, Microwave & OFDM Radio)

- **Cyber & Telco Security**

(Understand Offense, Defense, and Governance using NIST Framework. Able to perform Penetration Testing web & mobile infrastructure using Kali Linux and Windows OS and understand Network & Telco Security Signaling including 2G, 3G, 4G & 5G Network)

- **Digital Forensics**

(Understand Evidence Collection, Preservation, Analysis in Computer Network & IoT)

#### **Papers**

##### **2022**

- **APPLE HOMEPOD MINI FORENSICS** (Submitted at ICOICT, 2022)

Fakhmi Kemal Islamy, Irwan Hariyanto, Wawan Setiawan

- **PEMODELAN ANCAMAN DAN PEMBANGUNAN USE CASE MONITORING PADA PT. TELKOMSEL** (Capstone Project, 2022)

Fakhmi Kemal Islamy

**2015**

- **RANCANG BANGUN SISTEM PENERIMAAN DAN PEREKAMAN DATA SATELIT BERBASIS NOAA AUTOMATIC PICTURE TRANSMISSION (APT) SEBAGAI SARANA EDUKASI** (LAPAN, 2015)

Nurmajid Setyasaputra, Fakhmi Kemal Islamy, Sutan Takdir Ali Munawar

**2010**

- **ANALISIS IMPLEMENTASI DETEKTOR ZERO-CROSSING MENGGUNAKAN HALF-CYCLE BANDPASS LIMITER PADA PENERIMA LORAN-C BERBASIS TMS** (IT Telkom, 2010)

Fakhmi Kemal Islamy

### Organization & Work Experiences

**2023**

- **AFDI Member** – Asosiasi Forensik Digital Indonesia (2023 – Present)  
Professional member of Information Indonesia Digital Forensics Association
- **CDEF Community Member** – CDEF (2023 – Present)  
Active member of Indonesia Cyber Defense Forum as Podcaster in Weekly Update

**2022**

- **ICSFTU Student Member** – ICSFTU Telkom University (2022 – Present)  
Vice President of Ikatan Cendekiawan Sains Forensik Telkom University
- **ISACA Student Member** – ISACA Indonesia (2022 – Present)  
Student member of Information Systems Audit and Control Association Indonesia chapter
- **SKKNI Cryptography BSSN** – BSSN (2022)  
Member of Drafting Team SKKNI Cryptography Represent Industry Sector

**2021**

- **Network Security Defensive Engineer** – Telkomsel (December 2021 – Present)  
Telkomsel Network Security Defensive Management. Conduct SOC & SIEM Development
  1. Developing Network Security Operation Center (NSOC)
  2. Adopted Tier-less SOC with 3 Departments: Inform, Develop, Respond
  3. IR & Forensics Leadership in Signalling & Telecom IT
  4. Shift-Left Strategy enablement with DevSecOps
  5. Vertical SOC Expansion using OpenAI
  6. Autonomic Security Operation Center
  7. Telco DFIR Lab Development
- **Cyber Security Talent** – Telkomsel (April 2021 – Present)  
Telkomsel Digital Prodigy as Cyber Security talent. Implement security culture into DevSecOps and Data Loss Prevention (DLP) program.

**2012**

- **Radio, Transport & Power Operation** – Telkomsel (2012 – 2021)

Daily operation of Telkomsel Mobile Infrastructure. Handling fault of Radio, Transport and Power incident of 2G, 3G, 4G systems.

Develop good collaboration with other departments and experience supervise to design & develop radio access brings me & my team many achievements such as:

1. Best WLC National 2015
2. Best Rollout Productivity 2016
3. Best Payload CMON NARU & RAFI 2017
4. Best Regional RTPO in 2017 & 2018
5. Best Availability NARU 2019

## 2011

- **Network Incident Management** – Dimension Data (September – December 2011)

Handling incident management of Telkomsel national network. Escalation of Major and Critical severity to an impacted service area. Maintaining SLA & OLA to meet KPI.

This pilot project of Dimension Data Indonesia brings comprehensive and agile incident management in Telkomsel with a structured ITIL framework.

## 2010

- **Network Operation Center** – Pasifik Satelit Nusantara (August 2010 – 2011)

Monitoring & fault handling of PSN global satellite & terrestrial network services. The service including internet, private network & closed user group for banking & custodian.

Awarded as the best NOC Fault Handler in H2 2011.

- **Amateur Radio Member** – ORARI (September 2010 – 2011)

Research and sharpening the skill of HAM Radio activities on many levels of frequencies. Including LF, HF, UHF, VHF & Microwave. Actively using Digital Signal Processing (DSP) to perform a Software Defined Radio (SDR) AMSAT receiver.

More advanced technology comes from this community, for example, Internet Gateway, Automatic Position Reporting System, and Wireless Mesh Network. It brings my research as a hobby even further on amateur frequencies.

## 2009

- **Satellite Association Student Member** – ASSI (March 2009 – 2010)

Defining slot and frequency management of national capacity requirements. Escalation to ITU-WRC of the Issues. Annually held an APSAT Conference from Asia-Pacific members. Promote Nanosatellite research in students of IT Telkom.

- **Laboratory Assistant** – Antenna Laboratory IT Telkom (2009 – 2010)

Handling lab activities including research of Smart Antenna & Nanosatellite. Organize annual Cellular Drive Test training of CDMA, 2G & 3G networks. Co-Founded origins of two organizations, such as IT Telkom Satellite Society & Amateur Radio Club IT Telkom.

## Training & Certifications

- **ZeroFox Certified SE** – ZeroFox (2023)  
(Certification for Sales Engineering in ZeroFox EMEA Region)
- **5G Security & Technology Deployment** – HUAWEI (2023)  
(Bootcamp for 5G Security Threat Landscape, Countermeasure & Huawei Solution)
- **Certified DevOps Practitioner** – Studi DevSecOps (2023)  
(Bootcamp & Certification of DevSecOps Development)

- **Certified AppSec Practitioner (CAP)** – The SecOps Group (2023)  
(Certification for App Security Practitioner)
- **Cyber Threat Intelligence 101** – ArcX (2023)  
(Certification for Foundation Level Threat Intelligence Analyst)
- **Google IT Support (Google ITS)** – Google Coursera (2022)  
(Certification for IT Support Handling and Cyber Security)
- **NSE 7** – Fortinet (2022)  
(Certification for Fortinet NAC & IoT)
- **Computer Hacking Forensic Investigator (CHFI)** – EC Council (2022)  
(Certification for Forensic Investigator of Cyber Crime in Computer Network & IoT)
- **Advanced Network Intelligence** – Sandvine (2022)  
(Training for Deep Packet Inspection for Fraud Detection Analysis in Telco Environment)
- **5G Security & Privacy Practices** – SkillSoft (2021)  
(Training about 5G Security Protocol and Handling Privacy Practices)
- **Sekolah Hacker** – Cilsy Fiolution (2021)  
(Bootcamp for Penetration Testing of Web and Mobile apps using Kali Linux)
- **TED Cyber Security Academy** – Telkomsel (2020)  
(Bootcamp of Cyber Security including Offensive, Defensive and Governance)
- **OFDM Transport** – Cambium Networks (2020)  
(Design and Troubleshoot OFDM Non-LOS Transport for Urban and Rural Network)
- **4G Optimization** – Telkomsel (2016)  
(OFDM structured frame in 4G and basic parameter tuning for optimization)
- **CCNA & CCNP Training** – Telkomsel (2014 & 2015)  
(Cisco CCNA & CCNP Training of Fundamental IP Network Concepts)
- **GPRS/UMTS PS Fundamental** – Huawei (2013)  
(Basic PS UMTS Operation of Fault Handling & Operation)

### Speakers

#### **2023**

- **Microwave Application & Security Challenges in Mobile Communication Industry** (ITERA, 2023)
- **Cyber Security Myth, Gaps & Modelling** (Telkom University, 2023)

#### **2022**

- **Information Security in Telecommunication System** (Polinema, 2023)