

**DEVELOPMENT OF NODE RELIABILITY DETECTION
ALGORITHM FOR WIRELESS SENSOR NETWORKS**

By

MOHAMAD AFIQ BIN AZMAN

FINAL PROJECT REPORT

Submitted to the Department of Electrical and Electronic Engineering in
Partial Fulfillment of the Requirements for the Degree

Bachelor of Engineering (Hons)

(Electrical and Electronic Engineering)

Universiti Teknologi PETRONAS

Bandar Seri Iskandar

31750 Tronoh

Perak Darul Ridzuan

CERTIFICATION OF APPROVAL

DEVELOPMENT OF NODE RELIABILITY DETECTION ALGORITHM FOR WIRELESS SENSOR NETWORKS

By

MOHAMAD AFIQ BIN AZMAN

A project dissertation submitted to the
Department of Electrical and Electronic Engineering
Universiti Teknologi PETRONAS
in partial fulfillment of the requirements for the
Bachelor of Engineering (Hons)
(Electrical and Electronic Engineering)

Approved:

Azrina binti Abdul Aziz

Project Supervisor

UNIVERSITI TEKNOLOGI PETRONAS

TRONOH, PERAK

January 2014

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contained herein have not been undertaken or done by unspecified sources or persons.

Mohamad Afiq bin Azman

ABSTRACT

The rapid growth in invention and innovation of technology has driven the communication field into a new phase in which wireless sensor applications have been widely used for various purposes. The large numbers of sensor nodes deployed in certain applications could have high failure rate which inflicted the reliability of the wireless sensor network (WSN). The failure of sensor nodes can be affected by certain factors such as battery drop, interference of signal and malfunction of device. Due to the sensor nodes' failure, the quality of data transmission will be degraded as the receiver would not be able to receive the data transmitted. Thus, this project presents a proposed algorithm which could assist in recognizing and identifying faulty sensor nodes in WSN by utilizing round trip delay (RTD) time method. The proposed algorithm is then implemented on hardware compounding of several IRIS sensor motes. The user interface known as Xsniffer software is used to observe the data transmitted as well as providing the user with information on time taken for the data to be delivered corresponding to the implemented algorithm. The analysis of the results obtained through tabulated data in the look-up tables has enables the user to successfully identify sensor node at fault within the network. The time taken for data to be delivered to target location evidently will exceed the threshold value (maximum time taken) to indicate that the node within the network is compromised.

ACKNOWLEDGEMENT

First and foremost, all praise to Allah, thanks for all the blessing and for giving the author good health throughout his studies and finally managed to complete this research.

The author would like to take this opportunity to express immense appreciation to his supervisor and his co-supervisor; Dr Azrina binti Abdul Aziz and Dr Abu Bakar Sayuti bin Hj Mohd Saman for their kind supervision, expert advice, beneficial guidance and suggestion in all aspects throughout the research work. Besides that, their insightful understanding and profound knowledge sharing are very much appreciated. Extra discussion sessions and motivational advices from the author's supervisor truly have enlighten his courage to fully committed towards the completion of this research.

The author also would like to dedicate deepest gratitude to FYP coordinator, Dr Nasreen binti Badruddin for organizing seminar and briefing sessions to assist students as well as scheduling ELECTREX and viva by inviting external examiners to evaluate the students. Besides that, the author would like to thank his family members and friends for their precious and concrete supports as well as strong encouragement from the beginning until the end of his research work

Last but not least, regards and blessings are offered in abundance to anyone who has assisted the author directly or indirectly in making his final year project a success. Thank you and God bless all of you.

TABLE OF CONTENTS

Title Page	i
Certification of Approval	ii
Certification of Originality	iii
Abstract	iv
Acknowledgement	v
Table of Contents	vi
List of Figures	viii
List of Tables	ix
List of Abbreviations	ix
CHAPTER 1: INTRODUCTION	1
1.1 Background Study	1
1.2 Problem Statement	3
1.3 Objective	3
1.4 Scope Of Study	4
1.5 Relevancy Of Project	4
1.6 Feasibility Of Project	4
CHAPTER 2: LITERATURE REVIEW	5
2.1 Factors That Affect Reliability Of Wireless Sensor Network (WSN)	5
2.2 Technique In Determining Reliability Of Wireless Sensor Network (WSN)	9
2.3 Detection Algorithms In Wireless Sensor Network	13
CHAPTER 3: METHODOLOGY	17
3.1 Implementation Of Round Trip Delay (RTD) Algorithm	19
3.2 Investigation On Factors Influencing Sensor Node's Failure	22
3.3 Tools Required	23
3.4 Key Milestone	24
3.5 Gantt Chart	25

CHAPTER 4: RESULTS AND DISCUSSION	27
4.1 Implementation Of Round Trip Delay (RTD) Algorithm	27
4.1.1 Network Topologies Set-up	27
4.1.2 Testing Faulty Condition Of The Topology Arrangements	30
4.2 Investigation On Factors Influencing Sensor Node's Failure	33
CHAPTER 5 : CONCLUSION AND RECOMMENDATION	38
CHARTER 6: REFERENCES	39
CHAPTER 7: APPENDICES	40
Appendix 1: Specifications of IRIS sensor mote	40

LIST OF FIGURES

Figure 1 : Wireless sensor network	1
Figure 2 : (a) Star and mesh topologies (b) clustered topology	6
Figure 3 : (a) with data aggregation (b) without data aggregation	7
Figure 4 : Energy depletion graphs result	7
Figure 5 : max (d_i) and min (d_i) versus S	8
Figure 6 : max (d_i) and min (d_i) versus R	8
Figure 7 : Overview of ComSen	9
Figure 8 : Performance of ComSen at various lost rate	10
Figure 9 : Diagram indicating all nodes are active	11
Figure 10 : Diagram indicating that node 4 is off	11
Figure 11 : Energy comparison diagram of routing algorithm with normal packet size	12
Figure 12 : WSN with four sensor nodes	13
Figure 13 : Flow Chart of the project progress	17
Figure 14 : Xsniffer's screen display user interface	20
Figure 15: Experimental procedures to determine faulty node	21
Figure 16: Experimental procedures to investigate on factors affecting reliability WSN	22
Figure 17 : Topology Arrangement 1	28
Figure 18 : Topology Arrangement 2	28
Figure 19 : Topology Arrangement 3	29
Figure 20 : Topology Arrangement 4	29
Figure 21 : Arrangement Of Sensor Nodes	34
Figure 22 : Graph of distance from base station node against light readings recorded by base station node	34
Figure 23: Arrangement of sensor nodes	35

Figure 24: Graph of distance from base station node against signal strength recorded by base station node 36

LIST OF TABLES

Table 1: Comparison between algorithms	15
Table 2: Comparison between IRIS sensor mote with MICAZ sensor mote	18
Table 3: Key Milestone for FYP I	24
Table 4: Key Milestone for FYP II	24
Table 5: Gantt Chart representing the process flow for FYP I	25
Table 6: Gantt Chart representing the process flow for FYP II	26
Table 7: Symmetrical Topology Arrangement 1	30
Table 8: Symmetrical Topology Arrangement 2	31
Table 9: Unsymmetrical Topology Arrangement 3	31
Table 10: Unsymmetrical Topology Arrangement	31
Table 11: Symmetrical Topology Arrangement 1	32
Table 12: Symmetrical Topology Arrangement 2	32
Table 13: Unsymmetrical Topology Arrangement 3	32
Table 14: Unsymmetrical Topology Arrangement 4	33
Table 15: Readings of Light Measurement in a room	34
Table 16: Readings of signal strength recorded by the base station node	36

LIST OF ABBREVIATIONS

RTD	Round Trip Delay
RTP	Round Trip Path
WSN	Wireless Sensor Network

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND STUDY

The current modern era of technology has instigated people to come out with ideas of simplifying complex systems to meet up the standard of having systems without too many wires/cables due to the space constraint, besides economic relevancy costs factor and other factors as well. A wireless sensor network (WSN) application is believed to be the new alternative which has been widely used in many applications such as battle field, oil and gas, environmental monitoring and disaster recovery. Basically, WSN is defined as a wireless network that composed of many small, cheap and potentially smart sensor nodes equipped with sensing, data processing and storage and communication capabilities that are distributed accordingly to monitor certain conditions at different locations.

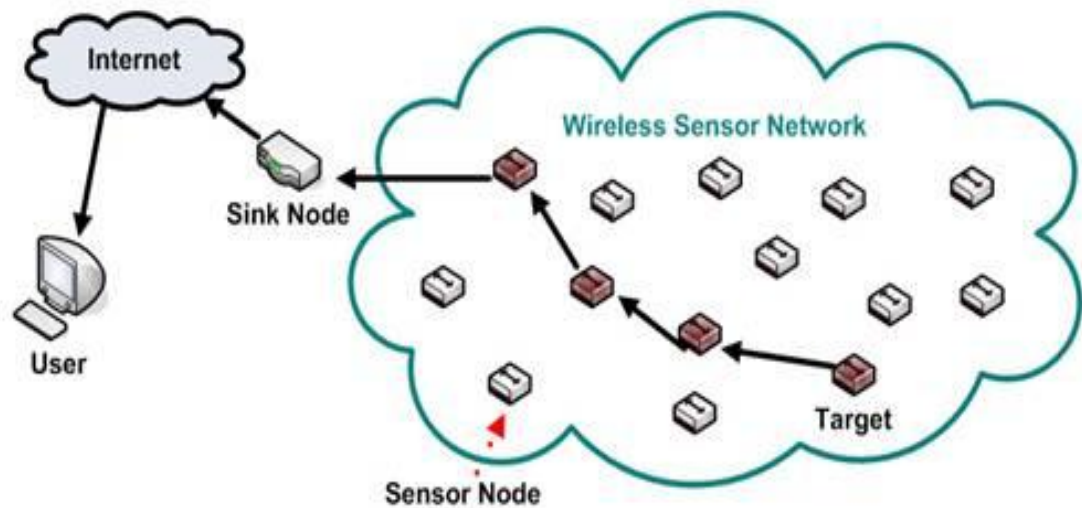


Figure 1 : Wireless sensor network

In Figure 1, WSN is implemented when multiple of sensor nodes are deployed and the data will be transmitted from a target node along the path established among the active nodes to the sink node. Sink node or parent node acts like an intermediate phase which received data from active sensor nodes and direct the data towards user's computer for monitoring and control purposes. However, the sensor nodes have some restriction such as limited memory, resources constraint and battery-powered which cannot last longer depending on the consumption of energy by those specific nodes since each node has different rate of energy consumption. The WSN is typically deployed in large scale, thus the data generated by neighboring sensor nodes are enormous and redundant. The reliability of WSN is determined through the transmission of data without loss from one node to another node because it is very important to have a reliable data transmission in order to achieve efficient data delivery. However, there are some factors which could have significant effects on the reliability of WSN. In practice, there are various factors that result in node failure such as battery drops, obstruction, mobility or interference during data transmission. Since the sensor nodes are battery-powered, the energy consumption by each node would be the important aspect which underlined the lifetime of specific sensor nodes within the network. Most of the previous researches being done portray the methods to minimize these inevitable factors – battery drop, interference and others, in order to maintain the reliability of the data transmission but it is not possible to completely mitigate all of these factors as the environmental condition in which the node sensors are deployed could play a pivotal role in influencing the data transmission. In this project, an algorithm to detect the reliability of the data transmission among nodes will be introduced to alert neighbors when the reliability of this data is compromised besides determining the factors which are identified to have negative implication on the transmitted data.

1.2 PROBLEM STATEMENT

Reliability data transmission plays an important role in guaranteeing efficient data delivery. Usually, the sensor nodes will be randomly or event-driven being placed on the field for the purpose of sensing, gathering information and processing collected data. Subsequently, these sensor nodes' performances are discovered to be affected by ultimate changes in environmental condition in which the sensor nodes are deployed. The likelihood of the inaccurate data transmitted from the nodes to the base station could possibly increase if there is no preventive measure being applied at the field. For instance, if the failed sensor nodes are unable to be detected before the lifetime of that sensor nodes ended, the neighbor nodes could not be alerted and eventually the transmitted data cannot be delivered successfully to the receiver (base station). In this case, the transmitted data could not find a way to deliver the message since one of the nodes in its path has not functioning anymore. Thus, many approaches have been proposed for providing the reliable data transport such re-routing method and others depending on the appropriateness of the application of sensor nodes. However, these approaches mostly cover Physical and MAC layers, but not the upper layer. Manually checking could be troublesome and time consuming. Therefore, the need for an algorithm to detect the sensor nodes at fault could be very efficient and helpful. The aim of this project is to develop an algorithm at the upper layer that can predict the node failure by observing the pattern of the data transmission. Based on this prediction, nodes will inform their neighbors to alert them so they can take further steps to mitigate the failure.

1.3 OBJECTIVES

1. To study node reliable detection algorithms.
2. To survey factors contributing to node failure in the network.
3. To implement the algorithm on a sensor network (hardware).
4. To simulate various factors causing the node failure and implement them in the hardware.
5. To measure and analyze the performance of the algorithm.

1.4 SCOPE OF STUDY

This project ideally focus on determining various factors which influence the reliability of Wireless Sensor Network (WSN) such as the energy consumption of each node involve and failure rate which subsequently underlined the lifetime of specific sensor nodes within the network. The algorithm will be implemented on the hardware provided which is IRIS sensor nodes. Both software and hardware specific for the application are needed in order to implement an efficient system which is capable of identifying the factors which cause failures in the system precisely as well as being able to predict the failure rate based on the pattern of data transmitted from the nodes. Motework which is a component-based, event-driven runtime environment specifically designed for wireless sensor networks will be utilized as the medium in programming the sensor nodes. Suitable algorithm will be implemented to analyze and anticipate the failed sensor node in the WSN precisely. The proposed algorithm enables the user to predict specific failed sensor node before the actual sensor node's failure really occur which indirectly improves the reliability of WSN.

1.5 RELEVANCY OF PROJECT

This project is relevant to be conducted as it will further improve the quality and the reliability of the current applications of wireless sensor network (WSN) by enabling the user to access and predict the faulty sensor nodes in the network. Besides that, the need for manual checking to determine the status of sensor nodes also can be discarded. Above all, this project aims to raise the degree of efficiency of WSN applications which have been widely deployed nowadays.

1.6 FEASIBILITY OF THE PROJECT

By accessing the whole possibilities in conducting this project, the project is feasible to be accomplished within the time frame set by the UTP FYP committees as this project required further analysis and reading on the programming softwares such as Motework and Tinyos. The foundation of utilizing Tinyos required the author to recall knowledge on C programming language which had been taught during the first year degree studies before. Previous notes on C programming will be referred to program the sensor nodes for this project.

CHAPTER 2

LITERATURE REVIEW

The applications of wireless sensor networks (WSN) has been broaden globally particularly with the development of ideal smart sensors with several advantages which provide user interface through data transmission from each sensor node [7]. The applications of WSN could be of any types but it has been classified to fall under three subcategories which are Environmental data gathering, Security checking and Sensor node tracking. Among the applications of WSN that have been developed include medical and disaster monitoring through CodeBlue infrastructure [8], object tracking application [9] and others. It is notable that sensor nodes utilized in WSN have certain restrictions which are limited memory capacity, resources constrain and battery-powered devices [10] [11] [2]. These restrictions basically will not enable the sensor nodes to perform heavy algorithms. On the other hand, the sensor nodes are identified to be deployed in two types of network which are structured and unstructured network. In structured network, the sensor nodes are placed at fixed location with fewer number nodes and require lower maintenance costs. Meanwhile for the unstructured network, the sensor nodes arrangement seems to be the opposite of the one in structured network, as they are randomly placed in a field which inflicted to the difficulty in detecting failure rate for each node.

2.1 FACTORS THAT AFFECT RELIABILITY OF WIRELESS SENSOR NETWORKS (WSN)

In order to implement WSN, the details of the system such as topology arrangement, energy consumption rate, network's lifetime and coverage area have to be

precisely identified. According to the analysis done in [5], the authors have come out with the ideas to enhance the network efficiency by selecting topology arrangement according to appropriateness of the mobile sensor nodes application while enhancing the energy consumption by nodes involved. In general, the network topologies are classified into three types which are mesh topology, star topology and cluster topology.

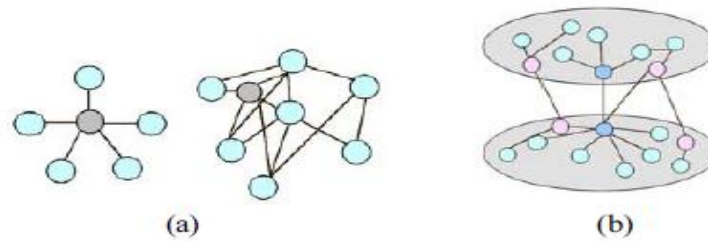


Figure 2 : (a) Star and mesh topologies (b) clustered topology [5]

In case whenever there are many sensor nodes that are going to be deployed, the authors would proposed a clustered hierarchy topology considering there are plenty of mobile nodes which can be selected to act as main node to interact with other nodes within the network [5]. Each node should have the information of its neighbor to ensure the connectivity between them is well established. As the number of sensor nodes deploy in certain area increases, the perimeter of the coverage area would possibly increases too. The high extent of coverage in specific area would require more sensor nodes to acquire results with high accuracy with energy conservation within the system has become priority in recent conducted researches [7]. Large coverage area indicates that huge amount of data can be transmitted through the network. However, the coverage area could be affected under certain circumstances such as obstruction in the network, environmental condition and noise either from internal or external of the network [12]. The main issue arises when the number of loss rate of packet data generated increases as the number of sensor nodes increases which subsequently leads to the high rate of energy consumption by each node. With reference to the research being done in [1], the authors have emphasized that battery energy depletion and device failure's rate will decide the lifetime of sensor nodes in the network (node aging). It is believed that the largest energy consumption is due to the large amount of data received from child nodes to the parent nodes in data gathering tree. The abundant of information received could be redundant and there might be many errors contained in the information too. In order to minimize the

usage of energy by each node, data aggregation technique is applied and the comparison of the results from the simulation is being compared to the one without using data aggregation technique.

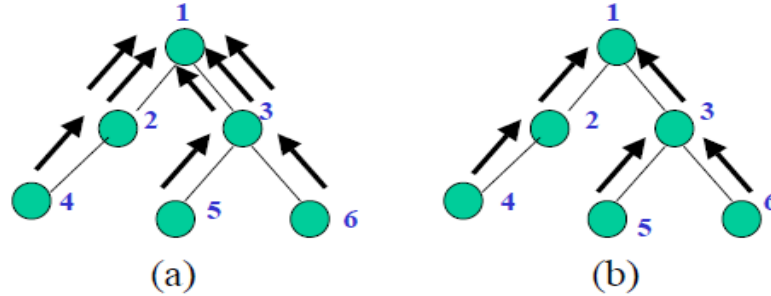
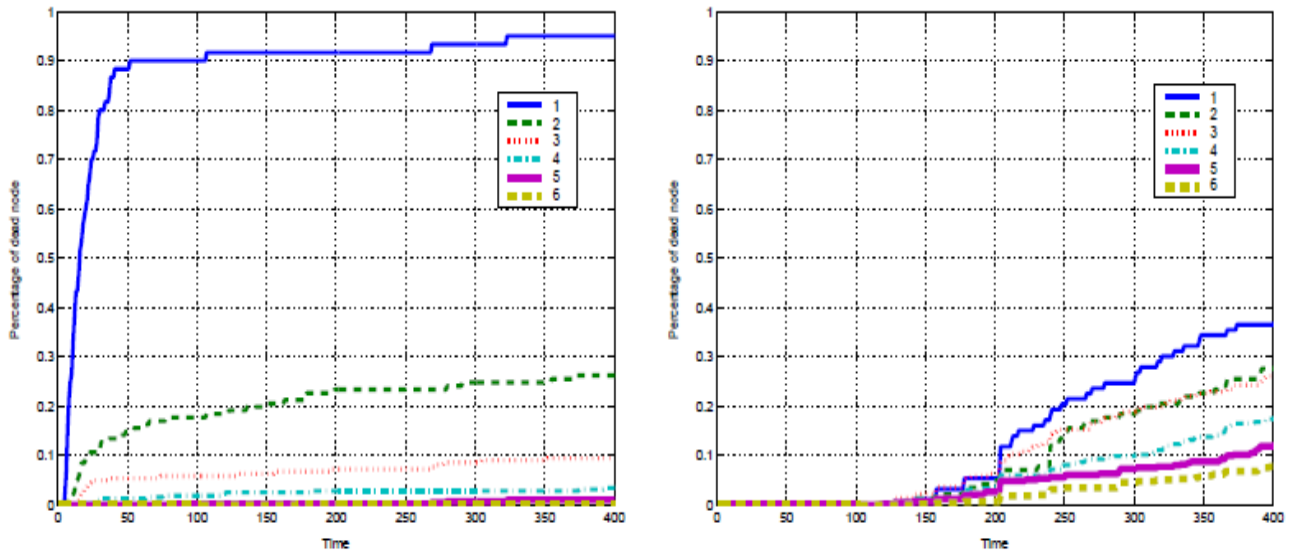


Figure 3 : (a) with data aggregation (b) without data aggregation [1]

By definition, data aggregation as in Figure 3, is referred to the practice of eliminating redundancy of data by filtering the data received from child nodes to minimize the number of data delivery in order to optimize energy consumption rate [1] [4]. The graphs below display the comparison results of data aggregation technique with a network without data aggregation technique over time.



(a) without data aggregation

(b) with data aggregation

Figure 4 : Energy depletion graphs result [1]

Based on the Figure 4, a network without data aggregation (Figure 4(a)) runs out of energy at faster period of time as compared to a network with data aggregation (Figure 4(b)) technique. Data aggregation technique is proven to be an efficient way in

optimizing the rate of energy consumption by each node and thus, prolonging the lifetime of that specific sensor nodes. The main reason the authors come out with this conclusion is because of the different number of packet data being forwarded to the sink which inclined the burden to the main node in a network without data aggregation technique [1]. However, according to [4], there is a delay setback which occur when data aggregation technique is applied because data released from the nearer source would be held for a while to wait for the data from farther source to arrived before being aggregated altogether. The graphical displays of the results are shown as in Figure 5 and Figure 6:

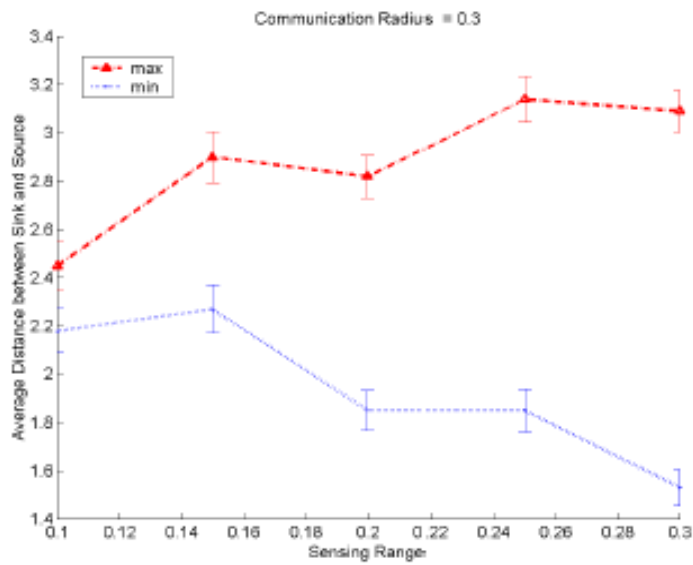


Figure 5 : $\max (d_i)$ and $\min (d_i)$ versus S [4]

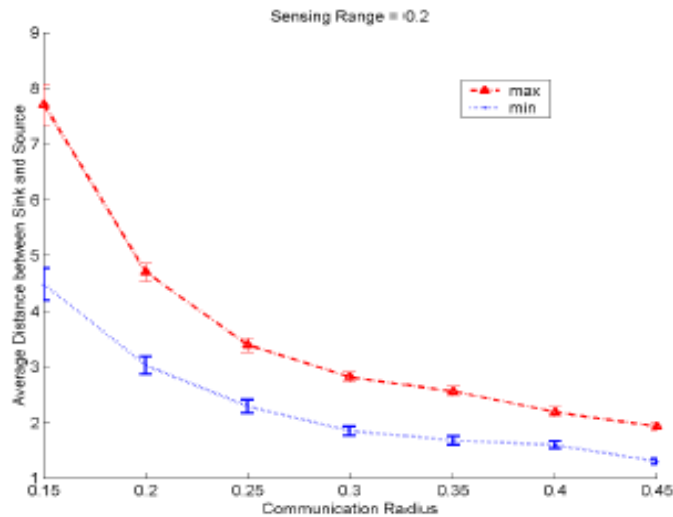


Figure 6 : $\max (d_i)$ and $\min (d_i)$ versus R [4]

The value for maximum and minimum is determined through the simulation. The difference between the two curves is high whenever the range is high, indicating that there are many sensor nodes being deployed and when the radius is in low value.

2.2 TECHNIQUE IN DETERMINING THE RELIABILITY OF WIRELESS SENSOR NETWORK (WSN)

In a security system, ‘ComSen’ method as display in Figure 7, has been introduced to identify compromised nodes in the network which utilized hybrid approach consisting of distributed component and centralized component which is very beneficial in maintaining a reliable WSN [2]. Distributed component is referred as a program that is applied for each node which responsible to look after its neighbor for any node breakdown which is expected to occur. Meanwhile, centralized component is run on the base station which performs aggregation process in filtering inaccurate information received before making any decision.

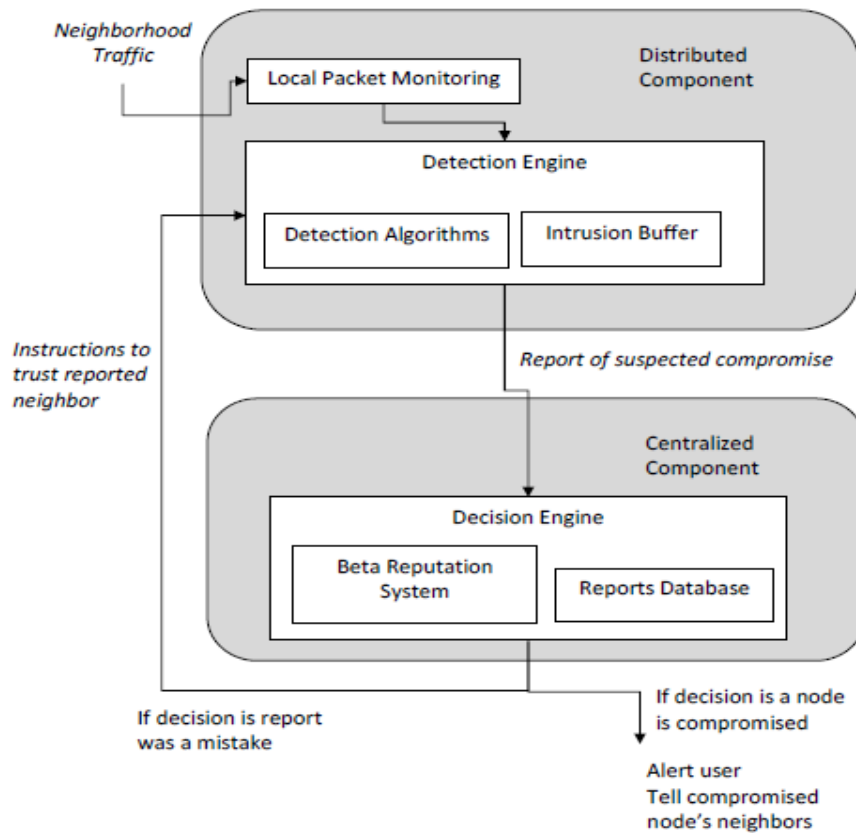


Figure 7 : Overview of ComSen [2]

In implementing this technique, certain metrics have been analyzed such as detection rate, false positive and detection time. Detection rate is defined as the actual detection percentage reported by the system. Meanwhile false positive is known as the reported compromised node in the system which could possibly be false or inaccurate, and detection time is underlined as time interval taken by the system to execute information before a decision is made whether the node is breakdown or not.

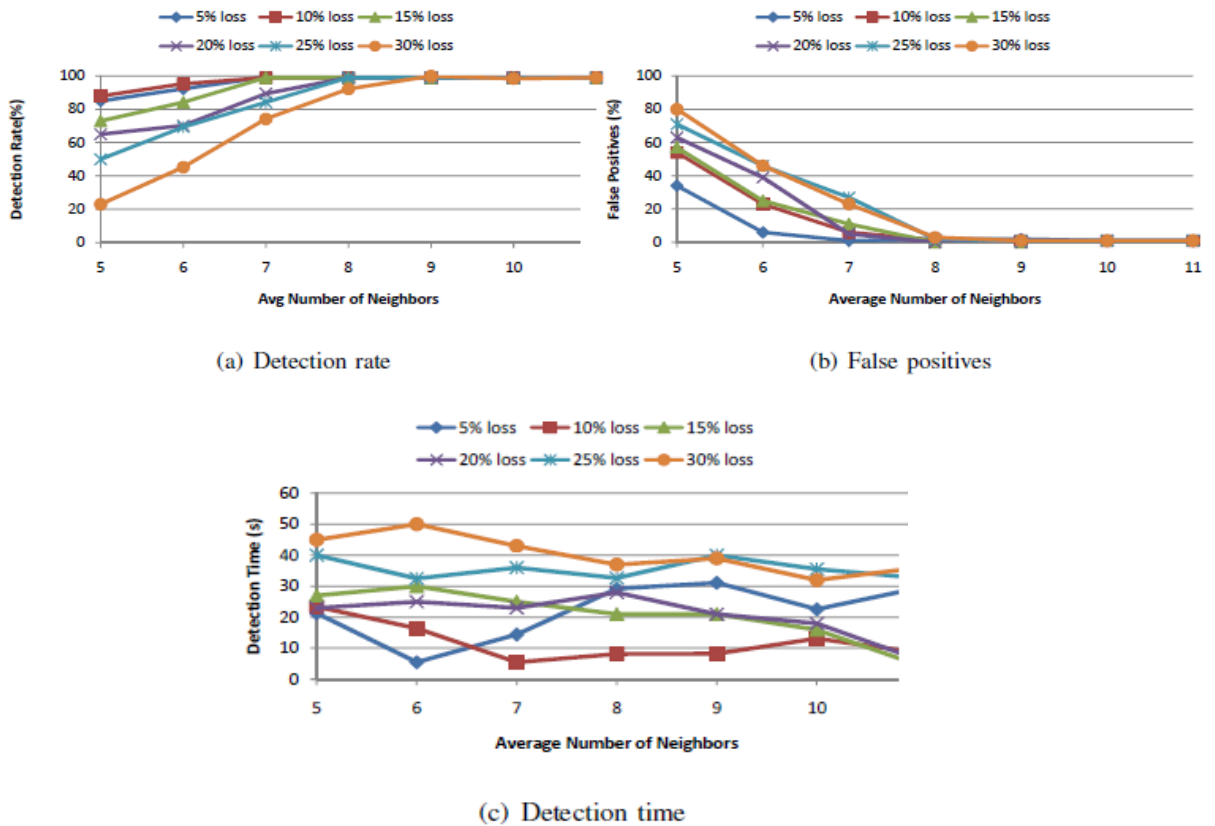


Figure 8 : Performance of ComSen at various lost rate [2]

In Figure 8(a), the detection rate inclined rapidly as the number of nodes increases since there are many sensor nodes available for detecting compromised nodes, and for Figure 8(b), false positive percentage values decrease as the number of average neighbors increase as there are more neighbors monitoring each other. Lastly, as for Figure 8(c), the data loss rate is directly proportional to the detection time. As the loss rate increases, the detection is found to be inclined too.

On the other hand, another method of determining the reliability of WSN is further analyzed by using a re-routing method once node failure is detected in direct path concerning the energy consumption by each node involve in improved virtual circuit routing algorithm (IVCRA) application [6]. The design works in such a way that any active nodes in the path have the likelihood of becoming a parent node if the node which receives data succeeds in recognizing its parent identification (PID). Once a safe path has been identified, the data will be safely delivered. Change of route will takes place if a node in the direct path is expected to breakdown. The whole design can be illustrated in the Figure 9 and Figure 10:

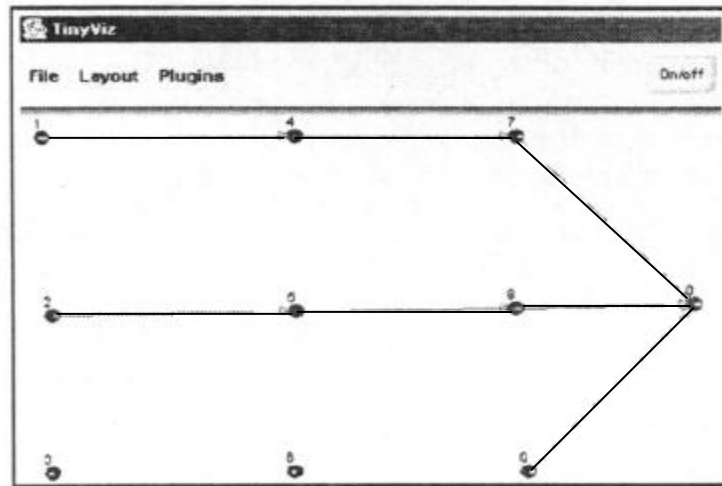


Figure 9 : Diagram indicating all nodes are active [6]

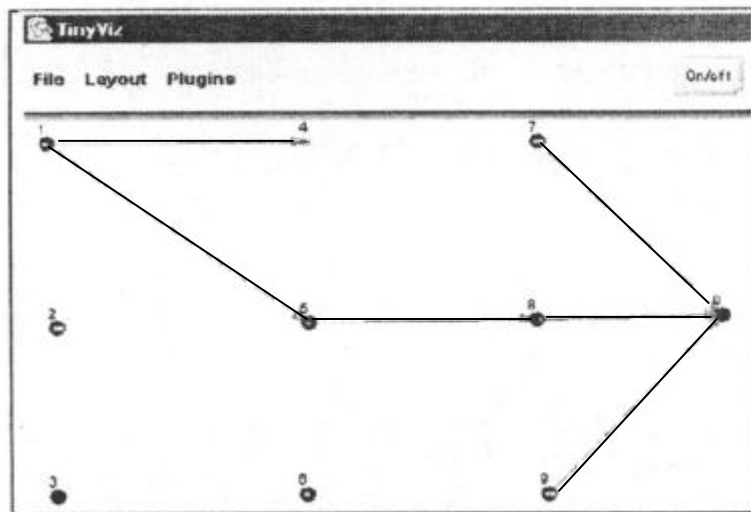


Figure 10 : Diagram indicating that node 4 is off [6]

The above Figure 9 and Figure 10 assigned node 0 as the base station and node 4 is turned off just to observe the change of route drastically taken by node 1. In Figure 10, the data delivery has been re-route through node 5 once node 1 detects that node 4 is no more in service [6]. This whole routing method can be written using Sensor Protocol for Information via Negotiation (SPIN) which emphasizes on data-centric protocol that reduce data redundancy and the rate of loss data packet is extremely low [11]. However, this method is not very efficient since the simulation results indicate that there is not much energy that can be saved through the application of IVCRA as portray in the diagram below (Figure 11).

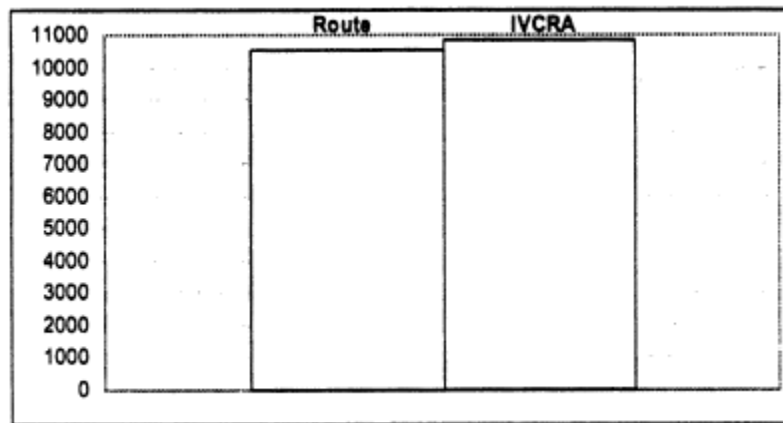


Figure 11 : Energy comparison diagram of routing algorithm with normal packet size [6]

The whole re-routing method can be further improved with the introduction of link-level retransmission and erasure code as described in [10]. Erasure code performs reconstruction of original message to mitigate the loss rate in the network if multiple of additional data packets are sent. As for the link-level retransmission, it is applied in multi-hop application. If a message is lost at specific hop, all the data previously transmitted before the hop will be lost. This method enables all data to be back in originated state through retransmission.

2.3 DETECTION ALGORITHMS IN WIRELESS SENSOR NETWORK (WSN)

With reference to [3], reliability of specific wireless sensor network which consist of large numbers of sensor nodes can be estimated precisely through a proposed algorithm utilizing round trip delay (RTD) time method. The RTD approach initially proposed in research conducted in [13] which required transmission of signal over the internet as it enables enormous numbers of devices from different locations to be connected together. However, internet transmission is discovered to experience larger time delay and more complex than other approaches. Hence, simplification of RTD method is discussed further in details in [3], which basically defines RTD as time taken for a signal to be transmitted from source node through the passageway established consisting of several active nodes and return back to the original source node. The algorithm to identify RTD values from specific trip path is shown through the diagram and expression:

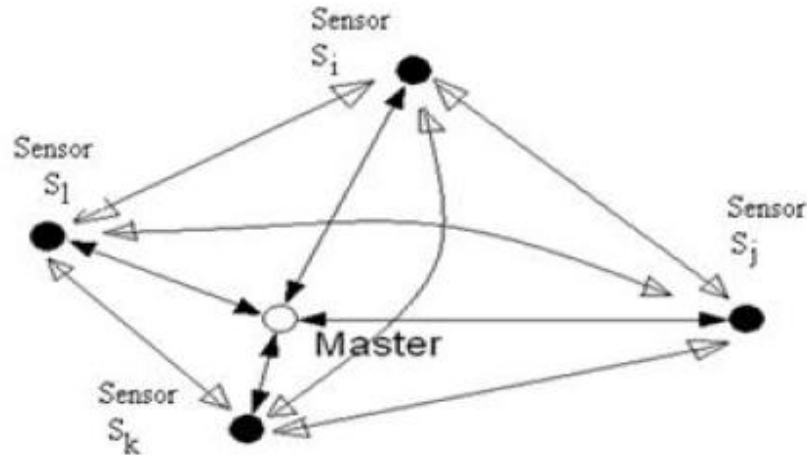


Figure 12 : WSN with four sensor nodes [3]

$$\tau_{RTD} = \tau(i, j) + \tau(j, k) + \tau(k, i) \quad \text{----- (1)}$$

Based on Figure 12, sensor nodes which involve in establishing a passageway for data transmission are S_i , S_j and S_k . The maximum number of trip paths is find out through Equation 1, $n_{RTD} = N(N - m)$, in which n_{RTD} is the maximum number of trip path, N is the total number of sensor nodes available and m is the minimum number of

nodes to be in each trip path which is three (3). From RTD value recorded, the confidence factor of RTD path is analyzed by comparing RTD values with threshold RTD values (maximum time delay values), in order to determine failed or malfunctioning nodes in the network. The expression of the algorithm is illustrated as in Equation 2:

$$\Delta_{\text{RTD}} = \begin{cases} \mathbf{1}, & \tau_{\text{RTD}} < \tau_{\text{RTD-Tr}} \\ \mathbf{0}, & \text{otherwise} \end{cases} \quad \text{----- (2)}$$

Where Δ_{RTD} is the confidence factor, τ_{RTD} is the instantaneous Round Trip Delay (RTD) value, $\tau_{\text{RTD-Tr}}$ is the threshold value. If RTD values are less than the threshold values, then the confidence factor is indicated as “1” which demonstrates that the sensor nodes within specific trip path are in good state and vice versa. This method is an improved method from the one proposed in [14] in which direction of arrival estimation method is impractical since malfunction of sensor nodes is not taking into consideration as the author assumed a case where a sensor does not emit any signal but still initiating signals can be ignored.

On the other hand, Peng Jiang in his paper [15], emphasized on method which focus on the exchange of data among neighbor nodes through testing to determine the status of nodes either at fault or in good condition, based on the majority numbers of neighboring nodes’ results. The proposed algorithm by testing among neighbor nodes mutually can be expressed in Equation 3:

$$\sum_{S_j \in \text{Neighbor}(S_i)} C_{ij} > \frac{\text{Num}(\text{Neighbor}(S_i))}{2} \quad \text{----- (3)}$$

C_{ij} is basically the test result acquired from data collected by sensor nodes, S_i and sensor node, S_j respectively. The node is considered faulty when the test results with neighboring nodes show that $C_{ij}=1$ is more than half of the number of nodes available in network. Otherwise, if the number of neighboring nodes indicating $C_{ij}=0$ is more than half, it would be vice versa and the tested node is noted as in normal state. The value of C_{ij} is obtained when the difference between value of data collected by sensor node, S_i with the value recorded by sensor node, S_j is compared to a certain threshold value. C_{ij} is considered 0 when the result from subtraction between data from sensor node, S_i and

sensor node, S_j does not exceed threshold value and vice versa. The analyses to these algorithms being done after certain criteria are taken into account which fit with the application to be implemented later. Pros and cons between these algorithms are as tabulated in Table 1.

	Advantages	Disadvantages																																									
RTD time method	<ul style="list-style-type: none"> Very efficient as the status of node can be determined precisely (each node's status in each round trip path is identified when trip path's confidence factor value is compared to each other to determine the compromised node) <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th rowspan="2">Round Trip Paths in WSN</th> <th colspan="5">Confidence Factor (Δ_{RTD}) Values</th> </tr> <tr> <th>Case I</th> <th>Case II</th> <th>Case III</th> <th>Case IV</th> <th>Case V</th> </tr> </thead> <tbody> <tr> <td>$S_i-S_j-S_l-S_i$ (RTD-1)</td> <td>0</td> <td>1</td> <td>0</td> <td>0</td> <td>1</td> </tr> <tr> <td>$S_i-S_k-S_l-S_i$ (RTD-2)</td> <td>0</td> <td>0</td> <td>0</td> <td>1</td> <td>1</td> </tr> <tr> <td>$S_i-S_j-S_k-S_i$ (RTD-3)</td> <td>1</td> <td>0</td> <td>0</td> <td>0</td> <td>1</td> </tr> <tr> <td>$S_j-S_k-S_l-S_j$ (RTD-4)</td> <td>0</td> <td>0</td> <td>1</td> <td>0</td> <td>1</td> </tr> <tr> <td>Faulty Sensor Node</td> <td>S_l</td> <td>S_k</td> <td>S_i</td> <td>S_j</td> <td>NIL</td> </tr> </tbody> </table>	Round Trip Paths in WSN	Confidence Factor (Δ_{RTD}) Values					Case I	Case II	Case III	Case IV	Case V	$S_i-S_j-S_l-S_i$ (RTD-1)	0	1	0	0	1	$S_i-S_k-S_l-S_i$ (RTD-2)	0	0	0	1	1	$S_i-S_j-S_k-S_i$ (RTD-3)	1	0	0	0	1	$S_j-S_k-S_l-S_j$ (RTD-4)	0	0	1	0	1	Faulty Sensor Node	S_l	S_k	S_i	S_j	NIL	<ul style="list-style-type: none"> several tests (around 20 times) have to be conducted to get the threshold value
Round Trip Paths in WSN	Confidence Factor (Δ_{RTD}) Values																																										
	Case I	Case II	Case III	Case IV	Case V																																						
$S_i-S_j-S_l-S_i$ (RTD-1)	0	1	0	0	1																																						
$S_i-S_k-S_l-S_i$ (RTD-2)	0	0	0	1	1																																						
$S_i-S_j-S_k-S_i$ (RTD-3)	1	0	0	0	1																																						
$S_j-S_k-S_l-S_j$ (RTD-4)	0	0	1	0	1																																						
Faulty Sensor Node	S_l	S_k	S_i	S_j	NIL																																						
Data-neighboring testing analysis	<ul style="list-style-type: none"> large numbers of sensor nodes can be deployed to ensure the continuous transmission of data/signal 	<ul style="list-style-type: none"> Time consuming process if there are many sensor nodes deployed (has to obtain all of its neighbors' results) The status of node could be misdiagnosed (the tested node could be in good state beforehand. However, if more than half of its neighbors' results indicating $C_{ij}=1$, then the tested node is assumed to be faulty) 																																									

Table 1 : Comparison between algorithms

Thus, RTD time method is the most suitable algorithm to be used in this project since the number of sensor nodes utilized in this project is 4 units in total. Besides that, this method also is a time-efficient method in determining the status of compromised node precisely. However, some improvements will be introduced to the chosen algorithm to cater to its limitation in order to have a more reliable wireless sensor network (WSN).

CHAPTER 3

METHODOLOGY

This project is conducted accordingly till the completion of the project in which desired results are obtained as expected. In Figure 13, the flow of project progress is displayed in orderly manner.

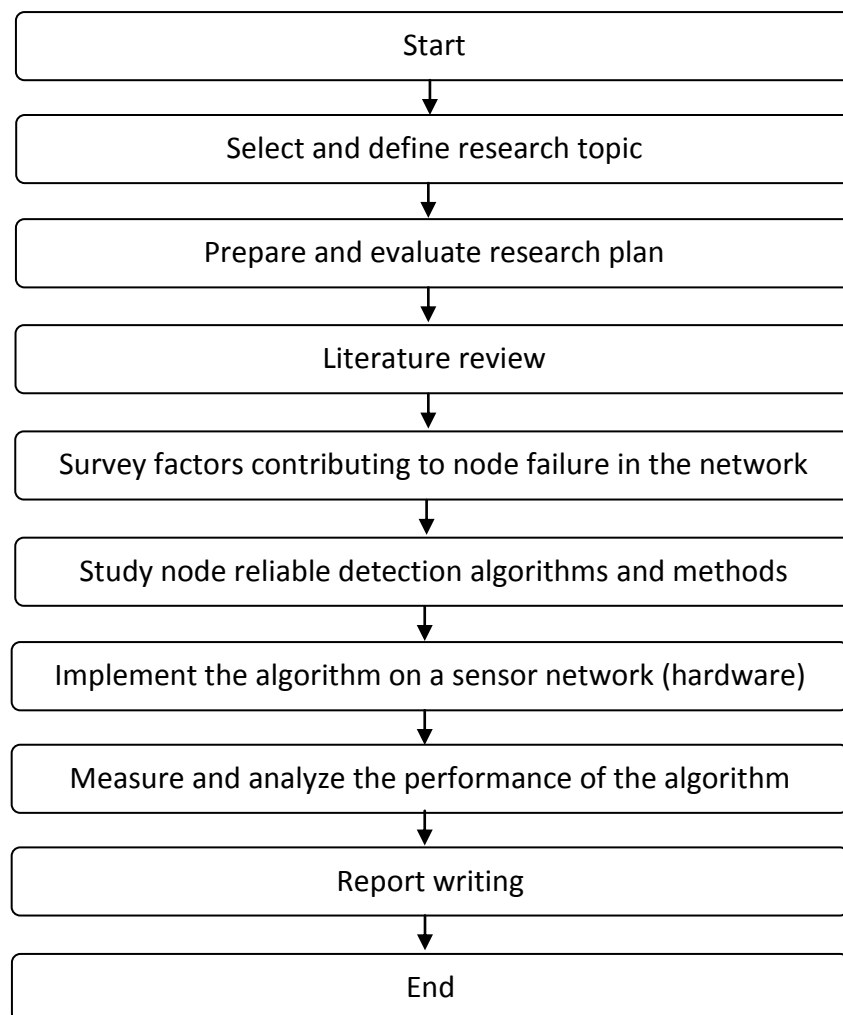




Figure 13 : Flow chart of the project progress

There are few steps taken towards the completion of the project which includes:

1. Implementation of Round Trip Delay (RTD) algorithm described in section 3.1
2. Investigation on the factors influencing sensor node's failure described in section 3.2
3. Tools required described in section 3.3

The initial step carried out is to recognize the type of sensor nodes to be used in this project according to the appropriateness of the application which the sensor nodes are going to be deployed. For this project, IRIS sensor motes are used based on its availability in the market. The specifications of IRIS sensor motes are as tabulated in Table 2.

Table 2: Comparison between IRIS sensor mote with MICAZ sensor mote

Specification	IRIS	MICAZ
		
Memory (RAM, Flash)	8K RAM, 640K Flash	4K RAM, 128K Flash
Microprocessor specification	Atmel Atmega 1281, 8 bit bus	Atmel Atmega 1281, 8 bit bus
Data rate transmission	250 kbps	250 kbps
Outdoor range	>300 m	75 m to 100 m
Indoor range	50 m	20 m to 30 m
Frequency band	2405 MHz to 2480 MHz	2400 MHz to 2483.5 MHz

IRIS sensor mote is basically the improved version from MEMSIC to the one they previously produced which is MICAZ sensor mote. IRIS sensor mote is superior to MICAZ sensor mote in terms of outdoor range which is three times than the outdoor range of MICAZ sensor mote. Besides that, IRIS sensor mote also has twice program memory than previously had by MICAZ sensor mote. The full specifications of IRIS sensor mote as provided by MEMSIC is appended in Appendix 1.

3.1 Implementation of the Round Trip Delay (RTD) Algorithm

The selected algorithm to be implemented in this project would be an approach which focuses on obtaining round trip delay (RTD) time value for respective round trip path (RTP) available in WSN. RTD time is generally the time taken for the signal/data being transmitted from source node through several active nodes in the trip path and back to the source node again. Motework software is used to write coding in nesC language and enable the user to install the specific coding program onto sensor motes. Then, a software known as Xsniffer is utilized to record the time delay (RTD) for the data to be transmitted along the trip path. Basically, Xsniffer acts as an interface between a user and deployed network of wireless sensor which enables the user to monitor and analyze the data received from sensor nodes as well as display the time taken for the data to be delivered in each hop network involved. Figure 14 shows the example of Xsniffer's screen display.

The screenshot shows the XSniffer application window with a menu bar (Log, All, Route, Health, Neighbor, Time Sync, Options) and a data table. The table has columns for Id, Seq#, Hops, Parent, Cost, Entries, Id1, Est1, Id2, Est2, Id3, Est3, Id4, Est4, Id5, Est5, Msg#, and Time. The data rows are as follows:

Id	Seq#	Hops	Parent	Cost	Entries	Id1	Est1	Id2	Est2	Id3	Est3	Id4	Est4	Id5	Est5	Msg#	Time
000	30	0	126	0	2	15	255	25	255							11	5
005	71	2	15	8	3	25	255	0	240	15	255					19	23
015	98	1	0	4	3	5	255	0	240	25	255					29	66
025	110	1	0	4	3	5	255	0	255	15	255					29	2

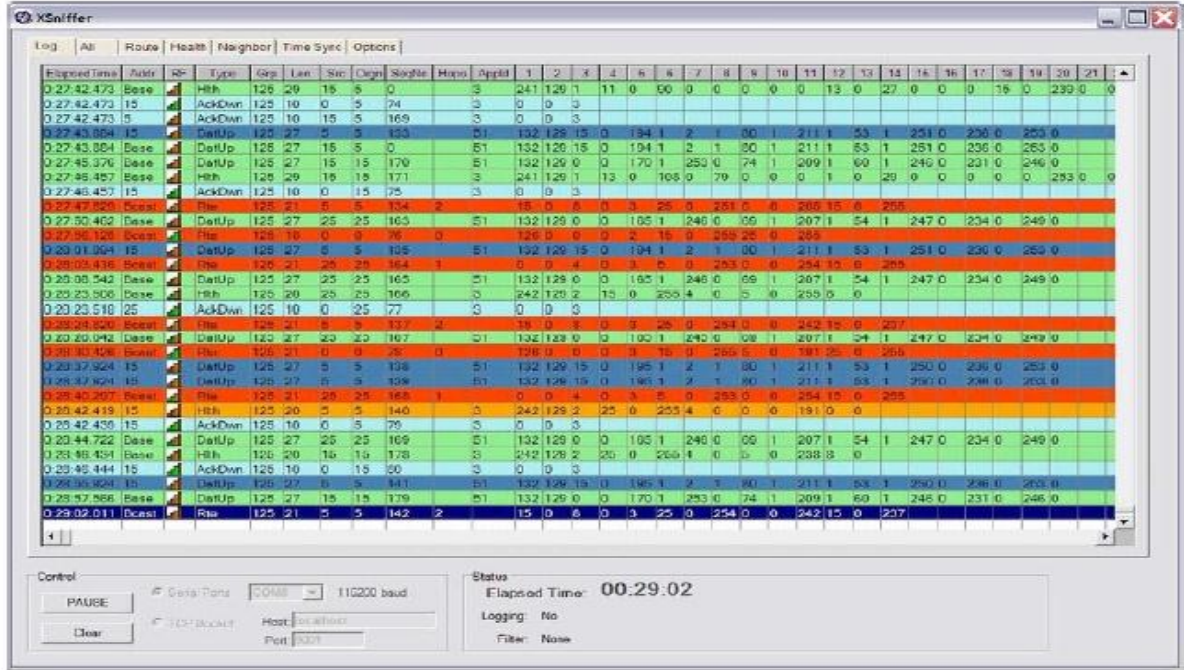


Figure 14 : Xsniffer's screen display user interface

In this project, total number of sensor nodes to be deployed would be 4 units. The maximum number of trip paths available in the implemented WSN would be 4 based on the Equation 4:

$$n_{RTD} = N(N - m) = 4(4 - 3) = 4 \text{ trip paths} \text{ ----- (4)}$$

Where n_{RTD} is the total number of round trip paths, N is the number of sensor nodes available, m is the minimum number of sensor nodes in a single round trip path.

In general, IRIS motes which are being used in this project have operating battery voltage range of 2.5 V until 3.6 V. The threshold value for specific RTP is acquired when at least a sensor node deployed in the network has the minimum operating battery voltage level of 2.5 V. The operating battery voltage of 2.5 V is set as the indication point. Thus, the time recorded to transmit the signal around a specific RTP which involve at least a sensor node being powered by 2.5 V is noted as the maximum time delay (threshold value). Any sensor node which has battery voltage level below than 2.5 V theoretically will consume more time to transmit signal as it affects the signal strength of sensor node

to be lower which subsequently exceed the threshold value and will be noted as faulty. Once instantaneous RTD values for respective RTPs are obtained, these values will be compared with the threshold value to determine the confidence factor of each trip path (RTP) before the results are tabulated accordingly to identify the compromised sensor node. The selected Round Trip Delay (RTD) algorithm works as follows:

Algorithm of Round Trip Delay (RTD) :

[Instantaneous RTD time \geq Threshold Value = 0] \rightarrow sensor node in trip path noted as faulty

[Instantaneous RTD time $<$ Threshold Value = 1] \rightarrow no faulty node in trip path

In order to acquire all the necessary data require proofing that the selected algorithm could provide a reliable WSN, the experimental procedures to be carried out are well prepared and organized as in Figure 15.

EXPERIMENTAL PROCEDURES TO DETERMINE FAULTY SENSOR NODE

1. Several topology arrangements are designed in order to have symmetrical and unsymmetrical topology arrangements for WSN
2. Every RTP in topology arrangements consist of a sensor node being powered up by the minimum operating battery voltage level (2.5 V) are run for multiple of times (around 20 times) to obtain the maximum delay value which is the threshold round trip delay time.
3. Run the coding on the hardware. The coding used to establish the connection between nodes
4. Determine instantaneous RTD value of each round trip path in the network. Then, the results obtained are tabulated accordingly
5. Estimate the sensor node at fault by knowing the confidence factor value (either 0 or 1)
6. In order to implement the algorithm back on the hardware after the faulty node is determined, routing process will be carried out in which the sensor node will be broadcasting its signal to other available nodes within range excluded the faulty node determined earlier.

Figure 15: Experimental procedures to determine faulty node

3.2 Investigation On The Factors Influencing Sensor Node's Failure

Distance from sensor nodes to the base station node has been recognized as one of the factors which could have significant influences on the failure rate of sensor nodes in WSN. Therefore, a number of experiments are scheduled to be carried out to study on the impacts that various distances between sensor nodes and base station node factor could have on the signal strength and data packets lost on a specific sensor node. In these experiments, a single hop network consists of only 2 sensor nodes is used in order to ease the process of getting the readings of signal strength and data packets received at the base station node. However, the battery voltage of the sensor node is kept constant at 3.0 V. The procedures are organized as in Figure 16

EXPERIMENTAL PROCEDURES TO STUDY THE EFFECTS OF DISTANCE BETWEEN SENSOR NODE AND BASE STATION NODE ON DATA PACKETS LOST AND SIGNAL STRENGTH

1. A single hop network (2 sensor nodes) is used and being placed at various distances from the base station node.

2. The distances are fixed to be at 10 cm, 30 cm, 60 cm , 90 cm and keeps on increasing from the base station node

3. Run the coding on the hardware. The coding used to establish the connection between nodes

4. Observe the pattern of the data received by the base station node.

Figure 16: Experimental procedures to investigate on factors affecting reliability of WSN

3.3 TOOLS REQUIRED

The tools required to carry out this project are determined to be:

- **Wireless sensor nodes (4 units)**

Because of the advantages of IRIS sensor motes over other types of sensor motes, IRIS sensor motes are utilized in this project in order to have a reliable WSN.

- **Low voltage battery (AA batteries)**

A single sensor mote required two units of AA battery to be powered up. The operating voltage range for every IRIS sensor mote is from 3.6 V to 2.5 V

- **Tinyos/Motework programming software**

Motework software is used specifically to upload programs onto deployed sensor nodes in the network. Besides that, a user interface known as Xsniffer also is used to display data transmitted by every nodes involved

3.4 KEY MILESTONE

The approach of this project is based on examination and understanding of the scope of work and the timing for the completion of the project. In accordance with the milestones provided in the guideline for final year project, several have been identified and summarized for FYP I and FYP II in Table 3 and Table 4 respectively.

Table 3: Key Milestone for FYP I

Key Milestone	Proposed Week
Submission of Extended Proposal Defense	Week 6
Proposal Defense	Week 9
Submission of Interim Draft Report	Week 13
Submission of Interim Report	Week 14

Table 4: Key Milestone for FYP II

Key Milestone	Proposed Week
Submission of Progress Report	Week 8
Pre-EDX	Week 11
Submission of Draft Report	Week 12
Submission of Dissertation (soft bound)	Week 13
Submission of Technical Paper	Week 13
Oral Presentation	Week 14
Submission of Project Dissertation (hard bound)	Week 15

The expected challenges that will be encountered in implementing a reliable sensor nodes network would be in programming the sensor nodes using Tinyos software (nesC language) in order to extract the function of specific nodes onto the hardware. This is because the node's database and specification have to be studied in depth to establish successful link connections between the nodes. Besides that, there might be a difficulty in analyzing the data received from nodes as the simulator in tinyos software is tends to be

affected by discrepancy in data values if there are more than one factors act on the specific sensor nodes.

3.5 GANTT CHART

Project activities and work process flows for FYP I are explained as in Table 5 and for FYP II are described in Table 6.

Table 5: Gantt chart representing the process flows for FYP I

Detail/Week	1	2	3	4	5	6	7	8	9	10	11	12	13	14	
Selection of Project Topic							Mid-Semester Break								
Preliminary Research Work <ul style="list-style-type: none"> • Determining the factors affecting network reliability • Identify the most suitable algorithm 															
Submission of Extended Proposal															
Proposal Defense															
Continuation of Project work <ul style="list-style-type: none"> • Information gathering (research on algorithm) • Start-off activities 															
Submission of Interim Draft Report															
Submission of Interim Report															

Table 6: Gantt chart representing the process flows for FYP II

Detail/Week	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Preliminary Research Work <ul style="list-style-type: none"> Working on the algorithm using Motework/Tinyos 	█	█	█	█	█	█	Mid-Semester Break									
<ul style="list-style-type: none"> Analyze the result obtain (able to predict node failure) 						█		█	█							
Submission of Progress Report								█								
Pre Sedex										█						
<ul style="list-style-type: none"> Validate the accuracy of data obtained from resulted algorithm 									█	█	█					
Submission of Draft Report												█				
Submission of dissertation (soft bound)													█			
Submission of technical paper													█			
Oral Presentation														█		
Submission of dissertation (hard bound)															█	

CHAPTER 4

RESULTS AND DISCUSSION

This section presents the results of the experiment conducted together with the analysis pertaining to the results obtained.

4.1 Implementation of the Round Trip Delay (RTD) Algorithm

4.1.1 Network Topologies Set-up

The initial step carried out was to come out with several topology arrangements with various lengths indicating the distances from the node's location being deployed to its neighboring nodes. Generally, there were two types of topologies utilized in this experiment which consist of symmetrical and unsymmetrical topologies. With reference to works done in [3], symmetrical topology used was found to be irrelevant prior to various distances among sensor nodes which is usually unsymmetrical to each other being deployed in real applications field. Thus, unsymmetrical topologies were introduced in this project to cater for the limitation in [3] for the implementation of the actual Wireless Sensor Network (WSN).

➤ **Symmetrical Topology Arrangements**

Under symmetrical topologies classification, Topology arrangement 1 (Figure 17) and Topology arrangement 2 (Figure 18) were symmetrically distributed (equal distance between each neighboring nodes). In both topologies, all of the trip paths share the same threshold values which are 28 seconds for Topology arrangement 1 and 27 seconds for

topology arrangement 2. It is notable that Topology arrangement 1 has bigger threshold value compare to Topology arrangement 2. This is evidently because of the distance between each sensor nodes deployed in Topology arrangement 1 is larger than the distance between each sensor nodes used in Topology arrangement 2. The longer the distances between neighboring nodes, the time taken for the message to be successfully delivered will increase. Threshold values for both symmetrical and unsymmetrical topology arrangements were recorded when sensor nodes deployed in the network has the minimum operating battery voltage level of 2.5 V. Once the instantaneous time taken to deliver data in specific Round Trip Path (RTP) exceeds the threshold value, the user acknowledge that the battery level of sensor nodes deployed could possibly falls below than 2.5 V or is significantly affected by other factors as well.

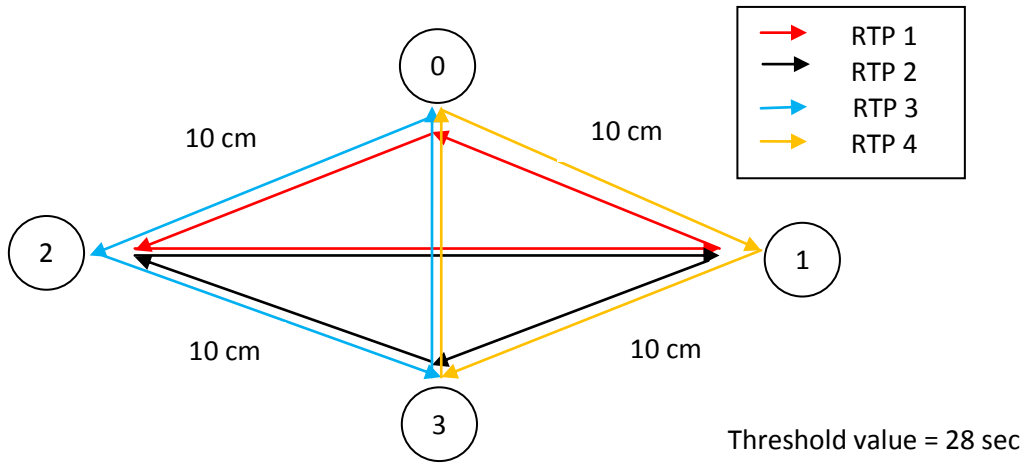


Figure 17: Topology Arrangement 1

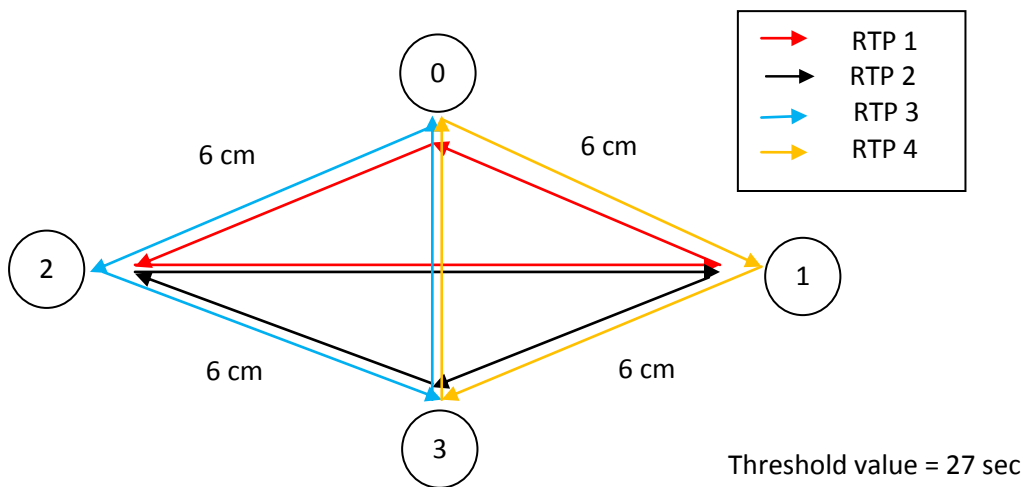


Figure 18: Topology Arrangement 2

➤ **Unsymmetrical Topology Arrangements**

Meanwhile, in Figure 19 and Figure 20, Topology arrangement 3 and Topology arrangement 4 display the position of sensor nodes deployed in WSN which are unsymmetrical to each other (distance varies between each neighboring sensor nodes). Each round trip path (RTP) has different threshold values with accordance to its distance from the neighboring sensor nodes. The needs for unsymmetrical topologies arrangement to be taken into account could be very important in order to have a reliable WSN in practice.

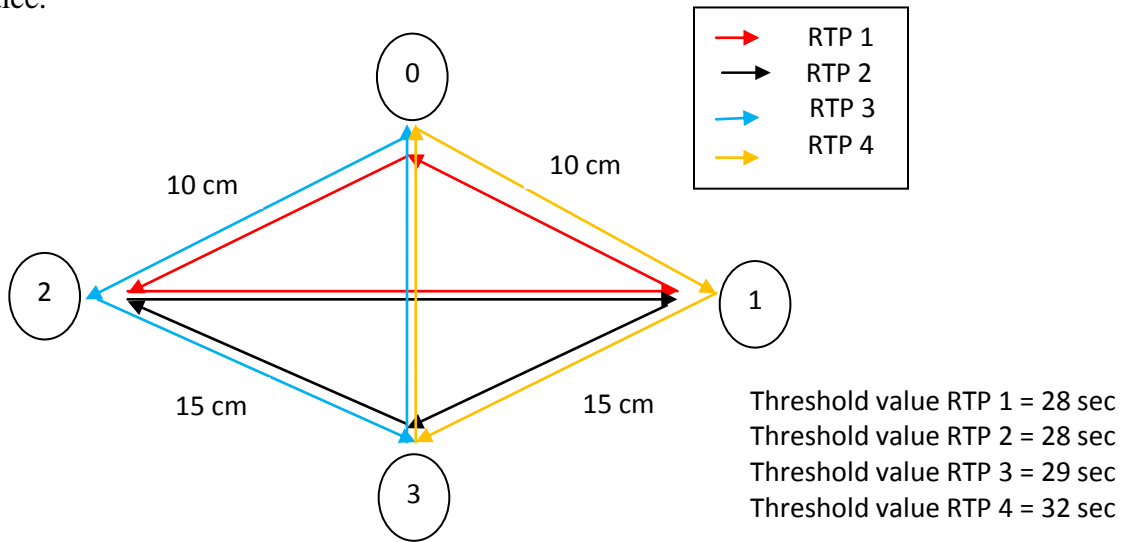


Figure 19: Topology Arrangement 3

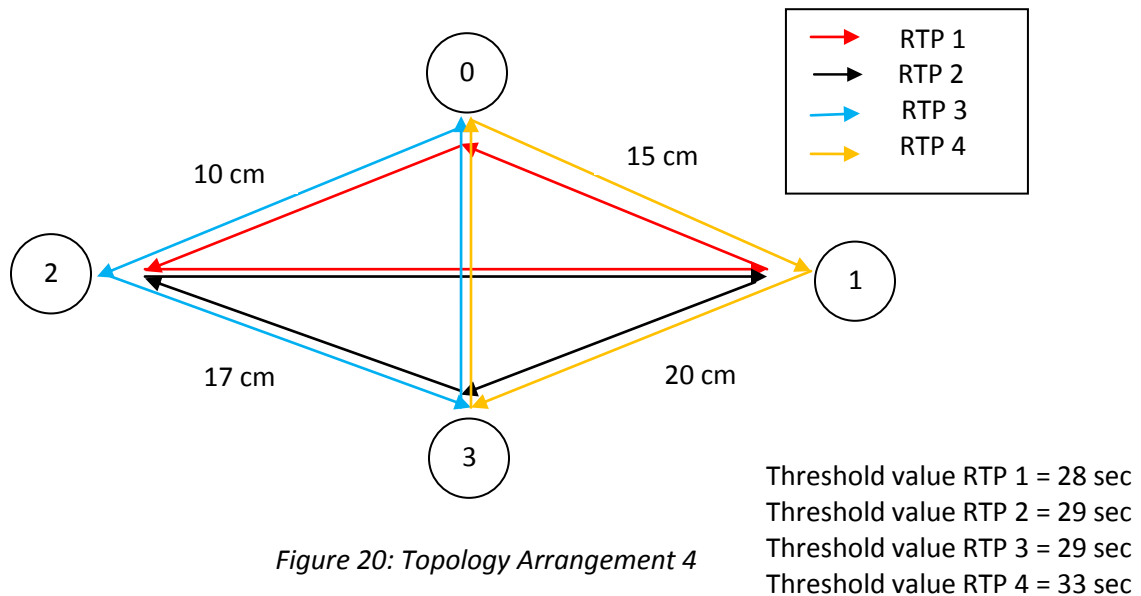


Figure 20: Topology Arrangement 4

4.1.2 Testing Faulty Condition Of The Topology Arrangements

A series of experiments were conducted to testify on the precision of the selected algorithm to determine the faulty node. Basically, two conditions were used to evaluate the status of sensor nodes in each topologies or networks as in section 4.1.1. The first condition was set up in a way that all sensor nodes deployed in the network have battery voltage level to be more than 2.5 V to indicate no failure. Next, one of the sensor nodes in the networks (sensor node 1) was purposely being powered by 2.4 V which is less than 2.5 V and the results obtained should comply with the expected outcome based on the algorithm. This was made to be the second conditions of the experiment. Whichever sensor nodes that have battery voltage level to be less than 2.5 V should be indicated as faulty. Battery voltage level of 2.5 V was selected as the indication level because it is the minimum operating battery voltage for IRIS motes which ranges from 3.6 V to 2.5 V. These are the results obtained from the experiments:

Condition 1: All deployed nodes have battery voltage more than the indication voltage level (> 2.5 V)

Algorithm of Round Trip Delay (RTD) :

[Instantaneous RTD time \geq Threshold Value = 0] \rightarrow sensor node in trip path noted as faulty

[Instantaneous RTD time < Threshold Value = 1] \rightarrow no faulty node in trip path

Symmetrical Topology Arrangements

TOPOLOGY 1 (TABLE 7)

Trip Path	Nodes Involved	Instantaneous RTD time	Confidence Factor
RTP 1	Node 1 \rightarrow Node 0 \rightarrow Node 2 \rightarrow Node 1	27 seconds	1
RTP 2	Node 1 \rightarrow Node 3 \rightarrow Node 2 \rightarrow Node 1	27 seconds	1
RTP 3	Node 3 \rightarrow Node 0 \rightarrow Node 2 \rightarrow Node 3	27 seconds	1
RTP 4	Node 1 \rightarrow Node 3 \rightarrow Node 0 \rightarrow Node 1	27 seconds	1
Faulty node :			NONE

TOPOLOGY 2 (TABLE 8)

Trip Path	Nodes Involved	Instantaneous RTD time	Confidence Factor
RTP 1	Node 1 → Node 0 → Node 2 → Node 1	26 seconds	1
RTP 2	Node 1 → Node 3 → Node 2 → Node 1	25 seconds	1
RTP 3	Node 3 → Node 0 → Node 2 → Node 3	26 seconds	1
RTP 4	Node 1 → Node 3 → Node 0 → Node 1	26 seconds	1
Faulty node :			NONE

Unsymmetrical Topology Arrangements

TOPOLOGY 3 (TABLE 9)

Trip Path	Nodes Involved	Instantaneous RTD time	Confidence Factor
RTP 1	Node 1 → Node 0 → Node 2 → Node 1	27 seconds	1
RTP 2	Node 1 → Node 3 → Node 2 → Node 1	27 seconds	1
RTP 3	Node 3 → Node 0 → Node 2 → Node 3	26 seconds	1
RTP 4	Node 1 → Node 3 → Node 0 → Node 1	31 seconds	1
Faulty node :			NONE

TOPOLOGY 4 (TABLE 10)

Trip Path	Nodes Involved	Instantaneous RTD time	Confidence Factor
RTP 1	Node 1 → Node 0 → Node 2 → Node 1	27 seconds	1
RTP 2	Node 1 → Node 3 → Node 2 → Node 1	28 seconds	1
RTP 3	Node 3 → Node 0 → Node 2 → Node 3	28 seconds	1
RTP 4	Node 1 → Node 3 → Node 0 → Node 1	30 seconds	1
Faulty node :			NONE

Since all of sensor nodes utilized in the both types of topology arrangements have battery voltage level to be more than 2.5 V, the results obtained as tabulated in the look-up tables (Table 7, Table 8, Table 9 and Table 10) indicate that none of the nodes were detected to be faulty. Instantaneous RTD times for every RTP in all topology arrangements were recorded to be less than the threshold values. Besides that, all of the sensor nodes also were found not to be affected by other factors which results in instantaneous RTP time to be less than threshold values.

Condition 2: One of the node in network has battery voltage to be less than the indication voltage level (< 2.5 V)

❖ Let Node 1 be the node which has a battery voltage of 2.4 V

Algorithm of Round Trip Delay (RTD) :

[Instantaneous RTD time \geq Threshold Value = 0] \rightarrow sensor node in trip path noted as faulty

[Instantaneous RTD time < Threshold Value = 1] \rightarrow no faulty node in trip path

Symmetrical Topology Arrangements

TOPOLOGY 1 (TABLE 11)

Trip Path	Nodes Involved	Instantaneous RTD time	Confidence Factor
RTP 1	Node 1 \rightarrow Node 0 \rightarrow Node 2 \rightarrow Node 1	28 seconds	0
RTP 2	Node 1 \rightarrow Node 3 \rightarrow Node 2 \rightarrow Node 1	28 seconds	0
RTP 3	Node 3 \rightarrow Node 0 \rightarrow Node 2 \rightarrow Node 3	27 seconds	1
RTP 4	Node 1 \rightarrow Node 3 \rightarrow Node 0 \rightarrow Node 1	34 seconds	0
Faulty node :			NODE 1

TOPOLOGY 2 (TABLE 12)

Trip Path	Nodes Involved	Instantaneous RTD time	Confidence Factor
RTP 1	Node 1 \rightarrow Node 0 \rightarrow Node 2 \rightarrow Node 1	28 seconds	0
RTP 2	Node 1 \rightarrow Node 3 \rightarrow Node 2 \rightarrow Node 1	27 seconds	0
RTP 3	Node 3 \rightarrow Node 0 \rightarrow Node 2 \rightarrow Node 3	26 seconds	1
RTP 4	Node 1 \rightarrow Node 3 \rightarrow Node 0 \rightarrow Node 1	32 seconds	0
Faulty node :			NODE 1

Unsymmetrical Topology Arrangements

TOPOLOGY 3 (TABLE 13)

Trip Path	Nodes Involved	Instantaneous RTD time	Confidence Factor
RTP 1	Node 1 \rightarrow Node 0 \rightarrow Node 2 \rightarrow Node 1	28 seconds	0
RTP 2	Node 1 \rightarrow Node 3 \rightarrow Node 2 \rightarrow Node 1	28 seconds	0
RTP 3	Node 3 \rightarrow Node 0 \rightarrow Node 2 \rightarrow Node 3	27 seconds	1
RTP 4	Node 1 \rightarrow Node 3 \rightarrow Node 0 \rightarrow Node 1	32 seconds	0
Faulty node :			NODE 1

TOPOLOGY 4 (TABLE 14)

Trip Path	Nodes Involved	Instantaneous RTD time	Confidence Factor
RTP 1	Node 1 → Node 0 → Node 2 → Node 1	28 seconds	0
RTP 2	Node 1 → Node 3 → Node 2 → Node 1	30 seconds	0
RTP 3	Node 3 → Node 0 → Node 2 → Node 3	27 seconds	1
RTP 4	Node 1 → Node 3 → Node 0 → Node 1	35 seconds	0
Faulty node :			NODE 1

With reference to the results obtained (Table 11 until Table 14), sensor node 1 has been deployed in all round trip paths except for RTP 3. This is the reason for sensor nodes deployed in RTP 3 not being faulty and always gets confidence factor value to be equal to 1. Meanwhile, for the remaining round trip paths (RTP 1, RTP 2 and RTP 4) which consist of faulty sensor node 1 (battery voltage less than 2.5 V for condition 2) have confidence factor value to be equal to 0. Thus, the algorithm utilized in this network is proven to be correct as the battery voltage level decreases less than 2.5 V, the instantaneous RTD time taken to deliver the message will exceeds the threshold value of respective round trip paths.

4.2 Investigation On The Factors Influencing Sensor Node's Failure

To conduct researches on Wireless Sensor Network (WSN), there are many aspects that have to be studied in details and one of them is recognize to be the factors that could have significant influences on the failure rate of sensor nodes. In this project, the scope of study has been narrowed down only to focus on the impacts that distance between neighboring nodes factor could has on the signal strength of sensor nodes and the rate of data packets lost in WSN. Ideally, as the battery voltage level getting smaller, the strength of signal emitted by sensor nodes also will be significantly affected. The longer the distance of specific sensor nodes from the base station, the number of data being transmitted could possibly lost along the transmission process. A test was carried out in a fixed room condition to clarify on the number of data packets lost along the transmission process. The distances between sensor node and base station node were varied to observe the amount of ambient light measurement readings recorded by the base station node corresponding to its distances. To ease the process of the experiment, only

one hop network was utilized and the distance between this node and base station node were made to be variety. The illustration of the sensor node being placed inside the room is as displayed in Figure 21:

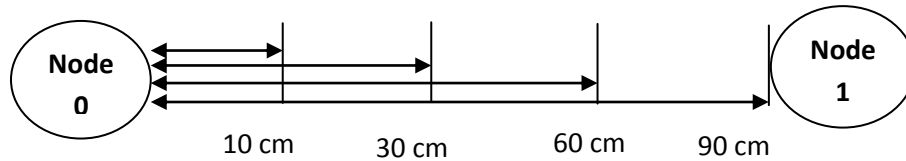


Figure 21: Arrangement of sensor nodes

In Figure 21, sensor node 1 was used to sense the readings, meanwhile sensor node 0 which acted as the base station node, recorded the readings that it received. The battery voltage of sensor node 1 used in this test is kept constant to be at 3.0 V and these are the results obtained (Table 15 and Figure 22):

Distance from base station node	Light readings recorded by the base station node (Joule)
10 cm	88
30 cm	85
60 cm	83
90 cm	82

Table 15: Readings of Light Measurement in a room

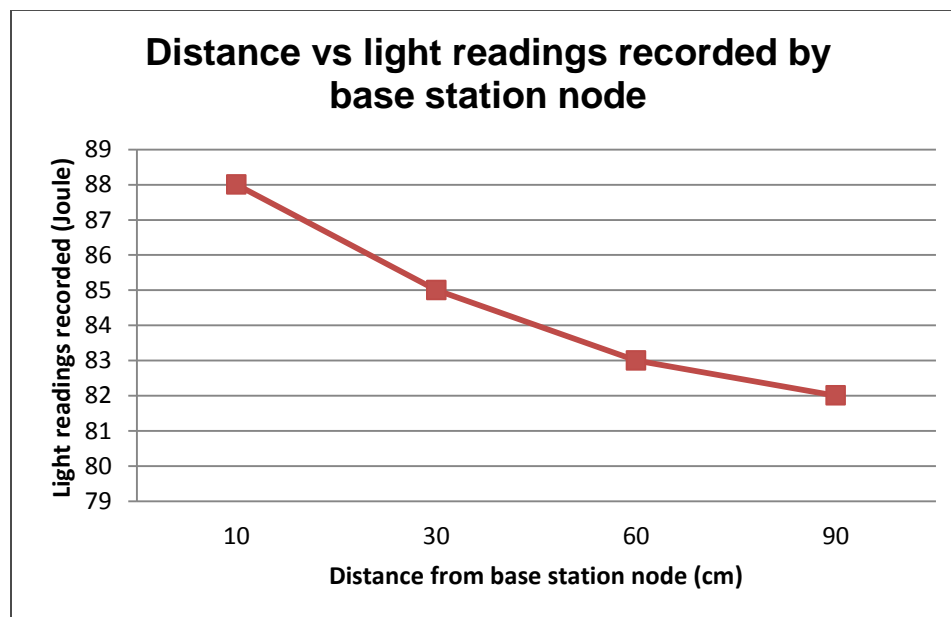


Figure 22: Graph of distance from base station node against light readings recorded by base station node

The pattern of the readings recorded in Table 15 and Figure 22, was observed to be decreasing as the distances between sensor node and base station node keep on increasing. The likelihood for the transmitted data packets to be lost along the transmission process increases as the distances between sensor nodes also increases. Thus, the results conclude that the signal transmitted which carry the data is lost to the surrounding and the base station node failed to receive the exact actual amount of data sensed by another sensor node as the distances between sensor nodes increase.

On the other hand, the experiment to clarify on the loss of signal strength as the distances of sensing sensor node from base station node being varied was also conducted. The illustration of the locations of sensing sensor node from base station node is displayed in Figure 23.

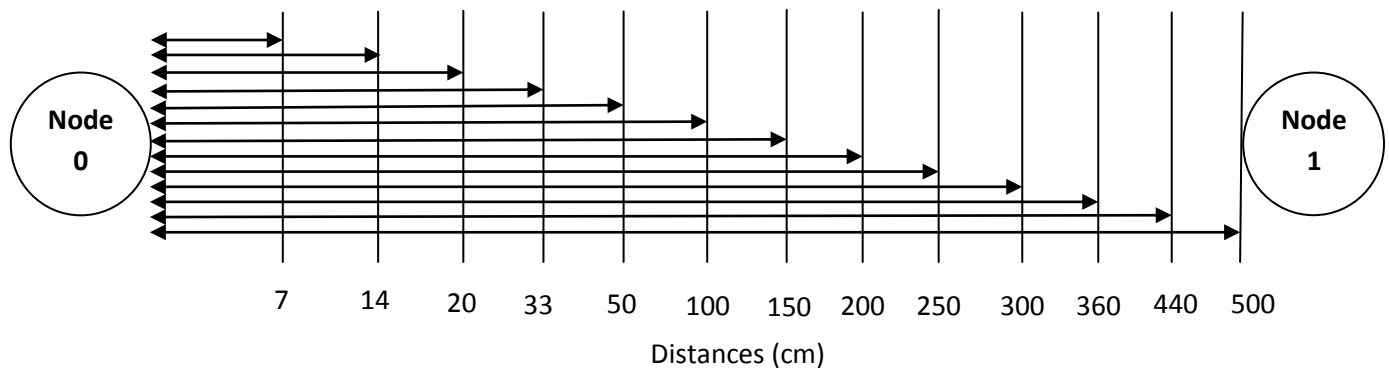


Figure 23: Arrangement of sensor nodes

In Figure 23, sensor node 1 was used to sense the readings, meanwhile sensor node 0 which acted as the base station node, recorded the values of the signal strength it received from sensor node 1. The battery voltage of sensor node 1 used in this test is kept constant to be at 3.0 V and the results obtained are tabulated in Table 16.

Distance from base station (cm)	Signal strength (dbm)
7	5
14	5
20	4
33	4
50	3
100	3
150	3
200	3
250	2
300	2
360	1
440	1
500	0

Table 16: Readings of signal strength recorded by the base station node

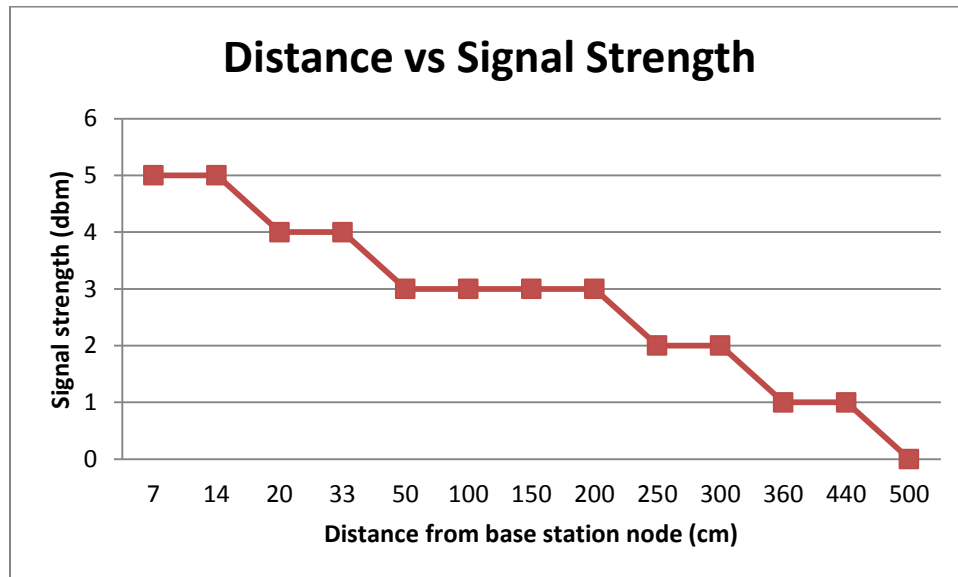


Figure 24: Graph of distance from base station node against signal strength recorded by base station node

The graphical display in Figure 24 indicates the decreasing of the value in signal strength as the distance of sensing node from base station node increases. The originated signal from the sensing sensor node 1 is loss to the surrounding which is determined to be influenced by environmental factor. As the result, the base station failed to record the actual amount of data from sensor node 1 (as in Figure 22) because the loss in signal strength indirectly relates to the failure of data packets to be delivered from sensing sensor node to the base station node. Besides that, the base station node also will experiences and indicates loss in signal strength if there is obstruction in the established hop network. The obstruction will somehow block the delivered signal and only allow certain values of signal from the original signal to be directed towards the base station node.

CHAPTER 5

CONCLUSION AND RECOMMENDATION

The main goal of this project ideally is to develop an algorithm which enables users to anticipate and detect compromised sensor node in the network. This is because a specific wireless sensor network is presumed as reliable when the system is able to detect compromised node precisely and further required actions can be taken either to replace the node or others. Thus, the algorithm chosen based on Round Trip Delay (RTD) time has been implemented on hardware and the analysis to the results obtained has been carried out from the data display in Xsniffer software. The performance of the selected algorithm on the other hand, provides accurate results as in theoretical approach. Besides that, the effect of factors such as distance and obstruction could have on the reliability of WSN also have been studied and the results obtained are presented in the graphical display.

As for the recommendation, rechargeable batteries to power up the sensor nodes should be utilized should the normal AA batteries' lifetime are much shorter. This is very significant to ensure that the project is very cost-effective. The inability of the algorithm to determine more than a single compromised sensor node is regarded as the disadvantage of the algorithm. However, this problem can be overcome by having large numbers of Round Trip Path (RTP) within the network which somehow complicate the users to analyze and manually tabulated the results in look up table.

CHAPTER 6 : REFERENCES

- [1] J.-J. Lee, B. Krishnamachari, and C.-C. J. Kuo, "Impact of energy depletion and reliability on wireless sensor network connectivity," in *Defense and Security*, 2004, pp. 169-180.
- [2] Y.-T. Wang and R. Bagrodia, "ComSen: A Detection System for Identifying Compromised Nodes in Wireless Sensor Networks," in *SECURWARE 2012, The Sixth International Conference on Emerging Security Information, Systems and Technologies*, 2012, pp. 148-156.
- [3] A. N. Ducher and N. Sarwade, "Sensor node failure or malfunctioning detection in wireless sensor network," *Aceee International Journal on Communication*, vol. 3, 2012.
- [4] L. Krishnamachari, D. Estrin, and S. Wicker, "The impact of data aggregation in wireless sensor networks," in *Distributed Computing Systems Workshops, 2002. Proceedings. 22nd International Conference on*, 2002, pp. 575-578.
- [5] S. Sajadian, A. Ibrahim, E. P. de Freitas, and T. Larsson, "Improving Connectivity of Nodes in Mobile WSN," in *Advanced Information Networking and Applications (AINA), 2011 IEEE International Conference on*, 2011, pp. 364-371.
- [6] A. A. Minhas, C. Steger, R. Wei, and M. S. Ehsan, "Node failure detection and path repairing scheme in virtual circuit routing algorithm for wireless ad hoc micro sensor networks," in *Emerging Technologies, 2005. Proceedings of the IEEE Symposium on*, 2005, pp. 86-91.
- [7] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, pp. 2292-2330, 8/22/ 2008.
- [8] K. Lorincz, D. J. Malan, T. R. F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, *et al.*, "Sensor networks for emergency response: challenges and opportunities," *Pervasive Computing, IEEE*, vol. 3, pp. 16-23, 2004.
- [9] J. Shin, "Multi-object Tracking and Identity Management in Wireless Sensor Networks," Stanford University, 2004.
- [10] S. Kim, R. Fonseca, and D. Culler, "Reliable transfer on wireless sensor networks," in *Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on*, 2004, pp. 449-459.
- [11] Z. Reheana, K. Kumar, S. Roy, and N. Mukherjee, "SPIN implementation in TinyOS environment using nesC," in *Computing Communication and Networking Technologies (ICCCNT), 2010 International Conference on*, 2010, pp. 1-6.
- [12] C. F. García-Hernández, P. H. Ibarquengoytia-Gonzalez, J. García-Hernández, and J. A. Pérez-Díaz, "Wireless sensor networks and applications: a survey," *IJCSNS International Journal of Computer Science and Network Security*, vol. 7, pp. 264-273, 2007.
- [13] W. Hu, G.-P. Liu, and D. Rees, "Networked predictive control over the Internet using round-trip delay measurement," *Instrumentation and Measurement, IEEE Transactions on*, vol. 57, pp. 2231-2241, 2008.
- [14] T. W. Pirinen, J. Yli-Hietanen, P. Pertila, and A. Visa, "Detection and compensation of sensor malfunction in time delay based direction of arrival estimation," in *Circuits and Systems, 2004. ISCAS'04. Proceedings of the 2004 International Symposium on*, 2004, pp. IV-872-5 Vol. 4.
- [15] P. Jiang, "A new method for node fault detection in wireless sensor networks," *Sensors*, vol. 9, pp. 1282-1294, 2009.

Specifications of IRIS sensor mote

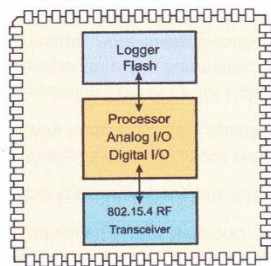
IRIS

WIRELESS MEASUREMENT SYSTEM

- 2.4 GHz IEEE 802.15.4, Tiny Wireless Measurement System
- Designed Specifically for Deeply Embedded Sensor Networks
- 250 kbps, High Data Rate Radio
- Wireless Communications with Every Node as Router Capability
- Expansion Connector for Light, Temperature, RH, Barometric Pressure, Acceleration/Seismic, Acoustic, Magnetic and other MEMSIC Sensor Boards

Applications

- Indoor Building Monitoring and Security
- Acoustic, Video, Vibration and Other High Speed Sensor Data
- Large Scale Sensor Networks (1000+ Points)



XM2110CA Block Diagram



IRIS

The IRIS is a 2.4 GHz Mote module used for enabling low-power, wireless sensor networks. The IRIS Mote features several new capabilities that enhance the overall functionality of MEMSIC's wireless sensor networking products.

Product features include:

- Up to three times improved radio range and twice the program memory over previous MICA Motes
- Outdoor line-of-sight tests have yielded ranges as far as 500 meters between nodes without amplification
- IEEE 802.15.4 compliant RF transceiver
- 2.4 to 2.48 GHz, a globally compatible ISM band
- Direct sequence spread spectrum radio which is resistant to RF interference and provides inherent data security
- 250 kbps data rate
- Supported by MoteWorks™ wireless sensor network platform for reliable, ad-hoc mesh networking
- Plug and play with MEMSIC's sensor boards, data acquisition boards, gateways, and software

MoteWorks™ enables the development of custom sensor applications and is specifically optimized for low-power,

battery-operated networks. MoteWorks is based on the open-source TinyOS operating system and provides reliable, ad-hoc mesh networking, over-the-air-programming capabilities, cross development tools, server middleware for enterprise network integration and client user interface for analysis and configuration.

Processor & Radio Platform

The XM2110CB is based on the Atmel ATmega1281. The ATmega1281 is a low-power microcontroller which runs MoteWorks from its internal flash memory. A single processor board (XM2110) can be configured to run your sensor application/processing and the network/radio communications stack simultaneously. The IRIS 51-pin expansion connector supports Analog Inputs, Digital I/O, I2C, SPI and UART interfaces. These interfaces make it easy to connect to a wide variety of external peripherals.

Sensor Boards

MEMSIC offers a variety of sensor and data acquisition boards for the IRIS Mote. All of these boards connect to the IRIS via the standard 51-pin expansion connector. Custom sensor and data acquisition boards are also available. Please contact MEMSIC for additional information.

Processor/Radio Board	XM2110CB	Remarks
Processor Performance		
Program Flash Memory	128K bytes	
Measurement (Serial) Flash	512K bytes	> 100,000 Measurements
RAM	8K bytes	
Configuration EEPROM	4K bytes	
Serial Communications	UART	0-3V transmission levels
Analog to Digital Converter	10 bit ADC	8 channel, 0-3V input
Other Interfaces	Digital I/O,I2C,SPI	
Current Draw	8 mA	Active mode
	8 µA	Sleep mode (total)
RF Transceiver		
Frequency band	2405 MHz to 2480 MHz	ISM band, programmable in 1 MHz steps
Transmit (TX) data rate	250 kbps	
RF power	3 dBm (typ)	
Receive Sensitivity	-101 dBm (typ)	
Adjacent channel rejection	36 dB	+ 5 MHz channel spacing
	34 dB	- 5 MHz channel spacing
Outdoor Range	> 300 m	1/4 wave dipole antenna, LOS
Indoor Range	> 50 m	1/4 wave dipole antenna, LOS
Current Draw	16 mA	Receive mode
	10 mA	TX, -17 dBm
	13 mA	TX, -3 dBm
	17 mA	TX, 3 dBm
Electromechanical		
Battery	2X AA batteries	Attached pack
External Power	2.7 V - 3.3 V	Molex connector provided
User Interface	3 LEDs	Red, green and yellow
Size (in)	2.25 x 1.25 x 0.25	Excluding battery pack
(mm)	58 x 32 x 7	Excluding battery pack
Weight (oz)	0.7	Excluding batteries
(grams)	18	Excluding batteries
Expansion Connector	51-pin	All major I/O signals



IRIS Mote (bottom view)



MIB520CA Mote Interface Board

Notes
 *5 MHz steps for compliance with IEEE 802.15.4/D18-2003.
 Specifications subject to change without notice

Base Station

A base station allows the aggregation of sensor network data onto a PC or other computer platform. Any IRIS Mote can function as a base station when it is connected to a standard PC interface or gateway board. The MIB510 or MIB520 provides a serial/USB interface for both programming and data communications. MEMSIC also offers a stand-alone gateway solution, the MIB600 for TCP/IP-based Ethernet networks.

Reference Board

Model	Description
XM2110CA	2.4 GHz IRIS OEM Reference Board

MEMSIC, Inc. 1235.131.131.131