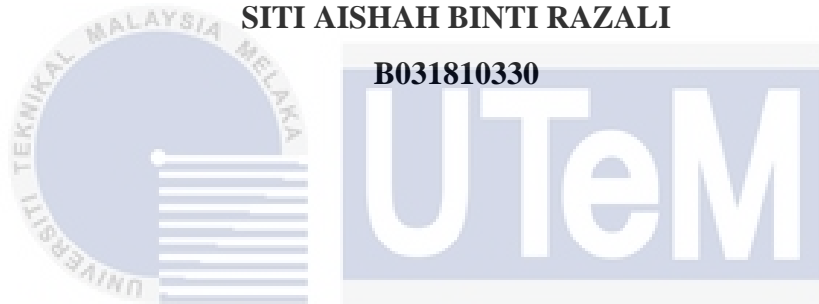


**COMPARISON OF HYBRID TECHNIQUE OF INTRUSION DETECTION  
SYSTEM IN 6LOWPAN**

**SITI AISHAH BINTI RAZALI**

**B031810330**



اونيورسيتي تيكنيكل مليسيا ملاك

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

**UNIVERSITY TEKNIKAL MALAYSIA MELAKA**

## BORANG PENGESAHAN STATUS LAPORAN

JUDUL: COMPARISON OF HYBRID TECHNIQUE OF INTRUSION DETECTION SYSTEM IN 6LOWPAN

SESI PENGAJIAN: 2020/2021

Saya: SITI AISHAH BINTI RAZALI

mengaku membenarkan tesis Projek Sarjana Muda ini disimpan di Perpustakaan Universiti Teknikal Malaysia Melaka dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. \* Sila tandakan (✓)

\_\_\_\_\_ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

\_\_\_\_\_ TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi / badan di mana penyelidikan dijalankan)

\_\_\_\_\_ TIDAK TERHAD

  
\_\_\_\_\_  
(TANDATANGAN PELAJAR)

Alamat tetap: 53 JALAN RK 3/3  
RASAH KEMAYAN, SEREMBAN,  
70300, NEGERI SEMBILAN

  
\_\_\_\_\_  
(TANDATANGAN PENYELIA)

EN. MOHAMMAD RADZI MOTSIDI

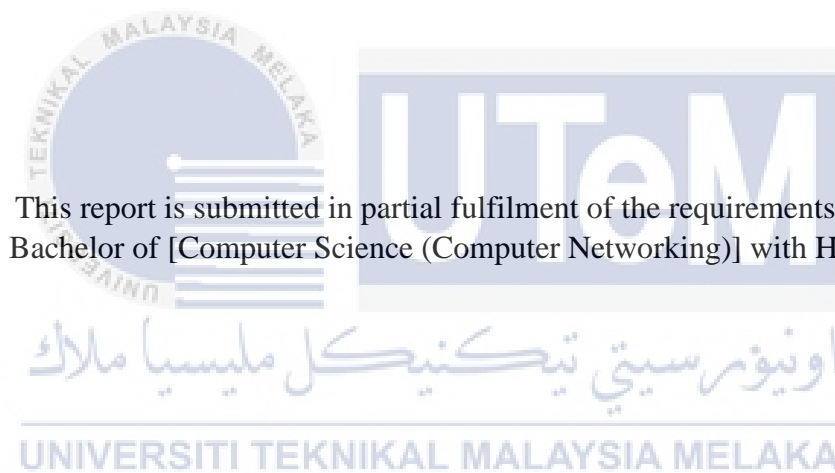
Tarikh: 10 September 2021

Tarikh: 10 September 2021

CATATAN: \* Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

COMPARISON OF HYBRID TECHNIQUE OF INTRUSION DETECTION  
SYSTEM IN 6LOWPAN

SITI AISHAH BINTI RAZALI



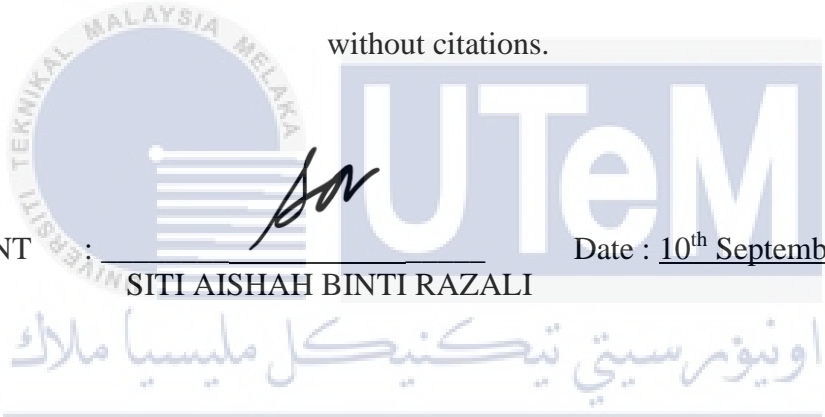
FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY  
UNIVERSITI TEKNIKAL MALAYSIA MELAKA  
2021

## DECLARATION

I hereby declare that this project report entitled  
**COMPARISON OF HYBRID TECHNIQUE OF INTRUSION DETECTION  
SYSTEM IN 6LOWPAN**

is written by me and is my own effort and that no part has been plagiarized  
without citations.

STUDENT :  Date : 10<sup>th</sup> September 2021  
SITI AISHAH BINTI RAZALI

  
I hereby declare that I have read this project report and found  
this project report is sufficient in term of the scope and quality for the award of  
Bachelor of [Computer Science (Computer Networking)] with Honours.

SUPERVISOR :  Date : 10<sup>th</sup> September 2021  
EN. MOHAMMAD RADZI MOTSIDI

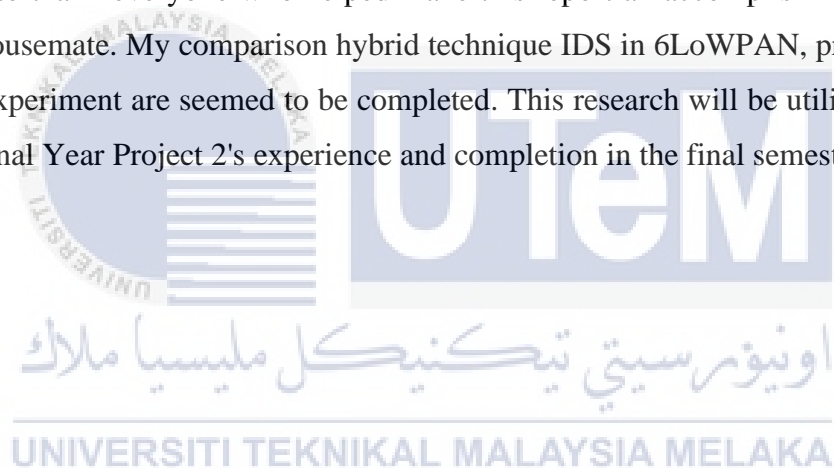
## DEDICATION

In honour of my supporting and wonderful friends, siblings and parents, who have always supported, led the way, and pushed me on my scholastic travels, I dedicate my final year project 1. Many thanks to my helpful instructor for his contribution to encourage me from the start to the end of my research.



## ACKNOWLEDGEMENTS

All glory be to Allah, I shall succeed in the end, and I have completed my final year assignment 1 (FYP 1). I would like to recognize my project's supervisor, En. Mohammad Radzi Motsidi, for his important position, dedication, and endless patience during the project's development and evaluation of me. Without his assistance, the project report could not be finished. I would also want to credit my wonderful family, which includes all of my siblings, for their aid and encouragement throughout my challenging struggle to accomplish my project. Additionally, I would want to thank everyone who helped make this report an accomplishment, especially my housemate. My comparison hybrid technique IDS in 6LoWPAN, project research and experiment are seemed to be completed. This research will be utilised as a guide for Final Year Project 2's experience and completion in the final semester.



## ABSTRACT

The term "Internet of Things" refers to the connectivity of physical items, such as smart objects, that exchange data and provide services through the internet. The network between IoT nodes can be protected by avoiding attacks with conventional mechanisms such as encryption and authentication, however these methods will not detect all potential attacks. The resource-constrained sensors node in an IoT environment are causing untrusted connection were made since the connection are made through internet using IPv6 and because communication protocol is IPv6 over Low -Power Wireless Personal Area Networks (6LowPAN). 6LowPAN is a communication protocol that were used for resource-constrained applications. Since the attack are more likely to happen, Intrusion Detection System are necessary to detect the attack that occur in the system or network by analysing the activity in the system or in the network and get the IDS log information about it and get the alarm report. In this project research will be focus on hybrid detection method using Network Intrusion Detection System (NIDS). The project experiment is a comparison between two extended version of existing computer simulation of hybrid detection method IDS, SVELTE. The Cooja network simulator will be used as the Routing Protocol for Low-Power and Lossy Networks (RPL) simulator in a 6LowPAN environment to create nodes of IoT and the attacker such as sink node using set of source code. The simulation produced network traffic and the data, metrics, and graph of RPL that can be collect and analyse.

## ABSTRAK

Istilah "Internet of Things" merujuk kepada penyambungan item fizikal, seperti objek pintar, yang saling bertukar data dan menyediakan perkhidmatan melalui internet. Jaringan antara nod IoT dapat dilindungi dengan menghindari serangan dengan mekanisme keselamatan seperti enkripsi dan pengesahan, namun kaedah ini sukar untuk mengesan semua serangan terhadap nod sensor yang terhad sumber dalam persekitaran IoT ini. Ini merisikokan rangkaian tersebut kerana IoT digunakan melalui internet dengan menggunakan IPv6 dan protokol komunikasi dalam IoT adalah IPv6 melalui Rangkaian Kawasan Peribadi Tanpa Wayar Rendah-Kuasa (6LowPAN). 6LowPAN adalah protokol komunikasi yang digunakan untuk peranti yang kekurangan sumber. Oleh kerana serangan lebih cenderung berlaku, Sistem Pengesanan Pencerobohan (IDS) diperlukan untuk mengesan serangan yang berlaku di sistem. Dalam projek ini penyelidikan akan difokuskan pada kaedah pengesanan hibrid menggunakan Sistem Pengesanan Pencerobohan Rangkaian (NIDS). Eksperimen projek ini adalah perbandingan antara dua versi simulasi komputer yang telah dinaik taraf daripada IDS sedia ada, iaitu IDS kaedah pengesanan hibrid, SVELTE. Simulator rangkaian Cooja akan digunakan sebagai simulator *Routing Protocol for Low-Power and Lossy Networks* (RPL) di persekitaran 6LowPAN untuk membuat nod IoT dan penyerang seperti *sink node* menggunakan set kod sumber. Simulasi dihasilkan melalui graf rangkaian dan data, metrik, dan graf RPL untuk dikumpulkan dan dianalisis untuk hasil perbandingan.



## TABLE OF CONTENTS

DECLARATION .....	II
DECLARATION .....	II
DEDICATION .....	III
ACKNOWLEDGEMENTS .....	IV
ABSTRACT.....	V
ABSTRAK .....	VI
TABLE OF CONTENTS .....	VII
LIST OF TABLES .....	X
LIST OF FIGURES.....	XI
LIST OF ABBREVIATION .....	XII
CHAPTER 1 : INTRODUCTION.....	1
1.1 Introduction.....	1
1.2 Problem Statement.....	1
1.3 Project Question.....	2
1.4 Project Objective.....	3
1.5 Project Scope.....	3
1.6 Project Contribution.....	4
1.7 Report Organisation .....	5
1.8 Conclusion .....	7
CHAPTER 2 : LITERATURE REVIEW.....	8
2.1 Introduction .....	8
2.2 Internet Of Things .....	8
2.3 Security In IoT .....	9
2.4 6LOWPAN Network.....	9
2.5 RPL .....	10

2.6	Intrusion Detection System .....	12
2.6.1	SVELTE .....	18
2.7	Critical Review .....	19
2.7.1	Introduction .....	19
2.7.2	Previous Existing Product .....	19
2.8	Conclusion .....	22
CHAPTER 3 : PROJECT METHODOLOGY .....		23
3.1	Introduction .....	23
3.2	Methodology .....	23
3.2.1	Planning Phase .....	23
3.2.2	Analysis Phase .....	24
3.2.3	Design Phase .....	24
3.2.4	Implementation Phase .....	27
3.2.5	Testing Phase .....	27
3.2.6	Integration And Analysis Phase .....	28
3.3	Project Milestone .....	29
3.4	Conclusion .....	31
CHAPTER 4 : DESIGN .....		32
4.1	Introduction .....	32
4.2	Problem Analysis .....	32
4.3	Requirement Analysis .....	33
4.3.1	Project Requirement .....	33
4.3.2	Dataset .....	35
4.4	Project Design .....	38
4.4.1	Simulation Design .....	38
4.4.2	Data Validation .....	41
4.5	Conclusion .....	42

CHAPTER 5 : IMPLEMENTATION .....	43
5.1 Introduction .....	43
5.2 Source Code Of IDS.....	43
5.3 Project Simulation Setup.....	44
5.3.1 Experiment 1: No Attacker And No IDS Setup .....	45
5.3.2 Experiment 2: Two Attacker And No IDS Setup.....	47
5.3.3 Experiment 3: Two Attackers With IDS Setup .....	49
5.4 Conclusion .....	51
CHAPTER 6 : TESTING AND ANALYSIS.....	53
6.1 Introduction.....	53
6.2 Testing And Analysing Method.....	53
6.2.1 Testing Experiment .....	53
6.3 Analysis Experiment.....	53
6.3.1 Power Consumption .....	54
6.3.2 Average Of ETX Value.....	55
6.4 Summary Of Analysis.....	57
6.5 Conclusion .....	59
CHAPTER 7 : PROJECT CONCLUSION .....	60
7.1 Introduction.....	60
7.2 Project Summarization .....	60
7.3 Project Contribution .....	61
7.4 Project Limitation.....	61
7.5 Future Work .....	62
7.6 Conclusion .....	62
REFERENCES.....	63
APPENDIX.....	66

## LIST OF TABLES

<b>Table 1.1 Problem Statement (PS)</b> .....	2
<b>Table 1.2 Project Question (PQ)</b> .....	2
<b>Table 1.3 Project Objective (PO)</b> .....	3
<b>Table 1.4 Project Scope</b> .....	4
<b>Table 1.5 Project Contribution (PC)</b> .....	4
<b>Table 2.1 Past research of related project</b> .....	19
<b>Table 2.2 Comparison of Hybrid technique IDS</b> .....	21
<b>Table 3.1 Simulation Parameter IDS by Matsuna et. al (2015)</b> .....	25
<b>Table 3.2 Simulation Parameter IDS by Shreenivas et. al (2017)</b> .....	26
<b>Table 3.3 Project Simulation Parameters on Contiki A</b> .....	26
<b>Table 3.4 Project Simulation Parameters on Contiki B</b> .....	27
<b>Table 4.1 Experiment parameters</b> .....	33
<b>Table 4.2 Creating simulation example</b> .....	38
<b>Table 5.1 Project Simulation File Path</b> .....	44
<b>Table 5.2 Experiment 1(a) parameters</b> .....	45
<b>Table 5.3 Experiment 1(b) parameters</b> .....	46
<b>Table 5.4 Experiment 2(a) parameters</b> .....	48
<b>Table 5.5 Experiment 2(b) parameters</b> .....	48
<b>Table 5.6 Experiment 3(a) parameters - Contiki A</b> .....	49
<b>Table 5.7 Experiment 3(a) parameters - Contiki B</b> .....	50
<b>Table 5.8 Experiment 3(b) parameters - Contiki A</b> .....	50
<b>Table 5.9 Experiment 3(b) parameters - Contiki B</b> .....	51

## LIST OF FIGURES

<b>Figure 2-1 Architecture of Network in 6LowPAN .....</b>	<b>10</b>
<b>Figure 2-2 An example of RPL DODAG with N nodes and IPv6 addresses</b>	<b>11</b>
<b>Figure 2-3 Intrusion Detection System Categorization .....</b>	<b>13</b>
<b>Figure 2-4 Host-IDS (Technology types).....</b>	<b>14</b>
<b>Figure 2-5 Network IDS (Technology Type) .....</b>	<b>15</b>
<b>Figure 2-6 Hybrid IDS(Technology types).....</b>	<b>15</b>
<b>Figure 2-7 Wireless-IDS (Technology Types).....</b>	<b>16</b>
<b>Figure 3-1 Project software requirement (VMware Workstation Pro 16) ...</b>	<b>24</b>
<b>Figure 3-2 Project Software requirement ( Contiki OS ) .....</b>	<b>25</b>
<b>Figure 3-3 Diagram of Experiment of IDS in Cooja flow.....</b>	<b>27</b>
<b>Figure 3-4 Example of average power consumption graph in Cooja.....</b>	<b>28</b>
<b>Figure 3-5 Milestone of project.....</b>	<b>29</b>
<b>Figure 4-1 Algorithm proposal 2 Shreenivas et. al. (2017).....</b>	<b>37</b>
<b>Figure 4-2 Algorithm proposal 2 Shreenivas et. al. (2017).....</b>	<b>38</b>
<b>Figure 4-3 attack_sinkhole_ids_demo.csc in Cooja .....</b>	<b>39</b>
<b>Figure 4-4 Mote Type Information.....</b>	<b>40</b>
<b>Figure 4-5 Motes in network windows in Cooja (Raza et. al.).....</b>	<b>41</b>
<b>Figure 4-6 Collect View of Sky mote .....</b>	<b>42</b>
<b>Figure 5-1 Code Snippet of IDS rules.....</b>	<b>43</b>
<b>Figure 5-2 Experiment 1(a) Network Structure .....</b>	<b>46</b>
<b>Figure 5-3 Experiment 1(b) Network Structure.....</b>	<b>47</b>
<b>Figure 5-4 Experiment 2(a) Network Structure .....</b>	<b>48</b>
<b>Figure 5-5 Experiment 2(b) Network Structure.....</b>	<b>49</b>
<b>Figure 5-6 Experiment 3(a) Network Structure .....</b>	<b>50</b>
<b>Figure 5-7 Experiment 3(b) Network Structure.....</b>	<b>51</b>
<b>Figure 6-1 Average Power Consumption of 10 nodes.....</b>	<b>54</b>
<b>Figure 6-2 Average Power Consumption of 20 nodes.....</b>	<b>55</b>
<b>Figure 6-3 Average ETX value of 10 nodes .....</b>	<b>56</b>
<b>Figure 6-4 Average ETX value of 20 nodes .....</b>	<b>57</b>
<b>Figure 6-5 Power Consumption in 10 nodes and 20 nodes.....</b>	<b>58</b>
<b>Figure 6-6 ETX value in 10 nodes and 20 nodes .....</b>	<b>59</b>

## LIST OF ABBREVIATION

<b>6LowPAN</b>	-	<b>IPv6 over Low -Power Wireless Personal Area Networks</b>
<b>RPL</b>	-	<b>Routing Protocol for Low-Power</b>
<b>IDS</b>	-	<b>Intrusion Detection System</b>
<b>DODAG</b>	-	<b>Destination-Oriented Directed Acyclic Graph</b>
<b>IoT</b>	-	<b>Internet Of Things</b>
<b>LLN</b>	-	<b>Low Power and Lossy Network</b>
<b>DIS</b>	-	<b>DODAG Information Solicitation</b>
<b>WSN</b>	-	<b>Wireless Sensor Network</b>
<b>6BR</b>	-	<b>IPV6 Border Router</b>
<b>OS</b>	-	<b>Operating System</b>
<b>DIO</b>	-	<b>DODAG Information Object</b>
<b>OF</b>	-	<b>Objective Function</b>
<b>ETX</b>	-	<b>Expected Transmission Count</b>

## CHAPTER 1 : INTRODUCTION

### 1.1 Introduction

Chapter 1 will focus on the planning of the project where the problem statement (PS), project question (PQ), project objective (PO), project scope and project contribution (PC) will be discussed. The project is about research of the analysis of hybrid technique approach in the intrusion detection system. The Cooja network simulator will be used as the RPL simulator in a 6LowPAN environment to create nodes of Internet Of Things (IoT) and the attacker such as sink node using set of source code. RPL stands for IPv6 Routing Protocol for Low-Power and Lossy Networks. Source code of Intrusion Detection System (IDS) implementation will be used inside the simulation. The simulation produced network traffic and the data, metrics, and graph of RPL that can be collect and analyse (tuz-Zahra et al., 2020).

There would be the comparison of hybrids IDS technique in order to compare the IDS evaluation. The result of false positive, false negative, number of nodes, time before an attack are collected in order to count the average percentage of the detection rate IDS (Nygaard, 2017). The attack from dataset csc file extension that would be evaluate is sinkhole attack and selective forwarding attack. Sinkhole attack enables intruders to interrupt and alter network traffic which that if occurred together with selective forwarding attack will effect larger part of the network to be controlled by the intruders (Raza et al., 2013). Hence, it is important to detect these two attacks.

### 1.2 Problem Statement

Network Intrusion Detection System has been introduced for few years back on, and so are the hybrid technique as one of the techniques commonly used in Intrusion Detection System. This project would be identified to differentiate between the existing computer simulation hybrid technique IDS to identify which hybrid

technique IDS suitable according to environment. As most IDS technique require different routing schemes that are not based on standardized mechanisms (Raza et al., 2013).

*Table 1.1 Problem Statement (PS)*

<b>PS</b>	<b>Problem Statement</b>
PS <sub>1</sub>	To identify the most stable network between existing computer simulation hybrid technique Intrusion Detection System in IoT environment.

### 1.3 Project Question

Problem statement element to be measure are power consumption, and the Expected Transmission Count (ETX) value of the network. These components were used to determine the quality of the IDS implemented causing to the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) environment. Since the IDS are implemented around network layers it is important to know how the performance being monitored. In Internet of Things (IoT), the Low Power and Lossy Network (LLN) is a sector that includes constrained devices such as sensors and RFIDs. The routing protocol for Low Power and Lossy Networks (LLN) is called Routing Protocol for Low-Power (RPL) that is an open routing protocol that enables nodes to interact in a mesh topology of 6LowPAN (Bhattacharyya and Pushpalatha, 2018).

RPL routing protocol in 6LowPAN are vulnerable to attacks. The link in the RPL can brings various of attacks through Destination-Oriented Directed Acyclic Graph (DODAG) Information Solicitation (DIS) when transmitting nodes to join a network (Wallgren et al., 2013). This issue arises a question on how can Network IDS in hybrid detection method help to overcome the attacks? Apart from that, there are many hybrid techniques in computer simulation to implement IDS, how would these hybrid techniques be any different from each other? This question arises and would be discover within this project.

*Table 1.2 Project Question (PQ)*

<b>PS</b>	<b>PQ</b>	<b>Project Question</b>
PS <sub>1</sub>	PQ <sub>1</sub>	How the simulation performance of IDS in IoT environment monitored?
	PQ <sub>2</sub>	How a hybrid detection method IDS in IoT environment help to overcome the RPL attacks?
	PQ <sub>3</sub>	What is the difference between the existing



	hybrid detection method IDS(s) in computer simulation of IoT environment?
--	---

#### 1.4 Project Objective

The objective of the project are to investigate the implementation of hybrid detection method Intrusion Detection System in simulation IoT, 6LoWPAN network environment. Next, objective to compare the effectiveness between the hybrid detection method of IDS(s) in simulated IoT environment based on the experiment analysis and lastly to make recommendations of best simulation environment settings based on the experiment analysis of hybrid detection method IDS in simulated IoT, 6LoWPAN network environment.

*Table 1.3 Project Objective (PO)*

PS	PO	Project Objective
PS <sub>1</sub>	PO <sub>1</sub>	To investigate the implementation of hybrid detection method Intrusion Detection System in simulated IoT, 6LoWPAN network environment.
	PO <sub>2</sub>	To compare the effectiveness between the hybrid detection method of IDS(s) in simulated IoT environment based on the experiment analysis.
	PO <sub>3</sub>	To make recommendations of best simulation environment settings based on the experiment analysis of hybrid detection method IDS in simulated IoT, 6LoWPAN network environment

#### 1.5 Project Scope

There were several detection methods of Intrusion Detection System (IDS), one of it was hybrid detection method. Hybrid detection method IDS are the mixture of both signature and anomaly detection method which are more efficient to detect more types of attacks than signature and anomaly detection method. The project scope is focusing on comparison hybrid detection method of IDS.

The experiment of the comparison will be implemented on simulation software which is Cooja network simulator that will be use inside a Contiki Operating System (OS) since Cooja has been demonstrated to be an excellent tool for simulating IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) in Wireless Sensor Network (WSNs).

The comparison are involving the extension version of existing computer simulation, SVELTE by Raza et al. (2013), that is IDS by Matsunaga et al. (2015) and IDS by Shreenivas et al. (2017). The source code that will be use in this project would be the existing computer simulation SVELTE by Raza et al. (2013), where the dataset of IPV6 Border Router (6BR) inside the IPv6 over Low -Power Wireless Personal Area Networks (6LowPAN) are to specified the rank metrics of the IoT nodes in, next the IDS client and also the malicious node. The source code will be manipulated according to algorithm of Matsunaga et al. (2015) and Shreenivas et al. (2017) proposed. The evaluation of the experiment will be the dataset of experiment, power consumption and ETX average value.

*Table 1.4 Project Scope*

<b>Project Scope</b>	<b>Details</b>
Experiment of	IDS Computer Simulation
Intrusion Detection System Type	Hybrid IDS
Platform	Virtual Machine (VMWare Workstation)
Operating System	Contiki
Source Code	IDS by SVELTE, Matsunaga et.al (2015) and Shreenivas et. al (2017)
Network Simulator	Cooja
Dataset	Data from Cooja 'Collect-view' features
Evaluation component	1. Power Consumption 2. ETX average value

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

## 1.6 Project Contribution

The project analyzes the comparison between the hybrid detection method Intrusion Detection System by power consumption and ETX value. These comparison benefits to user who uses IOT environment network as part of their life as the implementation of IDS in hybrid technique works differently in each environment. Hybrid technique also was chosen for this project also as it the better method than signature and anomaly detection method because hybrid detection method overcome the weaknesses of signature and anomaly technique (Napiah et al., 2018).

*Table 1.5 Project Contribution (PC)*

<b>PS</b>	<b>PQ</b>	<b>PO</b>	<b>PC</b>	<b>Project Contribution</b>
PS <sub>1</sub>	PQ <sub>1</sub>	PO <sub>1</sub>	PC <sub>1</sub>	Proposed a technical process of how the

			hybrid detection method IDS working in simulation environment.	
		PO <sub>2</sub>	PC <sub>2</sub>	Proposed a comparison result of detection rate and accuracy rate of existing hybrid detection method IDS in computer simulation IoT environment.
		PO <sub>3</sub>	PC <sub>3</sub>	Proposed analysis report based on best simulation environment settings based on the experiment analysis of hybrid detection method IDS in simulated IoT, 6LoWPAN network environment.

## 1.7 Report Organisation

### Chapter 1: Introduction

This chapter discuss about the analysis planning towards hybrid technique of network Intrusion Detection System. The planning is as important as to figure the main component to be analyzed and the component to be evaluate in implementation phase. Problem statement is to identify the most stable network between existing computer simulation hybrid technique Intrusion Detection System in IoT environment.

There are three project questions developed from the problem statement, which is PQ<sub>1</sub>, How the simulation performance of IDS in IoT environment monitored? next PQ<sub>2</sub>, how a hybrid detection method IDS in IoT environment help to overcome the RPL attacks? and PQ<sub>3</sub>, what is the difference between the existing hybrid detection method IDS(s) in computer simulation of IoT environment? Project scope for this project as per discussed, the IDS detection method, the simulation software, the dataset and the component to be evaluated.

Lastly project contribution is to propose a technical process of how the hybrid detection method IDS working in simulation environment., proposed a comparison result of detection rate and accuracy rate of existing hybrid detection method IDS in computer simulation IoT environment and proposed analysis report based on best simulation environment settings based on the experiment analysis of hybrid detection method IDS in simulated IoT, 6LoWPAN network environment.

## **Chapter 2: Literature Review**

The project's literature analysis will be the subject of Chapter 2. These would aid in the development of a theoretical framework and technique for the topic study field, as well as a picture of material similarities in each subject. This chapter will describe chosen content relevant to Intrusion Detection System (IDS) for 6LoWPAN network hybrid technology. In this chapter, the proposed strategy for each item will be justified. Hybrid technique is one of the most often used techniques in Intrusion Detection Systems (IDS). This paper will analyse and evaluate major components of hybrid technique requirements using selected academic sources.

## **Chapter 3: Project Methodology**

The project's methodology will be identified and detailed in Chapter 3. This project's technique would be to implement the project using a model System Development Life Cycle (SDLC). The phases are planning phase, analysis phase, design phase, implementation phase, testing phase, integration and analysis phase. Each phase's aspects will be identified and developed. This chapter will also cover the project's major milestones. The project strategies may be used to specify how procedures, components, and processes are organised, as well as architecture, division, and perspective.

## **Chapter 4: Design**

In this chapter, the planning of project will be inspected to make sure the project can be done realistically. This chapter will emphasize the project prerequisite in terms of software requirement, programming specifications and the project limitation. The simulation design and data validation will be elaborated in detail in this chapter to emphasize the component involved in this project experiment.

## **Chapter 5: Implementation**

The previous chapter discussed over project design, and this chapter will go over project implementation. This chapter will enlighten on how the simulation environment will be configured based on the source of main Intrusion Detection System (SVELTE) according to IDS by Matsunaga et. al. (2015) and Shreenivas et. al. (2017).

## **Chapter 6: Testing and Analysis**

The project's testing procedure is described in the sixth chapter. Furthermore, testing is essential to confirm that the finished product and system fulfil the requirements and function properly. In addition, this step will strengthen the project's involvement in achieving the project's goal. The testing will be involving the experiments that will be done in this project. There would be eight experiments in total. All components and modules will be verified to guarantee that the experiment is done according to the project requirement and precisely.

## **Chapter 7: Project Conclusion**

This chapter will summarize the project's conclusion and progress. It will discuss the overall project progress and achievement of this project's contribution, as well as the project's capabilities, weaknesses, and future improvements. Furthermore, every project specific will be clarified and comprehensible by giving the project overview. This chapter will also go through the changes that will be made and how they will be implemented for the next phase of the experiment.

### **1.8 Conclusion**

This chapter discuss about the analysis planning towards hybrid technique of network Intrusion Detection System. The planning is as important as to figure the main component to be analyzed and the component to be evaluate in implementation phase. In this chapter, problem statement (PS), project question (PQ), project objective (PO), project scope and project contribution (PC) were discussed. Next chapter would literature review of the project.

## **CHAPTER 2 : LITERATURE REVIEW**

### **2.1 Introduction**

Chapter 2 will focus on the literature analysis of the project. Literature review is a survey of scholarly sources on a particular field of research. It refers to the collection of published materials on certain field of research to be analyzed, synthesized, and evaluated. These would help to see the picture of similarity of the materials on the specific field and helps to develop theoretical framework and methodology of the topic research field.

This chapter would summarize the selected material related to Intrusion Detection System (IDS) for hybrid technique in 6LoWPAN network. The suggested approach of each material would be justified in this chapter. Hybrid technique has been one of the most practiced technique in Intrusion Detection System (IDS), this may help to analyses and evaluate key components of requirement in hybrid technique based on the selected scholar sources.

### **2.2 Internet Of Things**

Internet of Things refers to the connection between physical devices such as smart objects that exchanging data and offer services using internet (Ahmed et al., 2017). The connection between the IoT nodes may be secured by preventing attacks using standard mechanism like cryptography and authentication process but these way will not detect all possible attacks (Bostani and Sheikhan, 2017). However, because IPv4 has a limited address space, items in the Internet of Things (IoT) employ IPv6 to expand their address space.

The Internet of Things (IoT) is a hybrid network of small devices, usually WSNs, and the traditional Internet. A wireless sensor network (WSN) is a collection of

sensor nodes that detect, record, and transmit environmental data to a sink node. The sink node then processes the data it has received and corresponds with the router nodes. The sensor nodes are limited-resource devices with limited computation power, that is all basically overall of the concept of IOT.

### 2.3 Security In IoT

Because of the rapid expansion of the Internet of Things, its security has become one of the most complex concerns in such a connected and mutual framework (Hajiheidari et al., 2019). Now, the number of smart things connected to the Internet is growing as a rising number of developing WSNs employ IP. Over trillion smart objects will be controlled and connected via the Internet and a variety of applications. As the number of devices connected to the Internet grows, security becomes a more pressing concern.

The resources-constrained like sensors node in IoT environment are causing untrusted connection were made since the connection are made through internet using IPv6 and also because communication protocol is 6LowPAN (Raza et al., 2013) (Bostani and Sheikhan, 2017). Since the attack are more likely to happen, Intrusion Detection System are necessary in order to detect the attack that occur in the system or network by analysing the activity in the system or in the network and get the IDS log information about it and get the alarm report (Raza et al., 2013).

Despite the fact that IoT networks can only be accessed by authorised users, they are vulnerable to a variety of assaults. These attacks try to interrupt network connection or capture personal information. Denial-of-service (DoS) attacks, for example, degrade communication at the network layer very quickly (Oh et al., 2014).

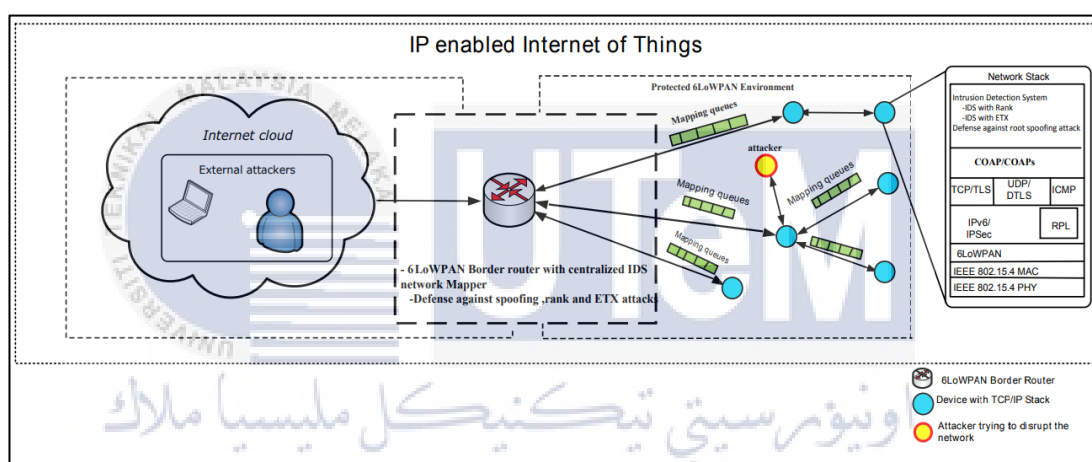
Sinkhole attack are one of the RPL attacks that often occurs. Sinkhole attack is when a malicious node propagates its rank with a high value, which is usually anything like the sink's rank. Consequently, its neighbours will choose it as their preferable parent and traffic will be directed to it. To drop all the traffic attracted, the sinkhole attack is frequently paired with the selective forwarding attack.

### 2.4 6LowPAN Network

6LowPAN is a communication protocol that were used for resource-constrained applications (Raza et al., 2013). A 6LoWPAN network is a multi-hop wireless

network with lossy communication links and resource-constrained devices that are frequently powered by batteries. As a result, in 6LoWPAN networks, the connectionless

User Datagram Protocol (UDP) is a basic OSI transport layer protocol based on Internet Protocol for client/server network applications (IP). UDP is commonly utilised in application to run in real-time. For example, for this project will utilised UDP due to the real-time data collecting. 6LoWPAN is an IPv6 stub network network design for low-power wireless area networks. It compresses or decompresses IPv6 datagrams and fragments or assembles them. It may be used on any device and is not limited to constrained devices alone (Napiah et al., 2018).



UNIVERSITI TEKNIKAL MELISIA ملاك  
Figure 2-1 Architecture of Network in 6LoWPAN

In Figure 2-1 shows that the 6LoWPAN Border Router (6BR) is used to link all the device nodes to the Internet, which are also the Destination-Oriented Directed Acyclic Graph (DODAG) that was constructed by RPL. RPL stands for IPv6 Routing Protocol for Low-Power and Lossy Networks, and it is a standardized routing protocol for IP-connected IoT.

## 2.5 RPL

RPL is a flexible protocol that allows communication between many-to-one, many-to-many, and one-to-one. It constructs a Destination-Oriented Directed Acyclic Graph (DODAG) and supports two modes of operation: unidirectional traffic