

Republic of Iraq
Ministry of Higher Education and Scientific Research
University of Anbar
College of Computer Science and Information Technology
Department of Computer Science



ICMetric Technology for Embedded Devices Security

A Thesis

*Submitted to the Department of Computer Science - College
of Computer Science and Information Technology,
University of Anbar as Partial Fulfilment of the Requirement
for Master Degree of Science in Computer Science.*

By

Duaa Abd Alsatar Rokan

Supervised by

Assist. Prof. Dr. Salah Sleibi AlRawi

Assist. Prof. Dr. Khattab M. Ali Alheeti

1441 A.H

2019 B.C

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

يَرْفَعُ اللَّهُ الَّذِينَ ءَامَنُوا مِنْكُمْ وَالَّذِينَ

أُوتُوا الْعِلْمَ دَرَجَاتٍ وَاللَّهُ بِمَا تَعْمَلُونَ

خَيْرًا

صدق الله العظيم

سورة المجادلة الآية: (١١)

Dedication

This thesis is dedicated to:

My parents

My brothers

My sisters

and my friends.

Duaa Aldosary

2019

Acknowledgments

First of all, thanks to Allah for guidance that enabled me to complete my study.

I would like to have the opportunity to say thank you for all those who has a hand in the completion of this academic work. I would like to express my appreciation and gratitude to my supervisors Dr. Salah Sleibi AlRawi and Dr. Khattab M. Ali Alheeti for their guidance, encouragement, advice and support during this work.

Special thanks are due to Dr. Salah Awad for his advice.

Special thanks are due to the Dean of the College of Computer Science and Information Technology and the staff.

Finally, I express my deep gratitude for the great support I had from my brothers Dr. Abd Aljabbar Abd Alsatar and Dr. Omar Abd Alsatar. Without their continuous support, this thesis would not have seen the light.

Duaa Aldosary

2019

Supervisor Certification

*We certify that this thesis entitled “**ICMetric Technology for Embedded Devices Security**” was prepared under our supervision at the department of computer science – College of Computer – Anbar University, by “**Duaa Abd Alsatar Rokan**” as a partial fulfillment of the requirements of the degree of Master of Science in Computer Science.*

Signature:

Name:

Title:

Date:

Signature:

Name:

Title:

Date:

Certification of the Examination Committee

We the examination committee certify that we have read this thesis entitled " *ICMetric Technology for Embedded Devices Security* " and have examined the student "Duaa Abd Alsatar Rokan", in its contents and what is related to it, and that in our option it is adequate to fulfill the requirements for the degree of Master of Computer Science.

Signature:

Name: Prof. Dr. Sufyan Tayih Farj (Chairman)

Date: / / 2019

Signature:

Name: Prof. Dr. Saad Najem Alsaad (Member)

Date: / / 2019

Signature:

Name: Assist. Prof. Dr. Abd Alkareem A. Najem (Member)

Date: / / 2019

Signature:

Name: Assist. Prof. Dr. Salah Sleibi AlRawi (Supervisor)

Date: / / 2019

Signature:

Name: Assist. Prof. Dr. Khattab M. Ali Alheeti (Supervisor)

Date: / / 2019

*Approved by the Dean of the College of Computer Science and Information
Technology, University of Anbar.*

Signature:

Name: Assist. Prof. Dr. Ahmed Noori Rashid (Dean of the College)

Title: Dean of the College

Date: / / 2019

Abstract

The interesting in embedded systems is related to the matters of providing privacy, safety, and security. The security of any data kept on the system can be exposed by any unauthorised access. It was found that no security system is perfect for all applications; this keeps the research area open for suggesting a new security system or improving an old one, therefore, a security system is suggested in this thesis.

The proposed system is presented to apply identification and improve the security of embedded devices. However, the proposed system is based on a new technology called an Integrated Circuit Metric (ICMetric), which relies on the special internal features of each device. By using the ICMetric, low level device features are used to create an identification for device.

The proposed work is based on using the bias in accelerometer, gyroscope, and magnetometer to create a unique ICMetric number for every device. This number is utilised in dataset extracted from trace file that has been generated by Network Simulator Version two (ns-2) to perform identification and detection. The proposed system is composed through three main phases. The first phase is bias readings extracted from sensors. Whereas, in the second phase, ICMetric number is generated by using the bias readings that extracted from sensors in the first phase. In the third phase, the security system is tested and evaluated to measure its effectivity. In other words, it is tested with dataset that extracted from the trace file of network simulator. In this phase performance metrics are calculated, which are error rate, confused matrix and accuracy rate.

An identification system is proposed in this thesis for providing identification of intelligent wheelchairs in two schemes. The first proposed scheme is based on the bias readings that generated by gyroscope and magnetometer sensors. Whereas, the second proposed scheme is depended on three ICMetric numbers provided by bias readings generated from three types of sensors.

The proposed schemes have been simulated by using the dataset extracted from trace files. The simulation results have been compared and studied for high levels of detection capability and performance metrics.

List of Abbreviations and Symbols

<i>Abbreviations</i>	<i>Details</i>
AODV	Ad hoc On-Demand Distance Vector
AI	Artificial Intelligent
ANN	Artificial Neural Network
AHRS	Attitude Heading Reference System
CL-PKC	Certificate Less- Public Key Cryptography
CPS	Cyber-Physical System
CPI	Cycles Per Instruction
DSR	Dynamic Source Routing
EC	Evolutionary Computing
FFNN	Feed Forward Neural Network
FL	Fuzzy Logic
GPS	Global Positioning System
GA	Genetic Algorithm
HAI	Hybrid Artificial Intelligent
IC	Integrated Circuit
ICMetric	Integrated Circuit Metric
IoT	Internet of Thing
IP	Internet Protocol
IDS	Intrusion Detection System
K-nn	K- Nearest Neighbor
MAC	Media Access Control
MEMS	Micro Electro Mechanical System
NN	Neural Network
NAM	Network Animator
ns-2	Network Simulator 2
PC	Program Counter
RSA	Rivest–Shamir–Adleman
SoC	System on Chip
SHA1	Secure Hash Algorithm 1

SHA2	Secure Hash Algorithm 2
SVM	Support Vector Machine
TORA	Temporally Ordered Routing Algorithm
TCL	Tool Command Language
TCP	Transmission Control Protocol
UART	Universal Asynchronous Receiver Transmitter
USB	Universal Serial Bus
UDP	User Datagram Protocol
VANETs	Vehicular Ad-Hoc Networks
WSNs	Wireless Sensor Networks
IQR	Inter Quartile Range
FP	False Positive
TN	True Negative
FN	False Negative

Notation

<i>Notation</i>	<i>Explanation</i>
N_s	Number of the Sending Packet
N_r	Number of the Receiving Packet
S	Packet Size
ST	Simulation Time
N	Number of Connections
x	Particular Sample Reading
\bar{X}	Mean
σ^2	Standard Deviation
s	Skewness Distribution
CI	Confidence Interval
$Q3$	Upper Quartile
$Q1$	Lower Quartile

Contents

<i>Chapter One – Introduction</i>	
1.1 Introduction	1
1.2 Related Works	3
1.3 Problem Statement	7
1.4 Thesis Objectives	8
1.5 The Main Contributions	9
1.6 Thesis Structure	9
<i>Chapter Two- Theoretical Background</i>	
2.1 Introduction	10
2.2 Security Concept	10
2.3 Security Attacks and Vulnerabilities	11
2.3.1 Security Attacks	12
2.3.2 Targets of Attacks	13
2.3.3 Security Vulnerabilities	13
2.4 Integrated Circuit Metric Technology	14
2.4.1 Calibration Phase	15
2.4.2 Operational Phase	15
2.5 Intelligent Wheelchair Application	16
2.6 MyAHRS_plus Sensor	17
2.7 MEMS Sensor	18
2.7.1 MEMS Accelerometer	19
2.7.2 MEMS Gyroscope	20
2.7.3 MEMS Magnetometer	20
2.8 Hardware Imperfection	22
2.9 Intelligent Wheelchair Sensors	23
2.9.1 MEMS Accelerometer in Intelligent Wheelchair	23
2.9.2 MEMS Gyroscope in Intelligent Wheelchair	24
2.9.3 MEMS Magnetometer in Intelligent Wheelchair	24
2.10 Sensors Bias Measurement	24

2.10.1 Gyroscope Bias Measurement	25
2.10.2 Magnetometer Bias Measurement	25
2.10.3 Accelerometer Bias Measurement	25
2.11 Artificial Intelligence	26
2.12 Support Vector Machine	26
2.13 Network Simulator	27
2.14 Routing Protocol	28
2.15 Source Collection of the Dataset	29
<i>Chapter Three - Design and Implementation</i>	
3.1 Introduction	31
3.2 The Proposed ICMetric-Security System	32
3.2.1 The General Architecture of Proposed System	32
3.2.2 Methodology	33
3.2.2.1 Simulation Environment and Initial Parameters	35
3.2.2.2 Generating Mobility and Traffic Model	36
3.2.2.3 Acquire of Dataset	36
3.2.2.4 Pre-processing Phase of the Extracting Features	38
3.2.2.5 Extraction of Features from Trace File	39
3.2.2.6 Integration of ICMetric Number into Dataset	39
3.2.2.7 Training and Testing Phases	41
3.3 ICMetric Technology for Intelligent Wheelchairs	41
3.4 Performance Metrics	42
<i>Chapter Four – Results and Discussion</i>	
4.1 Introduction	44
4.2 Experimental Results of MEMS Bias Establishment	44
4.2.1 Gyroscope Bias Analysis	45
4.2.2 Magnetometer Bias Analysis	49
4.2.3 Accelerometer Bias Analysis	53
4.3 Statistical Analysis Results for ICMetrics	56
4.4 Experimental Evaluation and Results	61
4.4.1 The First Scheme Based on Bias Readings of Gyroscope and Magnetometer Sensors	62

4.4.2 The Second Scheme Based on Bias Readings of Gyroscope, Magnetometer and Accelerometer Sensors	63
4.5 Compressions of Experimental Results	64
4.5.1 Comparison between the First Scheme and System without ICMetric	64
4.5.2 Comparison between the Second Scheme and System without ICMetric	66
4.5.3 Comparison between the Proposed System and the Previous Studies	67
4.5.4 Comparison between the Two Proposed Schemes	69
4.6 Additional Performance Matrices	69
4.7 Chapter Summary	71
<i>Chapter Five - Conclusion, Future Works and Limitations</i>	
5.1 Conclusion	72
5.2 Future Works	72
<i>References</i>	

List of Figures

<i>Figure No.</i>	<i>Title</i>	<i>Page No.</i>
1.1	Embedded System Applications	1
2.1	Flow Diagrams of ICMetric Phases	16
2.2	Intelligent Wheelchair	17
2.3	MyAHRS_plus Sensor	17
2.4	Schematic Illustration of MEMS Components	19
2.5	The Principle of Working MEMS Accelerometer (a) No Acceleration Output in the Same Capacitance on the Static Plates (b) Change Caused by Acceleration in Capacitance between the Static Plate	19
2.6	The Principle of Working MEMS Gyroscope (a) Movement of the Drive Arm with Rotation (b) Movement of the Drive Arm with A Side Movement	20
2.7	Magnetometer Sensor	21
2.8	The Difference between Conventional Sensors and Magnetometer Sensors in the State of Physical Properties Measurement	22
	(a) Conventional Sensor	21
	(b) Magnetometer Sensor	22
2.9	Protocols Types	28
2.10	AODV Protocol Trace Information	30
3.1	Overall ICMetric-Security System Architectural	32
3.2	The Flowchart of the Proposed Algorithm	34
3.3	Screenshot of Simulation in the ns-2 NAM	36
3.4	Code of Symbols and Letters Transformation in MATLAB	38
3.5	Import Data of Trace File into MATLAB	39
4.1	Population Mean and Sample Mean Relationship	46

4.2	Readings of the First Gyroscope Sensor, (a) x-axis graph (b) y-axis graph (c) z-axis graph	47
4.3	Readings of the Second Gyroscope Sensor, (a) x-axis graph (b) y-axis graph (c) z-axis graph	48
4.4	Readings of the Third Gyroscope Sensor, (a) x-axis graph (b) y-axis graph (c) z-axis graph	49
4.5	Readings of the First Magnetometer Sensor, (a) x-axis graph (b) y-axis graph (c) z-axis graph	50
4.6	Readings of the Second Magnetometer Sensor, (a) x-axis graph (b) y-axis graph (c) z-axis graph	51
4.7	Readings of the Third Magnetometer Sensor, (a) x-axis graph (b) y-axis graph (c) z-axis graph	52
4.8	Readings of the First Accelerometer Sensor, (a) x-axis graph (b) y-axis graph (c) z-axis graph	54
4.9	Readings of the Second Accelerometer Sensor, (a) x-axis graph (b) y-axis graph (c) z-axis graph	55
4.10	Readings of the Third Accelerometer Sensor, (a) x-axis graph (b) y-axis graph (c) z-axis graph	56
4.11	Number of Sent, Received and Dropped Packets	70

List of Tables

<i>Table No.</i>	<i>Title</i>	<i>Page No.</i>
3.1	Initial Parameters of ns-2	35
3.2	Significant Features of AODV from Trace File	37
4.1	Statistical Analysis of the First Triple Axial Gyroscope Sensor	57
4.2	Statistical Analysis of the Second Triple Axial Gyroscope Sensor	57
4.3	Statistical Analysis of the Third Triple Axial Gyroscope Sensor	58
4.4	Statistical Analysis of the First Triple Axial Magnetometer Sensor	58
4.5	Statistical Analysis of the Second Triple Axial Magnetometer Sensor	59
4.6	Statistical Analysis of the Third Triple Axial Magnetometer Sensor	59
4.7	Statistical Analysis of the First Triple Accelerometer Sensor Axes	60
4.8	Statistical Analysis of the Second Triple Accelerometer Sensor Axes	60
4.9	Statistical Analysis of the Third Triple Accelerometer Sensor Axes	61
4.10	Types of Alarms for the First Method in the Proposed System	62
4.11	Accuracy and Error Rate of the First Method in the Proposed System	63
4.12	Detection Rate of the First Method in the Proposed System	63
4.13	Types of Alarms for the Second Method in the Proposed System	63
4.14	Accuracy and Error Rate of the Second Method in the Proposed System	64

4.15	Detection Rate of the Second Method in the Proposed System	64
4.16	Compression of Accuracy and Error Rate between the First Method in Proposed System and System without ICMetric	65
4.17	Compression of Alarms Rate between the First Method in Proposed System and System without ICMetric	65
4.18	Compression of Detection Rate between the First Method in Proposed System and System without ICMetric	65
4.19	Compression of Accuracy and Error Rate between the Second Method in Proposed System and System without ICMetric	66
4.20	Compression of Alarms Rate between the Second Method in Proposed System and System without ICMetric	66
4.21	Compression of Detection Rate between the Second Method in Proposed System and System without ICMetric	67
4.22	Compression of Detection Rate and Error Rate between the First Method in Proposed System and Previous Study	67
4.23	Compression of Detection Rate and Error Rate between the Second Method in Proposed System and Previous Study	67
4.24	Compression of Alarms Rate between the First Method in Proposed System and Previous Study	68
4.25	Compression of Alarms Rate between the Second Method in Proposed System and Previous Study	68
4.26	Compression of Alarms Rate, Accuracy Rate and Error Rate between Two Methods Presented in Proposed System	69
4.27	Additional Performance Metrics	70
4.28	Number of Generated, Received and Dropped Packets	70

CHAPTER ONE

Introduction

CHAPTER ONE

Introduction

1.1 Introduction

An embedded system is a special-purpose computer system, which is fully encapsulated in the device it controls. These systems have special requirements and complete pre-defined tasks [1]. Currently, embedded system spread in many devices and the users of these devices are capable of performing the network/internet applications that run on these devices. These devices are also involved in transport of secure data over public networks that require defense from unauthorised access [2]. As a result, security in embedded systems has spread every passing day in many fields like aerospace, telecom, healthcare and wearable devices [3]. Figure 1.1 illustrates embedded systems applications, such as railways, mobile phones, consumer electronics, tables, laptops, and healthcare application.



Figure 1.1: Embedded System Applications

Embedded devices spread in a wide range of applications and these devices handle critical information. For this reason, it is desirable to have some security mechanism deployed on embedded devices either in the form of software or hardware. However, embedded devices security is a challenging function and treated as open research case due to the resource-constrained nature of these devices.

The security of embedded systems can become an issue even bigger than the insufficiency of security of current desktop computers. The reasons for this lack of security is hardware devices constraints when performing measures of security and security cost. Manufacturers attempt to reduce costs of production to gain a market advantage for price critical products [4].

In the area of computing and networking, security has traditionally been a subject of robust research. Currently, the increasing number of embedded systems, such as home automation products, mobile phones, household appliances and industrial monitoring is submitted to a growing number of threats as the hacker groups is starting to pay interest to these systems. On the other hand, the implementation of security is not easy because of the constraints on resources of this type of devices [1].

Growing embedded systems number with complexity are present in all our lives aspects. Embedded system devices are often networked via wireless communication links to accomplish advantageous tasks. However, the wireless nature between the embedded devices makes them vulnerable to attacks and adversaries. Therefore, security of embedded systems is a main aspect of embedded systems design and is currently a major field of scientific research.

ICMetrics is a technology that has been advanced in connection with the security requirement in applications of embedded system. The ICMetrics exploit characteristics of system to present identification. It indicates a new technology that can be employed to extract the hardware and software attributes. Each device is unique in its inside environment. Therefore, the features that make each device diverse can be utilised to create a unique number of device. ICMetric number is not stored on the system and can be regenerated when needed. If the system is attacked, there will be no theft because the ICMetric is non-stored [5].

The ICMetrics technology is fundamentally based on measurement of internal behaviour that are acquired from embedded system characteristics under various circumstances. By the features analysing and employing, a unique identifier can be provided and exploited to determine or describe the embedded system. ICMetrics is a technology that can generate unique identifiers from the special characteristics of the software and hardware related with a specific electronic device. Electronic devices sense different environmental condition by internal and external sensors, trigger the

execution of various software, accomplish different tasks and even interact differently with various users. Different features can be provided by digital devices' operation that may be integrated together to provide unique identifiers for every device or create devices identification [6].

ICMetrics exploits behaviour of an embedded system, and gain a collection of features and properties for system identification. In principle, an ICMetric provided the additional advantage that no data of user is needed, which is important for applications that is no explicit interaction with human operators. A considerable change in the system's operation or the sensors readings that will cause changing in properties and features of the system, also the identifier of a system will be changed. Therefore, the ICMetrics could improve both dependability and security based on utilisation of the system's unique behaviour [7].

In this thesis, an identification system is proposed for applying identification of devices. The proposed system uses ICMetric technology to provide identification of intelligent wheelchair application. The ICMetric technology uses internal features of an intelligent wheelchair to generate an identification called an ICMetric. It can be used to provide services related to attack detection and authentication. The generation of ICMetric does not need user intervention and is generated when needed and discarded thereafter. Thus minimizing the chances of identity deterioration.

1.2 Related Works

Several researchers present overall security methods that are based on ICMetric technology. This section shows the previous studies that have been related to this work. Some of these researches are summarised below:

Hopkins *et al.* (2007) introduced research relating to an ICMetrics and capable of recovering the security concerns of System on Chip (SoC) based devices and their data. They aimed to provide an identification of each device and verifying the tampering lack using each device's unique features and properties. Their research provides a methodology to reproduce values of low level feature from a SoC by reconfiguration of its current debug support circuits that were originally designed to assist system-level monitoring and development. A novel proposed system approach for feature extraction yields an area saving of over 30% percent compared with dedicated circuits [8].

Yevgeniya K. and Gareth H. (2011) proposed technology applied on a healthcare environment. They aim to integrate the ICMetric system into an intelligent and autonomous wheelchair. The ICMetric technology are based on the concept of deriving encryption keys straight from features of electronic systems. The proposed technology provides an entirely template-free encryption model for electronic systems protection and data exchange. In addition, the ICMetrics allows for secure communication in case of both machine-machine and human-machine interaction [9].

Yevgeniya K. et al. (2012) introduced a new ICMetric technique that can be used for the aim of generating encryption keys, preventing malfunction of hardware components and systems, electronic signatures, detecting attempts of frauds. The technology is based on using characteristics of electronic devices to derive measurable features in order to produce identifiers that uniquely set the devices. They have addressed ICMetric features that allow for unique identification of the devices. They are deduce that proper ICMetric features can be extracted from frequencies of the program counter occurrences and their sequences observed during programs' execution flow [10].

Bin Y. et al. (2013) used ICMetric technology for the creation of encryption keys relating to the servers by employment of measurable features obtained from characteristics of specified cloud computing servers. The features should be identical, while the values of these features should permit for unique identification of each of the system servers. In their proposal, they are considered the properties of the server behaviors as a possible ICMetric feature and explored that the system's performance stability influences by the number of samples being inputted into the ICMetric system [11].

Hasan T. et al. (2014) proposed a secure filter task that is man-in-the-middle attack resilient. In order to make the plan more secure, they have depended on the latest ICMetric technology. This technology supports the use of single system attributes to create a single ICMetric number that can be utilised to system identification. Therefore, they suggested passing the number through a hash function because the ICMetric number cannot be straight transmitted because of security matters. They used Secure Hash Algorithm 1 (SHA1) and Secure Hash Algorithm 2 (SHA2) that possess individual feature and the complication of the SHA2 is reflected in the execution times of their proposed scheme. The outcome shows that SHA1 with ICMetric is totally

flexible and can be practically used with the experimented maximum size of 200 participants, whereas, SHA2 is complex and should be used for populations of up to 100 of members [12].

Hasan T. and Klaus M. (2014) presented a new security protocol that presents authentication for members of group and then it generates a group key and transfer method based on ICMetric. They proposed a unique protocol because it makes a single communication of group key that is created by individual supporting from each client in the group. In order to make the protocol even more flexible, the protocol is based on the employing of ICMetric. It supports the use of a hardware/ software characteristics to present a unique number that is distinct for every device. ICMetric number differs from device to device because each device has a different environment, software and hardware profile. The presented protocol uses the created ICMetric and applies a series of communications and computations between the clients and group controller [13].

Xiaojun Z. et al. (2015) analysed CPI (Cycles Per Instruction) and PC (Program Counter) from an embedded system for discovering compromised programs. The proposed system can be used to detect abnormal behavior in embedded devices. The proposed system offers protection at different levels for embedded architectures, such as function call sequence, internal control flow and instruction stream within each function. Since the main aim of their research is to apply a real-time security solution for complex embedded computer architectures, more evaluation of realistic attacks for the proposed algorithms investigated. Results achieved in their experiment show that the proposed method can identify unknown program behaviours not covered in the training set with accuracy at 90.9% and 98.7% [4].

Hasan T. et al. (2015) used accelerometer located in many spread devices for device identification. The proposed system is based on a variety of health devices provided with accelerometer sensor. ICMetric number is produced from readings of accelerometer sensor. These readings are analysed statistically and mathematically to create an ICMetric number. Shimmer health sensor embedded with accelerometer is utilised to create an ICMetric. Three axes readings are gained from a collection of five Shimmer sensors. The proposed system proves that it is possible to use the MEMS accelerometer for the providing identification of a device. It is proven that the

regeneration of the ICMetric is possible and each device or sensor produces unique identification supplied and there is not interference in process of generation [14].

Hasan T. et al. (2015) used the MEMS accelerometer characteristics to create an identification of sensor called the device ICMetric. This device ICMetric is created without intervention by human and only when it is needed. ICMetric of device and all attached data are removed from the system after using. In the presented system, ICMetric functionalities with a symmetric key protocol are combined for supplying authentication, access control and confidentiality of health data in a resource effective method. ICMetric technology prevents the major threats like man-in-the-middle attack, key theft and brute force attack associated with health data communication [15].

Ruhma T. et al. (2016) proposed a framework that exploits the security advantages of the device ICMetric to provide authentication, non-repudiation and confidentiality. They combined ICMetric of device and create a symmetric key generation method for preventing threats like man-in-the-middle attack, key theft and brute force attack associated to secure data communication [16].

Khattab M. and Klaus M. (2017) proposed a system based on ICMetric technology that uses the specific bias characteristics of infrared sensors to supply defense to the external communication of autonomous vehicles. The vehicle ICMetric basis number resulting from the infrared sensors is employed to identify self-driving vehicles. The ICMetric-IDS (ICMetric-Intrusion Detection System) is proposed for training and testing both abnormal and normal behaviors. It has a capacity to the external and internal identification of attacks. This ICMetric-IDS presents protection to VANETs (Vehicular Ad-Hoc Networks) with the first use of ICMetric in protecting the external communication of autonomous vehicles. The anomaly ICMetric-IDS detect some reasonable performance in identifying malicious vehicles for the external communication in self-driving and semi-autonomous vehicles. The ICMetric-IDS has the ability to notice and even block other kinds of attacks such as wormhole and Sybil attacks [17].

Khattab M. et al. (2017) proposed a system based on ICMetric technology that uses gyroscope sensor and other features of system in order to apply a new identification of vehicle identified as the vehicle ICMetric. The proposed system has important defensive ability against unseen attacks. The presented security system displays

effective performance in identifying and blocking malicious vehicles in vehicular ad-hoc networks of driverless vehicles and semi driverless vehicles. ICMetric-IDS has the capability to identify both the existing and earlier unexpected attacks. The ICMetric-IDS is a new security system that provides secure external communication, which is for the first time providing ICMetric in VANETs. They have exposed effective performance in recognizing and blocking malicious vehicles in VANETs of self-driving vehicles with using FFNN-IDS and k-NN-IDS [18].

Ruhma T. et al. (2017) proposed a cloud based ICMetric patient monitoring system. The proposed system combines the functionalities of ICMetric based secure transmission protocol for supplying integrity, authentication and confidentiality of data in a resource effective manner. The system is based on using MEMS sensor to generate a device ICMetric. The cryptographic key generated by ICMetric is utilised to perform encryption and decryption of patient's data communicated to health professionals [19].

Hasan T. et al. (2018) used a system for providing security in wearable devices based on ICMetric technology. ICMetric technology uses the features of a device to produce an identification for the provision of cryptographic services. Accelerometer and gyroscope sensors are used to generate device ICMetric. Since wearable devices often run in a group setting also a group identification is utilised to provide services like authentication, confidentiality, secure admission and symmetric key generation. Experiment and simulation results explain that the project shows high levels of security without compromising on resource demands [20].

1.3 Problem Statement

Execution of unknown or malicious software on an embedded system may trigger harmful system behaviour targeted at stealing sensitive data and/or causing damage to the system. It is considered a potential and significant threat to the security of embedded systems. Many techniques have been proposed to provide security yet do not focus on the most important question about who has access to the system.

An alternate approach for providing the security of system from measurable properties of a target device is named ICMetric. In this research, a security system is proposed, which based on ICMetric technology that exploits the characteristic and behaviour of an embedded system to obtain a collection of properties and features,

which aims to uniquely identify and secure an embedded system based on its own behavioural identity. The ICMetric technology allows a device to generate an identity for providing authentication and a range of other security services.

In addition, some security techniques depend on the stored keys to enable secure information. Such techniques have a failure, when the stored keys compromised, the security of any data protected by these keys will be compromised. Thus, it is important to employ security mechanisms to protect these systems from attackers. ICMetric technology has been designed as a method of deterring key theft by exploiting features of device to provide ICMetric number that will be utilised for identification of device. ICMetric number is not stored and generated when required by lightweight equation.

1.4 Thesis Objectives

In this thesis, a system is proposed to develop embedded devices security. The proposed system uses ICMetric technology, which proposes using features of a device to generate ICMetric number that used for device identification. The objectives behind proposing ICMetric security system were to overcome the problems related to accuracy rate, the failure to detect new attacks and the increased number of false alarms.

In this thesis, the objectives are as follows:

- Designing a security system for identification of embedded devices based on utilising ICMetric technology that depend on features that make each device different to generate a single and unique number called ICMetric number, which used for device identification.
- Solving security problem presented in embedded device by applying device identification.
- Proving that MEMS sensors can be used to improve security and apply identification of device. Bias reading generated by these sensors can be utilised to provide identification of device.
- Generating ICMetric number by applying some statistical and mathematical analysis on bias readings extracted from MEMS sensors. ICMetric number is integrated to the dataset extracted from trace files for improving identification and other security services.
- Detection of abnormal scenarios by generating the ns-2 trace file.

- Testing, evaluating system performance metrics, which are confused matrix, accuracy rate and error rate.

1.5 The Main Contributions

The proposed system depends on utilising ICMetric technology that exploits device features to generate a unique number called ICMetric number, which used for device identification. The earlier research proposed generating single ICMetric number by using one type of MEMS sensor [18], while the proposed system has the following main Contributions:

1. Hybrid ICMetric numbers are generated by exploiting bias readings extracted from two types of MEMS sensors, which are magnetometer and gyroscope sensors.
2. Triple ICMetric numbers are generated by exploiting bias readings extracted from three types of MEMS sensors which are magnetometer, gyroscope and accelerometer sensors.

These numbers are utilised in dataset extracted from the trace file that has been generated by ns-2 to perform detection and authentication.

1.6 Thesis Structure

This thesis is presented in five chapters. The first chapter presents the introduction, scope and objectives of the research.

Chapter Two: presents the theoretical background and basic concept of ICMetric technology.

Chapter Three: explains the steps of the suggested system and techniques that are used. A whole description of the suggested system is given.

Chapter Four: presents the results of tests that have been implemented to estimate the system performance. The results of experimental examinations are discussed.

Chapter Five: summaries the final conclusions, recommendations for future works and limitation of this research.

CHAPTER Two

Theoretical Background

CHAPTER TWO

Theoretical Background

2.1 Introduction

Currently, the concern is to protect the hardware and software from the attack. Security means protecting systems of computers from damage and unauthorised access by hackers and malicious software such as viruses. Data security is to maintain the authentication of data so companies are currently seeking to achieve security to maintain the authentication of data and do not lose the reputation in the event of data theft or damage by the attackers. Security is the common name for the collection of tools designed to defend data.

Network security means that data during their transmission need to be protected. The network security term is somewhat misleading, because virtually all business and government interconnect with a collection of interconnected networks. Such a collection is often referred to as an internet, and the term internet security is used. There were no obvious limits between these two forms of security. For example, the computer virus is one of the most common types of attacks in information systems. A virus can physically enter a system when it reaches an optical disc, and then it moves into a computer. Viruses can also arrive via the Internet. Once the virus resides in a computer system, security tools are needed to detect and stop the virus.

This chapter states the concept of security also types of attacks and vulnerabilities presented. ICMetric technology and its phases explained in this chapter as technology for providing security services. This chapter provides some details of intelligent wheelchairs as application used in this research and MEMS sensors embedded with it.

2.2 Security Concept

Security aims for achieving the protection of system information in order to preserve the data from manipulation and theft and to attain the availability, confidentiality and integrity. It includes protection of hardware, software, information and telecommunications [21].

Security is a term used to describe different states, such as lack of risks and threats situation, prevention of risks or achieve confidence. Achieving security is required in many areas at the level of individuals and organisations. Ensuring security requires individuals with competence and experience so the level of security varies from one organisation to another. To ensure better security for organisations and individuals, it is important for network users to use the systematic approach, which involves analysing, designing, implementing, and maintaining a required network security system [22].

There are many goals of security as illustrated below [21]:

- **Authentication:** Means verifying the identity of a device or person.
- **Confidentiality:** Means preserving the information confidential to prevent unauthorised access to the information. Confidentiality loss of information means disclosure of information, which leads to loss of information.
- **Availability:** Means the data is available when needed. Failure to access information in a timely manner causes a system malfunction.
- **Integrity:** Means ensuring that the information is sound from manipulation and destruction. Lack of integration means that information is subject to modification or sabotage.
- **Non-repudiation:** Ensures that information can never deny ever sending or receiving the message.
- **Access Control:** Block illegitimate or unwanted access by restricting access only for authenticated entities.

In order to gain illegitimate access, adversaries are capable of exploiting system weaknesses. It is essential to guarantee the hardware and software security of any system.

2.3 Security Attacks and Vulnerabilities

Security threats and vulnerabilities are pervasive and threaten systems. In order to protect systems from attacks and vulnerabilities, security experts must assess and identify the risks and vulnerabilities of the system and define how to use mechanisms that ensure security for the safety of the system. Section below presents a discussion of possible attacks of the system and their propagation in daily life.

2.3.1 Security Attacks

The system can be exposed to attacks of the external type, which manipulates the messages and distort them or the system can be exposed to attacks of the internal type that is within the networks. In other respects, the attacker can be classified as active, this type of attacker will modify the data or passive attack that is related to eavesdropping [23]. Many types of attacks, such as focused attack, cryptanalytic attacks and network attacks. In this chapter, the concern is with network attacks, where systems are vulnerable to external attack through networks. This type of attack is done through monitoring, password hiding and spoofing. Types of network attacks presented below with some details [3]:

a- Passive Attacks

A passive attack observes unprotected or weakly encrypted communications between two nodes to acquire authentication information or passwords that may be passed to parties that may compromise the system.

b- Active Attacks

By circumventing, executing malicious codes and injecting viruses or trojans, the attacker can tamper with system protection. If it can access the servers, the active attacker can fail the system or the entire network.

c- Insider Attack

This type of attack is performed by persons within the system who cannot be satisfied with the service for a particular reason and attempt to sabotage.

d- Phishing Attack

In this type of attack, the attacker creates fake web sites and asks users to enter their data. The attacker uses this data to log onto other sites and carry out sabotage and theft.

e- Hijack and Spoof Attacks

In this type of attack, the attacker gets the communication session. The other party in the session thinks that is communicated with the original party, which leads to the disclosure of information that may be important and very dangerous.

f- Denial of Service Attacks (DoS)

In the networks, availability of nodes is considered very essential for the fact that a communication network is depended by all users. Packet drop attacks or black hole attack is a kind of DoS attack that have negative and direct impact on routing protocols or network layer.

2.3.2 Targets of Attacks

The system is exposed to the different of attacks, some of these attacks are presented in the following subsections. Generally, expected attacks are divided into three groups: the attacks against availability, authenticity and confidentiality [24]:

1. Threats on Availability

Two categories of threats on availability are mentioned, which are:

- a- Message Suppression Attack:** packets are dropped by the attackers from the network, they exploit these packets in other time. This type of attacks causes a lot of problems on the network.
- b- Drop the package:** Black hole attack is a dropping attack, where the existence of this type of attack is the reason of package losing [25].

2. Threats to Integrity

An example of this threats are alteration attack that happens when the attack changes message content. Re-send or delay of the message considered one of the forms of this attack.

3. Threats on Authentication

An example of this threats is fabrication Attack. Attackers can gain their goals by broadcasting false messages in the network. These false messages, such as certificates, warnings and identities.

2.3.3 Security Vulnerabilities

A vulnerability is a weakness in the system or weakness in controlling the protection of the system during the implementation process and the difficulty of maintaining its internal elements. This encourages the attacker to attack the system. Vulnerabilities

lead the system to possible hacking operations that are at the level of one file for a mobile device or a computer to a huge database at the enterprise level. Weaknesses in any system lead to loss of stored information. The size of the damage caused by the attack varies depending on the type of attack. Threat sources may be individuals, groups, organizations, or entities that check to use an organization's dependence on cyber resources. A threat event is a situation that could cause unwanted results [23].

2.4 Integrated Circuit Metric Technology

Encryption systems rely on the use of algorithms that depend on the use of the stored secret key. Trying to increase the size of the key to stop the brute force, but increasing the size of the key cannot always protect the security of the system and deter theft [15].

In order to eliminate the theft and by relying on the special features of each device, identification of device is created. Other hardware techniques differ from the ICMetric technology in the selection of device characteristics. Traditional fingerprinting techniques depend on the characteristics that are easily exposed to capture, deception or repetition by the attackers. ICMetric technology uses some of the attributes that increase the complexity of generated ICMetric and they are hard for an attacker to predict, such as Media Access Control (MAC) addresses and serial numbers. Other features are utilised, which are application usage special, such as browsing histories, camera resolutions, common user files, system profiles [15].

ICMetric technology retains the idea of storing the key, where there is no encryption key in the system this will reduce the attackers. It uses hardware and software feature of device to create ICMetric used for encryption services. There is a similarity between the biometric systems and the ICMetric, as these systems used features for identification of different persons. Similarly ICMetric uses the characteristics of the device to identify each device uniquely and thus eliminates and deters theft of stored keys [26].

ICMetrics points to a new technique that can be employed to extract features from the hardware and software environment of a system. Every device is singular in its internal environment then the features that make every device diverse can be employed to create a unique and single number for each device. It is based on the next concepts [5]:

1. ICMetric number is not store on the system and can be recreated when needed.

2. If the system is attacked, there will be no theft because the ICMetric is non-store.
3. ICMetric number and any proceeding outcomes that are based on the ICMetric number will be change if any adjusting done with the software, hardware or environment.
4. There is no requirement to store any template that can serve the aim of device validating.

The generation of ICMetric system is required two phases, which are calibration phase and operation phase.

2.4.1 Calibration Phase

In this phase, the characteristics are documented and analysed, normalisation distributions are utilised on feature values noticed in the system. A device ICMetric basis number can be created by applying statistical and mathematical operations on the extracted feature values. This phase is utilised once only when the system needs the ICMetric basis number. The features on which the ICMetric is based are unique, therefore it is difficult for the attacker to detect or generate it. This is an important case to improve the ICMetric strength [23].

2.4.2 Operational Phase

In this phase, the unique number is generated depending on the extracted features. The preprocessing phase can be applied to generate unique features that distinguish it from others [23]. Figure 2.1 shows how the ICMetric basis number is generated by first applying the calibration phase. In this phase, the sensor readings are obtained, after that they are subjected to statistical operations in the operation phase. In the operation phase an attempt is made to generate a resulting device ICMetric basis number through either feature concatenation or feature addition [23].

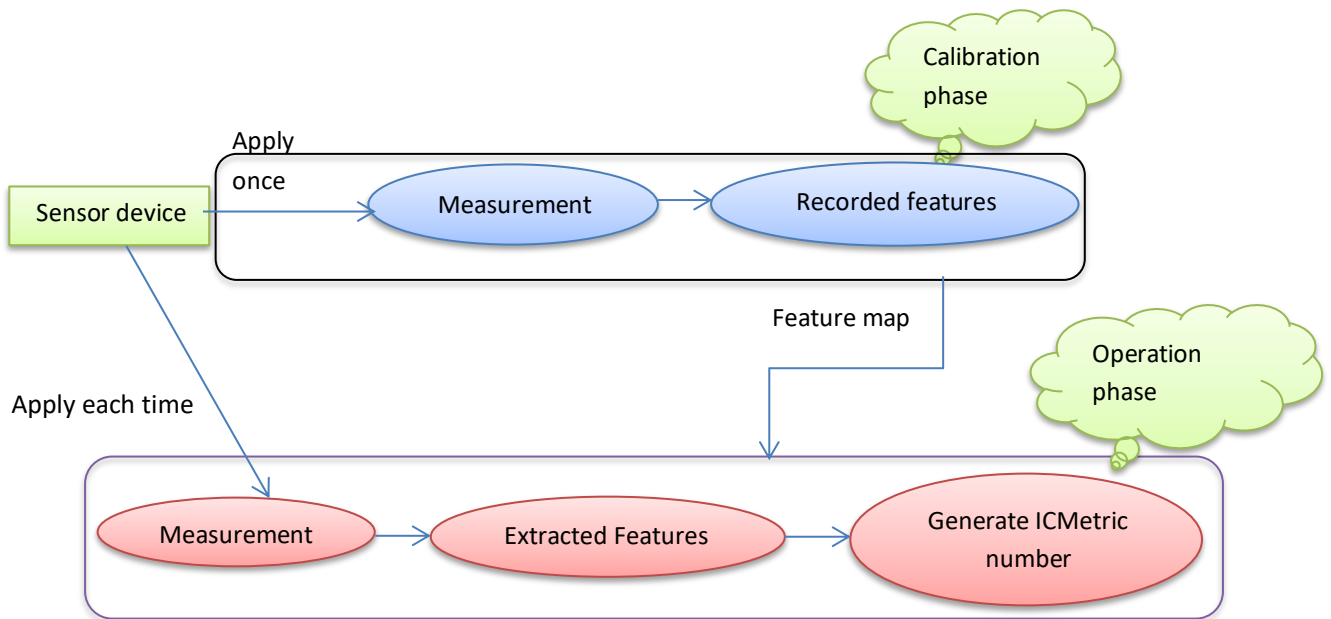


Figure 2 .1: Flow Diagrams of ICMetric Phases [27]

The ICMetric technology has some limitations, which can be illustrated below:

1. An essential requirement for generation of the proposed ICMetric is that the aimed device must be embedded with MEMS sensors. This situation restricts the researcher to the particular type of device.
2. Readings extraction from sensors is another limitation. The sensor must be placed on place that is stable and free from movements and vibrations to achieve correct readings.
3. The entropy and length of the generated ICMetric number is a limitation of proposed ICMetric. The proposed system generates strong ICMetric number in order to apply device identification for more security of system.
4. The stability of ICMetric number is one of the limitations that depends on several factors, such as number of sensors available for applying readings and the environment of their operation, features employed and mathematical equations.

2.5 Intelligent Wheelchair Application

Intelligent wheelchair can be defined as a uniquely modified powered wheelchair, which is provided with a control system and variant sensors. It also can be defined as a mobile robot base equipped with a seat. Intelligent wheelchairs are designed to provide

several services to users in different ways. It eliminates the user's responsibility for moving the wheelchair. User types of intelligent wheelchairs are different according to their situations and disabilities. According to this, there will be different designs of intelligent wheelchair. The aim of intelligent wheelchair is to grant higher independence to people with lower mobility such as disabled or elderly individuals [28]. Figure 2.2 states intelligent wheelchair.



Figure 2.2: Intelligent Wheelchair [29]

In this thesis, ICMetric technology is integrated into an intelligent wheelchair. MEMS sensors embedded in intelligent wheelchair are utilised to ensure effective usage and to provide identification.

2.6 MyAHRS_plus Sensor

In this research, the bias readings that were created from the accelerometer, gyroscope and magnetometer sensors are utilised to identify the device. The myAHRS_plus is a low-cost high-performance AHRS (Attitude Heading Reference System) with USB/UART/I2C interface. Figure 2.3 shows the myAHRS_plus sensor [30]:



Figure 2.3: myAHRS_plus Sensor [30]

MyAHRS_plus sensor is considered one of the most perfect sensors in the scientific research area. It is an embedded sensor triple axis magnetometer, accelerometer and gyroscope with a sensitivity of $\pm 16g$. A various number of bias reading is obtained from myAHRS_plus to generate ICMetric basis number. The security system needed to determine the optimal number of offset readings that were used to apply identification for device. Many features of myAHRS_plus sensor are described as below [30]:

- ❖ Easy: All the settings can be organised through the dedicated monitoring program with graphic interface. It also presents the sensor data in real time and can hold and save the sensor data.
- ❖ Versatile: The myAHRS_plus data packets can be parsed for user applications and sample codes are presented.
- ❖ Cost Efficient: Very reasonable price, while it provides better data compared with other sensors.
- ❖ Wide Compatibility: Provides interfaces (USB/UART//I2C) for simple integration to various types of host systems and peripherals.

The myAHRS_plus sensor embedded with 3-axis gyroscope, 3-axis accelerometer and 3-axis magnetometer sensor. Output data of sensors is rotation, acceleration, and magnetic orientation respectively. The myAHRS_plus sensor size is 21mm x 27mm (PCB) [30].

In the proposed security system, myAHRS_plus sensor is utilised in design ICMetric security system. To generate ICMetric basis number various number of bias reading is obtained from myAHRS_plus sensor.

2.7 Micro Electrical and Mechanical System

Micro Electrical and Mechanical System (MEMS) combines mechanical and electrical components through generating miniature integrated devices. They are created using Integrated Circuit (IC) batch processing techniques and can range in size from a limited micrometers to millimetres. These devices have the ability to sense, control and actuate on the small scale, and produce a result on the large scale [31]. Modern smartphones, laptops, vehicles and wearable devices are provided with many MEMS based sensors [20]. The sensors recognise and translate thermal, mechanical,

magnetic, chemical and optical phenomena into digital readings by utilising specified electrical components [26]. Figure 2.4 illustrates Schematic illustration of MEMS components.

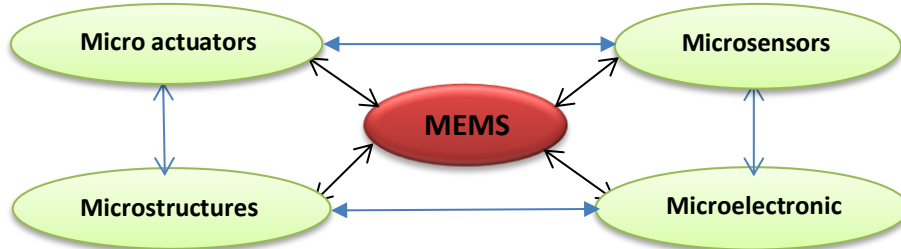


Figure 2.4: Schematic Illustration of MEMS Components [31]

As illustrated in the figure 2.4, MEMS system is comprised of four elements i.e. Microsensors, microelectronic, microstructures and micro actuators.

2.7.1 MEMS Accelerometer

The accelerometer is a displacement sensor based on capacitance. It is made of static plates located in a mobile mass mounted on a spring. By a change in capacitance, capacitive sensors detect physical input. Capacitance change is so small that it can only be read using specific electronic components. The sensor contains set of plates that are suspended in a movable mass. A voltage is utilised across the plates so that a change in capacitance can be measured, when the sensor is submitted to an external strength. When applying the acceleration, the movable mass moves, which in turn provide a change between the suspended plates and the movable mass in capacitance. a voltage has been applied to the plates suspended in the movable mass [26]. Figure 2.5 shows the principle of working MEMS accelerometer (a) no acceleration output in the same capacitance on the static plates (b) the change caused by acceleration in capacitance between the static plates [26].

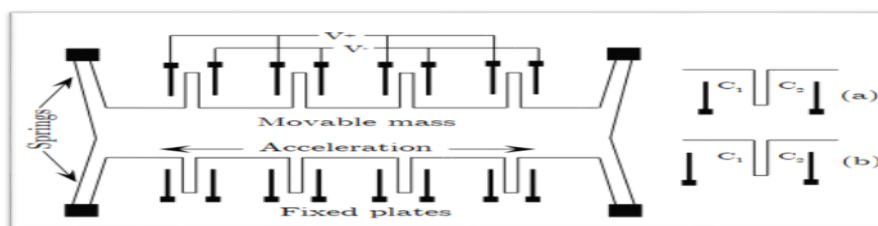


Figure 2.5: The Principle of Working MEMS Accelerometer (a) No Acceleration Output in the Same Capacitance on the Static Plates (b) Change Caused by Acceleration in Capacitance between the Static Plate [26]

When static plates in the sensor are applied with voltage V , a voltage creates a capacitances $C1$ and $C2$ between the static plates and the movable mass. If the device is fixed or moving at a stable velocity then the two capacitances $C1$, $C2$ will be equal.

Both capacitances $C1$, $C2$ will not be similar if the device experiences a change in velocity. When a MEMS accelerometer owns an imperfection, it is reflected in the readings gained from the sensor. Therefore, if an acceleration is provided to the axes of a sensor, then the readings of the detected acceleration will vary from those that are applied. The readings from a recent accelerometer explain the acceleration (m/sec^2) along the three axes of motion [26].

2.7.2 MEMS Gyroscope

MEMS gyroscope sensor is based on the coriolis impact [32]. This impact is occurred via a body, when it is submitted to velocity in a rotating frame of reference. The drive arms are formed to be tall structures that resonate according to the sensed rotation. The MEMS gyroscope construction and how the drive arm behaves shown in Figure 2.6. This figure illustrates principle of working MEMS Gyroscope in two cases, the first case when driving arm movement with rotation and the second case, when drive arm movement with lateral movement [26].

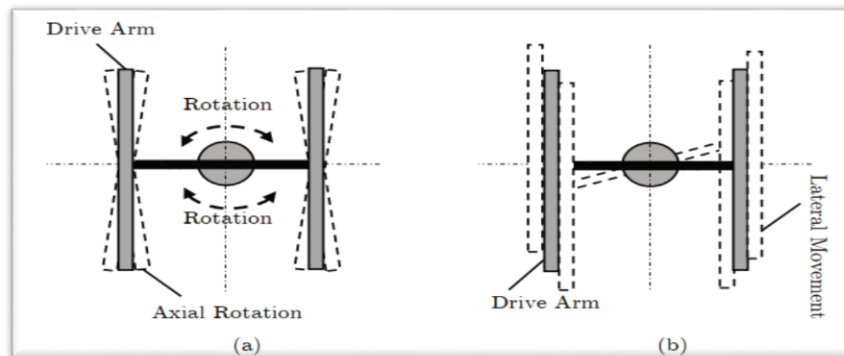


Figure 2.6: The Principle of Working MEMS Gyroscope (a) Movement of the Drive Arm with Rotation (b) Movement of the Drive Arm with A Side Movement [26]

Readings from a gyroscope can be utilised to discover bias presence [33]. Gyroscope owns an imperfection exhibit in the readings acquired from the sensor. The readings from a recent gyroscope represent the rotation (deg/sec) along the three axes of motion.

2.7.3 MEMS Magnetometer

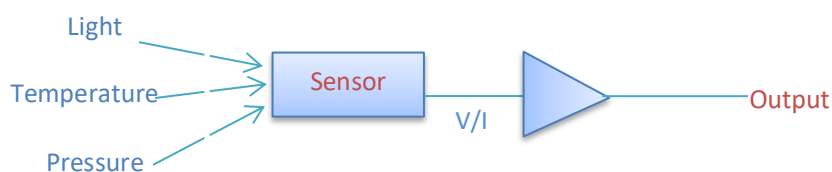
Magnetometer sensors are now widely used in many fields, in response to the demands of users in the automotive industry, Judgment, military/aerospace and consumer [34]. They are widely used with a magnetic field vector of the earth to determine the heading of the device, for example, a digital compass. Magnetometers are affected by magnetic field troubles that can cause bias, scale and loss of orthogonality in the signals measurement [35].

MEMS technology provides the most popular MEMS magnetometers. Intelligent wheelchairs utilised magnetometer sensors for measuring and detecting magnetic fields. Hall Effect, magneto-resistive effect and fluxgate effect are the most common principles in magnetometer sensors [42,43]. Magnetometer sensors play important role in designing intelligent wheelchairs applications. The proposed system depended on features extracted from bias readings of magnetometer sensors. Intelligent wheelchair application utilised MEMS magnetometer based on Hall Effect to measure the magnetic fields as presented in the figure 2.7.

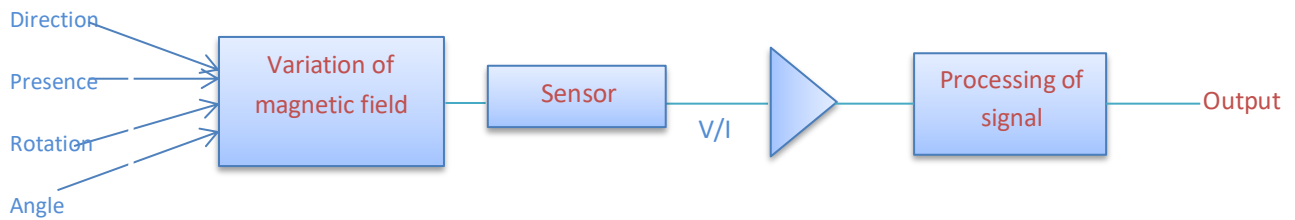


Figure 2.7: Magnetometer Sensor [38]

Magnetometer sensors differ from conventional sensors in physical properties detection. Conventional sensors detect a physical property directly, while the magnetometer sensors detect changes in magnetic fields and from them derive information on physical properties as explained in the figure 2.8.



(a) Conventional Sensors



(b) Magnetometer Sensor

Figure 2.8: The Difference between Conventional Sensors and Magnetometer Sensors in the State of Physical Properties Measurement [39].

2.8 Hardware Imperfection

Both the device and the embedded sensors analysis are required for exploring sensor imperfections during its readings. Some sensors do not have adequate distinguishable features so not all sensors produce an identification of hardware. Even if a sensor has special features an attacker may be capable of reproducing the readings by applying another sensor in the surrounding area of the target sensor so that attacker can gain very closer readings. So, a process is needed that permits to find imperfection in sensor using implicit features, which is not possible to be reproduced by an attacker [40].

When MEMS sensors are placed on the board, simulation is applied to produces a constant bias. The case is similar when a sensor is under operation, where accuracy of sensor output is affected by unclear damages due to mistreating [41]. Sensor bias can be produced by many types of mechanical effects while the electrical integrity is preserved. Sensors biases are different from one to another. Calibrations attempt to recompense for readings error by combining a linear value into the raw values applied by the sensor [42].

The new concept is applied by using sensor imperfections with the ICMetric technology. Earlier researches use bias of sensor for only device identification. The ICMetric technology is the first to use features of sensor and bias for device identification, which is used for security services [26].

There are many features of devices, which can be utilised for identification processes. The complexity with using features of devices is that the extracting of some features is so hard or may not identify a device uniquely. Features of device are used for generating an ICMetric. Different readings are being extracted as a result of various instances of

the same device incorporated with the same sensor even when a similar stimulus is being offered [43].

Each sensor has a bias, which is generated by a standard stimulus. Since the ICMetric should be created without any intervention by user, therefore, a stimulus is needed, which does not request specific device or any work by a user. For example, the magnetometer bias can be exploited for producing an ICMetric but this sensor is influenced by the existence of electrical equipment like speakers and is also influenced by the signals of communication. Therefore, to use the magnetometer would grow ICMetric generation complexity and greatly decrease system practicality.

2.9 Intelligent Wheelchair Sensors

In order to apply features measuring of wheelchair, specific hardware circuits along with a software-based monitoring infrastructure is needed to be prepared and integrated in the system. Features can be read from various integrated sensors and large origin of features is also the system's behavior [44]. For obstacles avoiding, intelligent wheelchairs need sensors to perceive their surroundings. Many sensors are used by intelligent wheelchairs as explained below [45]:

- Ultrasonic sensors are very precise when the sound wave emitted by the sensor strikes an object at a right angle or head on.
- Infrared (IR) sensors, that emit light, rather than sound, and can be fooled by dark or light absorbent material rather than sound absorbent material.
- Laser Range Finders (LRFs), which offer a 180°, two-dimensional scan within the plane of the obstacles in the environment. Another option is a "laser striper," which contains of a laser emitter and a charge-coupled device camera. The image of the laser stripe returned by the camera can be used to determine distances to obstacles and drop-offs based on breaks in the stripe.

MEMS sensors have many applications in measuring either acceleration or angular velocity about one or several axes as an input to control a system [46]. Some details of accelerometer, gyroscope and magnetometer sensors used in this research presented below:

2.9.1 MEMS Accelerometer in Intelligent Wheelchair

The MEMS accelerometer is a highly sensitive sensor and capable of detecting the tilt. This sensor changes the direction of the wheelchair by depending on tilt. For

example, if the tilt is to the right side, then the wheel-chair moves in the right direction and if the tilt is to the left side then the wheel moves in the left direction. The wheel-chair movement can be controlled in forward, reverse, left and right direction with obstacle detection using ultrasonic sensor. This wheel-chair automatically senses the presence of an obstacle in its path and turn its direction of movement [47].

2.9.2 MEMS Gyroscope in Intelligent Wheelchair

The MEMS gyroscope sensor provides an angular velocity of the wheelchair's wheel as compared to translate the acceleration values to rotation angles for calculating wheel rotations. Angular velocities are used directly to estimate linear speeds and distances traveled, which allows to provide wheelchair users with real time feedback through smartphone applications [48].

2.9.3 MEMS Magnetometer in Intelligent Wheelchair

Intelligent wheelchairs used MEMS magnetometer sensors for measuring and detecting magnetic fields. Hall Effect, magneto-resistive effect and fluxgate effect are the most popular principles in magnetometer sensors. Magnetometer sensor measure the magnetic fields based on Hall Effect [52-53].

The proposed ICMetric security system presented here uses bias readings that have been generated from sensor devices. These readings are used to apply ICMetric basis numbers that were utilised as identification for device. Current research in sensor-based identification field has proved that the use of sensory data is possible and that it is feasible to provide device identification [54-55].

2.10 Sensors Bias Measurement

In some cases, it is not feasible to collect the bias in the sensor. Sensors are required for generating the bias readings of a system, which do not require user intervention and are not influenced by external factors [20].

MEMS is a technology that combine mechanical and electrical components. There are many MEMS based sensors that are being embedded into recent vehicles, wearable devices, laptops, and smartphones. The most commonly used and good examples of MEMS sensors are the accelerometer, the magnetometer and the gyroscope. Accelerometers are intended to measure the acceleration of an object, while

gyroscopes measure angular velocity [20]. Magnetometer sensors are used for measuring and detecting magnetic fields [37]. MEMS sensors are used in many researches because they are readily available and also because the required stimulus is easy to create [26].

2.10.1 Gyroscope Bias Measurement

The myAHRS+ is embedded with a gyroscope sensor, which measures rotations per second. For bias generation, the stimulus must be specified. One of the advantages of stimulus is that it does not need a specific device to evaluate it, but is equipped by the user. The readings generated by the sensor must be equal to the stimulus applied to the sensor. Every axis owns a different bias, which is showed in the readings. Experiments prove that the bias in the gyroscope is unique and reproducible. Gyroscope bias is an implicit feature because it cannot be predicted for any specific sensor [20].

2.10.2 Magnetometer Bias Measurement

MEMS magnetometer sensors are used for measuring and detecting magnetic fields [37]. It must be placed on place that is stable and free from erratic movements to extract the offset values. The output readings from the magnetometer sensors are utilised to prove that each sensor behaves differently when subjected to the same stimulus. Each axis of magnetometer sensor owns a bias, which is unique and showed in the readings. The bias in the magnetometer is unique and represents an implicit feature of sensor because it cannot be predicted for any specific sensor [17].

2.10.3 Accelerometer Bias Measurement

The sensor should be placed on surface that is stable and away from vibrations or electronic alarms in order for the readings to be correct. In order to generate the bias, the stimulus must be specified. One of the advantages of stimulus is that it does not need a specific device to evaluate it, but is equipped by the user. The readings generated by the sensor must be equal to the stimulus applied to the sensor. Every axis owns a bias, which is unique and showed in the readings. Experiments also prove that accelerometer bias is unique and reproducible when the stimulus applied remains the same. Accelerometer bias is implicit feature because it cannot be predicted for any specific sensor. Statistical differences in the histograms gained from the various sensors makes accelerometer bias a good implicit feature for the generation of ICMetric [20].

2.11 Artificial Intelligence

Artificial Intelligence (AI) is a branch of computer science, which plays an important role in many research areas [50]. AI has the ability to gather knowledge to solve hard problems. It is the study and developments of intelligent machines and software to learn, collect knowledge, manipulate, communicate and understand the objects. AI technologies offer benefits in many of their applications. The major areas of AI are [51]:

- Expert Systems
- Speech Understanding
- Robotics and Sensory Systems
- Natural Language Processing
- Computer Vision and Scene Recognition
- Neural Computing
- Intelligent Computer-Aided Instruction

AI enters into many fields to solve complex problems and makes decisions. It ensures reliability and effectiveness in terms of cost. Although it makes our lives easier by solving complex problems in a short time, it has drawbacks as it can replace humans in many areas and this can lead to people without jobs [52]. AI is mainly based on the techniques designed on the basis of scientific findings, such as statistics, math and biology. Many techniques applied in artificial intelligence are NN, EC, GA, FL and HAI [43,44].

2.12 Support Vector Machine

Machine learning is subfield of the AI that relates with the development of methods and techniques for allowing the computer to learn. Machine learning concerned with the development of algorithms, which support the machine to learn and implement tasks and activities. It is related with constructing computer program that develop its performance with experience. By using a sample set of training data, machine learning system is trained to improve performance, when the system is used to implement the needed function based on the learning experienced. Recently many effective machine learning applications have been acquired; among them are data mining programs, autonomous vehicles, pattern recognition system, and information filtering systems

[53]. In this research, SVM is discussed as a method of training for the proposed ICMetric security system. SVM is learning algorithms of classification and regression prediction that uses machine learning concept to maximise accuracy of predictive and automatically avoiding overfitting to the data. SVM robust, accurate and effective they have their roots in statistical learning theory and have achieved importance even when using a small training sample. It is essentially binary classifiers; they can be implemented to handle the multiple classification tasks general in remote sensing searches [54].

SVM approves the basis of structural risk minimisation, it solves the matters over learning and applied good ability of generalisation. It implements data vectors classification by a hyperplane or set of hyperplanes in a high dimensional space. In the input space, the data points are not linearly separable so they need nonlinear conversion into a high dimensional space and then the linear maximum margin classifier can be employed. For this purpose, kernel functions are used at the training time of the classifiers to choose the support vectors along the surface of the function. For data classification SVM uses these support vectors to outline the hyperplane in space of the feature [55].

2.13 Network Simulator 2

Network Simulator 2 (ns-2) is an open-source event-driven simulator proposed specially for studies in computer communication networks. It is gained great interest from government, academia and industry since its serving in 1989 [56]. Having been under constant growing and investigation for years, ns-2 comprises modules for numerous components of the network, such as transport layer protocol, routing and application. Researchers can simply utilise an easy-to-use scripting language to test performance of network, configure a network, and observe results applied by ns-2. Obviously, ns-2 has become open source network simulator widely [56].

The ns-2 is an alternative system to a real network. It is designed to work on the Linux operating system and may be executed under windows operating system with Cygwin [57]. This system simulation improved a lot of researches and experiments effectively for various networks protocols.

C++ and Tool Command Language (TCL) are used to increase efficiency of the simulation in ns-2. In order to specify the path of nodes movement and behaviour of communication TCL script file is used. In addition, the output of simulation requires two files are trace file and Network Animator (NAM) file is specified by using TCL script file. TCL language was created by John Oosterhout [58]. It allows for programmers a fast development of the projects. TCL is free, flexible and it provides a graphical interface (NAM).

Researchers are employed ns-2 because it has some properties that support them in their works, such as efficient, open source, a rich library and widespread in research area [56]. The researchers prefer to utilise ns-2 if the proposed security system on physical, network and data link layers. On the other hand, ns-3 is more suitable if the proposed security system on transport, application layers [59].

2.14 Routing Protocol

Notification messages, sensitive information, control data and warning messages are transferred between nodes via three methods: Bi-directional, multi-hop and multi hop position based [23]. In order to transfer data to all nodes, a protocol is needed that avoids collisions and congestion and handles messages. One of the most essential things is choosing the suitable routing protocol. Choosing protocol depends on the nature of network work. There are two main protocols, topology and geographic-based routing [60]. In this research, the topology based routing is utilised. This protocol is divided into two types reactive and proactive routing protocol. Figure 2.9 presented below offers routing protocol types:

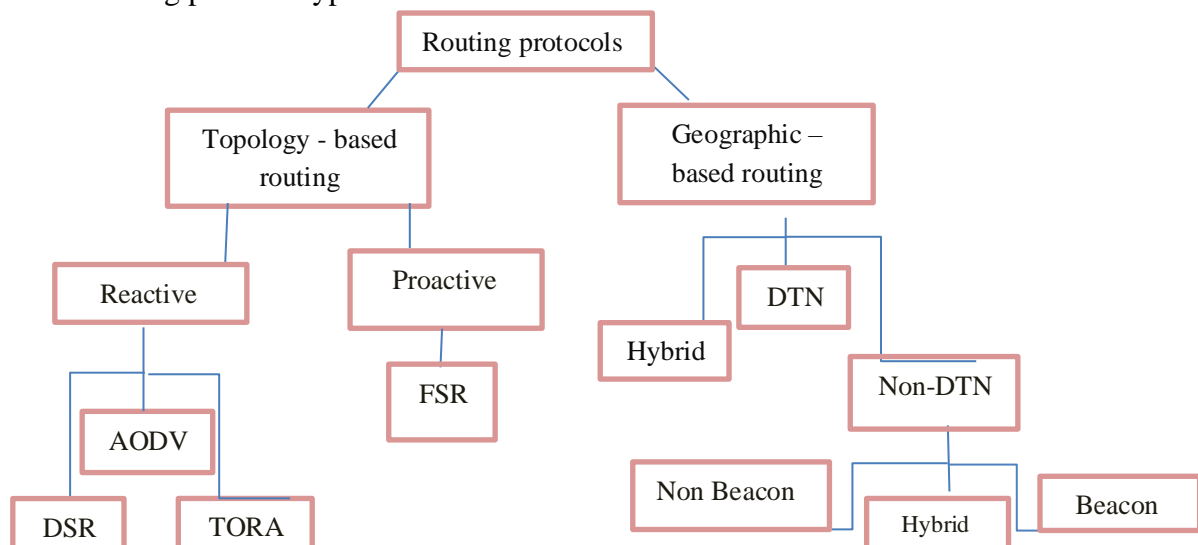


Figure 2.9: Protocols Types

- Reactive Protocol: This type of protocol will reduce the burden on the network. It transmits packets only to the available paths.
- Proactive Protocol: Routing information to forward the package to the next hop must be addressed without attention to request of the connection.

In this research, the reactive protocol is utilised. This protocol has many types, such as Ad hoc On Demand Distance Vector (ADOV), Temporally Ordered Routing Algorithm (TORA) and Dynamic Source Routing (DSR). The routing protocol AODV is appropriate for working in this research and it is selected for some reasons:

1. Even if the connection fails, this protocol can respond.
2. AODV is suitable when a large number of nodes.
3. AODV reduces the burden on the network compared with the other protocols (reduces messages flooding in the network).

2.15 Source Collection of the Dataset

In order to evaluate the performance of the proposed ICMetric security system, a trace file is used. The trace file generated from ns-2 and can be used to evaluate the performance, such as the number of packets transferred between nodes, the delay in the transfer of the packets, packet drop and Internet Protocol (IP). In this case, the number and type of the features are very essential for the proposed system efficiency. The information obtained from the trace file of the AODV is separated into three major parts [61], as presented in figure 2.10:

- AODV trace file basic information: Main nodes information is shown in this section of the trace file.
- IP trace part: Source IP and destination IP of nodes are defined in this section of the trace file, including live time and the next hop of the node.
- Extra information in the trace file: Main additional information in the trace file is declared in this section. These include the hops number, ID of the broadcast, destination sequence number, IP of the destination, IP of the source.

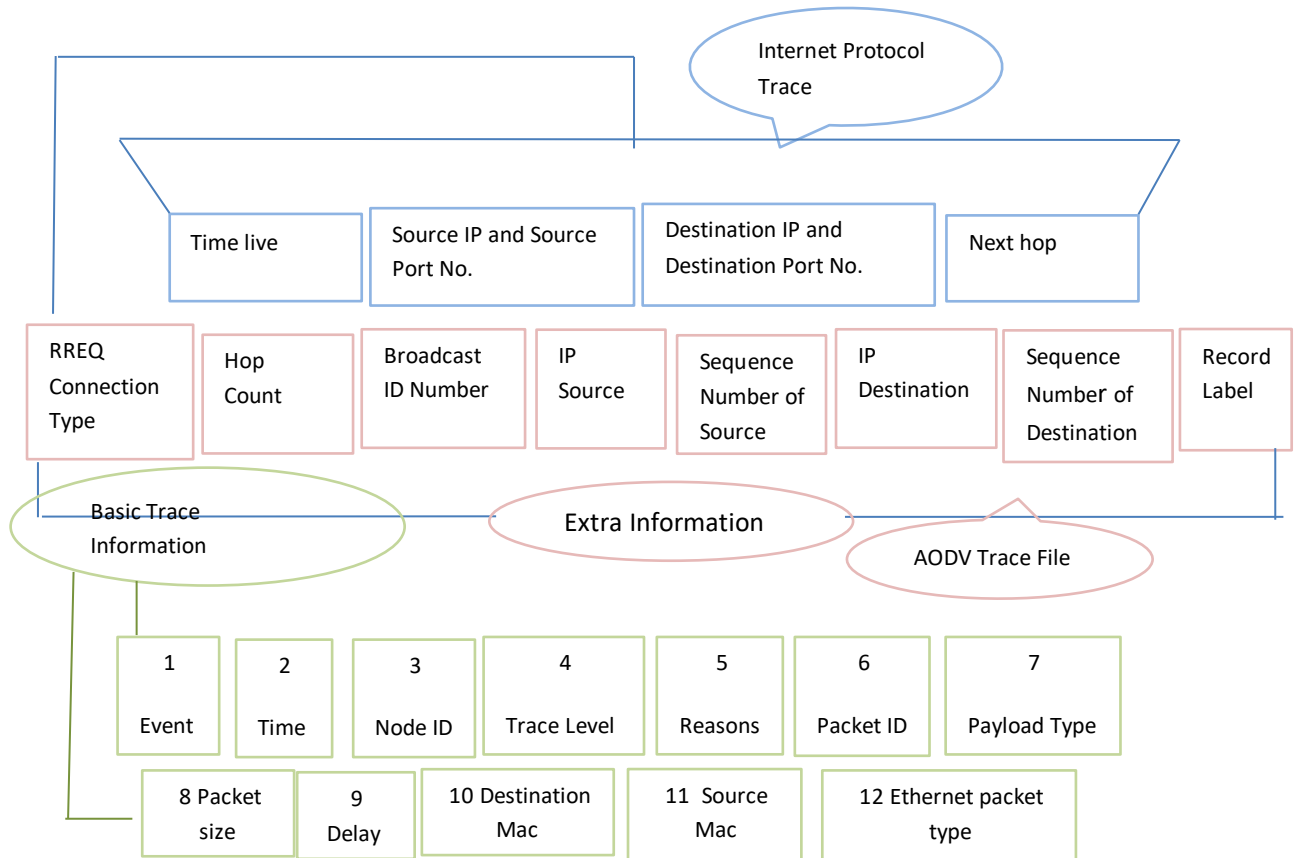


Figure 2.10: AODV Protocol Trace Information

CHAPTER THREE

Design and Implementation

CHAPTER THREE

Design and Implementation

3.1 Introduction

A device can use many approved features for identification, but these features can be captured by opponents. ICMetric technology generates a unique device identifier that can be exploited for many security services, such as authentication, integrity, key generation and privacy. Identification of device is provided for applying security services by using ICMetric technology. The security of a system based on utilising ICMetric technology depends on exploring appropriate features to generate an ICMetric device. Many recent devices have been used embedded MEMS sensor for the providing of many services. The MEMS sensors, such as accelerometer, magnetometer and gyroscope have a bias, which is used for ICMetric generation.

In this chapter, ICMetric basis number is generated from bias readings that have been provided from sensors inside intelligent wheelchairs application. The ICMetric technology allows a device to generate an identity, which is exploited for many security services. This chapter discusses the capability of providing an ICMetric by utilising features generated from MEMS sensors. Trying on unique features for the creation of an ICMetric is based on a myAHRS_plus Sensor.

The following are the basic resources required in developing and executing the proposed model:

1. Network simulator 2 (ns-2) is utilised to apply trace file, where the proposed system is tested with the date set extracted from the trace file.
2. The proposed system requires utilising myAHRS+ sensor. It is an embedded sensor triple axis magnetometer, accelerometer and gyroscope. In the proposed security system myAHRS+ sensor is utilised in design ICMetric security system. To generate ICMetric basis number various number of bias reading is obtained from myAHRS+ sensor.
3. The training phase in the proposed system is implemented by using Python language and the environment used is PyCharm Community Edition 2018.2.5.

4. In the training and testing, ICMetric security system is based on utilising SVM algorithm that is efficient and effective with low rate of error.

3.2 The Proposed ICMetric-Security System

Current some defensive mechanisms are not enough for preventing attacks in device, since they require security system as protection system to increase their security. ICMetric technology depends on measurable features, which have been achieved from the properties of a particular embedded system. The focus is on utilising MEMS sensors that are provided in the new system.

In this research, an intelligent wheelchair is required, where the bias readings extracted from sensors embedded in intelligent wheelchair are utilised in ICMetric security system generation. These bias readings are employed to create an ICMetric basis number that is used as identifications for device. The proposed system explained in more details in the following sections:

3.2.1 The General Architecture of Proposed System

The design and implementation process of the proposed system is composed from three main phases:

- **Phase_1:** extracting bias readings from MEMS sensors to generate ICMetric number.
- **Phase_2:** pre-processing of dataset extracted from ns-2 trace file in MATLAB.
- **Phase_3:** training and testing phase in Python.

The general architecture of the proposed security system is shown in figure 3.1:

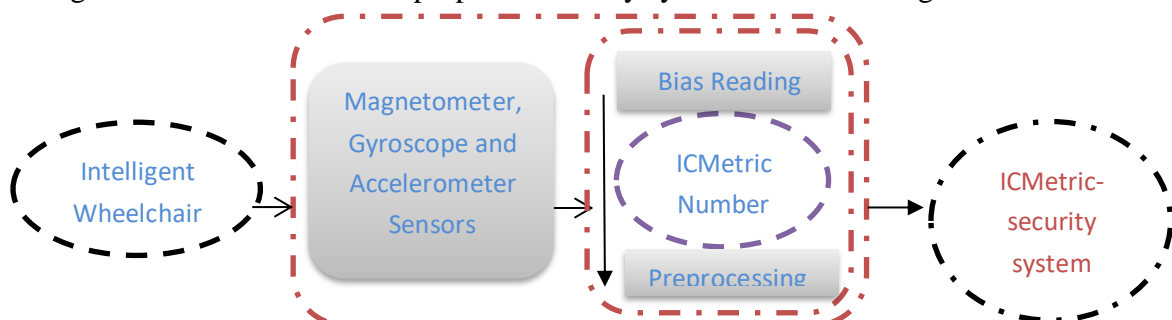


Figure 3.1: ICMetric-Security System Architectural

In this proposed system, bias readings are collected from MEMS sensors that are equipped in intelligent wheelchair. The bias readings are obtained from the sensors utilised in the generation of ICMetric numbers that were integrated to the dataset as identification for device.

3.2.2 Methodology

The proposed algorithm for ICMetric security system is summarised in the following steps:

The Implement ICMetric Algorithm
Input: Behaviour features that extracted from trace file of ns-2
Output: Normal or abnormal behaviour.
<p>Step 1: Establishing parameters for simulation.</p> <p>Step 2: Generating mobility and traffic model.</p> <p>Step 3: Extracting dataset from trace file.</p> <p>Step 4: Pre-processing of the extracting features.</p> <p>Step 5: Integrating of ICMetric number that generated by MEMS sensors.</p> <p>Step 6: Separating the extracted dataset into training set and testing set.</p> <p>Step 7: Training phase.</p> <p>Step 8: Testing phase.</p> <p>Step 9: Results</p>

The steps of the proposed algorithm are illustrated in the diagram 3.2.

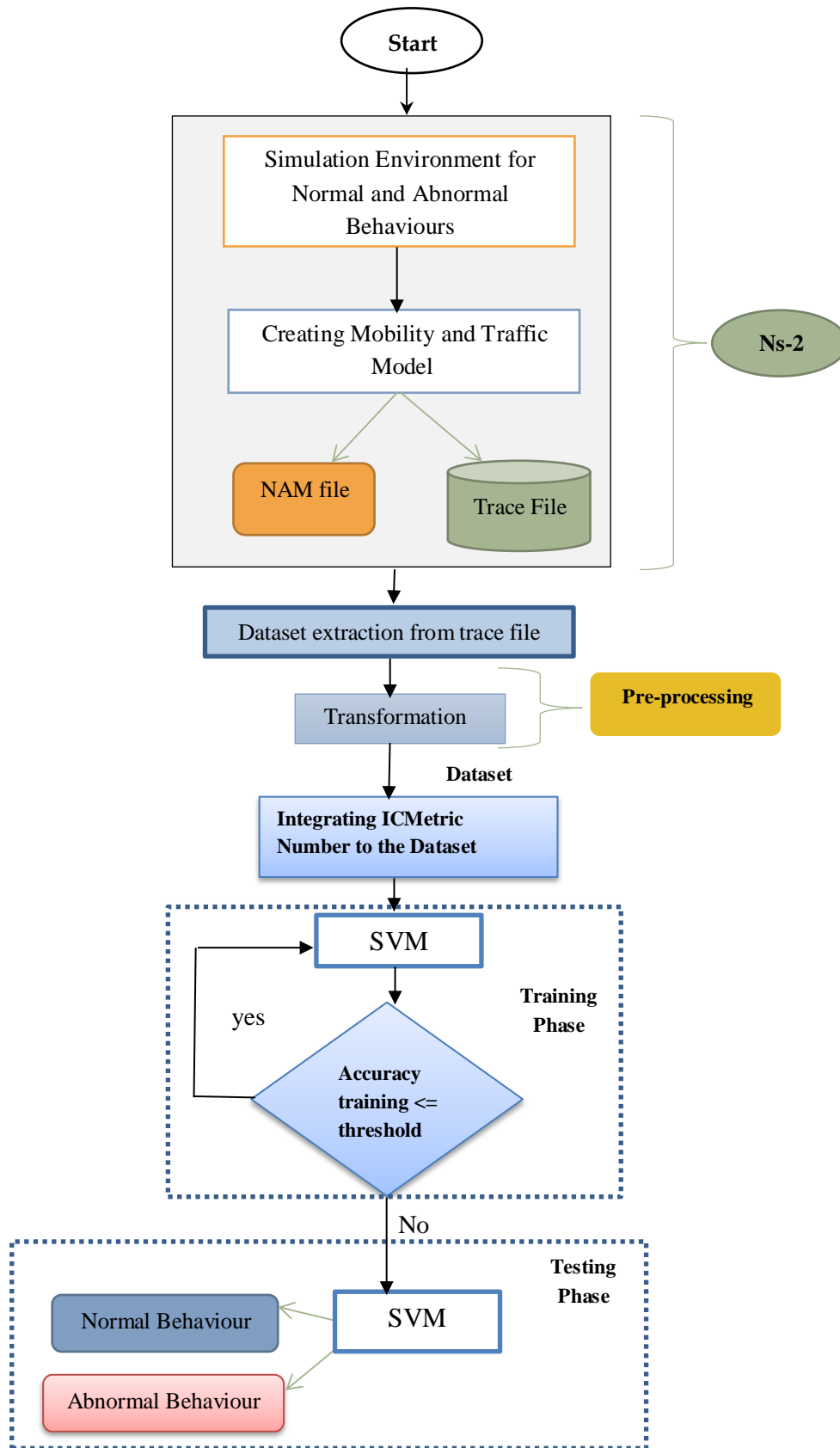


Figure 3.2: The Block Diagram of the Proposed Algorithm

In this sections, the steps of the proposed system are described with details:

3.2.2.1 Simulation Environment and Initial Parameters

In this thesis, ns-2 utilised for generation of communication between nodes as well as mobility system is established. Creating of normal/abnormal behaviour is one of evaluation process in the system. This behaviour is an important feature of assessing the efficiency of the proposed system. Therefore, The AODV routing protocol is utilised in this proposed system. AODV routing protocol files at the network layer of simulator are modified to establish dropping/ malicious behaviour. The proposed system is ought to have the ability to detect the malicious nodes from the rest of the nodes present in the network via identification of any abnormal behaviour.

Initial parameters are considered very essential of ns-2. In more details, these parameters play important role to determine performance of the simulation system. They determine the behaviour and performance in the ns-2. Table 3.1 presents initial parameters that utilised at the proposed system.

Table 3.1 Initial Parameters of ns-2

Parameter	Value
Routing Protocol	AODV
Number of nodes	13 Nodes
Simulation Time	200s
Topology	Mesh
Distance	1000 x 1000 (m)
Type of Traffic	Constant Bit Rate (CBR)
Packet Size	512
Queue Length	50 packets
Radio Propagation Model	Two Ray Ground
MAC protocol	IEEE 802.11
Interface queue type	Priority Queue
Network Interface type	Physical Wireless

3.2.2.2 Generating Mobility and Traffic Model

In this system, ns-2 is utilised to generate normal and abnormal behaviours. In this simulation, the output is composed of two files, which are Network Animator (NAM) file and trace file (text). Tool Command Language (TCL) is used to increase efficiency of the simulation in ns-2. In order to specify the path of nodes movement and behaviour of communication, TCL script file is used. In addition, the output of simulation requires two files are trace file and NAM file is specified by using TCL script file. NAM file of ns-2 is employed to present connection environment of intelligent wheelchair nodes shown in Figure 3.3.

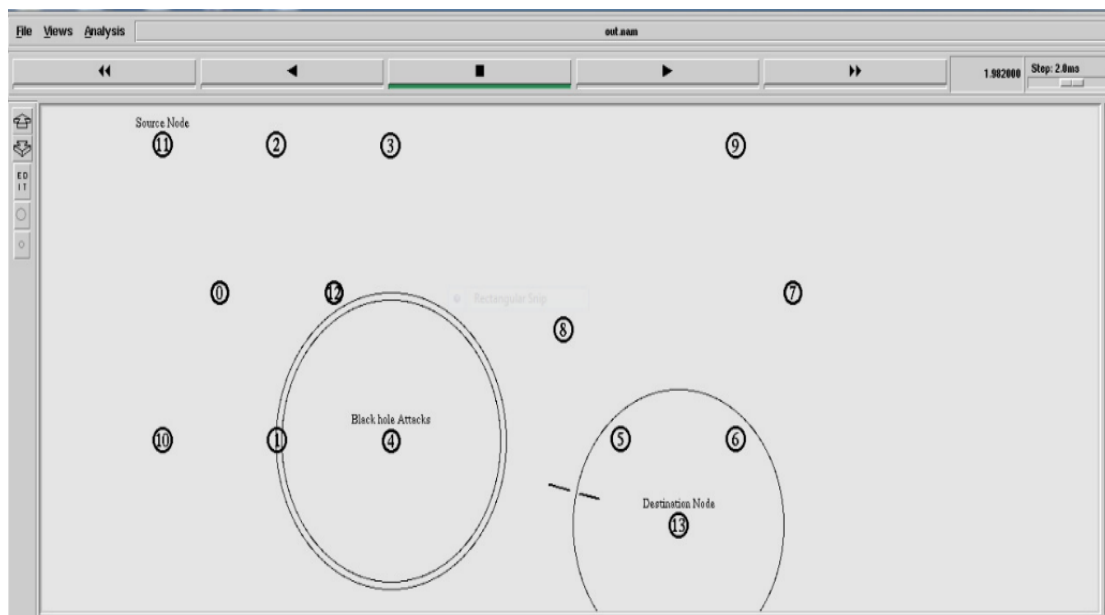


Figure 3.3: Screenshot of Simulation in the ns-2 NAM

3.2.2.3 Acquire of Dataset

The output of simulation generated by ns-2 is composed of two files, which are NAM and trace file (text) file. NAM file of ns-2 is utilised to presented connection environment of intelligent wheelchair nodes. Whereas trace file that generated from ns-2 is employed to extracted dataset. In this thesis, the generated dataset is employed at training and testing phases for the proposed system. In other words, a dataset is extracted from the trace file of simulator.

The information of dataset that extracted from the AODV trace file is categories into three parts of information, which are basic information, Internet Protocol (IP)

information and addition information [62]. The extracted features that describes all node events are shown in table 3.2.

Table 3.2 Significant Features of AODV from Trace File

Basic Information	AODV Information	IP Information
label, Number of Node, Period, level of Trace, MAC for Source Node and Destination Nodes, Size of Payload and Kind, ID for Packet, Delay Time, Internet Protocol for Packet and Ethernet	Count of Hop, Tagged for Packet, Internet Protocol for Destination as well as Sequence value and Internet Protocol for Source as well as Sequence value, Identification for Broadcast	TTL and value that determine the next Hop for node, Internet Protocol for Destination and Source

To increase knowledge about the extracted dataset, one sample record of connection is explained below:

```
"s 0.018997577 _5_ MAC --- 0 AODV 106 [0 ffffffff 5 800] ----- [5:255 -1:255 27 0] [0x2 4 1 [13 0] [11 4]] (REQUEST)"
```

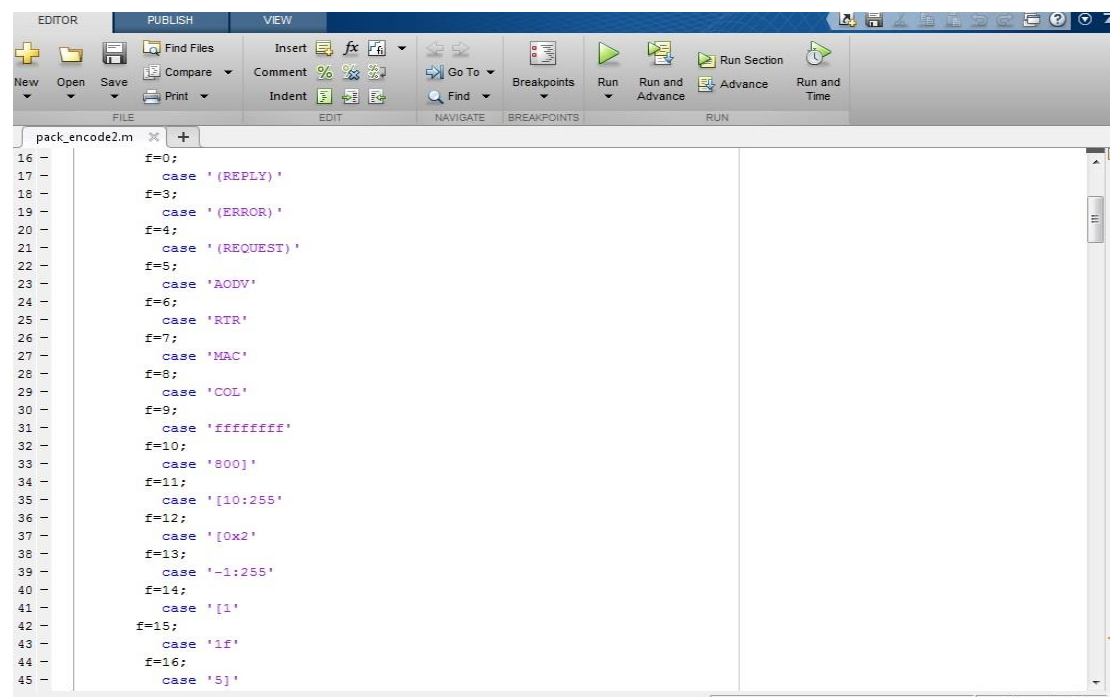
- Node “_5_” sends (i.e., “s”) at specific time “0.018997577” s.
- Level of trace is at “MAC” layer of network.
- The delay time is “0” at MAC over the underlying channel.
- ID packet is “5”, contains a payload type is “AODV”, and size is “106” bytes.
- The source MAC is “0” while destination MAC is “ffffffff”.
- IP packet over an Ethernet is “800”.
- IP source address is “5” and IP destination addresses is “1”.
- “255” is the port address for source and destination.
- “27” is total time to live while “0” is address of the next hop.
- “0x2” is ID that tagged with Request packet.

- “4” is number of hops while “1” is broadcast ID.
- “13” is destination IP address while “0” is sequence number.
- “11” is source IP address while “4” is sequence number.
- “REQUEST” confirms that this is packet is RREQ.

3.2.2.4 Pre-processing Phase of the Extracting Features

This phase is required to generate training and testing dataset from the extracted features of trace file. However, these features are composed from letters, symbols and numbers. SVM is just working with numeric values for this the pre-processing phase is trying to transfer these letters and symbols to numeric values.

This phase comprises transformation operations that utilised to convert all symbols and letters to numeric values. However, MATLAB program is just applied for one time to encoding all of them directly as shown in Figure 3.5.



```

EDITOR PUBLISH VIEW
New Open Save Find Files Compare Print Insert Comment Indent Go To Find Breakpoints Run Run and Advance Run Section Advance Run and Time
pack_encode2.m
16 f=0;
17 case '(REPLY)'
18 f=3;
19 case '(ERROR)'
20 f=4;
21 case '(REQUEST)'
22 f=5;
23 case 'AODV'
24 f=6;
25 case 'RTR'
26 f=7;
27 case 'MAC'
28 f=8;
29 case 'COL'
30 f=9;
31 case 'fffffff'
32 f=10;
33 case '000]'
34 f=11;
35 case '[10:255'
36 f=12;
37 case '[0x2'
38 f=13;
39 case '-1:255'
40 f=14;
41 case '[1'
42 f=15;
43 case '1f'
44 f=16;
45 case '5]'

```

Figure 3.4: Code of Symbols and Letters Transformation in MATLAB

The preprocessing process is considered important because the feature vector fed to the input layer of SVM and has to be numerical.

3.2.2.5 Extraction of Features from Trace File

In the trace file created by ns-2, analysis of nodes' behaviour is carried out to determine whether the behaviour is normal or Black hole. However, extraction process of observation from the trace file of ns-2 holds great emphasis for the proposed system as the majority of the work is dependent on these features. In this case, MATLAB is utilised to extract significant features from trace file as shown in Figure 3.4.

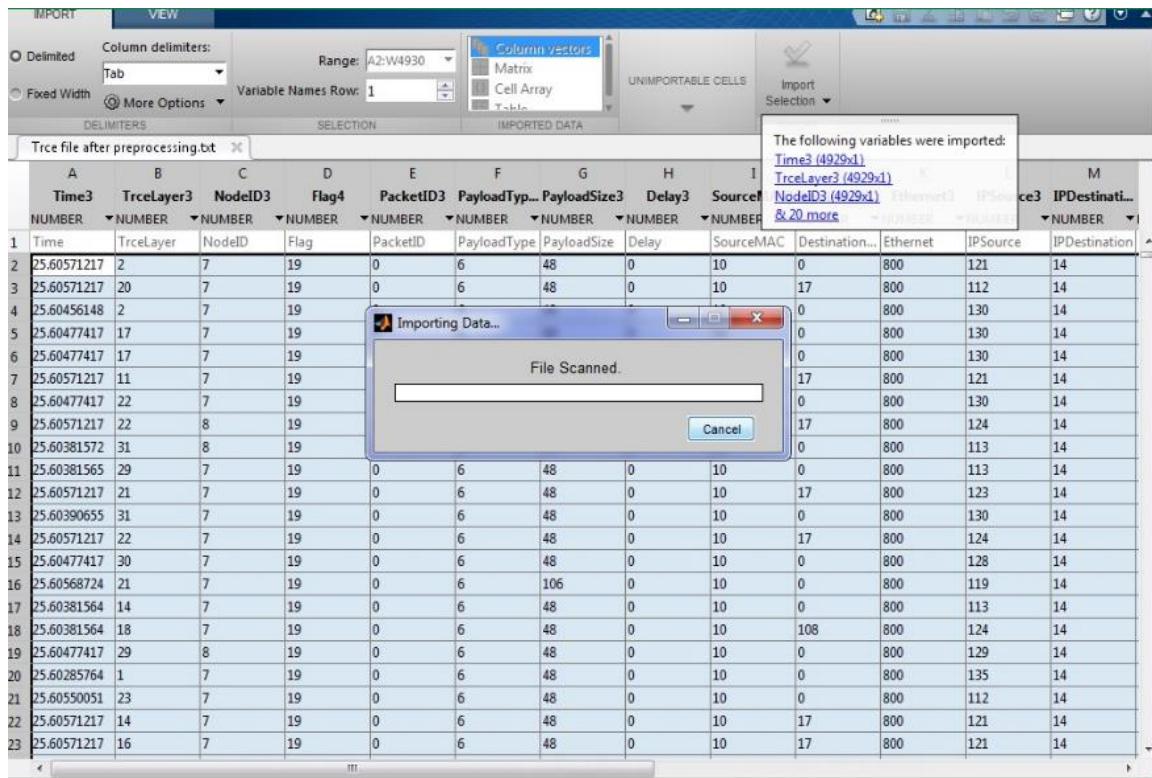


Figure 3.5: Import Data of Trace File into MATLAB

3.2.2.6 Integration of ICMetric Number into Dataset

In this research, ICMetric number used to apply identification and improve security of embedded device. It is generated from bias readings extracted from MEMS sensors by simple mathematical model. The generated ICMetric number will be inserted to the dataset extracted from the trace file generated by ns-2. In this system, two schemes are proposed to generate ICMetric number, which are:

- 1) The first scheme based on bias readings extracted from gyroscope and magnetometer sensors. In this scheme, hybrid ICMetric numbers are generated by lightweight equations and can be integrated to the dataset.

2) The second scheme based on bias readings extracted from gyroscope, magnetometer and accelerometer sensors. In this scheme, triple ICMetric numbers are generated and can be inserted to the dataset.

Below some statistical analysis required for ICMetric number generation utilising to apply identification of device. The generating process needs a probability mass (x) function to determine the precise value from the bias reading because these readings are a discrete random variable.

$$p(x) = \frac{1}{\sigma\sqrt{2n}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \quad (3.1)$$

If \bar{X} is represent mean, x is represent particular sample reading from accelerometer, magnetometer and gyroscope and n is total number of reading then [14].

$$\bar{X} = \frac{1}{n} \sum_{i=1}^n x_i \quad (3.2)$$

In order to complete ICMetric generation process, σ^2 is calculated as explained below. Where σ^2 is the standard deviation :

$$\sigma^2 = \sum_{i=1}^n p(x_i)(x_i - \bar{X})^2 \quad (3.3)$$

Furthermore, other statistical and mathematical function are utilised to analyse the generated reading. For example variance (s^2) is calculated as explained in the following equation:

$$s^2 = \frac{1}{n-1} \sum_{i=1}^n (x - \bar{X})^2 \quad (3.4)$$

Where s^2 is a measure of dispersion for extracting readings.

The skewness distribution (S) is a measure of asymmetry of the probability distribution of bias readings. It can be negative or positive:

$$S = \frac{3(\bar{X}-m)}{s^2} \quad (3.5)$$

To prove the uniqueness of the bias generated from accelerometer, magnetometer and gyroscope sensors, 95% confidence interval has been used. If \bar{X} is the mean, σ is the standard deviation and n is the total number of observations then the confidence interval CI is given in the equation 3.6. The numeric value $v = 1.96$ represents the confidence coefficient for the 95% confidence interval [23].

$$CI = \bar{X} \pm v \frac{\sigma}{\sqrt{n}} \quad (3.6)$$

In addition, other statistical and mathematical functions are utilised to analyse the generated reading, such as Inter Quartile Range (IQR) that represents difference between the third and the first quartile in offset data. IQR can be calculated according to the equation 3.7, where $Q3$ represent upper quartile and $Q1$ represent lower quartile.

$$IQR = Q3 - Q1 \quad (3.7)$$

3.2.2.7 Training and Testing Phases

After generation of ICMetric number and integrating to the dataset, training and testing the dataset is the next phase in the proposed system. In the training phase, SVM is employed to improve the detection rate and reduce the false alarm rate of the proposed security system. SVM is efficient, effective with low error rate in improving detection rate. The data set with 1000 records used in this proposed system to describes the behaviour and whether it is normal or abnormal. The data set is divided into three subsets, which are the training set (60%), validation set (20%) and testing set (20%).

To determine accuracy rate of detection and four types of alarms, testing phase is utilised. There are some metrics for measuring the efficiency, such as throughput, detection rate, the number of false alarms, End-to-End delay, PDR. Training/testing phase carried out by exploiting Python language and PyCharm environment.

3.3 ICMetric Technology for Intelligent Wheelchairs

While many security techniques are now developed, these cannot necessarily defend against unauthorised activity when the security and safety cannot be absolutely assured. The use of ICMetric technology to provide identification represents a new concept of controlling access to devices and is explicitly aimed at providing protection against attacks and improving security.

The ICMetric security system proposed in this research uses bias readings that have been extracted from sensor devices. These readings exploited to create ICMetric basis numbers that were working as identification for device. Currently, many research demonstrated that the use of sensory data is possible to create identification of the device.

In this research, a suitable features are extracted from the sensors to describe behaviour of intelligent wheelchair, such as gyroscope, magnetometer and

accelerometers. The offset is utilised in the sensor measurement to propose a security system that apply an ICMetric basis number using the sensor bias readings.

In this research, ICMetric technology is integrated into an intelligent wheelchair to ensure effective usage of the intelligent wheelchair and the need to protect the safety of each wheelchair. The advantages are to provide identification of intelligent wheelchair to confirm the user's right to access the system and information and defend against identity theft and fraud. For achieving these aims, ICMetrics represents a new method for generating unique identifiers for embedded devices and improve security by reducing fraudulent activity.

ICMetric technology can improve secure communication between devices and reducing fraudulent activity, detection of unauthorised access to the systems and devices connected with the wheelchair, implicit detection of tampering of the software or hardware associated with the wheelchair and prevention of the fraudulent cloning or imitation of the electronics associated with the wheelchair.

The challenge in the project of the ICMetric basis number applied for generating appropriate features and identifying the characteristics of sensor device's. The appropriate features must consider the sensor devices characteristics, the process of the extraction and the analysis should not significantly affect performance of the device.

3.4 Performance Metrics

ICMetric security system have been evaluated using a number of ways based on trace file evaluation. The ICMetric-security system can be generally evaluated from two views [63]:

1. Accuracy: This portion also termed effectiveness classification characterises the ability of the system to separate between intrusive and non-intrusive activities. The accuracy of the detection should be calculated as follows:

$$Accuracy = \frac{\text{Number of correctly classified patterns}}{\text{Total number of patterns}} \quad (3.8)$$

2. Efficiency: This portion deals with the resources required to be allocated to the system including CPU cycles and main memory.

System features can be evaluated in the terms of performance, correctness and usability. Researchers used metrics to assess the performance of the system. Many performance measures are used to evaluate the system that is based on the dataset extracted from the trace file created by ns-2.

The identification rate and four alarms are utilised as a performance metric to test the proposed system. To measure and evaluate the proposed system performance, four types of alarms are needed to calculate: True Positive (TP), False Positive (FP), True Negative (TN) and False Negative (FN). The measures will be calculated as follows [23]: Let

TP = normal connection recored classified as normal

TN = attack connection record classified as attack

FP = normal connection record classified as attack

FN = attack connection rcored as normal

then:

$$TP_{Rate(sensitivity)} = \frac{TP}{TP + FN} \quad (3.9)$$

$$TN_{Rate(specificity)} = \frac{TN}{TN + FP} \quad (3.10)$$

$$FN_{Rate(1-sensitivity)} = \frac{FN}{FN + TP} \quad (3.11)$$

$$FP_{Rate(1-specificity)} = \frac{FP}{FP + TN} \quad (3.12)$$

In addition, some extra metrics are utilised to evaluate system performance, such as packet delivery rate (PDR), throughput and end – to –end delay [23].

- Packet Delivery Ratio (PDR): The ratio between the number of packets sent from the origin and the proportion of packets received at the destination.

$$PDR = \sum N_r / \sum N_s \quad (3.13)$$

Where, N_r = Number of the packet received and N_s = Number of the packet sent.

- Throughput: The total number of packets that are transferred in the system. Throughput of a system can be presented as shown in the following equation.

$$\text{Rate of Throughput(kbps)} = N_r * S / ST \quad (3.14)$$

Where, N_r = Number of packet received and S = packet size and ST = Simulation Time .

- Average End-to-End Delay: The average time for packets reaching from the origin to the destination. average end-to-end delay explained in the following equation:

$$\text{Rate End - to - End Delay (ms)} = \left(\frac{\sum \text{endtime} - \text{starttime}}{\sum N} \right) \quad (3.15)$$

Where N represent a number of connections.

CHAPTER FOUR

Results and Discussion

CHAPTER FOUR

Results and Discussion

4.1 Introduction

In this chapter, the proposed system role is explained in developing and enhancing for current security systems that employed for applied identification. The proposed system is tested with the features extracted from the trace file created by the ns-2 to evaluate the system performance. The difference between bias readings that extracted from sensors and some statistical analysis are presented in this chapter. Bias reading can be utilised for generating ICMetric number that can be used for device identification. In this chapter performance metrics is calculated, which are error rate, confused matrix and accuracy rate for the two methods presented by the proposed system.

4.2 Experimental Results of MEMS Bias Establishment

Various number of bias reading is obtained from myAHRS_plus sensor to generate ICMetric number. The system needs to determine the optimal number of readings used in identification processes to control the stability of the statistical processes of the ICMetric generation.

The number of readings influences the stability of the ICMetric basis number. A large number of readings ensures that sufficient population representation is used in the statistical analysis. If the number of readings is too small, then the resulting statistical analysis will be flawed as this does not fully represent the full population. To determine the optimal number of readings, population mean result is calculated and compared with the mean value calculated for a smaller subset of readings. In order to realise a mean convergence point, the optimal number of readings is 750. In this experiment, 1000 bias readings are utilised to achieve a more precise system as presented in figure 4.

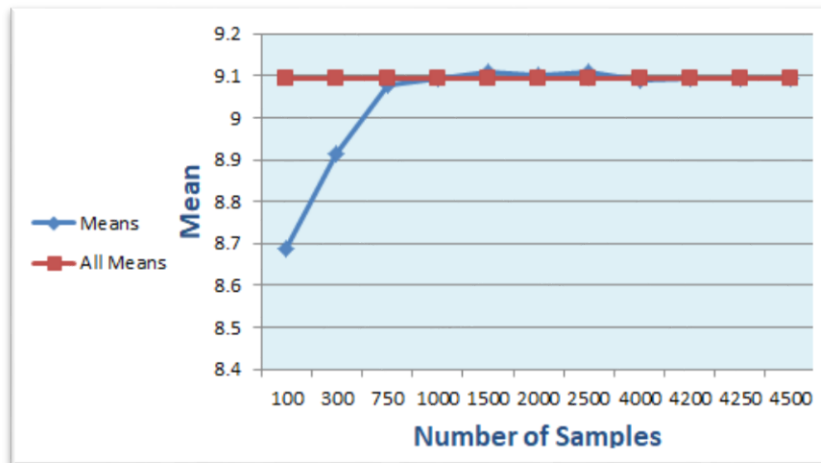
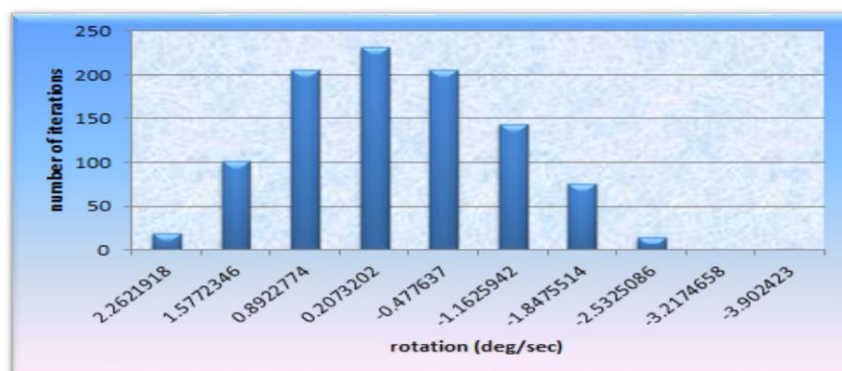


Figure 4.1: Population Mean and Sample Mean Relationship

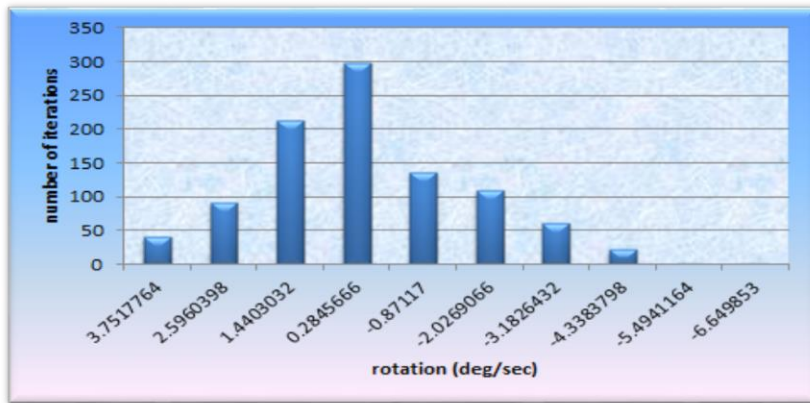
The study on MEMS sensors exhibits that the bias in a sensor can be utilised to create a device identification. Experiments prove that each sensor has a bias, which is unique and can be recreated if the sensor is exposed to the same stimulus. The difference between bias readings that is extracted from sensors is illustrated in the following sections. Bias readings can be utilised to generate ICMetric that can be used for device identification.

4.2.1 Gyroscope Bias Analysis

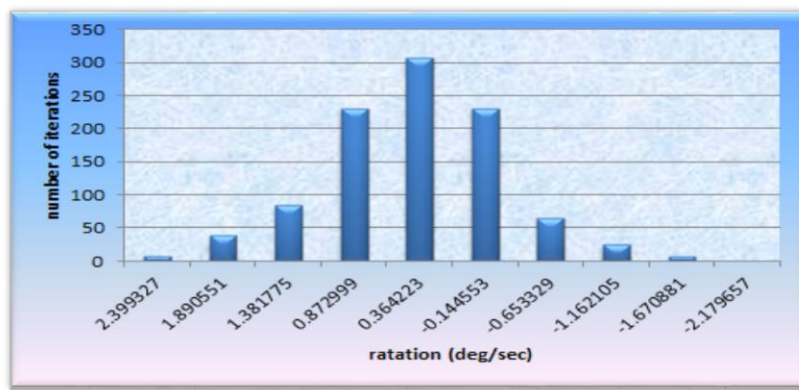
Unimodal distribution for three gyroscope sensors presented in figures 4.2, 4.3 and 4.4. Figure 4.2 shows bias readings that generated from the first gyroscope sensor, where each sensor owns a bias, which is unique to the sensor. The readings extracted from gyroscope sensor can be employed for providing an ICMetric basis number.



(a)



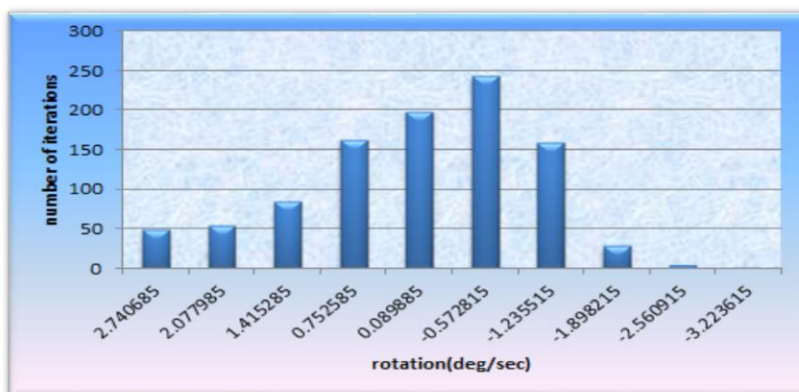
(b)



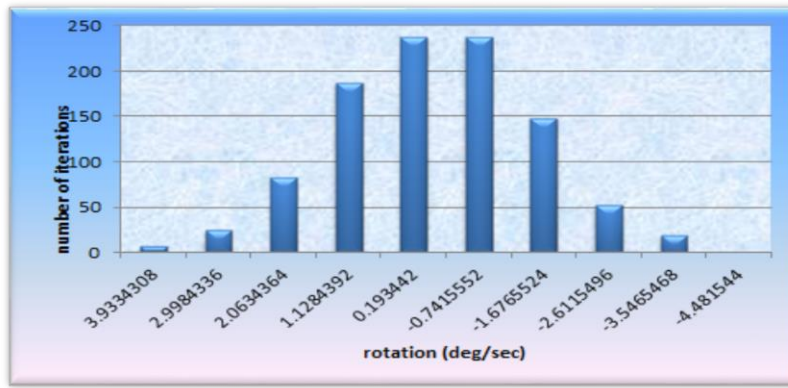
(c)

Figure 4.2: Readings of the First Gyroscope Sensor, (a) x-axis graph (b) y-axis graph (c) z-axis graph

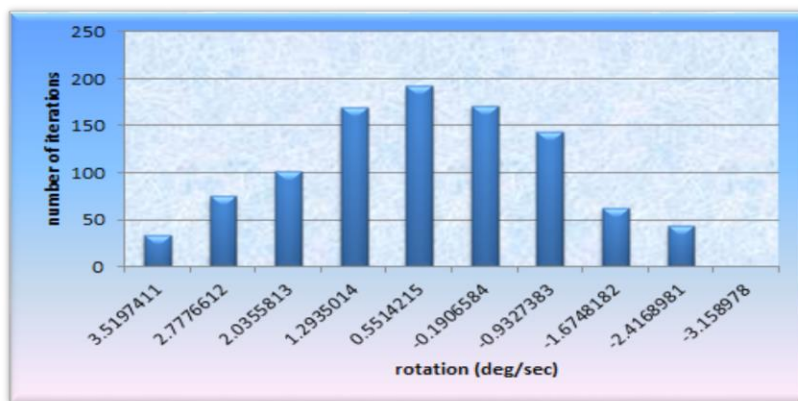
The graphs (a), (b) and (c) presented in figure 4.3 show bias readings that generated from the second gyroscope sensor.



(a)



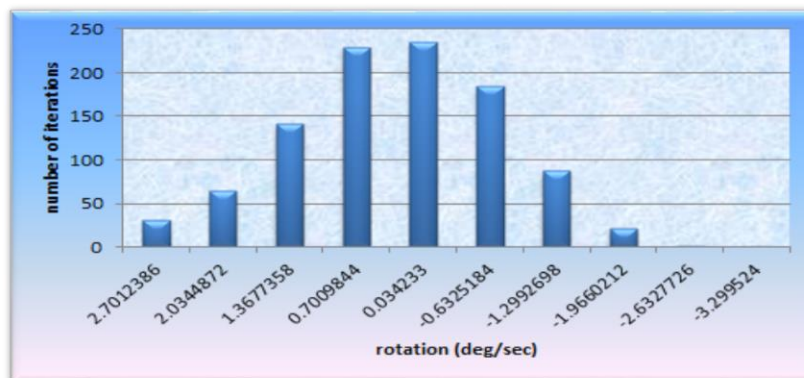
(b)



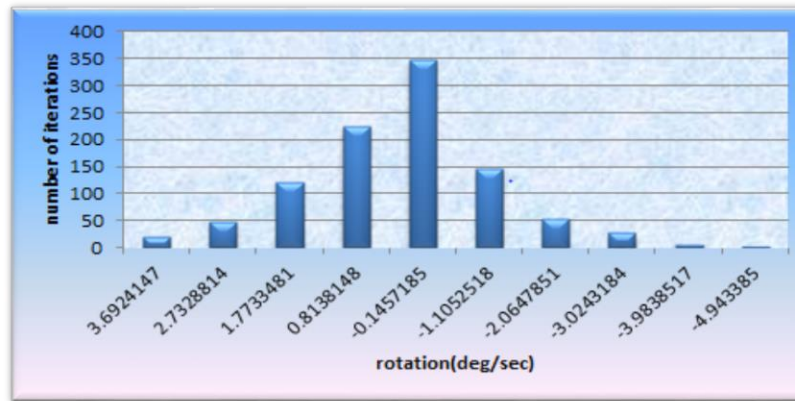
(c)

Figure 4.3: Readings of the Second Gyroscope Sensor, (a) x-axis graph (b) y-axis graph (c) z-axis graph

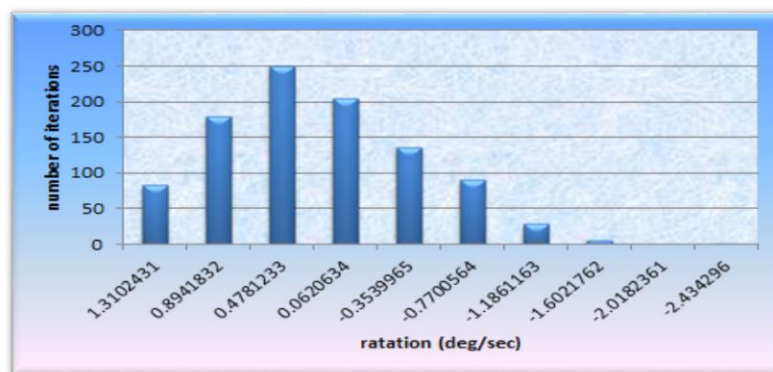
Figure 4.4 presents a graphs (a), (b) and (c) that show bias readings that generated from the third gyroscope sensor.



(a)



(b)



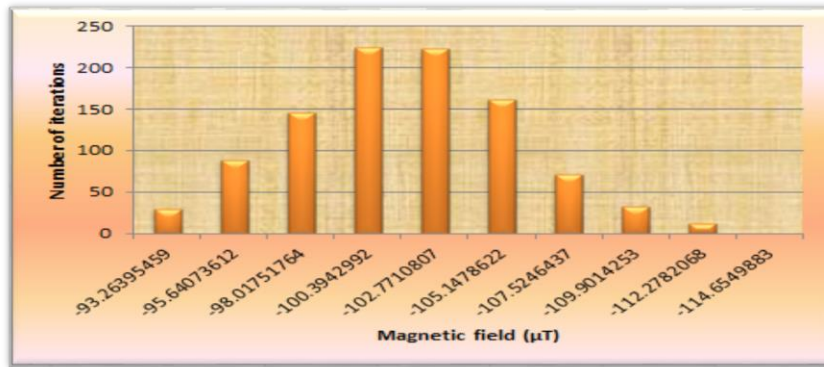
(c)

Figure 4.4: Readings of the Third Gyroscope Sensor, (a) x-axis graph (b) y-axis graph (c) z-axis graph

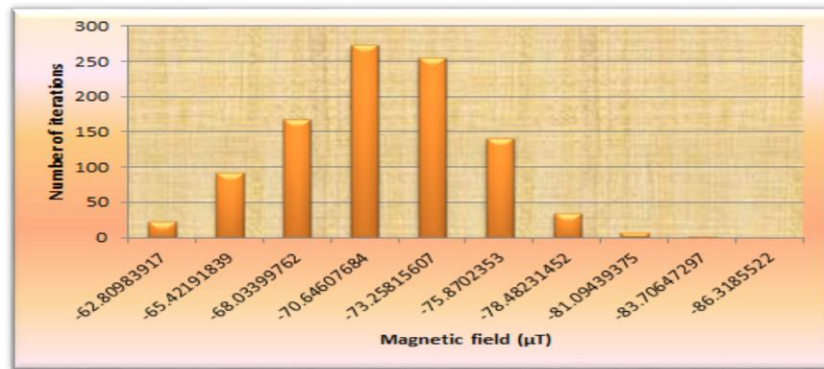
Figures 4.2, 4.3 and 4.4 present the histograms of calibrated gyroscope achieved from three identical sensors. Three gyroscope sensors were exploited in this proposed security system to create ICMetric basis number utilised to provide identification and improve security. The graphs show that each axis presents a various bias and that there is no similarity between the sensors and no correlation between any axes.

4.2.2 Magnetometer Bias Analysis

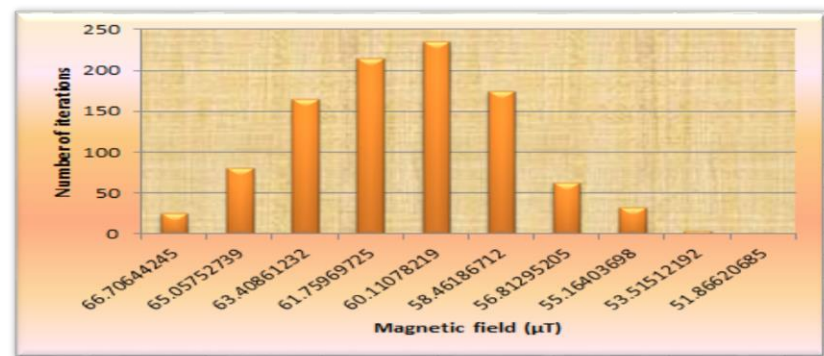
In this section, figures 4.5, 4.6 and 4.7 are presented to show normal distribution for three magnetometer sensors. Figure 4.5 shows that each sensor owns a bias, which is unique to the sensor. The readings extracted from magnetometer sensors can be employed for the providing of an ICMetric basis number. Figure 4.5 presents (a), (b) and (c) graphs that show bias readings generated from the first magnetometer sensor.



(a)



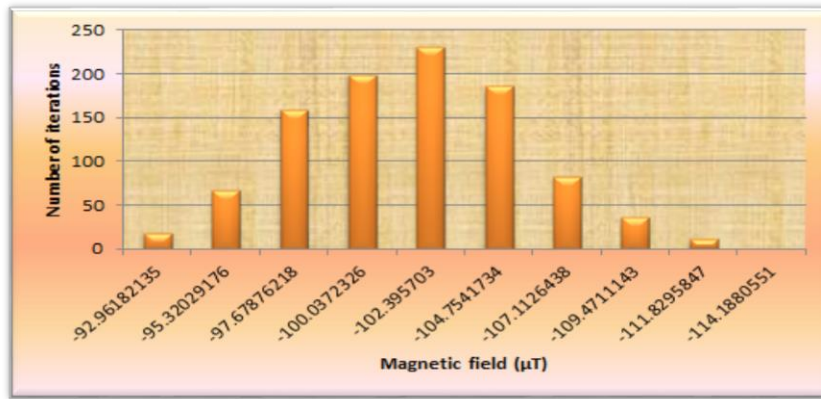
(b)



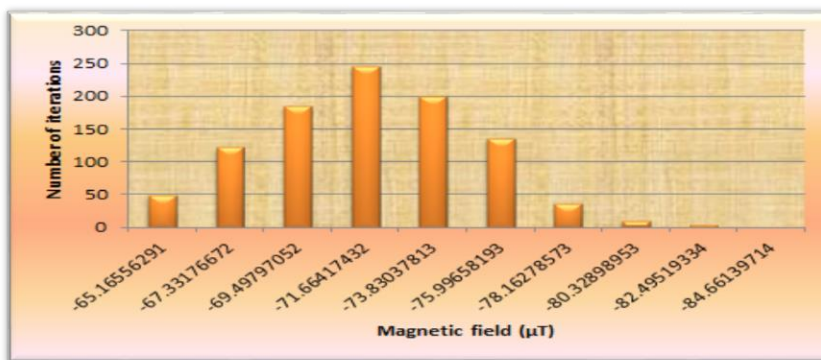
(c)

Figure 4.5: Readings of the First Magnetometer Sensor, (a) x-axis graph (b) y-axis graph (c) z-axis graph

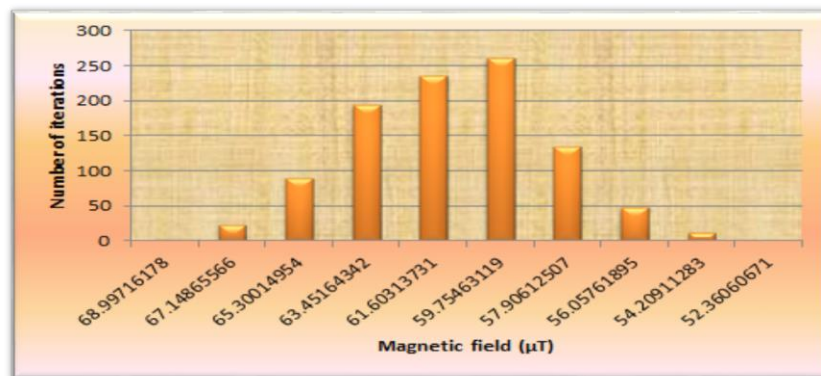
The graphs (a), (b) and (c) in figure 4.6 show bias readings that generated from the second magnetometer sensor.



(a)



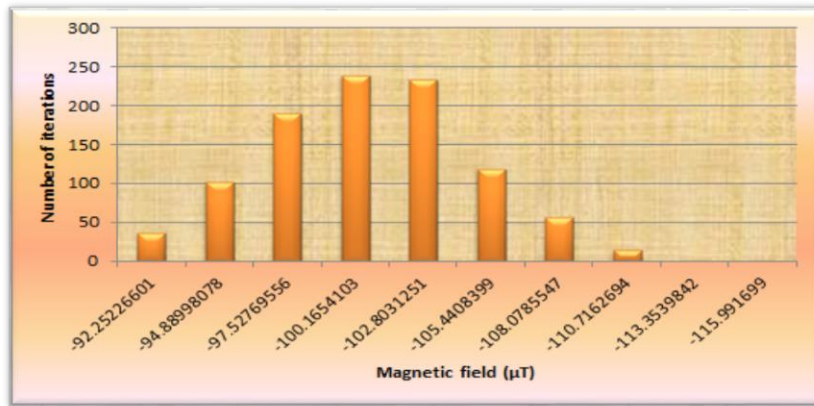
(b)



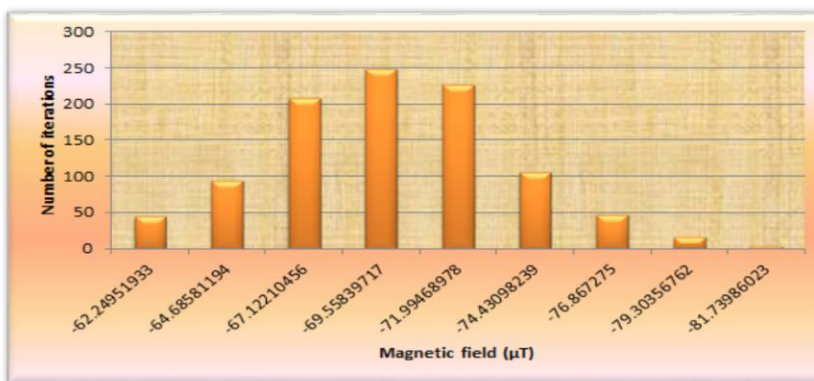
(c)

Figure 4.6: Readings of the second magnetometer sensor, (a) x-axis graph (b) y-axis graph (c) z-axis graph

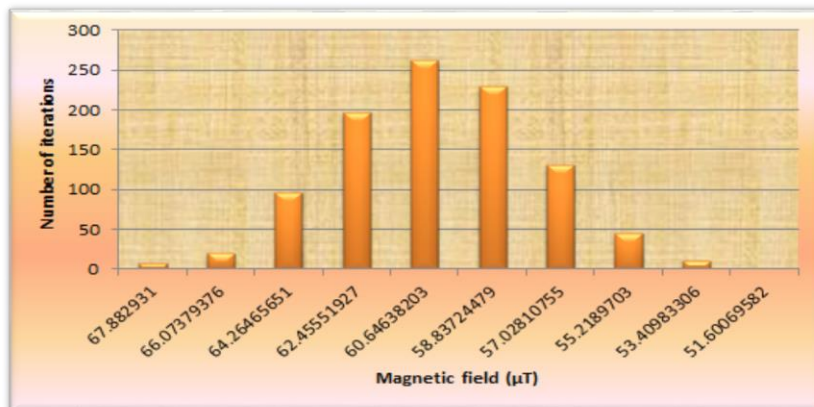
Figure 4.7 provides (a), (b) and (c) graphs that show bias readings that generated from the third magnetometer sensor.



(a)



(b)



(c)

Figure 4.7: Readings of the Third Magnetometer Sensor, (a) x-axis graph (b) y-axis graph (c) z-axis graph

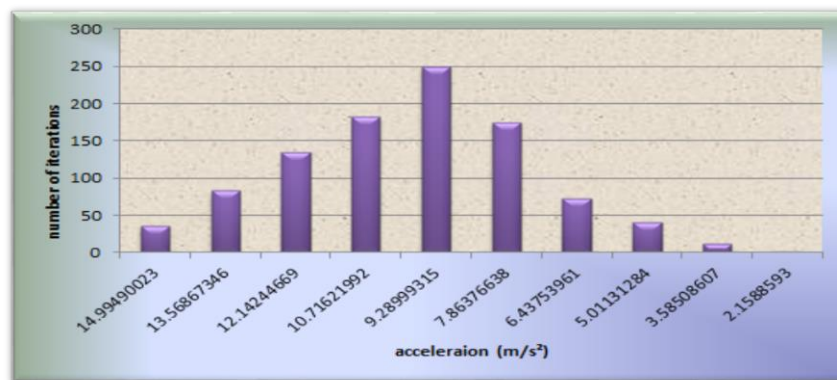
Figures 4.5, 4.6 and 4.7 present the calibrated magnetometer histograms achieved from three identical sensors. In proposed security system three magnetometer sensors

were exploited to create ICMetric basis number utilised for providing identification to protect the system from possible attacks. From the graphs it is obvious that each axis presents a various bias and that there is neither a likeness between the sensors nor an interconnection between any axes.

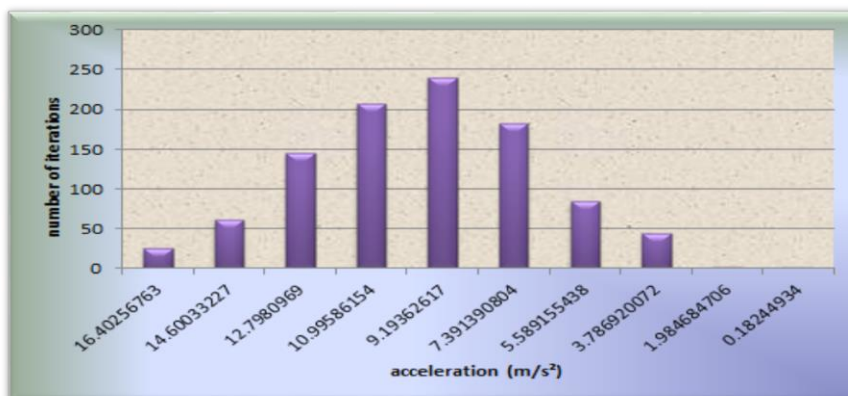
4.2.3 Accelerometer Bias Analysis

Three accelerometer sensors provide normal distribution as explained in figures 4.8, 4.9 and 4.10. Figure 4.8 shows that each sensor owns a bias, which is unique to the sensor. The readings extracted from accelerometer sensors can be used for the establishment of an ICMetrics basis number.

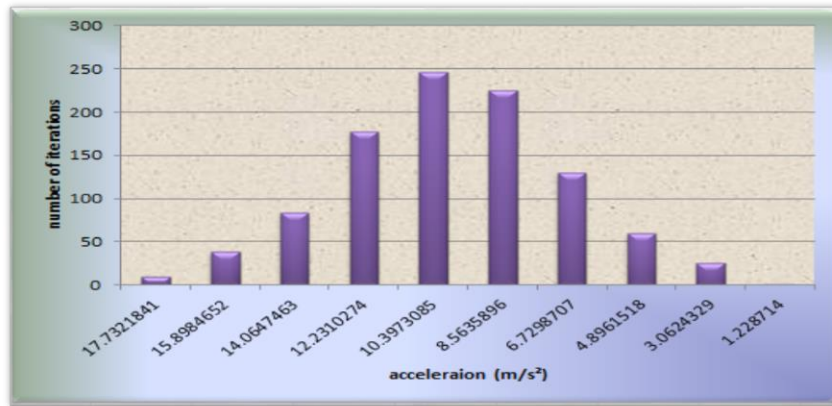
Figure 4.8 presents (a), (b) and (c) graphs that illustrate bias readings that generated from the first accelerometer sensor.



(a)



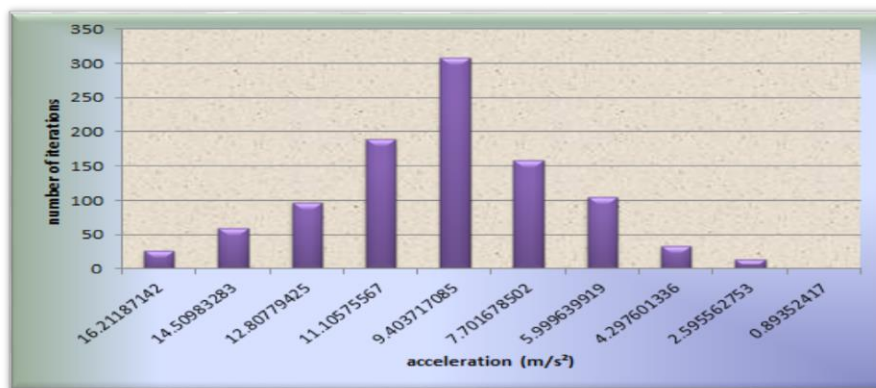
(b)



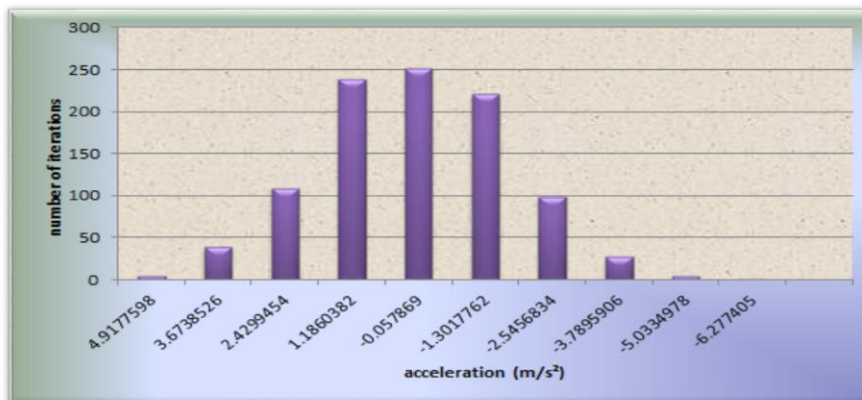
(c)

Figure 4.8 Readings of the First Accelerometer Sensor, (a) x-axis graph (b) y-axis graph (c) z-axis graph

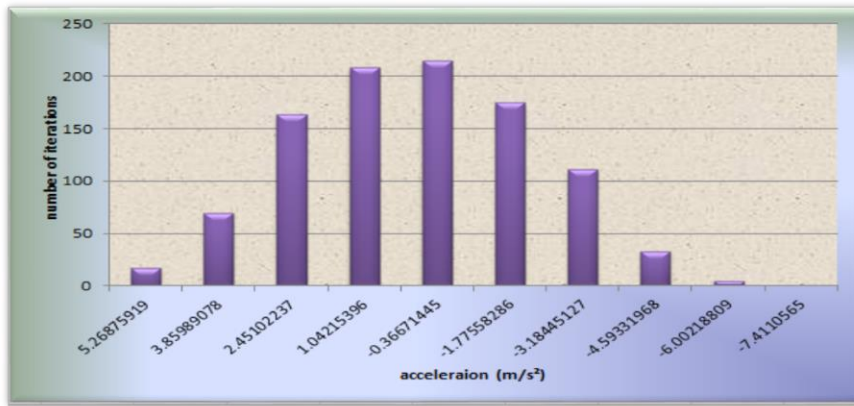
Figure 4.9 presents (a), (b) and (c) graphs that show bias readings that generated from the second accelerometer sensor.



(a)



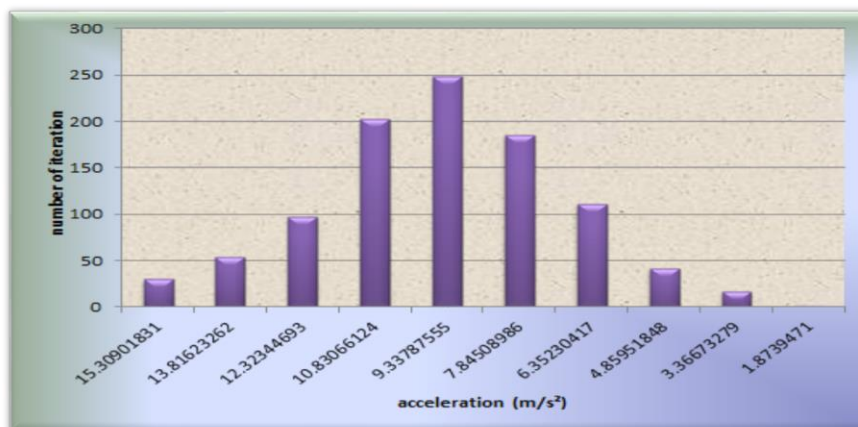
(b)



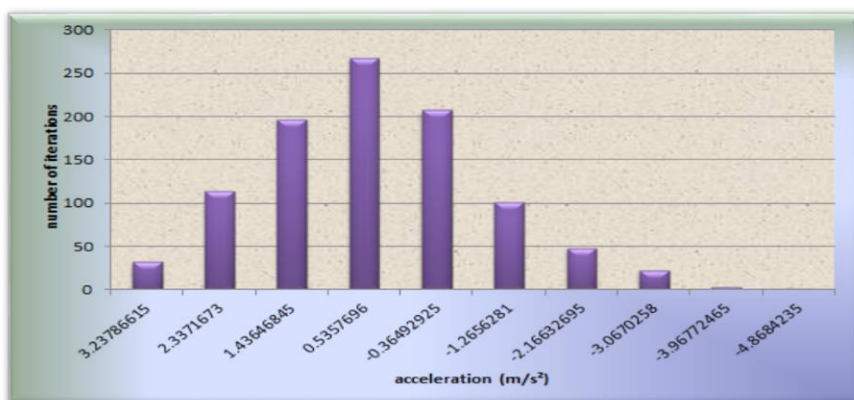
(c)

Figure 4.9 Readings of the Second Accelerometer Sensor, (a) x-axis graph (b) y-axis graph (c) z-axis graph

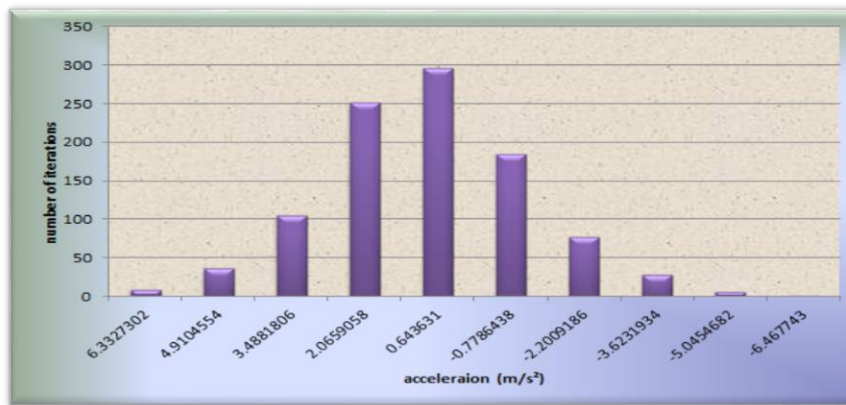
Figure 4.10 presents (a), (b) and (c) graphs that show bias readings that generated from the third accelerometer sensor.



(a)



(b)



(c)

Figure 4.10 Readings of the Third Accelerometer Sensor, (a) x-axis graph (b) y-axis graph (c) z-axis graph

The bias differs for each specific axis and there is no correlation between three axes or sensors. Figures 4.8, 4.9 and 4.10 present a graphs of three different accelerometer sensors readings. The graphs show that each axis is unique and presents a unimodal distribution.

4.3 Statistical Analysis Results for ICMetrics

The processes of ICMetric number generation require simple mathematical equations and a statistical analysis of the values of the features because this number not stored and can be created when needed.

To show that there is a significant difference between the axis of a sensor. The most important indicator of statistical significance is the p-value. The p-value ranges between zero and one where p-values equal 0 this indicate a statistically significant difference between the set of readings. If the p-value equals one, then this indicates that statistically there is no significant difference between the set of readings. More, according to the equations 3.2, 3.3, 3.4, 3.5, 3.6 and 3.7 mentioned in the previous, some statistical and mathematical functions are applied in tables 4.1, 4.2 and 4.3.

Table 4.1: Statistical Analysis of the First Triple Axial Gyroscope Sensor

		Gyroscope_1		
		x-axis	y-axis	z-axis
Statistical functions	Confidence interval (<i>CI</i>)	(-0.2798,-0.4109)	(-0.1644,-0.4057)	(0.1943,0.10866)
	Standard deviation (σ^2)	1.057460501	1.946444674	0.691476508
	Inter quartile range (<i>IQR</i>)	1.54140325	2.27847475	0.89227225
	Mean (\bar{X})	0.34538804	0.285080131	0.151523562
	Skewness (<i>S</i>)	0.109740322	0.072086021	0.161009518
	Variance (s^2)	1.11822271	3.788646869	0.478139761
	p-value	0.0	0.0	0.0

Table 4.2: Statistical Analysis of the Second Triple Axial Gyroscope Sensor

		Gyroscope_2		
		x-axis	y-axis	z-axis
Statistical functions	Confidence interval (<i>CI</i>)	(-167.0497,167.199)	(-530.354,530.5348)	(0.228,0.0459)
	Standard deviation (σ^2)	1.211160058	1.458852046	1.473156
	Inter quartile range (<i>IQR</i>)	1.61198525	1.94805825	2.094709
	Mean (\bar{X})	-167.12482	0.530444435	0.137225
	Skewness (<i>S</i>)	0.641566849	0.215075162	0.115859
	Variance (s^2)	1.466908685	2.128249291	2.170189
	p-value	0.0	0.0	0.0

Table 4.3: Statistical Analysis of the Third Triple Axial Gyroscope Sensor

		Gyroscope_3		
		x-axis	y-axis	z-axis
Statistical functions	Confidence interval (<i>CI</i>)	(25.9757,26.1058)	(0.17611,0.35196)	(64.08581,64.00352)
	Standard deviation (σ^2)	1.049579	1.418639	0.663885
	Inter quartile range (<i>IQR</i>)	1.439749	1.569408	0.90712
	Mean (\bar{X})	0.02604	0.26403	0.064045
	Skewness (<i>S</i>)	0.164015	0.076927	0.2587
	Variance (s^2)	1.101617	2.012537	0.440743
	p-value	0.0	0.0	0.0

Some statistical and mathematical function are applied in tables 4.4, 4.5 and 4.6 that were earlier used to determine the metrics for the graphs in the above figures 4.4, 4.5 and 4.6.

Table 4.4: Statistical Analysis of the First Triple Axial Magnetometer Sensor

		Magnetometer_1		
		x-axis	y-axis	z-axis
Statistica 1 functions	Confidence interval (<i>CI</i>)	(-102.4991, -103.005)	(-72.329, -72.785)	(60.236,59.906)
	Standard deviation (σ^2)	4.086745963	3.684409234	2.666794659
	Inter quartile range (<i>IQR</i>)	5.44068725	4.918820763	3.69197668
	Mean (\bar{X})	-102.7524674	-72.55744499	60.07166967
	Skewness (<i>S</i>)	0.024220124	0.126656585	0.016271328
	Variance (s^2)	16.70149257	13.57487141	7.111793754
	p-value	0	0	0

Table 4.5: Statistical Analysis of the Second Triple Axial Magnetometer Sensor

		Magnetometer_2		
		x-axis	y-axis	z-axis
Statistical functions	Confidence interval (<i>CI</i>)	(-102.521, -103.018)	(-72.573, -73.002)	(60.374,60.040)
	Standard deviation (σ^2)	4.015104407	3.466054182	2.690850552
	Inter quartile range (<i>IQR</i>)	5.706198312	4.94399854	3.68968779
	Mean (\bar{X})	-102.7699637	-72.78785363	60.20756554
	Skewness (<i>S</i>)	0.065459667	0.016225336	0.04191755
	Variance (s^2)	16.1210634	12.01353159	7.240676692
	p-value	0	0	0

Table 4.6: Statistical Analysis of the Third Triple Axial Magnetometer Sensor

		Magnetometer_3		
		x-axis	y-axis	z-axis
Statistical functions	Confidence interval (<i>CI</i>)	(-101.6587, -102.1710)	(-70.774, -71.244)	(59.5824,59.2527)
	Standard deviation (σ^2)	4.132523997	3.788275436	2.659678513
	Inter quartile range (<i>IQR</i>)	5.62150946	4.96230964	3.36008789
	Mean (\bar{X})	-101.9149358	-71.00961638	59.41761528
	Skewness (<i>S</i>)	0.055419203	0.108231939	0.035697616
	Variance (s^2)	17.07775458	14.35103078	7.073889791
	p-value	0	0	0

The tables 4.4, 4.5 and 4.6 show statistical analysis of the readings acquired from three similar magnetometers.

Some statistical and mathematical function are applied in tables (4.7), (4.8) and (4.9) that were earlier used to determine the metrics for the graphs in the above figures 4.7, 4.8 and 4.9.

Table 4.7: Statistical Analysis of the First Triple Accelerometer Sensor Axes

		Accelerometer-1		
		x-axis	y-axis	z-axis
Statistical functions	Confidence interval (CI)	(9.3159,9.0025)	(0.0907, -0.0867)	(-0.5547,0.7360)
	Standard deviation (σ^2)	2.527947461	1.431675069	1.461817352
	Inter quartile range (IQR)	3.377323	1.821392055	2.195487988
	Mean (\bar{X})	9.159219616	0.002032883	0.645400818
	Skewness (S)	0.100232538	0.211393438	0.457515397
	Variance (s^2)	6.390518366	2.049693504	2.136909971
	p-value	0	0	0

Table 4.8: Statistical Analysis of the Second Triple Accelerometer Sensor Axes

		Accelerometer-2		
		x-axis	y-axis	z-axis
Statistica l functions	Confidence interval (CI)	(8.177568,7.8487)	(0.497395,0.785187)	(1.2297, -2.5300)
	Standard deviation (σ^2)	2.652895942	2.321628014	2.831670337
	Inter quartile range (IQR)	3.6397855	3.40873335	2.74675755
	Mean (\bar{X})	8.01314065	0.641291534	-4.404250862
	Skewness (S)	0.370291516	0.033822549	-1.020575945
	Variance (s^2)	7.037856881	5.389956637	8.018356899
	p-value	0	0	0

Table 4.9: Statistical Analysis of the Third Triple Axial Accelerometer Sensor

		Accelerometer-3		
		x-axis	y-axis	z-axis
Statistical functions	Confidence interval (<i>CI</i>)	(0.044, 0.0450)	(0.46424, 0.4645)	(0.9237, 0.9242)
	Standard deviation (σ^2)	0.002786645	0.002685458	0.004253021
	Inter quartile range (<i>IQR</i>)	0.003906369	0.003906369	0.005859554
	Mean (\bar{X})	0.044917386	0.464407727	0.923983764
	Skewness (<i>S</i>)	0.094714823	0.01420003	0.150220506
	Variance (s^2)	7.76539E-06	7.21169E-06	1.80882E-05
	p-value	0	0	0

Statistical analysis of the accelerometer histograms shows that each sensor has a bias, which is unique. The tables 4.7, 4.8 and 4.9 mentioned above present the statistical analysis of the readings acquired from three similar accelerometers.

4.4 Experimental Evaluation and Results

The experimental setup involves a set of three gyroscopes, magnetometers and accelerometers are embedded in myAHRS_plus sensors for generating ICMetric basis number that is utilised to provide identification of device. To gain some precise readings from the sensors, MEMSs are placed devices in a situation free from magnetic and vibration interference. The bias readings are obtained from the gyroscope, magnetometer and accelerometer sensors to create the ICMetric numbers. The statistical analysis is done on the recording data or offset readings to establish ICMetric basis number. In general, the proposed ICMetric security system is integrated in intelligent wheelchair application that provides an essential role in identification.

In order to evaluate the performance of the proposed ICMetric security system, performance metrics are calculated, which are detection accuracy rate and four types of alarms: True Positive (TP), False Positive (FP), True Negative (TN) and False Negative (FN). In this chapter, the results are applied for the two proposed schemes of ICMetric

security system proposed to provide identification of intelligent wheelchair application. The first proposed method is based on the bias readings that generated by gyroscope and magnetometer sensors. This number will be used to apply identification of intelligent wheelchairs. Whereas, the second proposed method is depended on triple ICMetric numbers provided by bias readings generated from three types of MEME sensors.

4.4.1 The First Scheme Based on Bias Readings of Gyroscope and Magnetometer Sensors

In this system, gyroscope and magnetometer sensors are utilised in generating the bias readings to establish the ICMetric basis number. These readings are employed in designing ICMetric security system for applying identification of device.

In the testing phase, the extracted features are utilised to evaluate the accuracy rate in the proposed system. The proposed system is tested with the dataset provided from the trace file created by ns-2 to calculate accuracy rate of detection and four types of alarms. Cross validation for SVM is employed to evaluate the performance of the proposed security system. Confused Matrix, accuracy rate and error rate of the first method in the proposed system shown in the table 4.10 and table 4.11.

Table 4.10 Types of Alarms for the First Method in the Proposed System

Alarms Rate	True Positive (TP)	True Negative (TN)	False Positive (FP)	False Negative (FN)
	99.57%	99.88%	0.12%	0.43%

Table 4.11: Accuracy and Error Rate of the First Method in the Proposed System

Performance Metrics	
Accuracy rate	Error rate
99.77%	0.23%

Table 4.12: Detection Rate of the First Method in the Proposed System

Detection rate	
Normal	Abnormal
99.5%	99.88%

According to the results in tables (4.11) and (4.12) ICMetric security system that based on SVM algorithm and utilised ICMetric numbers generated from readings of magnetometer and gyroscope sensors is more efficient, effective for applying identification with low error rate.

4.4.2 The Second Scheme Based on Bias Readings of Gyroscope, Magnetometer and Accelerometer Sensors

In this experiment, readings are extracted from three identical gyroscopes, magnetometers and accelerometers sensors. To achieve a mean convergence, point a minimum of around 1000 samples is required. The bias readings are produced from the three identical sensors to create the ICMetric basis number. These readings are employed in designing a new ICMetric security system for achieving identification.

The proposed system is tested with the dataset provided from the trace file created by ns-2, in order to calculate accuracy rate of detection and four alarms. Cross validation for SVM is applied to evaluate the performance of the proposed security system. Four types of alarms, error rate and accuracy rate of the second method in the proposed ICMetric security system are shown in the tables 4.13 and 4.14.

Table 4.13 Types of Alarms for the Second Method in the Proposed System

Alarms Rate	True Positive (TP)	True Negative (TN)	False Positive (FP)	False Negative (FN)
	99.57%	100 %	0%	0.43%

Table 4.14: Accuracy and Error Rate of the Second Method in the Proposed System

Performance Metrics	
Accuracy rate	Error rate
99.85%	0.15%

Table 4.15: Detection Rate of the Second Method in the Proposed System

Detection rate	
Normal	Abnormal
99%	100%

The results presented in tables 4.14 and 4.15 represent strong indicator for the good results. The proposed system utilised three ICMetric numbers generated by magnetometer, gyroscope and accelerometer for providing efficient accuracy and low error rate.

4.5 Compression of Experimental Results

This section offers compression of the results presented in two methods proposed that utilised ICMetric technology. The proposed schemes have been searched by comparing between the two schemes that exploit the ICMetric technology. Also the compressions of the results of the proposed system with previous studies presented in this section. Aims of the comparison to show that the proposed system in this thesis can be utilised to provide identification of devices with higher levels of accuracy and low error rate.

4.5.1 Comparison between the First Scheme and System without ICMetric

When the ICMetric security system that utilised gyroscope and magnetometer to apply identification of the system is compared with the system without ICMetric, the proposed ICMetric security system was more effective with efficient accuracy rate and low false negative alarms rate. The comparison of the performance is shown in table 4.16

Table 4.16 Compression of Accuracy and Error Rate between the First Method in Proposed System and System without ICMetric

Class	Accuracy	Error rate
System with ICMetric	99.77%	0.23%
System without ICMetric	99.75%	0.25%

The proposed system based on ICMetric and utilised two sensors provides better accuracy rate and low error rate than the system without ICMetric according to table

4.16. The proposed system based on ICMetric is more efficient than the system without ICMetric according to the results in table 4.17.

Table 4.17 Compression of Alarms Rate between the First Method in Proposed System and System without ICMetric

System without ICMetric		System with ICMetric	
Alarms Type	Accuracy	Alarms Type	Accuracy
True Positive	99.57%	True Positive	99.57 %
True Negative	99.84%	True Negative	99.88%
False Positive	0.16%	False Positive	0.12%
False Negative	0.43%	False Negative	0.43 %

Table 4.18 Compression of Detection Rate between the First Method in Proposed System and System without ICMetric

Performance Metrics	Detection Rate		
	Normal	Abnormal	Average
System without ICMetric	99.57%	86.53%	93.05%
System with ICMetric	99.5%	99.88%	99.69%

According to the table 4.18, the system that utilised ICMetric technology provides better detection rate than system without ICMetric. The first method in proposed ICMetric security system that depends on bias readings extracted from magnetometer and gyroscope sensors can achieve significant security improvement on the external communication system.

4.5.2 Comparison between the Second Scheme and System without ICMetric

When the results of the proposed system that utilised three types of MEMS sensors to apply identification are compared with the system without ICMetric, higher accuracy rate of detection with low rate of false alarms and error rate for the proposed ICMetric system is obtained. The compression of the results is shown in the tables 4.19, 4.20 and 4.21. According to table 4.19, the proposed system based on ICMetric and utilised three sensors provides better accuracy rate and low error rate than the system without ICMetric.

Table 4.19 Compression of Accuracy and Error Rate between the Second Method in Proposed System and System without ICMetric

Class	Accuracy	Error rate
system with ICMetric	99.85%	0.15%
system without ICMetric	99.75%	0.25%

According to the results in table 4.20, the proposed system based on ICMetric that utilised three sensors is more efficient than the system without ICMetric.

Table 4.20 Compression of Alarms Rate between the Second Method in Proposed System and System without ICMetric

System without ICMetric		System with ICMetric	
Alarms Type	Accuracy	Alarms Type	Accuracy
True Positive	99.57%	True Positive	99.57 %
True Negative	99.84%	True Negative	100 %
False Positive	0.16	False Positive	0 %
False Negative	0.43%	False Negative	0.43 %

The proposed ICMetric security system can achieve the significant security improvement as illustrated in in table 4.21.

Table 4.21 Compression of Detection Rate between the Second Method in Proposed System and System without ICMetric

Performance Metrics	Detection Rate		
	Normal	Abnormal	Average
System without ICMetric	99.57%	86.53%	93.05%
System with ICMetric	99%	100%	99.5%

4.5.3 Comparison between the Proposed System and the Previous Studies

In [17], the authors proposed a detection system based on ICMetric technology that utilised magnetometer sensor to apply secure external communication of semi-self-driving and self-driving vehicles. The results of the proposed ICMetric security system

that utilised magnetometer and gyroscope sensors are compared with the authors results in the term of detection rate and error rate as shown in table 4.22.

Table 4.22 Compression of Detection Rate and Error Rate between the First Method in Proposed System and Previous Study

Performance Metrics	Detection Rate			Error Rate
	Normal	Abnormal	Average	
The proposed system	99.5%	99.88%	99.69%	0.23%
Alheeti system [17]	99.77%	98.78%	99.27%	0.72%

On the other hand, a results of the proposed ICMetric security system that utilised magnetometer, gyroscope and accelerometer sensors are compared with the authors result in the term of detection rate and error rate as shown in table 4.23.

Table 4.23 Compression of Detection Rate and Error Rate between the Second Method in Proposed System and Previous Study

Performance Metrics	Detection Rate			Error Rate
	Normal	Abnormal	Average	
The proposed system	99%	100%	99.5%	0.15%
Alheeti system [17]	99.77%	98.78%	99.2%	0.72%

Tables 4.22 and 4.23 show that the detection rate applied by the first method, which utilising two sensors for generating ICMetric number was better than the second method, which utilising three sensors for generating ICMetric number when compered the two methods with previous study.

The authors in [18] suggested a system based on ICMetric technology, which utilised gyroscope sensor and has defensive ability against unpredicted attacks. The results of the proposed ICMetric security system that utilised magnetometer and gyroscope sensors are compared with the authors result in the term of alarms rate as shown in table 4.24.

Table 4.24 Compression of Alarms Rate between the First Method in Proposed System and Previous Study

Alheeti System [18]		The Proposed System	
Alarms Type	Accuracy	Alarms Type	Accuracy
True Positive	99.76%	True Positive	99.57 %
True Negative	99.01%	True Negative	99.88%
False Positive	0.98%	False Positive	0.12%
False Negative	0.22%	False Negative	0.43 %

As illustrated in table 4.24, the proposed system decreases the number of false positive alarms and improve the rate of detection with the higher accuracy equal to 99.77% and low error rate about 0.23%, while accuracy rate of authors proposed system about 99.28% and error rate about 0.71%.

Also, a results of the proposed system that utilised magnetometer, gyroscope and accelerometer sensors are compared with the authors results in the term of alarms rate, accuracy rate and error rate as shown in table 4.25.

Table 4.25 Compression of Alarms Rate between the Second Method in Proposed System and Previous Study

Alheeti System [18]		The Proposed System	
Alarms Type	Accuracy	Alarms Type	Accuracy
True Positive	99.76%	True Positive	99.57 %
True Negative	99.01%	True Negative	100%
False Positive	0.98%	False Positive	0%
False Negative	0.22%	False Negative	0.43 %

Table 4.25 shows that the proposed system decreases the number of false positive alarms and improve the rate of detection with the higher accuracy equal to 99.85% and low error rate about 0.15%, while accuracy of authors proposed system about 99.28% and error rate about 0.71%.

4.5.4 Comparison between the Two Proposed Schemes

The results of the first method of the proposed ICMetric security system that utilised bias readings generated from two types of MEMS sensors are compared with the proposed method that utilised bias readings generated from three types of MEMS sensors, which are magnetometer, gyroscope and accelerometer sensors. Higher rate of accuracy is obtained with low rate of false alarms and error rate for the proposed method

that utilise three sensors. The compression of the results is shown in table 4.26:

Table 4.26 Compression of Alarms Rate, Accuracy Rate and Error Rate between Two Methods Presented in Proposed System

First Method		Second Method	
True Positive Rate	99.57%	True Positive Rate	99.57 %
True Negative Rate	99.88%	True Negative Rate	100 %
False Positive Rate	0.12%	False Positive Rate	0%
False Negative Rate	0.43%	False Negative Rate	0.43%
Accuracy Rate	99.77%	Accuracy Rate	99.85%
Error Rate	0.23%	Error Rate	0.15%

Table 4.26 shows that the second method in the proposed system that depends on three types of MEMS sensors decreases the rate of false positive alarms and the rate of false negative alarms was the same in the two methods. The second method in the proposed system improves the rate of detection with the higher rate of accuracy equal to 99.85% and low error rate about 0.15%, while rate of accuracy in the first method was at 99.77% and error rate about 0.23%.

4.6 Additional Performance Metrics

In order to test and evaluate the performance of the proposed ICMetric security system, two types of scenarios (normal, abnormal) are applied and simulate ns-2 these under certain conditions to acquire real data. The proposed evaluation criteria are Packet Delivery Ratio (PDR), throughput average and end-to-end delay average [64]. These performance metrics of the network are presented in table 4.27 according to the previous mentioned equations 3.11, 3.12 and 3.13.

Table 4.27 Additional Performance Metrics

Performance matrices	Throughput	PDR	End to End Delay
Normal	78.57%	97.68%	1.4751 ms
Abnormal	38.27%	47.58%	1.47772 ms

Table 4,27 shows the significant additional performance metrics: throughput, PDR and End-to-End delay under normal and abnormal scenarios. The number of the of

generated, received and dropped packets in the external communication system of the normal and abnormal scenarios are illustrated in table 4.28.

Table 4.28 Number of Generated, Received and Dropped Packets

Performance Matrices	Number of Generated Packets	Number of Received Packets	Number of Dropped Packets
Normal	1944	1899	46
Abnormal	1944	925	1020

Table 4.28 shows better rate of generated and received packet in the normal state, where the number of the generated and received packet increased. Number of dropped packets are decreased in the normal state.

The number of sent, received and dropped packets is shown in figure 4.11 as presented below:

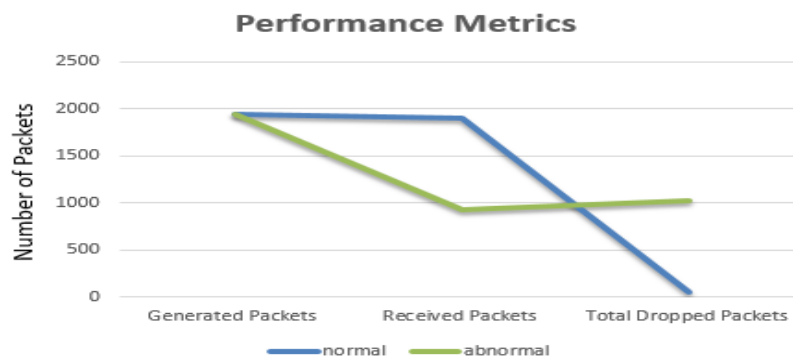


Figure 4.11: Number of Sent, Received and Dropped Packets.

4.7 Chapter Summary

The motivation behind the proposed system is to apply identification and improve security of embedded devices. This system is implemented via many phases, where readings extracting from sensors and statistical analysis phase made on these readings to apply ICMetric number serves for identification, preprocessing phase and finally training / testing phase.

The experiment in the Python show that the proposed system is effective for identification with a low error rate at 0.23% in the proposed system that utilised hybrid ICMetric numbers provided by utilising bias readings generated by two types of MEMS sensors. On the other hand, the system that utilised triple ICMetric numbers provided by utilising bias readings generated by three types of sensors has a low error rate about

0.15%, which is a good indicator of the results. In the two cases system involves efficient accuracy detection.

The results of the two methods in the proposed ICMetric security system are compared with the system without ICMetric. The proposed system that utilises ICMetric technology for applying identification has a higher rate of accuracy and low error rate.

Finally, the results of the proposed ICMetric security system are compared with the authors in [17,18]. The proposed system presented higher rate of detection with low error rate when compared with the authors in [17]. Low false positive alarms, low error rate and higher accuracy of the proposed system when compared with the authors in [18]. Some additional performance matrices are applied in this chapter to test and evaluate the performance.

CHAPTER FIVE

Conclusion, Future Works and Limitations

CHAPTER FIVE

Conclusion, Future Works and Limitations

5.1 Conclusion

In this research, a security system is proposed to apply identification of embedded devices. The proposed system based on ICMetric technology, which relies on special internal features of each device. The following points are concluded in this research:

1. In this thesis, a security system is proposed to apply identification of embedded devices.
2. SVM is efficient, effective with low error rate in improving detection rate.
3. The first method in the proposed system that based on bias readings generated from magnetometer and gyroscope sensors provides 99.77% accuracy rate and 0.23% error rate. Whereas, the second proposed method that based on bias readings generated from three types of sensors provides better accuracy rate was at 99.85% and lower error rate was at 0.15%.
4. The proposed system exhibits higher accuracy rate and low error rate when compared it with the earlier studies.

5.2 Future Works

The proposed research attempts to apply identification and improve security of embedded devices, which also opens up new area for future research. There are some ideas for future extensions of the work presented in below.

1. The thesis has established the design of an ICMetric by using different features of device. Therefore, the aim of the future research is to discover more features, which can strengthen device ICMetric.
2. ICMetric technology has not been researched in bitcoins and block chains. It can be integrated into bitcoin to provide secrecy of transactions.
3. This experiment applied on intelligent wheelchair, which is embedded with the gyroscope, magnetometer and accelerometer sensors that utilised in this research for providing readings. Future experiments can be applied on others

applications for example, wearable devices and healthcare devices to improve devices identification.

References

References

- [1] J. Lizarraga, R. Uribeetxberria and U. Zurutuza, “*Security in Embedded Systems*,” IADIS Int. Conf. Appl. Comput., pp. 697–699, 2006.
- [2] M. Anoop, “*Security needs in embedded systems*,” IACR Cryptol. ePrint Arch., pp. 1–14, 2008.
- [3] S. V. Nayani, “*Designing Secure Solutions For Embedded Systems*,” Oulu University of Applied Sciences, 2017.
- [4] X. Zahi, K. Appiah, S. Ehsan, G. Howells, H. Hu and D. Gu, “*Exploring ICMetrics to Detect Abnormal Program Behaviour on Embedded Devices*,” J. Syst. Archit., pp. 1–9, 2015.
- [5] Sh. Tahir and M. Afzal, “*An ICMetric based Key Generation Scheme for Controlled Group Communication*,” IISA 2014, 5th Int. Conf. Information, Intell. Syst. Appl. Chania, 2014, pp. 373–378, 2014.
- [6] X. Zhai, K. Appiah, and S. Ehsan, “*Application of ICmetrics for Embedded System Security*,” 2013 Fourth Int. Conf. Emerg. Secur. Technol. Appl., pp. 4–7, 2013.
- [7] X. Zhai, K. Appiah, S. Ehsan, and M. Wah, “*A Self-Organising Map Based Algorithm for Analysis of ICMetrics Features*,” Fourth Int. Conf. Emerg. Secur. Technol., pp. 93–97, 2013.
- [8] T. Hopkins, K. D. McDonald-Maier, E. Papoutsis, and W. G. J. Howells, “*Ensuring Data Integrity Via ICMetrics Based Security Infrastructure*,” NASA/ESA Conf. Adapt. Hardw. Syst. AHS-2007, pp. 75–81, 2007.
- [9] Y. Kovalchuk, K. McDonald-Maier, and G. Howells, “*Overview of ICMetrics Technology – Security Infrastructure for Autonomous and Intelligent Healthcare System*,” Int. J. u- e- Serv. Sci. Technol., vol. 4, no. 3, pp. 49–60, 2011.
- [10] Y. Kovalchuk, W. G. J. Howells, H. Hu, and D. Gu, “*A Practical Proposal For*

References

- Ensuring The Provenance Of Hardware Devices And Their Safe Operation,”* 7th IET Int. Conf. Syst. Safety, Inc. Cyber Secur. Conf. 2012, pp. 11–11, 2012.
- [11] B. Ye, G. Howells, and M. Haciosman, “*Investigation of Properties of ICMetric in Cloud,*” Proc. - 2013 4th Int. Conf. Emerg. Secur. Technol. EST 2013, pp. 107–108, 2013.
- [12] Hasan T., G. Howells, H. Hu, D. Gu, and K. Mcdonald-maier, “*On the Incorporation of Secure Filter in ICMetrics Group Communications,*” 2014 Fifth Int. Conf. Emerg. Secur. Technol., pp. 77–81, 2014.
- [13] Hasan T. and K. Mcdonald-maier, “*A Group Secure Key Generation and Transfer Protocol Based on ICMetrics,*” 2014 9th Int. Symp. Commun. Syst. Networks Digit. Sign (CSNDSP), Manchester, 2014, pp. 733–738, 2014.
- [14] Hasan T., Rahma T., and K. Mcdonald-maier, “*Securing MEMS Based Sensor Nodes in the Internet of Things,*” 2015 Sixth Int. Conf. Emerg. Secur. Technol. Secur., pp. 44–49, 2015.
- [15] Hasan T. and K. Mcdonald-maier, “*Securing Health Sensing Using Integrated Circuit Metric,*” Sensors 2015, vol. 15, pp. 26621–26642, 2015.
- [16] Rahma T., Hasan T., K. McDonald-Maier, and A. Fernando, “*A Novel ICMetric Based Framework For Securing The Internet Of Things,*” 2016 IEEE Int. Conf. Consum. Electron. ICCE 2016, pp. 469–470, 2016.
- [17] K. M. A. Alheeti and K. McDonald-Maier, “*An Intelligent Intrusion Detection Scheme For Self-Driving Vehicles Based On Magnetometer Sensors,*” 2016 Int. Conf. Students Appl. Eng. ICSAE 2016, pp. 75–78, 2017.
- [18] K. M. A. Alheeti, R. Al-Zaid, J. Woods, and K. McDonald-Maie, “*An Intrusion Detection Scheme for Driverless Vehicles Based Gyroscope Sensor Profiling,*” 2017 IEEE Int. Conf. Consum. Electron., pp. 2–3, 2017.
- [19] Rahma T., Hasan T., A. Sajjad, and K. McDonald-Maier, “*A secure cloud framework for ICMetric based IoT health devices,*” Proc. Second Int. Conf. Internet things Cloud Comput. - ICC ’17, pp. 1–10, 2017.
- [20] Hasan T., Rahma T., and K. Mcdonald-maier, “*On the security of consumer*

References

- wearable devices in the Internet of Things*,” PLoS One, vol. 13(4), pp. 1–21, 2018.
- [21] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5th ed. Stallings William, 2011.
- [22] M. Alshahrani and H. Teymourlouei, “*Network Security: Threats and Vulnerabilities*,” Int’l Conf. Secur. Manag., pp. 115–121, 2016.
- [23] Khattab M. Ali, “*Intrusion Detection System in External Communication for Self-Driving Vehicles*,” phd thesis, University of Essex, 2017.
- [24] G. Samara, W. A. H. Al-salihy, and R. Sures, “*Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)*,” 4th Int. Conf. New Trends Inf. Sci. Serv. Sci. Gyeongju, pp. 393–398, 2010.
- [25] X. Lin, R. Lu, C. Zhang, H. Zhu and X. Shen, “*Security in Vehicular Ad Hoc Networks*,” IEEE Commun. Mag., vol. 46, no. 4, pp. 88–95, 2008.
- [26] Hasan T., “*An ICMetric Based Multiparty Communication Framework*,” phd thesis, University of Essex, 2017.
- [27] X. Zhai, K. Appiah, and S. Ehsan, “*Application Of ICMetrics For Embedded System Security*,” 2013 Fourth Int. Conf. Emerg. Secur. Technol., pp. 4–7, 2013.
- [28] B. M. Faria, S. Vasconcelos, L. P. Reis, and N. Lau, “*A Methodology For Creating Intelligent Wheelchair Users’ Profiles*,” ICAART 2012 - Proc. 4th Int. Conf. Agents Artif. Intell., pp. 171–179, 2012.
- [29] T. Röfer, C. Mandel, and T. Laue, “*Controlling An Automated Wheelchair Via Joystick/Head-Joystick Supported By Smart Driving Assistance*,” 2009 IEEE Int. Conf. Rehabil. Robot. ICORR 2009, pp. 743–748, 2009.
- [30] “*ITHROBOT*” [Online]. Available: <http://withrobot.com/en/sensor/myahrplus/?ckattempt=3>. [Accessed: 01-Apr-2019].
- [31] A. Shaikh, “*Micro-Electromechanical System (MEMS) Sensor*,” Int. J. Sci. Eng. Res., vol. 3, no. 11, pp. 1–8, 2012.

References

- [32] L. S. B. Preethi and V. S. Selvakumar, “***Design and Analysis of MEMS Gyroscopes,***” *proceeding 2012 COMSOL Conf. banglore*, pp. 1–39, 2013.
- [33] O. Willers, C. Huth, J. Guajardo, and H. Seidel, “***MEMS-based Gyroscopes as Physical Unclonable Functions,***” *CCS '16 Proc. 2016 ACM SIGSAC Conf. Comput. Commun.*, pp. 591–602, 2015.
- [34] Y. Cai, Y. Zhao, X. Ding, and J. Fennelly, ***Magnetometer Basics For Mobile Phone Applications***, vol. 54. 2012.
- [35] G. Troni and R. M. Eustice, “***Magnetometer Bias Calibration Based on Relative Angular Position: Theory and Experimental Comparative Evaluation,***” *IEEE Int. Conf. Intell. Robot. Syst.*, pp. 444–450, 2014.
- [36] A. V. Rao D, Natrajan P and Ahmed R, “***Onboard Estimation and Correction of Magnetometer Bias In MEMS based Tri Axial Inertial Measurement Unit,***” *ICIUS-2013-274*, 2013.
- [37] D. Ren, L. Wu, M. Yan, M. Cui, Z. You, and M. Hu, “***Design and Analyses of A MEMS Based Resonant Magnetometer,***” *Sensors*, vol. 9, no. 9, pp. 6951–6966, 2009.
- [38] P. Jain, “***Magnetometers,***” 2012. [Online]. Available: <https://www.engineersgarage.com/articles/magnetometer>. [Accessed: 19-Oct-2018].
- [39] M. Caruso, T. Bratland, C. Smith, and R. Schneider, “***A New Perspective on Magnetic Field Sensing,***” *Sensors (Peterborough, NH)*, vol. 15, pp. 1–19, 1998.
- [40] C. P. Mayer, “***Security and Privacy Challenges in the Internet of Things,***” *Electron. Commun. EASST*, vol. 17, pp. 1–13, 2009.
- [41] R. Vemal., “***MEMS vs . IC Manufacturing : Is Integration Between Processes Possible,***” *2009 1st Asia Symp. Qual. Electron. Des.*, pp. 3–7, 2009.
- [42] D. J. Fonseca and M. Sequera, “***On MEMS Reliability and Failure Mechanisms,***” *Hindawi Publ. Corp. Int. J. Qual. Stat. Reliab.*, vol. 2011, pp. 1–7, 2011.

References

- [43] T. Van Goethem, W. Scheepers, D. Preuveneers, and W. Joosen, “*Accelerometer-Based Device Fingerprinting for Multi-factor Mobile Authentication*,” *springer*, pp. 106–121, 2016.
- [44] Y. Kovalchuk and K. McDonald-maier, “*Overview of ICMetrics Technology – Security Infrastructure for Autonomous and Intelligent Healthcare System*,” *Int. J. u- e- Serv. Sci. Technol.*, vol. 4, no. 3, pp. 49–60, 2011.
- [45] R. C. Simpson, “*Smart Wheelchairs : A Literature Review*,” *J. Rehabil. Res. Dev.*, vol. 42, no. 4, pp. 423–436, 2005.
- [46] M. dadafshar, “*Accelerometer and Gyroscopes Sensors: Operation, Sensing, and Applications*,” *maxim Integr.*, pp. 1–11, 2014.
- [47] M. T. Scholar, “*Wheel-Chair Control Using Accelerometer Based Gesture Technology*,” *Int. J. Adv. Res. Comput. Eng. Technol.*, vol. 4, no. 5, pp. 1802–1806, 2015.
- [48] S. V Hiremath, D. Ding, and R. A. Cooper, “*Development and evaluation of a gyroscope- based wheel rotation monitor for manual wheelchair users*,” *J Spinal Cord Med. 2013 Jul*, vol. 36, no. 4, pp. 347–356, 2013.
- [49] S. Dey, N. Roy, W. Xu and R. Choudhury, “*AccelPrint : Imperfections of Accelerometers Make Smartphones Trackable*,” *Netw. Distrib. Syst. Secur. Symp.*, pp. 23–26, 2014.
- [50] S. Shubhendu and J. Vijay, “*Applicability of Artificial Intelligence in Different Fields of Life*,” *Int. J. Sci. Eng. Res.*, vol. 1, no. 1, pp. 28–35, 2013.
- [51] M. T. Pannu, “*Artificial Intelligence and its Application in Different Areas*,” *Certif. Int. J. Eng. Innov. Technol.*, vol. 4, no. 10, pp. 79–84, 2015.
- [52] Mariam K. AlSedrah, “*Artificial Intelligence*,” *Adv. Anal. Des. CNIT 380*, pp. 1–12, 2018.
- [53] A. R. Ahmad and R. Yusof, “*Machine Learning Using Support Vector Machines*,” pp. 1–8, 2019.
- [54] G. Anthony, H. Greg, M. Tshildzi, I. Engineering, and S. Africa, “*Classification*

References

- of Images Using Support Vector Machines,”* 2007.
- [55] K. Baba, T. Nakatoh, Y. Yamada, and D. Ikeda, “**A Review of Classification Approaches Using Support Vector Machine in Intrusion Detection,**” *Commun. Comput. Inf. Sci.*, vol. 252, pp. 610–615, 2011.
- [56] T. I. and E. Hossain, **Introduction to Network Simulator NS2**, Second Edi. Springer, Boston, MA, 2012.
- [57] “**The Network Simulator - ns-2.**” [Online]. Available: <https://www.isi.edu/nsnam/ns/>. [Accessed: 11-Apr-2019].
- [58] J. Wang, “**ns- Tutorial (1),**” *Event (London)*, no. 1, pp. 1–16, 2004.
- [59] “**Learn more about Network Simulator.**” [Online]. Available: <https://www.sciencedirect.com/topics/computer-science/network-simulator>. [Accessed: 12-Apr-2019].
- [60] P. S. N. D. and N. S. Kumari, “**A Survey Of Routing Protocols for VANET in Urban Scenarios,**” *2013 Int. Conf. Pattern Recognition, Informatics Mob. Eng.*, pp. 464–467, 2013.
- [61] “**Manual interpretation of ns2 trace file.**” [Online]. Available: <https://getch.wordpress.com/2010/11/20/manual-interpretation-of-ns2-trace-file/>. [Accessed: 13-Apr-2019].
- [62] “**6.Trace File Definition | Network Simulator 2.**” [Online]. Available: <https://cloudns2.wordpress.com/trace-file-definition/>. [Accessed: 07-Apr-2019].
- [63] G. Kumar, “**Evaluation Metrics for Intrusion Detection Systems - A Study,**” *Int. J. Comput. Sci. Mob. Appl.*, vol. 2, pp. 11–17, 2014.
- [64] A. Eltahir and R. Saeed, “**Performance Evaluation of An Enhanced Hybrid Wireless Mesh Protocol (E-HWMP) Protocol for VANET,**” *Proc. - 2015 Int. Conf. Comput. Control. Networking, Electron. Embed. Syst. Eng. ICCNEEE 2015*, pp. 95–100, 2016.

الخلاصة

ان الأمر المثير للاهتمام في الأنظمة المدمجة يتعلق بمسائل توفير الخصوصية والأمان، حيث يمكن الكشف عن أمان أي بيانات محفوظة على النظام من خلال الوصول غير مصرح إليها. غالبا لا يوجد نظام أمن مثالي لجميع التطبيقات؛ وهذا يعني أن مجال البحث مفتوح لاقتراح نظام أمن جديد أو تحسين نظام قديم، وبالتالي، فقد تم اقتراح نظام أمني في هذه الرسالة.

تم اقتراح النظام لتطبيق التعريف وتحسين أمان الأجهزة المدمجة. حيث يعتمد النظام المقترح على تقنية جديدة تسمى مقياس الدوائر المتكاملة (ICMetric)، والتي تعتمد على الميزات الداخلية الخاصة لكل جهاز. باستخدام ICMetric، تم استخدام ميزات الجهاز ذات المستوى المنخفض لإنشاء تعريف للجهاز.

يستند العمل المقترح إلى استخدام التحيز في مقياس accelerometer و gyroscope و magnetometer لإنشاء رقم ICMetric الفريد لكل جهاز. يتم استخدام هذا الرقم في مجموعة البيانات المستخرجة من ملف التتبع الذي تم إنشاؤه بواسطة Network Simulator الإصدار الثاني (ns-2) من أجل الوصول الى الهدف من خلال التعرف والكشف. يتكون النظام المقترح من ثلاث مراحل رئيسية. المرحلة الأولى هي قراءات التحيز المستخرجة من أجهزة الاستشعار. بينما، في المرحلة الثانية، يتم إنشاء رقم ICMetric باستخدام قراءات التحيز المستخرجة من أجهزة الاستشعار في المرحلة الأولى. في المرحلة الثالثة، يتم اختبار وتقييم النظام لقياس فعاليته. بمعنى آخر، يتم اختباره باستخدام مجموعة البيانات التي يتم استخراجها من ملف التتبع الخاص بمحاكاة الشبكة. في هذه المرحلة، يتم حساب مقاييس الأداء، وهي معدل الخطأ، confused matrix ومعدل الدقة.

تم اقتراح نظام تعريف او الكشف في هذه الأطروحة لتوفير التعرف على الكراسي المتحركة الذكية في طريقتين. تعتمد الطريقة الأولى المقترحة على قراءات التحيز التي تولدها أجهزة استشعار الجيروسكوب وأجهزة قياس المغنوميتير. بينما تعتمد الطريقة الثانية على ثلاث أرقام ICMetric المتولدة من قراءات التحيز الناتجة عن ثلاثة أنواع من أجهزة الاستشعار.

تم محاكاة الطرق المقترحة باستخدام مجموعة البيانات المستخرجة من ملفات التتبع. تمت مقارنة نتائج المحاكاة ودراستها للحصول على مستويات عالية من القدرة على الكشف ومقاييس الأداء.



جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة الانبار
كلية علوم الحاسبات وتكنولوجيا
المعلومات

تقنية ICMetric لحماية الأجهزة المدمجة

رسالة مقدمة الى

كلية علوم الحاسبات وتكنولوجيا المعلومات – قسم علوم الحاسبات -
جامعة الانبار وهي جزء من متطلبات نيل درجة الماجستير في علوم
الحاسبات

قدمت من قبل

دعاء عبد الستار روكان

بإشراف

أ.م.د. صلاح صليبي الراوي

أ.م.د. خطاب معجل الهيتي