西南交通大学学报

第 54 卷 第 3 期
2019 六 3 月

JOURNAL OF SOUTHWEST JIAOTONG UNIVERSITY

Vol.54 No.3
June 2019

ISSN - 0258-2724

DOI：10.35741/issn.0258-2724.54.3.17

Research article

AN ICMETRIC SECURITY SYSTEM FOR INTELLIGENT WHEELCHAIRS BASED ON TRIPLE MEMS SENSORS

Duaa Al_Dosary [a,] *, Khattab M Ali Alheeti [a, b], Salah Sleibi Al-Rawi[b]
[a] College of Computer and Information Technology
University of Anbar, Anbar –Iraq , mobileip39@gmail.com
[b] College of Computer and Information Technology
University of Anbar, Anbar –Iraq, co.khattab.alheeti@uoanbar.edu.iq

Abstract

Embedded systems are increasing in many areas, some examples of an embedded system are mobile phones, video game consoles, and industrial monitoring. Currently, interest with embedded systems is concerned with the issues of the providing safety, privacy and security. Security techniques rely on keeping the keys hidden, system can be exposed when the keys are described. We propose a system based on ICMetric that exploits the features of an embedded device to produce the identification of device. This paper proves that unique device features can be utilized to present an identity to a device which can be consumed for the providing security. The ICMetric technology has the facility to protect the systems by exploiting features of device. The proposed system uses the embedded MEMS magnetometer, gyroscope and accelerometer in the myAHRS_plus sensor to create a device ICMetric. An intelligent wheelchair is required which is equipped with the MEMS sensors. The proposed system is built on the features which have been produced by bias values of magnetometer, gyroscope and accelerometer. Reading generated from sensors are analyzed statistically to generate a triple ICMetric numbers used for device identification. The ICMetric number is not stored on the system and can be reproduced when necessary. If the system is attacked, there will be no theft because the ICMetric number is non-store. The proposal system proves that using MEMS sensors to generate an ICMetric number which using for device identification increase authentication and security of embedded devices.

Keywords: accelerometer; device identification; embedded systems; gyroscope; ICMetric; magnetometer.

摘要 嵌入式系统在许多领域都在增加，嵌入式系统的一些例子是移动电话，视频游戏控制台和工业监控。目前，对嵌入式系统的兴趣涉及提供安全性，隐私性和安全性的问题。安全技术依赖于保持密钥隐藏，系统可以在描述密钥时暴露。我们提出了一种基于 ICMetric 的系统，该系统利用嵌入式设备的特性来产生设备的识别。本文证明可以利用独特的设备特征向设备呈现身份，该身份可以用于提供安全性。 ICMetric 技术具有利用设备功能保护系统的功能。所提出的系统使用 myAHRS_plus 传感器中的嵌入式 MEMS 磁力计，陀螺仪和加速度计来创建设备 ICMetric。需要配备 MEMS 传感器的智能轮椅。所提出的系统建立在磁力计，陀螺仪和加速度计的偏置值产生的特征之上。从统计上分析从传感器生成的读数以生成用于设备识别的三重 ICMetric 数。 ICMetric 编号未存储在系统中，必要时可以复制。如果系统受到攻击，则不会被盗，

因为 ICMetric 编号是非存储的。该提案系统证明使用 MEMS 传感器生成 ICMetric 数，该 ICMetric 数用于设备识别，增加了嵌入式设备的认证和安全性。

关键词: 加速度计; 设备识别; 嵌入式系统;陀螺仪;ICMetric;磁力计。

I. INTRODUCTION

Embedded systems exist in many devices. Cellular phones, toys, PDAs, home appliances, automotive and aircraft devices, and industrial equipment an example of daily products of embedded systems. The main characteristics of an embedded system are accomplished a specific operation and must compute certain results in real time with no delay. It must be based on a microprocessor or micro-controller. Embedded system basic structure explained in the figure (1) include many elements each of them have a specific task and these differ from the typical desktop or laptop computer [1].

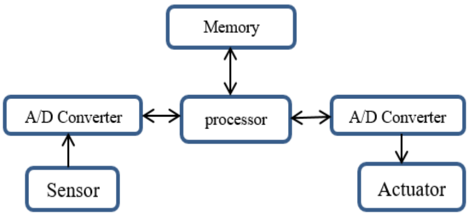


Figure1. The basic structure of an embedded system [1]

Using of embedded systems nowadays has increased in most aspects of life with which one application can perform large-scale operations. Embedded devices are networked through wireless links of communication to complete valuable jobs [2]. security of embedded systems is a key feature of the design of embedded systems and is now a main area of study because the wireless communication channel between the embedded devices makes them exposed to attacks [3]. The ICMetric is a technology that has been used to ensure security in embedded systems [4]. ICMetrics utilized device features to present identification to the device [5]. ICMetric uses unique device features to generate a basis number, which can be consumed to generate device identification [6].

In this paper, the proposed ICMetric security system apply a novel aspect to present security systems. The proposed system uses bias readings generated from the magnetometer, gyroscope and accelerometer sensors to generate an ICMetric number used to supply identification of the device. Using ICMetric number generated from sensors increases security and identification of the device. We introduced ICMetric-security system to provide security for the intelligent wheelchair application. The proposed system exploits ICMetric technology in providing identification of intelligent wheelchair used by persons need it. The rest of this paper is organized as follows: section 2 provides related works; section 3 summarizes integrated circuit metric (ICMetric); section 4 discusses the proposed ICMetric security system; in section 5 we talked about magnetometer, gyroscope and accelerometer sensors followed by exploiting MEMS imperfections in section 6; our experimental setup discussed in section 7; We explain how the ICMetric number is generated in section 8; section 9 shows experimental results; discussion introduced in section 10; conclusions are mentioned in section 11.

II. PURPOSE OF THE STUDY

In this paper, the system presented an attempt to improve embedded devices security. The proposed system employs ICMetric technology which suggests using device features to create ICMetric number used for identification of device.

III. RELATED WORKS

Several researchers present a wider framework of security that is made on ICMetric technology. This section presents some previous studies related to this work. Hasan T. et al. tested their proposed system on health sensors provided with an accelerometer. They are produced an ICMetric number from readings are achieved from the sensor. They have exploited the accelerometer sensor to create an ICMetric exploited to apply identification of the device [7]. In [8], the authors used the MEMS accelerometer to create sensor identification. In the proposed scheme they have combined the ICMetric functionalities with the protocol of a symmetric key for supplying confidentiality, access control and authentication of health data in an efficient manner. Khattab M. and Klaus M. offered a system based on ICMetric technology that used the bias reading characteristics of infrared sensors to supply defense to the external communication of autonomous vehicles [9]. In [10], the authors proposed a system based on ICMetric technology that uses the MEMS gyroscope and features of the system to produce a vehicle identification. The proposed system has a significant capability to defend against attacks. In [11], the author studied activity data as an ICMetrics feature and examined how the number of samples of the feature values affects ICMetrics system's performance. Hasan T. et al. proposed the system for the supporting of wearable devices security based on ICMetric technology that exploits the features of a device to provide an identification. They are using an accelerometer and gyroscope sensor to produce device ICMetric [12].

IV. Integrated Circuit Metric (ICMetric)

The ICMetric is a technology that depends on the device characteristics to prove security. There are differences in the internal environment of the devices, although these devices have the same model and the company manufactured. Addresses, serial numbers, program counter data, data in the RAM, data in the cache and other features can be employed for ICMetric generation a basis number for apply device identification [13]. Each device is unique therefore, the feature that makes each device different can be exploited to generate a unique number for each device. The ICMetric number is not stored on the system and can be recreated when necessary. If the system is attacked, there will be no theft because the ICMetric is non-store [14].

ICMetric system generation requires two phases which are the calibration phase to collect feature values of the system for normalization processes. In this phase, the features mapping studied for their skewness, confidence interval, standard deviation, and inter-quartile range. The second phase is an operation phase to distribute each extracted features for typical sensors. Operation phase includes two techniques which are feature addition and feature concatenation that can be used for linking the individual feature values [8].

V. ICMetric-security system

Current defensive mechanisms are insufficient for preventing attacks in the device since they need ICMetric security system as a protection system to raise their security. ICMetrics technology rely on measurable features, which have been gained from the properties of a particular embedded device [15]. In this research, we will integrate ICMetrics technology with medical intelligent wheelchair to provide identification and security. The control architecture of intelligent wheelchair used in this research is shown in Figure 2. Our experiment used bias readings extracted from MEMS (gyroscope, magnetometer and accelerometer) sensors embedded in intelligent wheelchair to provide identification.

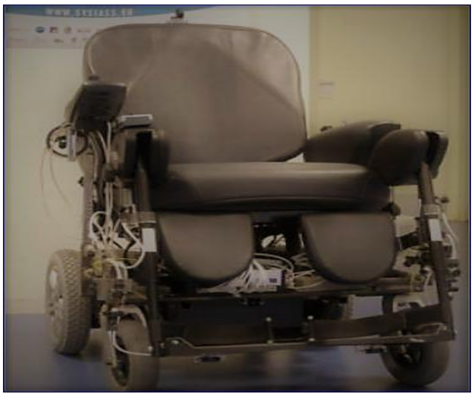


Figure 2. The intelligent wheelchair used in this research [16]

The focus is on using MEMS sensors that are embedded in current systems. In this research, the bias reading that has been applied by magnetometer, gyroscope and accelerometer sensors devices is utilized to generate ICMetric security system. The bias readings were utilized to produce an ICMetric basis number that used to supply identification for the device.

The phases of the proposed identification system; explained as below:

- The **first stage** related to reading extraction from the magnetometer, gyroscope and accelerometer sensors to generate an ICMetric number. simple statistical and mathematical works are used to produce the ICMetric number. The ICMetric number used in the ICMetric-security system. Figure 2 displays the myAHRS-plus sensor which contains the magnetometer, gyroscope and accelerometer sensors.

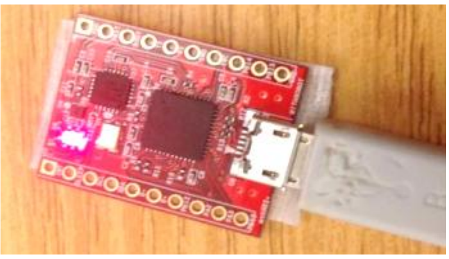


Figure 3. myAHRS_plus sensor [9]

- Pre-processing is the **second stage** in the proposed system. Features are required transferring some letters and symbols into numbers and extracted features are normalized to make the performance of ICMetric-security system more effective.

- Training phase- support vector machine (SVM) is the **third stage** in the ICMetric security system. The SVM is trained with the dataset for generating the ICMetric-security system.

- The testing phase is the **fourth Stage** to determine the accuracy of the detection rate and four types of alarms.

The general design of the proposed security system is presented in the figure 2 where the proposed system includes many phases start with extract reading from MEMS sensors to generate ICMetric number used for device identification.

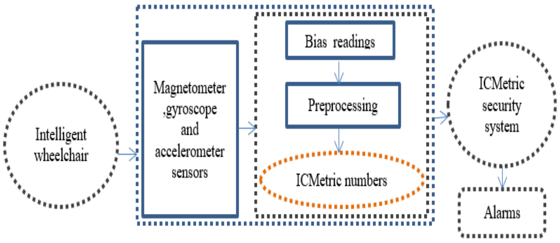


Figure 4. Overall ICMetric system Architectural

The proposed security system it is based on features that are obtained from characteristics of an intelligent wheelchair sensors. The generated features can be utilised to provide identification for the device. For ICMetric generation those features which can be signified as a unimodal distribution are chosen. At first the proposed system generates the bias reading by the magnetometer, gyroscope and accelerometer sensors to apply ICMetric numbers serves for identification.

VI. MEMS SENSORS

Micro-electro-mechanical-system (MEMS) include a magnetometer, gyroscope and accelerometer sensors, because of their small size and low costs are widely used in many areas [17]. Magnetometer sensors are now used in many fields, in response to the demands of users in the automotive industry, Judgment, military/aerospace and consumer [18]. Magnetometers are 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 [19]. Micro Electro Mechanical System (MEMS) technology provides the most popular MEMS magnetometers. intelligent wheelchairs used MEMS magnetometer sensors for measuring and detecting magnetic fields. Hall Effect, Magneto-resistive effect and fluxgate effect are the most common principles in magnetometer sensors. Magnetometer sensor based on Hall Effect to measure the magnetic fields [20][21].

The MEMS gyroscope is a sensor built on the Coriolis impact [22]. Gyroscopes fixed on a frame and able to measure an angular velocity if the frame is rotating [23]. Gyroscopes used in many applications in intelligent wheelchair, industrial robotics, space, and automobiles. Gyroscope using widely in smartphones where it gives us a new way to interface for motion and gestures with our smart device [24]. The MEMS accelerometer is a micro-electromechanical sensor which is very sensitive sensor and capable of detecting the tilt. Accelerometer used in many applications for example intelligent wheelchair. This sensor changes the direction of the wheelchair depending on tilt [24]. Magnetometer, gyroscope and accelerometer sensors play an important role in designing intelligent wheelchairs applications. The proposed system depends on features which have been generated by bias readings of magnetometer, gyroscope and accelerometer sensors.

VII. MEMS IMPERFECTIONS EXPLOITATION

The manufacturing process of MEMS magnetometer, gyroscope and accelerometer presents slight imperfections that lead to the generation of bias in these sensors. When the MEMS ingredients is collected, then a bias is presented. More bias can be created due to strain applied by the board. Since several factors affect the sensors operations, therefore the presented bias is a task of several variables which cannot be expected and these variables are outside of the manufacturer control [7]. Hardware devices when being invented are presented imperfections. MEMS sensors are placed on the board; simulation is used to supply bias. When a sensor is under operation, its accuracy of output is affected by unclear damages [25]. There are many types of powered effects that generate sensor bias while the electrical safety is preserved. Sensors biases are different from one to another. Calibrations try to reparation for readings error by combining a linear value into the raw values acquired from the sensor [26]. The new concept is applied by using sensor imperfections with the ICMetric technology. Earlier researches proposed the sensor bias for only device identification.

The ICMetric uses the sensor features and bias to supply identification which is utilized for security services [27]. Devices have many features which can be used for identification processes. The difficulty with using features of devices is that particular features are hard to produce or cannot apply device identification only. Features of the device are used for generating an ICMetric. Different readings being extracted because several samples of the same device combined with the same sensor even when the same stimulus is being offered [28].

VIII. EXPERIMENTAL SETUP

Our experiment involves of a myAHRS_plus sensor placed on a board free from trembling and magnetic intervention [29]. The myAHRS_plus sensor is equipped with a 3-axis magnetometer, gyroscope and accelerometer sensor. The myAHRS_plus is considered one of the most accurate sensors in the scientific research area. It is an embedded sensor triple axis magnetometer, gyroscope and accelerometer with a sensibility of ±16g. Several numbers of bias reading are gained from myAHRS_plus to produce ICMetric basis number. The security system required to determine the optimal number of offset readings used to apply device identification [30].

Using the myAHRS_plus sensor as an experimental platform, we obtained 1000 individual readings from the magnetometer, gyroscope and accelerometer sensors. The output readings from the sensors are used to prove that each sensor works differently when exposed to the same stimulus. Each axis of magnetometer, gyroscope and accelerometer sensors possess an exclusive bias which is presented in the readings. Our experiments also approve that the bias of sensors is unique and represent an implicit feature of sensors because it cannot be expected for any specific sensor. When the values are gained a statistical and mathematical analysis is prepared on the data acquired. Statistical differences for histograms achieved from different sensors make the bias of magnetometer, gyroscope and accelerometer sensors a helpful feature for ICMetric generation.

IX. GENERATION OF THE ICMETRIC IDENTIFICATION

The ICMetric generation requires mathematical processes and a statistical analysis of the values of the features [8]. The features are chosen for ICMetric generation, these features can be indicated as a unimodal distribution [12]. The reading extracted from the magnetometer, gyroscope and accelerometer sensors utilized to generate a frequency distribution which will cause in a histogram that shows the unimodal distribution [31]. The number of readings required and produced from the sensors is determined by factors like accuracy and the sampling rate of the sensor [27]. For ICMetric generation process, probability mass $(\boldsymbol{x})$ function is needed to determine the precise value from the bias reading. If we assume that $\boldsymbol{\bar{x}}$ represents the mean, $\boldsymbol{x}$ is represent specific sample reading from the magnetometer, gyroscope and accelerometer and $\boldsymbol{n}$ is a total number of reading then [7]:

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} xi \qquad (1)$$

In order to complete ICMetric generation process and compute probability mass $(\boldsymbol{x})$ function, we must calculate the standard deviation $\boldsymbol{\sigma^2}$:

$$\sigma^2 = \sum_{i=1}^{n} p(x_i)(\,x_i - \bar{x})^2 \qquad (2)$$

We can calculate probability mass $(\boldsymbol{x})$ function as below:

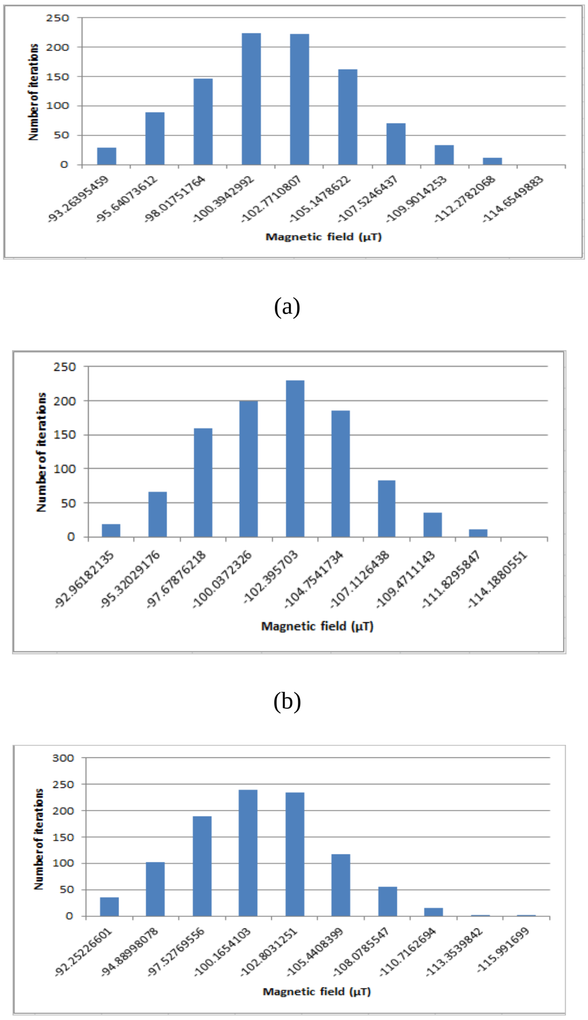
$$p(x) = \frac{1}{\sigma\sqrt{2n}} e^{\frac{-(x-\mu)^2}{2\sigma^2}} \qquad (3)$$

Confidence interval CI is computed for more analysis. If $\boldsymbol{\bar{x}}$ is the mean, $\boldsymbol{\sigma}$ is the standard deviation and $\boldsymbol{n}$ is the number of observations then the the 95% confidence interval $\boldsymbol{CI}$ is given in the equation (4) where the numeric value $\boldsymbol{v}$ equal to 1.96 [12].

CI of upper and lower bound presented in the following equation:

$$CI = \bar{x} \pm v\frac{\sigma}{\sqrt{n}} \qquad (4)$$

Our experiment show that there is a considerable difference between the readings extract from a sensor. This difference adequate for producing an ICMetric number. Given in figure (5), (6) and (7) are diagrams that display normalization for three separate magnetometer sensors. We have supplied the behavior of x, y and z axes of three separate magnetometers.

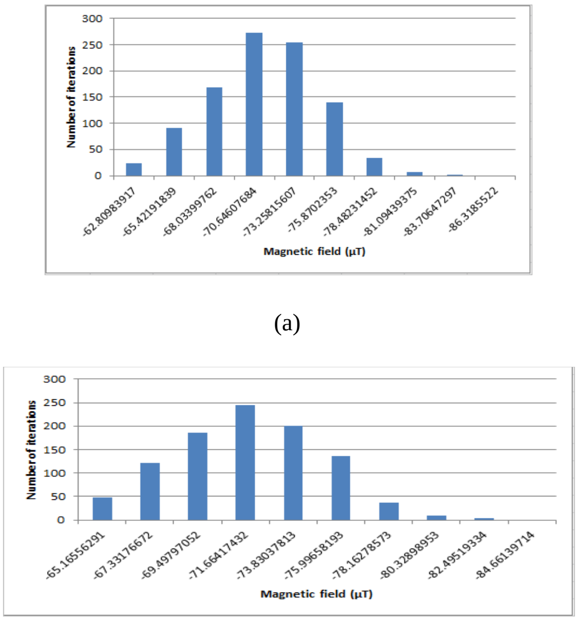


(a)

(b)

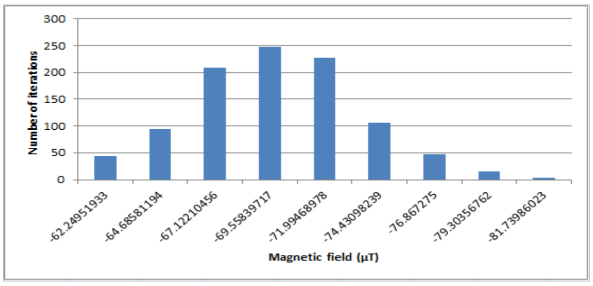
(c)

Figure 5. (a) graph of x-axis (b) graph of x-axis (c) graph of x-axis of reading acquired from three various magnetometer sensors.



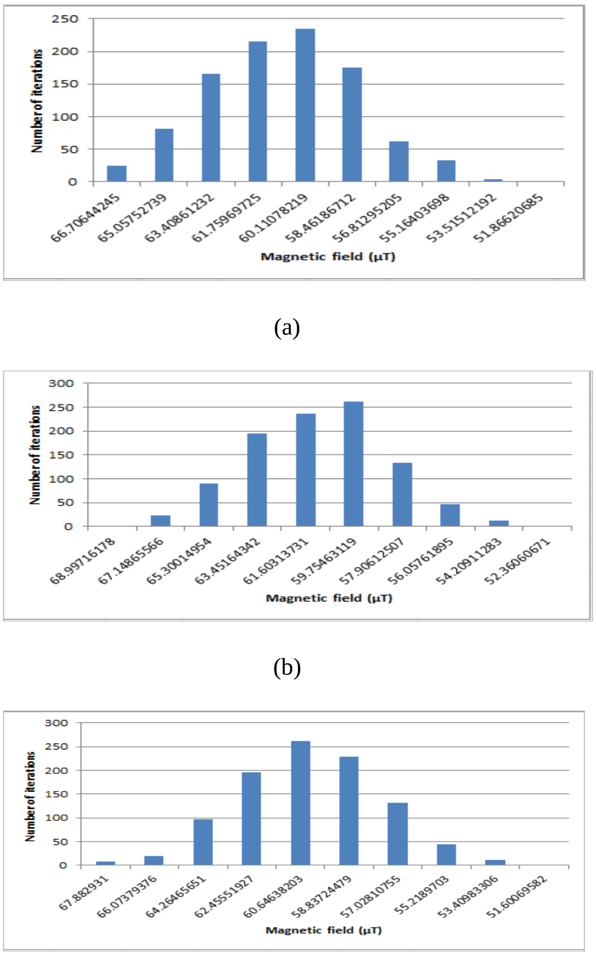
(a)

(b)



(c)

Figure 6. (a) graph of y-axis (b) graph of y-axis (c) graph of y-axis of reading acquired from three various magnetometer sensors.



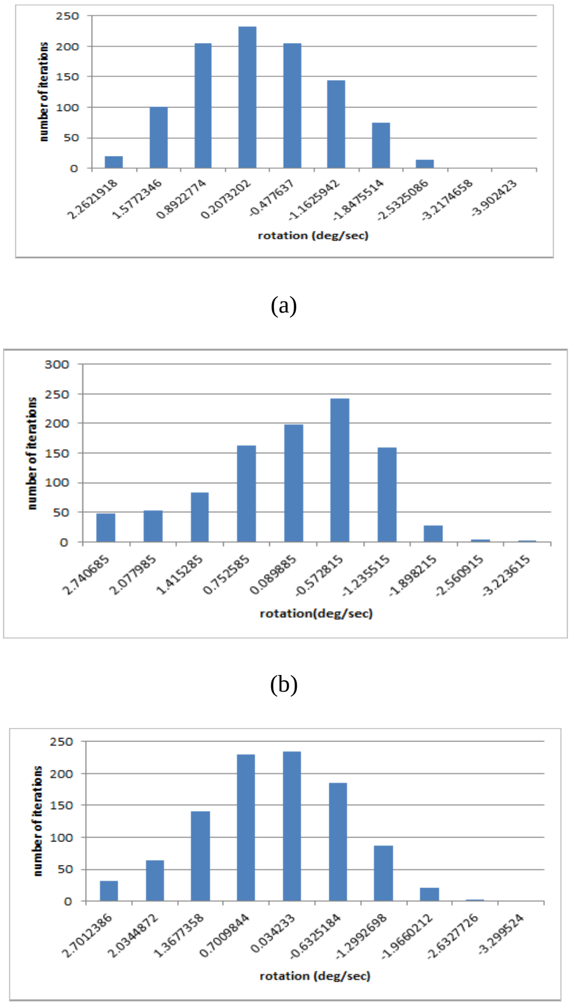
(a)

(b)

(c)

Figure 7. (a) graph of z-axis (b) graph of z-axis (c) graph of z-axis of reading acquired from three various magnetometer sensors.

Given in figure (8), (9) and (10) are diagrams that display normalization in three separate gyroscopes. We are presented the behavior of x, y and z axes of three separate gyroscopes.

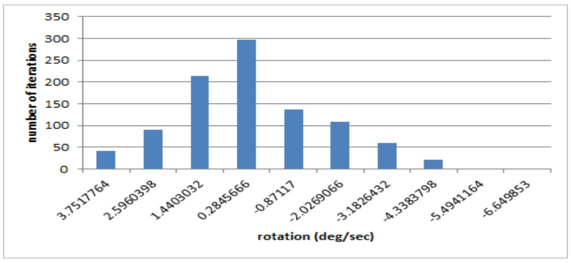


(a)

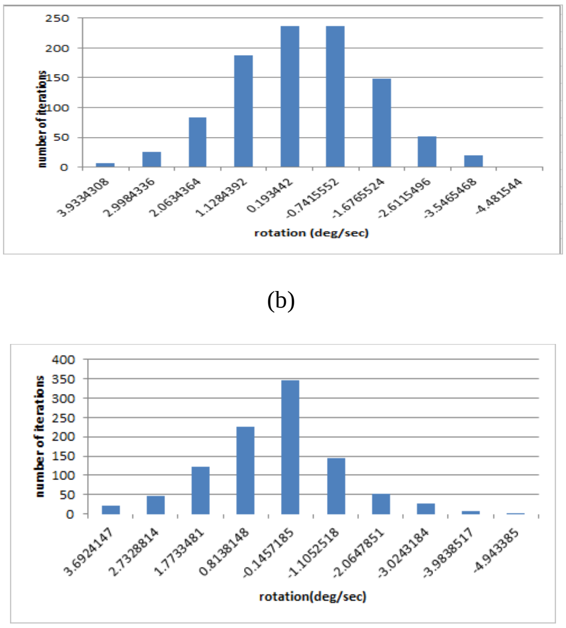
(b)

(c)

Figure 8. (a) graph of x-axis (b) graph of x-axis (c) graph of x-axis of reading acquired from three various gyroscope sensors.



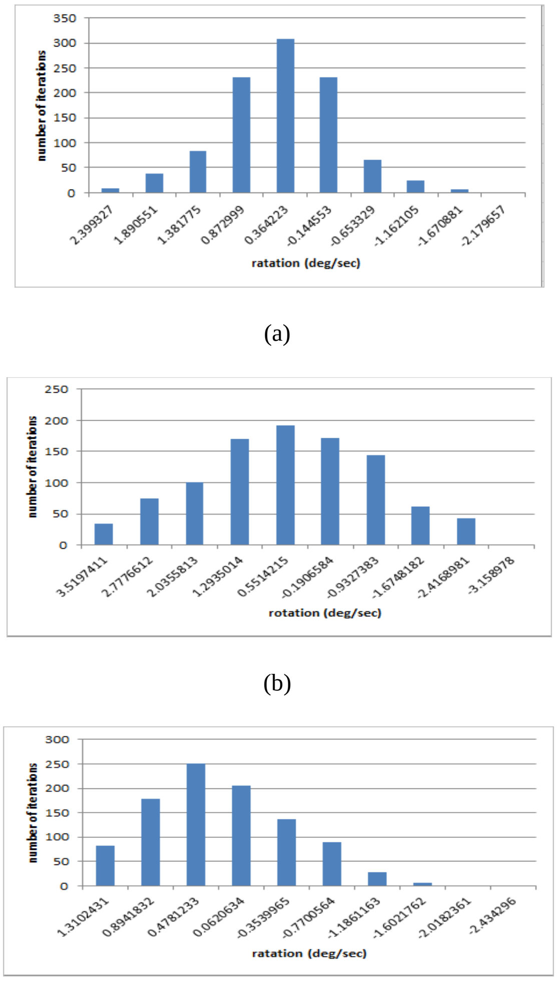
(a)



(b)

(c)

Figure 9. (a) graph of y-axis (b) graph of y-axis (c) graph of y-axis of the reading acquired from three various gyroscope sensors.



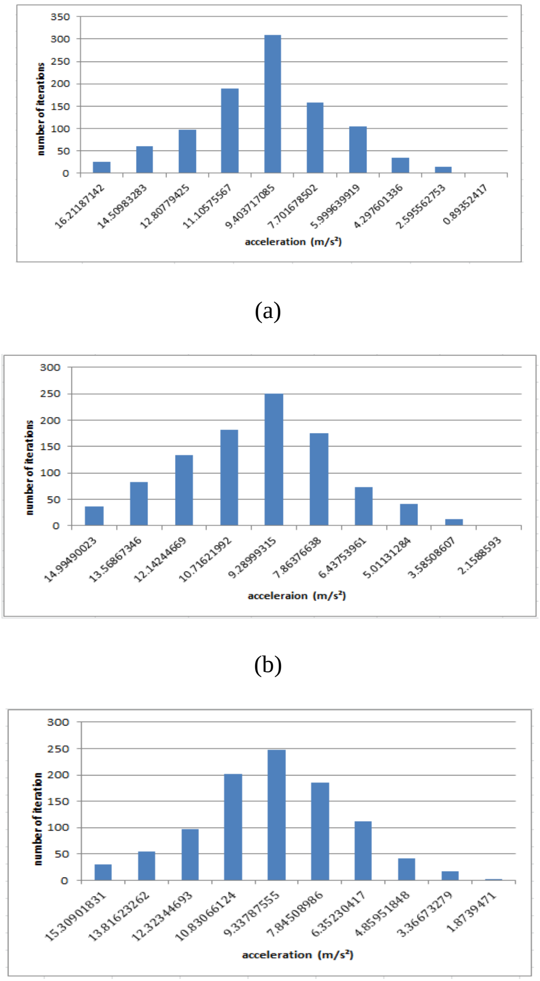
(a)

(b)

(c)

Figure 10. (a) graph of z-axis (b) graph of z-axis (c) graph of z-axis of the reading acquired from three various gyroscope sensors.

Given in figure (11), (12) and (13) are diagrams that display normalization in three various accelerometers. We have provided the behavior of x, y and z axes of three various accelerometers.

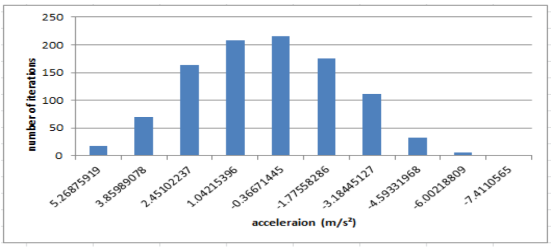


(a)

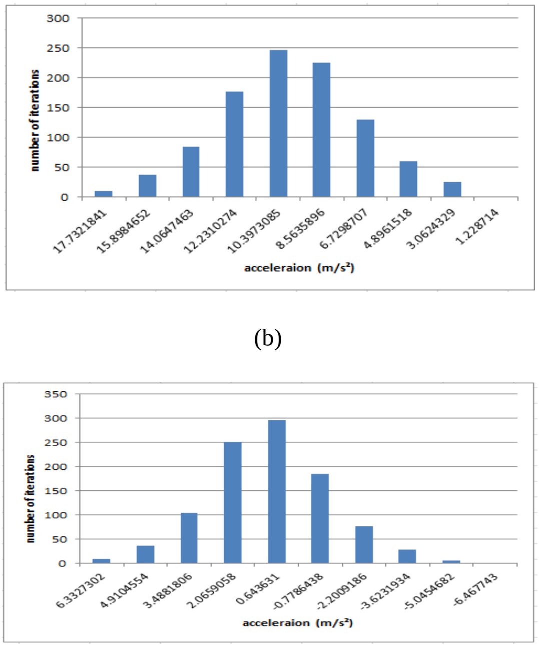
(b)

(c)

Figure 11. (a) graph of x-axis (b) graph of x-axis (c) graph of x-axis of reading acquired from three various accelerometer sensors.



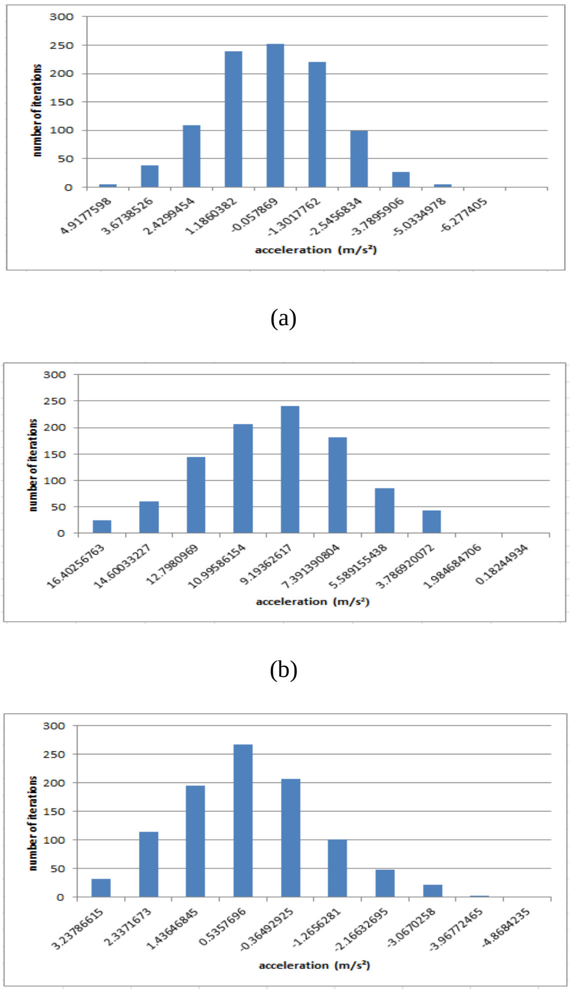
(a)



(b)

(c)

Figure 12. (a) graph of y-axis (b) graph of y-axis (c) graph of y-axis of reading acquired from three various accelerometer sensors.



(a)

(b)

(c)

Figure 13. (a) graph of z-axis (b) graph of z-axis (c) graph of z-axis of reading acquired from three various accelerometer sensors.

The analysis in this experience displays that the readings are singular for every sensor. Our experiment show that each sensor has a singular bias which can be exploited to produce the device ICMetric. The x-axis readings for the graph a, b and c in the figure 5 are different. Similar results are displayed in (y, z) axes diagrams in 6 and 7 figures. The diagrams display that each sensor owns a dissimilar bias even at the same axis. Every sensor will produce single statistical and mathematical findings. A statistical analysis is required to verify that there is adequate bias necessary to apply ICMetric. A statistical analysis of the value acquired from the magnetometer, gyroscope and accelerometer indicates that every sensor presents a single bias.

Table 1, table 2 and table 3 show the metrics for the diagrams applied in figure 5, figure 6 and figure 7 respectively.

Table 1. X-axis statistical analysis for two separate magnetometers

	X-axis	
	Magnetometer1	***Magnetometer2***
Confidence interval	(-102.499,103.005)	(-102.521,-103.018)
Mean	-102.7524674	-102.7699637
Standard Deviation	4.086745963	4.015104407
Skewness	-0.024220124	0.065459667

Table 2. Y-axis statistical analysis for two various magnetometers

	Y-axis	
	Magnetomete1	***Magnetometer2***
Confidence interval	(-72.3290,-72.7858)	(-72.5730,-73.0026)

Mean	-72.55744499	-72.78785363
Standard Deviation	3.684409234	3.466054182
Skewness	0.126656585	-0.016225336

Table 3. Statistical analysis of z-axis for two various magnetometers

	Z-axis	
	Magnetomet1	***Magnetometer2***
Confidence interval	(60.2369,59.9063)	(60.37434,60.0407)
Mean	60.07166967	60.20756554
Standard Deviation	2.666794659	2.690850552
Skewness	0.016271328	-0.04191755

Table 4, table 5 and table 6 show the metrics for the graphs shown in figure 7, figure 8 and figure 9 respectively.

Table 4. Statistical analysis of x-axis for two various gyroscopes

	X-axis	
	Gyroscope-1	***Gyroscope-2***
Confidence interval	(-0.2798,-0.4109)	(-167.049,-167.199)
Mean	-0.34538804	-167.12482
Standard Deviation	1.057460501	1.211160058
Skewness	-0.109740322	0.641566849

Table 5. Statistical analysis of y-axis for two various gyroscopes

	Y-axis	
	Gyroscope-1	***Gyroscope-2***
Confidence interval	(-0.1644,-0.4057)	(-530.354,530.534)
Mean	-0.285080131	-0.530444435
Standard Deviation	1.946444674	1.458852046
Skewness	-0.072086021	0.215075162

Table 6. Statistical analysis of z-axis for two various gyroscopes

	Z-axis	
	Gyroscope-1	***Gyroscope-2***
Confidence int.	(0.1943,0.1086)	(0.2285,0.0459)
Mean	0.151523562	0.137225
Standard dev.	0.691476508	1.473156
Skewness	0.161009518	0.115859

Table 7, table 8 and table 9 show the metrics for the graphs shown in figure 11, figure 12 and figure 13 respectively.

Table 7. Statistical analysis of x-axis for two various accelerometers

	X-axis	
	Accelerometer1	***Accelerometer2***
Confidence interval	(8.1775,7.8487)	(9.3159,9.0025)
Mean	8.01314065	9.159219616
Standard Deviation	2.652895942	2.527947461
Skewness	0.370291516	0.100232538

Table 8. Statistical analysis of y-axis for two various accelerometers

	Y-axis	
	Accelerometer1	***Accelerometer2***
Confidence interval	(-0.4973,0.7851)	(0.0907,-0.0867)
Mean	-0.641291534	0.002032883
Standard Deviation	2.321628014	1.431675069

Skewness	0.033822549	-0.211393438

Table 9. Statistical analysis of z-axis in two various accelerometers

	Z-axis	
	Accelerometer1	***Accelerometer2***
Confidence interval	(1.2297,-2.5300)	(-0.9237,0.9242)
Mean	-4.404250862	-0.923983764
Standard Deviation	2.831670337	0.004253021
Skewness	-1.020575945	0.150220506

X. Experimental Results

MEMS sensors were utilised to apply ICMetric numbers utilized for providing intelligent wheelchair identification. For the generation of ICMetric number**,** the bias readings are achieved by each three magnetometers, gyroscope and accelerometer sensors and 1000 readings were detailed for three separate axes. Through the training and testing support vector machine with (Misuse Detection), we applied the same dataset in both phases to evaluate the proposed system performance. In the testing phase, the extracted data is exploited for testing the facility of the ICMetric security system in alarms detection. The four types of alarms True Positive (TP), False Positive (FP), True Negative (TN) and False Negative (FN) also the accuracy of alarms detection is specified to evaluate the performance of the proposed ICMetric security system. The system accuracy result should be calculated as follows [32]:

$$accuracy = \frac{Nu\text{循}ber\ of\ instances\ classified\ correctly}{Total\ number\ of\ the\ instances}$$

The measures will be applied as given below [33-38]:

$TP = normal\ behavior\ classified\ as\ normal$
$TN = attack\ behavior\ classified\ as\ attack$
$FP = normal\ behavior\ classified\ as\ attack$
$FN = attack\ behavior\ cla\ \blacksquare sified\ as\ \blacksquare ormal$
then

$$TP_{rate} = \frac{TP}{TP+FN} \qquad (5)$$

$$TN_{rate} = \frac{TN}{TN+FP} \qquad (6)$$

$$FN_{rate} = \frac{FN}{FN+TP} \qquad (7)$$

$$FP_{rate} = \frac{FP}{FP+TN} \qquad (8)$$

The results of alarms rate are applied in table 10, when the system utilized ICMetric and another case for the system without ICMetric.

Table 10. Recognition rate

System without ICMetric		**System with ICMetric**	
Alarm Type	**Accuracy**	**Alarm Type**	**Accuracy**
TP	99.57%	**TP**	99.57 %
TN	99.84%	**TN**	100 %
FP	0.16	**FP**	0 %
FN	0.43%	**FN**	0.43 %

Table 11 offers the detection rate of the ICMetric security system and for the system without ICMetric.

Table 11. Detection rate.

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

The accuracy rate and rate of error are determined in order to evaluate the ICMetric system performance and the system performance without ICMetric.

Table 12. Performance metrics feature extraction

Performance Metrics	Accuracy rate	Error rate
System without ICMetric	99.75%	0.25%
System with ICMetric	99.85%	0.15%

XI. Discussion

Our proposed system using the ICMetric technology to prevent theft of the key by consuming the sensor features. The ICMetric is a key theft prevention technology and also supplies device identification. The main motivation of the proposed system is to apply identification of the device. This system is implemented by three phases: reading extraction and pre-processing phase, the training phase, and the testing phase. Sensors readings are exploited for determining the bias that utilized to provide the ICMetric number for generating a device identification.

The proposed system increases security and authentication. Comparing our results with the earlier works of the authors [32], the here ICMetric system apply a better accuracy with low false alarms rate.

XII. Conclusion

Nowadays, the use of embedded devices is required in many fields. The embedded devices are getting increasingly connected and are more and more required in network communications. Applications that belong to the network / Internet can now be implemented on embedded devices this requires protection of data from attacks or unwanted access so it is necessary to provide safety requirements for these devices. Interest in the security of embedded devices is becoming increasingly necessary every day.

In this research, we offer the usage of the ICMetric in the embedded devices. The ICMetric uses features of the device to provide an identification of device. This paper searches a device ICMetric generation by exploiting the MEMS magnetometer, gyroscope and accelerometer located in several embedded devices. We consume the established magnetometer, gyroscope and accelerometer in myAHRS_plus sensor to create a device ICMetric. To extract the magnetometer, gyroscope and accelerometer bias, an intelligent wheelchair application is essential which is prepared with the sensors. In our experience, we achieve three readings axes by every sensor.

Reading generated from the sensors are analyzed statistically to generate triple ICMetric numbers utilized for device identification. A statistical analysis of readings for the sensor shows practical to employ the MEMS magnetometer, gyroscope and accelerometer for a device identification generation. System security can be improved by combining other features of device. Accuracy rate of the proposed system equal to 99.85 where the error rate is 0.15% this make the ICMetric security system is helpful and efficient for detection of alarms with a high rate of accuracy and a low rate of false positive alarm.

References

[1] W. Stallings, (2016) *Foundations of Modern Networking*. Dave Dusthimer.

[2] R. Tahir, H. Hu, D. Gu, K. McDonald-Maier, and G. Howells, (2013) A scheme for the generation of strong icmetrics based session key pairs for secure embedded system applications. *2013 27th Int. Conf. Adv. Inf. Netw. Appl. Work.*, no. March 2013, pp. 689–696.

[3] L. Khelladi, Y. Challal, A. Bouabdallah, and N. Badache, (2008) On security issues in embedded systems: challenges and solutions. *Int. J. Inf. Comput. Secur.*, vol. 2, no. 2, p. 140.

[4] E. Papoutsis, G. Howells, A. Hopkins, and K. Mcdonald maier, (2007) Integrating Multi-Modal Circuit Features within an Efficient Encryption System. *Third Int. Symp. Inf. Assur. Secur.*, pp. 83–88.

[5] E. Papoutsis, G. Howells, A. Hopkins, and K. Mcdonald-maier, (2009) Ensuring Secure Healthcare Communications via ICmetric based Encryption on unseen Devices. *2009 Symp. Bio-inspired Learn. Intell. Syst. Secur.*, pp. 113–117.

[6] R. Tahir and K. Mcdonald-maier, (2012) Improving Resilience against Node Capture Attacks in Wireless Sensor Networks using ICmetrics. *2012 Third Int. Conf. Emerg. Secur. Technol.*.

[7] H. Tahir, R. Tahir, and K. Mcdonald-maier, (2015) Securing MEMS Based Sensor Nodes in the Internet of Things. *2015 Sixth Int. Conf. Emerg. Secur. Technol. Secur.*, no. 2015 Sixth Int. Conf. Emerg. Secur. Technol. Secur., pp. 44–49.

[8] H. Tahir and K. Mcdonald-maier, (2015) Securing Health Sensing Using Integrated Circuit Metric. *Sensors 2015, 15, 26621-26642; doi10.3390/s151026621*, pp. 26621–26642.

[9] K. M. A. Alheeti and K. McDonald-Maier, (2015) An intelligent intrusion detection scheme for self-driving vehicles based on magnetometer sensors. in *2016 International Conference for Students on Applied Engineering, ICSAE 2016*, pp. 75–78.

[10] K. M. A. Alheeti, R. Al-Zaid, J. Woods, and K. McDonald-Maie, (2017) "An Intrusion Detection Scheme for Driverless Vehicles Based Gyroscope Sensor Profiling," *2017 IEEE Int. Conf. Consum. Electron.*, pp. 2–3.

[11] S. Yadav, (2017) Analysis of ICMetrics Features / Technology for Wearable Devices IOT Sensors. in *2017 Seventh Int. Conf. Emerg. Secur. Technol.*, pp. 175–178.

[12] H. Tahir, R. Tahir, and K. Mcdonald-maier, (2018) On the security of consumer wearable devices in the Internet of Things. *PLoS One*, pp. 1–21.

[13] H. Tahir, G. Howells, H. Hu, D. Gu, and K. Mcdonald-maier, (2014) On Secure Group Admission Control Using ICMetrics. *2014 Fifth Int. Conf. Emerg. Secur. Technol.*, pp. 82–87.

[14] M. T. Shahzaib Tahir, Mehreen Afzal, (2014) An ICMetric based Key Generation Scheme for Controlled Group Communication. in *IISA 2014, 5th Int. Conf. Information, Intell. Syst. Appl. Chania, 2014*, pp. 373–378.

[15] X. Zhai, K. Appiah, and S. Ehsan, (2013) Application of ICmetrics for Embedded System Security. in *2013 Fourth Int. Conf. Emerg. Secur. Technol.*, pp. 4–7.

[16] A. Kokosy, M. Pepper, and C. Donzé, (2012) SYSIASS – an intelligent powered wheelchair. *Int. Conf. Syst. Comput. Sci. Sep 2012, Lille, Fr.*, no. August.

[17] Z. Wu, (2018) Magnetometer and Gyroscope Calibration Method with Level Rotation. *Sensors*.

[18] Y. Cai, Y. Zhao, X. Ding, and J. Fennelly, (2012) Magnetometer basics for mobile phone applications. *Electron. Prod. (Garden City, New York)*, vol. 54, no. 2.

[19] G. Troni and R. M. Eustice, (2014) Magnetometer bias calibration based on relative angular position: Theory and experimental comparative evaluation. *IEEE Int. Conf. Intell. Robot. Syst.*, pp. 444–450.

[20] A. V. Rao D, Natrajan P, Ahmed R, (2013) Onboard estimation and correction of magnetometer bias in MEMS based Tri axial Inertial Measurement Unit. *9th Int. Conf. Intell. Unmanned Syst.*, no. September 2013, p. ICIUS 2013 274.

[21] D. Ren, L. Wu, M. Yan, M. Cui, Z. You, and M. Hu, (2009) Design and analyses of a MEMS based resonant magnetometer. *Sensors*, vol. 9, no. 9, pp. 6951–6966.

[22] B. Preethi, L. Sujatha, and V. S. Selvakumar, (2013) Design and Analysis of MEMS Gyroscope. *2012 COMSOL Conf. bangalore*.

[23] V. M. N. Passaro, A. Cuccovillo, L. Vaiani, M. De Carlo, and C. E. Campanella, (2017) Gyroscope Technology and Applications : A Review in the Industrial Perspective. *Sensors*.

[24] M. T. Scholar, (2015) Wheel-Chair Control Using Accelerometer Based Gesture Technology. in *Int. J. Adv. Res. Comput. Eng. Technol.*, vol. 4, no. 5, pp. 1802–1806.

[25] R. Vemal *et al.*, (2009) MEMS vs .

IC Manufacturing: Is Integration Between Processes Possible. in *2009 1st Asia Symp. Qual. Electron. Des.*, no. M, pp. 3–7.

[26] D. J. Fonseca and M. Sequera, (2011) On MEMS reliability and failure mechanisms. in *Int. J. Qual. Stat. Reliab.*, vol. 2011.

[27] H. Tahir. (2017) AN ICMETRIC BASED MULTIPARTY COMMUNICATION FRAMEWORK. thesis (PhD.), University of Essex.

[28] T. Van Goethem, W. Scheepers, D. Preuveneers, and W. Joosen, (2016) Accelerometer-Based Device Fingerprinting for Multi-factor Mobile Authentication. *springer*, pp. 106–121.

[29] M. A. Haseeb *et al.*, (2018) Head Gesture-based Control for Assistive Robots. *11th ACM Int. Conf. PErvasive Technol. Relat. to Assist. Environ. (PETRA), Corfu Greece, June 2018*, pp. 379–383.

[30] Khattab M. Ali. (2017) Intrusion Detection System in External Communication for Self-Driving Vehicles. thesis (PhD.), University of Essex.

[31] David Leblanc, (2004) *Statistics: Concepts and Applications for Science*. Jones & Bartlett.

[32] K. M. A. Alheeti, A. Gruebler, and K. D. Mcdonald-maier, (2015) An Intrusion Detection System Against Malicious Attacks on the Communication Network of Driverless Cars. *IEEE 12th Consum. Commun. Netw. Conf. 2015*, pp. 916–921.

[33] G. Kumar, (2014) Evaluation Metrics for Intrusion Detection Systems - A Study. *Int. J. Comput. Sci. Mob. Appl.*, l. 2, pp. 11–17.

[34] K. M. Ali Alheeti, L. Al-Jobouri, and K. McDonald-Maier, (2013) Increasing the rate of intrusion detection based on a hybrid technique. in *2013 5th Comput. Sci. Electron. Eng. Conf. CEEC 2013 - Conf. Proc.*, pp. 179–182.

[35] K. M. A. Alheeti, A. Gruebler, and K. D. Mcdonald-maier, (2015) An Intrusion Detection System Against Malicious Attacks on the Communication Network of Driverless Cars. in *12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, Las Vegas, pp. 916–921.

[36] K. D. M.-M. Khattab M. Ali Alheeti, Anna Gruebler, (2015) On the Detection of Grey hole and Rushing Attacks in SelfDriving Vehicular Networks. in *2015 7th Comput. Sci. Electron. Eng. Conf.*, pp. 231–236.

[37] K. M. Ali Alheeti and K. McDonald-Maier, (2016) Hybrid intrusion detection in connected self-driving vehicles. in *2016 22nd Int. Conf. Autom. Comput. ICAC 2016 Tackling New Challenges Autom. Comput.*, pp. 456–461.

[38] K. M. A. Alheeti, A. Gruebler, and K. Mcdonald-maier, (2016) Intelligent Intrusion Detection of Grey Hole and Rushing Attacks in Self-Driving Vehicular Networks. in *Comput. 2016*, vol. 16, pp. 12–14.

参考文:

[1] W. Stallings, (2016) 现代网络基础 Dave Dusthimer

[2] R. Tahir, H. Hu, D. Gu, K. McDonald-Maier 和 G. Howells, (2013) 为安全嵌入式系统应用生成基于强 icmetrics 的会话密钥对的方案 2013 年第 27 届国际 CONF 进阶天道酬勤 网络 申请工作, 不 2013 年 3 月, 第 689-696 页

[3] L. Khelladi, Y. Challal, A. Bouabdallah 和 N. Badache, (2008) 关于嵌入式系统中的安全问题：挑战和解决方案诠释 J. Inf COMPUT Secur, vol 2, 没有 2, p. 140

[4] E. Papoutsis, G. Howells, A. Hopkins 和 K. Mcdonald maier, (2007) 在多个高效加密系统中集成多模态电路特性

第三国际 SYMP 天道酬勤 亚述 Secur，第83-88页

[5] E. Papoutsis，G. Howells，A. Hopkins 和K. Mcdonald-maier， (2009) 通过基于 ICmetric 的加密在看不见的设备上确保安全医疗保健通信 2009 Symp 生物启发学习 INTELL SYST Secur，第113-117页

[6] R. Tahir 和 K. Mcdonald-maier，(2012) 使用 ICmetrics 提高无线传感器网络节点捕获攻击的抵御能力 2012年第三届国际 CONF EMERG SECUR TECHNOL .

[7] H. Tahir，R。Tahir 和 K. Mcdonald-maier， (2015) 在物联网中保护基于 MEMS 的传感器节点 2015 年第六届国际 CONF EMERG SECUR TECHNOL 安全， 没有 2015 年第六届国际 CONF EMERG SECUR TECHNOL Secur， pp. 44-49

[8] Tahir 和 K. Mcdonald-maier， (2015) 使用集成电路度量标准确保健康传感传感器 2015, 15, 26621-26642; doi10.3390 / s151026621， 第 26621-26642页

[9] K. M. A. Alheeti 和 K. McDonald-Maier， (2015) 一 种基于磁力计传感器的自动驾驶车辆智能入侵检测方案 2016 年应用工程专业国际会议，ICSAE 2016， 第75-78页

[10] K. M. A. Alheeti，R. Al-Zaid，J. Woods 和 K. McDonald-Maie，(2017) “无人驾驶车辆基于陀螺仪传感器分析的入侵检测方案”， 2017 IEEE Int CONF 消费 电子，第 2-3页

[11] S. Yadav，(2017) 可穿戴设备 IOT 传感器的 ICMetrics 特性/技术分析 2017 年第七届国际 CONF EMERG SECUR Technol，pp. 175-178

[12] H. Tahir，R. Tahir 和 K. Mcdonald-maier，(2018) 关于物联网中消费者可穿戴设备的安全性 PLoS One，第1-21页

[13] H. Tahir，G. Howells，H. Hu，D. Gu 和 K. Mcdonald-maier， (2014) On Secure Group Admission Control Using ICMetrics 2014 年第五届国际 CONF EMERG SECUR Technol, pp. 82-87

[14] M. T. Shahzaib Tahir，Mehreen Afzal，(2014) 基于 ICMetric 的受控群组通信密钥生成方案 在 IISA 2014，5th Int CONF 信息，Intell SYST 申请 Chania， 2014 年，第373-378页

[15] X. Zhai，K. Appiah 和 S. Ehsan, (2013) ICmetrics for Embedded System Security 的应用 2013年第四届国际 CONF EMERG SECUR 技术，第 4-7页

[16] A. Kokosy，M. Pepper 和 C.Donzé，(2012) SYSIASS - 智能动力轮椅 诠释 CONF SYST COMPUT 科学 2012 年 9 月，里尔，神父，没有八月

[17] Z. Wu， (2018) 具有水平旋转的磁强计和陀螺仪校准方法 传感器

[18] Y. Cai，Y. Zhao，X. Ding 和 J. Fennelly, (2012) Magnetometer baseics for mobile phone applications 电子 PROD (纽约花园城)， 第一卷，54，不 2

[19] G. Troni 和 R. M. Eustice，(2014) 基于相对角位置的磁强计偏差校准：理论和实验比较评估 IEEE Int CONF INTELL 机器人 Syst，pp.444-450

[20] A. V. Rao D，Natrajan P，Ahmed R，(2013) 基于 MEMS 的三轴惯性测量单元中的磁力计偏差的板载估计和校正 第 9 届国际 CONF INTELL 无人系统，没有 2013 年 9 月，p. ICIUS 2013 274

[21] D. Ren，L. Wu，M. Yan，M. Cui，Z. You 和 M. Hu，(2009) 设计和分析基于 MEMS 的谐振磁强计传感器，第一卷 9，不 9，pp. 6951-6966

[22] B. Preethi，L. Sujatha 和 V. S. Selvakumar，（2013）MEMS 陀螺仪的设计和分析 2012 COMSOL Conf 班加罗尔

[23] V.M.N. Passaro，A. Cuccovillo，L.Vaiani，M. De Carlo 和 C. E. Campanella，(2017) 陀螺仪技术与应用：工业视角的回顾 传感器

[24] M. T. Scholar，(2015) 使用基于加速度计的手势技术的轮椅控制在

国际 J. Adv RES COMPUT 工程 Technol，vol 4，不 5，pp. 1802-1806

[25] R. Vemal 等人，(2009) MEMS vs. IC 制造：过程之间的整合是可能的 2009 年第一届亚洲赛事 资格赛电子 Des，没有 M，第 3-7 页

[26] D. J. Fonseca 和 M. Sequera，(2011) 关于 MEMS 可靠性和失效机理。在国际 J. Qual 统计 Reliab，vol 2011

[27] H. 塔希尔 (2017) 基于 ICMETRIC 的多方通信框架 埃塞克斯大学论文 （博士）

[28] T. Van Goethem，W. Scheepers，D. Preuveneers 和 W. Joosen，(2016) 基于加速度计的设备指纹识别用于多因素移动认证 斯普林格，第 106-121 页

[29] M. A. Haseeb 等人，(2018) 基于头部姿态的辅助控制

[30] Khattab M. Ali (2017) 自动驾驶车辆外部通信入侵检测系统。埃塞克斯大学论文（博士）

[31] David Leblanc，(2004) 统计：科学的概念和应用琼斯和巴特利特

[32] K. M. A. Alheeti，A. Gruebler 和 K. D. Mcdonald-maier，(2015)一个针对无人驾驶汽车通信网络上的恶意攻击的入侵检测系统 IEEE 第 12 次消费 COMMUN 网络 CONF 2015 年，第 916-921 页

[33] G. Kumar，(2014) 入侵检测系统评估指标 - 一项研究 诠释 J. Comput 科学 暴民 Appl，l 2，pp.11-17

[34] K. M. Ali Alheeti，L. Al-Jobouri 和 K. McDonald-Maier，(2013) 提高基于混合技术的入侵检测率 2013 年第五届 Comput 科学 电子 工程 CONF CEEC 2013 - 会议 Proc，pp.179-182

[35] K. M. A. Alheeti，A. Gruebler 和 K. D. Mcdonald-maier，(2015)一种针对无人驾驶汽车通信网络恶意攻击的入侵检测系统 第 12 届 IEEE 消费者通信和网络会议 (CCNC)，拉斯维加斯，第 916-921 页

[36] K. D. M.-M. Khattab M. Ali Alheeti，Anna Gruebler，(2015) 关于 SelfDriving 车载网络中灰洞和冲击攻击的检测 2015 年第 7 届 Comput 科学电子 工程 Conf，pp.231-236

[37] K. M. Ali Alheeti 和 K. McDonald-Maier，(2016) 混合入侵检测在连接的自动驾驶车辆中 2016 年第 22 届国际 CONF 奥波 COMPUT ICAC 2016 应对新挑战 Autom Comput，pp.456-461

[38] K.M.A. Alheeti，A. Gruebler 和 K. Mcdonald-maier，(2016) 自动驾驶车载网络中灰洞和冲击攻击的智能入侵检测。在 Comput 2016 年，第一卷 16，pp.12-14