A Comparison Study for Intelligent Wheelchair Based on MEMS Sensors

IOP Conf. Series: Materials Science and Engineering **928** (2020) 032075 doi:10.1088/1757-899X/928/3/032075

A Comparison Study for Intelligent Wheelchair Based on MEMS Sensors

Duaa Abdul Satar Al_Dosary
College of Computer and Information Technology
Computer Sciences Department
University of Anbar, Anbar -Iraq
mobileip39@gmail.com

Khattab M Ali Alheeti
College of Computer and Information Technology
Computer Networking Systems Department
University of Anbar, Anbar -Iraq
co.khattab.alheeti@uoanbar.edu.iq

Salah Sleibi Al-Rawi
College of Computer and Information Technology
Information Systems Dept., University of Anbar, Anbar -Iraq
dr_salah_rawi@yahoo.com
Abstract— Today, the security of the system must be improved. A new approach is proposed that achievements the Integrated Circuit Metrics (ICMetric) technology to support identification of devices. ICMetric is a novel technology that generates the identification of devices based on the internal behavior of device features. In this paper, a comparative study is presented between two of our systems. These protection systems are designed to provide protection systems for intelligent wheelchairs. However, we proved that node identification can be provided by utilizing the three types of MEMS sensors. Extracted readings are acquired from the sensors and analyzed mathematically and statistically to provide an ICMetric basis that used to introduce identification of the device. Simulation results show that the proposed system can increase authentication and security.
Index Terms—*Security; MEMS sensor; ICMetric; intelligent wheelchair.*

I. Introduction

Currently, people with spinal cord harm are depending on using wheelchairs to facilitate their lives [1]. To ensure effective usage of the intelligent wheelchairs and the need to protect the safety of each wheelchair it is advantageous 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.

ICMetric offered as a new method for providing unique identifiers for the devices and improve security by reducing fraudulent activity. ICMetric technology can improve secure communication between devices and reducing fraudulent activity, detection of unauthorized access to the devices and systems connected with the wheelchair [2].

In previous research [3], the authors proposed a system based on ICMetric that uses the gyroscope sensor and device features to apply vehicle identification. The presented security system displays effective performance in detecting and isolating abnormal behavior in VANETs vehicular ad-hoc networks of autonomous cars and semi-autonomous cars. In [4], a new method is proposed based on ICMetric. They are aimed to provide security in wearable devices. To achieve an improvement in the proposed system, they are depending on using two types of MEMS sensors to generate device ICMetric. Their experiment results explain that the project shows high security without compromising the demands of resources. In [5] authors utilized MEMS sensors to create ICMetric used for identification. In their research, they are aimed to achieve the security of embedded devices. They are used two types of sensors to generate ICMetric numbers.

IOP Conf. Series: Materials Science and Engineering **928** (2020) 032075 doi:10.1088/1757-899X/928/3/032075

However, the generated numbers integrated into features extracted from trace file network simulator version 2 (ns-2). Their simulation results are compared and studied for high levels of performance metrics and security.

In this paper, we are trying to compare two schemes of our methods proposed in the same research area. The first one is heavily based on two MEMS sensors whereas the second one is dependent on three MEMS sensors. All of them are utilized ICMetric technology to provide identification of devices by using features of the device itself. In our study, an important contribution is made to show us the vital role in the type and number of MEMS sensors on the security system.

In this research, we made an effort to combine ICMetric technology with an intelligent wheelchair to design a robust security system of applying identification.

This paper is organized as follows: Section II discusses the idea of security. Section III presents some details of ICMetric technology. Section IV presents some information about using MEMS sensors in intelligent wheelchairs. Security goals for applying ICMetric in an intelligent wheelchair are discussed in section V. In section VI the limitations related to ICMetrics implementation are presented. The proposed system is presented in section VII. The simulation results of our proposed system are presented in section VIII. Finally, discussion and conclusions are presented in section IX and X respectively.

II. IDEA OF SECURITY

Security goal is achieving the protection of system information to provide the availability, confidentiality, and integrity by preventing manipulation and theft of the data. It includes the protection of information, telecommunications, software, and hardware [6].

Security goals are illustrated below [6]:

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

Security is a term used to describe different states, such as a 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 organizations. Ensuring security requires individuals with competence and experience so the level of security varies from one organization to another. To ensure better security for organizations and individuals, network users need to use the systematic approach, which involves analyzing, designing, implementing, and maintaining a required network security system [7].

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.

III. INTEGRATED CIRCUIT METRIC TECHNOLOGY

The identification of the device is created to eliminate the theft of data by depending on the special features of each device. 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 [8].

ICMetric technology uses hardware and software features of the device to create ICMetric numbers used for security services. There is a similarity between the ICMetric and the, as ICMetric uses the characteristics of the device to identify each device uniquely and thus eliminates and deters the theft of stored keys. Similarly, biometric systems used features for the identification of different persons [9].

The generation of the ICMetric system is required two phases, which are the calibration phase and operation phase [5]. In the calibration phase, the characteristics are documented and analyzed, normalization distributions are utilized 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 utilized once only when the system needs the ICMetric basis number.

In the operational 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.

ICMetrics is involved in the following:

1. The number generated during ICMetric processes is not stored 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. No requirements to store any template for device validating.
4. ICMetric number will be changed if any adjusting done with the software, hardware, or environment.

IV. USING MEMS SENSORS IN INTELLIGENT WHEELCHAIRS

MEMS sensors have many applications in measuring either acceleration or angular velocity about one or several axes as an input to control a system [10]. 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. The ultrasonic sensors control the movement of the wheel-chair in the left, right forward, and reverse direction by the detection of an obstacle. This wheel-chair turns the movement of its direction when detects an obstacle in its path.

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. The magnetometer sensor measures the magnetic fields based on Hall Effect.

The MEMS gyroscope sensor provides an angular velocity of the wheelchair's wheel. Angular velocities are used to define distances traveled and linear speeds to present real-time feedback of wheelchair users.

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 utilized as identification for the device. Current research in the sensor-based identification field has proved that the use of sensory data is possible and that it is feasible to provide device identification.

V. SECURITY GOALS FOR APPLYING ICMETRIC IN AN INTELLIGENT WHEELCHAIR

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. While many security techniques are now developed, these cannot necessarily defend against unauthorized activity when security and safety cannot be assured.

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

In this research, features are extracted from the gyroscope, magnetometer and accelerometers sensors to the describe behavior of intelligent wheelchairs. The offset is utilized in the sensor measurement for generating an ICMetric basis number by 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 an 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.

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

ICMetric technology can improve secure communication between devices and reducing fraudulent activity, detection of unwanted access to the devices, and systems connected with the wheelchair.

VI. LIMITATIONS RELATED TO ICMETRICS IMPLEMENTATION

ICMetric technology has some limitations, which can be presented below:

1. Readings extraction from sensors is another limitation. The sensor must be placed on a place that is stable and free from movements and vibrations to achieve correct readings.
2. An essential requirement for the generation of the proposed ICMetric is that the aimed device must be embedded with MEMS sensors. This situation restricts the researcher to a particular type of device.

3. The stability of the ICMetric number is one of the limitations that depends on several factors, such as the number of sensors available for applying readings and the environment of their operation, features employed, and mathematical equations.
4. The entropy and length of the generated ICMetric number is a limitation of the proposed ICMetric. The proposed system generates a strong ICMetric number in order to apply device identification for more security of the system.

VII. THE PROPOSED SYSTEM

Bias readings extracted from MEMS sensors embedded in an intelligent wheelchair are utilized in this proposed system. These readings utilized to create an ICMetric number that was integrated into the dataset generated from the trace file of the simulator for intelligent wheelchair identification.

Our systems are dependent on utilizing ICMetric technology that exploits device features to generate a unique number called ICMetric number, which used for device identification. The proposed system has two schemes, which are:

1. Two ICMetric numbers are generated by exploiting bias readings extracted from two types of MEMS sensors, which are magnetometer and gyroscope sensors.
2. Three 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 utilized in the dataset extracted from the text file that has been extracted by the simulator to perform detection and identification.

There are many stages of our system is illustrated in figure 1, and those are:

- Extracting bias reading from sensors and generate ICMetric numbers. In this phase, we extracted the bias from the MEMS sensors on an intelligent wheelchair. Some mathematical lightweight operations are applied bias reading from the sensor to generate ICMetric numbers used for identification.
- The trace file is generated by using network ns-2. Datasets used in this system is achieved from the trace file of ns-2. ICMetric numbers will be integrated into the dataset for identification.
- Pre-processing is very necessary for the proposed system. such as some non-numerical should be transferred to numbers to create the ICMetric-security system performance more effectively in identification, stopping abnormal behavior, and improve ICMetric security.
- Support Vector Machine (SVM) is utilized in the training phase. The SVM is trained with an extracted dataset for creating the ICMetric system.
- The testing phase is to determine the rate of accuracy and four types of alarms.

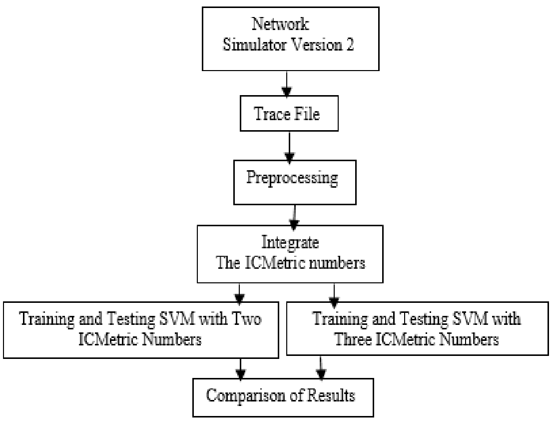

Fig. 1: Architecture of the proposed System

VIII. SIMULATION RESULTS

Some statistical analysis is required to generate ICMetric number. Statistical analysis involves applying the confidence interval, mean value, standard deviation, of the normal distribution [8]. In this experiment, some statistical and mathematical function is applied for the generation of ICMetric numbers.

IOP Conf. Series: Materials Science and Engineering **928** (2020) 032075 doi:10.1088/1757-899X/928/3/032075

The dataset used in this research is generated from the text file. Some pre-processing is employed on generated significant features. In this case, training and testing datasets are ready for the performance measurement of our identification method. Cross-validation employed for SVM to test the efficiency of the suggested protection scheme. However, the extracted datasets are split into two groups which are the training phase and testing phase. This process will be frequent to calculate system performance. Table 1 shows the accuracy rate and error rate of the proposed system.

TABLE 1 COMPARISON FOR PERFORMANCE METRICS

Class	**Accuracy**	**Error Rate**
The First Scheme	99.77%	0.23%
The Second Scheme	99.85%	0.15%

The accuracy rate and four types of alarms are utilized as metrics to test the efficiency of the proposed system. Accuracy is calculated as following [11]:

$$Accuracy = \frac{\text{Number of correctly classified records}}{\text{Total number of records}} \quad (1)$$

Alarm types, which are: True Positive (TP), False Positive (FP), True Negative (TN) and False Negative (FN) calculated as follows [12] [13]: Let

TP = normal connection record classified as normal

TN = attack connection record classified as attack

FP = normal connection record classified as attack

FN = attack connection record as normal
then:

$$TP_{Rate(\text{sensitivity})} = \frac{TP}{TP + FN} \quad (2)$$

$$TN_{Rate(\text{specificity})} = \frac{TN}{TN + FP} \quad (3)$$

$$FN_{Rate(1-\text{sensitivity})} = \frac{FN}{FN + TP} \quad (4)$$

$$FP_{Rate(1-\text{specificity})} = \frac{FP}{FP + TN} \quad (5)$$

Alarms are calculated for performance evaluation of the two schemes in the proposed system. The experimental results are presented in Table 2:

TABLE 2 ALARMS RATE

Alarm Type	**The First Scheme**	**The Second Scheme**
TP	99.57%	99.57%
TN	99.88%	100%
FN	0.43%	0.43%
FP	0.12%	0%

Table 3 shows the detection rate of the two schemes in the proposed.

TABLE 3 COMPARISON FOR PERFORMANCE METRICS

Performance Metrics	Detection Rate		
	Normal	**Abnormal**	**Average**
System with the first scheme	99.5%	99.88%	99.69%
System with the second scheme	99%	100%	99.5%

According to table 3, the first method in the proposed system that depends on bias readings extracted from magnetometer and gyroscope sensors can achieve significant security improvement on the external communication system.

IX. DISCUSSION

In this paper, our proposed system shows that is capable of identification of the devices. The results are compared with the previous research of the authors [14], the previous works utilized one sensor to provide ICMetric number. In our experiment, we used three types of MEMS sensors. Our proposed system applies a low error rate with a better rate of accuracy. According to tables 1, 2, and 3, we can observe that the second scheme in the proposed system makes slight changes in the results when compared with the first scheme. The results exhibit that it is possible to be satisfied with three sensors for identification.

X. CONCLUSION

A comparison study is presented in this paper to shown the role number and MEMS sensors on the security system based on ICMetric technology. The security of the system can be improved by combining other features of the device.

In this experimental setup, MEMS sensors are used because they are readily available and also because the required stimulus is easy to create. Readings generated from MEMS sensors are analyzed statistically to generate ICMetric number utilized for device identification. ICMetric number is integrated into the dataset extracted from the ns-2 trace file. SVM is efficient, effective with a low error rate in improving the detection rate. For system evaluation, performance metrics are calculated, which are accuracy rate, error rate, and alarm types. The first method in the proposed system based on bias readings generated from magnetometer and gyroscope sensors provides a 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 a better accuracy rate was at 99.85% and the lower error rate was at 0.15%.

REFERENCES

[1] D. Kokosy, Anne-Marie , Floquet, Thierry , Howells, Gareth , Hu, Huosheng , Pepper, Matthew G. and Sakel, Mohamed, “SYSIASS – an intelligent powered wheelchair,” *First Int. Conf. Syst. Comput. Sci. Sep 2012, Lille, Fr.*, 2012.

[2] 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.

[3] 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.

[4] H. Tahir, R. Tahir, and K. Mcdonald-maier, “On the security of consumer wearable devices in the Internet of Things,” *PLoS One*, vol. 13(4), pp. 1–21, 2018.

[5] Duaa Al-Dosary, Khattab M Ali Alheeti and S. S. Al-Rawi “ICMetric Security System for Achieving Embedded Devices Security, acceped in” *ISCUB-2019 Int. Sci. Conf. Univ. Babylon*, p. 2019, 2019.

[6] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5th ed. Stallings William, 2011.

[7] M. Alshahrani and H. Teymourlouei, “Network Security : Threats and Vulnerabilities,” *Int’l Conf. Secur. Manag.*, pp. 115–121, 2016.
[8] H. Tahir and K. Mcdonald-maier, “Securing Health Sensing Using Integrated Circuit Metric,” *Sensors 2015*, vol. 15, pp. 26621–26642, 2015.
[9] 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.
[10] G. Sensors, “Accelerometer and Gyroscopes Sensors: Operation, Sensing, and Applications,” *maxim Integr.*, pp. 1–11, 2014.
[11] and M. S. A. R. M. Khattab Ali, W. Venus, “The Affect of Fuzzification on Neural Networks Intrusion Detection System,” *IEEE Comput. Soc.*, 2009.
[12] Khattab M. Ali, “Intrusion Detection System in External Communication for Self-Driving Vehicles,” University of Essex, 2017.
[13] D. Al_Dosary, K. M. A. Alheeti, and S. S. Al-Rawi, “An ICMetric Security System for Intelligent Wheelchairs Based on Triple MEMS Sensors,” *J. Southwest Jiaotong Univ.*, vol. 54, no. 3, 2019.
[14] K. M. A. Alheeti, A. Gruebler, and K. D. Mcdonald-maier, “An Intrusion Detection System Against Malicious Attacks on the Communication Network of Driverless Cars,” *IEEE 12th Consum. Commun. Netw. Conf. 2015*, pp. 916–921, 2015.