ICMetric Security System for Achieving Embedded Devices Security

ICMetric Security System for Achieving Embedded Devices Security

Duaa Al_Dosary[1], Khattab M Ali Alheeti[2], Salah Sleibi Al-Rawi[3]

[1]College of Computer and Information Technology, Computer Sciences Department, University of Anbar, Anbar -Iraq.

[2]College of Computer and Information Technology, Computer Networking Systems Department, University of Anbar, Anbar -Iraq

[3]College of Computer and Information Technology, Information Systems Dept., University of Anbar, Anbar -Iraq

mobileip39@gmail.com
co.khattab.alheeti@uoanbar.edu.iq
dr_salah_rawi@yahoo.com

Abstract. The interesting with embedded systems is related to the matters of providing privacy and security. There is a need to ensure the integrity and authenticity of the system. The methods such as passwords can be stolen or forgotten therefore the security of any data kept on the system can be exposed by any unauthorised access. In this paper, a new proposal is introduced that exploits Integrated Circuit Metrics (ICMetric) technology to provide identification and improve system security. ICMetric generates device identification based on the features of a device. In this paper, device identification can be generated by using the MEMS sensors, which are gyroscope and magnetometer embedded in many devices. The experiment is based on sensors embedded in intelligent wheelchair. Readings are obtained from the sensors and analysed mathematically and statistically to generate ICMetric number that used to provide identification of the device. ICMetric number is integrated to the dataset extracted from the trace file generated by network simulator version two (ns-2). If the system is attacked, there will be no theft because the ICMetric is not stored on the system and can be regenerated when necessary. The proposed system shows that the using of MEMS sensors to generate ICMetric number increase authentication and security of the system. The simulation results have been compared and studied for high levels of performance metrics and detection capability.

Keywords. ICMetric, identification, MEMS sensors, security, embedded systems.

1. Introduction

Embedded systems spread in many applications of different fields such as telecommunications, smart cards, and satellite systems. Embedded systems find in the healthcare field in many applications such as medical intelligent wheelchair application to provide many services to users in different ways and to eliminate the user's responsibility for moving the wheelchair. Intelligent wheelchair is presented in the figure 1.

Figure 1. Intelligent wheelchair [1].

In western countries, the users of the wheelchair are increasing expected at 60-200 per 10,000 in the last decade. The number of users is expected to grow with increased survival from neurological situations where people with spinal cord injury are expected to rely on using a wheelchair for the rest of their lives. The capability to move with no need for human help may be useful to patient care, reintegration into society and independence. For supporting older people, care should be provided by using intelligent wheelchair services [2].

One of the major challenges with embedded systems is related to the issues of privacy, safety, and security. There is a need to ensure the integrity and authenticity of the system. There is a method such as passwords that can be stolen or forgotten. And, private keys of encryption have to be stored, the security of any data kept on the system can be exposed by any unauthorized access to them [3]. In this paper, a new proposal is introduced that exploits ICMetric technology to provide identification and improve system security. This paper study how identification can be generated by using ICMetric technology, which exploiting values gained from MEMS sensors. ICMetric technology uses characteristics of device to improve security. The features are acquired from sensors to describe behaviour of intelligent wheelchairs such as the gyroscope and magnetometer. The offset is used in sensor measurement to propose a security system that applies an ICMetric basis number using sensor bias readings.

ICMetric technology is distinguished with some properties make it traverse weaknesses in another security system. ICMetric number can be regenerated when required and is not stored on the system. There will be no theft if the system attacked because the ICMetric is non-store. ICMetric system generation is involved in two phases which are the calibration phase to collect feature from the device and then generate the unimodal distributions for every feature. Statistical values are created from the unimodal distribution serve for ICMetric creation. The second phase is the operation phase that uses the statistical values produced by the calibration phase to generate ICMetric number [4].

Several researchers offer a complete framework about security that is made on ICMetric technology. This section shows the previous studies related to this work. Hasan T. et al. proposed a system based on Integrated Circuit Metric (ICMetric) technology for presenting security in wearable devices. They are used gyroscope and accelerometer sensors to provide device identification which is then used for applying services like the authentication, confidentiality, secure admission, and symmetric key generation [4]. Yevgeniya K. and Gareth H. suggested a technology, which useful for the healthcare environment. They were aiming to integrate ICMetric technology into an autonomous and intelligent wheelchair. The ICMetric technology is based on gaining encryption keys from the characteristics of performance for electronic systems. The main benefit of the proposed technology is that it is used a template-free encryption model for defending electronic systems and data exchange [5]. Hasan T. et al. proposed a system uses health sensors provided with the accelerometer. They have used values achieved from the accelerometer embedded in the Shimmer health sensor to provide of ICMetric number. They will use an ICMetric number for device identification [6]. Hasan T. et al. suggested a system for the supporting of security in wearable devices based on ICMetric technology that used an accelerometer and gyroscope sensor to produce device ICMetric to provide an identification [7]. Khattab M. et al.

proposed a system based on ICMetric technology that uses the MEMS gyroscope and other system features to generate a new identification of the vehicle [8].

The remainder of this paper is organized as follows: section 2 methodology of the proposed ICMetric security system; In section 3**,** experimental results are provided; Section 4 shows discussion; Finally, conclusions are mentioned in section 5.

2. Methodology

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

2.1. Establishing Simulation environment and parameters for simulation

Network Simulator Version 2 utilised for generation of communication between nodes [9]. 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 [10]. 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 2.

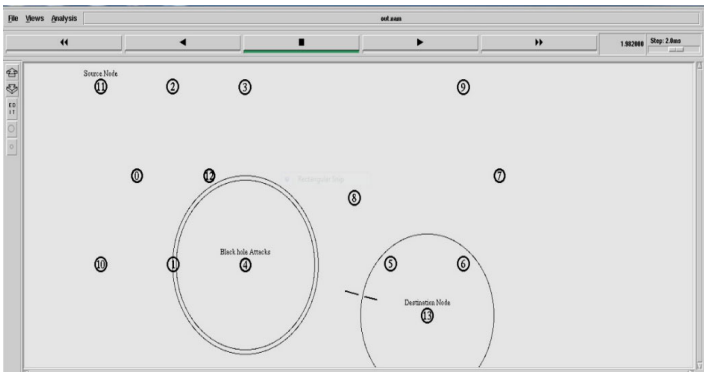

Figure 2. Screenshot of simulation in the ns-2 NAM

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 1 presents initial parameters that utilised at the proposed system.

Table 1. Initial Parameters of ns-2

Parameter	Value
Routing Protocol	AODV
Number of nodes	51 Nodes
Simulation Time	200s
Topology	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

2.2. Extracting features from the trace file

In trace file created by ns-2, analysis of nodes' behaviour is carried out to determine whether the behaviour is Black hole or normal. 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.

2.3. Pre-processing 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. Support Vector Machine (SVM) is just working with numeric values [11]. 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.

2.4. Extracting a sensor bias

MyAHRS+ sensor is applied by a 3-axis gyroscope and magnetometer sensor with a sensibility of ±16g. The myAHRS+ is considered one of the most precise sensors in the scientific research fields [12]. Several numbers of bias reading are achieved from sensor to provide ICMetric basis number. The sensor must be placed in a location free from vibrations and magnetic interface. In this experiment, every gyroscope, and a magnetometer sensor exposed to the same stimulus. 1000 individual readings are obtained from every sensor. Readings acquired from the sensors show that each sensor works differently when subjected to the same stimulus. in this research, sensors bias are proved unique also act as an implicit feature of sensors. Normal distribution for sensors shows bias readings that generated from the sensors, where each sensor owns a bias, which is unique to the sensor. The readings extracted from the sensors can be employed for providing an ICMetric basis number. In figure 3 diagrams are provided that display normalization tendency in gyroscope and magnetometer sensors.

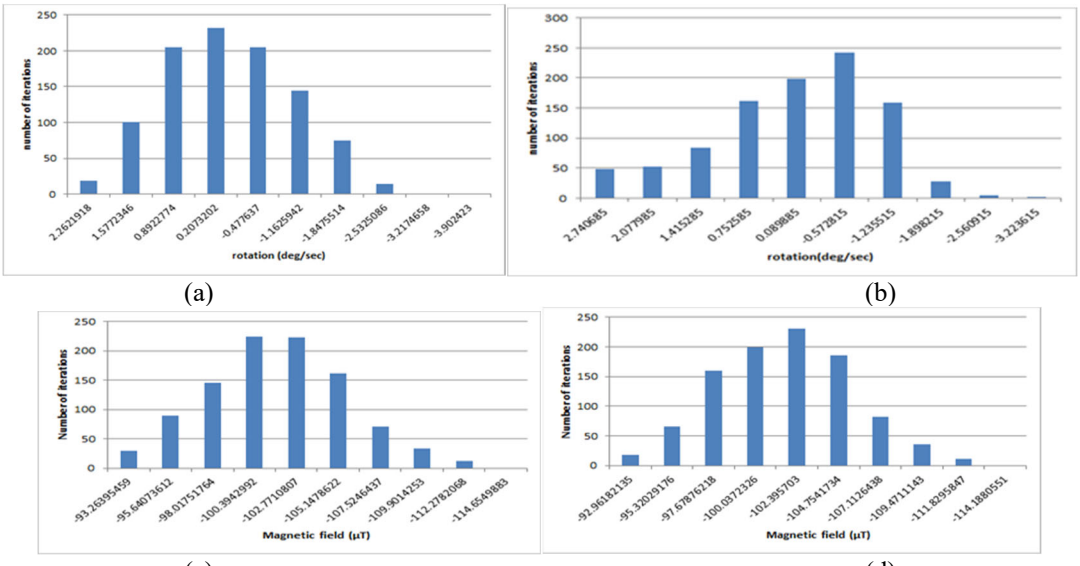

Figure 3. Unimodal distributions for two different devices evaluating x-axis (a) gyroscope (b) gyroscope (c) magnetometer (d) magnetometer.

Figure 3 presents a graphs to show that each axis presents a various bias and that there is no similarity between the sensors and no correlation between any axes. Bias extracted from gyroscope and magnetometer sensors can be utilized for generating of ICMetric number used for devices identification.

2.5. Generating ICMetric numbers

When bias readings are achieved from the sensors, a statistical and mathematical study is applied to the data acquired. Normal distributions analysis involves applying the confidence interval, interquartile range, mean value, standard deviation, skewness and the variance of the normal distribution. Probability

mass function $p(x)$ is represent an indicator for the normal distribution study. Probability mass function is provided by:

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

where σ is represent standard deviation.

The confidence interval another statistical indicator that guaranteed that the interval mean is confined in the outlines of the normal distribution. To gain satisfaction and confidence within a high level, 95% confidence interval are used for upper and lower as presented in the following equation:

$$CI = \bar{x} \pm w\frac{\sigma}{\sqrt{n}} \quad (2)$$

Where, $\bar{x}$ is represent mean of the axis, w value is 1.96 and n is represent the number of the distribution [7]. This experiment shows there are a difference in readings obtained from sensors. The difference between sensors is appropriate for ICMetric number generation. ICMetric number is integrated to the dataset extracted from the trace file generated by ns-2 for device identification.

Some statistical and mathematical function are presented in the table 2.

Table 2. Statistical analysis of the normal distribution for the first gyroscope.

Gyroscope	
Statistical functions	X-axis
Confidence Interval	(-0.27984595,-0.41093021)
Mean	0.34538804
Standard Dev	1.057460501
Skewness	0.109740322
Magnetometer	
Statistical functions	Y-axis
Confidence Interval	(-72.32908294,-72.78580704)
Mean	-72.55744499
Standard Dev	3.684409234
Skewness	0.126656585

Statistical analysis of the gyroscope and magnetometer histograms show that each sensor owns a bias, which is unique.

2.6. Integrating of ICMetric numbers to the dataset

One of the important steps of the proposed system is to generate ICMetric number. A statistical and mathematical study is applied for ICMetric basis number generation. ICMetric number is integrated to the dataset set extracted from the trace file generated by ns-2. In the proposed system, hybrid ICMetric number generated by gyroscope and magnetometer sensors and then integrated to the dataset for identification.

2.7. Training phase and testing phase

After generation of ICMetric number and integrating to the dataset, training and testing the dataset is the following phase in the proposed system. In the training phase, SVM are 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 [13].

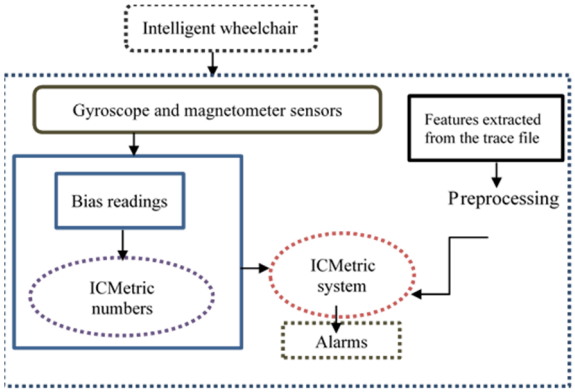

Figure 4. ICMetric security system architectural.

At first, readings are generated from the MEMS sensors for ICMetric numbers generation. Preprocessing phase is required because the features extracted from the trace file are composed from letters, symbols and numbers. In training and testing phase, SVM is just working with numeric values for this, the pre-processing phase is trying to transfer these letters and symbols to numeric values. Lightweight statistical and mathematical functions are used for ICMetric number generation. In this paper, ICMetric number is integrated to the dataset extracted from trace file that has been generated by ns-2 for device identification of intelligent wheelchair.

3. Experimental Results

In this experiment, the bias readings that were extracted from the gyroscope and magnetometer sensors are utilised in creating ICMetric security system for identification of device. The bias readings are extracted from the sensors to generate ICMetric numbers, and 1000 readings were applied for three separate axes. In the testing phase, the dataset extracted from the trace file generated by ns-2 are used to evaluate the proposed system. During the training and testing phase, SVM is utilised in the proposed system. In order to evaluate performance of the proposed system, accuracy rate of detection and error rate specified. In order to test and evaluate 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. Tables 3 shows performance metrics of the proposed ICMetric system with average accuracy rate 99.77%.

Table 3. Detection rate.

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

The proposed evaluation criteria are Packet Delivery Ratio (PDR), throughput average and end-to-end delay average are presented in table 4.

Table 4. 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

4. Discussion

The proposed system is useful and capable for providing identification of device with a low rate of false negative alarm. The proposed system that utilised ICMetric technology is compared with the system without ICMetric. The proposed ICMetric system was more effective with efficient accuracy rate and low false negative alarms rate. Rate of detection is improved by using ICMetric technology. Tables 3, 4 show a significant role of the proposed system by calculating performance metrics. Also, the results are compared with the previous research that utilised one sensor to provide ICMetric number [9]. In this

experiment, two types of MEMS sensors are used to generate ICMetric number used for identification services. The proposed system increases security and authentication, where it applies low error rate with a better rate of accuracy equal to 99.77, while the previous work applies 98.97 accuracy rate with a high rate of error.

5. Conclusions

In this paper, the proposed system is integrated into an intelligent wheelchair to provide identification and ensure effective usage of intelligent wheelchair when improving authentication and security. The embedded gyroscope and magnetometer in myAHRS+ sensor are used to create device ICMetric. Each sensor will have unique readings utilised to provide ICMetric number which is used in the identification process. Reading generated from sensors are analysed statistically to generate ICMetric number, which integrated to the dataset extracted from the trace file generated by ns-2. A statistical study of the sensor readings shows practical to use the MEMS sensor for the generation of device identification. The security of the system can be increased by combining other device features. Though the rate of error for the proposed system is 0.23%, yet the ICMetric security system is active and useful with high rate of accuracy.

References

[1] N. Ragot, G. Caron, M. Sakel, and K. Sirlantzis, 2015, "COALAS: A EU multidisciplinary research project for assistive robotics neuro-rehabilitation," IEEE/RSJ International Conference on Intelligent Robots (IROS).

[2] A. Kokosy, M. Pepper, and C. Donzé, 2012, "SYSIASS – an intelligent powered wheelchair," in First International Conference on Systems and computer Science, Sep 2012, Lille, France.

[3] M. T. Shahzaib Tahir, Mehreen Afzal, 2014, "An ICMetric based Key Generation Scheme for Controlled Group Communication". IISA 2014, The 5th International Conference on Information, Intelligence, Systems and Applications, Chania, 2014, pp. 373-378.

[4] H. Tahir, R. Tahir, and K. McDonald-Maier, 2018, "On the security of consumer wearable devices in the Internet of Things," PLoS One, vol. 13, no. 4, pp. 1–21.

[5] Y. Kovalchuk, K. McDonald-Maier, and G. Howells, 2011, "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.

[6] H. Tahir, R. Tahir, and K. Mcdonald-maier, 2015, "Securing MEMS Based Sensor Nodes in the Internet of Things," IEEE, 2015 Sixth International Conference on Emerging Security Technologies Securing, pp. 44–49.

[7] H. Tahir and K. Mcdonald-maier, 2015, "Securing Health Sensing Using Integrated Circuit Metric," Sensors 2015, vol. 15, pp. pp. 26621–26642.

[8] 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.

[9] T. I. and E. Hossain, Introduction to Network Simulator NS2, Second Edi. Springer, Boston, 2012.

[10] J. Wang, "ns- Tutorial (1)," Event (London), no. 1, pp. 1–16, 2004. M. A. Davenport,

[11] R. G. Baraniuk and C. D. Scott, "Controlling False Alarms with Support Vector Machines," 2006 IEEE International Conference on Acoustics Speech and Signal Processing Proceedings, Toulouse, 2006, pp. V-V.

[12] "ITHROBOT" [Online]. Available: http://withrobot.com/en/sensor/myahrsplus/?ckattempt=3. [Accessed: 01-Apr-2019].

[13] B. Mukherjee, L. T. Heberlein, and K. N. Levitt, "Network intrusion detection," IEEE Netw., vol. 8, no. 3, pp. 26–41, May 1994.

[14] 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.