Online ISSN : 2249-4596
Print ISSN : 0975-5861
DOI : 10.17406/GJRE

Global Journal

of Researches in Engineering: F

Electrical and Electronic Engineering

Call Drop Optimization

Electromagnetic Antenna Cloaking

Highlights

Cryptoprotection of IT Systems

Nature Inspired Computing Machine

Discovering Thoughts, Inventing Future

VOLUME 22 ISSUE 1 VERSION 1.0

© 2001-2022 by Global Journal of Researches in Engineering, USA

Global Journal of Researches in Engineering: F
Electrical and Electronics Engineering

Global Journal of Researches in Engineering: F
Electrical and Electronics Engineering

Volume 22 Issue 1 (Ver. 1.0)

Open Association of Research Society

© Global Journal of Researches in Engineering. 2022.

All rights reserved.

This is a special issue published in version 1.0 of "Global Journal of Researches in Engineering." By Global Journals Inc.

All articles are open access articles distributed under "Global Journal of Researches in Engineering"

Reading License, which permits restricted use. Entire contents are copyright by of "Global Journal of Researches in Engineering" unless otherwise noted on specific articles.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without written permission.

The opinions and statements made in this book are those of the authors concerned. Ultraculture has not verified and neither confirms nor denies any of the foregoing and no warranty or fitness is implied.

Engage with the contents herein at your own risk.

The use of this journal, and the terms and conditions for our providing information, is governed by our Disclaimer, Terms and Conditions and Privacy Policy given on our website http://globaljournals.us/terms-and-condition/menu-id-1463/.

By referring / using / reading / any type of association / referencing this journal, this signifies and you acknowledge that you have read them and that you accept and will be bound by the terms thereof.

All information, journals, this journal, activities undertaken, materials, services and our website, terms and conditions, privacy policy, and this journal is subject to change anytime without any prior notice.

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

*(A Delaware USA Incorporation with "Good Standing"; **Reg. Number: 0423089**)*

Sponsors: Open Association of Research Society
Open Scientific Standards

Publisher's Headquarters office

Global Journals® Headquarters
945th Concord Streets,
Framingham Massachusetts Pin: 01701,
United States of America
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Journals Incorporated
2nd, Lansdowne, Lansdowne Rd., Croydon-Surrey,
Pin: CR9 2ER, United Kingdom

Packaging & Continental Dispatching

Global Journals Pvt Ltd
E-3130 Sudama Nagar, Near Gopur Square,
Indore, M.P., Pin:452009, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please email us at *local@globaljournals.org*

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *investors@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Excluding Air Parcel Charges):

Yearly Subscription (Personal & Institutional)
250 USD (B/W) & 350 USD (Color)

Editorial Board

Global Journal of Research in Engineering

Dr. Ren-Jye Dzeng

Professor Civil Engineering, National Chiao-Tung University, Taiwan Dean of General Affairs, Ph.D., Civil & Environmental Engineering, University of Michigan United States

Dr. Iman Hajirasouliha

Ph.D. in Structural Engineering, Associate Professor, Department of Civil and Structural Engineering, University of Sheffield, United Kingdom

Dr. Ye Tian

Ph.D. Electrical Engineering The Pennsylvania State University 121 Electrical, Engineering East University Park, PA 16802, United States

Dr. Eric M. Lui

Ph.D., Structural Engineering, Department of Civil & Environmental Engineering, Syracuse University United States

Dr. Zi Chen

Ph.D. Department of Mechanical & Aerospace Engineering, Princeton University, US Assistant Professor, Thayer School of Engineering, Dartmouth College, Hanover, United States

Dr. T.S. Jang

Ph.D. Naval Architecture and Ocean Engineering, Seoul National University, Korea Director, Arctic Engineering Research Center, The Korea Ship and Offshore Research Institute, Pusan National University, South Korea

Dr. Ephraim Suhir

Ph.D., Dept. of Mechanics and Mathematics, Moscow University Moscow, Russia Bell Laboratories Physical Sciences and Engineering Research Division United States

Dr. Pangil Choi

Ph.D. Department of Civil, Environmental, and Construction Engineering, Texas Tech University, United States

Dr. Xianbo Zhao

Ph.D. Department of Building, National University of Singapore, Singapore, Senior Lecturer, Central Queensland University, Australia

Dr. Zhou Yufeng

Ph.D. Mechanical Engineering & Materials Science, Duke University, US Assistant Professor College of Engineering, Nanyang Technological University, Singapore

Dr. Pallav Purohit

Ph.D. Energy Policy and Planning, Indian Institute of Technology (IIT), Delhi Research Scientist, International Institute for Applied Systems Analysis (IIASA), Austria

Dr. Balasubramani R

Ph.D., (IT) in Faculty of Engg. & Tech. Professor & Head, Dept. of ISE at NMAM Institute of Technology

Dr. Sofoklis S. Makridis

B.Sc(Hons), M.Eng, Ph.D. Professor Department of Mechanical Engineering University of Western Macedonia, Greece

Dr. Steffen Lehmann

Faculty of Creative and Cultural Industries Ph.D., AA Dip University of Portsmouth United Kingdom

Dr. Wenfang Xie

Ph.D., Department of Electrical Engineering, Hong Kong Polytechnic University, Department of Automatic Control, Beijing University of Aeronautics and Astronautics China

Dr. Hai-Wen Li

Ph.D., Materials Engineering, Kyushu University, Fukuoka, Guest Professor at Aarhus University, Japan

Dr. Saeed Chehreh Chelgani

Ph.D. in Mineral Processing University of Western Ontario, Adjunct professor, Mining engineering and Mineral processing, University of Michigan United States

Belen Riveiro

Ph.D., School of Industrial Engineering, University of Vigo Spain

Dr. Adel Al Jumaily

Ph.D. Electrical Engineering (AI), Faculty of Engineering and IT, University of Technology, Sydney

Dr. Maciej Gucma

Assistant Professor, Maritime Univeristy of Szczecin Szczecin, Ph.D.. Eng. Master Mariner, Poland

Dr. M. Meguellati

Department of Electronics, University of Batna, Batna 05000, Algeria

Dr. Haijian Shi

Ph.D. Civil Engineering Structural Engineering Oakland, CA, United States

Dr. Chao Wang

Ph.D. in Computational Mechanics Rosharon, TX, United States

Dr. Joaquim Carneiro

Ph.D. in Mechanical Engineering, Faculty of Engineering, University of Porto (FEUP), University of Minho, Department of Physics Portugal

Dr. Wei-Hsin Chen

Ph.D., National Cheng Kung University, Department of Aeronautics, and Astronautics, Taiwan

Dr. Bin Chen

B.Sc., M.Sc., Ph.D., Xian Jiaotong University, China. State Key Laboratory of Multiphase Flow in Power Engineering Xi?an Jiaotong University, China

Dr. Charles-Darwin Annan

Ph.D., Professor Civil and Water Engineering University Laval, Canada

Dr. Jalal Kafashan

Mechanical Engineering Division of Mechatronics KU Leuven, Belglum

Dr. Alex W. Dawotola

Hydraulic Engineering Section, Delft University of Technology, Stevinweg, Delft, Netherlands

Dr. Shun-Chung Lee

Department of Resources Engineering, National Cheng Kung University, Taiwan

Dr. Gordana Colovic

B.Sc Textile Technology, M.Sc. Technical Science Ph.D. in Industrial Management. The College of Textile? Design, Technology and Management, Belgrade, Serbia

Dr. Giacomo Risitano

Ph.D., Industrial Engineering at University of Perugia (Italy) "Automotive Design" at Engineering Department of Messina University (Messina) Italy

Dr. Maurizio Palesi

Ph.D. in Computer Engineering, University of Catania, Faculty of Engineering and Architecture Italy

Dr. Salvatore Brischetto

Ph.D. in Aerospace Engineering, Polytechnic University of Turin and in Mechanics, Paris West University Nanterre La D?fense Department of Mechanical and Aerospace Engineering, Polytechnic University of Turin, Italy

Dr. Wesam S. Alaloul

B.Sc., M.Sc., Ph.D. in Civil and Environmental Engineering, University Technology Petronas, Malaysia

Dr. Ananda Kumar Palaniappan

B.Sc., MBA, MED, Ph.D. in Civil and Environmental Engineering, Ph.D. University of Malaya, Malaysia, University of Malaya, Malaysia

Dr. Hugo Silva

Associate Professor, University of Minho, Department of Civil Engineering, Ph.D., Civil Engineering, University of Minho Portugal

Dr. Fausto Gallucci

Associate Professor, Chemical Process Intensification (SPI), Faculty of Chemical Engineering and Chemistry Assistant Editor, International J. Hydrogen Energy, Netherlands

Dr. Philip T Moore

Ph.D., Graduate Master Supervisor School of Information Science and engineering Lanzhou University China

Dr. Cesar M. A. Vasques

Ph.D., Mechanical Engineering, Department of Mechanical Engineering, School of Engineering, Polytechnic of Porto Porto, Portugal

Dr. Jun Wang

Ph.D. in Architecture, University of Hong Kong, China Urban Studies City University of Hong Kong, China

Dr. Stefano Invernizzi

Ph.D. in Structural Engineering Technical University of Turin, Department of Structural, Geotechnical and Building Engineering, Italy

Dr. Togay Ozbakkaloglu

B.Sc. in Civil Engineering, Ph.D. in Structural Engineering, University of Ottawa, Canada Senior Lecturer University of Adelaide, Australia

Dr. Zhen Yuan

B.E., Ph.D. in Mechanical Engineering University of Sciences and Technology of China, China Professor, Faculty of Health Sciences, University of Macau, China

Dr. Jui-Sheng Chou

Ph.D. University of Texas at Austin, U.S.A. Department of Civil and Construction Engineering National Taiwan University of Science and Technology (Taiwan Tech)

Dr. Houfa Shen

Ph.D. Manufacturing Engineering, Mechanical Engineering, Structural Engineering, Department of Mechanical Engineering, Tsinghua University, China

Prof. (LU), (UoS) Dr. Miklas Scholz

Cand Ing, BEng (equiv), PgC, MSc, Ph.D., CWEM, CEnv, CSci, CEng, FHEA, FIEMA, FCIWEM, FICE, Fellow of IWA, VINNOVA Fellow, Marie Curie Senior, Fellow, Chair in Civil Engineering (UoS) Wetland Systems, Sustainable Drainage, and Water Quality

Dr. Kitipong Jaojaruek

B. Eng, M. Eng, D. Eng (Energy Technology, Asian Institute of Technology). Kasetsart University Kamphaeng Saen (KPS) Campus Energy Research Laboratory of Mechanical Engineering

Dr. Yudong Zhang

B.S., M.S., Ph.D. Signal and Information Processing, Southeast University Professor School of Information Science and Technology at Nanjing Normal University, China

Dr. Burcin Becerik-Gerber

University of Southern Californi Ph.D. in Civil Engineering Ddes, from Harvard University M.S. from University of California, Berkeley M.S. from Istanbul, Technical University

Dr. Minghua He

Department of Civil Engineering Tsinghua University Beijing, 100084, China

Hiroshi Sekimoto

Professor Emeritus Tokyo Institute of Technology Japan Ph.D., University of California Berkeley

Dr. Philip G. Moscoso

Technology and Operations Management IESE Business School, University of Navarra Ph.D. in Industrial Engineering and Management, ETH Zurich M.Sc. in Chemical Engineering, ETH Zurich, Spain

Dr. Shaoping Xiao

BS, MS Ph.D. Mechanical Engineering, Northwestern University The University of Iowa, Department of Mechanical and Industrial Engineering Center for Computer-Aided Design

Dr. Stefano Mariani

Associate Professor, Structural Mechanics, Department of Civil and Environmental Engineering, Ph.D., in Structural Engineering Polytechnic University of Milan Italy

Dr. A. Stegou-Sagia

Ph.D., Mechanical Engineering, Environmental Engineering School of Mechanical Engineering, National Technical University of Athens, Greece

Dr. Ciprian Lapusan

Ph. D in Mechanical Engineering Technical University of Cluj-Napoca Cluj-Napoca (Romania)

Diego Gonzalez-Aguilera

Ph.D. Dep. Cartographic and Land Engineering, University of Salamanca, Avilla, Spain

Dr. Francesco Tornabene

Ph.D. in Structural Mechanics, University of Bologna Professor Department of Civil, Chemical, Environmental and Materials Engineering University of Bologna, Italy

Dr. Maria Daniela

Ph.D in Aerospace Science and Technologies Second University of Naples, Research Fellow University of Naples Federico II, Italy

Dr. Omid Gohardani

Ph.D. Senior Aerospace/Mechanical/ Aeronautical, Engineering professional M.Sc. Mechanical Engineering, M.Sc. Aeronautical Engineering B.Sc. Vehicle Engineering Orange County, California, US

Dr. Paolo Veronesi

Ph.D., Materials Engineering, Institute of Electronics, Italy President of the master Degree in Materials Engineering Dept. of Engineering, Italy

Contents of the Issue

i. Copyright Notice
ii. Editorial Board Members
iii. Chief Author and Dean
iv. Contents of the Issue

1. Electromagnetic Antenna Cloaking with Metamaterial Structures. *1-5*
2. Nature Inspired Computing Machine. *7-12*
3. Bluelock a Tool to Prevent Bluetooth Attacks. *13-23*
4. Real-Time Application of the Formant Analysis Algorithms for Cryptoprotection of IT Systems. *25-31*
5. FPGA-Based Multi-Channel A/D Converter by Optimal Duty-Cycle Modulation Technique. *33-38*
6. Handover and Call Drop Optimization. *39-44*

v. Fellows
vi. Auxiliary Memberships
vii. Preferred Author Guidelines
viii. Index

Global Journal of Researches in Engineering: F
Electrical and Electronics Engineering
Volume 22 Issue 1 Version 1.0 Year 2022
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

Electromagnetic Antenna Cloaking with Metamaterial Structures

By Ronald J. Spiegel & Shengbing Shi

Duke University

Abstract- Electromagnetic (EM) cloaks, based on spatial transformations, can potentially be utilized as shielding devices for antennas in close proximity with multiple antenna arrangements as well as highly scattering environments. In these environments each antenna can be enclosed in a cloak that is designed to be shield at the transmitting frequencies of the neighboring antennas, but assumes free space values for the shielded antenna so it can radiate unimpeded. Perfect EM cloaking is, however, difficult owing to the anisotropic, inhomogeneous material parameters of the cloak. The physical embodiment of such structures, as well as numerical calculations, is exceedingly difficult, if not impossible, for realistic 3-D structures. To overcome these immense issues, this research utilizes dispersive media (Drude or Lorentz models) that can minimize some of the problems (anisotropic, inhomogeneous material parameters) associated with "true" cloaks, but can yield similar cloaking properties. The resulting cloak is frequency dependent which cloaks at a specific frequency and is transparent at other frequencies. The resulting medium is isotropic and homogeneous.

GJRE-F Classification: FOR Code: 090699

Strictly as per the compliance and regulations of:

© 2022. Ronald J. Spiegel & Shengbing Shi. This research/review article is distributed under the terms of the Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0). You must give appropriate credit to authors and reference this article if parts of the article are reproduced in any manner. Applicable licensing terms are at https://creativecommons.org/licenses/by-nc-nd/4.0/.

Electromagnetic Antenna Cloaking with Metamaterial Structures

Ronald J. Spiegel [α] & Shengbing Shi [σ]

Abstract- Electromagnetic (EM) cloaks, based on spatial transformations, can potentially be utilized as shielding devices for antennas in close proximity with multiple antenna arrangements as well as highly scattering environments. In these environments each antenna can be enclosed in a cloak that is designed to be shield at the transmitting frequencies of the neighboring antennas, but assumes free space values for the shielded antenna so it can radiate unimpeded. Perfect EM cloaking is, however, difficult owing to the anisotropic, inhomogeneous material parameters of the cloak. The physical embodiment of such structures, as well as numerical calculations, is exceedingly difficult, if not impossible, for realistic 3-D structures. To overcome these immense issues, this research utilizes dispersive media (Drude or Lorentz models) that can minimize some of the problems (anisotropic, inhomogeneous material parameters) associated with "true" cloaks, but can yield similar cloaking properties. The resulting cloak is frequency dependent which cloaks at a specific frequency and is transparent at other frequencies. The resulting medium is isotropic and homogeneous.

I. Introduction

The operation of high power antennas in complicated environments, such as the presence of large mounting structures on ships or aircraft, where multiple antennas may exist in close proximity has been a serious issue for a long time. Near field EM coupling between antennas can severely distort radiation patterns as well as affect antenna electrical input parameters. Likewise EM scattering from near-by metal structures can also induce unwanted currents on the antenna elements which can produce adverse effects. Many attempts over the last several years have been utilized to reduce coupling and scattering effects, but, to date, there has been no "silver bullet" to completely eliminate the problem.

With the relatively recent advent of theoretical developments in EM cloaking,[1,2] a new approach is potentially available to solve antenna coupling issues in complex scattering environments. The approach, however, is not without difficult issues, especially in the physical implementation of such devices. One major problem is the complex media associated with cloaks is based on spatial transformations. The resulting media of the cloak is generally inhomogeneous and anisotropic with properties that do not exist normally in nature. To overcome the problem, metamaterial technology has been utilized in the GHz range.[3] While the resulting structure works in a laboratory setting, the transition to a more commercial venue poses problems because of the cumbersome physical features of the cloaking structure.

The problem that is addressed by this study is illustrated in Fig. 1 involving two antennas and two cloaks.[4] In Fig.1 (a.) antenna A_1, operating at frequency f_1, transmits and receives through cloak C1, A near-by antenna A_2 which is cloaked by C_2 and is designed to cloak EM fields at frequency f1. The roles are reversed in Fig. 1(b.). In general 3-D cloaks with inhomogeneous and anisotropic media cannot be modeled with commercially available computer codes (e.g. CST, COMSOL) owing to the complexity of the problem. For example, COMSOL can only handle 2-D objects with anisotropic media. Also, the physical embodiment of such structures is exceedingly difficult, if not impossible, for realistic 3-D cloak-based structures.

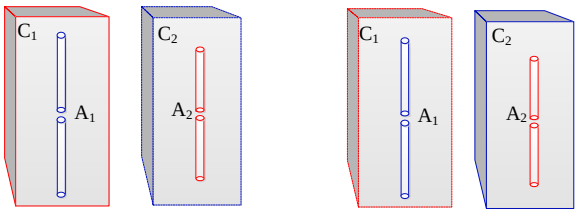

Fig. 1: Frequency configurations of antennas A_1, A_2 and cloaks C_1, C_2. (a.) A_1 radiating at f_1 and (b.) A_2 radiating at f_2. Solid boundaries for the cloaks indicate cloaking, while the dashed boundaries indicate the cloaks that are transparent

To overcome these immense issues, the cloaks developed in this study are not based on spatial transformations. Rather they are based on the dispersive properties of media, which will be shown to have similar cloaking properties as "true" cloaks for the antenna coupling problem. The resonance behavior of a material, such as a metamaterial, can be described with a bulk material model described by the Lorentz dispersion equation

$$\varepsilon_r = \varepsilon_\infty + \left[\left(\varepsilon_s - \varepsilon_\infty\right)\omega_0^2\right] / \left(\omega_0^2 + i\omega\delta - \omega^2\right) \qquad (1)$$

where ε_r is the relative dielectric constant; ω_0 is the resonance frequency; δ is the damping frequency; ε_s is

Author α: Department of Electrical and Computer Engineering, Duke University, Durham, NC 27709. e-mail: rjs24@duke.edu
Author σ: School of Physics, University of Electronic Science and Technology of China, Chengdu 610054, China.

© 2022 Global Journals

the static dielectric constant; and $\varepsilon\infty$ is the dielectric value as the frequency becomes very large. To illustrate Eq. 1, numerical calculations presented below contain the following parameter values: $\omega_0 = 34.54 \times 10^9$ rad/s or $f_0 = 5.5$ GHz; $\delta = 0.628 \times 10^9$ rad/sec or 0.1 GHz; $\varepsilon_\infty = 1$; and $\varepsilon_s = 2$. Fig. 2 shows the real and imaginary parts of the dispersive relative dielectric constant, εr, for the listed parameter values.

There are some important features of these curves that should be emphasized. First, note that at the resonance frequency the real part of ε_r equals zero. The height and width of the imaginary component are controlled by the damping frequency. Above resonance, as the frequency becomes larger, the dielectric constant assumes the free space value. Below resonance frequency ε_r approaches 2. Note also that at f_0 the loss tangent of the material is infinity.

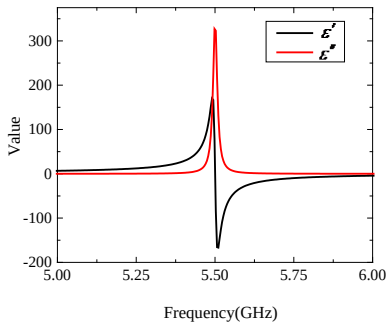

Fig. 2: Real and imaginary curves for ε_r

The complex wave number for the dispersive media can be expressed as $k = \omega k_0 \sqrt{\mu_r \varepsilon_r}$ with $\mu_r = 1$

$$k = \omega k_0 \sqrt{\varepsilon_r' + i\varepsilon_r''} \quad (2)$$

where ε_r' and ε_r'' are the real and imaginary components of ε_r, respectively, and k0 is the free space propagation constant. At the resonance frequency, $\varepsilon_r' = 0$ and k becomes imaginary so the wave in the media becomes strongly evanescent and virtually no EM fields exist in the material. In other words, the material acts almost like a perfect electric conductor (PEC). Thus, the two important features of this material are: (1) at the resonant frequency it acts almost like a perfect shield and (2) above and below the resonant frequency the material is almost transparent. If utilized in a manner depicted in Fig. 1, its properties can mimic a "true" cloak; hence the designation pseudo cloak. It should also be pointed out that the Lorentz model can be used for permeability. In Eq. (1) just replace ε with μ. Now at resonance the material acts like a perfect magnetic conductor (PMC).

To compare the properties of this cloak with those of a "true" cloak consider the following. An ideal cloak can only work for monochromatic (single frequency) EM waves. Generally, for an ideal cylindrical or spherical cloak, the radial constitutive parameters ε and μ are required to vanish (go to zero) at the inner boundary at the single frequency.[2] The singularity of the wave equation inside the cloak will form impenetrable PEC, PMC walls for EM waves. This is very similar to the condition of the pseudo cloak when ε_r or $\mu_r = 0$ at the resonance frequency forming a PEC or PMC like boundary. The difference, of course, is that for the pseudo cloak the entire layer acts like a shield whereas for an ideal cloak the barrier occurs at the inner boundary. This difference is essentially immaterial for cloaking antennas.

Finally, some difficulties of both cloaks should be pointed out. For non-monochromatic waves (all antennas have bandwidth) the shielding efficacy rapidly deteriorates away from the central frequency. The bandwidth limitations for an ideal cloak have been elaborated elsewhere.[5-7] It suffices to say that the main reason is based on group velocity delay. This delay is extenuated as the size of the shield gets larger, so that most ideal cloaks have to be small. For the pseudo cloak the reason is easy to see from Fig. 2 (a.). At resonance, when $\varepsilon_r = 0$, the slope of the response is very steep, resulting in a fairly narrow range of frequencies around the resonant frequency where ε_r values are close to zero. The saving grace is that most continuous wave communication antennas have very narrow bandwidths. However, some high peak power pulsed antennas may have wide bandwidths. Size limitations do not appear to be a problem for pseudo cloaks, except for the fact that large structures could influence the radiation patterns of nearby antennas.

Metamaterials (MMs) can produce EM phenomena that are not available in natural materials. Before construction of a prototype MM structure, numerical simulation can be used to design and analyze the MM structure as well as show that its properties are comparable to bulk properties of materials that are defined by ε and μ. For this study a split ring resonator (SRR) and a flat wire MM unit cell, as shown in Fig. 3, will be utilized. The split rings are comprised of a copper embedded on the top of a substrate and the flat copper strip id located on the back side of the substrate as shown in Fig. 3. The MM-based structure would consist of many of these small unit cells.

© 2022 Global Journals

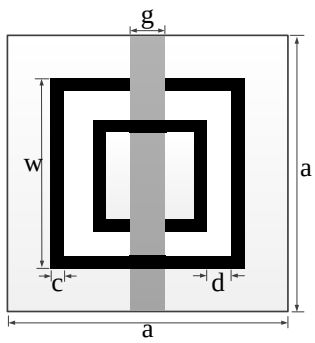

Fig. 3: SRR and flat strip MM unit cell (SRR on the front surface and the flat strip on the back side of the PCB board). Cell dimensions: gap and strip width g = 1.0 mm, a = 10 mm, w = 6 mm, d = 1.0 mm, c = 0.5 mm and substrate thickness = 0.5 mm. The substrate is comprised of a dielectric constant of 3.84 and a loss tangent of 0.018.

For a wave incident on SRR MM structure the S-parameters (S_{11} and S_{21}) for the structure are first calculated. The S parameters are related to the reflected, transmitted, and absorbed waves by the MM structure. The bulk properties (ε_{eff} and μ_{eff}) of the MM can then be calculated using either the Lorentz or Drude dispersive models. CST Studio can accomplish this by best fitting the parameters (ω_0, δ, ε_s and ε_s) associated with the Lorentz model (see Eq. 1) from the S-parameters associated with the MM structure. There are generally two approaches: parameter fitting of dispersion models and analytical extraction of medium parameters from S- parameters.[8]

The dispersion approach minimizes the difference between the S-parameters (scattering parameters) of the MM structure and a block of a homogeneous material with the same thickness as the MM unit cell. A Quasi-Newton optimization algorithm, which is built into CST's optimizer, is used to provide the best fit of the S-parameters of the dispersion model and the MM unit cell. The "goal" function in CST is to be minimized and for this case takes the form

$$Goal = \sum_{n} \begin{pmatrix} \left|S_{11} - S_{11ref}\right| + \left|S_{21} - S_{21ref}\right| \\ + \left|\angle S_{11} - \angle S_{11ref}\right| + \left|\angle S_{21} - \angle S_{21ref}\right| \end{pmatrix} \quad (3)$$

where the equation includes both the magnitude and phase of the S-parameters and the summation is over all n frequency samples in the range of interest.

From CST's extraction procedure, the bulk properties of the associated with the SRR/flat plate structure were acquired. The extracted permittivity profile (not shown) was that of the Lorentz model and essentially the same as in Fig. 2, except the resonance frequency was approximately 4.49 GHz.

It is difficult to construct a spherical or a spheroidal antenna cloak out of MMs which are generally comprised of flat surfaces, a pseudo cloak was fashioned out of a rectangular box. The box structure contained the extracted permittivity profile for the SRR/flat plate structure. A view of the pseudo cloak is shown in Fig. 4, along with the dipole transmitter(1)/receiver(2) antennas. The dipole antennas were designed to operate at the Lorentz resonance frequency of the MM, approximately 5.5 GHz. To prove the effectiveness of the box to act as a cloak several different calculations were performed: e.g., S_{11}; S_{22}; S_{21}; a dipole operating inside and outside the cloak at both the resonance frequency and an off resonance frequency; and the radiating pattern of the transmitting dipole. However, space does not permit to show them all, but they all provided the necessary numerical proof that the concept was sound. To illustrate the point Fig. 5 contains the EM fields inside and outside the box produced by the transmitter antenna operating at the Lorentz resonance frequency. As observed the box provides very good shielding allowing very little energy to penetrate into interior of the box. In addition, the calculated induced current in the receiver antenna was approximately 9×10^{-4} with the box absent versus 2×10^{-10} with box present. These numerical data provide a good basis to proceed to the next step: construction of the pseudo cloak out of actual MM comprised of unit cells based on SRR/flat plate unit cell of Fig. 3.

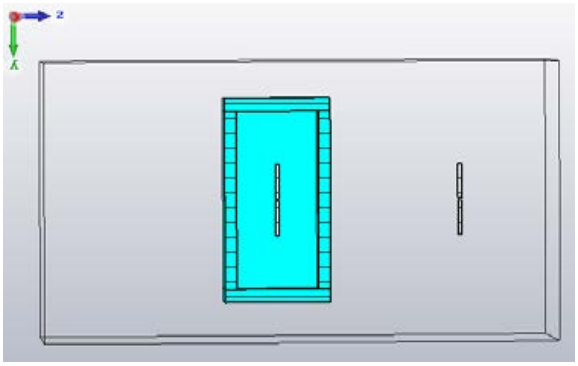

Fig. 4: Cross sectional view of a rectangular box shaped cloak, along with dipole antennas. Interior dimensions: sides 12 cm × 12 cm; top, bottom 6 cm × 6 cm; thickness 1.3 cm.

To verify the numerical results, MM boards with substrates comprised of woven E-glass and Epoxy were designed according to the specifications listed in Fig. 3 and fabricated (Better Boards, Inc., Cary, NC). Rectangular box structures of various sizes were assembled from the MM boards. The experimental set-up is shown in Fig. 6. Two monopoles were located over a ground plane and separated by 10 cm. Monopole 1 was primarily used as the transmit antenna and monopole 2 was utilized as the receiver antenna, although the roles of each antenna could be reversed. They were designed to operate at approximately the Lorentz resonance frequency of the MM structure (see

© 2022 Global Journals

Fig. 2). Three different sized MM boxes were utilized in the study: sides of 3 × 3, 5 × 5, and 6 × 6 unit cells. The use of these MM structures allowed the determination whether the number of MM unit cells played a significant role in the cloaking features of the boxes. Measurements determined that all three boxes provided essentially the same cloaking performance, therefore, only the structure with sides containing 9 unit cells (3 × 3) and dimensions of 6 cm × 6 cm × 6 cm are presented here. This box is shown in Fig. 6. All the measurements were conducted using an Agilent Technologies (E8362B) 18 MHz – 20 GHz network analyzer.

Both monopoles were designed to operate at a resonance frequency of approximately 5.5 GHz. Fig. 7 contains the measured S11 and S21 profiles for the monopole antennas. As observed from Fig. 7 (a.) the lowest return loss for monopole 1 (similar for monopole 2) occurs at 5.26 GHz (approximately the Lorentz resonance frequency for the MM structure). From Fig. 7 (b.) note that S21 has a value of about -30 dB over most of the band covered (5 – 6 GHz).

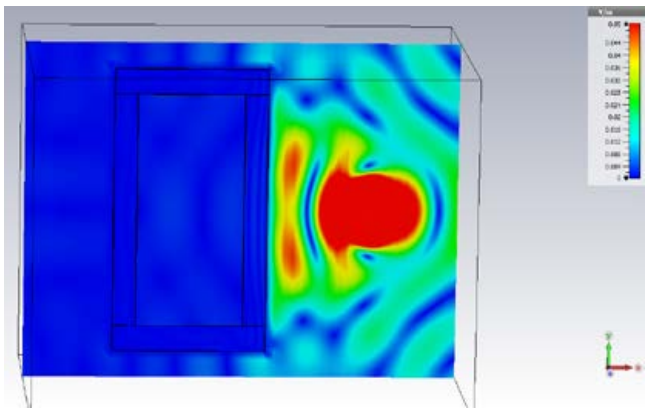

Fig. 5: EM fields inside and outside the box shaped cloak produced by an external 5.5 GHz dipole located 10 cm from the center of the box

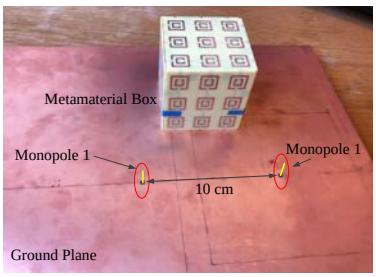

Fig. 6: A photograph of the experimental set-up

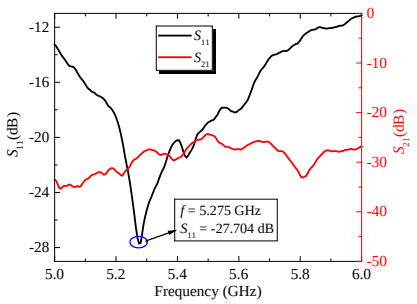

Fig. 7: S_{11} for monopole 1 and the coupling (S_{21}) between monopoles 1 and 2

Fig. 8 contains the results when the rectangular cloak is placed over either the transmit monopole or the receive monopole. When the MM box covers monopole2 (receive antenna), the S21 results are contained in Fig. 8 (a.). Observe that the cloak provide a very good shield (-85 dB) at a frequency of 5.59 GHz, which is very close to the extracted Lorentz frequency of 5.5 GHz. Fig 8 (b.) reveals similar results when monopole 1 (transmit antenna) is covered by the box, except the resonance frequency is slightly different (5.59 GHz versus 5. 62 GHz). It is likely that the small discrepancies in these measured resonance frequencies and calculated frequency (5.49 GHz) are due to small differences in the dielectric properties of the simulated and actual substrates.

Finally it is important to observe from the data in Fig. 8, for frequencies above and below the absorption band, the MM structure acts like it is essentially transparent to the incident fields. As shown the coupling values return to the levels measured when no box is shielding either antenna.

The experimental results verified the numerical predictions of the numerical simulations. MM cloaks at the resonant frequency almost act like a perfect shield and (2) above and below the resonant frequency the material is almost transparent. Its properties, for the antenna shielding problem, can mimic a “true” cloak with much less complexity in the properties of the MM structure. The measured shielding efficiency is over 99.9%.

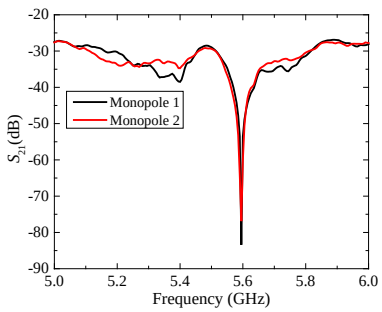

Fig. 8: Cloaking provided by the MM box.

© 2022 Global Journals

Further work needs to be performed relative to the radiation patterns of two antennas in close proximity, when one or both antennas are covered by a MM box. Calculated results (not shown) have demonstrated that the radiation pattern may be slightly distorted by a rectangular MM box in close proximity to a radiating antenna. These numerical results, however, need to be verified by measured data. Radiation distortion may be improved by a smaller box or by a different structure with curved sides such as a sphere or spheroid. Of course, other antennas, such as a patch antenna, that radiate upwards rather than to the side as does a dipole-type antenna, help eliminate the problem.

The authors would like to thank Paul Killough for his expert help in some of the fabrication aspects of the project.

References Références Referencias

1. Zhang, B., "Extraordinary Surface Voltage Effect in the Invisibility Cloak with an Active Device Inside," Phys. Rev. Letter 100, 063904 (2008).
2. Eleftheriades, G.V., "Transforming Electromagnetics Using Metamaterials," IEEE Micro. Mag. 13, 26-38 (2012).
3. Schurig, D., "Metamaterial Electromagnetic Cloak at Microwave Frequencies," Science. 314, 977-980 (2006).
4. Kwon, D., "Restoration of Antenna Parameters in Scattering Environments Using Electromagnetic Cloaking," Phys. Rev. Lett. 101, 063902 (2008).
5. Zhang, B., "Rainbow and Blue Shift Effect of a Dispersive Spherical Invisibility Cloak Impinged on by a Non-Monochromatic Plane Wave," Phys. Rev. Lett., 101, 063902(2008).
6. Craeye, C., "Rule of Thumb for Cloaking Bandwidth Based on a Wave Packet Argument," IEEE Trans. Antennas Propag. 60, 3516-3520 (2012).
7. Monticone, F., "Invisibility Exposed: Physical Bounds on Passive Cloaking," Optical, 3, 718-724 (2016).
8. Ekmekci, E., "Investigation of Effective Permittivity and Permeability for Novel V-Shaped Metamaterial Using Simulated S-Parameters," 5th international Conference on Electrical and Electronics Engineering, Bursa, Turkey, 251-254 (2007).

© 2022 Global Journals

This page is intentionally left blank

© 2022 Global Journals

Global Journal of Researches in Engineering: F
Electrical and Electronics Engineering
Volume 22 Issue 1 Version 1.0 Year 2022
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

Nature Inspired Computing Machine

By Ranganathan Vijayaraghavan & Samanvita Nagaraju

Abstract- An alternate method of representation of number system is proposed. The alternate method is based on reflection (0) and inverted reflection (1). Using an inverted reflected plane, one can create consecutive places of a number system. The alternate method has the advantage of creating empowered system representation with all places of the same power of the base. Three axioms are identified and can be proved by the method of mathematical induction to complete the process. The three axioms are, a creation of number system using inverted reflection, unique non-repetitive inverted reflection count generates natural numbers and taking inverted reflection with sign bit generates two's complement representation of negative numbers. It enabled us to create any desired number system and explained with the help of two versions of the decimal system. Typically, powered system representation leads to random switching within the representation.

Keywords: computing machine; number representation; decimal system; thermometer coding; dual and symmetry; minimal switching; glitch.

GJRE-F Classification: FOR Code: 290901

Strictly as per the compliance and regulations of:

© 2022. Ranganathan Vijayaraghavan & Samanvita Nagaraju. This research/review article is distributed under the terms of the Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0). You must give appropriate credit to authors and reference this article if parts of the article are reproduced in any manner. Applicable licensing terms are at https://creative-commons.org/ licenses/by-nc-nd/4.0/.

Nature Inspired Computing Machine

Ranganathan Vijayaraghavan [α] & Samanvita Nagaraju [σ]

Abstract- An alternate method of representation of number system is proposed. The alternate method is based on reflection (0) and inverted reflection (1). Using an inverted reflected plane, one can create consecutive places of a number system. The alternate method has the advantage of creating empowered system representation with all places of the same power of the base. Three axioms are identified and can be proved by the method of mathematical induction to complete the process. The three axioms are, a creation of number system using inverted reflection, unique non-repetitive inverted reflection count generates natural numbers and taking inverted reflection with sign bit generates two's complement representation of negative numbers. It enabled us to create any desired number system and explained with the help of two versions of the decimal system. Typically, powered system representation leads to random switching within the representation. Contrary to that, new representation provides uniform switching and minimal uniform switching thus minimising glitch. Through this method, one proves that thermometer coding act as a number system so that all arithmetic operations are possible with thermometer coding. New representation brings out the fact that decimal representation confirms to dual form, in binary form is empowered representation and in decimal digit form powered representation. Uniform switching representation of decimal digit resembles the human finger digit, and its dual representation leads to exploiting symmetry.

Keywords: computing machine; number representation; decimal system; thermometer coding; dual and symmetry; minimal switching; glitch.

I. Introduction

For a long time, the number system (Behroohz Parhami, 2000) is considered to be obtained by the power of the base. This led to the dominance of the binary system as the basis of mechanisation even though humans are more comfortable with the decimal system (GorjiSinaki & Ercegovac, 1981) Moreover, one failed to understand the enormous amount of effort needed to maintain the binary-based system and live with the rigidity dictated by binary system and also a creation of artificial intelligence(Avron Barr, & et al., 1982) thus making humanity to forget the real value human intelligence and make the society machine dependent. After carefully going through the literature by experts like Alan Turing(Turing, 1950; Turing, 1937; Richard P Feynman, 1985; Herbert Simon, 1996; Simon, Herbert A, 1995) on various aspects of computation led to the thought process that a better representation (WU Ting, et al., 2010) of the number system needed.

The new method of representation of number system through the concept of reflection and inverted reflection explained. Inverted reflection leads to entanglement (Chris Bern Hardt, 2019) and the entire gamut of knowledge of mathematics addresses how to manage the entanglement and device methods to unentangle the system under consideration.

II. New Number System Representation

In nature, two phenomena can happen i.e. reflection and inverted reflection. If reflection (buffer) considered as 0 and inverted reflection (inverters) considered 1, the entire nature is composed of combinations of buffers and inverters. Based on this, define mathematics(Underwood Dudley, 2010) as a subject of study of managing inverted reflection and also considered as entanglement, which is of concern to us. Hence a representation of inverted reflection (not gate) and reflection without inversion (buffer) leads to the creation of number system.

Now a new way to represent the number system is proposed as an inverted reflection. For example, if you have 0 with inverted reflection, 1 gets generated. Thus, with single inverted reflection binary digits are generated. Now consider the two adjacent cells with 0's. Thus, we have 00, 01 and if we take an inverted reflection of this, the series 00 01 | 10 11. Where | denotes inverted reflector. Thus, we have created two-bit binary numbers. Now create three bits of two-bit combinations with the most significant bit as 0 to generate 000, 001, 010,011. Now putting an inverted reflection of this series, we generate000,001,010,011| 100,101,110,111.

Thus, three-bit binary numbers are created. In this way, one can create a number system using the inverted reflection, which is much more fundamental than the powered system. It becomes evident that binary representation is the fundamental way to represent any number system to utilise the inverted reflection concept. The second axiom to be satisfied by this concept is that this generated number system creates natural numbers through new inverted reflection but not repeated inversions. Take, for example, two-bit combinations we see that we have natural numbers 0,1 with fresh inverted reflection, 2 with a count two new inverted reflection and 3 with one more new inverted reflection. One more axiom to be needed by inverted

Author α: CEO E-Spectrum Consulting Bangalore.
e-mail: drvrangan@gmail.com
Author σ: Associate Professor, Department of Electrical and Electronics Engineering Nitte Meenakshi Institute of Technology, Bangalore.

© 2022 Global Journals

reflection to complete the number system generation in creating negative numbers. To create negative numbers if you do inverted reflection with the most significant bit has sign bit then two's complement numbers are generated. In the above explanation if third-bit acts as a sign bit, then the inverted reflection of three bits are two's complement of the two-bit numbers. As seen 000,001,010,011,100,101,110,111 represent 0,1,2,3,0, -3, -2, -1.

III. Axioms of Representation

To summarise the definition of creation of number system needs to obey three axioms:

1. Number systems are generated using inverted reflection of binary equivalent. 2. Natural numbers are generated by counting fresh inverted reflections leading to generation of 1 up to that point.
2. Affixing a sign bit and taking inverted reflection with respect that creates negative numbers in two's complement form.

IV. Advantages of New Representation

Let us now analyse what special advantages one gets out of this new way representation of number system.

1. It is possible to create arbitrary number systems. For example, thermometer coding (Rasit Onur Topalogulu, 2007; Toru Nakura,& Kunihiro Asada, 2013; Fereshteh Jafarzadehpour et al., 2019) can be proved as a number system.
2. One can create empowered number systems in which all binary digits have same power. Thus, first the time, a representation for empowered systems accomplished.
3. Particular representations having uniform switching (all switching with the same level of switching), minimal uniform switching (all switching with uniformly one switching only) can be generated that cannot be achieved by powered number system representation.
4. Unlike binary representation decimal representation follows dual (Williams, 1996; Girvin, 1996) system of binary empowered and decimal powered system. Thus symmetry (De Haro, Butterfield, 2019; Ruben Aldrovandi et al., 2013; Dr. Ivan Fernandoz-Corbaton, 2019) can be exploited
5. A new system satisfies the concept in field of Mathematics(Givant, Steven & HalmosPaul, 2009)as addition, multiplication, subtraction and division is possible and mechanisation realised through Boolean algebra(George Boole, 2011; Foster, 1991) and CMOS technology (Lee, 2019; Rohit Sharma, 2018).

V. Example of New Representation

To illustrate advantages mentioned above decimal representation taken as example.

Consider thermometer coding with nine binary digits of power 2^0as shown in Figure 1

© 2022 Global Journals

		2^0	2^0	2^0	2^0	2^0	2^0	2^0	2^0	2^0
000000000	0	0	0	0	0	0	0	0	0	0
000000001	1	0	0	0	0	0	0	0	0	1
000000011	2	0	0	0	0	0	0	0	1	1
000000111	3	0	0	0	0	0	0	1	1	1
000001111	4	0	0	0	0	0	1	1	1	1
000011111	5	0	0	0	0	1	1	1	1	1
000111111	6	0	0	0	1	1	1	1	1	1
001111111	7	0	0	1	1	1	1	1	1	1
011111111	8	0	1	1	1	1	1	1	1	1
111111111	9	1	1	1	1	1	1	1	1	1

Inverted reflection enabled cell

Figure 1: A decimal system based on thermometer coding using Inverted Reflection

Thus, the above decimal numbers are generated using inverted reflection satisfying the first axiom, natural numbers are generated using afresh inverted reflection that leads to the generation of 1 and if a sign bit appended and inverted reflection taken produce negative numbers in two's complement form. Thus, with the new concept, a decimal number system is generated. Inherently this representation satisfies uniform and minimal switching (Jaakko Astola & Radomir S. Stankovic, 2006) from one digit to the other. Many advantages of the thermometer coding are already available in the literature and exploited in the hardware (Stanley Wolf, 2002; Sung Kyu Lim, 2008; Holdsworth & Woods, 2003) development as well.

But if one tries to generate addition and multiplication circuits using this representation, it needs huge logic and consumes lot of area. To overcome this and also to illustrate the generation of arbitrary number system consider uniform switching but not minimal. In this representation, we take five bits with four 2^1bits as Most significant bits and the least significant bit with power 2^0. Then our new decimal numbers are generated using inverted reflection as given in Figure 2.

Again, the above decimal system satisfies all three axioms put forward for inverted reflection method of generation of a new number system. Here if you observe the switching is not minimal but uniform. Since only five bits are used, combinations needed to generate arithmetic circuits (LaMeres, 2019; Jiang et al., 2019)will be much less compared to thermometer coding. Here also since there is empowerment for higher-order bits it has the advantages of thermometer coding. Coincidently, human finger systems have such an arrangement and hence form the basis for an analysis of the human digit system.

© 2022 Global Journals

		2^1	2^1	2^1	2^1	2^0
000000000	0	0	0	0	0	0
000000001	1	0	0	0	0	1
000000011	2	0	0	0	1	0
000000111	3	0	0	0	1	1
000001111	4	0	0	1	1	0
000011111	5	0	0	1	1	1
000111111	6	0	1	1	1	0
001111111	7	0	1	1	1	1
011111111	8	1	1	1	1	0
111111111	9	1	1	1	1	1

Inverted Reflection Enabled Cell

Figure 2: Decimal system generation with uniform switching with 5 bits

The number system generation depicted as a machine consisting of inverters and buffers illustrated in Figure 3 and Figure 4 for the decimal systems discussed earlier.

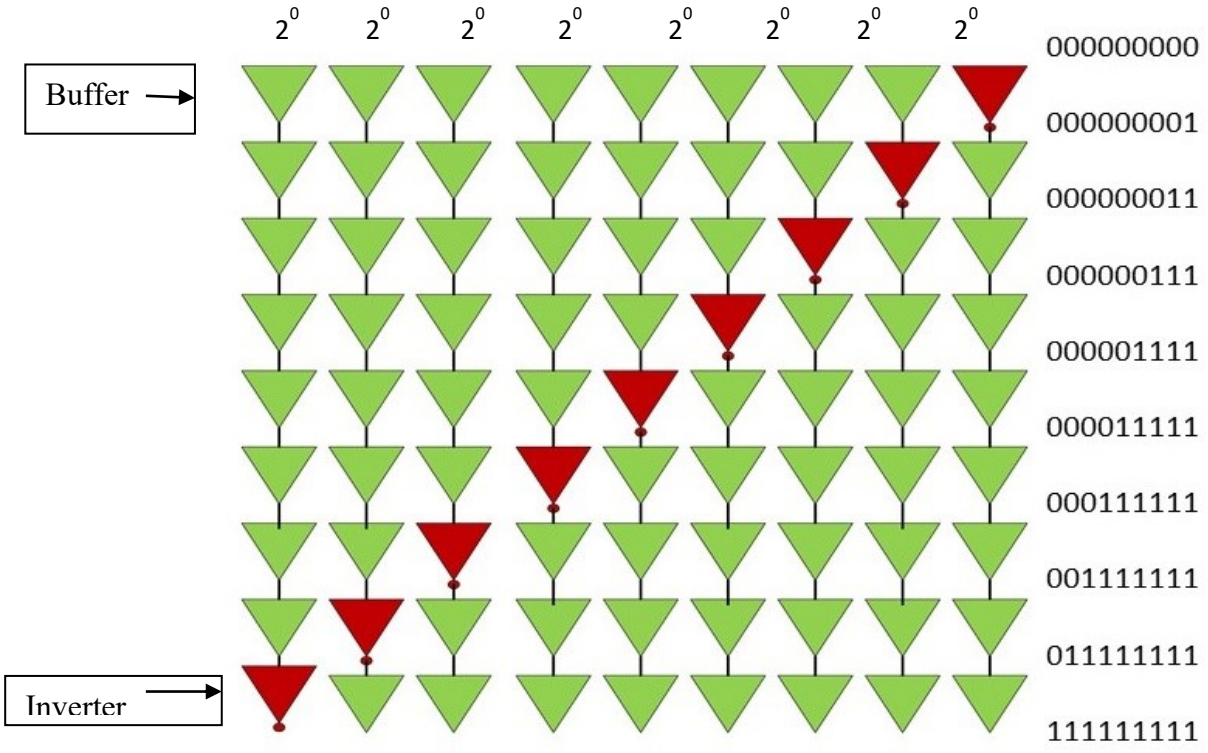

Figure 3: Natural Inverted Reflection based representation of 9 bit decimal with 2^0 as weight

© 2022 Global Journals

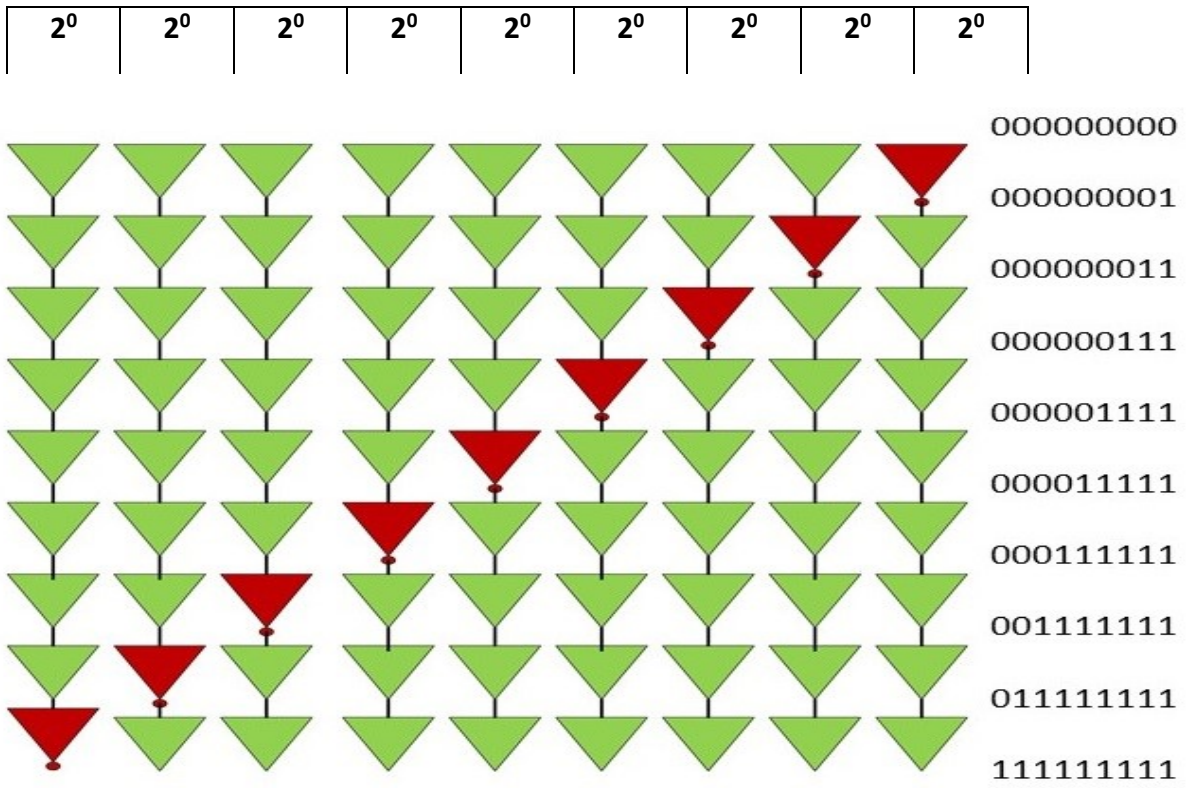

Figure 4: Natural Inverted Reflection Based Machine with uniform switching with weight $2^1 2^1 2^1 2^1 2^0$

VI. Scope of New Representation

This Nature Inspired Machine capable of generation of various number systems. They are considered Natural as it uses various natural aspects like reflection and inverted reflection, new cell generation and existing cell. This brings out the natural generation numbers as a unique count of inverted reflection leading to the generation of new 1's. Any number system consists of a field of buffers and inverters arranged in a matrix of the size based on the weight age given to each element and number of bits taken into consideration.

New decimal representation obeys dual system. At binary level bits are empowered and at digit level digits are powered. This unique advantage gives many applications and mainly manages power and glitch (Ki-Seok Chung et al., 2002) in a better way. This dual nature of empowered and powered enable to create various innovative applications if carefully researched. One immediate observation in human digits applying this dual concept brings out a better understanding of the human system. These pave the way for many in-depth studies of the human digits system and bring better understanding. Glitch free circuits become possible through a representation of any number system with equivalent thermometer coding before mechanisation. These become feasible through our new number system representation.

References Références Referencias

1. Behroohz Parhami. (2000). Algorithms and Hardware Designs, in Computer Arithmetic Oxford University Press.
2. GorjiSinaki, A., & Ercegovac, M. D.(1981). Design of a digit slice on line arithmetic Unit, IEEE 5th Symposium on Computer Arithmetic (ARITH).
3. Avron Barr, and Edward, A. FeigenBaumed (1982). Hand Book of Artificial Intelligence, Vol 2, Heuris Tech Press and William Kaufman Inc.
4. Turing, A.M. (1950). Computing Machinery and Intelligence, Mind 49:433-460.
5. Turing, A.M (1937).On computable Numbers with an application to the Entsschei dungs problem, EDN.
6. Richard P Feynman (1985). The computing machines in Furture, Nishina Memorial Lecture at Gakushuin University.
7. Herbert A Simon, (1996). The Science of the Artificial, The MIT Press.
8. Simon Herbert, A. (1955). On a class of skew Distribution Functions, Biometrika, 42(3-4), 425-440.
9. WU Ting, Zhang Min, Huan-qiang, D.U., & WANG Rang-bo. (2010). On optimal binary signed representations of integer, Appl. Math. J, Chinese Univ, 25(3): 331-340.
10. Chris Bern Hardt. (2019). Quantum Computing for Everyone, The MIT Press.

© 2022 Global Journals

11. Underwood Dudley. (2010). What is Mathematics for? Notices of the AMS, Vol 57 Number 3.
12. Rasit Onur Topalogulu. (2007). Process Variation Aware Multiple-Fault Diagnosis of Thermometer Coded Current-Steering DACs, IEEE Transactions on Circuits and Systems—2: Express Briefs, Vol. 54, No. 2.
13. Toru Nakura & Kunihiro Asada. (2013). Pulse Width Controlled PLL/ DLL using Soft Thermometer Code, IEEE Asian Solid-State Circuits Conference A-SSCC.
14. Fereshteh Jafarzadehpour, Amir Sabbagh Molahosseini, zadeh Alsadat Emrani Zarandi, & Leonel Sousa, (2019). Efficient Modular Adder Designs Based on Thermometer Coding and One-Hot Coding, IEEE Transactions On Very Large Scale Integration (VLSI) Systems, Vol. 27, NO. 9.
15. Williams, H.P. (1996). Duality in Mathematics and linear and integer programming, Journal of Optimization Theory and Applications Vol 90, pages 257–278.
16. Girvin, Duality, S M. (1996). in Perspective, Science Vol. 274 issue 5287, pp524-525.
17. De Haro, S. (2019). Butterfield, J. On symmetry and duality Synthese.
18. Ruben Aldrovandi & José Geraldo Pereira. (2013). Duality Symmetry, In: Teleparallel Gravity. Fundamental Theories of Physics, Vol 173.Springer, Dordrecht.
19. Dr. Ivan Fernandoz-Corbaton. (2019). Duality and Symmetry, Special issue of Symmetry, Vol 11, issue , MDPI.
20. Givant, Steven, & Halmos Paul, (2009).Introduction to Boolean Algebras, Springer.
21. George Boole. (2011). The Mathematical Analysis of Logic, Project Gutenberg's.
22. Foster, D.J. (1991).Silicon Processing CMOS Technology, Electronic Materials, in Miller L.S., Mullin J.B. (eds) Electronic Materials. Springer.
23. Lee, B.H. (2019). CMOS technology on another level. Nat Electron 2, 272–273.
24. Rohit Sharma. (2018). Characterization and Modelling of Digital circuits Second Edition, Paper Back.
25. Jaakko Astola, & Radomir S. Stankovic. (2006). Fundamentals of Switching Theory and Logic Design A Hands-on Approach, Springer US.
26. Stanley Wolf. (2002). Silicon Processing for VLSI Era, Vol 4 Deep-Submicron Process Technology, Lattice Pr.
27. Sung Kyu Lim. (2008). Practical Problems in VLSI Physical Design Automation, Springer. Holdsworth, B., & Woods, R.C. (2003). Arithmetic Circuits, in Digital Logic Design Elsevier Ltd.
28. LaMeres, B.J. (2019). Arithmetic Circuits. In: Introduction to Logic Circuits & Logic Design with Verilog. Springer, Cham.
29. Jiang, H., Liu L., Lombardi, F., & Han, J. (2019) Approximate Arithmetic Circuits: Design and Evaluation. In: Reda S., Shafique M. (eds) Approximate Circuits. Springer, Cham.
30. Ki-Seok Chung, Taewhan Kim & Liu, C. L. (2002). A Complete Model for Glitch Analysis in Logic Circuits, Journal of Circuits, Systems and Computers Vol. 11, No. 02, pp. 137-153.

© 2022 Global Journals

Global Journal of Researches in Engineering: F
Electrical and Electronics Engineering
Volume 22 Issue 1 Version 1.0 Year 2022
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

Bluelock a Tool to Prevent Bluetooth Attacks

By Gerardo Alberto Castang Montiel, Fernando Betancourt Duque & Luz Adriana Peña Salazar

Universidad Distrital Francisco José de Caldas

Abstract- The mobile device manufacturers and Internet Of Things are searching for more compatible and easy to connect protocols that increase coverage, which generates the user an effective experience when using different devices. Nevertheless, the constant updating process opens a security gap that exposes the users' personal information. Bluetooth is a communication protocol openly used by manufacturers because of their excellent information transfer capacities, allowing hackers to exploit it. The manufacturers work daily, generating security patches for communication protocols but this hasn't been enough to mitigate vulnerabilities. The security has always been on the manufacturer's side but the final user is limited to use a few security customization options to protect his network perimeter. Based on the wireless devices' background we wonder, Is there any way in which the user has the chance to reduce the possible dangers that wireless devices face? We can answer this question through the development of a research in the more vulnerable areas, simulating the attacks on a mobile device to generate a possible solution that allows the user to have more control over his bluetooth connections.

Keywords: *bluetooth, android, security, attacks.*

GJRE-F Classification: *FOR Code: 290903*

Strictly as per the compliance and regulations of:

© 2022. Gerardo Alberto Castang Montiel, Fernando Betancourt Duque & Luz Adriana Peña Salazar. This research/review article is distributed under the terms of the Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0). You must give appropriate credit to authors and reference this article if parts of the article are reproduced in any manner. Applicable licensing terms are at https://creativecommons.org/ licenses/by-nc-nd/4.0/.

Bluelock a Tool to Prevent Bluetooth Attacks

Gerardo Alberto Castang Montiel [α], Fernando Betancourt Duque [σ] & Luz Adriana Peña Salazar [ρ]

Abstract- The mobile device manufacturers and Internet Of Things are searching for more compatible and easy to connect protocols that increase coverage, which generates the user an effective experience when using different devices. Nevertheless, the constant updating process opens a security gap that exposes the users' personal information. Bluetooth is a communication protocol openly used by manufacturers because of their excellent information transfer capacities, allowing hackers to exploit it. The manufacturers work daily, generating security patches for communication protocols but this hasn't been enough to mitigate vulnerabilities. The security has always been on the manufacturer's side but the final user is limited to use a few security customization options to protect his network perimeter. Based on the wireless devices' background we wonder, Is there any way in which the user has the chance to reduce the possible dangers that wireless devices face? We can answer this question through the development of a research in the more vulnerable areas, simulating the attacks on a mobile device to generate a possible solution that allows the user to have more control over his bluetooth connections.

Keywords: bluetooth, android, security, attacks.

I. Introduction

Advances in wireless communication have faced compatibility issues, which has forced technology manufacturers to regulate communication protocols. One of the most popular has been Bluetooth used to interconnect mobile devices and IoT technology. This protocol was created in 1994 by the electric engineer Jaap Haartsen and it has been updated throughout the years that has allowed it to be one the best protocols due to its information transfer rate.

Because of its popularity, coming from manufacturers, this has been the target of hackers who have used vulnerabilities to attack other users and obtained their private information from their mobile devices. The response to these attacks is usually reactive. Such attacks have compromised thousands of users' information, even installing apps that act like malware, that allows access to the peripherals connected to the victim's device, like a camera, mic, GPS, and others.

Author α: Ingeniero electrónico, Universidad Distrital Francisco José de Caldas, Colombia. Correo electrónico: gerardocastang@gmail.com
Author σ: Tecnólogo en sistematización de datos, Universidad Distrital Francisco José de Caldas, Colombia.
Correo electrónico: duquefernandobetancourt@gmail.com
Author ρ: Tecnóloga en sistematización de datos, Universidad Distrital Francisco José de Caldas, Colombia.
Correo electrónico: luapenas@correo.udistrital.edu.co

Smartphones are the most used devices for Bluetooth technology due to its features and the storage capacity in Android. The manufacturers keep reactive during the attacks, generating patches and updates, saving the security recommendations.

To generate a preventive solution, we propose the user is able to manage the Bluetooth interface so it can be used without exposing private information when the device is active. To accomplish this, a testing environment is set up to deploy Bluetooth attacks to identify possible vulnerabilities that could be reduced by an Android app for Smartphones.

a) Glossary

Android is a mobile operating system based on a modified version of the Linux kernel and other open source software, designed primarily for touchscreen mobile devices such as smartphones and tablets. Android is developed by a consortium of developers known as the Open Handset Alliance and commercially sponsored by Google.

- *Attacks:* In this project an attack is a cyberattack, and it is the attempt caused by someone who wants to get control over an informatic system once he gets access to it.

The attacks have several purposes in order to cause damage through espionage to get money or to find vulnerabilities in the system.

- *BlueLock:* It is the created tool for Android devices that allows control over the Bluetooth interface by the user to manage connectivity among active devices.
- *Bluetooth:* It is a short-range wireless technology standard that is used for exchanging data between fixed and mobile devices over short distances using UHF radio waves in the ISM bands, from 2.402 GHz to 2.48 GHz, and building personal area networks (PANs).
- *Kali Linux:* Kali Linux *(formerly known as BackTrack Linux)* is an open-source, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali Linux contains several hundred tools targeted towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering. Kali Linux is a multi platform solution, accessible and freely available to information security professionals and hobbyists.
- *Pentesting and Ethical hacking:* The terms 'penetration testing' and 'ethical hacking' are often

© 2022 Global Journals

used interchangeably when referring to internal cyber security tests, but they're not exactly the same. Penetration testing is a type of security test in which an organisation hires a certified professional to assess the strength of its cyber security defences. The goal of ethical hacking – like criminal hacking – is to find security vulnerabilities in an organisation's systems. However, as the word 'ethical' suggests, the person conducting the attack must have the organisation's approval before proceeding.

- *Information security:* The state of being protected against the unauthorized use of information, especially electronic data, or the measures taken to achieve this.
- *Vulnerability:* It is a failure in the security system in which the user can access a system to manipulate information, app or take control over the system.

II. Attack Deployment

Knowing the different types of attacks over Bluetooth, they are possible to duplicate through Pentesting. The tests done are known as "white box" (tandem), because we implement the attack environment using the platform pentesting Kali Linux, keeping track of every tool and designing the hacking tests for Bluetooth.

To begin, through Kali Linux we ensure that Bluetooth is activated using the following commands:

```
root@kali:~# service bluetooth start
root@kali:~# service bluetooth status
● bluetooth.service - Bluetooth service
   Loaded: loaded (/lib/systemd/system/bluetooth.service; enabled; vendor preset
   Active: active (running) since Sun 2018-11-11 11:35:52 -05; 5h 33min ago
           Docs: man:bluetoothd(8)
 Main PID: 622 (bluetoothd)
   Status: "Running"
           Tasks: 1 (limit: 4915)
   Memory: 4.0M
   CGroup: /system.slice/bluetooth.service
           └─622 /usr/lib/bluetooth/bluetoothd
```

After, we validate the Bluetooth interface (Mac Address)

```
root@kali:~# hciconfig
hci0:   Type: Primary  Bus: USB
    BD Address: C8:FF:28:A6:15:F1  ACL MTU: 820:8  SCO MTU: 255:16
    UP RUNNING PSCAN ISCAN
    RX bytes:3857 acl:0 sco:0 events:602 errors:0
    TX bytes:28371 acl:0 sco:0 commands:388 errors:0
```

We use the Bluelog tool from Kali Linux that allows us to see and register detectable devices on the Bluetooth network and it is executed as you will find below:

```
root@kali:~# bluelog
Bluelog (v1.1.2) by MS3FGX
-------------------------
Autodetecting device...OK
Opening output file: bluelog-2018-11-11-1655.log...OK
Writing PID file: /tmp/bluelog.pid...OK
Scan started at [11/11/18 16:55:26] on C8:FF:28:A6:15:F1.
Hit Ctrl+C to end scan.
```

Blue Scanner is another Kai Linux tool that allows us to scan through the Bluetooth network adapter, capturing connectivity features from connected devices on the network and it is executed as follows

```
root@kali:~# btscanner
```

Keyword "i" produces and scans all devices on the network and generates a file directory called by the MAC's device name with all the information obtained, using these tools we can start to validate the attacks and check their functionality.

© 2022 Global Journals

- *Bluejacking attack:* To make this possible, we need to create a contact user, instead of the name, the message will be written, in the directory folder that will act as the attacker and the contact user is saved. After That, an area with several mobile devices is found and the option “send via Bluetooth" is chosen, and it is sent to the target devices.
- *Bluesmack:* a line executed directly from the attacker’s console device. which deploys several calls in a specific frame of time, causing the Bluetooth denial service in the host or hacked device. The script is:

```
root@kali:~# while read r; do l2ping -s 50 84:C7:EA:57:36:D7; done < numscans
```

we created a file called: numscans with a timer from 1 to n, to be used in the script and avoid memory leaking in the attacker's device.

```
root@kali:~# while read r; do l2ping -s 50 84:C7:EA:57:36:D7; done < numscans
Ping: 84:C7:EA:57:36:D7 from C8:FF:28:A6:15:F1 (data size 50) ...
0 bytes from 84:C7:EA:57:36:D7 id 0 time 5.91ms
0 bytes from 84:C7:EA:57:36:D7 id 46 time 63.44ms
Send failed: Connection reset by peer
Ping: 84:C7:EA:57:36:D7 from C8:FF:28:A6:15:F1 (data size 50) …
```

a) Attack results

We can see the Bluetooth protocol is designed to facilitate device connection, and it is a mandatory approach for IoT communication devices, so through the software we designed we do not want to limit or block the protocol’s functionality automatically by a service or app, but we want to give the user this option, designing an app that allows him to see the connectivity events, paired devices, and allows the user the chance to block any device at anytime.

III. Design Phase

a) Software structure

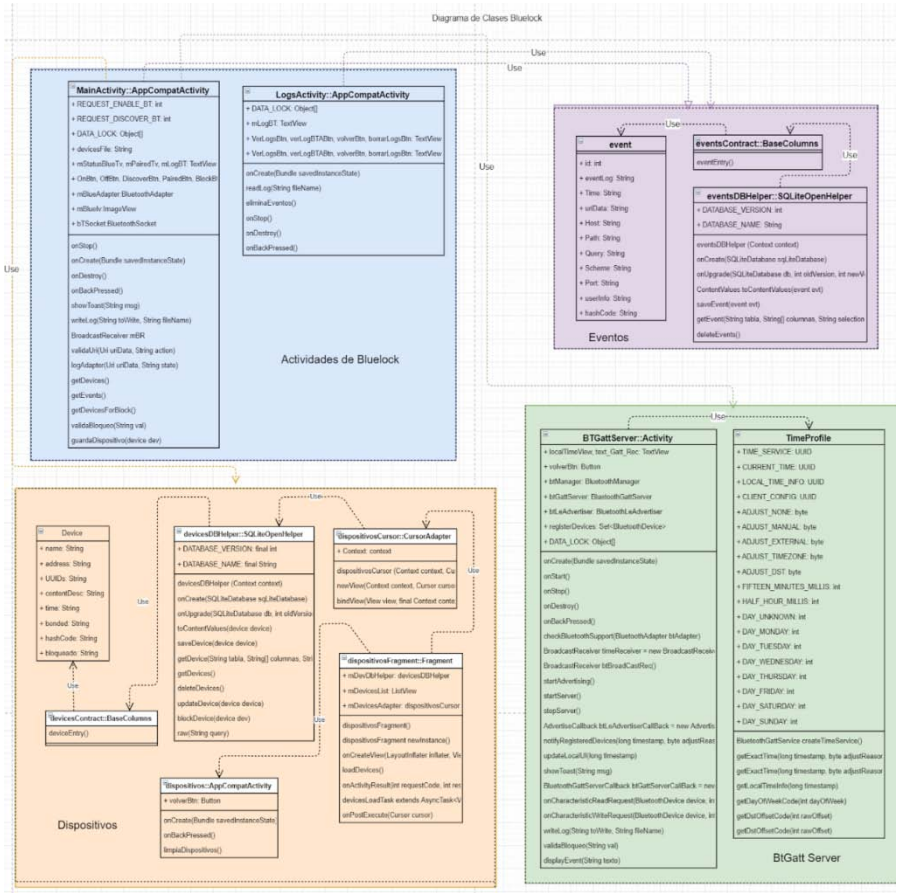

Fig. 1: Class Diagram

© 2022 Global Journals

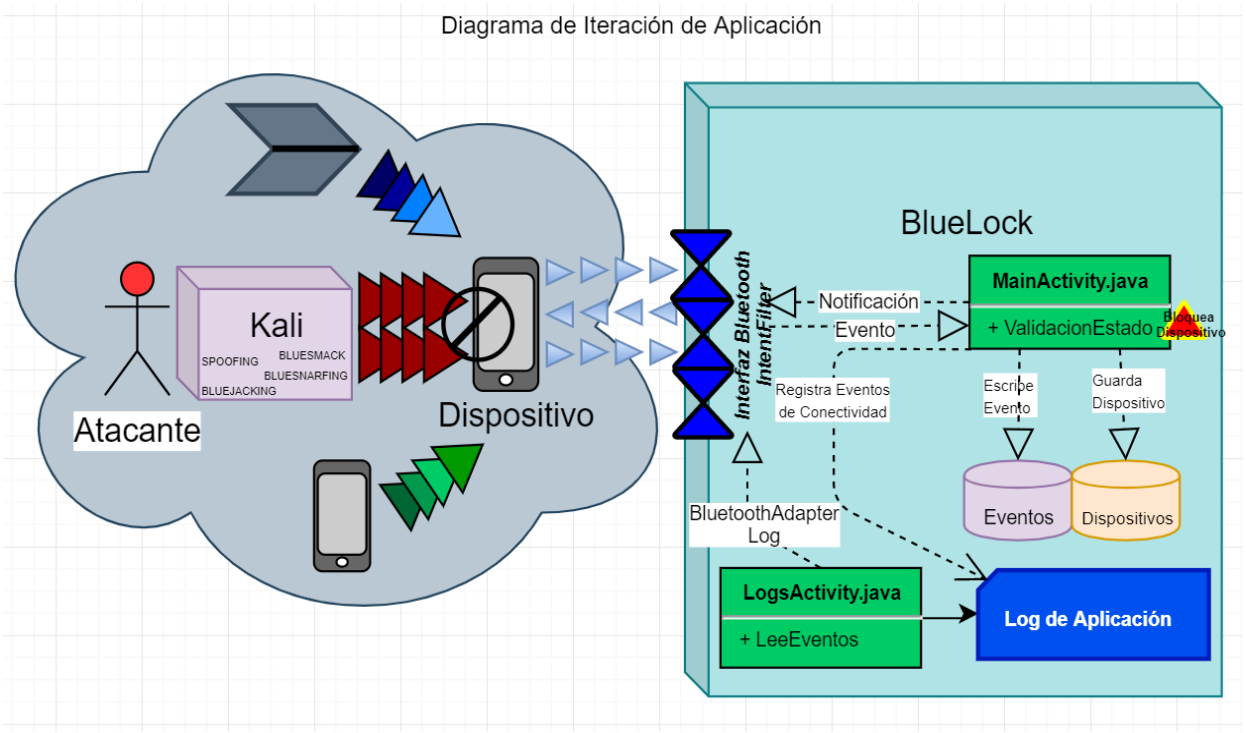

Fig. 2: Iteration Diagram

The diagram shows the device and the app running, participating in different communications with different devices, the device is in a susceptible environment when it is often attacked via Bluetooth. The device has a Bluetooth interface that communicates with the app (Bluelock) that manages the Bluetooth adapter.

The app (BlueLock) has an event filter that detects specific changes in the Bluetooth adapter, such as incoming connections, and registering all the information in a database, and the app log.

IV. Development Phase

App development

As a solution a mobile app for Android is proposed that allow people to control the Bluetooth interface communication, turn on and off the Bluetooth controller, enable finding new devices, consult paired devices, check the Bluetooth event's logs, block access to multiple devices.

App features

1. User's interface to control the Bluetooth device.
2. Generate bluetooth log events detected by the app.
3. block device interface through Bluetooth interface.
4. Generate a non-relational database that allows storing information about Bluetooth connected devices and their related events.

a) Code documentation

Bluetooth filter packages: The main feature consists in the BroadcastReceiver function, that allows sending and managing the communication events sent by the Bluetooth adapter in the Context.sendBroadcast. This function filters and controls states detected by the adaptor, does the actions generated by the bluetooth device and writes the log events.

© 2022 Global Journals

```
//BroadcastReceiver
private final BroadcastReceiver mBR = new BroadcastReceiver() {
    @Override
    public void onReceive(Context context, Intent intent) {
        final String action = intent.getAction();
        String evento = "";
        boolean bloqueo = false;
        final Uri uriData = intent.getData();
        event evt = validaUri(uriData, action);
        eventsDBHelper dbHelper = new eventsDBHelper(getApplicationContext());
        String log = "", showToastLog = "";
        boolean logger;
        if(action.equals(BluetoothAdapter.ACTION_STATE_CHANGED)
                ||action.equals(BluetoothAdapter.ACTION_DISCOVERY_STARTED)
                    ||action.equals(BluetoothAdapter.ACTION_DISCOVERY_FINISHED)
                        ||action.equals(BluetoothAdapter.ACTION_SCAN_MODE_CHANGED)) {
            final int estado = intent.getIntExtra(BluetoothAdapter.EXTRA_STATE,
BluetoothAdapter.ERROR);
            switch (estado) {
                case BluetoothAdapter.STATE_OFF:
                    evento = "<font color='blue'>BluetoothAdapter.STATE_OFF";
                    log += logAdapter(uriData,evento);
                    break;
                case BluetoothAdapter.STATE_ON:
                    evento = "<font color='blue'>BluetoothAdapter.STATE_ON";
                    log += logAdapter(uriData,evento);
                    break;
                case BluetoothAdapter.STATE_TURNING_OFF:
                    evento = "<font color='purple'>BluetoothAdapter.STATE_TURNING_OFF";
                    log += logAdapter(uriData,evento);
                    break;
                case BluetoothAdapter.STATE_TURNING_ON:
                    evento = "<font color='purple'>BluetoothAdapter.STATE_TURNING_ON";
                    log += logAdapter(uriData,evento);
                    break;
```

Fig. 3: Broadcast Receiver Function

Validation of the connection state of the device in the event "connecting". If the device is blocked, a remove Band event is generated which eliminates the paired device from the Bluetooth device list, blocking every attempt from other devices to connect.

```
case BluetoothAdapter.STATE_CONNECTING:
  evento = "<font color='purple'>BluetoothAdapter.STATE_CONNECTING";
  log += logAdapter(uriData,evento);
  BluetoothDevice device = intent.getParcelableExtra(BluetoothDevice.EXTRA_DEVICE);
  bloqueo = validaBloqueo(device.getAddress());
  UUID uuid = UUID.randomUUID();
  if(bloqueo){
    try {
      Log.w("ACTION_ACL_CONNECTED","Entró a removeBond");
      Method m = device.getClass()
          .getMethod("removeBond", (Class[]) null);
      m.invoke(device, (Object[]) null);

      evento = "<font color='red'>Dispositivo Bloqueado ("+uuid+"):
"+device.getAddress()+"; "+device.getName();
```


© 2022 Global Journals

```
            log += logAdapter(uriData,evento);
            showToast("Dispositivo bloqueado ("+uuid+") : "+device.getAddress()+" : "+
device.getName());
        } catch (Exception e) {
            Log.w("ACTION_ACL_CONNECTED", e.getMessage());
            evento = "<font color='red'>Error de Dispositivo Bloqueado ("+uuid+"):
"+device.getAddress()+"; "+device.getName();
        }
        log += logAdapter(uriData,evento);
    }
    break;
```

Fig. 4: Event Connecting

We validate the other BluetoothAdapter status. Every event generates a line in the Log events that can be consulted by the app. It was designed to have styles so when the .txt is rendered, shows with colors the severity of the case.

```
case BluetoothAdapter.STATE_CONNECTED:
            evento = "<font color='green'>BluetoothAdapter.STATE_CONNECTED";
            log += logAdapter(uriData,evento);
            break;
        case BluetoothAdapter.STATE_DISCONNECTING:
            evento = "<font color='green'>BluetoothAdapter.STATE_DISCONNECTING";
            log += logAdapter(uriData,evento);
            break;
        case BluetoothAdapter.STATE_DISCONNECTED:
            evento = "<font color='purple'>BluetoothAdapter.STATE_DISCONNECTED";
            log += logAdapter(uriData,evento);
            break;
        case BluetoothAdapter.SCAN_MODE_CONNECTABLE_DISCOVERABLE:
            evento = "<font color='purple'>BluetoothAdapter.SCAN_MODE_CONNECTABLE_DISCOVERABLE";
            log += logAdapter(uriData,evento);
            break;
        case BluetoothAdapter.SCAN_MODE_CONNECTABLE:
            evento = "<font color='purple'>BluetoothAdapter.SCAN_MODE_CONNECTABLE";
            log += logAdapter(uriData,evento);
            break;
        case BluetoothAdapter.SCAN_MODE_NONE:
            evento = "<font color='purple'>BluetoothAdapter.SCAN_MODE_NONE";
            log += logAdapter(uriData,evento);
            break;
        default:
            break;
    }
    logger = writeLog(log, "BluetoothAdapter.txt");
    evt.setEventLog(evento);
    dbHelper.saveEvent(evt);
}
if(action.equals(BluetoothAdapter.ACTION_CONNECTION_STATE_CHANGED)) {
    final int estado = intent.getIntExtra(BluetoothAdapter.EXTRA_CONNECTION_STATE, BluetoothAdapter.ERROR);
    evento = "<font color='red'>BluetoothAdapter.ACTION_CONNECTION_STATE_CHANGED :" + estado;
    log += logAdapter(uriData, evento);
    evt.setEventLog(evento);
    dbHelper.saveEvent(evt);
    logger = writeLog(log, "BluetoothAdapter.txt");
    showToast(showToastLog);
}
```


© 2022 Global Journals

```
if(action.equals(BluetoothAdapter.ERROR)){
  log += String.valueOf(BluetoothAdapter.ERROR);
  evento = "<font color='red'>BluetoothAdapter.ERROR";
  log += logAdapter(uriData,evento);
  evt.setEventLog(evento);
  dbHelper.saveEvent(evt);
  showToastLog = "BluetoothAdapter.ERROR";
  logger = writeLog(log, "BluetoothAdapter.txt");
  showToast(showToastLog);
}
```

Fig. 5: Bluetooth Adapter States

The next state is to validate when finding other available devices within range, so we store the found device MAC and its NAME. Having the information about unconnected devices, available in the app.

```
if(action.equals(BluetoothDevice.ACTION_FOUND)){
  BluetoothDevice device = intent.getParcelableExtra(BluetoothDevice.EXTRA_DEVICE);
  int rssi = intent.getShortExtra(BluetoothDevice.EXTRA_RSSI, Short.MIN_VALUE);
  Log.w("ACTION_ACL_CONNECTED","Entróa
ACTION_ACL_CONNECTED"+device.getName()+"\n"+device.getAddress()+"\n"+rssi);
  device dev = new device();
  dev.setId(0);
  dev.setName(device.getName());
  dev.setAddress(device.getAddress());
  dev.setContentDesc(String.valueOf(rssi));
  dev.setBloqueado(String.valueOf(false));
  dev.setTime(String.valueOf(Calendar.getInstance().getTime()));
  dev.setBonded(String.valueOf(false));
  dev.setHashCode(String.valueOf(device.hashCode()));
  boolean result = guardaDispositivo(dev);
  evento = "<font color='green'>BluetoothDevice.ACTION_FOUND";
  log += logAdapter(uriData,evento);
  evt.setEventLog(evento);
  dbHelper.saveEvent(evt);
  logger = writeLog(log, "BluetoothAdapter.txt");
  showToastLog = "BluetoothAdapter.ACTION_FOUND";
  showToast(showToastLog);
}
```

Fig. 6: Find available devices Function

Then, it validates the connection adapter status, so it validates the blocked devices, if the device is blocked, we can remove it from the device adapter's list, in other cases, we create the link between devices to pair them.

```
if(action.equals(BluetoothDevice.ACTION_ACL_CONNECTED)) {
  Log.d("ACTION_ACL_CONNECTED","Entró a ACTION_ACL_CONNECTED");
  log                +=                logAdapter(uriData,"BluetoothDevice."+BluetoothDevice.EXTRA_NAME+" -
"+BluetoothDevice.ACTION_ACL_CONNECTED);
  evento = "<font color='green'>BluetoothDevice.ACTION_ACL_CONNECTED";
  evt.setEventLog(evento);
  BluetoothDevice device = intent.getParcelableExtra(BluetoothDevice.EXTRA_DEVICE);
  bloqueo = validaBloqueo(device.getAddress());
  UUID uuid = UUID.randomUUID();
  if(bloqueo){
    try {
      Log.w("ACTION_ACL_CONNECTED","Entró a removeBond");
      Method m = device.getClass()
          .getMethod("removeBond", (Class[]) null);
      m.invoke(device, (Object[]) null);
```


© 2022 Global Journals

```
        evento = "<font color='red'>Dispositivo Bloqueado ("+uuid+"):
"+device.getAddress()+"; "+device.getName();
        log += logAdapter(uriData,evento);
        showToast("Dispositivo bloqueado ("+uuid+") : "+device.getAddress()+" : "+
device.getName());
      } catch (Exception e) {
        Log.e("ACTION_ACL_CONNECTED", e.getMessage());
        evento = "<font color='red'>Error de Dispositivo Bloqueado ("+uuid+"):
 "+device.getAddress()+"; "+device.getName();
      }
    }else{
      try {
        Log.d("ACTION_ACL_CONNECTED", "Start Pairing...");
        Method m = device.getClass()
            .getMethod("createBond", (Class[]) null);
        m.invoke(device, (Object[]) null);
        Log.w("ACTION_ACL_CONNECTED", "Pairing finished.");
        evento = "<font color='green'>Dispositivo Conectado ("+uuid+"):
"+device.getAddress()+"; "+device.getName();
        log += logAdapter(uriData,evento);
      } catch (Exception e) {
        Log.w("ACTION_ACL_CONNECTED", e.getMessage());
        evento = "<font color='red'>Error Dispositivo Conectado ("+uuid+"): "+device.getAddress()+";
"+device.getName();
      }
    }
      if(action.equals(BluetoothDevice.ACTION_ACL_DISCONNECTED)) {
        log += logAdapter(uriData,"BluetoothDevice."+BluetoothDevice.EXTRA_NAME+" –
"+BluetoothDevice.ACTION_ACL_DISCONNECTED);
        evento = "<font color='green'>BluetoothDevice.ACTION_ACL_DISCONNECTED";
        evt.setEventLog(evento);
        dbHelper.saveEvent(evt);
        logger = writeLog(log, "BluetoothAdapter.txt");
        showToastLog = "BluetoothDevice."+BluetoothDevice.EXTRA_NAME+" –
"+BluetoothDevice.ACTION_ACL_DISCONNECTED;
        showToast(showToastLog);
      }
    }
};
```

Fig. 7: Adapter State Connection Validation function

© 2022 Global Journals

b) Device blocking

The state the device is found, is extremely important for the app. Therefore, if the app finds a device and this is active, when establishing a connection, it can be blocked to avoid negative actions to our device from this unwanted device. The following method blockDevice validates the state from this device and updates the blocked column from the Devices chart.

```
/*
 * Valida el estado del dispositivo y actualiza la columna bloqueado
 * */
public boolean blockDevice(device dev){
   boolean result = false;
   String estado = "bloqueado";
   try {
      String args [] = new String[1];
      args[0] = dev.getAddress();
      Cursor cursor =
this.getDevice(devicesContract.deviceEntry.tableName,null,devicesContract.deviceEntry.address+
"=?",args,null,null,null);
      if (cursor.getCount() > 0){
         cursor.moveToFirst();
         String bloqueado =
cursor.getString(cursor.getColumnIndex(devicesContract.deviceEntry.bloqueado));
         if(bloqueado == null){
            estado = "bloqueado";
         }
         else if(bloqueado.equals("bloqueado")) {
            estado = "desbloqueado";
         }
      }else{
         Log.e("deviceDBHelper", "Error bloqueando Dispositivo no
emparejado:"+dev.getAddress() );
      }
      ContentValues cv = new ContentValues();
      cv.put(devicesContract.deviceEntry.bloqueado, estado);
      SQLiteDatabase db = getWritableDatabase();
      db.update(devicesContract.deviceEntry.tableName, cv,
devicesContract.deviceEntry.address + "='" +
dev.getAddress()+"'", null);
      result = true;
   }catch (Exception e){
      Log.e("deviceDBHelper", "Error bloqueando Dispositivo: " + e.toString());
   }
   return result;
}
```

Fig. 8: Block Device Function

V. Testing Phase

a) Bluejacking attack phase

Attack deploy: To start we use the app BlueLock in the target device 2 with MAC A0:8D:16:88:A5:BD and block all the devices that have bluetooth activated. Then, we create a new contact in the attacker device 1 with MAC MAC C0:8C:71:84:94:A1 and it is sent or shared to the target device.

© 2022 Global Journals

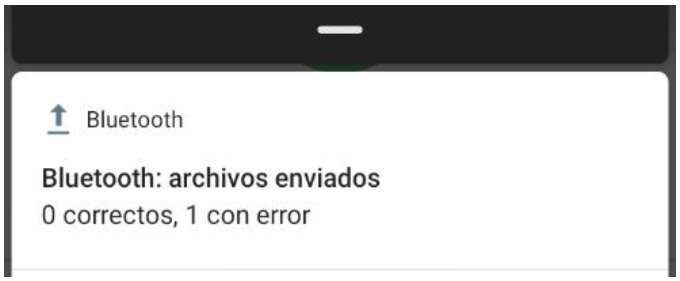

Fig. 9: Bluejacking Attack -Error message on contact transfer.

i. *Bluejacking attack results*

After executing the test, we can see the app blocks the contact sent, blocking all the communication channels between those devices.

b) Bluesnarfing attack test

i. *Deploying attack*

This attack is similar to the previous one, but it enters and steals information from the attacked device. We execute the same previous commands and we get the results shown in the console.

```
root@kali:~# sdptool browse --tree --l2cap C0:8C:71:84:94:A1
Failed to connect to SDP server on C0:8C:71:84:94:A1: Connection timed out
root@kali:~# sdptool browse --tree --l2cap C0:8C:71:84:94:A1
Failed to connect to SDP server on C0:8C:71:84:94:A1: Operation already in progress
root@kali:~# sdptool browse --tree --l2cap C0:8C:71:84:94:A1
Failed to connect to SDP server on C0:8C:71:84:94:A1: Connection timed out
root@kali:~#
```

ii. *Bluesnarfing attack results*

The attacked device avoids the description services reading and keeps inaccessible to the attacker device.

VI. Analysis Results

When we deployed the attacks and used the app Bluelock, we got a positive result due to the effectiveness when blocking attacker devices trying to deploy their attacks. In the bluejacking, it does not allow incoming notifications from the corrupted contact, and in the Bluesnarfing it was completely stopped since the device tried to start communication.

The app, through the blocking device functionality, offers better security and control of the device Bluetooth connections, because it allows the user to choose the devices that will be able to establish a connection and keep track of the bluetooth connections events. After testing the file transfer and Bluetooth attacks we see in the app the functionality filter for the bluetooth adapter states works as expected, so its functionalities could be expanded, defining protocols for every single state of the Bluetooth adapter, increasing the app's usability and security to protect our information from Bluetooth attacks.

The log registration allows us to access the Bluetooth adapter communication events in a short time range and to detect unusual events that take place in the Bluetooth interface range.

The functionality of the app consists in the device's bluetooth adapter control. In case the interface does not respond, it will need to be reseted to get control again, this action can be done by BlueLock.

An app that allows us to see the Bluetooth interface actions is not easily found, because they happen under a transparent communication cape for the user. So with the app BlueLock we can offer a better control of the use that bluetooth connections represent and the events at the moment of establishing connections.

V. Conclusions

The synergy between hacking and the bluetooth attacks, along with software development, allows them to complement each other, facilitating the design, development, testing and deploying of software solutions that improve security in device communication interface, and allow the implementation of closed mobile communication systems.

Most Bluetooth attacks are done while the device's interface is active, due to the protocol working as a receptor waiting for incoming communications and in that state attacks like Bluesnarfing can take place and steal information, taking advantage of the human factor to reach closeness of the target device.

Software solutions for mobile devices focused on connection validation and data packages can improve Android devices' security in places like

© 2022 Global Journals

apartment buildings where there are a lot of mobile devices active and we have a higher chance to be hacked in such environments. BlueLock is a security app oriented to connectivity events that allows unwanted device detection and offers the chance to block them at any time. This is possible by validating the Bluetooth interface state through Intent filters, that is sensible to the Bluetooth adapter changes.

The robustness of the testing set for BlueLock solution, has given positive security results that allow us to block BLuejacking or Bluesnarfing attacks coming from previously blocked devices. In conclusion, we are allowing the user to be responsible for managing the device he allows or not to connect.

References Références Referencias

1. Ramos, A., Barbero, C., Martínez, R., García, A. y González, J. (2015). *Hacking y seguridad de páginas web*. Colombia: Ediciones U, Ra – Ma.
2. Nolasco, J. (2016). Desarrollo de aplicaciones móviles con Android. Segunda edición. Colombia: Ediciones U, Ra – Ma.
3. Ciampa, M. (2018). *Security+ Guide to Networks Security Fundamentals*. Sexta edición. Boston, USA: Cengage.
4. Haataja. K., Hypponen, K. Pasanen, S. y Toivanen, P. (2013). *Bluetooth Security Attacks: Comparative analysis, attacks and countermeasures*. Finlandia: Springer.
5. Conkin, A., White G., Cothren, C., Davis, R., y Williams, D., (2018). *Principles of Computer Security: CompTIA Security+ and Beyond*. USA: McGraw Hill Professional.
6. Minar, N. y Tarique, M. (2012). Bluetooth Security Threats and Solutions: A Survey. International Journal of Distributed and Parallel Systems (IJDPS). 3(1). Recuperado de https://www.researchgate.net/publication/267200901_Bluetooth_Security_Threats_And_Solutions_A_Survey
7. Weed, M. (2018). Bluetooth IoT Applications: From BLE to Mesh. USA: IoT for all. Recuperado de https://www.iotforall.com/bluetooth-iot-applications/
8. García, C. (2010). Hablemos de Spoofing. Hacking Ético. Recuperado de https://hacking-etico.com/2010/08/26/hablemos-de-spoofing/
9. OCCUPYTHEWEB. (2016). The Hacks of Mr. Robot: How to Hack Bluetooth. Los Angeles, California: Wonder How To. Recuperado de https://null-byte.wonderhowto.com/how-to/hacks-mr-robot-hack-bluetooth-0163586/
10. Mitra, A. (2017). What is Bluestack Attack?. The Security Buddy. Recuperado de https://www.thesecuritybuddy.com/bluetooth-security/what-is-blue smack-attack/2/
11. Android. (2019). Conoce android studio. USA: Developers Android. Recuperado de https://developer.android.com/studio/intro/?hl=es-419
12. Android. (2019). Documentation, android.bluetooth. USA: Developers Android. Recuperado de https://developer.android.com/reference/android/bluetooth/package-summary.
13. Alma del Cid, Méndez R. y Sandoval F. (2011). *Investigación. Fundamentos y metodología*. Segunda edición. México: Pearson.
14. ADN Sureste. (2019). Este "error" en el Bluetooth pone en riesgo tu celular. México. Recuperado de https://www.adnsureste.info/este-es-error-en-el-bluetooth-pone-en-riesgo-tu-celular-2130-h/.
15. Clarín. (2019). Advierten sobre los peligros de utilizar el Bluetooth de tu celular. Buenos Aires, Argentina. Recuperado de https://www.clarin.com/tecnologia/advierten-peligros-utilizar-bluetooth-celular_0__WpofinjL.html.
16. Álvarez, R. (2017). Se descubre una "grave vulnerabilidad" en Bluetooth que deja expuestos los dispositivos a posibles ataques. España. Recuperado de https://www.xataka.com/seguridad/se-descubre-grave-vulnerabilidad-bluetooth-que-deja-expuestos-dispositivos-a-posibles-ataques.
17. Carro, G. (2019). Esto es lo que puede pasar si tienes el bluetooth del móvil siempre conectado. Revista GQ. España. Recuperado de https://www.revistagq.com/noticias/articulo/bluetooth-movil-siempre-conectado-peligros-hackers.

© 2022 Global Journals

This page is intentionally left blank

© 2022 Global Journals

Global Journal of Researches in Engineering: F
Electrical and Electronics Engineering
Volume 22 Issue 1 Version 1.0 Year 2022
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

Real-Time Application of the Formant Analysis Algorithms for Cryptoprotection of IT Systems

By Vyacheslav Kunev

Technical University of Moldova

Abstract- We examine applications of expanded algorithms of formant analysis of modern number theory for protection of binary information from hacking and intentional distortion in various IT-systems. These include real-time confidential conversations and information exchange between server and client through local or external networks, as well as phone and mobile communications based on a modified RSA-m cryptosystem, which realizes quick change of keys and guarantees the degree of secrecy in short or medium term.

Keywords: information protection, number theory, formant analysis, cryptography, algorithms, RSA-mAB.

GJRE-F Classification: FOR Code: 090699

Strictly as per the compliance and regulations of:

© 2022. Vyacheslav Kunev. This research/review article is distributed under the terms of the Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0). You must give appropriate credit to authors and reference this article if parts of the article are reproduced in any manner. Applicable licensing terms are at https://creativecommons.org/ licenses/by-nc-nd/4.0/.

Real-Time Application of the Formant Analysis Algorithms for Cryptoprotection of IT Systems

Vyacheslav Kunev

Abstract- We examine applications of expanded algorithms of formant analysis of modern number theory for protection of binary information from hacking and intentional distortion in various IT-systems. These include real-time confidential conversations and information exchange between server and client through local or external networks, as well as phone and mobile communications based on a modified RSA-m cryptosystem, which realizes quick change of keys and guarantees the degree of secrecy in short or medium term.

Keywords: information protection, number theory, formant analysis, cryptography, algorithms, RSA-mAB.

I. Introduction

The inefficiency of existing implementations of RSA cryptosystem in real-time applications calls for identifying new methods that would allow to take advantage of its otherwise attractive features. Currently there are no known methods analogous to RSA algorithms that could protect information in real-time applications such as mobile or voice communications. We consider the possibility of using a modified RSA algorithm, labeled RSA-m. The idea underlying the modification is to send not the encrypted information through open or even secured channels but only some specific data about its encryption instead. We offer several versions of such a modification which, however, require additional research. The ultimate purpose is to increase the working speed of the algorithm similar to RSA system to exploit its full potential in real-time information transmission.

The relatively low working speed but high cryptographic resistance of the RSA system motivate the cryptographers' search for potential improvements to the system to enable its use with the typical information flows or for securing of real-time information where privacy needs to be protected in the short term (from few minutes to several months). Below we consider one of such procedures, based on transmitting not the information itself, but only some indirect data about this information in real time. The amount of these data is much lower than the original information and, therefore, these data can be transmitted in encrypted form with required crypto resistance through the channels with limited speed and bandwidth (e.g., 64 KB/s) based on the use of, e.g., RSA cryptosystem, but without significant delays in time. The amount of transmitted information can be significantly reduced, e.g., by representing it in the formant form, which allows to reduce its encryption (decryption) time to be commensurate with the bandwidth of mobile communication channels. Another strategy for modifying encryption algorithms in mobile communications in this case is based on the use of short keys, but with the provision of the high speed of their turnover. The author considers this extension in another publication.

II. Information Protection using RSA-MAB Algorithm

The main idea of the proposed algorithm is in using so-called *numeric formants*, which were introduced in [1] and detailed in [2] and [3]. Numeric formants allow to represent any

Author: Technical University of Moldova and IT-company Director, Chisinau, Republic of Moldova. e-mail: kunev@deeplace.md

© 2022 Global Journals

number as a simple linear structure. Moreover, the time needed to represent and to recover the number for the encryption and decryption will be significantly lower than the time required when using of the algorithms of the classical RSA system.

It is known from [1], that linear and/or nonlinear formants using only 3 or a few more parameters, *allow to significantly reduce the length of the digital message* regardless of the length of the transmitted number n. The advantage of such an approach is that the so-called base of the formant can be any simple or composite number of substantially lower length than is required for the encryption in the classic RSA cryptosystem.

Below we consider several algorithms using linear formants for the transmission of the information requiring short-term secrecy, where the amount of time needed for encryption and decryption is considerably reduced, even after accounting for the additional operations for transforming the message.

a) AB1 Algorithm

As known from [2] and [3], any number N can be represented, in terms of the formant analysis, as a binomial structure $N = pk + q$, where p is the formant's base, k is the core and q is the remainder. Knowing these three arguments allows us to easily recover the initial number. Types, properties and characteristics of the formant algebra are described in [1].

This way of representing numbers allows to encrypt not the number N itself, but only 3 small numbers instead. The main difference is that N is a large number of the order of $10^{20} \dots 10^{500}$ or higher, while p, k and q are any whole numbers, simple or composite, the length of which is determined only by the required transmission speed through an open channel. It is recommended to choose the base of the formant p as a number with a length of the order of magnitude of the RSA key, such as a number, corresponding to the block cipher and which doesn't lead to the reduction of the transmission speed. This recommendation allows to use the RSA keys of the medium length, while the presence of the fast simple number generator in the system allows to change them quickly, even in the block format, which will obviously increase the difficulty of hacking.

To implement the RSA-m algorithm, a dynamic database is created in the memory, for instance, in a format of the matrix $\boldsymbol{P}$ with indexed cells which keep pre-generated information used for the formant construction. For example, a 100×100 matrix can contain such information for 10,000 different formants.

After each single use of all of the values p_{ij} of the matrix $\boldsymbol{P}$ the algorithm prescribes an automatic update of all cells of the matrix, on sending and receiving sides.

Depending on the required strength of the encryption, the matrix in the memory of the microprocessor may be built with a hard or flexible updating program, with an automatic or manual transmission of the matrix. In one version it could even be the same matrix, where the cell names are changed based on an index. The remainder and the core values are then encrypted using the RSA-m algorithm, cryptoresistance of which is guaranteed by the switch in real-time of the keys for each binomial $d-$bit number of an analog signal or of a symbol (number, byte, block) in an open digital message. On the receiving end, the message is decrypted with a special procedure, which recognizes transmitted cell addresses and decrypts other arguments of each formant, allowing to restore the true value of the transmitted numerical message. The message itself can be a text message in any possible language, an image of any class and type, a piece of speech or music, etc. Figure 1 contains a block-scheme of the AB1 algorithm.

© 2022 Global Journals

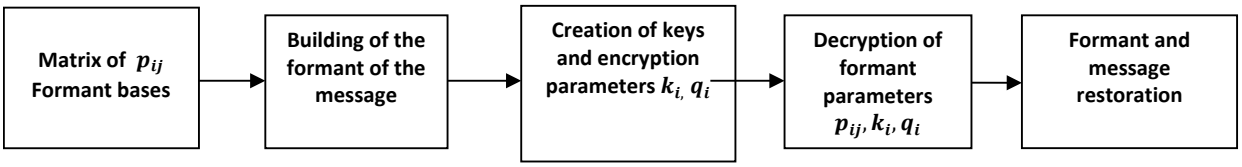

Figure 1: Block-Diagram of AB1 algorithm

1. From the analog signal being transmitted, after digitizing it, the block is formed: binomial message of 32(64)... bit;
2. From the basic matrix block in the memory of the device the base of the formant p_{ij} is randomly chosen and recorded in the cell $d1$;
3. Numeric block 64 bit (Ex. 1) is represented in the formant format. Its core k and remainder q are defined: $k_i = d2$ and $q_i = d3$;
4. The encription keys for encrypting numbers $k_i = d2$ and $q_i = d3$ are chosen;
5. The message $d1d2d3$ about the formant is formed;
6. The message $d1d2d3$ about the formant is encrypted;
7. Encrypted data is passed through an open channel;
8. The block of 64...bit is received;
9. The base of the formant p_{ij} is extracted from the received block;
10. Numbers $k_i = d2$ and $q_i = d3$ are extracted from the block;
11. The message-formant is recovered: $F = p_{ij} \cdot k_i + q_i = p_i \cdot d2 + d3$.

Let's consider a simple example that illustrates the RSA-m algorithm's application.

Example 1. Let's encrypt the message " $HFTY$ ". For simplicity we will use small numbers (in practice, much larger numbers are used, by several orders of magnitude).

1. Let's pick two simple numbers $p = 3$ and $q = 11$. *Their product* is $N = 3 \cdot 11 = 33$.
2. Find $(p-1)(q-1) = 2 \cdot 10 = 20$. Therefore, the number for the private key d can be chosen to be smaller than 20 and a co-prime integer with 20, e.g., $d = 3$ (or another: 7, 11, 13, 17, 19, ...).
3. Now let's select an open key - number e. We can choose any number that satisfies the relation $(e \cdot d) = 1(mod\,20)$. With d =33, e must satisfy $(e \cdot 3)(mod\,20) = 1$ as e.g., $e = 7$ does. Indeed, $7 \cdot 3 = 21$; $21(mod\,20) = 1$.
4. Let's represent the message that is being encrypted as a sequence of whole numbers by applying, e.g., the following assignment: $F \to 1$, $T \to 2$, $H \to 3$, $Y \to 4$. Then the encoded message is then: "$HFTY$"= $(\mathbf{3}, \mathbf{1}, \mathbf{2}, \mathbf{4}) = S1$. Let's encrypt this message using an open key $\{e, N\} = \{7, 33\}$.

   Cipher $T1 = (P^7)(mod\,N) = (3^7)(mod\,33) = \mathbf{2,187\ (mod\ 33)} = \mathbf{9}$; *first we raise the number to the power, then divide it by modulo* N. *The division remainder yields the result of the encryption.*

   $Cipher\ T2 = (A^7)(mod\,N) = (1^7)(mod\,33) = \mathbf{1\ (mod\ 33)} = \mathbf{1}$,

   $Cipher\ T3 = (E^7)(mod\,N) = (2^7)(mod\,33) = \mathbf{128\ (mod\ 33)} = \mathbf{29}$.

© 2022 Global Journals

$$Cipher\ T4 = (H^7)(mod\, N) = (4^7)(mod\, 33) = \mathbf{16,384\ (mod\ 33) = 16}.$$

Thus, the open message $S1 = HFTY = (3, 1, 2, 4)$ can be represented as an encrypted message $SE1$, i.e., the numerical sequence $SE1 = (\mathbf{9, 1, 29, 16})$, which, for instance, *corresponds to the text* "***PFLJ***".

5. Now let's create an encrypted message *for the transmission through an open channel* that includes the auxiliary information, for example, of the following type (it can be of any order or content).

$$\underbrace{003}_{\text{for 3 ranks}}\ \underbrace{023}_{\text{cell address}}\ \underbrace{009}_{\text{P}}\ \underbrace{001}_{\text{A}}\ \underbrace{029}_{\text{E}}\ \underbrace{016}_{\text{H}}\ \ldots\ \underbrace{[0?101\&]}_{\text{add'l information}}$$

- The first three decimals - the digit number for the code processing; shows us the length of the machine word, i.e. every three decimal digits.
- The second group of decimals - the cell number of matrix P in memory, which the controller on the receiving side must extract from memory.
- The third group of three decimal digits contains information for the decryption with RSA algorithm (can contain any number of the "triples" depending on the length of the sent block of bits - 16, 32, 64 etc.).
- The last, for instance, 6 or more digits include additional service information: the ending of the sent message, the parity check etc. Thus, while sending 64...-bit, we must choose the first and the last 6 digits, which contain all the information about decryption of the remaining 58 decimal digits.

We created encrypted message $\{9, 1, 29, 16\}$, which is the result of the cryptography with a secret key $\{7, 33\}$. On the receiving side in the cell $p_i = p_{23}$ the corresponding numbers are located: "private key d" and the modulus of the cryptokey: $d = 3$; $N = 33$. That is why it is so easy to decrypt the encrypted message "912916".

Let's decrypt the received encrypted message $(9, 1, 29, 16) = PFLJ$ on the basis of the private key $\{d, N\} = \{3, 33\}$. We get

$$\begin{aligned}
Initial\ T1 &= (9^3)(mod\, 33) = 729\,(mod\, 33) = \mathbf{3},\\
Initial\ T2 &= (1^3)(mod\, 33) = 1\,(mod\, 33) = \mathbf{1},\\
Initial\ T3 &= (29^3)(mod\, 33) = 24389\,(mod\, 33) = \mathbf{2},\\
Initial\ T4 &= (16^3)(mod\, 33) = 4096\,(mod\, 33) = \mathbf{4};\quad (3, 1, 2, 4) \rightarrow "HFTY".QED.
\end{aligned}$$

b) AB2 Algorithm

Version 1. Storage cells indexing.

1. In the matrix of 10,000 cells (1000 rows x 1000 columns) the cells are numbered in the natural order; they can also be represented as a double-index variable p_{ij}, where $ij = 00, 01, \ldots 99$. For example, the cell #457 has index p_{0457}, and the cell #4057 will have the number or index-address p_{4057}.
2. Each cell $P_{ij}(e, d, n)$ of the matrix P, will now contain the index number, which is encrypted by RSA-m system. For instance, in the cell #0009 this number is 3; cell

© 2022 Global Journals

#0001 will contain number 1; cell #0029 - number 2; cell #0016 - number 4, which corresponds to the decryption with the key d = 3; N = 33; and encrypted with the key $e = 7$. Other cells of the array will be filled in exactly same way.

3. The algorithm of the cell mixing in Version 1 does not change the cell's content; it only changes it's index number.

To further increase the cryptoresistance level of the RSA-mAB algorithm, we could randomly change the length of the encrypted blocks, with the corresponding change of the cryptokeys' length. The number of such arrays and their size depend on how long the information needs to be kept secret and on the memory size of the controller on which the RSA-mAB will be realized.

Version 2. Application of the formant analysis. The block-message with the length 32 (64)... bit is formed.

1. The p_{ij} formant base is randomly selected from the basic matrix and its number is written as the message $d1$ (the base of the created formant is stored in the cell $d1$).
2. The initial number of the formed informational block is represented in the formant form, and all its remaining parameters (the core $k_i = d2$ and remainder $q_i = d3$, are defined by the selected base and are written in the messages $d2$ and $d3$.
3. Transmitted message $d1d2d3$ is formed.
4. Crypto keys for encryption of cores k_i and remainders q_i are generated.
5. The message about the $d1d2d3$ formant is encrypted.
6. Encrypted message is transmitted through an open communication channel.
7. The block 64... bit is received.
8. Coordinate-address p_{ij} is extracted from the received block.
9. The value of the formant base is restored.
10. k_i and q_i are extracted from the corresponding block.
11. The formant is restored from the encrypted message using the standard formula.

As a similar example, consider the encryption of the message "EDA" or of its numeric code 651. Let's represent the 651 code in the formant form, i.e. as the sum of a product and a remainder, and choose as the base, e.g., random simple numbers 237, 54, 119, etc. The matrix of the RSA-m system keys from Version 1 is replaced by the format's base matrix, which creates the first set of the randomly chosen bases of various length and properties (simple or composite). Returning to our example, recall that our message is: $S2 = 651$.

- We choose the base randomly, e.g., $p = 54$. In the controller's storage write down $d1 = 54$.
- Calculate the formant of the number 651 on the base 54: $F_{\mathbf{54}}(651) = 12 \times \mathbf{54} + 3$. Write down in the storage it's arguments: $k_i = d2 = 12$ and $q_i = d3 = 3$.
- The machine defines the length of the information block $S0$ being formed for encrypting (for example, the first three triples of decimals): $S0 = 054\,012\,003$.
- Choose the encryption key e from the cell #54 of the key matrix in memory.
- The message is encrypted:

$$C_1 = 54^7 (mod\, 33) = 24,794,911,296\, (mod\, 33) = 12;$$

© 2022 Global Journals

$$C_2 = 12^7 (mod\, 33) = 35,831,808\, (mod\, 33) = 12;$$

$$C_3 = 3^7 (mod\, 33) = 823,543\, (mod\, 33) = 28.$$

Thus, the encrypted message will take the following form: 012 012 028. Next, we form the transmitting block with the additional service information and send it through the open channel to be decrypted on the receiving side:

- Decrypt the block, which yields $\underbrace{54}_{base}\ \underbrace{12}_{core}\ \underbrace{3}_{remainder}$
- Restore the formant: $S2 = 54 \times 12 + 3 = 651 \rightarrow EDA$.

III. Conclusion

The discussion and the examples provided above illustrate the conceptual possibility of transmitting encrypted voice messages in real-time mode with transmission speed of about 64 kb/s, using, for example, the connection channel such as Telegram or Telegram Messenger.

Clearly, other approaches based on the use of formants for message transmission are also possible, e.g., 10 different approaches are described in [3]. We considered the most obvious ones. For example, matrix $M1$ 12×12 contains $64 \times 64 = 4,096$ decimals (digits), which will be encrypted with 64 different keys. First, 64 bit digits are encrypted (rank: 6 decimal digits). Double the number of digits and begin encrypting 124-bit numbers in order to raise the rank to 12 decimal digits. $2^{10} = 1,024$ bit-numbers and each 10-bit number is located in the cell of matrix $10 \times 10 = 1,000 \approx 1024$.

For matrix $M2$ 64×64 – a matrix with a rank of 10 decimals (number of bits) – there are $4,096 = 2^{12}$ of digits selected, which are encrypted with the key $K1$. In matrix $M2$ the same 4,096 digits are selected, but encrypted with another key $K2$, etc. Then, matrices $MZ - K\ Z$, where Z represents the length (number of bits) of encryption keys, for example 10 or 100 etc. what allows to significantly reduce the duration of encryption by replacing multiple number multiplications with simpler processes. This allows to use the RSA-mAB1 algorithm for protection of real-time information and to improve the stability of cryptographic keys with frequent changes in the block length.

MZ matrices can be built separately (independently) using different methods. In the $AB1$ algorithm this operation differs with respect to the content of the matrices, because they were created with the use of different keys.

$AB2$ algorithm uses one and the same matrix, with unchanged content of its cells, but it changes cell addresses. The redistribution of cells' contents of matrix M can be implemented in various ways. It can be random or according to some algorithm applied to each matrix cell such as, e.g., the relation $p_{ij} = p_{(i+k,j+l)}$, changing k and j in a such way, that all or just some cells are affected by the algorithm.

Our library of algorithms includes an extended $AB - univ$ algorithm which allows to use any of the algorithms described above for real-time crypto-problems. Obviously, such message will be more difficult to decrypt in a relevantly short time. Even with writing a message on hard media, it can not be reasonably quickly decrypted so that hacking will require dozens of years, as the hacker knows neither the length (range) of keys, nor the block length, nor the transition rule from one pair of keys to another. Besides, he doesn't know the keys at all.

© 2022 Global Journals

This is *internal information of the security system*. Each external communication can of the same type, but its content will differ in the meaning of the information transmitted in each session and the same phonemes will be represented in different messages by different codes.

References Références Referencias

[1] Balabanov A. A., Agafonov A. F. Сопоставительный анализ и его приложения. Классические и современные задачи теории чисел и криптографии. [Comparative analysis and its applications. Classical and modern problems of the theory of numbers and cryptography.] Lambert Publishers, Germany. 2016. ISBN 978-3-659-92621-1

[2] Balabanov A. A., Kunev V. V. Защищённые IT-системы на основе алгоритмов формантного анализа. [Protected IT-systems based on the formant analyses algorithms.] Lambert Publishers, Germany. 2016. ISBN 978-3-659-94826-8

[3] Balabanov A. A., Kunev V.V. Способ шифрования двоичной информации и устройство для его осуществления. [A method of binary information encryption and application for its implementation.] Patent of RM, http://www.findpatent.ru/patent/209/2099885.html

[4] Balabanov A. A., Agafonov A. F., Riku V. A. Алгоритм быстрой генерации ключей в криптографической системе RSA. [An algorithm for quick key generation on the cryptographic RSA system.] http://www.vntr.ru/ftpgetfile.php?id=323

[5] Balabanov A. A., Agafonov A. F., Kojuhari I., Возможности создания новых и модернизированных алгоритмов для системы RSA. [Possibilities of creating new and advanced algorithms for RSA system.] http://www.vntr.ru/ftpgetfile.php?id=451

[6] Romantev I. B. , Timofeev P. A. , Shanighin B. F. Защита информации в компьютерных системах и сетях. [Information Protection in computer systems and networks.] Edited by Shanighina V. F. -2nd edition revised and extended. M.: Radio i svyazi. 2001. ISBN 5-256-01518-4

[7] Bikov V. A., Babenko L. K., Spiridonov O. B. Новые технологии электронного бизнеса и безопасности. [New technologies of electronic business and security.] Pub: Radio i svyazi, 2002. ISBN 5-256-0182-6

© 2022 Global Journals

This page is intentionally left blank

© 2022 Global Journals

Global Journal of Researches in Engineering: F
Electrical and Electronics Engineering
Volume 22 Issue 1 Version 1.0 Year 2022
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

FPGA-Based Multi-Channel A/D Converter by Optimal Duty-Cycle Modulation Technique

By Gisele Beatrice Sonfack & Robert Tchitnga

University of Dschang

Abstract- In this article, we present the multichannel architecture of the analog-to-digital converter based on the duty cycle modulation technique with prototyping on FPGA hardware targets. This diagram is the continuation of the work presented in [1],[2] proving the feasibility of the single-channel version of this converter on the one hand and its characterization on the other. This conversion approach is based on the use of parallel duty cycle modulation cells, each used as an independent 1-bit interfacing circuit per analog channel. In addition, all of the modulated output bits associated with all of the analog inputs are simultaneously sampled and processed. The principle already demonstrated [11] and the important properties revealed by this A / D conversion scheme studied in depth in the review articles are presented, then, an experiment with a 4-channel virtual oscilloscope is presented, in order to show the potential results of the prototype of the multi-channel version of the FPGA-based converter.

Keywords: analog-to-digital converster, optimal duty-cycle modulation, iir decimation filter, FPGA, JTAG communication, virtual and hardware co-simulation, embedded instrumentation systems, virtual simulation, multichannel.

GJRE-F Classification: FOR Code: 090699

Strictly as per the compliance and regulations of:

© 2022. Gisele Beatrice Sonfack & Robert Tchitnga. This research/review article is distributed under the terms of the Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0). You must give appropriate credit to authors and reference this article if parts of the article are reproduced in any manner. Applicable licensing terms are at https://creativecommons.org/licenses/by-nc-nd/4.0/.

FPGA-Based Multi-Channel A/D Converter by Optimal Duty-Cycle Modulation Technique

Gisele Beatrice Sonfack [α] & Robert Tchitnga [σ]

Abstract- In this article, we present the multichannel architecture of the analog-to-digital converter based on the duty cycle modulation technique with prototyping on FPGA hardware targets. This diagram is the continuation of the work presented in [1],[2] proving the feasibility of the single-channel version of this converter on the one hand and its characterization on the other. This conversion approach is based on the use of parallel duty cycle modulation cells, each used as an independent 1-bit interfacing circuit per analog channel. In addition, all of the modulated output bits associated with all of the analog inputs are simultaneously sampled and processed. The principle already demonstrated [11] and the important properties revealed by this A / D conversion scheme studied in depth in the review articles are presented, then, an experiment with a 4-channel virtual oscilloscope is presented, in order to show the potential results of the prototype of the multi-channel version of the FPGA-based converter. The design and implementation are carried out by software and hardware co-simulation using platforms such as the Simulink / Xilinx based system generators in which the ODCM-ADC is implemented, and the programming tool Vivado 2019.2 from Xilinx. The hardware platform consists of the Zynq 7000 FPGA kit (25 MHz sample clock), equipped with an integrated FPGA-based IIR (infinite impulse response) digital decimation filter and a JTAG communication cable / connectors on PC. The co-simulation systems are built and successfully tested for a modulating bandwidth of 3 KHz. These performance levels, obtained under virtual and hardware co-simulation conditions, show a relevant challenge of an oversampling multichannel ADC, compared to most ADC oversampling techniques. As a merit, the proposed FPGA-based ADC technique is a novel and relevant ADC architecture for on-board instrumentation systems and industrial electronics.

Keywords: analog-to-digital converster, optimal duty-cycle modulation, iir decimation filter, FPGA, JTAG communication, virtual and hardware co-simulation, embedded instrumentation systems, virtual simulation, multichannel.

I. Introduction

Multichannel analog-to-digital converters (ADCs) are necessary in a context of digital processing of signals coming from several sensors or sources given that nature is essentially analog through its manifestations which can be images, sound, vibrations. The great power of digital computers has revolutionized the fields of industrial instrumentation and systems engineering through analog-to-digital converters which combine the role of interface between the analog world and the computer. Many applications require the digitization of signals from current output sensors, such as photo sensors and photodiodes, and in multichannel conversion systems lower power per channel is important so that as the number of channels increases, the power does not increase. not increase drastically [3], [4]. Thus, the possibility of directly digitizing the currents without current-to-voltage conversion saves the energy, the surface area and the design time necessary for the implementation of the converters. The main objective of this article is to study and implement on FPGA and test an optimal multichannel cyclic cycle modulation ADC. This circuit provides an interface to analog sensors and minimizes the dynamic range dependence of the conventional oversampling ADC on the supply voltage. The following sections explain the history, background, of the duty cycle modulation technique.

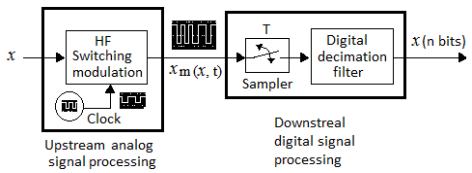

Fig. 1: Oversampling ADC principle[1]

In Section II, the knowledge on the DCM-based ADC topology is outlined. Then, a case study and prototyping multi-channel A/D converter is presented in Section III, followed in Section IV by the hadware co-simulation results. Then, the conclusion of the paper is presented in Section V.

II. Recall of ODCM-ADC Architecture

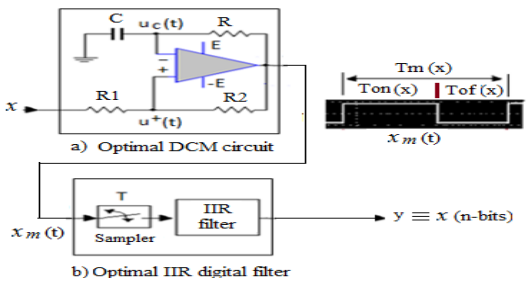

Fig. 2: DCM-Based ADC topology*[1]*

Author α: Douala Advanced Vocational Technology Center, Electrical Department, Douala, Cameroon. e-mail: beatricesonfack@gmail.com
Author σ: University of Dschang, Falculty of Sciences, Department of Physics, Dschang, Cameroon. e-mail: tchitnga@yahoo.fr

© 2022 Global Journals

The block diagram of our multi-channel ODCM-ADC is inspired by the single-channel converter taken from [2], and is shown in Fig. 1. It consists of two main parts, connected in tandem, that is to say an optimal upstream DCM circuit (see Fig. 2 (a)) with modulating input x and DCM output xm (t), and an optimal downstream digital filter IIR (Infinite Impulse Response) (see Fig. 2 (b)). The optimal DCM demodulator circuit is modeled by a set of nonlinear parameters which form a constrained optimization problem, while the optimal IIR filter is synthesized according to the specifications of the weighted pth standard. The optimal parameters of multi-channel ADC system prototyping based on optimal duty cycle modulation considered in this section are taken from previous work [] namely: fs = 25MHz (sampling period or Ts = 1 / fs = 40 ns so equivalent), fs = 3KHz (modulating bandwidth), fm (0) = 172 KHz (DCM base oversampling frequency), E = 9 volts (power), * = 0.012366816265686 where α * = R1 / (R1 + R2) and RC = 0.000115510618677 s. It should be remembered from [1] that the DCM circuit shown in Fig.2 is modeled by equation (1), which is quite easy to implement in the Matlab / Simulink framework. In addition, the transfer function z of the second-order optimal digital IIR decimation filter is given by (2).

$$\begin{cases} u^{+}(t) = \alpha\ x_m(t) + (1-\alpha)x(t) & \text{(a)} \\ \varepsilon(t) = u^{+}(t) - u_C(t) & \text{(b)} \\ x_m(t) = E\ sign\left(\varepsilon(t)\right) & \text{(c)} \\ \dfrac{du_C(t)}{dt} = -\dfrac{1}{\tau}uc(t) + \dfrac{1}{\tau}x_m(t) & \text{(d)} \\ x(t) < E & \text{(e)} \end{cases} \quad (1)$$

$$F_0(z) = \frac{b2\,z^2 + b1\,z + b0}{z^2 + a1\,z + a0} \quad (2)$$

with

$b2 = 8.263545624646787\ e^{-08}$
$b1 = 1.652709124929357\ e-07$
$b0 = 8.263545624646787\ e-08$
$a1 = -1.999777875893610$
$a0 = 0.9997782064354348$

III. FPGA-Based of Multi-Channel ODCM-ADC Design

The FPGA-Based multichannel ODCM-ADC design is conducted under Simulink workspace, according to the schematic diagram presented in Fig.4. The upstream subsystem shown in Fig.3(c). As in the case of single input ODCM or sigma-delta A/D converters ([1],[2]), an important problem to take into account when sampling a discrete sequence given by "Eq. 3", is the over sampling phenomenon [10] It is due to the fact that theanalog original version of "Eq. 3" is a time varying square wave, with a wider bandwidth compared tothat of the modulating wave *x(t)* encapsulated in $R_m(x(t))$.

$$(2R_m(x,\alpha) - 1)E + \frac{4E}{\pi}\sum_{n=1}^{\infty}\sin\left(\frac{n\,\pi\,R_m(x,\alpha)}{n}\right)\cos\frac{2\pi\,n\,t}{T_m(x)} \quad (3)$$

Thus, the sampling theorem used in digital signal processing [1],is applicable in this case to the target modulated wave $x_m(t)$ to be sampled. Let *fosc* (*x j t*))(being the fundamental frequency of the oscillator associated with the *jth* channel, its maximum value *fosc* max which occurs for *xj*(t) =0, is assumed tobe an identical constant for all channels, in which case the bandwidth *f* max related to the periodic square wave is large enough compared to *f* max [9]. Thus, assuming that the admissible bandwidth of the *j*th analog signal *xj*(t) is a constant *fBj*, then the following constraint should be satisfied when choosing the simultaneous sampling frequency *fs* ,

$$\begin{cases} f_{max}(0,\alpha) = \dfrac{1}{2.\tau.\ln\left(\frac{\alpha+1}{1-\alpha_1}\right)} \\ f_{min}(x_{max},\alpha) = \dfrac{1}{\tau.\ln\left(\frac{[((1-\alpha)x_{max})^2-((\alpha+1)E)^2]}{[((1-\alpha)x_{max})^2-((\alpha-1)E)^2]}\right)} \end{cases} \quad (4)$$

Fig. 3(a) is a Simulink-based model of the DCM circuit given by (1), with analog modulating input Xs ≡ x as in Fig. 2(a), and with a sampled modulation output xm. Then, the downstream subsystem presented in Fig. 2(b) is modelled as a digital IIR filter given by (2), which is implemented using visual building resources and configuration panels available in Xilinx System generator frame work. The IIR filter is implemented according to the direct form approach. The implemented only required 5multipliers, 5 registers and an added tree, although the full resolution is maintained across the multipliers and the tree. In addition, the data width cannot grow indefinitely, and thus a quantization block is placed at the output of the adder to reduce the width of the data. At this step, it is worth noting that the whole schematic diagrams presented in Fig 2, is tested over the modulating band width followed by the creation and the configuration of an additional hwcosimblock for further hardware co-simulation requirements. In addition, the DSP code for the target FPGA is generated as an input module for XilinxISE framework. As an implication the related high level RTL diagram shown in Fig. 4, is organized into 9 digital processing modules.

a) Virtual Simulation of the multichannel ODCM-Based ADC System

Following (2), the ODCM-based ADC system, designed in depth in this section, has been implemented in Simulink framework as shown in the virtual model (see Fig. 4). It consists of a visual model of the optimal DCM block as shown in Fig. 4 (a), corresponding to the first order dynamic model(2), and a discrete transfer function F(z) of the optimal second order digital IIR filter.

The simulation required for performance evaluation of the overall prototyping ODCM-based ADC, is conducted over a sufficiently wide range of frequency including the modulating bandwidth of 3 KHz. In

© 2022 Global Journals

addition, a sample of detailed result related to a sine modulating input (1 KHz, 100Hz, 1.5kHz, 2kHz, 1 Vpp) is presented in Fig. 4, whereas all results of hardware co-simulation obtained under variable modulating frequencies are summarized in Fig. 4 [5].

b) Design chart of a multichannel ODCM-ADC based on FPGA

The design workflow for an FPGA application is usually done in several stages. First of all, algorithmic specifications make it possible to define the architecture by an algorithm-architecture fit approach. This architecture is then described with the HDL language. You can then simulate the system and modify it if necessary [2]. Then come the phases of synthesis and routing placement, which consist in determining which elements will actually be used in the FPGA and how they will be connected to each other, where in the component they will be placed, etc. Each phase requires verification of the correct timing and, if necessary, modifications.

The hardware description language such as VHDL or Verilog, usually used for the development of FPGAs, are of a concurrent nature. Programming in VHDL implies a good knowledge not only of the algorithm but also of the FPGA and the compiler used[2]. To better exploit the intrinsic parallelism of the algorithm, it is necessary to perform the processing tasks in parallel (non-sequential) to satisfy the time constraints. For most control or signal processing specialists who are very often software researchers and engineers, these hardware languages are unfamiliar and sometimes difficult to use. This is probably one of the reasons holding back the democratization of FPGA technology. In an attempt to provide an appropriate solution to this problem, co-design platforms by association of several development environments have been proposed. The general System Generator/Silulink chart is schown in figure 3.

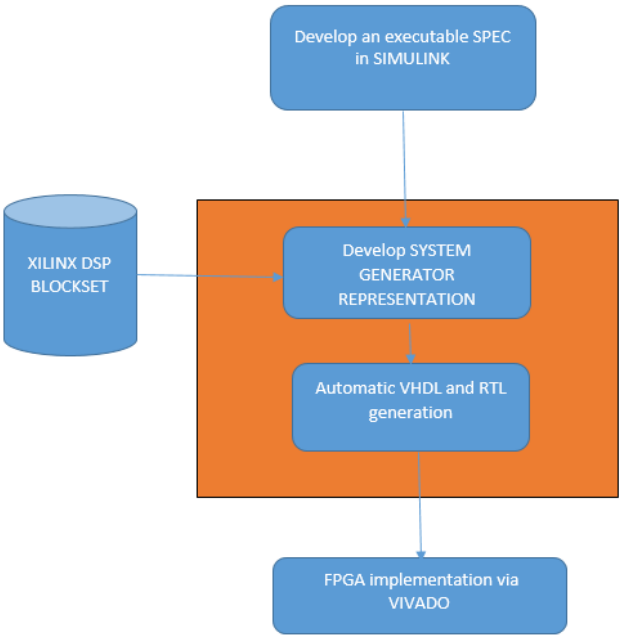

Figure 3: General diagram of the design flow

IV. Hardware Co-Simulation of Multichannel ODCM-ADC

Co-design is the design technique of the day for its many advantages so one can co-use MATLAB / Simulink software and System Generator building blocks to implement SISO downlink chip systems. or to propose a design of QPSK modulator on FPGA which consumes little power and using the hardware co-simulation, to obtain a reduction in the cost of the hardware requirements.

As part of this work, the development of the converter prototype is carried out with the XSG software. This is a toolkit developed by Xilinx to be integrated into the Matlab/Simulink environment and which lets the user create highly parallel systems for FPGAs. The created models are displayed as blocks, and can be linked to other blocks and to other Matlab-Simulink toolkits such as SPS. Once the system is complete, the VHDL code generated by the XSG tool exactly reproduces the behavior observed in Matlab. For rapid prototyping, the choice of this tool is easily explained. As the conversion system needs to be checked and simulated often and quickly throughout development, it is much easier to analyze the results with Matlab than with the tools usually associated with VHDL, such as Modelsim[6], [7].

© 2022 Global Journals

When the prototype is up and running, the switch to the hardware platform for field testing is rapid, making validation of the prototype a feasible project in the short term. The PC and the FPGA board are connected via a suitable communication cable/connectors (USB, Ethernet or JTAG). Thus, in a hardware co-simulation context, the digital signals involved in a DSP/FPGA chip are automatically uploaded to the PC-based virtual platform for real-time visualization. During a co-simulation session, the virtual simulator and the hardware DSP are simultaneously started and driven under the same operating conditions (input and parameters), while the real-time behavior of the hardware DSP is brought to the virtual simulation environment for rapid design, visualization and performance evaluation [8]. The co-simulation environment created in this research work for the rapid computation and evaluation of the predicted and experimental characteristics of multi-channel ODCM-ADC prototyping based on FPGA, is presented in Fig. 4

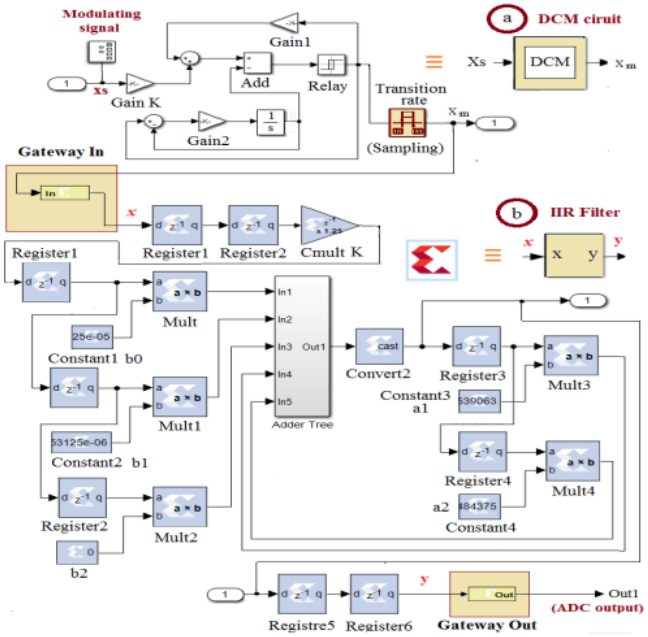

Figure 4: *FPGA-Based ODCM-ADC design architecture*[2]

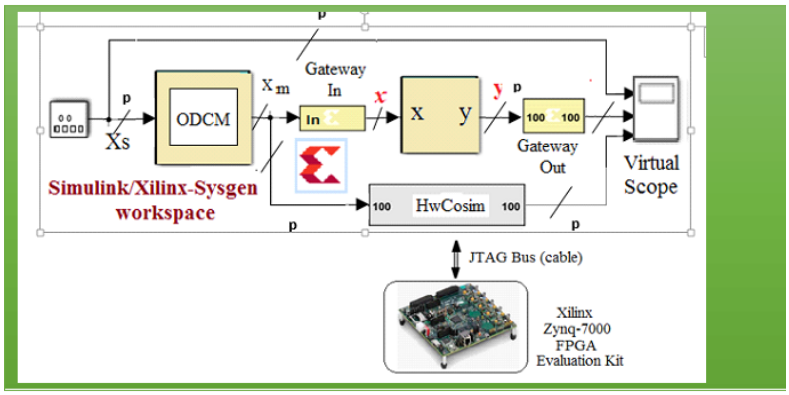

Figure 5: Hardware Co-Simulation environment

Finally, a summary of simulation results obtained are presented in Fig. 7.

The results presented here show that, the proposed multichannel ODCM-based ADC offers high performance within 3 KHz of modulating bandwidth. The high level of predicted performance obtained from virtual simulation of a prototyping system, is a great challenge an oversampling ADC topology, consisting of a piece of ODCM circuit with impressive properties, and a single stage of optimal 2nd order digital decimation filter.

© 2022 Global Journals

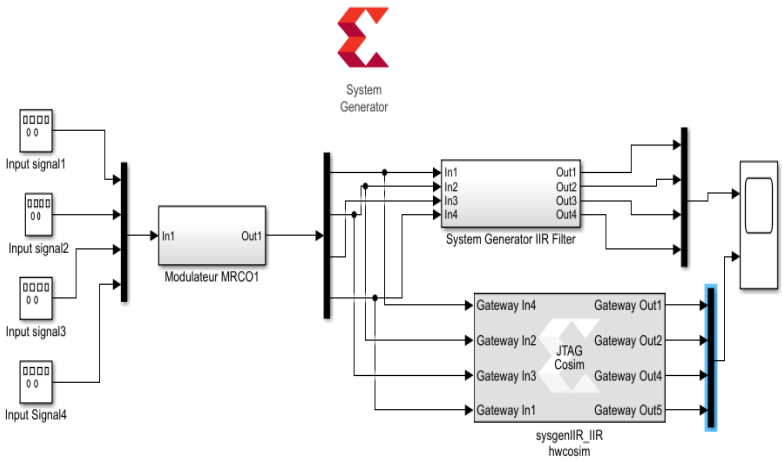

Figure 6: Co-simulation model

The figure above shows the converter model produced in Matlab's Simulink environment. The modulator is realized in Simulink while the second order RII filter is realized together in simulink for virtual simulation. For the software co-simulation, the blocks of the Xilinx System Generator toolbox were used. A successful simulation in the System Generator environment generates the hardware co-design block that allows the Matlab/Simulinx environment to interact with the Zynq 7000 board. The filter will be implemented using the 4x4Filter block from Xilinx . The 4x4Filter block is a 4x4 mask that scans four lines of the input signal at a time to apply the chosen filter. Therefore, the system requires a buffer that accepts four lines of inputs at a time to be fed into the filter. Figure 5 is the model which shows how to design for the assembly.

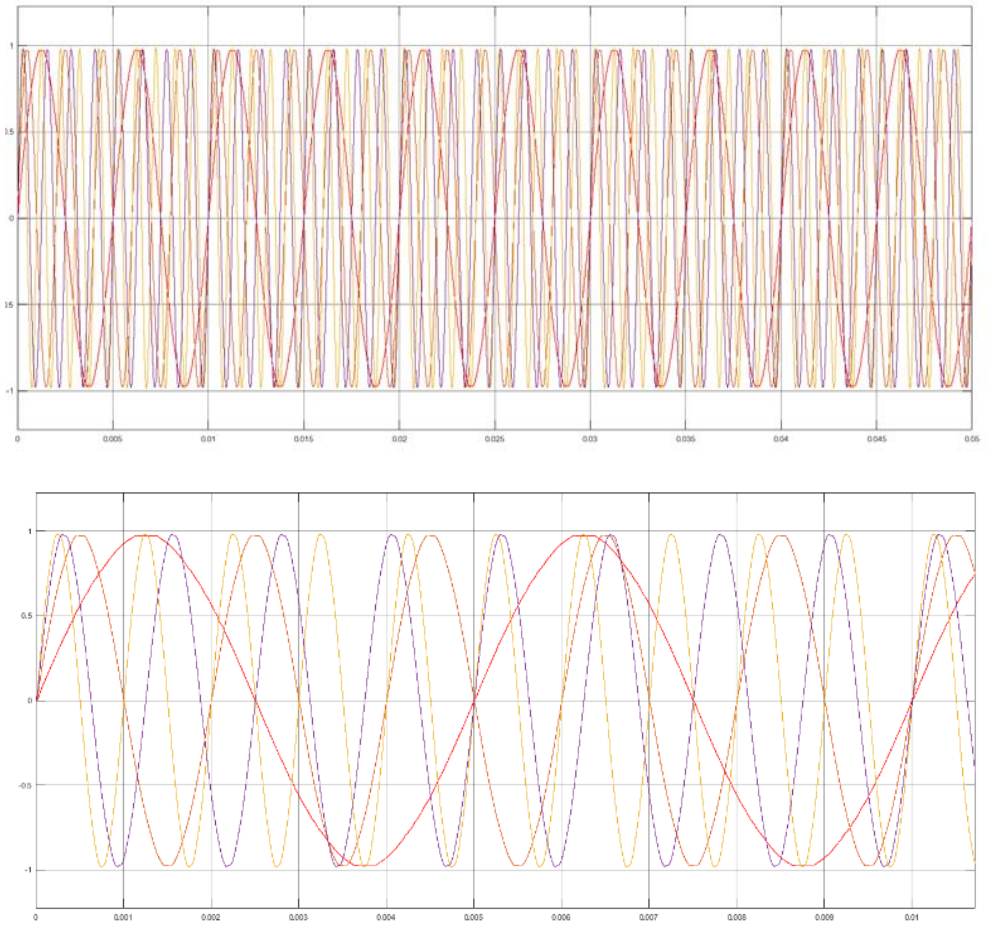

Figure 7: Summary of a sample of Co-simulation results obtained

© 2022 Global Journals

V. Conclusion

This research was carried out in phases. First, the use of a filtering block with an input multiplexer and an output demultiplexer was studied, then 4x4 filtering blocks were studied. A unique way has been identified to incorporate these design techniques into the existing analog-to-digital converter so that the advantages of this mode of circuit design can be used to overcome some existing problems in the multi-channel architecture. The applications of this architecture are then defined. The sub-blocks of the architecture have been defined and designed according to the required specifications. The design and co-simulation have been successfully implemented on the Xilinx ZYNQ 7000 FPGA hardware target. It should be noted that the analog-to-digital converter thus produced based owes its low cost of implementation and its high quality (stability, precision and robustness) both to the material simplicity and to the topological relevance of its DCM circuit. interfacing. As a major discovery, the FPGA-based multichannel ODCM-ADC presented in this article, could be used as a potential new architectural solution for on-board instrumentation systems.

References Références Referencias

1. Sonfack, G. B. and. Mbihi, J.(2018), FPGA-Based Analog-to-Digital Conversion via Optimal Duty-Cycle Modulation. *Journal of Electrical and Electronic Engineering, JEEE,* 8(2), pp. 29-36.
2. Sonfack, G. , Mbihi, J. and Moffo, L. B.(2017), Optimal Duty-Cycle Modulation Scheme for Analog-To-Digital Conversion Systems. *World Academy of Science, Engineering and Technology,* 11(3).
3. Moffo Lonla B., Jean Mbihi, Leandre Nneme Nneme, "Low Cost and High Quality Duty–Cycle Modulation Scheme and Applications". *International Journal of Electrical, Computer, Energetic, Electronic and communication Engineering*. 2014; 8(3):82–88p.
4. Moffo Lonla B., Mbihi J., Nneme Nneme L., Kom M."A Novel Digital–to–Analog Conversion Technique using Duty-Cycle Modulation". *International Journal of Circuits, Systems and Signal processing.* 2013; 7(1):42–49p –87p.
5. Moffo Lonla B., Mbihi J. A, "Nouvelle technique de coversion N/A des signaux par modulation numérique en rapport cyclique et applications en instrumentation virtuelle", Ph/D thesis, ENSET, University of Douala, July 2016.
6. MoffoLonla B., Mbihi J. A."Novel Digital Duty–Cycle Modulation Scheme for FPGA-Based Digital-to-Analog Conversion," *IEEE Transaction on circuits and system II*. 2015; 62(6):543–547p.
7. H. Inose, Y. Yasuda and J. Marakami, "A telemetering system by code modulation, delta-sigma modulation," IRE Trans. on Space, Electronics and Telemetry, SET-8, pp. 204-209, Sept 1962.
8. N. Doley and A. Kornfeld, "Comparison of Sigma-Delta converter circuit architectures in digital CMOS technology", Journal of circuits, systems ans computers", vol. 14, No 3, pp. 515-532, © World scientific publishing company, 2005.
9. J.Mbihi, B. Ndjali, and M. Mbouenda, "Modelling and simulations of a class of duty cycle modulators for industrial instrumentation," *Iranian J.Electr. Comput. Eng.*, vol. 4, no. 2, pp. 121–128, 2005.
10. Mbihi, J., Ndjali Beng, F., Kom, M., and Nneme Nneme, L."*A novel analog-to-digital conversion technique using nonlinear duty-cycle modulation*", International Journal of electronics and computer science engineering, 1(3), 2012, pp. 818-825.
11. Nneme Nneme L., Mbihi J. "Modeling and Simulation of a New Duty–Cycle Modulation Scheme for Signal Transmission System", *American Journal of Electrical and Electronic Engineering (AJEEE)*. 2014; 2(3):82.

© 2022 Global Journals

Global Journal of Researches in Engineering: F
Electrical and Electronics Engineering
Volume 22 Issue 1 Version 1.0 Year 2022
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

Handover and Call Drop Optimization

By Pa Malick Badjie & Goueye Bi Vanie

Abstract- Optimization initiatives generally include leveraging technologies and optimizing existing network systems for the purpose of quality of service (QoS) implementation, redundant data elimination, data compression, improved application delivery, traffic shaping to reduce packet loss. This article aims to meet the requirements by on-site engineers on solving handover and call drop problems. The challenges faced by telecommunications companies remains a menace and a huge problem for the Gambia and the world at large. The researchers have done some tremendous work in this branch of wireless communications, unfortunately, it still remains unraveled. Relatively, handover is closely very linked to call drop. Handover failure probably leads to call drop and therefore handover-caused call drop is arranged in handover success rate optimization. This paper describes the methods for evaluating network handover and call drop performance, testing and troubleshooting methods.

Keywords: *handover, call drop, and optimization.*

GJRE-F Classification: *FOR Code: 290901*

Strictly as per the compliance and regulations of:

© 2022. Pa Malick Badjie & Goueye Bi Vanie. This research/review article is distributed under the terms of the Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0). You must give appropriate credit to authors and reference this article if parts of the article are reproduced in any manner. Applicable licensing terms are at https://creativecommons.org/licenses/by-nc-nd/4.0/.

Handover and Call Drop Optimization

Pa Malick Badjie [α] & Goueye Bi Vanie [σ]

Abstract- Optimization initiatives generally include leveraging technologies and optimizing existing network systems for the purpose of quality of service (QoS) implementation, redundant data elimination, data compression, improved application delivery, traffic shaping to reduce packet loss. This article aims to meet the requirements by on-site engineers on solving handover and call drop problems. The challenges faced by telecommunications companies remains a menace and a huge problem for the Gambia and the world at large. The researchers have done some tremendous work in this branch of wireless communications, unfortunately, it still remains unraveled. Relatively, handover is closely very linked to call drop. Handover failure probably leads to call drop and therefore handover-caused call drop is arranged in handover success rate optimization. This paper describes the methods for evaluating network handover and call drop performance, testing and troubleshooting methods.

Keywords: handover, call drop, and optimization.

I. Introduction

As GSM technology continues to advance with extremely remarkable features especially in data evolution aspects like LTE and 5G, the need to provide proper and effective interfaces between those features and lower evolutions like Global System for Mobile (GSM) and Universal Mobile Telecommunications System (UMTS) which support voice is indeed a great necessity to ensure uninterrupted continuous of services [4]. One of the most remarkable features of the 3G network is their integration with 2G networks. The current deployment of CS networks provides enabling interoperability and flexibility in handling handovers to allow uninterrupted continues of services.

The Wireless Local Area Network (WLAN) coverage on one hand provides an extra coverage in the low signal strength region [1]. When a User Equipment (UE) establishes a call while in one UTRAN Registration Area (URA) and moving to another URA, in the handover region, the UE measures and compares the signaling received from the new cell detected through cell reselection (IRAT reselection) processes and hence attempts to make a successful handover provided the cell it camps on (serving cell) has a neighboring relations with the best detected or measured cell and that minimum Ec/Io and RSCP are met [6]. If this attempt of handover fails it can then lead of a possible call drop.

Author α σ: Radio Network Planning and Optimization Engineer, Qcell Ltd, Qcell House, Kairaba Avenue, The Gambia.
e-mails: pamalickbadjie@gmail.com, pamalick.badjie@qcell.gm, goueyebi.vanie@qcell.gm

This document aims to meet the requirements by on-site engineers on solving handover and call drop problems and the optimization methodology required for evaluating network handover and call drop performance, testing and troubleshooting methods.

This paper is organized as follows: The Section I above describes a brief introduction of the concepts of handover and call drop being closely related. Section II represent the flow chart clearly indicating the necessary steps in detecting, evaluation, analysis and implementation of call drop and handover challenges. Section III represents the design and implementation of Drive Test (DT) procedure and optimization systems. Section IV aims at network optimization in handover success and call drop rates, detailing the specific network operation flow. In addition, to analyze common problems during network optimization; and finally the conclusions and references in the last Section V

II. Drive Test (Call Quality Test) Optimization Flow

Drive Test and Call Quality Test are important to network evaluation and optimization. Drive Test and Call Quality KPIs act as standards for verifying networks. Overall, Drive Test helps to know the entire coverage, to locate cells with missing neighbor and to locate cross-cell coverage. Hard Handover and inter-RAT (Radio Access Technology) handover are used in coverage solutions for special scenarios in which Call Quality Test is proper. In this section we will brieftly describe the Drive Test and Call Qaulity Test optimization flow in terms of SHO (Soft handover), HHO (Hard handover)u and inter-RAT handovers.

While Inter-RAT handover fails are due to imcomplete configuration data, ping-pong reselection, attention should be particularly paid on the data configurations such as RNC (Radio Network Controller) parameters like MCC (Mobile Country Code), MNC (Mobile Network Code), LAC (Local Area Code), BCC (Base station Color Code), etc.

Since handover failures are hardly due to data configurations errors or mismatch as the errors in these configurations most often leads to a related alarms usually displayed on the monitoring tool. Therefore, this section will focus on SHO to describe the optimization flow which which might not be seen on the monotoring tool except for a drive test collected data on-site.

The flowchart of the proposed Soft Handover Drive Test detection and analysis is shown in Fig: 2.1 below. The sequence of events are explained below:

© 2022 Global Journals

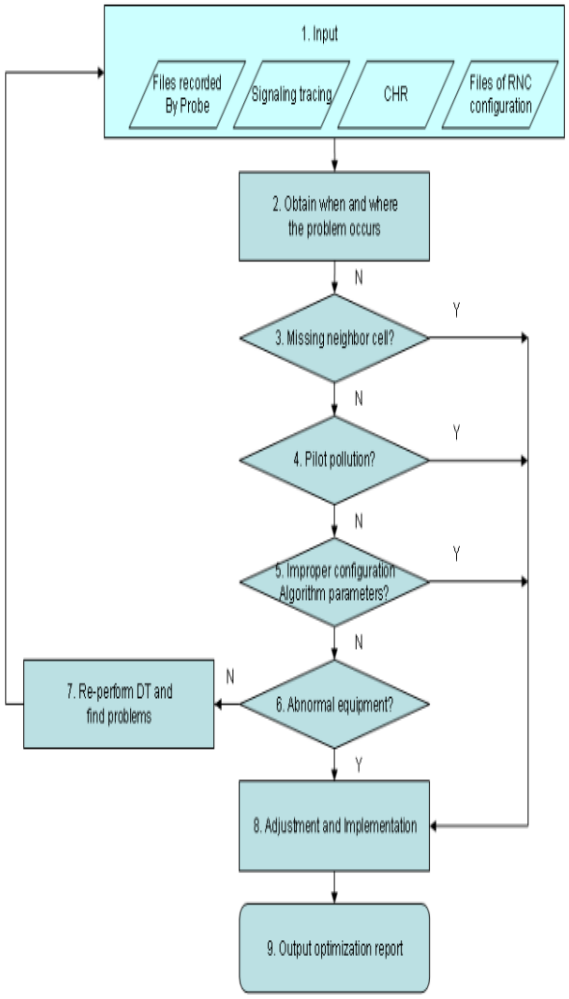

Figure 2.1: SHO DT data analysis flow

a) Inputting Analysis Data

In detecting and evaluating handover and call drop problems, a drive test is always a neccessity to collect data, understand related signaling trace, RNC CHR and RNC MML Script. During the test, SHO-caused call drop might occur or SHO might fail, this spot is to be recorded and the time of occurrence of the problem also be noted for further location and analysis.

b) Missing Neighbor Cell

During the early optimization, a premature guess would be a call drop is usually due to missing neighbors. For intra-frequency neighbor cells, the following methods should be used to comfirm intra-frequency missing neighbor cell.

✓ Check the active set Ec/Io recorded by UE before call drop and Best Server Ec/Io recorded by scanner. Check whether the Best Server scramble recorded by Scanner is in the neighbor cell list of intra-frequence measurement control before call drop. The cause might be intra-frequency missing neighbor cell if all the following conditions are met:

- The Ec/Io recorded by UE is bad
- The Best Server Ec/Io is good
- No Best Server scramble is in the neighor cell list of measurements control.

✓ If the UE reconnects to the network immediately after a call drop and the scramble of the cell that the UE camps on is different from that upon call drop, then missing neighbor cell is probable. Confirm it by measurement control (search the messages back from call drop for the latest intra-frequency measurement control message. Also check the neighbor cell list of this measurement control message)

As neighboring ralations between cells of a network are very important to allow continues use of services, and since missing neighbor cell causes call drop, redundant neighbor cells also impacts network performance and increases the consumption of UE intra-frequency measurement. If this problem becomes critically serious, the necessary cells cannot be listed.

c) Pilot Pollution

Another factor affecting call drop and handover failure is pilot pollution. Pilot pollution usually exist at a point where excessive strong pilots exists, but no one is stronge enough to be the primary pilot.

By definition, when setting rules for judging pilot pollution, confirm the following content:

✓ Definition of strong pilot: whether a pilot is strong depends on the absolute strength of the pilot, which is measured by Received Signal Code Power (RSCP). If the pilot RSCP is greater than a threshold, the pilot is a strong pilot, namely:

$$\text{CPICH_RSCP} > \text{Th}_{\text{RSCP_Absolute}}$$

✓ Definition of “excessive”: here the pilot number is the judgemental criteria. If the pilot number is more than a threshold, the pilots at a point are excessive, namely:

$$\text{CPICH_Number} > \text{Th}_{N}$$

✓ Definition of “No best server strong enough”: to compare the existence of the best stronger server, the judgement criteria is the relative strength of multiple pilots. If the strength difference of the strongest pilot and the number of the $(Th_N + 1)$ strong pilot is smaller than a threshold, then no best server strong enough exists at that point, namely:

$$(CPICH_RSCP_{1st} - CPICH_RSCP_{(Th_N+1)th}) < Th_{RSCP_Relative}$$

Following the descriptions, pilot pollution exists if the following conditions are met:

✓ The number of pilots satisfying $CPICH_RSCP > Th_{RSCP_Absolute}$ is more than Th_N.

✓ $(CPICH_RSCP_{1st} - CPICH_RSCP_{(Th_N+1)th}) < Th_{RSCP_Relative}$

© 2022 Global Journals

Set $Th_{RSCP_Absolute}$ = -95 dBm, Th_N= 3, and $Th_{RSCP_Relative}$= 5 dB, the judgement standards for pilot pollution are:

- The number of pilots satisfying *CPICH_RSCP* > -95*dBm* is greater than 3.
- $(CPICH_RSCP_{1st} - CPICH_RSCP_{4th}) < 5dBm$

d) Improper Configuration of SHO Algorithm Parameters

To eliminate problems of call drop and handover issues, the following two problems must be solved by adjusting algorithm parameters.

✓ Delay handover

By the signaling flow for CS serices, the UE fails to receive active set update command. After the UE reports measurement message, the Ec/Io of original cell signals decrease sharply. When the RNC sends active set update message, the UE powers off the transmitter due to asynchronization. The UE cannot receive active set update message. For PS services, the UE might fail to receive active set update message or perform TRB (Traffic Radio Bearer) reset before handover. The delayed handover might be one of the following:

- Turnng corner effect: The Ec/Io of original cell decreases sharply and that the target cell increases greatly in response (an over high value appears)
- Needlepoint effect: The Ec/Io of original cell decreases sharply before it increases and the Ec/Io of target cell increase sharply for a short time.

According to the signaling flow, the UE reports the 1a and 1c measurement reports of neighbor cells before a call drop. Then the RNC receives the event and sends the active set update, which the UE fails to receive.

✓ Ping-pong Handover

Ping-pong handover is of the two forms below

- Since the best server changes frequently, two or more cells continuously alternate to be the best server. Also, since the period for each cell to be best server is short, the RSCP of the best server is strong.
- Multiple cells exist with little difference of abnormal RSCP, the Ec/Io for each cell is bad and therefore, no primary pilot cell exists.

Referencing the signaling flow, when a cell is deleted, the 1a event is immediately reported. Consequently, the UE fails because it cannot receive the active set update command.

e) Abnormal Equipment

The failures or abnormal functionalities can always be troubleshooted starting with the alarm console for abnorma alarms. Meanwhile the trace messages are to be analyze, locate the SHO problem by checking the failure message.

f) Reperforming Drive Test and Locating Problems

If the problem is not due to any of the previous causes, perform DT again and collect DT data and supplemet data from problem analysis.

After confirming the cause to the problem, adjust the network by using the following pertinent methods:

- For handover problems caused by pilot pollution, adjust engineering parameters of antenna so that a best server forms around the antenna. Also, adjust engineering parameters of other antennas so that signals from other antennas become weaker and the number of pilots drop. In the event that the aforementioned suggestions fail, construct a new site to cover this area if the conditions permit or combine the two cells as one if the interference is from two sectors of the same NodeB.
- For abnormal equipment, consult customer service engineer for abnormal equipment and transport layer on alarms console If alarms are present on alarm console, cooperate with customer service engineers
- For call drop caused by delayed handover, adjust antennas to expand the handover areas, set the handover parameters of 1a event or increase CIO (Cell Independent Offset) to enable handover to occur in advance.
- For needle effect or turning corner effect, setting CIO to 5 dB is proper, but this increases handover ratio.
- For call drop caused by Ping-pong handover, adjust the antenna to form a best server or reduce Ping-pong handover by setting the handover parameter of 1B event, the 1B event threshold, 1B hysteresis and 1B delay trigger time.

© 2022 Global Journals

III. Hardware, Design and Implelemtation of Drive Test using Genex

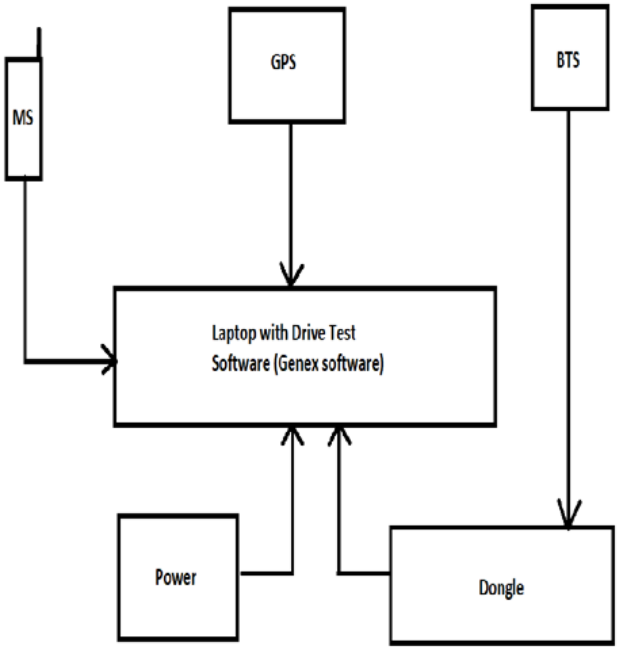

Fig: 3.1: Drive Test System

To conduct a successful drive test, the drive test engineer needs to make sure the engineering parameters are upto date to have accurate records of the UE events during the drive test; these include antenna azimuths, heights, tilting (mechnical and electrical), frequency band on site, etc as the data collected helps to find and analyze the causes of call drops, handover failures and other network problems. The basic Genex drive test tool consist of the following components:

- A laptop with drive test software and GPS connection capability, data cables and multi-connector port.
- A GPS tracker,
- A Drive test mobile phone (e.g. Huawei MT7-L09)
- An inverter

a) Laptop

The Genex software is installed in the laptop as a tool to collect visualized data being collected, the route taken during the drive test and records the data to be analyzed with another software called "Genex Assistant".

b) GPS Tool

The GPS tracker keeps tabsof the movemets of the drive test car on a map so as to cover the target route

c) Drive Test mobile phone

One of the most important tools is the MS as the purpose of the drive test is to understand its behaviour in idle and connected modes. The tools make a capture of the events the MS is going through during the drive test like attempted calls, successful andunsuccessful calls, handover success rates, call drop rates, while also measuring the thresholds sets (coverage, offset, etc) for minimum handovers.

d) The Inverter

The inverter used here will be a DC to AC inverter. Its purpose is to keep the laptop charged during the drive test as it might be discharged during the drive test when the target drive test is not completed leading to either stop the drive test or lossage of data when it turns off by its completely discharged.

IV. Network Optimization of Call Drop Rate and Handover

The call drop point is related to signaling flow before call drop. The call drop can also be seen during the drive test analysis on a Genex Assistant tool like shown in Figure 4.1

© 2022 Global Journals

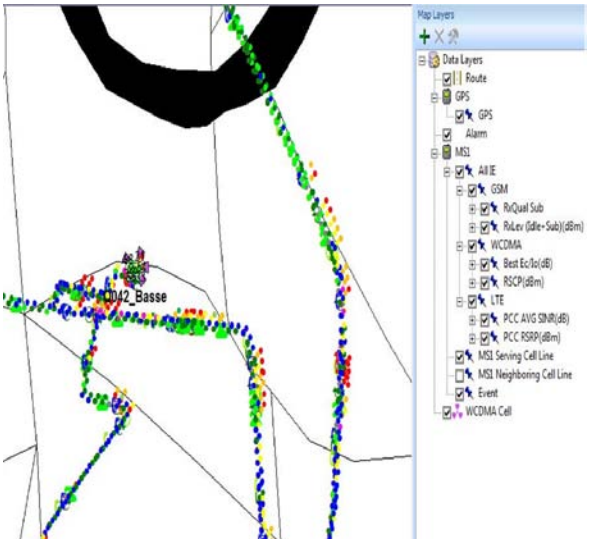

Fig. 4.1: Short Call drive test to determine handover and call drop

a) Analysis

Check the pilot test data from UE and scanner at call drop points. Then check the scrambles recorded by UE active set and scanner before call drop. In the analysis, we realized the measurement result of UE active set and scanner is inconsistent as the scanner has a scrambling code not existing in the UE active set. The cause might be due to missing neighbor cell or delayed handover as the scrambling code does not even exist in the UE monitor set as shwon in the figure 4.2 below.

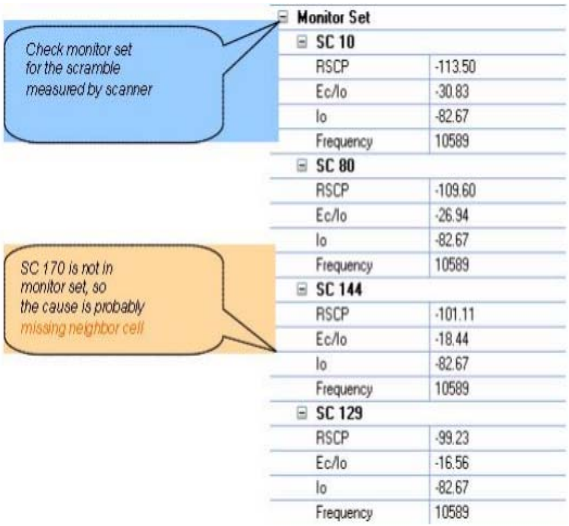

Fig. 4.2: Analysis of short Call drive test to determine handover and call drop

If only the UE recorded information during test, without scanner information, then the call drop due to missing neighbor cell is to be confirmed using the following methods:

- ✓ Confirm the scrambles of all cells in active set and the scrambles of cells in monitor set measured by UE before a call drop.
- ✓ Compare the scramble information of the cell where the UE camps on after reselection, after a call drop and the scrambles in UE active setand monitor set before a call drop. If the former scramble is not in the scramble list of active and monitor set before call drop, then the call drop is probably due to missing neighbor cell
- ✓ Check the neighbor cell list. This applies for solving call drop due to missing neighbor cell on site.

b) Solution

When a call drop is as a result of missing neighbor cell, then the neighbor cell should be added. This is because the RNC (Radio Network Controller) updates measurement control according to the best cell which is obtainable by searching for intra-frequency measurement report with 1D event before measurement control is sent.

In the post drive test, after adding the missing neighbors, another call drop was recorded but this time it was not due to RF (Radio Frequency) reason. The scrambles of all cells in active set and the scrambles of cells in monitor set measured by UE before and after a call drop are indeed neighbor cells as seen in figure 4.3

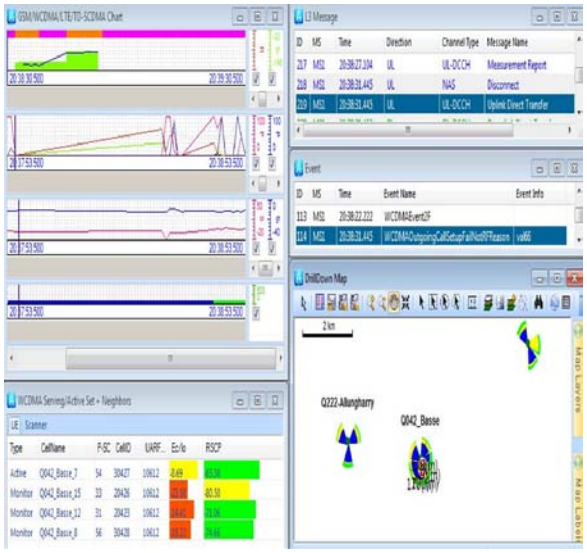

Fig 4.3: Post drive test result

V. Conclusions

In this paper, we have seen that handover is actually closely related to call drop. Hence, call drop minimization techniques employed here to reduce the number of call drops and enhance handover in mobile cellular networks are indeed efficient and reliable. One should not only limit to these techniques as there are many reasons leading to call drops and handover failures such a transmission failures, faulty channels, etc. However, for an optimization engineer, a drive test

© 2022 Global Journals

is always an necessary to confirm the cause of call drops or degradation in handovers.

References Références Referencias

1. D. Sarddar et all "Mininization of Handoff Latency by Angular Displacement Method Using GPS Based Map"IJASCI International Journal of Computer Science Issues, Vol. 7, Issue 3, No. 7, May 2010.
2. M. Li, M. Claypool, and R. Kinicki. Wbest: A bandwidth estimation tool for IEEE 802.11 wireless networks. In IEEE Conference on Local Computer Networks (LCN) pp. (374-381) October, 2008, Montreal, Canada.
3. Pa Malick Badjie, K. Lokesh Krishna, Sreeza Tarafder and Pappu Singha, "Smart Patient Monitoring System for Emergency Situations", 2018 AREEE Vol. 5, Issue Jan-Mar, 2018, pp. 13-17.
4. Ramanath S., Kavitha, V., Altman, E., (2010) Impact of mobility on call block, call drop and optimal cell size in small cell networks, IEEE XPLORE, doi: 10.1109/PIMRCW 20105670352.
5. Haring G. Marie R. Puigjaner R. Trivedi K. "Loss Formulae and their to optimization for Cellular System Nwetorks (2001), IEEE Transaction Vehicular Technology, 50(3), 664-673.
6. Boggia, G., Camarda, P., D'alconzo , A., Biasi, A. D., & Siviero, M., "Drop Call Probability in Established Cellular Networks" From data Analysis to Modelling. (2005) IEEE 61st Vehicular Technology Conference.

© 2022 Global Journals

Global Journals Guidelines Handbook 2022

www.GlobalJournals.org

Memberships

Fellows/Associates of Engineering Research Council

FERC/AERC Memberships

Introduction

FERC/AERC is the most prestigious membership of Global Journals accredited by Open Association of Research Society, U.S.A (OARS). The credentials of Fellow and Associate designations signify that the researcher has gained the knowledge of the fundamental and high-level concepts, and is a subject matter expert, proficient in an expertise course covering the professional code of conduct, and follows recognized standards of practice. The credentials are designated only to the researchers, scientists, and professionals that have been selected by a rigorous process by our Editorial Board and Management Board.

Associates of FERC/AERC are scientists and researchers from around the world are working on projects/researches that have huge potentials. Members support Global Journals' mission to advance technology for humanity and the profession.

FERC

Fellow of Engineering Research Council

FELLOW OF ENGINEERING RESEARCH COUNCIL is the most prestigious membership of Global Journals. It is an award and membership granted to individuals that the Open Association of Research Society judges to have made a 'substantial contribution to the improvement of computer science, technology, and electronics engineering.

The primary objective is to recognize the leaders in research and scientific fields of the current era with a global perspective and to create a channel between them and other researchers for better exposure and knowledge sharing. Members are most eminent scientists, engineers, and technologists from all across the world. Fellows are elected for life through a peer review process on the basis of excellence in the respective domain. There is no limit on the number of new nominations made in any year. Each year, the Open Association of Research Society elect up to 12 new Fellow Members.

Benefit

To the institution

Get letter of appreciation

Global Journals sends a letter of appreciation of author to the Dean or CEO of the University or Company of which author is a part, signed by editor in chief or chief author.

Exclusive Network

Get access to a closed network

A FERC member gets access to a closed network of Tier 1 researchers and scientists with direct communication channel through our website. Fellows can reach out to other members or researchers directly. They should also be open to reaching out by other.

Career | Credibility | Exclusive | Reputation

Certificate

Certificate, LoR and Laser-Momento

Fellows receive a printed copy of a certificate signed by our Chief Author that may be used for academic purposes and a personal recommendation letter to the dean of member's university.

Career | Credibility | Exclusive | Reputation

Designation

Get honored title of membership

Fellows can use the honored title of membership. The “FERC” is an honored title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., FERC or William Walldroff, M.S., FERC.

Career | Credibility | Exclusive | Reputation

Recognition on the Platform

Better visibility and citation

All the Fellow members of FERC get a badge of "Leading Member of Global Journals" on the Research Community that distinguishes them from others. Additionally, the profile is also partially maintained by our team for better visibility and citation. All fellows get a dedicated page on the website with their biography.

Career | Credibility | Reputation

© Copyright by Global Journals | Guidelines Handbook

Future Work

Get discounts on the future publications

Fellows receive discounts on the future publications with Global Journals up to 60%. Through our recommendation programs, members also receive discounts on publications made with OARS affiliated organizations.

Career | Financial

GJ Account

Unlimited forward of Emails

Fellows get secure and fast GJ work emails with unlimited storage of emails that they may use them as their primary email. For example, john [AT] globaljournals [DOT] org.

Career | Credibility | Reputation

Premium Tools

Access to all the premium tools

To take future researches to the zenith, fellows receive access to all the premium tools that Global Journals have to offer along with the partnership with some of the best marketing leading tools out there.

Financial

Conferences & Events

Organize seminar/conference

Fellows are authorized to organize symposium/seminar/conference on behalf of Global Journal Incorporation (USA). They can also participate in the same organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent. Additionally, they get free research conferences (and others) alerts.

Career | Credibility | Financial

Early Invitations

Early invitations to all the symposiums, seminars, conferences

All fellows receive the early invitations to all the symposiums, seminars, conferences and webinars hosted by Global Journals in their subject.

Exclusive

© Copyright by Global Journals | Guidelines Handbook

Publishing Articles & Books

Earn 60% of sales proceeds

Fellows can publish articles (limited) without any fees. Also, they can earn up to 70% of sales proceeds from the sale of reference/review books/literature/publishing of research paper. The FERC member can decide its price and we can help in making the right decision.

Exclusive | Financial

Reviewers

Get a remuneration of 15% of author fees

Fellow members are eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get a remuneration of 15% of author fees, taken from the author of a respective paper.

Financial

Access to Editorial Board

Become a member of the Editorial Board

Fellows may join as a member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. Additionally, Fellows get a chance to nominate other members for Editorial Board.

Career | Credibility | Exclusive | Reputation

And Much More

Get access to scientific museums and observatories across the globe

All members get access to 5 selected scientific museums and observatories across the globe. All researches published with Global Journals will be kept under deep archival facilities across regions for future protections and disaster recovery. They get 10 GB free secure cloud access for storing research files.

© Copyright by Global Journals | Guidelines Handbook

AERC

ASSOCIATE OF ENGINEERING RESEARCH COUNCIL

ASSOCIATE OF ENGINEERING RESEARCH COUNCIL is the membership of Global Journals awarded to individuals that the Open Association of Research Society judges to have made a 'substantial contribution to the improvement of computer science, technology, and electronics engineering.

The primary objective is to recognize the leaders in research and scientific fields of the current era with a global perspective and to create a channel between them and other researchers for better exposure and knowledge sharing. Members are most eminent scientists, engineers, and technologists from all across the world. Associate membership can later be promoted to Fellow Membership. Associates are elected for life through a peer review process on the basis of excellence in the respective domain. There is no limit on the number of new nominations made in any year. Each year, the Open Association of Research Society elect up to 12 new Associate Members.

To the institution

Get letter of appreciation

Global Journals sends a letter of appreciation of author to the Dean or CEO of the University or Company of which author is a part, signed by editor in chief or chief author.

Exclusive Network

Get access to a closed network

A AERC member gets access to a closed network of Tier 1 researchers and scientists with direct communication channel through our website. Associates can reach out to other members or researchers directly. They should also be open to reaching out by other.

Career | Credibility | Exclusive | Reputation

Certificate

Certificate, LoR and Laser-Momento

Associates receive a printed copy of a certificate signed by our Chief Author that may be used for academic purposes and a personal recommendation letter to the dean of member's university.

Career | Credibility | Exclusive | Reputation

Designation

Get honored title of membership

Associates can use the honored title of membership. The “AERC” is an honored title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., AERC or William Walldroff, M.S., AERC.

Career | Credibility | Exclusive | Reputation

Recognition on the Platform

Better visibility and citation

All the Associate members of AERC get a badge of "Leading Member of Global Journals" on the Research Community that distinguishes them from others. Additionally, the profile is also partially maintained by our team for better visibility and citation. All associates get a dedicated page on the website with their biography.

Career | Credibility | Reputation

© Copyright by Global Journals | Guidelines Handbook

Future Work

Get discounts on the future publications

Associates receive discounts on the future publications with Global Journals up to 60%. Through our recommendation programs, members also receive discounts on publications made with OARS affiliated organizations.

Career | Financial

GJ Account

Unlimited forward of Emails

Associates get secure and fast GJ work emails with unlimited storage of emails that they may use them as their primary email. For example, john [AT] globaljournals [DOT] org..

Career | Credibility | Reputation

Premium Tools

Access to all the premium tools

To take future researches to the zenith, associates receive access to all the premium tools that Global Journals have to offer along with the partnership with some of the best marketing leading tools out there.

Financial

Conferences & Events

Organize seminar/conference

Associates are authorized to organize symposium/seminar/conference on behalf of Global Journal Incorporation (USA). They can also participate in the same organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent. Additionally, they get free research conferences (and others) alerts.

Career | Credibility | Financial

Early Invitations

Early invitations to all the symposiums, seminars, conferences

All associates receive the early invitations to all the symposiums, seminars, conferences and webinars hosted by Global Journals in their subject.

Exclusive

Publishing Articles & Books

Earn 30-40% of sales proceeds

Associates can publish articles (limited) without any fees. Also, they can earn up to 30-40% of sales proceeds from the sale of reference/review books/literature/publishing of research paper.

Exclusive | Financial

Reviewers

Get a remuneration of 15% of author fees

Associate members are eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get a remuneration of 15% of author fees, taken from the author of a respective paper.

Financial

And Much More

Get access to scientific museums and observatories across the globe

All members get access to 2 selected scientific museums and observatories across the globe. All researches published with Global Journals will be kept under deep archival facilities across regions for future protections and disaster recovery. They get 5 GB free secure cloud access for storing research files.

© Copyright by Global Journals | Guidelines Handbook

Associate	Fellow	Research Group	Basic
$4800 **lifetime designation**	$6800 **lifetime designation**	$12500.00 **organizational**	APC **per article**
Certificate, LoR and Momento **2** discounted publishing/year **Gradation** of Research **10** research contacts/day **1 GB** Cloud Storage **GJ** Community Access	**Certificate,** LoR and Momento **Unlimited** discounted publishing/year **Gradation** of Research **Unlimited** research contacts/day **5 GB** Cloud Storage **Online Presense** Assistance **GJ** Community Access	**Certificates,** LoRs and Momentos **Unlimited** free publishing/year **Gradation** of Research **Unlimited** research contacts/day **Unlimited** Cloud Storage **Online Presense** Assistance **GJ** Community Access	**GJ** Community Access

We accept the manuscript submissions in any standard (generic) format.

We typeset manuscripts using advanced typesetting tools like Adobe In Design, CorelDraw, TeXnicCenter, and TeXStudio. We usually recommend authors submit their research using any standard format they are comfortable with, and let Global Journals do the rest.

Alternatively, you can download our basic template from https://globaljournals.org/Template.zip

Authors should submit their complete paper/article, including text illustrations, graphics, conclusions, artwork, and tables. Authors who are not able to submit manuscript using the form above can email the manuscript department at submit@globaljournals.org or get in touch with chiefeditor@globaljournals.org if they wish to send the abstract before submission.

BEFORE AND DURING SUBMISSION

Authors must ensure the information provided during the submission of a paper is authentic. Please go through the following checklist before submitting:

1. Authors must go through the complete author guideline and understand and *agree to Global Journals' ethics and code of conduct,* along with author responsibilities.
2. Authors must accept the privacy policy, terms, and conditions of Global Journals.
3. Ensure corresponding author's email address and postal address are accurate and reachable.
4. Manuscript to be submitted must include keywords, an abstract, a paper title, co-author(s') names and details (email address, name, phone number, and institution), figures and illustrations in vector format including appropriate captions, tables, including titles and footnotes, a conclusion, results, acknowledgments and references.
5. Authors should submit paper in a ZIP archive if any supplementary files are required along with the paper.
6. Proper permissions must be acquired for the use of any copyrighted material.
7. Manuscript submitted *must not have been submitted or published elsewhere* and all authors must be aware of the submission.

Declaration of Conflicts of Interest

It is required for authors to declare all financial, institutional, and personal relationships with other individuals and organizations that could influence (bias) their research.

POLICY ON PLAGIARISM

Plagiarism is not acceptable in Global Journals submissions at all.

Plagiarized content will not be considered for publication. We reserve the right to inform authors' institutions about plagiarism detected either before or after publication. If plagiarism is identified, we will follow COPE guidelines:

Authors are solely responsible for all the plagiarism that is found. The author must not fabricate, falsify or plagiarize existing research data. The following, if copied, will be considered plagiarism:

- Words (language)
- Ideas
- Findings
- Writings
- Diagrams
- Graphs
- Illustrations
- Lectures

© Copyright by Global Journals | Guidelines Handbook

- Printed material
- Graphic representations
- Computer programs
- Electronic material
- Any other original work

Authorship Policies

Global Journals follows the definition of authorship set up by the Open Association of Research Society, USA. According to its guidelines, authorship criteria must be based on:

1. Substantial contributions to the conception and acquisition of data, analysis, and interpretation of findings.
2. Drafting the paper and revising it critically regarding important academic content.
3. Final approval of the version of the paper to be published.

Changes in Authorship

The corresponding author should mention the name and complete details of all co-authors during submission and in manuscript. We support addition, rearrangement, manipulation, and deletions in authors list till the early view publication of the journal. We expect that corresponding author will notify all co-authors of submission. We follow COPE guidelines for changes in authorship.

Copyright

During submission of the manuscript, the author is confirming an exclusive license agreement with Global Journals which gives Global Journals the authority to reproduce, reuse, and republish authors' research. We also believe in flexible copyright terms where copyright may remain with authors/employers/institutions as well. Contact your editor after acceptance to choose your copyright policy. You may follow this form for copyright transfers.

Appealing Decisions

Unless specified in the notification, the Editorial Board's decision on publication of the paper is final and cannot be appealed before making the major change in the manuscript.

Acknowledgments

Contributors to the research other than authors credited should be mentioned in Acknowledgments. The source of funding for the research can be included. Suppliers of resources may be mentioned along with their addresses.

Declaration of funding sources

Global Journals is in partnership with various universities, laboratories, and other institutions worldwide in the research domain. Authors are requested to disclose their source of funding during every stage of their research, such as making analysis, performing laboratory operations, computing data, and using institutional resources, from writing an article to its submission. This will also help authors to get reimbursements by requesting an open access publication letter from Global Journals and submitting to the respective funding source.

Preparing your Manuscript

Authors can submit papers and articles in an acceptable file format: MS Word (doc, docx), LaTeX (.tex, .zip or .rar including all of your files), Adobe PDF (.pdf), rich text format (.rtf), simple text document (.txt), Open Document Text (.odt), and Apple Pages (.pages). Our professional layout editors will format the entire paper according to our official guidelines. This is one of the highlights of publishing with Global Journals—authors should not be concerned about the formatting of their paper. Global Journals accepts articles and manuscripts in every major language, be it Spanish, Chinese, Japanese, Portuguese, Russian, French, German, Dutch, Italian, Greek, or any other national language, but the title, subtitle, and abstract should be in English. This will facilitate indexing and the pre-peer review process.

The following is the official style and template developed for publication of a research paper. Authors are not required to follow this style during the submission of the paper. It is just for reference purposes.

Manuscript Style Instruction (Optional)

- Microsoft Word Document Setting Instructions.
- Font type of all text should be Swis721 Lt BT.
- Page size: 8.27" x 11'", left margin: 0.65, right margin: 0.65, bottom margin: 0.75.
- Paper title should be in one column of font size 24.
- Author name in font size of 11 in one column.
- Abstract: font size 9 with the word "Abstract" in bold italics.
- Main text: font size 10 with two justified columns.
- Two columns with equal column width of 3.38 and spacing of 0.2.
- First character must be three lines drop-capped.
- The paragraph before spacing of 1 pt and after of 0 pt.
- Line spacing of 1 pt.
- Large images must be in one column.
- The names of first main headings (Heading 1) must be in Roman font, capital letters, and font size of 10.
- The names of second main headings (Heading 2) must not include numbers and must be in italics with a font size of 10.

Structure and Format of Manuscript

The recommended size of an original research paper is under 15,000 words and review papers under 7,000 words. Research articles should be less than 10,000 words. Research papers are usually longer than review papers. Review papers are reports of significant research (typically less than 7,000 words, including tables, figures, and references)

A research paper must include:

a) A title which should be relevant to the theme of the paper.
b) A summary, known as an abstract (less than 150 words), containing the major results and conclusions.
c) Up to 10 keywords that precisely identify the paper's subject, purpose, and focus.
d) An introduction, giving fundamental background objectives.
e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition, sources of information must be given, and numerical methods must be specified by reference.
f) Results which should be presented concisely by well-designed tables and figures.
g) Suitable statistical data should also be given.
h) All data must have been gathered with attention to numerical detail in the planning stage.

Design has been recognized to be essential to experiments for a considerable time, and the editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned unrefereed.

i) Discussion should cover implications and consequences and not just recapitulate the results; conclusions should also be summarized.
j) There should be brief acknowledgments.
k) There ought to be references in the conventional format. Global Journals recommends APA format.

Authors should carefully consider the preparation of papers to ensure that they communicate effectively. Papers are much more likely to be accepted if they are carefully designed and laid out, contain few or no errors, are summarizing, and follow instructions. They will also be published with much fewer delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and suggestions to improve brevity.

Format Structure

It is necessary that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

All manuscripts submitted to Global Journals should include:

Title

The title page must carry an informative title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) where the work was carried out.

Author details

The full postal address of any related author(s) must be specified.

Abstract

The abstract is the foundation of the research paper. It should be clear and concise and must contain the objective of the paper and inferences drawn. It is advised to not include big mathematical equations or complicated jargon.

Many researchers searching for information online will use search engines such as Google, Yahoo or others. By optimizing your paper for search engines, you will amplify the chance of someone finding it. In turn, this will make it more likely to be viewed and cited in further works. Global Journals has compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Keywords

A major lynchpin of research work for the writing of research papers is the keyword search, which one will employ to find both library and internet resources. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining, and indexing.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy: planning of a list of possible keywords and phrases to try.

Choice of the main keywords is the first tool of writing a research paper. Research paper writing is an art. Keyword search should be as strategic as possible.

One should start brainstorming lists of potential keywords before even beginning searching. Think about the most important concepts related to research work. Ask, “What words would a source have to include to be truly valuable in a research paper?” Then consider synonyms for the important words.

It may take the discovery of only one important paper to steer in the right keyword direction because, in most databases, the keywords under which a research paper is abstracted are listed with the paper.

Numerical Methods

Numerical methods used should be transparent and, where appropriate, supported by references.

Abbreviations

Authors must list all the abbreviations used in the paper at the end of the paper or in a separate table before using them.

Formulas and equations

Authors are advised to submit any mathematical equation using either MathJax, KaTeX, or LaTeX, or in a very high-quality image.

Tables, Figures, and Figure Legends

Tables: Tables should be cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g., Table 4, a self-explanatory caption, and be on a separate sheet. Authors must submit tables in an editable format and not as images. References to these tables (if any) must be mentioned accurately.

Figures

Figures are supposed to be submitted as separate files. Always include a citation in the text for each figure using Arabic numbers, e.g., Fig. 4. Artwork must be submitted online in vector electronic form or by emailing it.

Preparation of Eletronic Figures for Publication

Although low-quality images are sufficient for review purposes, print publication requires high-quality images to prevent the final product being blurred or fuzzy. Submit (possibly by e-mail) EPS (line art) or TIFF (halftone/ photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Avoid using pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings). Please give the data for figures in black and white or submit a Color Work Agreement form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution at final image size ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs): >350 dpi; figures containing both halftone and line images: >650 dpi.

Color charges: Authors are advised to pay the full cost for the reproduction of their color artwork. Hence, please note that if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a Color Work Agreement form before your paper can be published. Also, you can email your editor to remove the color fee after acceptance of the paper.

Tips for Writing a Good Quality Engineering Research Paper

Techniques for writing a good quality engineering research paper:

1. Choosing the topic: In most cases, the topic is selected by the interests of the author, but it can also be suggested by the guides. You can have several topics, and then judge which you are most comfortable with. This may be done by asking several questions of yourself, like "Will I be able to carry out a search in this area? Will I find all necessary resources to accomplish the search? Will I be able to find all information in this field area?" If the answer to this type of question is "yes," then you ought to choose that topic. In most cases, you may have to conduct surveys and visit several places. Also, you might have to do a lot of work to find all the rises and falls of the various data on that subject. Sometimes, detailed information plays a vital role, instead of short information. Evaluators are human: The first thing to remember is that evaluators are also human beings. They are not only meant for rejecting a paper. They are here to evaluate your paper. So present your best aspect.

2. Think like evaluators: If you are in confusion or getting demotivated because your paper may not be accepted by the evaluators, then think, and try to evaluate your paper like an evaluator. Try to understand what an evaluator wants in your research paper, and you will automatically have your answer. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

3. Ask your guides: If you are having any difficulty with your research, then do not hesitate to share your difficulty with your guide (if you have one). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work, then ask your supervisor to help you with an alternative. He or she might also provide you with a list of essential readings.

4. Use of computer is recommended: As you are doing research in the field of research engineering then this point is quite obvious. Use right software: Always use good quality software packages. If you are not capable of judging good software, then you can lose the quality of your paper unknowingly. There are various programs available to help you which you can get through the internet.

5. Use the internet for help: An excellent start for your paper is using Google. It is a wondrous search engine, where you can have your doubts resolved. You may also read some answers for the frequent question of how to write your research paper or find a model research paper. You can download books from the internet. If you have all the required books, place importance on reading, selecting, and analyzing the specified information. Then sketch out your research paper. Use big pictures: You may use encyclopedias like Wikipedia to get pictures with the best resolution. At Global Journals, you should strictly follow here.

© Copyright by Global Journals | Guidelines Handbook

6. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right? It is a good habit which helps to not lose your continuity. You should always use bookmarks while searching on the internet also, which will make your search easier.

7. Revise what you wrote: When you write anything, always read it, summarize it, and then finalize it.

8. Make every effort: Make every effort to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in the introduction—what is the need for a particular research paper. Polish your work with good writing skills and always give an evaluator what he wants. Make backups: When you are going to do any important thing like making a research paper, you should always have backup copies of it either on your computer or on paper. This protects you from losing any portion of your important data.

9. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several unnecessary diagrams will degrade the quality of your paper by creating a hodgepodge. So always try to include diagrams which were made by you to improve the readability of your paper. Use of direct quotes: When you do research relevant to literature, history, or current affairs, then use of quotes becomes essential, but if the study is relevant to science, use of quotes is not preferable.

10. Use proper verb tense: Use proper verb tenses in your paper. Use past tense to present those events that have happened. Use present tense to indicate events that are going on. Use future tense to indicate events that will happen in the future. Use of wrong tenses will confuse the evaluator. Avoid sentences that are incomplete.

11. Pick a good study spot: Always try to pick a spot for your research which is quiet. Not every spot is good for studying.

12. Know what you know: Always try to know what you know by making objectives, otherwise you will be confused and unable to achieve your target.

13. Use good grammar: Always use good grammar and words that will have a positive impact on the evaluator; use of good vocabulary does not mean using tough words which the evaluator has to find in a dictionary. Do not fragment sentences. Eliminate one-word sentences. Do not ever use a big word when a smaller one would suffice.

Verbs have to be in agreement with their subjects. In a research paper, do not start sentences with conjunctions or finish them with prepositions. When writing formally, it is advisable to never split an infinitive because someone will (wrongly) complain. Avoid clichés like a disease. Always shun irritating alliteration. Use language which is simple and straightforward. Put together a neat summary.

14. Arrangement of information: Each section of the main body should start with an opening sentence, and there should be a changeover at the end of the section. Give only valid and powerful arguments for your topic. You may also maintain your arguments with records.

15. Never start at the last minute: Always allow enough time for research work. Leaving everything to the last minute will degrade your paper and spoil your work.

16. Multitasking in research is not good: Doing several things at the same time is a bad habit in the case of research activity. Research is an area where everything has a particular time slot. Divide your research work into parts, and do a particular part in a particular time slot.

17. Never copy others' work: Never copy others' work and give it your name because if the evaluator has seen it anywhere, you will be in trouble. Take proper rest and food: No matter how many hours you spend on your research activity, if you are not taking care of your health, then all your efforts will have been in vain. For quality research, take proper rest and food.

18. Go to seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

19. Refresh your mind after intervals: Try to give your mind a rest by listening to soft music or sleeping in intervals. This will also improve your memory. Acquire colleagues: Always try to acquire colleagues. No matter how sharp you are, if you acquire colleagues, they can give you ideas which will be helpful to your research.

20. Think technically: Always think technically. If anything happens, search for its reasons, benefits, and demerits. Think and then print: When you go to print your paper, check that tables are not split, headings are not detached from their descriptions, and page sequence is maintained.

21. Adding unnecessary information: Do not add unnecessary information like "I have used MS Excel to draw graphs." Irrelevant and inappropriate material is superfluous. Foreign terminology and phrases are not apropos. One should never take a broad view. Analogy is like feathers on a snake. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Never oversimplify: When adding material to your research paper, never go for oversimplification; this will definitely irritate the evaluator. Be specific. Never use rhythmic redundancies. Contractions shouldn't be used in a research paper. Comparisons are as terrible as clichés. Give up ampersands, abbreviations, and so on. Remove commas that are not necessary. Parenthetical words should be between brackets or commas. Understatement is always the best way to put forward earth-shaking thoughts. Give a detailed literary review.

22. Report concluded results: Use concluded results. From raw data, filter the results, and then conclude your studies based on measurements and observations taken. An appropriate number of decimal places should be used. Parenthetical remarks are prohibited here. Proofread carefully at the final stage. At the end, give an outline to your arguments. Spot perspectives of further study of the subject. Justify your conclusion at the bottom sufficiently, which will probably include examples.

23. Upon conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print for the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects of your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form which is presented in the guidelines using the template.
- Please note the criteria peer reviewers will use for grading the final paper.

Final points:

One purpose of organizing a research paper is to let people interpret your efforts selectively. The journal requires the following sections, submitted in the order listed, with each section starting on a new page:

The introduction: This will be compiled from reference matter and reflect the design processes or outline of basis that directed you to make a study. As you carry out the process of study, the method and process section will be constructed like that. The results segment will show related statistics in nearly sequential order and direct reviewers to similar intellectual paths throughout the data that you gathered to carry out your study.

The discussion section:

This will provide understanding of the data and projections as to the implications of the results. The use of good quality references throughout the paper will give the effort trustworthiness by representing an alertness to prior workings.

Writing a research paper is not an easy job, no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record-keeping are the only means to make straightforward progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear: Adhere to recommended page limits.

Mistakes to avoid:

- Insertion of a title at the foot of a page with subsequent text on the next page.
- Separating a table, chart, or figure—confine each to a single page.
- Submitting a manuscript with pages out of sequence.
- In every section of your document, use standard writing style, including articles ("a" and "the").
- Keep paying attention to the topic of the paper.

© Copyright by Global Journals | Guidelines Handbook

- Use paragraphs to split each significant point (excluding the abstract).
- Align the primary line of each section.
- Present your points in sound order.
- Use present tense to report well-accepted matters.
- Use past tense to describe specific results.
- Do not use familiar wording; don't address the reviewer directly. Don't use slang or superlatives.
- Avoid use of extra pictures—include only those figures essential to presenting results.

Title page:

Choose a revealing title. It should be short and include the name(s) and address(es) of all authors. It should not have acronyms or abbreviations or exceed two printed lines.

Abstract: This summary should be two hundred words or less. It should clearly and briefly explain the key findings reported in the manuscript and must have precise statistics. It should not have acronyms or abbreviations. It should be logical in itself. Do not cite references at this point.

An abstract is a brief, distinct paragraph summary of finished work or work in development. In a minute or less, a reviewer can be taught the foundation behind the study, common approaches to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Use comprehensive sentences, and do not sacrifice readability for brevity; you can maintain it succinctly by phrasing sentences so that they provide more than a lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study with the subsequent elements in any summary. Try to limit the initial two items to no more than one line each.

Reason for writing the article—theory, overall issue, purpose.

- Fundamental goal.
- To-the-point depiction of the research.
- Consequences, including definite statistics—if the consequences are quantitative in nature, account for this; results of any numerical analysis should be reported. Significant conclusions or questions that emerge from the research.

Approach:

- Single section and succinct.
- An outline of the job done is always written in past tense.
- Concentrate on shortening results—limit background information to a verdict or two.
- Exact spelling, clarity of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else.

Introduction:

The introduction should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable of comprehending and calculating the purpose of your study without having to refer to other works. The basis for the study should be offered. Give the most important references, but avoid making a comprehensive appraisal of the topic. Describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will give no attention to your results. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here.

The following approach can create a valuable beginning:

- Explain the value (significance) of the study.
- Defend the model—why did you employ this particular system or method? What is its compensation? Remark upon its appropriateness from an abstract point of view as well as pointing out sensible reasons for using it.
- Present a justification. State your particular theory(-ies) or aim(s), and describe the logic that led you to choose them.
- Briefly explain the study's tentative purpose and how it meets the declared objectives.

Approach:

Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done. Sort out your thoughts; manufacture one key point for every section. If you make the four points listed above, you will need at least four paragraphs. Present surrounding information only when it is necessary to support a situation. The reviewer does not desire to read everything you know about a topic. Shape the theory specifically—do not take a broad view.

As always, give awareness to spelling, simplicity, and correctness of sentences and phrases.

Procedures (methods and materials):

This part is supposed to be the easiest to carve if you have good skills. A soundly written procedures segment allows a capable scientist to replicate your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order, but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt to give the least amount of information that would permit another capable scientist to replicate your outcome, but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section.

When a technique is used that has been well-described in another section, mention the specific item describing the way, but draw the basic principle while stating the situation. The purpose is to show all particular resources and broad procedures so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step-by-step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

Materials may be reported in part of a section or else they may be recognized along with your measures.

Methods:

- Report the method and not the particulars of each process that engaged the same methodology.
- Describe the method entirely.
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures.
- Simplify—detail how procedures were completed, not how they were performed on a particular day.
- If well-known procedures were used, account for the procedure by name, possibly with a reference, and that's all.

Approach:

It is embarrassing to use vigorous voice when documenting methods without using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result, when writing up the methods, most authors use third person passive voice.

Use standard style in this and every other part of the paper—avoid familiar lists, and use full sentences.

What to keep away from:

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings—save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part as entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Use statistics and tables, if suitable, to present consequences most efficiently.

You must clearly differentiate material which would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matters should not be submitted at all except if requested by the instructor.

© Copyright by Global Journals | Guidelines Handbook

Content:

- Sum up your conclusions in text and demonstrate them, if suitable, with figures and tables.
- In the manuscript, explain each of your consequences, and point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation of an exacting study.
- Explain results of control experiments and give remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or manuscript.

What to stay away from:

- Do not discuss or infer your outcome, report surrounding information, or try to explain anything.
- Do not include raw data or intermediate calculations in a research manuscript.
- Do not present similar data more than once.
- A manuscript should complement any figures or tables, not duplicate information.
- Never confuse figures with tables—there is a difference.

Approach:

As always, use past tense when you submit your results, and put the whole thing in a reasonable order.

Put figures and tables, appropriately numbered, in order at the end of the report.

If you desire, you may place your figures and tables properly within the text of your results section.

Figures and tables:

If you put figures and tables at the end of some details, make certain that they are visibly distinguished from any attached appendix materials, such as raw facts. Whatever the position, each table must be titled, numbered one after the other, and include a heading. All figures and tables must be divided from the text.

Discussion:

The discussion is expected to be the trickiest segment to write. A lot of papers submitted to the journal are discarded based on problems with the discussion. There is no rule for how long an argument should be.

Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implications of the study. The purpose here is to offer an understanding of your results and support all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of results should be fully described.

Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact, you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved the prospect, and let it drop at that. Make a decision as to whether each premise is supported or discarded or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."

Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work.

- You may propose future guidelines, such as how an experiment might be personalized to accomplish a new idea.
- Give details of all of your remarks as much as possible, focusing on mechanisms.
- Make a decision as to whether the tentative design sufficiently addressed the theory and whether or not it was correctly restricted. Try to present substitute explanations if they are sensible alternatives.
- One piece of research will not counter an overall question, so maintain the large picture in mind. Where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

When you refer to information, differentiate data generated by your own studies from other available information. Present work done by specific persons (including you) in past tense.

Describe generally acknowledged facts and main beliefs in present tense.

The Administration Rules

Administration Rules to Be Strictly Followed before Submitting Your Research Paper to Global Journals Inc.

Please read the following rules and regulations carefully before submitting your research paper to Global Journals Inc. to avoid rejection.

Segment draft and final research paper: You have to strictly follow the template of a research paper, failing which your paper may get rejected. You are expected to write each part of the paper wholly on your own. The peer reviewers need to identify your own perspective of the concepts in your own terms. Please do not extract straight from any other source, and do not rephrase someone else's analysis. Do not allow anyone else to proofread your manuscript.

Written material: You may discuss this with your guides and key sources. Do not copy anyone else's paper, even if this is only imitation, otherwise it will be rejected on the grounds of plagiarism, which is illegal. Various methods to avoid plagiarism are strictly applied by us to every paper, and, if found guilty, you may be blacklisted, which could affect your career adversely. To guard yourself and others from possible illegal use, please do not permit anyone to use or even read your paper and file.

Criterion for Grading a Research Paper (Compilation) by Global Journals

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals.

Topics	Grades		
	A-B	**C-D**	**E-F**
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

Index

A

Asynchronization · 13

C

Conceptual · 21
Cryptoprotection · 17

D

Dispersion · 2, 3

E

Embodiment · 1
Espionage · 3

H

Hysteresis · 14

I

İntrinsic · 6

M

Menace · 11
Modulation · 4, 10

P

Pertinent · 14

S

Spheroid · 6

T

Tremendous · 11

Global Journal of Researches in Engineering

Visit us on the Web at www.GlobalJournals.org | www.EngineeringResearch.org
or email us at helpdesk@globaljournals.org

ISSN 9755861

© Global Journals