

Journal of Electronic Systems and Programming

**Libyan Center for Electronic Systems, Programming
and Aviation Research**

**Journal
of
Electronic Systems
and Programming**

Issue No: 9 - 2024

Editorial Board	
Mr. Abadul Hakim Alhadi Anaiba	Journal Manager
Dr. El-Bahlul Fgee	Editor-in-Chief
Dr. Khari A. Armih	Member
Dr. Mustafa Kh. Aswad	Member
Dr. Haitham S. Ben Abdelmula	Member
Dr. Hend Abdelgader Eissa	Member

Editorial:
9th Issue – Journal of Electronic Systems and Programming

We are delighted to announce the publication of the 9th issue of the Journal of Electronic Systems and Programming (JESP).

As the official publication of Libyan Center for Electronic Systems, Programming and Aviation Research (EPC), the JESP aims to provide a platform for both researchers from inside and outside the center to share their novel results and latest developments, and also to seek better understanding of the current situation on research related to the area of contributions of EPC.

Finally, we thank our reviewers and authors for their fundamental contribution to the 9th release of the Journal. We still hope authors could consider JESP to be a place where to publish their work.

Editorial Board

Table of Contents:

1	Design a Graphical User Interface and Control of Nonlinear System using PID Controller	1-20
2	Detection and Prevention of Distributed Denial of Service (DDOS) Attack on Networks Using Open-Source Tools	21-40
3	Simulation and Evaluation of AODV Routing Protocols Utilizing Random Waypoint and Random Walk Models	41-62
4	Multi Criteria Separated Random User Scheduling Algorithm	63-88
5	Advanced Self-Tuning Pole-Placement Control: Computational Modeling and Estimation Techniques for Optimizing Antenna System Performance	89-124
6	Towards a Safer Smart Home: Risks and Recommendations	125-170
7	Design and Implementation of a Quadrature Hybrid Coupler in Microwave Circuits	171-197



**Design a graphical user interface
and control of nonlinear system using
PID controller**

Design a graphical user interface and control of nonlinear system using PID controller

Amer Shebani

College of computer technology Zawia

amershebani@gmail.com

Abstract

This paper focus on design a graphical user interface (GUI) and control of nonlinear system using proportional integral derivative (PID) controller. A graphical user interface (GUI) is a digital interface in which a user interacts with graphical components such as buttons, menus, and icons. The components of the GUI are such as buttons, text fields, sliders, and menus act to identify and control an object without giving details, the GUI is very useful tool for nonlinear models such as DC motor system, and dual tank system. A variety of a non-linear complex system such as robotics and many other mechanical systems, and electrical systems require modeling and control. An example of the real complex systems dealt with in this paper is the dual tank system. GUI offers the advantages of performance identifying and controlling of nonlinear systems. The non-linear identification methods used to identify the dual tank system in this paper are Auto-Regressive Exogenous (ARX) model, Auto-Regressive Moving Average Exogenous (ARMAX) model, and Box-

Jenkins (BJ) model. The PID controller used to control of the dual tank system.

Keywords: Graphical user interface (GUI), dual tank system, ARX, ARMAX, BJ, proportional integral derivative controller (PID).

1. Introduction

1.1 System identification

System identification required to model dynamic systems, where the system identification is the field of modeling dynamic systems from experimental data. A dynamic system can be theoretically defined as shown in Figure 1, where $u(t)$ is the input, and $d(t)$ is the disturbance, and $y(t)$ is the output signal.

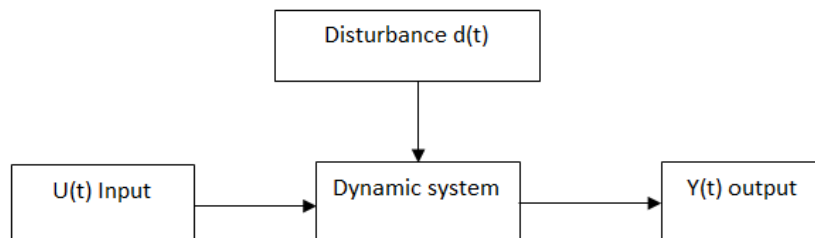


Figure 1: A dynamic system

Subjects like communications and control theories inform how to define appropriate controllers. The applicability of these theories is dependent on the availability of good models, it is hence, necessary to ask (and hopefully answer), the question "How do we construct a

good model of a given system?". This is a crucial question about the inference between the real world and the mathematical domain. The general answer to this question is that we have to study the system experimentally and make some inference from the observations. In practice there are two main ways, the first approach relies on physical laws and the second approach is based on experimentation I/O data from the system are recorded, and then, it exposed to data analysis in order to determine a system model [1] – [4].

Nonlinear systems are those systems that do not follow linear rules regarding the mutual interaction between elements, and their behavior cannot be easily predicted. Nonlinear systems are characterized by diversity, complexity, and dynamic interaction. This includes physical, environmental, social, economic, and psychological systems. This concept appears in behavior that is unexpected due to its own and multiple factors that affect the system. Examples of nonlinear systems include weather and climate, chemical reactions, biological reactions such as cell growth, and complex environmental interactions.

1.2 Approximation of nonlinear systems by linear systems

There are many nonlinear relationships between the variables of any electrical or mechanical system, for example, the saturation in the magnetic circuits and dependence of a resistance value on temperature, some of these nonlinear relationships cannot be considered linear, such as saturation of magnetic circuits, but in another type, we can neglect the nonlinearity, and consider it linear

such as changing the resistance value with temperature. To get the mathematical model from a nonlinear system, we suppose that the variables in the control system are not far from certain operating conditions, in other words, there is an operating point to the system, and the values of the variables must be near this point [5].

1.3 Approaches to identification

The system identification process in general is defined as [1], [4]:

1. From the process, collect input data and output data.
2. Decide on a set of candidate models.
3. Select one member of the model set as the best representative guided by the information in the data.

The complete identification procedure is an iterative one, and the cycle can be itemized as follows [1], [4]:

1. Design an experiment and collect input-output data from the process to be identified.
2. Filter the data by certain measure.
3. Select and define a model structure.
4. Choose the identification method to estimate the unknown parameters of the model.
5. Examine the obtained model to see whether it is an appropriate representation of the system.
6. If the model is good adequate, then stop: else, return to step 3 to try another model.

1.4 Parameter estimation methods for system identification

For identification of non-linear systems, parameter estimation methods have been considered by many researches; these methods have been very successful in many applications, but are limited in how good an approximation it may give. The most commonly models used is a linear difference is autoregressive exogeunes (ARX) model, the model is usually written as [6]:

$$A(z) Y(t) = B(z) U(t - nk) + d(t) \quad (1)$$

In which the polynomials A and B are defined as:

$$A(z) = 1 + a_1 z^{-1} + a_2 z^{-2} + \dots + a_{na} z^{-na} \quad (2)$$

$$B(z) = b_1 + b_2 z^{-1} + b_3 z^{-2} + \dots + b_{nb} z^{-nb+1} \quad (3)$$

Where B and A are polynomials in the delay operator z^{-1}

Here, the numbers na and nb are the orders of the respective polynomials. The number nk is the number of delays from input to output. Another very common model and more general, is the autoregressive moving average exogenous (ARMAX) model.

$$A(z) Y(t) = B(z) U(t - nk) + C(z) d(t) \quad (4)$$

In which the polynomial C is defined as:

$$C(z) = 1 + c_1 z^{-1} + c_2 z^{-2} + \dots + c_{nc} z^{-nc} \quad (5)$$

One more is the Box-Jenkins (BJ) model structure is given by

$$Y(t) = \frac{B(z)}{D(z)} U(t - nk) + \frac{C(z)}{F(z)} d(t) \quad (6)$$

In which the polynomials D and F are defined as:

$$D(z^{-1}) = 1 + d_1 z^{-1} + \dots + d_{nd} z^{-nd} \quad (7)$$

$$F(z^{-1}) = 1 + f_1 z^{-1} + \dots + f_{nf} z^{-nf} \quad (8)$$

All these models are special cases of the general parametric model structure:

$$A(z) Y(t) = \frac{B(z)}{D(z)} U(t - nk) + \frac{C(z)}{F(z)} d(t) \quad (9)$$

Where z is the shift operator, z^{-1} is the backward shift operator (delay operator), nk is the number of delays from system input to system output and na , nb , nc , nd and nf are the order of the polynomials A , B , C , D and F . Also $Y(t)$ and $U(t)$ are the system output and input sequences respectively and $d(t)$ is the disturbance affecting the system.

1.5 Control of nonlinear systems using proportional derivative integral (PID) controller

Control of nonlinear systems still represents big challenge for engineers. In spite of the development of more advanced control controllers, the industrial control systems still proportional derivative integral (PID) controller that because the concept of PID controller is well understood by their engineers. The function of the PID controller is to compares the actual output of the system with the desired input

that to determines the error, and produces a control signal that will reduce the error to zero (tends to zero). The routine in which the controller produces the control signal is called the control action. The PID controller has been widely used in industry, especially in electrical systems, mechanical systems, and chemical processes. Several methods for adjusting the three parameters of PID controller have been developed such as Ziegler and Nichols method [7], [8], [9], [10].

1.6 Problem formulation

In this paper, the system considered for system identification and controlling, is the dual tank system, this system is consists of two connected water tanks linked together by an orifice. In this system, an electrical water pump used to fed water into the tanks, where, the pump switched ON to move the water level in first tank one to certain level, as a result, the water level in second tank will increasing with a certain rate until it reached a steady state level. The scheme of the system is given in Figure 2. The inlet water quantity is indicated by q_i , the outlet quantities are q_1 and q_2 respectively. The water levels are indicated by L_1 and L_2 . The cross sections of a dual tank are A_1 and A_2 . The cross sections of the tubes are indicated by R_1 and R_2 [11].

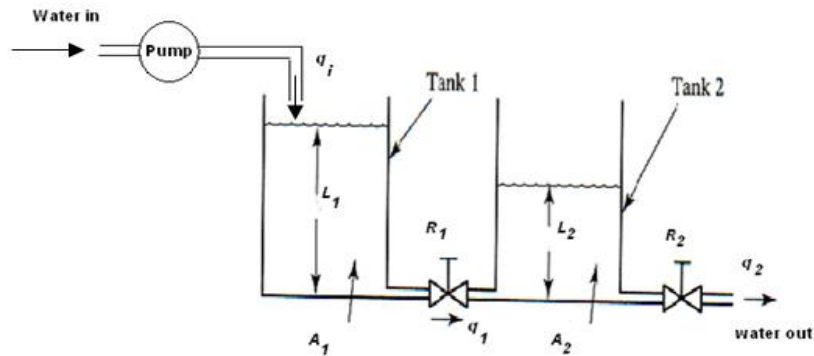


Figure 2: Block diagram representing a dual tank system structure [11]

The following differential equations describing the process dynamics of the dual tank system:

$$q_1 = (L_1 - L_2) / R_1 \quad (10)$$

$$q_2 = L_2 / R_2 \quad (11)$$

$$dL_1 / dt = (q_i - q_1) / A_1 \quad (12)$$

$$dL_2 / dt = (q_1 - q_2) / A_2 \quad (13)$$

The typical performance function used in this paper to reduce the error between actual output and estimated output is the mean square error (MSE). The MSE is shown in the following equation [12]:

$$\text{MSE} = \frac{1}{N} \sum_{i=1}^N (e_i)^2 = \frac{1}{N} \sum_{i=1}^N (t_i - y_i)^2 \quad (14)$$

Where t_i the target output and y_i is the estimated output.

Open loop system response of the dual tank system

When the reference input simulated using a unit step input, then the dual tank system output (water level) should have settling time less than 2 seconds, overshoot less than 5% and steady state error less than 1%, then, the results of the simulation should be as shown in Figure 3.

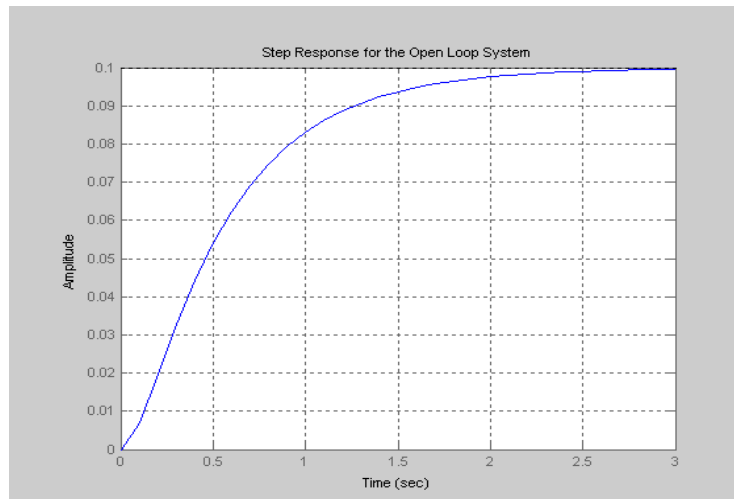


Figure 3: Open loop system response

Figure 3 shows that when 1 volt is applied to the dual tank system, the system can only achieve a maximum speed of 0.1 rad/sec.

PID controller for control of DC motor system

Proportional + Integral + Derivative (PID) controller:

A PID controller is a global feedback control loop commonly used in industrial control systems. PID stands for Proportional + Integral + Derivative, which is responsible for correcting the error resulting from the difference between the required value and the measured value.

P shows the reaction to the fault current, I proportional to the continuity of the error over time, and D proportional to the rate of change in error.

The above can be summarized into three basic functions:

Measurement function: This function is carried out by means of sensors or sensors, sometimes called transmitters. These sensors include temperature sensors, pressure sensors, movement sensors, current sensors, resistance sensors, frequency sensors, etc. The type of transmitter is chosen according to the process to be controlled.

Comparison and calculation function: The value measured via the transmitter is compared with the preset value to be accessed. The measured value is called PV while the controlled value is called SP. The result of the comparison results in a value called Error, which in turn is passed to one or a group of previous control elements and the result of processing or calculation is sent to the final control department for work.

Final control function: The types of final control elements vary depending on the process. For example, there are valves to open and close pipes, motors to control speed and direction, heaters to control temperature, and so on.

The block diagram of PID controller is shown in Figure 4.

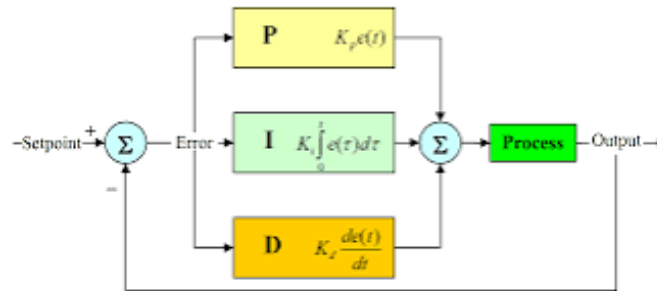


Figure 4: PID controller

The transfer function for a PID controller is

$$G_c(s) = (K_p) + (K_d S) + (K_i/S) \quad (15)$$

3. Design and running of graphical user interface (GUI)

In 1984, the researchers released its first GUI operating system. In a GUI, graphic elements represent actions can take, the common graphic elements in GUI are buttons, icons, and menus. Graphical User Interface (GUI), it is a user interface that enables the user to interact with the computer using graphical objects and images. It often consists of controls, windows, and pop-up menus in addition to texts that direct the user to use custom events such as clicking the mouse to add and enter texts. Let the computer do what the user wants. All

actions and tasks that a computer can perform are done by directly applying events to graphical elements (controls). Therefore, the purpose of GUIs is to allow persons to interact with a device's underlying code by separating users from the technical details and presenting a simplified interface to the user; this process is called abstraction. A graphical user interface allowed users to perform tasks by clicking or selecting items on the screen, rather than typing commands; this makes it a more user-friendly and user-friendly way to interact with a computer, especially for people who are not familiar with command line interfaces.

The graphical user interface has many advantages such as: even a person with no computer knowledge can use a computer and perform basic functions, searching becomes very easy as the GUI provides a visual representation of the files found and provides details about them every response from the computer is communicated visually through it, and a user who has no computer knowledge can actually start learning about the device because of it as it provides scope for users to explore and provides discoverability.

The GUI have been designed in this paper are shown in Figure (4), and it was used to implement and present the measured signal of dual tank system, ARX model response, ARMAX model response, Box-Jenkins model response, and dual tank system controlling using PID controller. To run a GUI, select run from the tools menu, or click the

run button on the tool bar, this will displays the functioning GUI outside the layout editor [9], [13].

Simulation tests:

The first part of GUI is (meas. signal & signal after approx. button) such as shown in Figure 5.

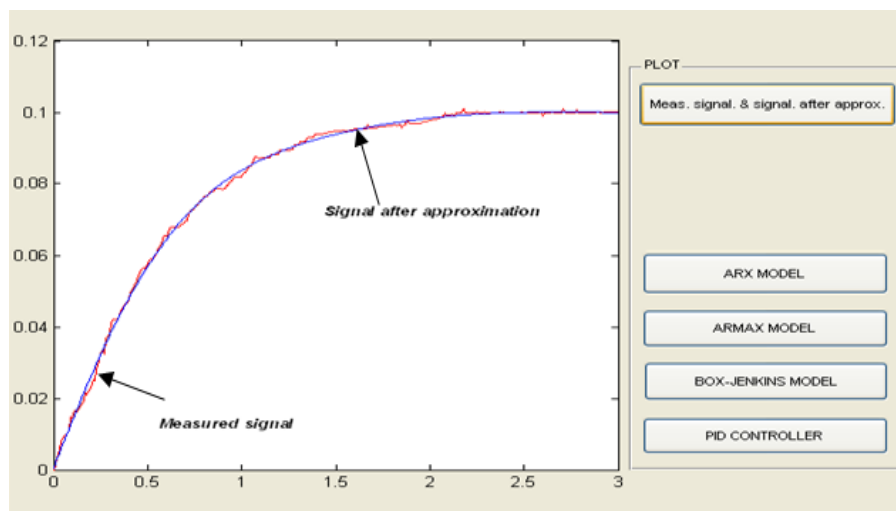


Figure 5: Measured signal and signal after approximation

The second part of GUI is (ARX MODEL button) such as shown in Figure 6.

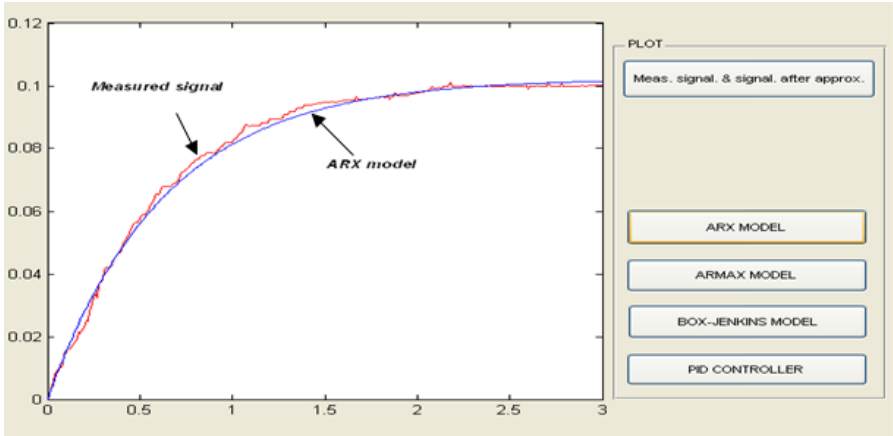


Figure 6: Measured signal and ARX model response

Simulation result shown in Figure 6 shows that the mean absolute percentage error was 4.01% for ARX model.

The third part of GUI is (ARMAX MODEL button) such as shown in Figure 7.

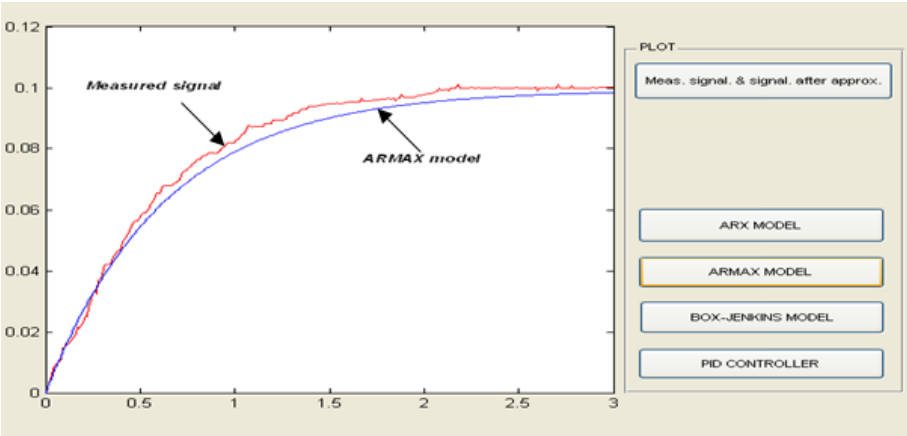


Figure 7: Measured signal and ARMAX model response

Simulation result shown in Figure 7 shows that the mean absolute percentage error was 5.71% for ARMAX model.

The fourth part of GUI is (BOX-JENKINS MODEL button) such as shown in Figure 8.

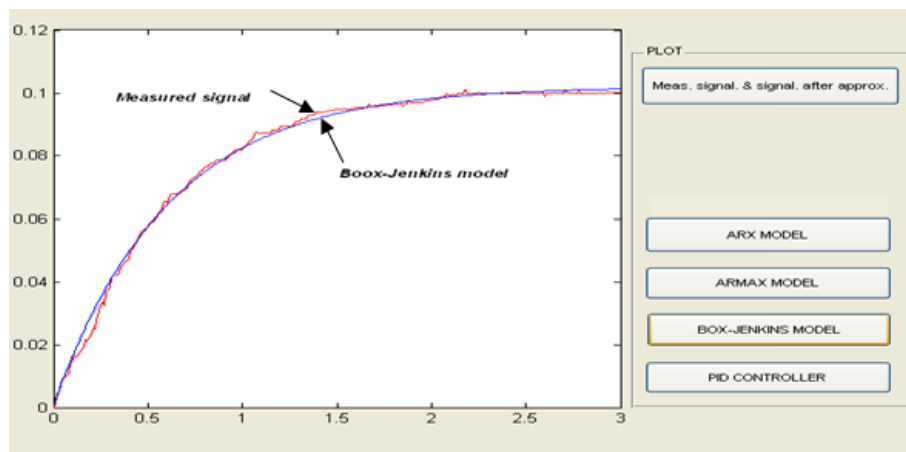


Figure 8: Measured signal and Box-Jenkins model response

Simulation result shown in Figure 8 shows that the mean absolute percentage error was 3.21% for Box-Jenkins model.

The fifth part of GUI is (PID CONTROLLER button) to get the result as shown in Figure 9.

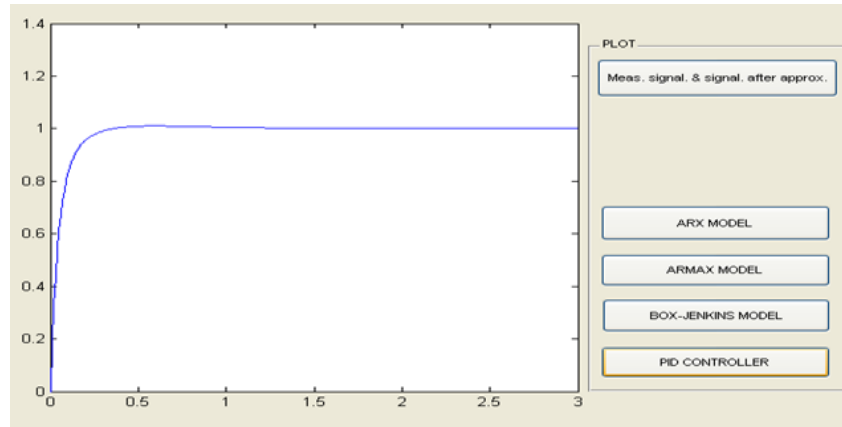


Figure 9: PID controllers for the dual tank system

Simulation results shown in Figure 9 show that the K_p , K_i and K_d are effect of each other, and the changing of one of these variables can change the effect of the other two. The PID controller $K_p = 170$, $K_i = 100$ and $K_d = 10$ are the optimum parameters used in this paper to satisfy the design requirements for the water level in the dual tank system that has an overshoot less than 5%, the steady state error less than 1% and the settling time less than 2 seconds.


4. Conclusion

A graphical user interface (GUI) designed in this work to implement of identification methods and control of nonlinear system. The models were used to identification of the dual tank system were: ARX model, ARMAX model, and Box-Jenkins model. When the results of these methods were compared, the Box-Jenkins model was the best identification model with mse of 3.21%, while the ARX model and

ARMAX model has good estimation to the system parameters. The proportional integral derivative controller (PID) used to control of dual tank system, it can concluded that the PID controller can control of the nonlinear systems efficiently. The Graphical User Interface allows the user to easily implement and compare the results of methods which are used to identifying an objects and controlling of the nonlinear systems using PID controller. Simulation tests and results were implemented using MATLAB program.

References

- [1]. Soderstrom T. and P. Stoica, (1989), "System Identification", Prentice Hall International, London.
- [2]. Phillips L. C. and H. T. Nagle, (1995), "Digital Control System Analysis and Design", third edition.
- [3]. Kuo C. B., (1995), "Automatic Control System", seventh edition.
- [4]. Manad M., (1993), "System identification", College of Electronic Engineering (BaniWleed), Libya.
- [5]. Elarbawi I., (1987), "Automatic Control Engineering", Birute
- [6]. Czarkowski D., (2002), "Identification and Optimization PID Parameters Using MATLAB", M.Sc project, DLX4- Cork .
- [7]. Chi. T., (1992), "Analog and Digital Control System Design", State University of New York.
- [8]. Ogata K., (1997), "Modern Control Engineering", third edition.
- [9]. MATLAB 6.5.1 Release 13,(2000 – 2004), toolbox user's guide.
- [10]. Sanchez J., (1996), "Adaptive Predictive Control", department of energy systems, Technical University of Madrid.
- [11]. Elbakush E., (2000) "Predictive Control Algorithms Applied for Linear Systems", M.Sc. Project, Budapest/Hungary.
- [12] C. Catalina-Lucia and G. Hakob, (2015), "An Artificial Neural Network for Data Forecasting Purposes," Informatica Economica, vol. 19.
- [13] Shebani A., (2006), "Identification and control of nonlinear systems are using PID controller and neural networks", MSc thesis, the academy of graduation studies, school of Engineering, Tripoli, Libya.



**Detection and Prevention of Distributed
Denial of Service (DDOS) Attack on
Networks Using Open-Source Tools**

2

Detection and Prevention of Distributed Denial of Service (DDoS) Attack on Networks Using Open-Source Tools

Adel Ali Eluheshi

Libyan Academy, Tripoli, Libya

Dept. of Electrical and Computer Engineering

adel.eluheshi@academy.edu.ly

Zahra Abdalla Elashaal

University of Tripoli, Tripoli, Libya

Faculty of Faculty of Information Technology

z.elashaal@uot.edu.ly

Sara Noredeen Fshekah

National Oil Corporation, Libya

IT department

sfshekah@noc.ly

Abstract

As more due to the obvious of the quickening pace of the digital transformation revolution, information and cyber security are becoming major challenges in industries like banking, telecommunications, and energy. As a branch of cyber security, network security is concerned with organizing and putting into practice safeguards against software and network hacking and illegal access. To guarantee security, the CIA security tried confidentiality, integrity, and availability must exist. Malicious actors frequently exploit distributed denial of service (DDoS) attacks to compromise availability. When it comes to DDoS detection and prevention, open-

source software is thought to be the most economical option. The purpose of this study is to investigate the efficacy and potential of open-source DDoS detection and prevention techniques. To ascertain the best open-source solution, how to launch attacks, and how to measure system performance metrics like CPU, RAM usage, packet loss, and delay, an experimental testbed was set up and assessed. Because PfSense firewall includes widely used intrusion detection/prevention systems (IDS, IPS) packages (such as Snort and Suricata), they are deployed to verify the system performance.

Keywords: DDoS - Cyber security – PfSense – IDS - Intrusion Prevention systems IPS.

1. Introduction

Network security is a critical concern due to the increasing reliance on computer systems for communication and information storage. Advanced security tools and methods are being developed to protect networks, but they are not enough to protect against threats like Distributed Denial of Service (DDoS). DDoS attacks exploit network security vulnerabilities, making them difficult to detect and prevent. Detecting and handling network traffic for DDoS attacks is a major challenge, as attackers can launch bot-networks to exhaust resources. Research has been conducted to classify DDoS attacks and suggest techniques to detect and mitigate them, with open-source-based intrusion and DDoS detection software being a popular choice due to their adaptability, support, and cost-effectiveness [1-2].

1.1 Related Work

DDoS attacks have become increasingly complex and difficult to mitigate due to the ever-changing threat landscape [3]. The size of these attacks has increased exponentially over the past two decades, as shown in Figure 1, from small-scale attacks with an estimated network traffic of 200Mbps in 2001 to over 2Tbps in 2020 [4]. Researchers have introduced various methodologies and techniques to reduce the effects or defend against DDoS attacks in different environments. One such method is the IP trace back mechanism, which focuses on tracing the origin of DDoS attacks and mitigating them by finding their sources [5]. However, traditional networks struggle to identify packet origins due to falsified source addresses. And the holistic view of the SDN control plane shows the value of finding mitigation solutions based on traceback [6].

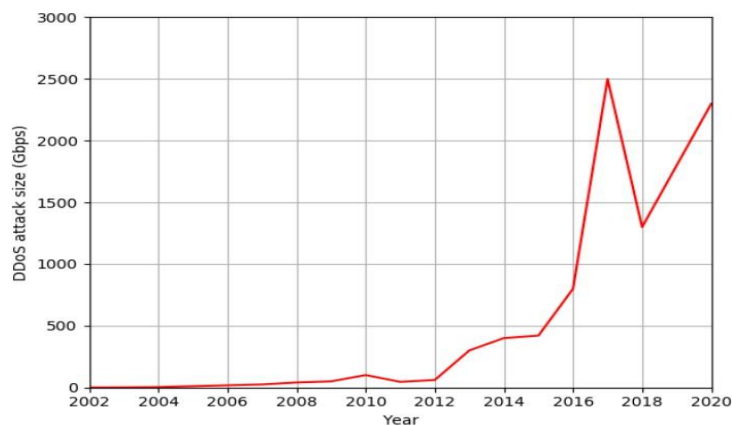


Figure 1: Largest DDoS attack size per year worldwide

A rate limit is a strategy used by SDN controllers to limit the volume of traffic that can be processed without becoming overloaded. This is often used in conjunction with Deep Packet Inspection procedures [7]. The flow filtering strategy, in [8-9] implemented natively in Open Flow-compliant devices, blocks malicious flows by considering the headers of packages. However, it can increase delay in detecting DDoS

attacks and create a bottleneck in the controller communication interface. Moving Target Defense (MTD) techniques use dynamic reconfiguration and updating of network or system characteristics based on random values to prevent attackers from making the target system unavailable [10]. A honeypot is a traditional attack mitigation technique used in isolation and monitored environments to collect information about malicious traffic [11-12]. Other approaches to DDOS attack reduction include firewalls, pseudo states in routers, data mining, and Artificial Neural Networks (ANN).

1.2 Problem Statement

This study focuses on attack detection and prevention using popular open-source tools installed on Linux operating systems. The main challenges include detecting attacks or malicious traffic without misclassifying legitimate traffic and implementing mitigation or prevention mechanisms to stop attacks before entering the internal network. Linux OS offers numerous network applications and features, making open-source intrusion and DDoS detection software available online and free, making them easy to configure and deploy in various environments. This paper investigates DDOS attacks, their ability to be launched without real source IP, the effectiveness of open-source tools in addressing DDOS, and their impact on network resources.

1.3 Research Methodology

The research methodology involves studying DDOS attacks, identifying suitable open-source software for detection and prevention, and creating an experimental testbed using a chosen open-source DDoS detection and prevention tool deployed in a Linux environment.

2. DDoS Attacks Classification

Two categories used for the classification of DDoS: one based on type and quantity, and the other on protocol.

2.1 DDoS Attacks Classification Based on Type and Quantity

DDoS attacks, also known as volume attacks, are the most common and simplest type of attacks. They aim to consume bandwidth within the target network or between the target network and the rest of the Internet, causing congestion and sending a large number of traffic that overwhelms the site's bandwidth. Common attacks include UDP flood, TCP flood, ICMP flood, and packet flood. ICMP floods send a lot of Echo request packets rapidly to the target resource, consuming both incoming and outgoing bandwidth. Protocol attacks cause service disruption by over-consuming server resources and network equipment. Application attacks are characterized by their deep knowledge of the application or protocol. Examples include HTTP flood attacks, which exploit legitimate HTTP GET or POST requests.

2.2 DDoS Attacks Classification Based on Protocol Vulnerabilities

The Internet simplicity means that core routers lack resources to implement sophisticated applications, leading to IP spoofing. Additionally, packets can travel on any path between the source and destination, making the Internet highly robust compared to traditional telephone networks.

TCP/IP protocols, the backbone of the Internet transmission structure, are a prime target for exploitive attacks. Initially, security concerns were minimal due to restricted network access. DDoS attacks can be more severe, taking down entire networks or data centers, making

them difficult to combat. These attacks use malicious traffic (TCP/UDP) to flood the victim and are classified based on TCP/IP Protocol vulnerabilities [2]. DDoS attacks can cause significant harm and disrupt legitimate users' services. DDoS attacks are classified as shown in Figure 2.

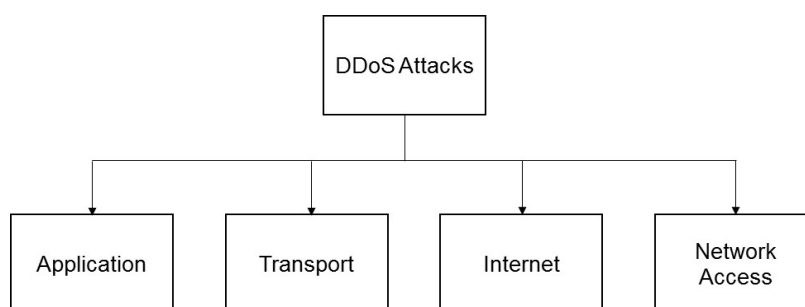


Figure 2: DDoS attacks classification based on TCP/IP protocol

Application layer attacks target weaknesses in an application or server, aiming to establish connections and exhaust processes and transactions. These sophisticated threats are harder to detect due to low traffic rates. Transport layer attacks involve volumetric attacks aimed at devastating the target machine, consuming resources until the server goes offline. DDoS attacks under transport layer include SYN flooding, UDP, and TCP flooding. Internet layer attacks exploit vulnerabilities in TCP/IP protocols, such as Smurf and ICMP flooding attacks. Network access layer attacks exploit weaknesses in network layer protocols, such as VLAN hopping, MAC flooding, DHCP attacks, and ARP poison. These attacks exploit weaknesses in network resources, causing network disruptions and causing network downtime.

3. Used OS And Tools in Experiment

Ubuntu, a free, open-source Linux distribution based on Debian, is a popular choice for cloud computing, offering three editions: Desktop,

Server, and Core, and supports OpenStack. Open-source software is software with source code available for inspection, modification, and enhancement. Originating in software development, it now encompasses a broader set of values, including open exchange, collaborative participation, rapid prototyping, transparency, meritocracy, and community-oriented development. Source code allows programmers to modify software, while proprietary or closed-source software is controlled by the creator. Open-source software licenses promote collaboration and sharing by allowing modifications to source code and incorporating them into projects. Popular open-source projects include Linux, Ansible, and Kubernetes. Both the operating systems for attackers and the mitigation solution in this study are open source.

Kali Linux is a flexible [13], Debian-based Linux distribution suitable for various information security tasks, including penetration testing, security research, computer forensics, and reverse engineering. It offers various DDoS attack tools, including information gathering, password attacks, wireless attacks, exploitation tools, and reverse engineering. These tools are mostly automated, making it easy for attackers to manage and coordinate large-scale DDoS attacks. Table 1 provides a summary of these tools. Hping3 was chosen as our attack tool in our thesis, it is installed in Kali Linux distribution.

Table-1: Attacks tools and their protocol for launching attacks

Name of Attack Tool	Protocols for launching attacks
Hping3	ICMP, UDP and TCP
LOIC	TCP and UDP
TFN	ICMP, UDP and TCP
MStream	ICMP and TCP
Trinoo	UDP
Stacheldraht	ICMP, UDP and TCP

PfSense is a free, open-source software that is designed for use as a firewall and router, managed via a web interface. It is distributed under the Apache 2.0 license and offers features such as firewall, state table, server load balancing, NAT, HA, multi-WAN, VPN, monitoring, dynamic DNS, and DHCP & Relay. PfSense is available as a hardware device, virtual appliance, and downloadable binary. Some packages are written by the PfSense community or developed by Netgate, with some providing a GUI interface for third-party software or extending the software's functionality.

The experiment used PfSense packages Suricata, Snort, and iperf. Snort is an open-source intrusion detection system (IDS) and intrusion prevention system (IPS) that provides real-time network traffic analysis and data packet logging. It uses Libpcap to sniff and log network packets, detecting real-time attacks like buffer overflows, CGI attacks, DoS, and DDoS attacks [14], and its overall architecture is shown in Figure 3.

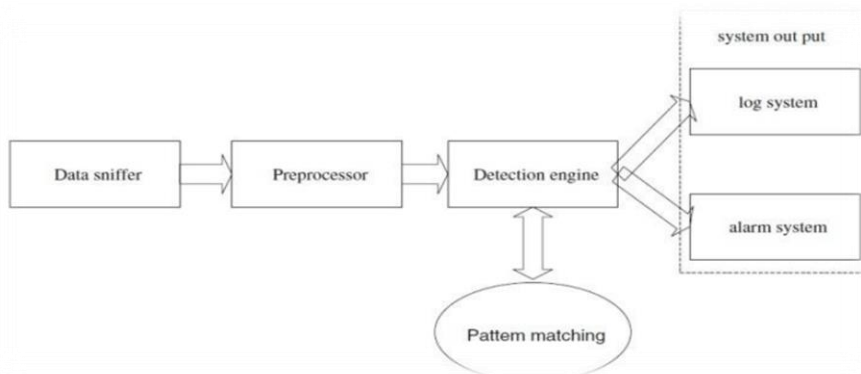


Figure 3: Snort workflow

Suricata is a high-performance Network IDS, IPS, and Network Security Monitoring engine developed by the Open Information Security Foundation (OISF) and can run on Windows, Mac, Unix, and Linux. It is multi-threaded, supports application layer protocols, supports hashing and le extraction, and has hooks for the Lua scripting

language [15]. Figure 4 shows how the thread module works. iperf3 is a tool for active measurements of the maximum achievable bandwidth on IP networks, tuning parameters related to timing, buffers, and protocols.

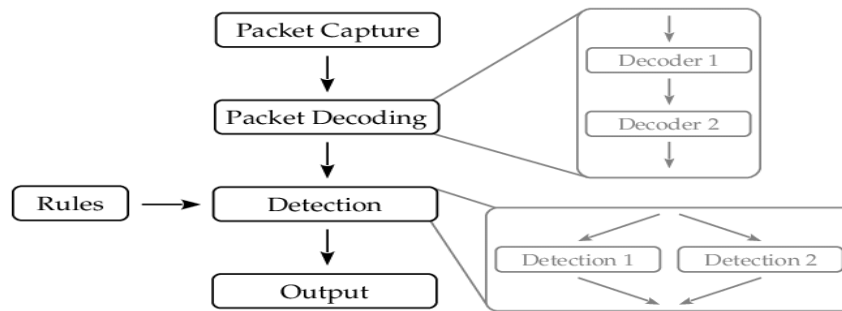


Figure 4: Suricata threat modules

4. Scenarios Used

This study tests the effectiveness of open-source tools such as snort and suricata (IDS/IPS) in protecting networks against DDoS attacks. PfSense was chosen as the most suitable software. The study involves four scenarios: testing network resources without attacks, launching attacks without defensive mechanisms, enabling snort packages, and enabling suricata packages during DDoS launch. The testbed simulates a victim end defense mechanism using PfSense installed on Ubuntu OS PC and VMware, with two network interface cards, a simple web-server, and DDoS attack tools, using the Kali Linux distribution as an attacker.

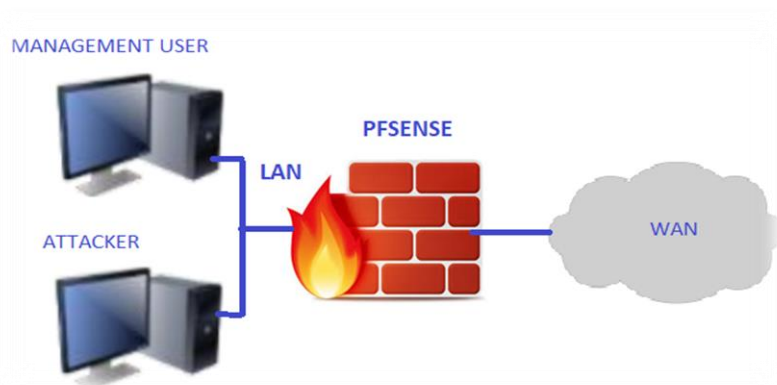
Table-2: OS and IP for the first three scenarios

	Attacker	Management User	PfSense LAN	PfSense WAN
OS	Kali Linux (vm)	Windows 7	Ubuntu (64 bit)	Ubuntu (64 bit)
RAM	2 GB	16 GB	8 GB	8 GB
IP	192.168.100.70	192.168.100.30	192.168.100.1	192.168.113.250

Table-3: OS and IP for the fourth scenario

	Attacker	Management User	PfSense LAN	PfSense WAN
OS	Kali Linux (vm)	Windows 10	PfSense (iso image)	PfSense (iso)
IP	192.168.100.70	Two NIC (DHCP & 192.168.100.2)	192.168.100.10	DHCP

Table 2 shows the OSs and IPs that were used in the first three scenarios, but with the same RAMs the OSs and IPs are different in scenario number four as indicated in Table 3, while the topology is designed for all scenarios as shown in Figure 5.

**Figure 5: Network topology used**

5. Results

The study used various tools to measure results, including the ping command for delay and the iperf tool for packet loss, jitter, and retransmission. The iperf3 tool was used for active measurements of bandwidth on IP networks, tuning timing, buffers, and protocols like TCP, UDP, and SCTP. It reported bandwidth, loss, and other parameters for each test, but is not backwards compatible. The chart in Figure 9 shows CPU and RAM utilization in seven scenarios, with normal traffic resulting in less than 5% CPU usage and 7% memory usage. After attacks without defense mechanisms, CPU processes reach 100% in TCP cases, higher than 60% in UDP. RAM usage is low due to PfSense package not enabling. Enabling snort or suricata IDS/IPS impacts CPU usage rapidly, with snort rules consuming more RAM, Figure 6 shows the resulted values of the test.

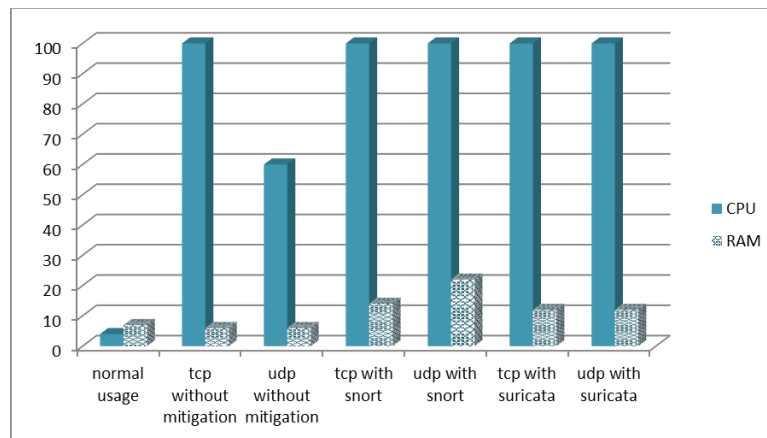


Figure 6: CPU & RAM utilization for all scenarios

Packet delay occurs in copying packets from NIC to user-space or processing packets in detection applications. The ping utility tests packet delay using defined scenarios before and after mitigation, measuring round trip times in milliseconds as shown in Figure 7.

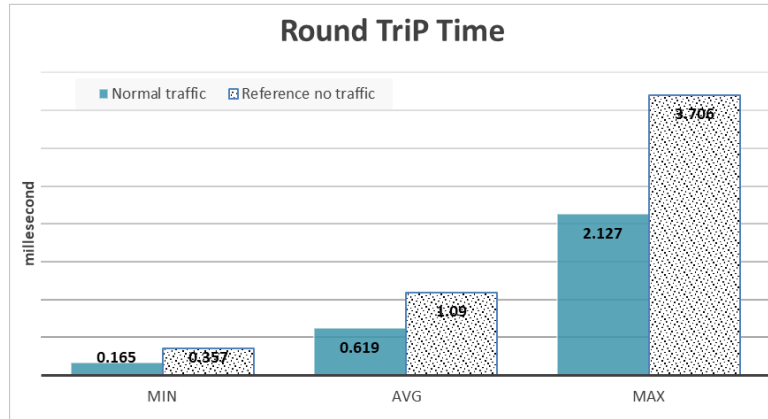


Figure 7: Packet delay under normal traffic versus the reference RTT

UDP flood attacks cause packet delay as indicated in Figure 8, while TCP-SYN floods cause packet delay and loss due to the detection engine's time re- quired to check TCP packets, as indicated in Figure 9, resulting in dropped incoming packets due to hardware's inability to cope with traffic speed.

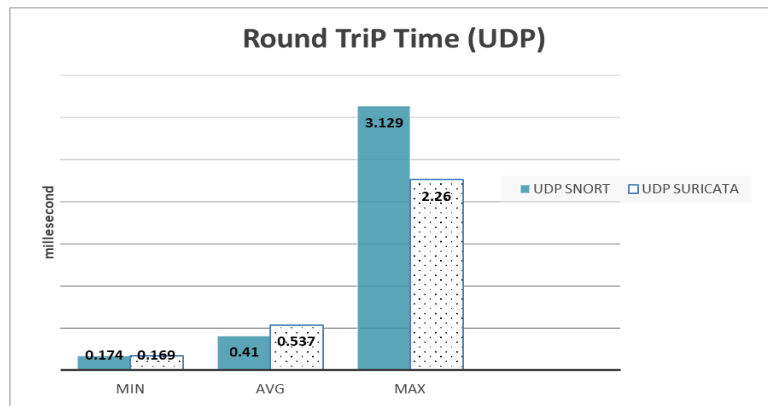


Figure 8: Packet delay under snort versus under suricata (UDP)

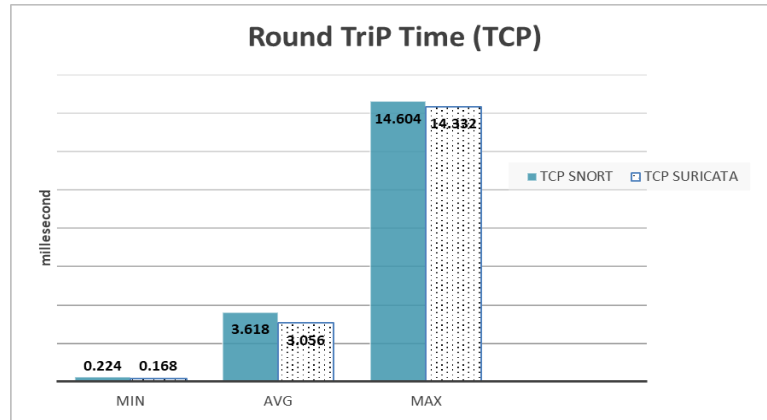


Figure 9: Packet delay under snort versus under suricata (TCP)

Packet loss and jitter are caused by DDoS attacks, while jitter is the variation in time between data packets. Cisco's Enterprise QoS Solution Reference Network Design Guide suggests guidelines for voice jitter, packet loss, and network latency tolerance. Packet loss should not exceed 1%, jitter should be less than 30ms, and network latency should not go over 150ms. TCP protocols ensure reliable delivery of packets, and if a packet is lost in TCP, it is resent along with every subsequent packet. All results are in acceptable range, except for packet loss when snort is enabled.

Tables 4, 5 show transmitted, received, losses, and retransmission packets. Tests were conducted at 60 and 120 seconds. 60 packets arrived with few jitters, while UDP packets had no loss. Increased time led to 2.5% packet loss in snort and before mitigation.

Table-4: Packet loss and jitter for UDP tests

	Tx(packet)	Rx(packet)	Packet loss	Jitter
UDP test for 60 second				
UDP SNORT	60	60	0%	0.083ms
UDP SURICATA	60	60	0%	0.095ms
UDP test for 120 second				
UDP SNORT	120	119	1.66%	0.075ms
UDP SURICATA	120	119	1.66%	0.151ms

Table-5: Packet loss and re-transmit for TCP tests

	Tx(packet)	Rx(packet)	Packet loss	Re-trans.
TCP test for 60 second				
TCP SNORT	60	59	1.66667%	1 packet
TCP SURICATA	60	60	0%	0 packet
TCP test for 120 second				
TCP SNORT	120	117	2.5%	3 packets
TCP SURICATA	120	120	0%	0 packet

6. Conclusion

This Study aims to highlight the benefits of open-source tools in Libya and study DDOS attacks, a dangerous cybersecurity threat. Successfully launching DDoS attacks with different source IP addresses was achieved using PfSense and built-in packages to detect and drop malicious traffic. The results are within acceptable range and reduce risk, but resource usage issues like CPU usage were found. Suricata IDPS is stable and has an advantage over Snort IDPS in terms of packet loss. Implementing PfSense as a firewall is beneficial for organizations or companies to protect their network. However, the

testing environment must be closed, controlled, and quarantined to avoid negative or legal repercussions.

7. Future Work


The proposal suggests increasing the number of CPU cores in modern commodity hardware for better DDoS detection performance. Increasing the attacker and victim scales could be done using distributed Raspberry Pi units. Using open-source mitigation software like fastnetmoon requires scripting and programming skills. Testing mitigation approaches in cloud or IoT is also recommended, as these topics have become trendy and require safety measures.

References

- [1] Meklit El yos Dekita, "Experimental evaluation of ddos detection and prevention using open-source and commodity hardware," *Master's thesis*, NTNU, 2018.
- [2] Stamatia Triantopoulou, Dimitrios Papanikas, and Panayiotis Kotzanikolaou, "An experimental analysis of current ddos attacks based on a provider edge router honeynet," *The 10th International Conference on Information, Intelligence, Systems and Applications (IISA)*, 2019, pp. 1-5.
- [3] Iman Sharafaldin, Arash Habibi Lashkari, Saqib Hakak, and Ali A Ghorbani, "Developing realistic distributed denial of service (ddos) attack dataset and taxonomy," *In 2019 international carnahan conference on security technology (ICCST)*, 2019, pp. 1-8.
- [4] Jose Nazario, "Ddos attack evolution," *Network Security*, vol. 7, 2008.
- [5] Abhinav Bhandari, AL Sangal, and Krishan Kumar, "Destination address entropy-based detection and traceback approach against distributed denial of service attacks," *International*

- Journal of Computer Network and Information Security*, vol. 7, 2015.
- [6] Wen Chen, Suchao Xiao, Leijie Liu, Xueqin Jiang, and Zhangbin Tang, "A ddos attacks traceback scheme for sdn-based smart city," *Computers & Electrical Engineering*, 2020.
- [7] Suman Sankar Bhunia and Mohan Gurusamy, "Dynamic attack detection and mitigation in iot using sdn," *In 27th International telecommuni- cation networks and applications conference (ITNAC)*, 2017, pp. 1-6.
- [8] Pablo Salva-Garcia, Jose M Alcaraz-Calero, Qi Wang, Jorge Bernal Bern- abe, and Antonio Skarmeta, "5g nb-iot: E cient network tra c ltering for multitenant iot cellular networks," *Security and Communication Networks*, 2018.
- [9] Alireza Shameli-Sendi, Makan Pourzandi, Mohamed Fekih-Ahmed, and Mohamed Cheriet, "Taxonomy of distributed denial of service mitigation approaches for cloud computing," *Journal of Network and Computer Applications*, issue. 58, 2015, pp. 165-179.
- [10] SUN Guozi, Wenti Jiang, GU Yu, REN Danni, and LI Huakang, "Ddos at- tacks and ash event detection based on ow characteristics in sdn," *In 15th IEEE international conference on advanced video and signal-based surveillance (AVSS)*, 2018, pp. 1-6.
- [11] Felipe S Dantas Silva, Esau Silva, Emidio P Neto, Marcilio Lemos, Au- gusto J Venancio Neto, and Flavio Esposito, "A taxonomy of ddos attack mitigation approaches featured by sdn technologies in iot scenarios, issue. 20, vol. 11, 2020.
- [12] Qiao Yan, Wenyao Huang, Xupeng Luo, Qingxiang Gong, and F Richard Yu, "A multi-level ddos mitigation framework for the industrial internet of things," *IEEE Communications Magazine*, issue. 56, vol. 2, 2018.

- [13] O Sec Services Limited, “Kali Linux - Penetration Testing and Ethical Hack- ing Linux Distribution,” *https://www.kali.org/*, August 2022. Accessed: 08 02, 2022.
- [14] RaviTeja Gaddam and M Nandhini, “An analysis of various snort-based techniques to detect and prevent intrusions in networks proposal with code refactoring snort tool in kali linux environment,” *In International Conference on Inventive Communication and Computational Technologies (ICICCT)*, 2017, pp. 10-15.
- [15] ATT Cybersecurity, “Suricata IDS: Threading Capabilities Overview,” *https://cybersecurity.att.com/blogs/security-essentials/suricata-ids-threading-capabilities-overview*, 2022. Accessed: 5 25, 2022.



**Simulation and Evaluation of AODV
Routing Protocols Utilizing Random
Waypoint and Random Walk Models**

3

Simulation and Evaluation of AODV Routing Protocols Utilizing Random Waypoint and Random Walk Models

Hisham Hejaji¹, Hend Abdelgader Eissa², Haitham S. Ben
Abdelmula³, Jamal Salem Ali Bzai⁴, Zuher H. Fhelelboom
^{1,2}College Electronic Technology - Tripoli, ^{2,3}Libyan Center for
Electronic Systems, Programming and Aviation Research, ^{3,5}College
of Computer Technology - zawia

h_alhejaji@yahoo.com¹, namarek2010@gmail.com²,
hsaa8383@gmail.com³, rahim.elhejjaji@gmail.com⁴,
zuher.h.f@gmail.com⁵

Abstract

Numerous factors influence the performance of mobile networks, with mobility models being a significant one. Within a network, a mobility model dictates the movement of nodes. The research aims to examine two types of mobility models where mobile nodes move independently of each other. This paper will present the results of an analysis comparing these models based on several performance metrics, such as end-to-end delay, throughput, and energy levels, using the AODV routing protocol and the 802.11 MAC protocol. The findings indicate that AODV under Random Walk and Random Waypoint mobility models yield similar results for comparable inputs;

however, as pause time increases, the performance differences become more pronounced. These models demonstrate variations in motion, direction, and angle.

Keywords: AD HOC, NS2, AODV routing protocol, Random Waypoint Model, Random Walk Model.

1. Introduction

During the last few years, technologies of wireless sensor networks (WSNs) have been a speedily growing interest in communication. And the network is composed of many tiny, low-power sensor nodes and one or multiple remote sinks, each equipped with actuators, and a wireless transceiver and some sensing devices. These nodes are hugely deployed in an area of need to collect information from their surroundings, and continuously report back to the remote sinks. Thus, WSNs can provide a comfortable way to monitor physical environments. In recent years, a large number of WSN-related applications for example security surveillance, health monitoring, object tracking and intelligent transportation have been proposed.

By introducing mobility to all the nodes or some of them in a WSN, we can enhance its flexibility and ability to support multiple jobs. Although WSN is usually considered as an ad-hoc network in which nodes are extended with sensing capability, mobile ad hoc network (MANET) and a mobile WSN are essentially different [1]. Mobility in

a MANET is overwhelmingly arbitrary, whereas mobility in a mobile WSN ought to be "intended". Put differently, we are able to control the movement of mobile sensors to conduct different missions.

The mobility model describes the movement of mobile sensors and how their velocity, position, and acceleration change over time. Given that mobility movement may play an important part in defining protocol performance, mobility models should be able to imitate the movement style of targeted real-life applications in a reasonable manner. When researching navigation tactics or novel communication methods, such models are routinely employed in simulation studies. Mobility management programmers for mobile communication systems employ mobility models to forecast future user positions [2]. A mobility model must attempt to simulate the motions of real mobile nodes as they occur, including changes in speed and direction, and they must occur within realistic time frames. Mobile nodes should not travel in straight lines at constant speeds since actual mobile nodes do not travel in such a constrained manner.

This research article will cover two different types of mobility models. The authors of [3] compared the performance of non-demand-based routing protocols (DSDV) and demand-based protocols (AODV) with continuous bit rate (CBR) traffic. They used the Random Waypoint Mobility Model (RWPM) to better understand the behaviour of various protocols, comparing performance parameters such as routing efficiency, throughput, normalised routing load,

packet delivery fraction, and average end-to-end time. Their research showed that AODV has lower fluctuation and beats DSDV in terms of throughput, routing overhead, and average end-to-end delay. Despite their careful investigation, the report contains various inaccuracies pertaining to pause duration and labelling; the pause times are not well-numbered, and part of the AODV and DSDV labelling is incorrect. They also assessed and compared CBR performance across several mobile scenarios provided by the Random Waypoint Mobility Model [4]. They compared the outcomes of the AODV and DSDV routing protocols for constant bit rate delay and drop rate performance using only two performance metrics: ratio and end-to-end delay.

They came to the conclusion that, when the number of connections and speed increased, DSDV lost a smaller proportion of the created data, but that the drop ratio rose. Furthermore, an increase in connections resulted in a higher DSDV end-to-end delay. While they did not offer a performance study for AODV, they did observe in their paper that CBR outperformed DSDV on AODV and was more stable in low mobility scenarios than in high mobility ones.

2. Random Waypoint and Random Walk Models

The Random Waypoint model and the Random Walk model are two commonly used mobility models in the field of wireless communication networks and mobile computing. While they both involve random movements of mobile nodes, they differ in certain aspects of their behavior.

2.1 Random Waypoint Model:

The Random Waypoint model, as described in the previous response, involves nodes moving between randomly selected waypoints within a defined area. The nodes remain stationary at each waypoint for a certain pause time and then randomly select a new destination. The movement between waypoints is typically characterized by a maximum speed, allowing nodes to move at different velocities.

2.2 Random Walk Model:

The Random Walk model is a simpler mobility model where nodes move in a more continuous and less structured manner. In this model, nodes start from an initial position and take steps in random directions. Each step has a fixed length, and the direction is chosen randomly from a uniform distribution. The nodes continue this random movement pattern without any predefined waypoints or pause times.

The main differences between the Random Waypoint model and the Random Walk model can be summarized as follows:

a. Movement Pattern: In the Random Waypoint model, nodes move between predefined waypoints, while in the Random Walk model, nodes move in a more continuous and unrestricted manner.

b. Pause Time: The Random Waypoint model includes a pause time during which nodes remain stationary at each waypoint. The Random

Walk model does not have a pause time since nodes continuously take steps in random directions.

c. Predictability: The Random Waypoint model allows for greater predictability of node movements since the waypoints are predetermined and nodes follow a specific pattern. In contrast, the Random Walk model results in more unpredictable and less structured movement patterns.

Both models have their own use cases and applications. The Random Waypoint model is often employed when simulating realistic mobility scenarios, such as in the evaluation of routing protocols and mobility management algorithms.

3. AODV Routing Protocols

The AODV (Ad hoc On-Demand Distance Vector) routing protocol is a popular routing protocol designed for mobile ad hoc networks (MANETs). It is a reactive routing protocol, meaning that routes are established on-demand as needed by the nodes when they want to communicate with each other. Here are some key features and characteristics of the AODV routing protocol:

Route Discovery: When a source node wants to send data to a destination node and does not have a valid route to it, it initiates a route discovery process. The source node broadcasts a Route Request (RREQ) packet to its neighboring nodes, which in turn forward the RREQ to their neighbors. This process continues until the RREQ

reaches the destination node or an intermediate node with a fresh route to the destination.

Route Reply: When the destination node or an intermediate node with a route to the destination receives the RREQ, it sends a Route Reply (RREP) packet back to the source node. The RREP contains the route information, such as the sequence numbers and hop count, allowing the source node to establish a route to the destination.

Route Maintenance: Nodes periodically exchange control packets called Hello messages to ensure the freshness of their routes. If a node detects a link failure or a destination becomes unreachable, it initiates a route error process. The affected node broadcasts a Route Error (RERR) packet to inform other nodes about the broken link or unreachable destination, and those nodes update their routing tables accordingly.

AODV is widely used in MANETs due to its reactive nature, which reduces the control packet overhead compared to proactive routing protocols. It is suitable for dynamic and mobile networks where nodes may frequently join, leave, or move within the network. AODV is implemented in various simulation tools.

4. METHODOLOGY

The primary aim of this study is to evaluate the performance of the Random Waypoint and Random Walk mobility models for MANET

routing protocols using available network simulators NS-2. The basic methodology involves first selecting the most representative parameters for a mobile ad-hoc network, then defining and simulating all scenarios, and finally analyzing the results.

This section outlines the research methodology employed to compare and analyze the performance of protocols across three different network environments, as previously discussed. The methodology follows the waterfall model, a step-by-step design process often used in research analysis.

Performance Metrics:

- At this point, we have chosen particular parameters to assess how well AODV routing algorithms work in the presence of random mobility. Energy level, throughput, and end-to-end delay are the selected measures.
- The calculation of the Average Energy Level involves dividing the total energy consumed by the total number of nodes.
- • Throughput: The volume of data sent from the source to the destination in a predetermined length of time is referred to as throughput in communication networks. The average rate of successful data delivery via a communication link is another way to characterize it.
- • End-to-End Delay: The interval of time between a packet's transmission and reception. It can also be defined as the total

of all packet store-and-forward delays in all routers, including network queuing delays.

The simulation method considered two scenarios of a wireless network: Random Waypoint and Random Walk, across three different network sizes consisting of 25, 50, and 100 nodes each, placed within a 600m x 600m area. The simulation runs for 600 seconds. Table 1 presents the significant simulation parameters used in this method.

Table 1: Page Simulation Parameter

PARAMETER	VALUE
SIMULATION TIME	600 SEC
SIMULATION AREA	600M X 600M
ANTENNA	OMNI ANTENNA
NO. OF NODES	25, 50 AND 100
UDP VARIANTS	UDP
PACKET SIZE	1000 BYTES
MAX QUEUE LENGTH	50
TRAFFIC	CBR
ROUTING PROTOCOL	AODV
MOBILITY MODEL	RANDOM WAYPOINT MODEL RANDOM WALK MODEL

5. Results

Using the Ns2 simulator on the OBINTU 14.04 operating system, along with tools like Bonnmotion, AWK script, and Microsoft Excel 365, we analyzed the results obtained from the trace files after running the RWPM and RWM simulations 31 times with different seeds each time.

A. Throughput

Throughput, measured as messages per second, is calculated by dividing the total number of delivered data packets by the total simulation time. This metric evaluates the performance of each routing protocol based on the number of messages delivered per second [5]. When comparing Random Waypoint (RWPM) and Random Walk (RWM) in terms of throughput, Figures 1.1 and 1.2 demonstrate that RWPM achieves higher throughput in small network areas and experiences a gradual decrease as the network area expands to medium and large sizes. In contrast, RWM exhibits lower throughput in large network areas, with an increase in performance observed in medium and small network areas.

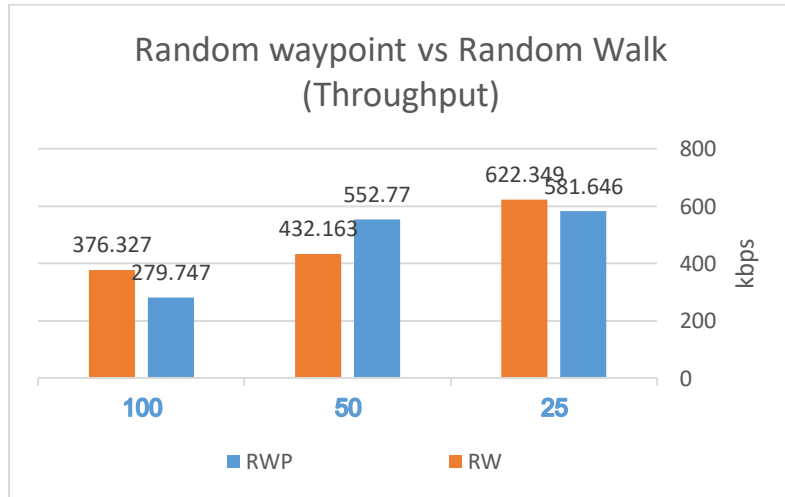


Figure 1.1: Comparing between RWP and RW in Throughput

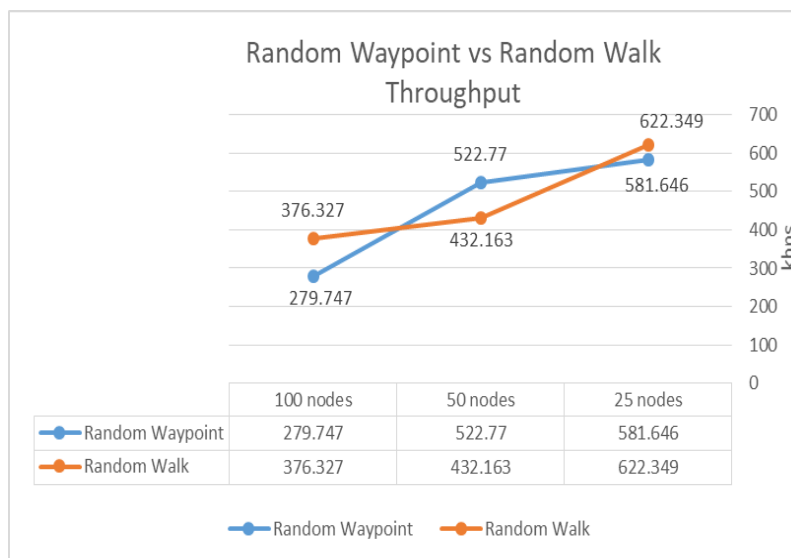


Figure 1.2: Comparing between RWP and RW

B. End to End delay

It shows average amount of time taken by packet to travel from the source node to the application layer of the destination node [6].

Comparing between Random Waypoint and Random Walk in End-to-End delay, Figure 2.1 and Figure 2.2 show Random Waypoint's End to End Delay is always higher than Random Walk for any number of nodes. It is interesting to see that there is an optimal End to End delay for RWP around 50 nodes. Random Walk shows less End to End delay as network area increases.

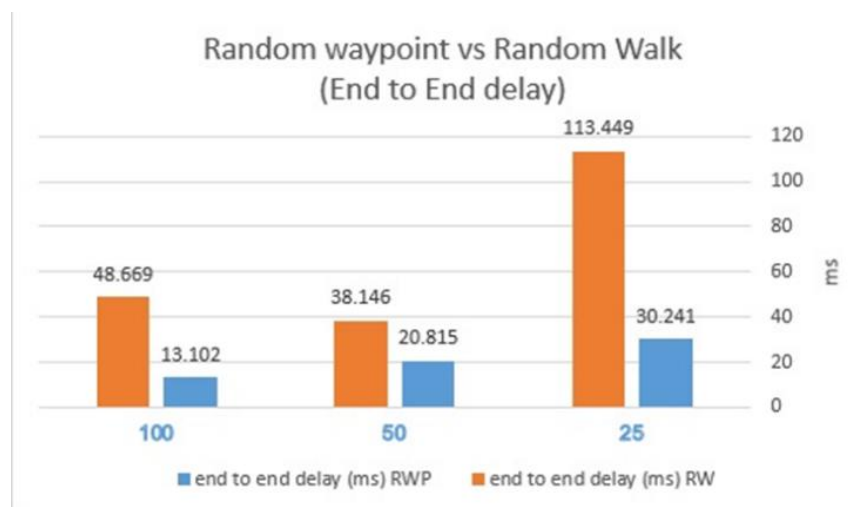


Figure 2.1: RWP vs RW (End to End delay)

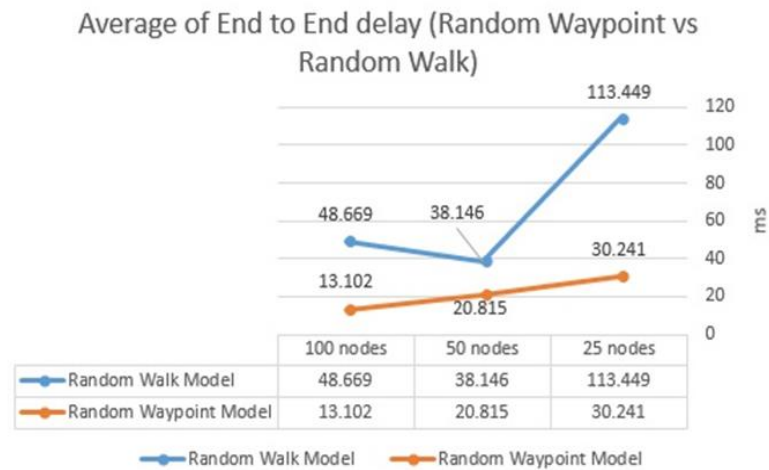


Figure 2.2: RWP vs RW (End to End delay)

C. Average of Energy

Average Energy is calculated by dividing the total energy consumed by number of nodes [7].

Comparing Random Waypoint versus Random Walk in Average Energy, Figure 3.1 and Figure 3.2 show that Random Waypoint is high for large network area and increases as network area decreases. Random Walk shows high average of energy at small network area and decreases for medium & large networks.

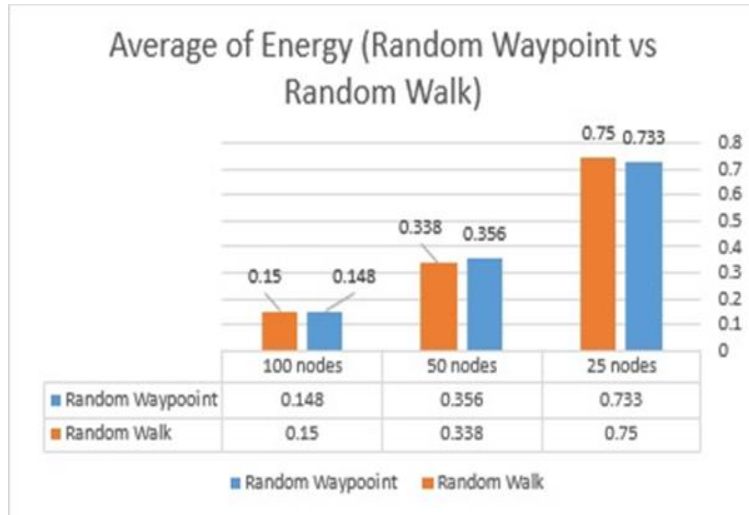


Figure 3.1: Average of Energy (RWP vs RW)

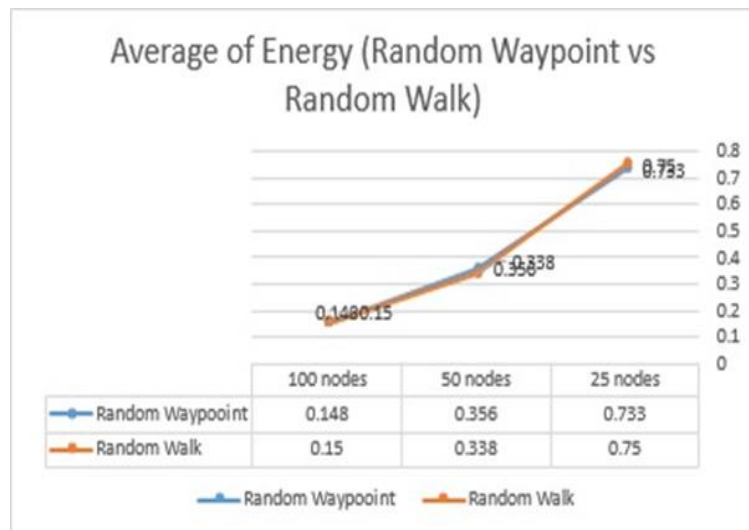


Figure 3.2: Average of Energy (RWP vs RW)

D. Total Received and Dropped-Packets.

Total Received and Dropped-Packets is calculated by dividing the number of packets received or dropped by the destination through the number of packets originated by the application layer of the source [8].

Comparing between Random Waypoint and Random Walk in Received and Dropped Packets, Figure 4.1 and Figure 4.2 show that Random Waypoint is high for medium and large network area as move to small network areas it's going low. Random Walk shows less Received and Dropped Packets at small network area and increases for medium and large networks.

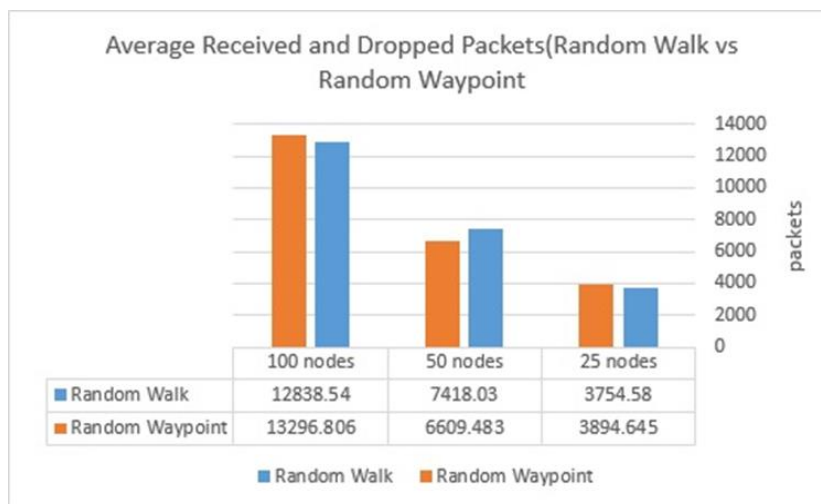


Figure 4.1: Received and Dropped Packets (RWP vs RW)

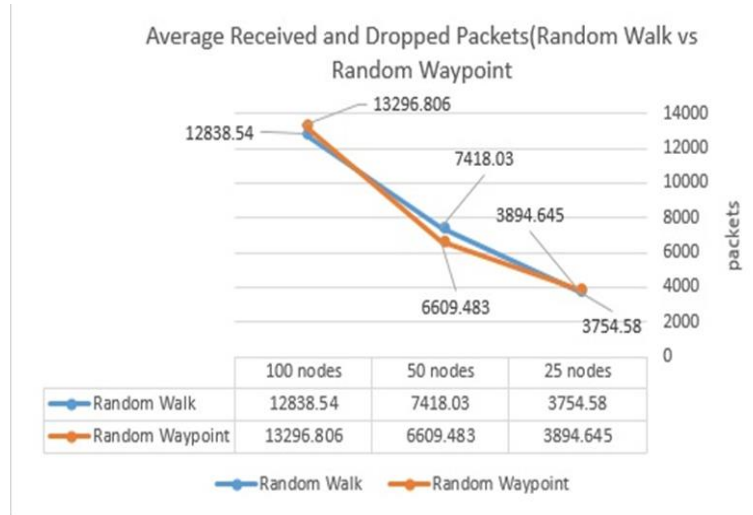


Figure 4.2: Received and Dropped Packets (RWP vs RW)

6. Conclusion

This paper provides a comprehensive analysis of the AODV reactive routing protocol by examining both the Random Waypoint and Random Walk mobility models. The NS2 Simulator was utilized to evaluate the performance metrics of these protocols. Key parameters such as end-to-end delay, throughput, packet loss and reception, and average energy levels were considered to assess the protocol's effectiveness. The simulation results indicate that the Random Waypoint model outperforms the Random Walk model when testing with 50 nodes, while the Random Walk model shows better performance with 25 and 100 nodes. The Random Waypoint model demonstrates a lower average end-to-end delay compared to the

Random Walk model, and similar trends were observed in terms of packet reception and loss. Ultimately, the study concludes that the Random Waypoint and Random Walk mobility models are fundamentally similar, with comparable motion patterns, angles, directions, and speeds.

References

- [1] Aguilar Igartua, Monica, "Performance evaluation of realistic scenarios", Universitat Politècnica de Catalunya. Departament d'Enginyeria Telemàtica, & Calzada Canero, Roger, (2011).
- [2] R.Alagu Pushpa A. Vallimayil V.R.Sarma Dhulipala," Impact of Mobility models on Mobile Sensor Networks", International Journal of Communication Network & Security,2011.
- [3] Anul K. Gupta, Harsh Sadawarti, Anil K rma of in rent, "Mobility Di Performance Analysis of MANET Routing Protocols Models", I.J. Information Technology and Computer Science,2013.
- [4] Subodh Kumar," Impact of CBR FTP Traffic patterns and varying node density on Performance of Routing Protocols in MANETs", G s. 11, Sudhir Kumar Sharma 201 January Agrawal, subodh Kumar et al 2015.
- [5] Aguilar Igartua, Mónica, Universitat Politècnica de Catalunya. Departament d'Enginyeria Telemàtica, & Calzada Cañero, Roger, "Performance evaluation of realistic scenarios for vehicular ad hoc networks with VanetMobiSim and NS2. Universitat Politècnica de Catalunya",2011.
- [6] Sahadevaiah, K., & Venkata, R. O. B. An Empirical Examination of Routing Protocols in Mobile Ad Hoc Networks. International Journal of Communications, Network and System Sciences, 3, 6, 511-522,January 01, 2010.

- [7] Said, S. M., El, E. I. M. M., & Kadim, S., "Comparative study between the Performance of proactive and reactive mobile ad-hoc networks (MANET) routing protocols with varying mobility", Scientific Research and Essays, 6, 6, 1256-1274, March 01, 2011.
- [8] Ahed Alshanyour¹ and Uthman Baroudi², "A Simulation Study: The Impact of Random and Realistic Mobility Models on the Performance of Bypass-AODV in Ad Hoc Wireless Networks Hindawi Publishing Corporation EURASIP", Journal on Wireless Communications and Networking.2010.



**Multi Criteria Separated Random User
Scheduling Algorithm**

4

Multi Criteria Separated Random User Scheduling Algorithm

Ahmed A. Ali Alsabri

Department of Computer Science

Faculty of Information Technology, University of Zawia

ah.ali20260@gmail.com

Abstract

Carrier Aggregation (CA) is one of the main physical transmission features in Long Term Evolution– Advanced (LTE-A). CA offer successively higher peak data rates in excess of 1 Gbps in the downlink and 500 Mbps in the uplink by aggregating multiple Component Carriers (CCs) each of 20 MHz. Separate Random User Scheduling (SRUS) is the prominent resource scheduling scheme, which has been adopted in 3GPP Rel.10. There is always a trade-off between simplicity and complexity for the aforementioned resource scheduling scheme. For instance, SRUS is simple but less efficient. However, it produces low throughput, high latency and unfairness to various user applications under heavy traffic loads. In this paper, optimum random user scheduling algorithm with CA for LTE-A downlink has been proposed. The main algorithm, namely Multi-Criteria-SRUS (MC-SRUS) has been implemented and integrated

with the proposed bandwidth estimation and bandwidth allocation. MC-SRUS is based on single CC. To guarantee equitable resource distribution, satisfactory throughput performance and allowable latency, the algorithm have fused together; channel quality indicator, average throughput and head of the line delay along with user's preferences, based on different Quality of Service (QoS) to form the core scheduling decision metric. The validation process was carried out by using the Matlab System Level Simulator. The MC-SRUS algorithm is compared with SRUS, Exponential/Proportional Fairness (EXP/PF-SRUS) and Best-CQI-SRUS. The simulation results shown that the MC-SRUS achieved 23.07% enhancement in the Fairness Index compared to EXP/PF-SURS. Moreover, MC-SRUS reduces packet delay by 1.2 ms compared to EXP/PF-SRUS.

Keywords: LTE-advanced, SRUS, fairness, carrier aggregation, Multi-Criteria-SRUS.

1. Introduction

With a few updates on the latest LTE requirements in Release 9, LTE Release 10 and 11 are the equivalent of LTE-Advanced. LTE-Advanced standard is progressing. As compared to LTE, LTE Advanced is capable of showcasing greater improved system performance. With regards to peak data, it can reach up to 1 Gbps in the downlink and 500 Mbps in the uplink, as opposed to LTE, which provides a maximum of 100 Mbps in the downlink and 50 Mbps in the

uplink. Along with considerable enhancements for cells and users, LTE Advanced also caters for two other objectives. (i) Proficient spectrum utilization. (ii) Increased power, productivity for users as well as infrastructure [1]. It can be recollected that several promising technologies are loaded in 3GPP LTE-Advanced. These include enhanced Inter-Cell Interference Coordination (eICIC), Carrier Aggregation (CA), Coordinated Multi-Point (CoMP), and advanced Multiple-Input Multiple-Output (MIMO) transmissions, which are capable of delivering an increasing spectral efficiency and effective transmission [2]. Carrier Aggregation (CA) is reputed to be the best vital technology due to its capability of providing high throughput for LTE-A networks. CA can be achieved by combining two or more component carriers to enhance the data rate. With the application of carrier aggregation technology, any user can be potentially programmed on either continuous or non-continuous component carriers (CCs) mode [3].

2. Separated Random User Scheduling

The SRUS scheme requires two-level scheduling. The first level is responsible for allocating users to only one CC. Here, a random sender is designated. Meanwhile, the load balance criterion is assumed to be guaranteed, which means that each CC must afford the transmissions of all U/C users (where U is the number of users and C the number of component carriers). Four different users can be allocated to two CCs randomly and uniformly.

It is a critical issue to ensure the performance of cell-edge users, especially after introducing CA. At the same time, backward compatibility is a very important feature of the LTE-Advanced system. Taking into account the system backward compatibility and coverage difference of carriers in system, it is a matter of concern to design appropriate carrier weight factors for users to improve the performance of cell-edge users and LTE users. The SRUS scheme has low complexity, but it cannot fully utilize the radio resource and the system throughput is low [3]. The RSs controls the second level of resource scheduling. The system should consist of the same number of RS and CC. Consequently, each RS's resource pool contains the resource from only one of the CCs [4-5]. $P_{k,i,m}$ of the user k can be calculated as:

$$P_{k,i,m} = \frac{R_{k,i,m}(t)}{\bar{R}_{k,i}(t)} \quad (1)$$

$\bar{R}_{k,i}(t)$ is the average throughput for user on the i -th CC

Hence an updated version:

$$\bar{R}_{k,i}(t+1) = \left(1 - \frac{1}{T}\right) \bar{R}_{k,i}(t) + \frac{1}{T} R_{k,i}(t) \quad (2)$$

$R_{k,i,m}(t)$ is the estimated throughput for user k at the m^{th} PRB group of the i -th CC at time slot t . Whereby T = average window length.

3. The Proposed Multi Criteria SRUS (MC-SRUS)

The existing SRUS algorithms have some limitations in terms of fairness, throughput and packet loss ratio. For instance, the PF-SRUS algorithm, despite providing a fair resource distribution, has several drawbacks in terms of limiting variations in channel condition which might otherwise result in poor service quality and prioritizing users with high CQI condition at the detriment of those with low CQI.

A solution for this issue is proposed by using the MC-SRUS algorithm for the LTE-A network. The MC-SRUS algorithm improves the system fairness while maintaining a higher bit rate. The proposed scheduling algorithm is based on multi-attribute decision making technique. It provides enhanced system fairness and throughput while not adding on to the complexity of the system. Each user will go through three phases of processing namely the Bandwidth Estimation Phase, the Bandwidth Allocation Phase and the Scheduling Phase. This algorithm based on multi phases is shown in Figure 1.

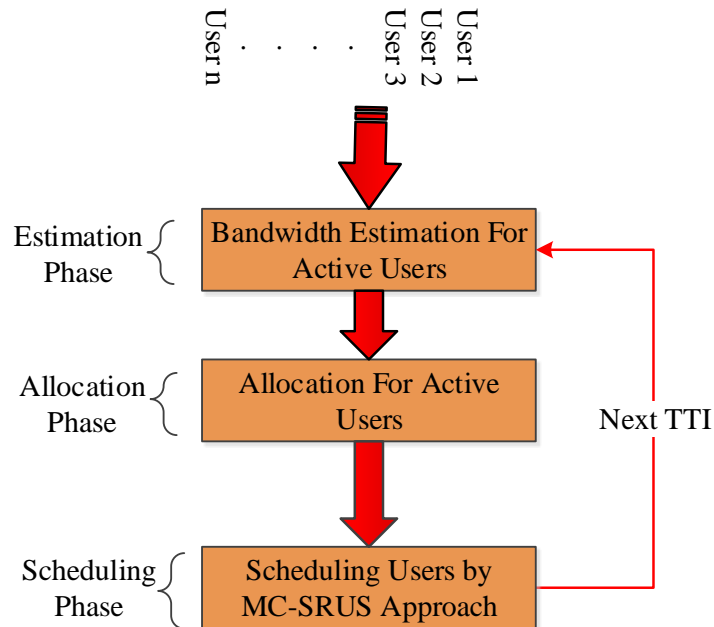


Figure 1: System Model for The Proposed MC-SRUS

3.1. Bandwidth Estimation Phase

With reference to Figure 1, since the number of active users is known by the eNB, the number of resources required to serve the active users are determined as explained in the following.

Owing to random variations in the radio conditions of an LTE-A network, the obtainable bit rate for an active user is supposed to vary. The information about whether or not there is enough bandwidth to allocate to a new user is required and this is obtained by determining the transmission data rate for each RB. The estimation for the RB data rate is based on the signal to interference noise ratio which is received

at UE from the eNB. Many factors influence the data transmission ability of each RB including the distance from the eNB, the power allocated for each RB and the external as well as internal noise. For the power allocation in this study, all the RBs have the same transmission power. The internal noise is the thermal noise of the receiver and the external noise is due to interference from neighboring eNBs.

The system capacity is first determined from the spectral efficiency and the operating bandwidth. At each interval (TTI), the user reports his signal to noise ratio value back to the eNB. The scheduler then determines the eligibility of each RB for data transmission as follows:

$$RB_{k,c}(t) = \frac{nb}{symbol} \times \frac{ns}{slot} \times \frac{nsl}{subcarrier} \times \frac{Ns}{RB} \quad (3)$$

Where,

c is the component carrier index

nb are the number of bits

ns are the number of symbols

nsl are the number of slots

Ns are the number of subcarriers, respectively

All the variables in the above Equation are fixed except the number of bits per symbol. The number of bits per symbol metric impacts the RB's obtainable data rate which changes along with SINR ratio. The estimated system capacity is then calculated by the summation of RBs

data rate for the RBs which have the transmission eligibility. This calculation is updated for each TTI.

The SINR is calculated as the channel gain multiplied by the assigned power for the RBs, over the noise and interference as shown in the Equation 5. The path loss and the channel gain are calculated for each user on c^{th} RB.

$$CH_{gain,c} = 10^{\frac{pathloss}{10} \times \frac{multi-fading}{10} \times \frac{fading}{10}} \quad (4)$$

$$SINR = \frac{CH_{gain,c} \times P_{subcarrier}}{N_0 + I} \quad (5)$$

where

CH is the channel gain.

N_0 is the thermal noise.

I is the interference from the surrounding eNB.

After the SINR feedback values from all the users are calculated, the exact amount of data transfer is then computed. CQI index and SINR value are directly proportional to each other. For all the active users, the demand data rate $R_{k,c}$ required by user k of c th component carrier at time slot t can be achieved by allocating n RBs for user k at time t with specific MCS following Equation 6. The number of the required RBs at time t for user k is then calculated according to Equation 7. It

is noted that all the RBs which are assigned to user k at time t have the same MCS.

$$n_k = \frac{R_{k,c}}{RB_{k,c}(t)} \quad (6)$$

$$NRB_k(t) = \frac{n_k}{d_k} \quad (7)$$

where,

n_k is the total number of RBs which is required to satisfy the user k .

$NRB_k(t)$ is the number of RBs which are required by user k at time t .

d_k is the maximum delay budget for user k .

3.2. Bandwidth Allocation Phase

Since the number of resource blocks can be accurately defined by the eNB, the bandwidth allocation phase will assign resources fairly among different users as shown in Pseudo-code 1.

Pseudo-code 1. Proposed bandwidth allocation algorithm

Bandwidth Allocation Algorithm

- 1: insert B, i ,
- 2: **calculate** Bandwidth demands for all active users.
- 3: **for** k , such that $1 \leq k \leq i$ and $k \in i$ **do**

```

4:   compute  $NRB_k(t)$ 

6:   if  $B \geq \sum_{k=1}^i R_{k,c}(t)$  then

7:     served user  $k \in [1, 2, \dots, i]$ 

8:   else

9:     calculate  $\delta$ ; where  $\delta \leq B_{k,c}$ , Allocate users  $k \in [1, 2, \dots, \delta]$ ;

12:  end if

13:  end for

14:  end procedure

```

where,

$B(t)$ is the offered bandwidth from the system at time t

δ is the difference value between the offered and demanded data rate.

$$\delta = \sum_{c=1}^q \sum_{k=1}^i n_{k,c} \quad (8)$$

Where,

q is the total number of available CC.

i is the total number of UEs.

3.3. Scheduling Phase

The scheduling phase computes the criteria values. Three criteria values for each user are calculated and inserted as input to the MC–SRUS algorithm as follows:

- a) The instantaneous to past average throughput metric: this metric gives the past average throughput of different users served by the eNB over time t . Since the metric is updated every TTI for each user, the fairness amongst users is thus guaranteed. The past average throughput is calculated as follows:

$$\bar{R}_{k,c}(t) = \alpha \times \bar{R}_{k,c}(t-1) + (1-\alpha) \times R_{k,c}(t) \quad (9)$$

where $0 \leq \alpha \leq 1$

Where,

$\bar{R}_{k,c}(t)$ is the past average throughput of user k of c th component carrier at time t .

α is a constant related to the window size.

$R_{k,c}(t)$ is the estimated data rate of user k of c th component carrier at time t .

- b) The metric $\eta_{CQI(i)}$: This metric determines the expected data rate for user k at the current TTI. Thus, the throughput among users is guaranteed.

$$\eta_{CQI(i)} = \frac{\sum_{k=1}^i \eta_{CQI(k)}}{i} \quad (10)$$

Where,

$\eta_{CQI(i)}$ is the average data rate among all active users.

- c) HOL metric: where each user k is calculated as ratio of the difference between current time and stamped time when the packet entered the eNB buffer queue. This metric considers the delay budget of each UE. By doing so the minimum delay is guaranteed.

$$HOL_k(t) = t - T_{stamp,p,k} \quad (11)$$

Where,

$HOL_k(t)$ is the head of line delay of user k at time t .

$T_{stamp,p,k}$ is the entrance time of user k 's packets into the buffer queue.

p is the packet index.

The MC_SRUS algorithm is based on the proportional linear transformation of the raw data (instantaneous/past average throughput, head of line delay and CQI efficiency). This algorithm ensures low complexity, dynamic adjustment and effective control of the scheduling algorithm behavior as well as in satisfying the application's demands. The dynamic weighting factors namely head of line delay, instantaneous/past average throughput and CQI

efficiency are used to adjust scheduling decisions with respect to the demands of each application. The MC_SRUS algorithm is described in Figure 2.

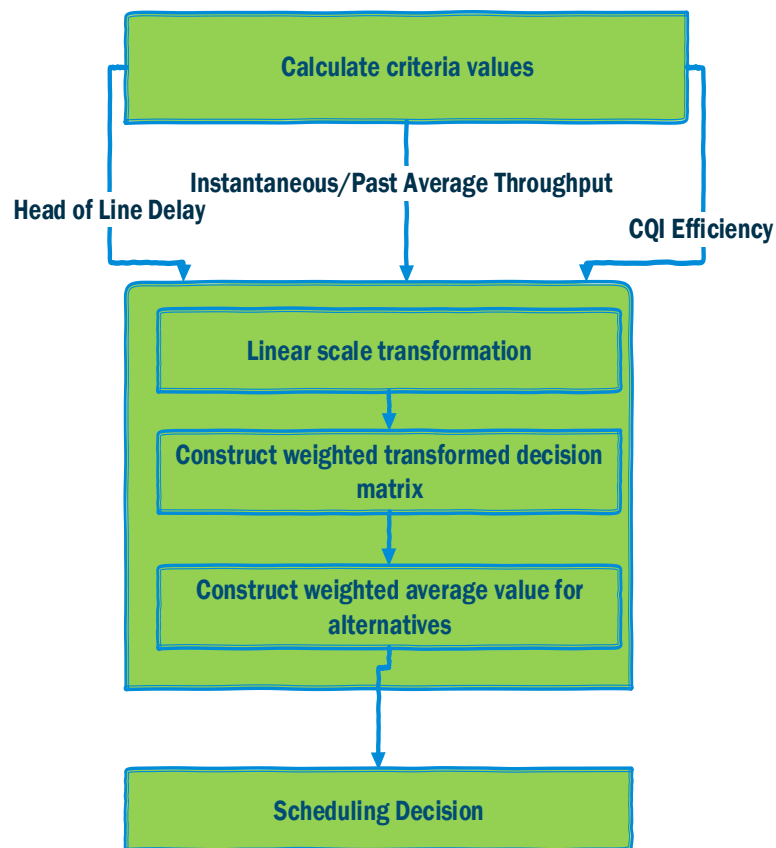


Figure 2: The MC-SRUS Model

The Linear scale transformation of the data collection is normalized by the maximum value of the criterion for all users as a process to unify all values up to one measurement scale for practical application. The weighted transformed decision matrix is then constructed. In this

step, a set of weight coefficients w_{th} , w_f and w_d are added to the transformed decision matrix to build the weighted transformed decision matrix. The weighted average value will then combine all the related metric values together with the weighting factors for the users. In the last stage, the users are scheduled based on the descending order of the $P_{k,c,m}$ value.

$$P_{kcm} = w_{th} \times \frac{\eta_{CQI(k)}(t)}{\sum_{k=1}^i \eta_{CQI(k)}(t)} + w_f \times \frac{\frac{R_{kcm}(t)}{R_{kc}(t)}}{\sum_{k=1}^i \frac{R_{kcm}(t)}{R_{kc}(t)}} + w_d \times \frac{Hol_k(t)}{\sum_{k=1}^i Hol_k(t)} \quad (12)$$

where $w_{th} + w_f + w_d = 1$

w_{th} is the throughput weight.

w_f is the fairness weight.

w_d is the delay weight. m^{th} is PRB group of the c^{th} component carrier at time slot t .

4. Simulation Model

The implemented system-level simulation is based on the LTE-A standard specifications. The used simulator for LTE-A network is made up of one eNB and a set of 21 UEs, whereby each sector is assumed to serve 7 users. The UEs are distributed in the cell randomly. A simulation methodology has been developed in order to assess the performance of SRUS scheme in LTE-Advanced system with carrier aggregation. The downlink is based on OFDMA with CA

feature. In each CC, there are R resource blocks that have K subcarriers in frequency domain, and a frame in the time domain. To attain a high data rate for transmission, Adaptive Modulation and coding is very essential. UEs have the possibility of estimating the CQI of the downlink transmission as well as the feedback to eNB.

The Effective Signal to Interference plus Noise Ratio Mapping (EESM) model is used to merge the SINR on each subcarrier to the RBs' SINR. Two carrier components are considered, each of them with 20 MHz bandwidth and they have been configured to form a wide band of 40 MHz. The Proportional Fair (PF) scheduling algorithm with an average window length of $T = 1,000$ is considered in the simulation. It is assumed as in [6-7] that the power allocation is uniform. Other parameters of the simulation are stated in Table 1.

Table 1: LTE-A simulation system configurations

Parameter	Setting and Value
Carrier Frequency	1900 MHz
Transmission Bandwidth	20 MHz per Component carrier
Cell Layout	Hexagonal grid, 7 cell-site, 3 sectors per eNB per CC
Subframe (TTI) Length	1 ms
MIMO Configuration	2×2 MIMO with Rank Adaptation
CCs Scheduling Scheme	Best-CQI, EXP/PF, PF, SRUS
Pathloss Model	Hata Model

Shadow Fading Model	Longnormal Fading Model
Modulation and Coding Scheme	QPSK, 16QAM, 64QAM
Granularity of Scheduling	1 TTI
Traffic Types	Full Buffer (RT and NRT)

5. Experimental Results and Analysis

The proposed algorithm MC-SRUS in LTE-A downlink has been evaluated in this section; various traffic models and varying users were experimented. The maximization of throughput and high fairness, which would provide each user with a higher data rate was the basis for the allocation method of the novel MC-SRUS algorithm. MC-SRUS downlink scheduler is assessed against the PF-SRUS, EXP/PF-SRUS and Best-CQI-SRUS downlink schedulers in terms of fairness, throughput, delay, and BLER.

The comparison to the existing EXP/PF-SRUS algorithm for the bit rates achieved by the users to the system fairness index obtained from the user's average achieved bit rate is depicted in Figure 3. Thus, the level of performance provided to those who lack the best channel conditions, is a measure of the fairness index of a network. Hence, studied applications have to make scheduling decisions depending on the needs of their customers and priority of their needs. It is also necessary to satisfy the application's demands for delay and instant

data rate, which are the heavy weight coefficients. Thus, even with increasing users, better QoS is a guarantee for user packets. An equal and even distribution of the network resources over different applications has made it possible for the new algorithm to show an enhanced performance of 23% as compared to EXP/PF-SRUS algorithm.

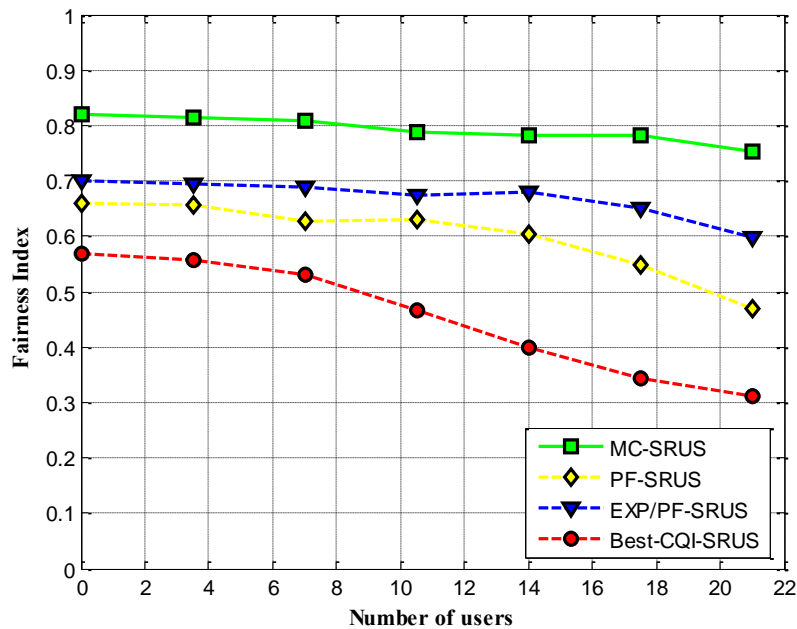


Figure 3: Average System Fairness Index

The system throughput versus the number of UEs in the cell is seen in Figure 4. As compared to the EXP/PF-SRUS, the MC-SRUS algorithm maintains a higher throughput by 9.2% when the number of users increases. It is clearly evident from the performance analysis of

the MC-SRUS algorithm, that the system is capable of serving up to 21 users in a concurrent manner. The factors responsible for the sturdiness and efficiency of the MC-SRUS algorithm are: Bandwidth estimation, Bandwidth allocation and the dynamic scheduling. When the number of users exceeds 21, the resources are distributed among the applications based on their allocation demands in terms of throughput, delay and spectral efficiency; this is applicable to bandwidth estimation and bandwidth allocation. Users are served, optimally, from different applications due to the proposed algorithm's capability.

The Best-CQI-SRUS algorithm gives the highest service priority to users with the best channel conditions as opposed to users with poor channel conditions. Therefore, its throughput of over 19 Mbps more than the MC-SRUS algorithm; but this throughput average is to the detriment of its cell-edge users who suffer repeated from prolonged delays and frequent packet drops. Thus, QoS from eNB is hardly guaranteed. While distributing the bandwidth between all users, the PF-SRUS system priorities its users based on their CQI; this results in the lowest performance among the algorithms.

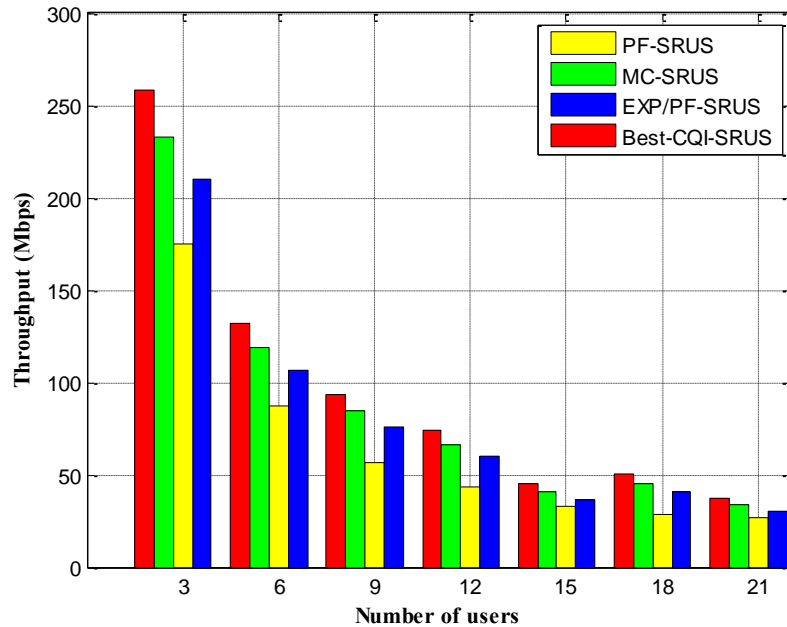


Figure 4: System Throughput

Since fewer resources are assigned to real time users' application, as compared to non-real time applications, a decrease in service quality occurs (most of the real time packets are exceeding the deadline budget). PF-SRUS algorithm exhibits a lower performance than the EXP/PF-SRUS algorithm since the latter distributes its resources equitably.

Figure 5. displays the overall system delays for studied scheduling algorithms. In comparison to EXP/PF-SRUS, the MC-SRUS algorithm displays the lowest delay by 1.2 ms. The users are served within the delay limits because the proposed algorithms consider the head of line delay (scheduling metric decision factor). Due to the

exponential delay growth having a high impact on the scheduling decision metric, PF-SRUS and Best-CQI-SRUS algorithms have a higher delay than the EXP/PF-SRUS algorithm.

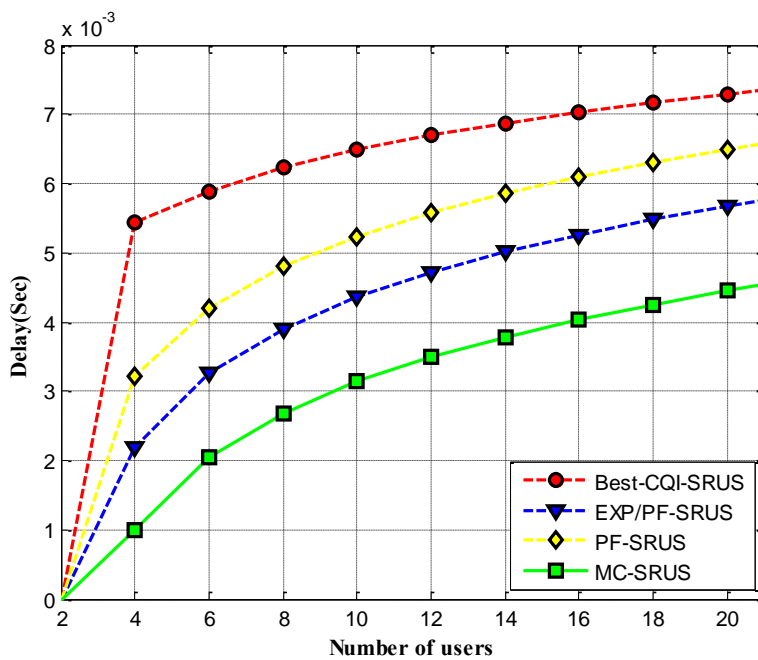


Figure 5: Delay for Over All System

Since PF-SRUS algorithm does not consider the delay metric as a scheduling decision parameter, its performance is moderate between the EXP/PF-SRUS and Best-CQI-SRUS algorithms. The policy of serving only the users with the highest CQI level has resulted in the Best-CQI-SRUS algorithm showing the worst performance as compared to other scheduling algorithms. Figure 6 depicts the overall system BLER vs SNR plot. Among all the scheduling algorithms compared, the MC-SRUS algorithm shows the lowest BLER as

compared to other scheduling algorithms. For the MC-SRUS algorithm, the desired average SNR received of $\text{BLER}^{10^{-2}}$, is less than the MC-SRUS algorithm by approximately 4.6 dB as compared to the EXP/PF-SRUS algorithm.

The proposed MC-SRUS enables the low Packet Drop Rate (PDR) till the users are serviced with its throughput level till the deadline threshold is reached. It is capable of providing priority in service those who are closer to the deadline threshold. This allows the MC-SRUS algorithm to maintain its low BLER rate and its sturdiness. In such prioritization, users who are still distant from the deadline threshold can be serviced later.

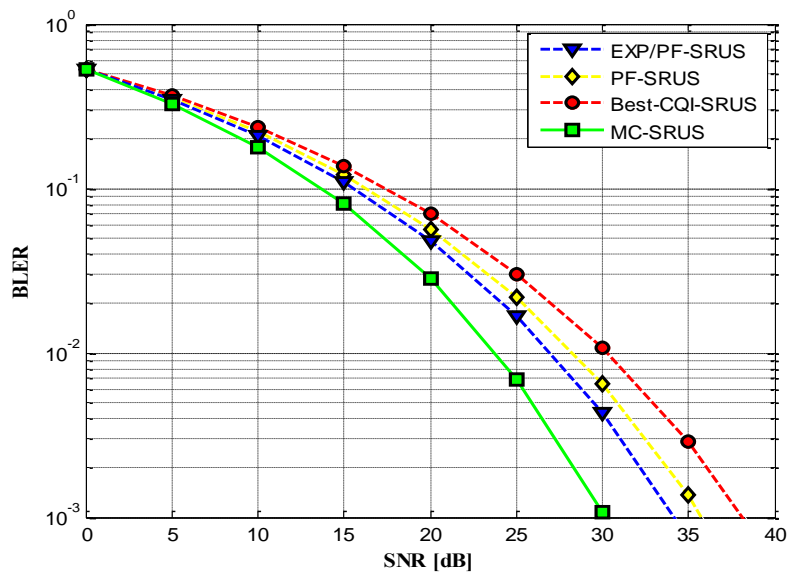


Figure 6: Overall System BLER vs. SNR

6. Conclusion


In this paper, the novel resource scheduling algorithm (MC-SRUS) has been recommended for LTE-A downlink, which offers a balance between the data rate and fairness index. This scheduler contains a simple methodology by influencing the AMC strategy closely after the allocation process of RBs. Moreover, the system level simulations illustrated that the MC-SRUS algorithm provides a tradeoff between the throughput and fairness when compared with the PF-SURS, EXP/PF-SURS and Best-CQI-SURS algorithms; it can be observed from the simulation results that the MC-SRUS algorithm achieved 23% enhancements in the fairness index as compared to EXP/PF-SRUS. The average received SNR at average BLER 10^{-2} for the MC-SRUS algorithm is less by approximately 4.6 dB as compared to the EXP/PF-SRUS algorithm. Moreover, the MC-SRUS algorithm showed the lowest delay by 1.2 ms as compared to the EXP/PF-SRUS algorithm. The MC-SRUS algorithm provides the highest throughput and fairness when compared with other scheduling algorithms and thus can be recommended for the allocation of radio resources in LTE-Advanced networks.

References

- [1] S. Kanchi, S. Sandilya, D. Bhosale, A. Pitkar & M. Gondhalekar, "Overview of LTE-A technology," *Global High Tech Congress on Electronics (GHTCE)*, 2013. pp. 195-200.
- [2] "Nokia. Carrier aggregation configurations and DL/UL linkage". 3GPP TDocs (written contributions) at Meeting, R1-59, Nov 11_13, 2009, Jeju Island, Republic of Korea.R1-094642,2009.
- [3] W. Fu, Q. Kong, Y. Zhang & X. Yan. A resource scheduling algorithm based on carrier weight in LTE-advanced system with carrier aggregation. *Wireless and optical communication conference (WOCC)*, 2013, pp. 1-5.
- [4] L. Zhang, K. Zheng, W. Wang & L, "Huang. Performance analysis on carrier scheduling schemes in the long-term evolution-advanced system with carrier aggregation," *IET communications*, 2011, pp. 612-619.
- [5] L. LIN, Y. LIU, L. Fang, X. Gang, K. LIU & X. GE, "Resource scheduling in downlink LTE-advanced system with carrier aggregation," *The Journal of China Universities of Posts and Telecommunications* 2012, pp. 44-123

- [6] Z. Shen, A. Papasakellariou, J. Montojo, D. Gerstenberger & F. Xu, "Overview of 3GPP LTE-advanced carrier aggregation for 4G wireless communications," *Communications Magazine, IEEE* 2012, pp. 122-130.

- [7] I. Gutiérrez, F. Bader & J. Pijoan, "Prioritization function for packet data scheduling in OFDMA systems," *Proceedings of the 4th Annual International Conference on Wireless Internet*. 2008, pp. 19.



**Advanced Self-Tuning Pole-Placement
Control: Computational Modeling and
Estimation Techniques for Optimizing
Antenna System Performance**

5

Advanced Self-Tuning Pole-Placement Control: Computational Modeling and Estimation Techniques for Optimizing Antenna System Performance

Hafed Efheij

College of Electronic Technology Tripoli, Libya

Hafedrs@gmail.com

Hasan Nuri Ali Naji

College of Electronic Technology Tripoli, Libya

hasan.naji2010@gmail.com

Adel Ghadedo

College of Electronic Technology Tripoli, Libya

Abstract

This Paper focuses on the development and analysis of a self-tuning Pole-Placement controller, utilizing a Discrete Transfer-Function, tailored for Single-Input Single-Output (SISO) Antenna systems. Self-tuning controllers represent an emerging and significant sector in control theory, with growing practical applications. This research hinges on the concept of self-tuning, which involves dynamically

adjusting controller parameters in response to the time-varying nature of the Antenna system's input/output characteristics. The core of this adaptive control approach involves the deployment of on-line estimators, specifically designed to track and adapt to the temporal variations in the system's parameters.

A key aspect of this research is the employment of the recursive least squares (RLS) technique, a prominent method for parameter estimation in such time-varying systems. The practical implementation of the proposed controller was carried out using MATLAB 15, incorporating the RLS estimator. The effectiveness of the developed controller was validated through extensive testing with a simulated Antenna model, yielding satisfactory performance results. Additionally, to enhance the usability and efficiency of the controller design, an interactive interface for tuning and evaluating the closed-loop performance was developed using MATLAB's Handle Graphics system. This Graphical User Interface (GUI) provides an intuitive and user-friendly means for users to interact with and adjust the controller settings.

Keywords: Recursive Least Squares (RLS), System Parameter Estimation, On-line Estimators, Kalman, Adaptive Control, Control System Simulation

1. INTRODUCTION

The utilization of sophisticated controller beyond the conventional Proportional-Integral-Derivative (PID) architecture in intricate control systems frequently offers notable benefits. Nevertheless, the complex calibration procedure for these advanced controllers presents notable difficulties due to the multitude of factors involved. The emergence of self-tuning controllers offers a solution to the difficulty associated with tuning. The pioneering study conducted by Åström and Wittenmark in 1973 presented a fundamental self-tuning controller specifically designed for minimizing variation in control issues, with the aim of reducing output variability. The controller was established based on the certainty-equivalence concept, utilizing recursive estimation to approximate the process and environmental models, and accepting these estimates as accurate representations of the actual models.

Although this basic self-tuning controller is effective in many situations, it is not suitable for all cases, especially in stochastic control problems where minimum variance control is not appropriate. This is particularly true for non-minimum phase plants or situations that require significant control signals for minimum variance. These scenarios can be restated as Linear-Quadratic-Gaussian (LQG) control issues. The LQG-based self-tuning controller, as described in Åström and Wittenmark (1974) and further refined in Åström et al. (1977), is more intricate than its predecessor since it includes steady-state Riccati equations or spectral factorization in each design phase. Clarke and Gawthrop (1975) introduced a simplified technique that utilizes a LQG approach with a one-step criterion. This algorithm greatly simplifies the procedure, although it does have certain limitations, as explained in Gawthrop (1977). [1] is to develop and simulate a discrete pole-placement controller and its transformation into a self-tuning controller, using discrete difference equations. The controller is responsible for managing the azimuth movement of the Antenna by making real-time adjustments to its settings through recursive methods. The primary aim is to evaluate and

contrast three different estimating methods - Recursive Least Squares (RLS), Extended RLS (ERLS), and Kalman Filter - in the context of the pole-placement approach. The project seeks to employ MATLAB software to simulate the design and visually demonstrate the results of the self-tuning controller.

2. ANTENNA MODELLING

It is desired to control the Azimuth of an Antenna designed to track the satellite in order to pick up signals from it as sketched in Figure (1). The Antenna and drive parts have a moment of inertia J' and damping Br arising to some extent from bearing and aerodynamic friction, but mostly from the back e (V) of the DC drive motor [3, 4, 5].

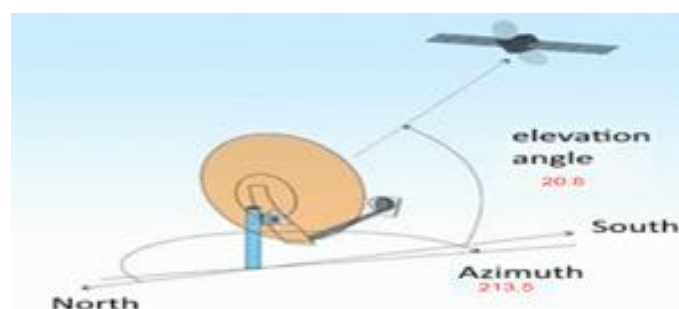


Figure 1: internal connection of DC-drive motor with the Antenna system. Here, the armature inductance L_a (Henry H) is negligible because it is usually small [6,7]

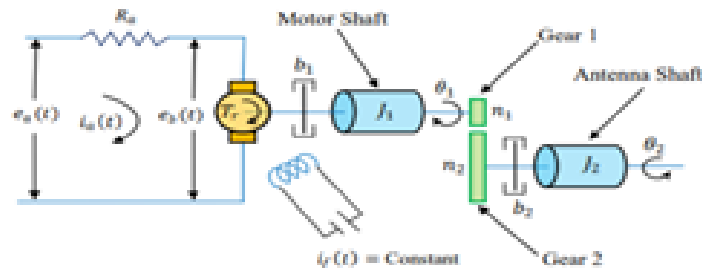


Figure 2: the Connection of DC-drive Motor with the Antenna System

The dynamic equation (1) reduced to:

$$\frac{1}{a} \ddot{\theta}_1(t) + \dot{\theta}_2(t) = u(t)$$

Where $\theta_2(t)$ rad is defined as the Antenna pointing angle, $\theta_1(t)$ rad is angular displacement of motor shaft. Where θ (rad) is the Antenna pointing angle, If we define: Transform previous equation to S-domain , yielding:

$$position(s) = \frac{a}{s(s+a)} U(s)$$

The $\theta(s)$ which is the angle of the system can be represented by a linear displacement position(s) when a worm gear is used.

The sampling system below takes a continuous time signal at its input and produces a continuous time signal at its output, so it has a transfer function $H(s)=Y(s)/X(s)$, However, in between, the signal is converted to a set of numbers, so there is a discrete time component to the system. The transfer function of the sampled system, depicted above, is ZOH transfer function $H(s)\equiv Y(s)/X(s)=(1-e^{-Ts})/ Ts$

$$ZOH = \frac{1-e^{-st}}{s} \quad .$$

By introducing (ZOH) to Antenna model yields the following

$$\mathbf{position}(s) = \frac{(1-e^{-st})}{s} \left(\frac{\mathbf{a}}{s(s + \mathbf{a})} \right) \mathbf{U}(s)$$

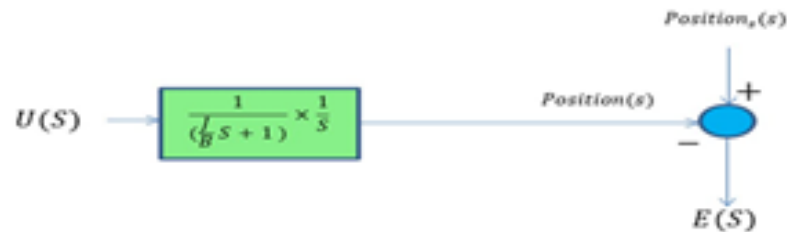


Figure 3: Model of Antenna Tracking Control

The aim of the design is to measure the error between the angle of the satellite position (m) and the Antenna and compute $U(s)$ so that the error $E(s)$ that is equal to $(\mathbf{Position}_s(s) - \mathbf{Position}(s))$ (*meter*), is always less than 0.001 meter during tracking.

In order to convert the transfer function of the system in the Z plan, the Z-transform is used. The derived antenna transfer function with ZOH is:

$$\frac{\mathbf{Position}(s)}{U(s)} = (1 - e^{-st}) \frac{a}{s^2(s+a)} = (1 - e^{-st}) \left[\frac{1}{s^2} - \frac{1}{a} \times \frac{1}{s} + \frac{1}{a} \times \frac{1}{(s+a)} \right] \quad (2.4)$$

The conversion of Eq. 4 into z plan is obtained as:

$$\frac{\mathbf{Position}(z)}{U(z)} = \frac{1}{a} \times \left[\frac{(1 - e^{-aTs} - aTs e^{-aTs}) + (-1 + aTs + e^{-aTs})z}{(z-1)(z - e^{-aTs})} \right]$$

The derived discrete Antenna model is transferred into difference equation in order to be programmed recursively using either MATLAB application or microcontroller unit for real time application. The transfer function of the system given in Eq. (5) can be simplified as follows:

$$\begin{aligned} \mathbf{Position}(z) - (1 + e^{-aTs}) \times z^{-1} \times \mathbf{Position}(z) + \\ e^{-aTs} \times z^{-2} \times \mathbf{Position}(z) = \frac{(1 - e^{-aTs} - a \times Ts \times e^{-aTs}) \times z^{-2}}{a} \times \\ U(z) + \frac{(-1 - a \times Ts + e^{-aTs}) \times z^{-1}}{a} \times U(z) \end{aligned}$$

Where:

$$\mathbf{Position}(k), z^{-1} \times \mathbf{Position}(z) = \mathbf{Position}(k - 1),$$

$$z^{-2} \times \mathbf{Position}(z) = \mathbf{Position}(k - 2).$$

$$U(z) = u(k), z^{-1} \times U(z) = u(k - 1), z^{-2} \times U(z) = u(k - 2)$$

Yields:

$$\begin{aligned} \mathbf{Position}(k) = (1 + e^{-aTs}) \times \mathbf{Position}(k - 1) - \\ e^{-aTs} \times \mathbf{Position}(k - 2) + \left(\frac{1 - e^{-aTs} - a \times Ts \times e^{-aTs}}{a} \right) \times \\ u(k - 2) + \frac{(-1 + a \times Ts + e^{-aTs})}{a} \times u(k - 1) \end{aligned}$$

The sampling time T_s is set to 1 second for simplification.

The final Antenna difference equation can be rewritten as:

$$\begin{aligned} \mathbf{Position}(k) &= 1.90483 \times \mathbf{Position}(k-1) - 0.9048 \times \\ &\mathbf{Position}(k-2) - 0.04674u(k-2) - 0.048374u(k-1) \end{aligned}$$

The above Antenna difference equation therefore can now be programmed recursively using MATLAB environment.

The code then is used for self-tuning control algorithm. The algorithm steps are shown in next sections simultaneously.

3. LEAST RLS, EX-RLS, AND KALMAN FILTER

METHODS

This paper presents a concise yet comprehensive examination of three predominant online estimation techniques for Antenna models: Recursive Least Squares (RLS), Extended Recursive Least Squares (EX-RLS), and the Kalman Filter (KF). These methods are pivotal in adaptive antenna systems for accurate parameter estimation in real-time.

- Recursive Least Squares (RLS): The RLS algorithm is grounded in iteratively minimizing the weighted sum of

squared differences between measured and predicted outputs. The update equation is given by:

- Extended Recursive Least Squares (EX-RLS): EX-RLS extends the RLS algorithm to nonlinear systems by incorporating an extended state vector. The update mechanism is similar to RLS, but with the inclusion of a Jacobian matrix $\backslash(J(t)\backslash)$ representing the partial derivatives of the output with respect to the parameters:
- Kalman Filter (KF): The KF is a recursive solution to the linear quadratic estimation problem. It updates estimates based on incoming measurements and a prediction model. The update equations are:

Each of these methodologies offers distinct advantages for real-time antenna model parameter estimation, with their applicability varying based on system dynamics and measurement characteristics.

To apply self-tuning discrete pole-placement controller for Antenna system presented this project, the transfer function of an Antenna plant model in discrete time system is needed as derived previous section and it is given by:

$$G(z) = \frac{0.048z + 0.0468}{z^2 - 1.905z + 0.9048}$$

In order to design a pole-placement control system, the transfer function is transformed into inverse Z-transform as follows:

$$G(z) = \frac{z^{-1}(0.048 + 0.0468z^{-1})}{1 - 1.905z^{-1} + 0.9048z^{-2}}$$

Referring to the prototype which is:

$$G(z^{-1}) = z^{-K} \frac{B(z^{-1})}{A(z^{-1})} \text{ gives: } K = 1, n_a = 2, \text{ and } n_b = 1$$

And it clear by comparing the prototype with equation (3.21) that:

$$A(z^{-1}) = 1 - 1.905 \times z^{-1} + 0.9048 \times z^{-2} = 1 + a_1 \times z^{-1} + a_2 \times z^{-2}$$

$$B(z^{-1}) = 0.048 + 0.0468 \times z^{-1} = b_0 + b_1 \times z^{-1}$$

4. SIMULATION AND RESULTS

- **Open-loop antenna response**

The unit step signal applied as input signal to the Antenna system and the Antenna system output will be seen by programming the Antenna's difference equation, which shows the relationship between output and input signals, as shown below:

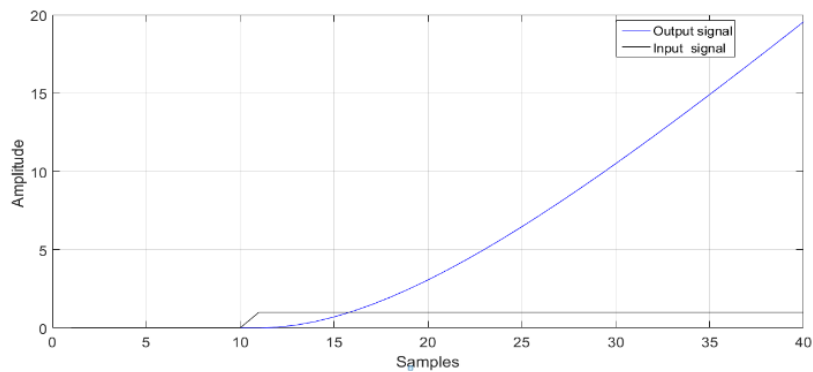


Figure 4: Response of the open loop Antenna system to unit step input

Referring to Figure 4, through the response of the system, the position of the Antenna is constantly increasing when the step function signal is applied, which mean that the Antenna system not reaching a stable state and this does not meet the design standard.

- **Closed-loop Antenna response**

The simulation of figure 5 shows the response of Antenna movement based on a unit step reference signal. The experiment samples value of the bookmark were determined with values ranging from 1 to and the values change oppositely from -1 to 1 every 5minutes, and the number of 800 seconds was recorded (13.33)(minutes) and to determine the system response specifications, the amount of natural frequency was entered with the value $\omega_n = 0.342$ rad/s as a constant value and the damping coefficient values were {0.7} as shown in the figure below:

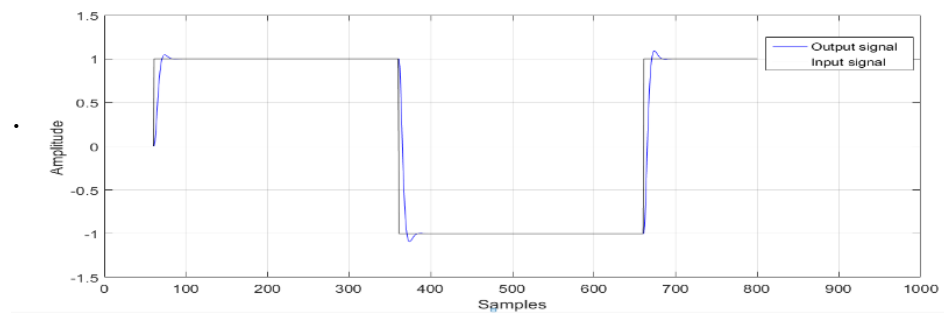


Figure 5: Response of the Antenna system

The controller output $u(k)$ signal known as control signal is shown in figure 6 below

:

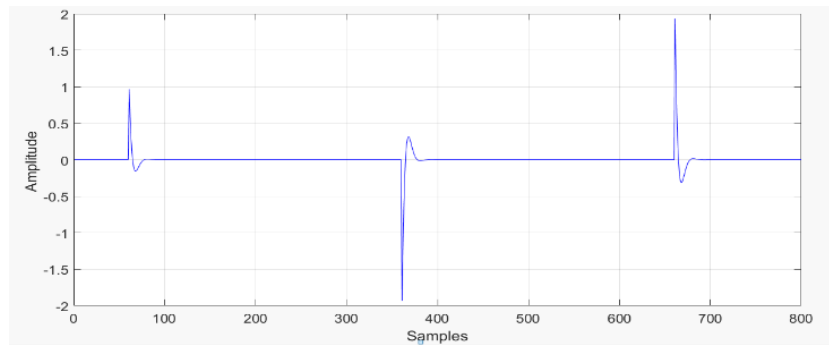


Figure 6: Control signal of the pole placement controller

Based on figure 6 the control signal able to force the output signal to match the desired reference signal.

- **Closed-loop Antenna response with changing one of parameters (without self- tuning)**

In this simulation, one of Antenna parameters was changing between samples (140—150) instances, which cause the change in output signal and the goal of simulation is to apply pole placement controller in order to see its ability to adjust Antenna position

The simulation shows the response of Antenna movement, Where the set point signal is unit step when change occurs

for plant parameters between samples (140—150) then causes the change in output signal to be unstable system

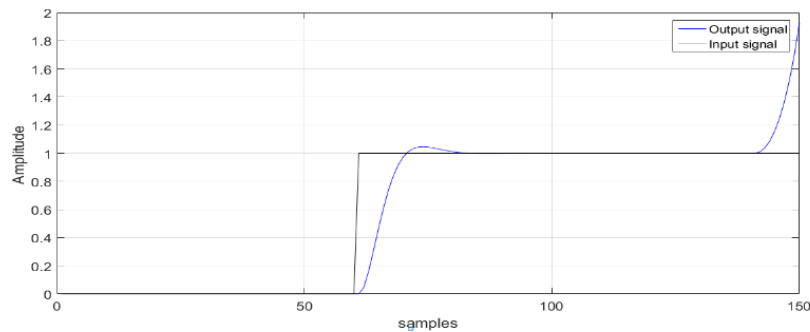


Figure 7: Response of the Antenna system (closed-loop)

Figure 7 shows that the controller was not able to adjust Antenna position, because of Antenna parameter change.

The controller output $u(k)$ signal known as control signal is shown in figure 8 below:

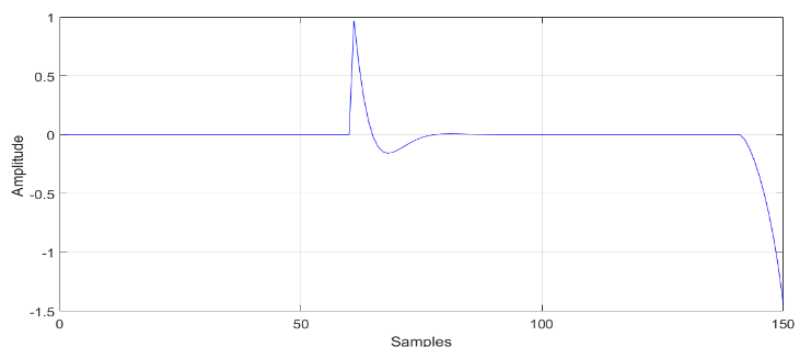


Figure 8: Control signal when change in one of parameters

Based on figure 8 the control signal is not able to force the output signal to match the desired reference signal because of the changing in plant parameters.

- **closed-loop system response with changing one of parameters (with self-tuning)**

In this simulation, one of Antenna parameters was changing between samples (140—150) instances, which cause the change in output signal and the goal of simulation is to apply pole placement (self-tuning) controller in order to see its ability to adjust Antenna position.

Simulation shows the response of Antenna movement. Where the set point signal is unit step when change occurs in plant parameters between samples (140-150) which cause no change in output signal, and the system is stilling stable.

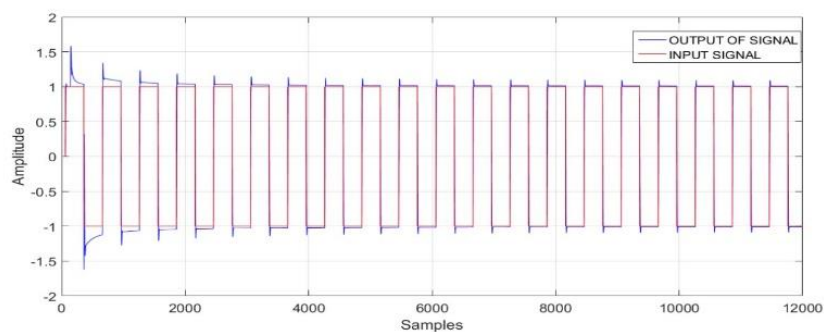


Figure 9: Response of the Antenna with change in parameter

using self-tuning. Figure 9 shows that the self-tuning pole placement controller able to adjust Antenna position, because the self-tuning technique observed the change in Antenna parameter.

The controller output $u(k)$ signal known as control signal is shown in figure 10 below:

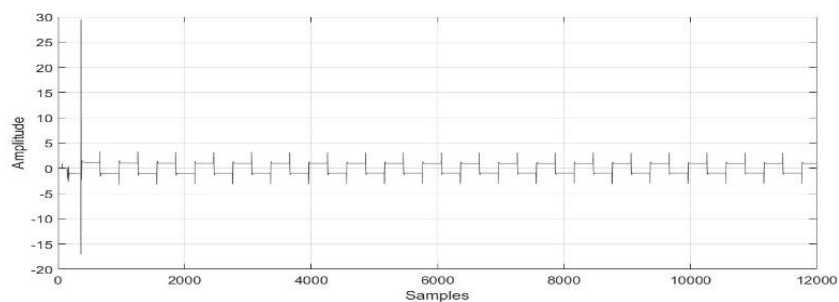


Figure 10: control signal of the pole placement (self-tuning) controller

Based on figure 10 the control signal able to force the output signal to match the desired reference signal when changing in plant parameters occurs.

Observe that when changing in one of parameters happening the control signal is trying to adjust the output based on the change in the parameter between samples (140-150).

Pole placement self-tuning trying to adjust estimated parameters as the actual Antenna parameters where is shown in figure 11 below:

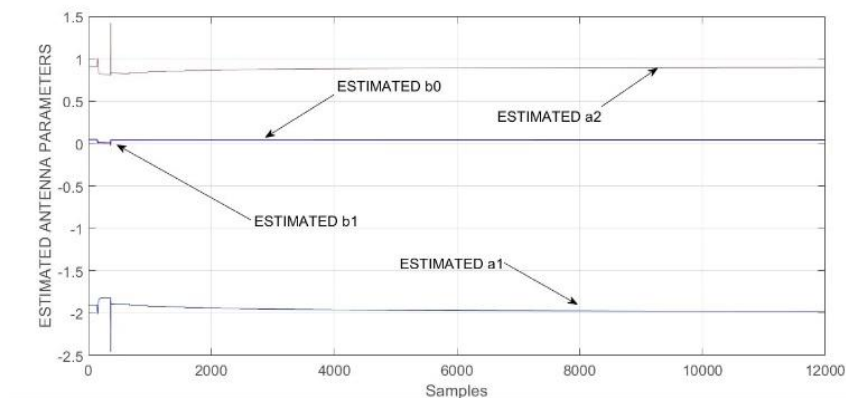


Figure 11: on-line estimated Antenna system parameters

In the above Figure 11, it was explained how to estimator the variables and through a figure shows how to RLS tries to adjust the variables to become ideal and in the best form, From the figure 11, observe that change in the plant parameters happening between samples (140-150) and the self-tuning technique trying to correct output as desired

- **Self-tuning pole-placement with Antenna black box**

The simulation of figure 12 shows the response of Antenna movement based on a unit step reference signal

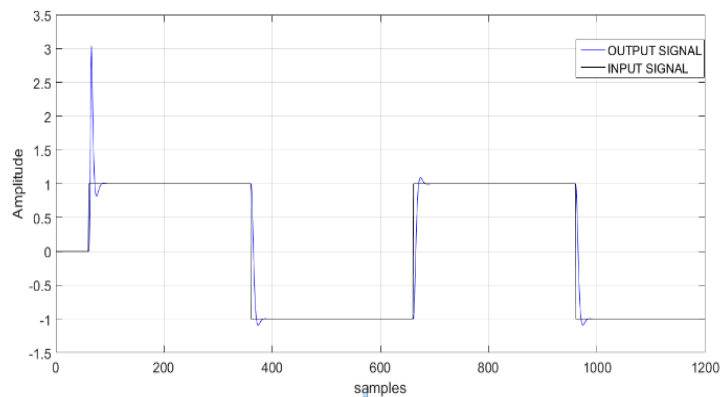


Figure 12: Response of the Antenna system (closed-loop) using self-tuning.

The above figure shows set point & output signal of the system, the difference between the set point and the output of the system was little, and the output of the system is stable, and the overshoot was high from above figure we notice that (Pole placement-self tuning) causes the above results (almost correct).

The controller output $u(k)$ signal known as control signal is shown in figure 13 below:

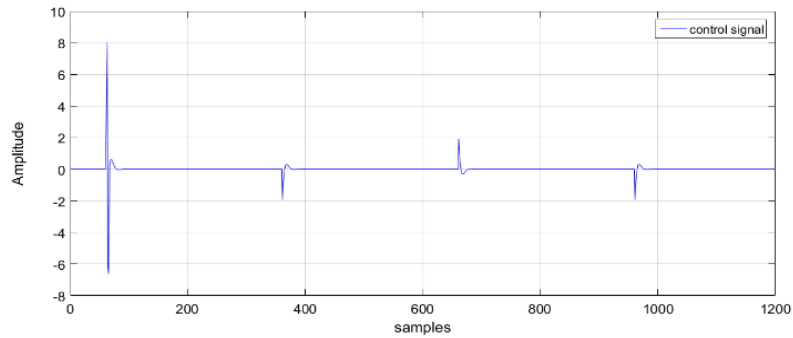


Figure 13: the control input of the Antenna system

The above figure shows how the control signal tracks the input signal and tries to adjust the output based on control signal.

Pole placement self-tuning trying to adjust estimated parameters as the actual Antenna parameters where is shown in figure 14 below:

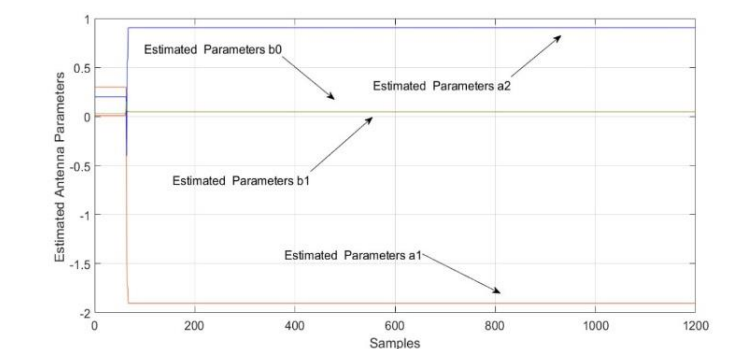


Figure 14: on-line estimated Antenna system parameters

In the above figure 14 it was explained how to estimator the variables and through a figure shows how to RLS tries to adjust the variables to become ideal and in the best form, From the figure 14 we can see that the error rate between Actual Antenna parameters & estimated Parameters using RLS is small, and thus we can say that it works correctly.

Table 1 estimation error of RLS pole placement control

Estimated Parameters using RLS	Actual Antenna parameters	Error	Percentage of error
$\widehat{a1}$ -1.9798	$a1$ - 1.9048	0.075	3.93%
$\widehat{a2}$ 0.8985	$a2$ 0.9048	0.0063	0.696%
$\widehat{b0}$ 0.0438	$b0$ 0.0484	0.0046	9.504%
$\widehat{b1}$ 0.0428	$b1$ 0.0468	0.004	8.547%

- **Comparison between (RLS & ERLS & KALMAN)**

Now it's to be talk about three recursive estimation techniques. They work independently without a control and compare which one is better in terms of adjusting estimated Antenna parameters according to system variables when the system input is a unit-step function.

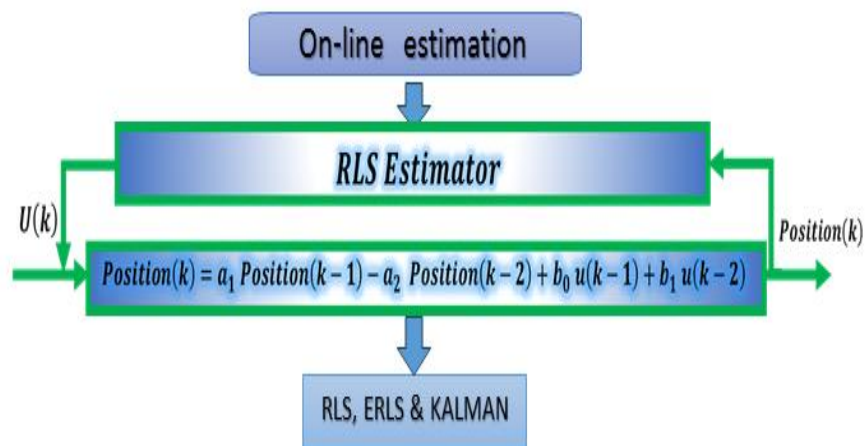


Figure 15: block diagram of RLS estimators

The input signal for three Techniques is showed below:

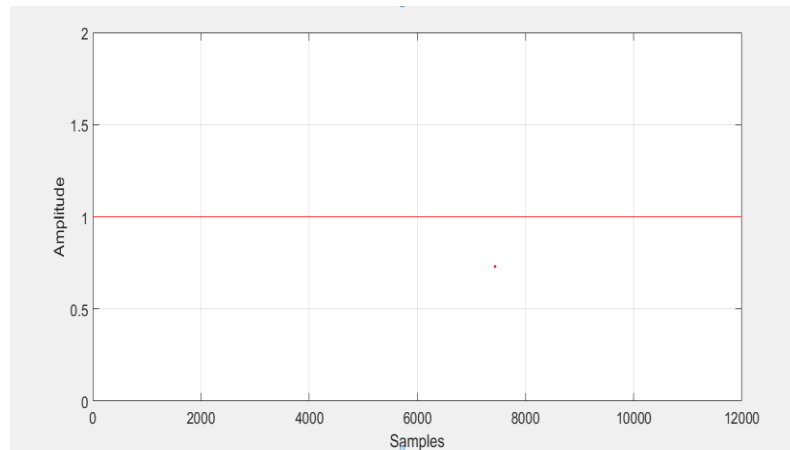


Figure 16: the input signal for comparison of the three systems

- **Recursive Least Square (RLS)**

Self-tuning technique trying to adjust estimated parameters as the actual Antenna parameters by using Recursive Least Square (RLS) as shown in figure 16 below:

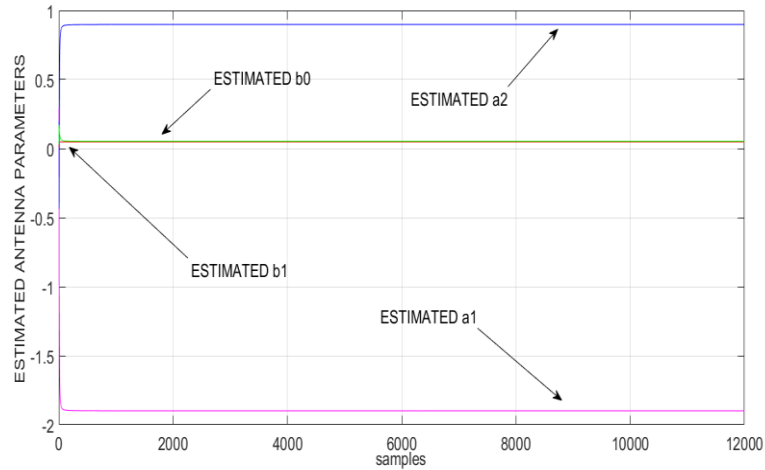


Figure 17: parameters estimated for an RLS estimator

In the above Figure 16 shows how the RLS tries to adjust the variables to become ideal and in the best form. From the figure, we can see that the error rate between Actual Antenna parameters & estimated Parameters using RLS is small, and thus we can say that it works correctly.

Now the purpose from this table is to compare between Actual Antenna parameters results & estimated Parameters using RLS results and shows error between them.

Table 2: Estimation error of RLS

Estimated Parameters using RLS		Actual Antenna parameters	Error	Percentage of error
$\widehat{a1}$	-1.8990	$a1$ 1.9048	- 0.0058	0.304 %
$\widehat{a2}$	0.8990	$a2$ 0.9048	0.0058	0.641%
$\widehat{b0}$	0.0482	$b0$ 0.0484	0.0002	0.413%
$\widehat{b1}$	0.0527	$b1$ 0.0468	0.0059	12.606%

We note that the error rate between the Actual Antenna parameters & estimated Parameters using RLS contains a rather large error rate in the variable $\widehat{b1}$

- **Extended Recursive Least square (ERLS)**

Extended Recursive Least Square (ERLS) is a type of adaptive control that can adjust their parameters

automatically to compensate for changing process condition, as shown in figure 18 below:

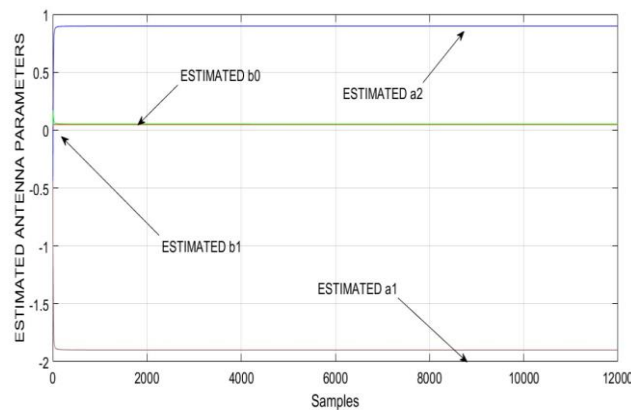


Figure 18: Parameters estimated for an ERLS estimator

In the above figure 18 shows how, ERLS tries to tune the estimators' parameters as real Antenna parameters, From the above figure, we can see that the error rate between real Antenna parameters & estimated Parameters using ERLS is smaller than RLS, and thus we can say that it works correctly.

Now the purpose from this table is to compare between Actual Antenna parameters results & estimated Parameters using ERLS results and shows error between them

estimated Parameters using ERLS		Actual Antenna parameters		error	Percentage of error
$\widehat{a1}$	-1.8999	$a1$	-1.9048	0.0049	0.257%
$\widehat{a2}$	0.8999	$a2$	0.9048	0.0049	0.541%
$\widehat{b0}$	0.0482	$b0$	0.0484	0.0002	0.413%
$\widehat{b1}$	0.0519	$b1$	0.0468	0.0051	10.89%

We note that the error rate between Actual Antenna parameters and estimated Parameters using ERLS contains a rather large error rate in the variable

- **KALMAN Estimator**

Using KALMAN to adjust estimated parameters as the real Antenna parameters as shown in figure 19 below:

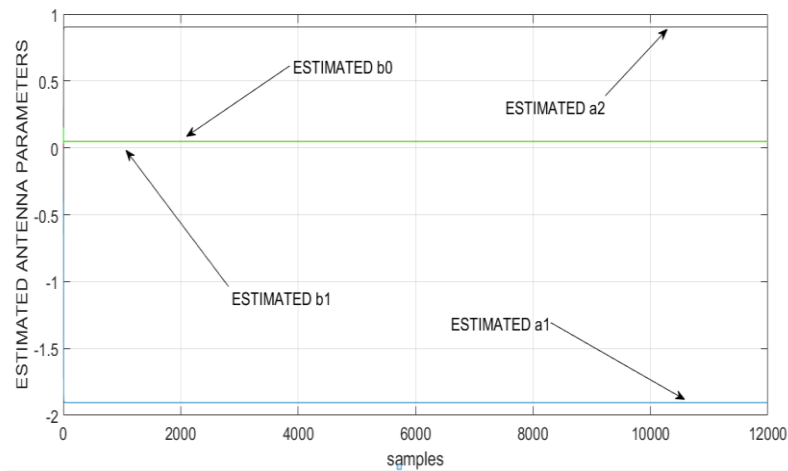


Figure 19: shows parameters estimated for a KALMAN estimator

In the above Figure 19 shows how to RLS tries to adjust the variables to become ideal and in the best form, From the figure, we can see that the error rate between Actual Antenna parameters & estimated Parameters using KALMAN is smaller than ERLS, and thus we can say that it works correctly.

Now the purpose from this table is to compare between Actual Antenna parameters results & estimated Parameters using KALMAN results and shows error between them.

Table 4: estimation error of KALMAN

estimated Parameters using (KALMAN)		Actual Antenna parameters		error	Percentage of error
$\widehat{a1}$	-1.9048	$a1$	-1.9048	0	0%
$\widehat{a2}$	0.9048	$a2$	0.9048	0	0%
$\widehat{b0}$	0.0484	$b0$	0.0484	0	0%
$\widehat{b1}$	0.0468	$b1$	0.0468	0	0%
estimated Parameters using (KALMAN)		Actual Antenna parameters		error	Percentage of error
$\widehat{a1}$	-1.9048	$a1$	-1.9048	0	0%
$\widehat{a2}$	0.9048	$a2$	0.9048	0	0%
$\widehat{b0}$	0.0484	$b0$	0.0484	0	0%
$\widehat{b1}$	0.0468	$b1$	0.0468	0	0%

Through the last table and the last figure, we notice that the best way to modify estimator parameters according to the system is (KALMAN ESTIMATOR) method.

5. CONCLUSION

This work focused on developing and simulating a Self-Tuning Pole Placement method for a Single-Input Single-Output (SISO) Antenna system. The technique utilized a particularly designed Discrete transfer function to achieve the main objective. The effectiveness of this strategy is clearly displayed in the results section, where the Self-Tuning Pole Placement method showcased its capacity to adjust to changes in Antenna characteristics, mostly caused by fluctuating weather conditions. The change successfully preserved the Antenna's response parameters and stability. The simulation research, specifically examining the Antenna case study in the time domain, demonstrated a notable improvement in both system performance and resilience against stability issues.

Additional findings from the experiment indicate that, out of the investigated estimators - Recursive Least Squares (RLS), Extended RLS (ERLS), and the Kalman estimator - the Kalman estimator proved to be the most efficient. The MATLAB platform, featuring an RLS estimator, played a

crucial role in enabling these sophisticated computational operations.

This research presents a significant advancement in antenna system optimization through the development of an advanced self-tuning pole-placement control system. Utilizing innovative computational modeling and estimation techniques, notably recursive least squares, this approach enhances the adaptability and performance efficiency of single-input single-output antenna systems. This work not only demonstrates practical improvements in antenna control mechanisms but also opens new avenues for future exploration in adaptive control systems, potentially influencing a wide range of applications in communication technologies. This research contributes to the ongoing evolution of antenna system performance, underscoring the importance of continuous innovation in control system design within the field of telecommunications.

REFERENCES

- [1] "Self-Tuning Controllers Based on Pole Placement Design." Accessed January 5, 2023. [Online]. Available: <https://portal.research.lu.se/en/publications/self-tuning-controllers-based-on-pole-placement-design>
- [2] "Antenna (Electronics)." Encyclopædia Britannica. Accessed May 5, 2023. [Online]. Available: <https://www.britannica.com/technology/antenna-electronics>
- [3]. Franklin, Gene F., J. David Powell, and Michael L. Workman. Digital Control of Dynamic Systems, 3rd ed. Addison-Wesley, 1998.
- [4] Nise, Normas S. Control System Engineering, 4th ed. John Wiley & Sons, 2004.
- [5] Ogata, Katsuhiko. System Dynamics, 2nd ed. Prentice Hall, 1992.
- [6] Chalam, V. V. Adaptive Control System Techniques and Application. Marcel Dekker, 1987.
- [7] Wellstead, P. E., and M. B. Zarrop. Self-Tuning Systems: Control and Signal Processing. John Wiley & Sons, 1991.
- [8] Bennett, S., and G. S. Virk. Computer Control of Real-time Processes. Peter Peregrinus Ltd, 1990.
- [9] Paraskevopoulos, P. N. Modern Control Engineering. CRC Press Taylor & Francis Group, 2002.
- [10] Wellstead, P.E., and M.B. Zarrop. Self-Tuning Systems: Control and Signal Processing. John Wiley & Sons, 1991.
- [11] Bobal, V., J. Bohm, and J. Fessl. Digital Self-Tuning Controllers: Algorithms, Implementation, and Application. Springer, 2005.
- [12] Z. Gao, "Scaling and bandwidth-parameterization based controller tuning," in Proceedings of the American control conference}, 2006

- [13] A. Karl and B. Wittenmark, Adaptive Control, Courier Corporation, 2013
- [14] Zhongshan Wu, 2001, 'Simulation Study And Instability Of Adaptive Control', MSc., The Department of Electrical and Computer Engineering, Louisiana State University, Louisiana, USA

Towards a Safer Smart Home: Risks and Recommendations

Towards a Safer Smart Home: Risks and Recommendations

Ftayem M. Binglew

Research Affairs Department

The Libyan Center for Electronic Systems, Programming and
Aviation Research Tripoli, Libya

f.binglew@apc.ly

Abstract

The Internet of Things (IoT) is a technology that connects devices used in daily life and enables them to provide a large number of services at anytime and anywhere to anyone or anything without significant human intervention. The smart home provides a more comfortable and productive life for the household. Home appliances collaborate to fulfill the residents' requirements, which range from completing daily tasks to monitoring, and providing security. However, as a result of their increasing prevalence and handling of residents' personal information, smart home appliances are prone to becoming the target of cyber-attacks aimed at violating privacy, theft, or sabotage. In this context, finding solutions and ways to make these useful applications safer for their users is important. This paper aims to investigate smart home security in terms of potential vulnerabilities and security attacks. Additionally, it aims to provide recommendations

and tips to smart home stakeholders to protect the applications and make them safer. The results obtained here would benefit smart home owners, device manufacturers, and Internet service providers.

Keywords: Internet of Things (IoT), smart home, security, counter-measures.

1. Introduction

With the emergence of smart devices that can communicate with their surroundings and provide services, people started to believe that they could use these devices to make their lives more comfortable and efficient. This idea gave birth to what is known as the Internet of Things (IoT) technology. The goal of IoT is to transform the way people live today by making things such as cars, microwaves, and refrigerators do their operations by themselves. That is, IoT aims to create a more connected world in which objects and devices around people know what people like, what they want, and what they need, and hence, act accordingly without explicit instructions [1],[2]. Useful IoT applications can emerge in people's live when things are able to understand their needs and are able to communicate with each other. IoT is also used to monitor and report environmental changes, prevent fires, and many other useful functions [3], which could potentially optimize the use of resources, increase the quality of services, and decrease the operational costs of services.

Smart homes are among the most popular IoT applications. Quite often, they are automated systems equipped with a set of interconnected components to serve the residents [4]. A smart home includes a variety of devices having different types of sensors that detect, for instance, temperature, light, and motion. It also includes devices such as smart TVs, door locks, home appliances, cameras, and microphones; hence, the smart home offers many applications that enable its residents to live comfortably and efficiently.

The features a smart home offers have made it a popular application in recent years, and its use continues to spread. This proliferation has made it the target of numerous attacks and security threats, increasing consumers' concern about their privacy and the valuable information or data found in their smart homes. These attacks target multiple smart devices in homes to grab homeowners' information such as credit card numbers and smart lock codes. Some attackers also manage to monitor homeowners by hacking surveillance cameras and headphones. The nature of the devices in a smart home application (hereafter referred to as “app”) facilitates a hacker’s job because devices do not have sufficient resources to enable them to protect themselves from penetration. Moreover, they have not been originally designed to communicate with others, and their manufacturers have not been obligated to pay due attention to securing them. All these make such devices vulnerable to security threats as attackers exploit them to infiltrate the smart home [5],[6],[7].

In [8] and [9] the authors underline the security in IoT applications and claim that traditional security methods are open to discussion in protecting IoT at home. The present work takes the scope more specific in itemizing potential vulnerabilities hence attacks. Additionally, it provides a broad base for further guidance to smart home owners, manufacturers, and finally Internet Service Providers (ISP).

This study aims to highlight the vulnerabilities that a smart home system may have and attacks that exploit those vulnerabilities. In addition, it aims to offer guidelines as to how to make a smart home safer to its stakeholders, including manufacturers, consumers, and ISP. In this scope, the contributions of the study can be summarized as follows:

- Security related to IoT, which is a rather new and developing technology, is a hot topic requiring further studies. Especially, there are very limited studies focusing on smart home security issues. Therefore, this study may contribute to the domain by providing comprehensive information about attacks targeting smart home applications and countermeasures to be used against those attacks. We believe that a study focusing specifically on smart home security will be more beneficial for smart home stakeholders, compared to the ones explaining security in general IoT, because the smart home has its

characteristics such as including heterogeneous products from different producers [10].

- The smart home is a new application that can be used by anyone, even by those who are not aware of the risks they can face in the future. This and similar studies may contribute to increasing awareness of the people and reducing risks that they may be exposed to.

- By offering recommendations to owners, device manufacturers, and ISPs, to the best of our knowledge, the present work is the only study providing security tips considering different smart home stakeholders. Therefore, it could help them to develop, install and maintain safer applications in the future.

The rest of the paper is organized as follows: Section 2 provides a literature survey about the discussed topic. The security issues that the smart home suffers from are presented in Section 3, which also includes the factors that make the smart home vulnerable to attacks in addition to the objectives and consequences of these attacks. Some recommendations and advice that can be considered to protect the smart home are discussed in Section 4 based on the responsibilities of different smart home stakeholders, namely manufacturers, owners, and ISPs. Finally, Section 5 concludes the paper.

2. Related Work

A smart home is a residence equipped with different types of smart technologies providing various tailored services to home residents to make their life easier and more comfortable. Despite its many advantages, several barriers are preventing its adoption and proliferation. In this scope, security and privacy together are considered as one of these barriers in many studies [4],[11],[12],[13],[14]. Therefore, smart home security is a hot topic requiring further studies to develop more applicable solutions and to raise awareness among all stakeholders.

Risk analysis for a smart home automation system is provided by [11], in which a total of 32 smart home-related risks are identified and classified as high (4 risks), moderate (19 risks), and low (9 risks). High risks are related to software components and human behavior. The authors concluded that security and privacy should be integrated into the design phase of smart home development. Almusaylim and Zaman in [14] reviewed the existing literature to analyze smart home challenges, suggest possible solutions for them, and illustrate the open issues that still need to be addressed. In the study, security, and privacy are considered two of those challenges. Similarly, [15] provides a literature survey taxonomizing smart home-related works into four categories, namely, reviews or surveys, research studies on apps, development attempts, and broad design proposals. The study considers security and privacy as one of the challenges related to smart homes and summarizes several studies discussing the subject.

[16] introduces a smart home threat model and analyze it in a test bed architecture considering off-the-shelf components. Their analysis results demonstrate that the existing smart home IoT infrastructure could be vulnerable to eavesdropping, impersonation, Denial of Service (DoS), and software exploitation attack vectors under specific conditions; for example, an attacker that manages to get access to an underlying network. Davis et al. provide a review of known vulnerability studies of smart home devices and a process of conducting vulnerability analysis in IoT devices [17]. They also analyze security postures of lesser-known vendors, and well-known vendors and conclude that well-known vendors/devices have stronger security postures, whereas lesser-known manufacturers/devices have a weaker security posture. All these studies clearly show that smart home devices are vulnerable to different types of attacks that may cause unpredictable and annoying consequences; hence, they expose the need to understand the importance of security.

In a more focused work, Batalla et al. present the current approaches to security in smart homes, including standards and outstanding mechanisms [18]. They describe smart home security issues by grouping them into 6 different requirements (confidentiality/privacy, integrity, authentication, authorization, non-repudiation, and availability). They look at security from a practical point of view and describe good practices for ensuring security goals within heterogeneous smart home systems. They conclude that the smart home is vulnerable in several aspects and that a secure management

system should be integrated into smart homes. Therefore, it is necessary to introduce external actors capable of managing the system and, for this, the network operators are the best positioned to give management support to smart homes. [4] and [7] discuss smart home security threats based on confidentiality, authentication, and access, and provide information about security supports of three IoT protocols, namely, 6LoWPAN, RPL, and CoAP. A smart home gateway architecture supported by web services for automatic device and network configuration and automatic system updates is proposed for solving security-related problems. In [6] a review study, discuss different issues such as how IoT is growing, objects and their specifications, the layered structure of the IoT environment, and various security challenges for each layer that occur in the smart home. In addition, they present some solutions that would help to overcome these security challenges. From this group of studies, it is seen that there are efforts to determine the security requirements of the smart home and to produce solutions for those requirements.

There are also some studies proposing solutions to specific issues related to smart homes. Most of them concentrate on network security with some works considering applications as well. In this scope, Kang et al. propose a security framework that uses self-signing technology to defend against other infiltrating codes and executable programs, and to block execution flow [19]. The authors claim that the proposed framework provides a security service for ensuring device

authentication, integrity, and availability. Chifor et al. propose a lightweight authorization stack for smart home IoT applications, where a Cloud-connected device relays input commands to a user's smart-phone for authorization [10]. A proof-of-concept solution which uses the Fast IDentity Online (FIDO) protocol is presented. The authors have shown that the delay caused by the FIDO protocol has low impact for a smart home application. In another study, a three-layer intrusion detection system is proposed for smart home IoT devices [20]. The three main functions of the proposed systems are type classification of the IoT devices, detection of wireless attacks against IoT devices, and classification of the attack types. The performance of the system for the given main functions are 96.2%, 90.0% and 98%, respectively. Poh and Gope propose a privacy-preserving scheme, PrivHome, which supports authentication, secure data storage and query for smart home systems [21]. PrivHome provides data confidentiality as well as entity and data authentication to prevent an outsider from learning or modifying the data communicated between the devices, service provider, gateway, and the user. It further provides privacy-preserving queries in such a way that the service provider and the gateway do not learn the content of the data. Meng et al. survey the emerging security and privacy challenges for the IoT in smart homes, and discuss the existing proposed counter-measures [22]. To prevent the attacks on the voice user interface of smart homes, they propose a novel wireless-signal-based liveness detection framework, named WiVo, which utilizes the

prevalent wireless signals in IoT environments to sense human mouth motion, and then verifies the liveness of voice commands according to the consistency between voice samples and channel state information data.

As given above, there are different studies discussing smart home security issues and protection mechanisms that can be used to defend smart home systems. These studies can be considered as a clear indication for the requirement of focusing on smart home security. Another point is that there are various studies discussing smart home security issues and solution proposals similar to the present study. The main novelty of the present study is the exploration of security measures from different stakeholder perspectives (manufacturers, consumers/owners, ISPs). We believe that it will provide a different view of smart home security and help stakeholders to understand their responsibilities.

3. Smart Home Security Issues

Day after day, the smart home has become a common requirement for many because of the services and features it provides. However, an important question comes to mind: Is a smart home safe for its users? The security of smart homes has always been - and, probably, will remain - a concern for consumers [23]. Smart home security is correlated in some way with people's privacy, routines, activities, contacts, data, images, and locations.

The security of every technology used in a smart home is linked to its application including wireless communications, networks, software, hardware, operating systems, protocols, and Cloud services [24].

The attackers use devices in the smart home such as surveillance cameras and microphones to spy on its residents [25],[26]. Unfortunately, many of these devices — from door lock to alarm systems — not protected enough against hacking. People can set their smart alarms to get to work on time, or send an order to a coffee maker for fresh coffee; however, cyber-criminals can use these devices to obtain valuable personal data about family habits.

A smart home is susceptible to various types of attacks such as eavesdropping, jamming, tampering, malicious code injection, replay, DoS, Man-In-The-Middle (MITM), wormhole, sybil and many others. These attacks may be sometimes very dangerous and even cause loss of life and property. This may occur, for instance, if an attacker tampers with alarms, locks, or fire detection systems [27],[28]. The targets of attacks on smart homes are concentrated in [29]:

- Harm that can cause damage in life, property or both
- Monitoring and leaking personal information
- Denial of service
- Counterfeiting of data exchanged between devices or stored in them

The top five smart devices that had an impact on cyber-security in 2019 were voice-activated assistants, linked automobiles, connected baby monitors, smart TVs, and cell phones, according to [30]. Several of these devices can also be used in smart homes. Table 1 shows a few popular and weak smart home appliances, their normal functions and how they can be used by attackers [31],[32],[33],[34],[35],[36].

Table 1. Hackable devices, their normal functions, and the targets of the attacks

Devices	Normal Function Samples	Attack Target Samples
Smart Lock	<ul style="list-style-type: none"> • lock and unlock doors, windows, and garages without a physical key • register permanent and temporary users who are entitled to enter the home and, sometimes, define their access schedules represented in days and times • raise the alarm in case of any break-in to warn residents • lock automatically after 	<ul style="list-style-type: none"> • open the door for strangers to enter the house • control the lock and deny home residents entry or exit • change the lock password remotely • disturb the residents by activating the intrusion alarm unnecessarily

	unlocking for a specified period of time. This happens in cases where residents forget to lock the house.	
Smart Refrigerator	<ul style="list-style-type: none"> • send an order to the online grocery store when there is a shortage of items in the refrigerator • record the expiration dates for the items in the refrigerator and alert residents upon expiry • prepare and send grocery lists to mobile devices for resident (such as smartphones or tablets) while they are near a grocery center. 	<ul style="list-style-type: none"> • order a large amount of groceries online beyond the needs of home residents • perish food in the refrigerator by manipulating the temperature gauge • manipulate the expiry dates to always indicate that food in the refrigerator is fresh, or deactivate expiry alarms entirely
Smart Coffee Maker	<ul style="list-style-type: none"> • prepare coffee using the timer or make an order remotely 	<ul style="list-style-type: none"> • stop the coffee preparation process completely

	<ul style="list-style-type: none">• allow residents to participate in the preparation of high-quality coffee by giving them the option to add a component or cancel a component as they like	<ul style="list-style-type: none">• make coffee without ordering at any time throughout the day• manipulate the coffee ingredients either by adding too much sugar or milk, or not at all• program the coffee machine to work non-stop even if it does not contain coffee beans
Smart Game	<ul style="list-style-type: none">• interact with its players in an educational way• own a feature that enables it to receive game-controlled orders from parents remotely• provide remote video and audio access for parents	<ul style="list-style-type: none">• record game players' voices and conversations with each other and leak these recordings online• contact game players unnecessarily and disturb them• scare game players by controlling or cancelling the game, or by raising the volume to make it noisy

		<ul style="list-style-type: none"> • hack the smart home network through the smart game to carry out other attacks or to learn about the location of the house
Smart Bulb	<ul style="list-style-type: none"> • enable control by mobile apps or websites • control brightness according to the available daylight • turn on or off as scheduled or according to the presence of the residents in the room 	<ul style="list-style-type: none"> • turn the light on or off at inappropriate times • turn on all lights in the house to overload the power system, increase energy consumption, and raise bills • turn the lights on and off repeatedly until the lamps are damaged
Smart Watch	<ul style="list-style-type: none"> • monitor the user's heart rate and provide a fitness tracker • track user activities • send reminders and alerts of an unexpected thing • allow users to answer 	<ul style="list-style-type: none"> • infiltrate the user's smart phone from the smart watch • steal user-related health data • send fake text messages from the smart watch as if they

	messages and receive calls from an associated mobile phone	were issued by the legitimate user
Baby Monitors	<ul style="list-style-type: none"> • monitor the baby at home 	<ul style="list-style-type: none"> • disturb family members • give wrong information about the baby
Home Gateway	<ul style="list-style-type: none"> • connect the smart home to the Internet • connect devices through Wi-Fi or other wireless protocols • provide gateway functions like WAN to-LAN bridging, Network Address Translation (NAT), IP Forwarding 	<ul style="list-style-type: none"> • connect to a fake or malicious URL to download malware • steal credentials or personally identifiable information (PII) through the gateway • block or modify connections to redirect them toward hidden malicious paths

4. Protecting Smart Homes

Despite many desirable features that a smart home offers, security risks and breaches of privacy have been, and still are, an important problem in a smart home application. Homeowners should take care to protect their smart home systems as much as they do protecting their

homes physically by purchasing locks and setting alarms. The fact that there have been more attacks on smart homes in the last few years has made this significant. For example, parents are interested in protecting their children from stairs and sharps. However, when they buy Internet-capable toys for their children, they don't think about the same thing or wonder whether these devices can be hacked or not.

Protecting a smart home requires the concerted efforts of a number of parties, namely owners, manufacturers and service providers. The next subsections contain recommendations on the role of the manufacturer, owners and ISP to make the smart home safer.

4.1 The Manufacturer Role

In the race of competing companies to produce smart devices at the cheapest prices and as soon as possible, they did not focus heavily on the issue of security of these device [37],[38]. As a result, multiple governments are putting additional pressure on makers of smart devices to improve the security of their goods. The growing demand for smart devices has also created another pressure point. To stay in the race to compete, companies must produce devices that have strong security measures to protect their users. There are some measures and procedures that might help manufacturers make their smart products safer. The following points are some of the recommendations and tips suggested by this paper that smart device developers can take into account when designing and producing their products for consumers.

Include security experts in manufacturing teams: The design and manufacture of any smart device with a high level of security requires the presence of information security engineers within the design and manufacturing team. These engineers' primary focus is on smart device security from the time of design to the point of production.

Information security engineers must take care of a number of factors in order to achieve this including:

- Users of smart devices and the purpose of their use of them.
- The type of data the smart device will handle and the environment it will operate in
- Potential security flaws in IoT devices that hackers might exploit, as well as the kind of security measures needed in the device to guard against this

These factors help determine the type of attacks that devices may be exposed to. As a result, the countermeasures of protection and prevention of these attacks are developed [11]. These measures are defined as security capabilities, features, or functions that devices provide through their own technical means [38].

Consider the security requirements: The IoT device designed and developed must have the ability to achieve important and basic security requirements such as secure authentication, authorization, confidentiality, secure communication and physical protection

[19][40],[41],[42]. The most important security requirements are as follows:

- **Authentication:** One important security requirement is user identity verification; for instance, two-way authentication can be implemented in IoT devices [27],[43],[44].
- **Confidentiality:** Protecting information stored in smart devices and sent between them is an urgent security requirement. The providing of technology to encrypt data during the design of smart devices contributes to meeting this requirement.
- **Secure Communication:** It would be a good idea for smart devices to use secure communication protocols such as IPsec, SSL, and HTTPS.
- **Physical Protection:** Several smart devices require their work to be placed in unprotected places, so it is important to be made of materials resistant to penetration and weather factors [27].

Certain company, like Develco Products, have started to develop smart devices that take these requirements into account [45]. These devices, for example, use installation codes, certificates and pre-defined keys to authenticate the connection when they attempt to join a network.

Produce devices compliant with current standards: Some governments have set standards for the minimum level of security that smart devices should have due to the risk of information leakage at the

level of individuals and organizations. To achieve the necessary level of security, some documents have been published containing guidelines that must be followed during the development and production of smart devices. Among these documents are ETSI TS 106445 V1.1.1 (2019-02), CYBER: Cyber Security for the Internet of Things for Consumers, and GDPR: General Data Protection Regulation. خطأ! لم يتم العثور على مصدر المرجع. [46],[47].

Add new security features: One of the most important services that smart device manufacturers can offer is to include security-supporting features and applications in these devices, provided that this service is updatable.

Establish distinct passwords: For all devices of the same type and version, manufactures typically use the same default password, which is placed in the device's operating manual. If the consumer does not change the default password for his smart device, the hacker can hack the device by using this password. Using manufacturers a unique password for each smart device prevents this from happening. This is a big step to strengthen the security of smart devices despite the large number of smart devices being produced. On the other hand, manufacturers should encourage and remind consumers to change their default passwords as an extra security measure for smart devices.

Establish a channel of communication between the manufacturer and the customer: Customers should be able to easily communicate

with the smart device manufacturer so they can submit any feedback or reports regarding any vulnerabilities they may find when using those devices. The manufacturer uses these reports to develop devices and also sends advice to its customers in case something goes wrong with the smart device. These advices must provide information to the consumer in simple language and without technical details.

Keep Software Updated: Without waiting for user request, a smart device manufacturer must inform users sooner when it upgrades the software, for whatever reason - for example, to fix a bug. The manufacturer may use the previously mentioned communication channels as a means of informing the customer of these updates. Another step is to make these updates easy to access and install by customers.

Minimize exposed attack surfaces: It is recommended that manufacturers minimize attack ports while developing any smart device. For example, unused programs, network ports, and hardware access methods (such as open serial access, ports, or test points) have to be disabled. Additionally, the device's code must to be restricted to what is necessary for it to function. It's crucial to take all of these measures to stop hackers from discovering any ports that they could exploit to breach a smart device.

Facilitate personal data deletion by consumers: The manufacturer must provide clear instructions to consumers regarding the complete

removal of their data from smart devices if, for example, they want to sell it or exchange it with someone else.

4.2 The Consumer Role

Even though most of the security problems are caused by vulnerabilities originating from the design and manufacturing issues, consumers have an important role in protecting and securing their smart homes. In addition to the security measures manufacturers take to help consumers secure their homes, there is also an important role that consumers themselves play in making their smart homes more secure.

Because IoT devices are becoming more and more popular such as Google Nest or Amazon Alexa, consumers must have the necessary awareness about how to use and protect these devices. This would lessen the risks that consumers would be exposed to if these devices are not properly secured and enable them to effectively contribute to the security of their smart homes. Important recommendations for consumers are listed below.

Purchase the top smart appliances for your home: The customers have to make an effort to locate the best smart devices, paying particular attention to their features and security level. The advice of professionals and user reviews can aid consumers in making decisions about buying the smart devices.

Companies like Amazon, Apple, Philips, and Samsung display their range of smart home devices on their websites for customers to choose from. These companies' websites explain the features, properties and prices of these smart devices. If the customer is confused in choosing between devices and companies, it should be noted that there are many sites that help the consumer in this confusing task of choice. These websites compare the newest and greatest smart home goods from various manufacturers, allowing the user to select the one that best meets their needs.

Map all connected devices: The devices that connect to the home network must be listed by the consumer. This will facilitate the process of identifying each device's weaknesses and assessing the security precautions required to fortify it. The evaluation aids the consumer in determining whether to upgrade or replace the smart device.

The consumer must disconnect non-essential or unnecessary smart devices (e.g., smart refrigerator or smart light bulbs) from the home information network because the fewer devices connected to the home network, the less potential danger. For if hackers manage to enter the smart device with its default login credentials, they can utilize it to take control of more devices that are linked to the same network. This procedure will lessen the entry points an intruder can use to access a smart home and facilitate the consumer's ability to identify a breach.

Disable unnecessary features and functionalities: Smart devices come with many features that are enabled by default. When a customer purchases smart device, he must disable features he does not need. An example of these features is the ability to access the device remotely, which is considered one of the most dangerous tools that an attacker uses to penetrate smart devices.

Change the default settings of the smart devices: Consumers control and interact with their smart home devices by entering a password and username as a form of authentication. For example, the SmartThings application is used to control devices such as smart refrigerator. Consumers open the SmartThings app on their smart phone and sign in a Wi-Fi account for the refrigerator by using default settings come in the refrigerator instruction booklet. This password is the same in all refrigerators of the same type and the same brand.

Nonetheless, a lot of users don't alter the device's basic settings, which include the password, username, and device name. In reality, default or weak access credentials put over 69% of vulnerable devices at risk, making it simple for hackers to access and take control of these devices.

Another important point is that consumers should not use the same password for all of their home devices. Because the hackers will have the passwords to all the other accounts if one of these accounts is compromised.

Update firmware: Firmware is a low-level software that runs on hardware and is included in read-only memory (ROM) which is critical to device operation [39]. For example, printer firmware is the program stored inside of a printer that allows it to receive information from the computer and turn it into a printed image. Old software on smart devices lacks the latest security measures and patches, which makes them vulnerable to security gaps. On the other hand, releasing a new update by the company often means discovering a new security vulnerability in the device that could be exploited by hackers to launch an attack on the device.

Hackers target outdated firmware of smart home devices to implant malware and hide other malicious code in it. For this reason, the customer should update the firmware regularly to keep the devices in home secure [38]. The updates can be over the Internet, and many devices regularly check for new firmware and automatically download and install them.

Unfortunately, according to Avast report, 59.1% of users worldwide have never updated the firmware despite the importance of this procedure [37].

Use authentication mechanisms: Homeowner should use strong and two-factors authentication to secure their smart devices. For two-factor authentication, consumers usually use a strong password as the first factor and, for example, a one-time six-digit code as the second

factor on the services that support it. This code can be received via a text message. Therefore, even if hackers manage to steal the password, it is unlikely that they can hack the consumer's phone as well in order to obtain the code. On the other hand, the use of biometric authentication, such as fingerprints, eye scans, voice and facial recognition, are some of the most powerful methods of proving identity that are difficult to forge or steal.

Secure the home Wi-Fi network: Over the years, smart devices have been produced that are different from each other in terms of design, configuration and features. That is why not all of them can be secured in the same manner. An effective solution to this is to protect the network that connects them, which is considered an entry point for attackers [48]. Among the methods used to protect the home network:

- Use a complex password to protect the router
- Prevent the access to the router from the Internet
- Use a strong Wi-Fi encryption method
- Use a network firewall

Nowadays, some companies have produced specialized devices for protecting the home network. The customer purchases these devices and connects them directly to the home router, so they act as a guard for the home network [25].

Replace outdated routers: The router is the primary component in any smart home and acts as a gateway that connects smart home

devices and makes them connectable to the world outside the home. In case the home router is hacked or badly configured, this allows attackers to access the network and gain control over most of the devices connected to it [38]. Therefore, building a more secure smart home starts with a strong router [49].

It is good for consumers to find the most secure router on the market and make sure to replace it with any new version produced because that means producing newer protocols, technologies, components and features that may help protect the router and network.

Split up the home network: In December 2019, the FBI warned that "your fridge and your laptop should not be on the same network. Keep your most private, sensitive data on a separate system from your other IoT devices." Consumers should not put all their smart devices in the same network because this means that having one hackable device may lead to the penetration of all devices connected with it in the same network. For example, they can assign a network to computers, tablets, printers and smartphones used in Internet banking, shopping, and general web activity; another can be assigned for the smart devices [50],[51]. To separate home networks, consumers can use, for example, Virtual Local Area Networks (VLAN) and assign different IP addresses to them. Also, separation can be done physically using more than one router.

Set up a guest network: To complement the previous point, the homeowner must allocate a network for guests and visitors so that it is

disconnected from the network of his smart devices. This network, for example, provides limited access to the Internet and at the same time does not represent a threat to the rest of the smart devices of the home.

Avoid public Wi-Fi networks: When a homeowner wants to manage his smart home remotely, he should avoid using public networks if possible, such as airports, cafes or hotels. In the absence of an alternative to public networks, the consumer should use protections such as using a VPN. For example, the VPN can hide the IP address of users and block their location [52].

Keep smartphones within sight at all times: The consumer should not put his smartphone anywhere so that it is capable of stealing or voyeurism, especially if he uses it in managing his smart home because in this case it contains all the passwords and verification information [53]. Additionally, users should disable Bluetooth and Wi-Fi while not in use, especially in congested areas where certain smartphones may automatically share data with other users due to misconfiguration.

Install malware protection: Applications downloaded on tablets, computers, and smartphones are used to manage smart home devices. So, hacking these devices will enable hackers to control them. To prevent this, customers must use the latest anti-malware software.

Use wired LAN if possible: Wireless networks are still widely used, although they experience problems with noise, interference and

interception of information. For these reasons, it is better for the user if it is possible to use wired networks to connect the largest number of devices to the central hub. By doing so, hackers have difficulty obtaining information.

Erase personal information: There are instances when consumers choose to get rid of a smart device because it is broken, doesn't work well for them, or they want to upgrade to a new model. In this instance, they should do a factory reset on the device to remove any personal data that is saved on it.

Consumers can also use factory reset restore in smart devices when they suspect a hack of their devices. This prevents the attacker from using the information stored in the devices

Seek professional aid: Certain smart home system providers include remote monitoring and customized installs in their packages. Utilizing this feature, which actively monitors the smart home system for any signs of issues or the appearance of unusual behavior, will give customers an additional layer of security.

4.3 The ISP Role

Homeowners can obtain Internet connection services via ISPs. While the main role of maintaining smart home security lies with the manufacturers and consumers, an ISP might also be able to help in this situation. In fact, there are discussions about the role that an ISP could play for smart home security, and it is possible to observe

reluctance on behalf of ISPs to take a certain degree of responsibility related to smart home security issues [26]. The following is a summary of the main causes of this reluctance:

Violation of privacy: ISP monitoring user activities within the Internet and analyzing and recording user activities is a way to provide security to the user. However, this has sparked a debate about whether it is possible for ISPs to use this data for other reasons, worrying internet privacy advocates.

The distinction between censorship and security: Imposed security mechanisms by ISPs could bring about restrictions for homeowners. Because of this, some users might consider these actions as a form of censorship and complain about ISP limitations by considering them as a treat for their freedom.

Taking responsibility over mistakes: Since they are unable to control the activity of each user, ISPs prefer not to take responsibility for mistakes made by users. Despite providing the best security measures in place, people can still do bad things that cause problems for ISPs and other service users.

Define scope of responsibilities: Some researchers have acknowledged that managing and securing the smart home platform requires the participation of several actors, including Internet service providers, although there is controversy about that. However, it is important to put in place regulations and laws that prevent ISPs from

exceeding their limits and powers, which is a major challenge [18],[54],[55],[56]. In this scope, a typical ISP can contribute to the issue as given below.

Secure own network: ISPs can ensure service availability by implementing various measures, including firewalls and Intrusion Detection Systems (IDS), on their infrastructure. This can be viewed as an indirect measure of client protection.

Provide high quality gateways: Many customers connect to the Internet using devices (e.g., a home router with in-built DSL modem) provided by ISPs. These devices may have additional functionalities to support security. For instance, they might have anti-virus/malware filtering, which is crucial for safeguarding IoT devices that are unable to defend themselves.

Provide technical support: ISPs could support smart home owners starting from the installation step. They can improve their organizations to provide such supports through call centers and sending experts to customers when needed.

Provide security services: ISPs could provide some security services to help their customers. These services can be free or paid. For example, they can provide data recovery and system hardening services which may help a targeted smart home owner after an attack incident. They could even provide system hardening service during installation.

Improve customer awareness: Smart home users may not be aware of risks they may be exposed to since they are not experts. ISPs can play an important role to improve users' awareness level. During the initial installation and from time to time, they may inform smart home owners about security risks and recommend solutions to prevent attacks.

5. Conclusion

The home, whether traditional or smart, is a place where a person relaxes and maintains his privacy. Many devices in a smart home are resource-limited and insufficient to enhance security or prevent attacks. This is why smart home infringement is not a difficult task for attackers. Given that the information circulating in smart homes is personal and sensitive, and in the event of any breach, this may lead to serious and potentially life-threatening consequences, the issue of smart home security should become a priority.

Due to the great benefit that the smart home app provides in human life, we have devoted this paper to highlight the importance of securing the smart home and protecting it from intruders. This work provides recommendations and advice to anyone interested in the success of this application - from consumers, to manufacturers, to Internet service providers. Upon following these guidelines, the smart home security is expected to improve significantly, in turn

encouraging further adoption of this technology by more people and under more confident and secure terms.

All parties involved in the smart home app stand to gain from increased safety, therefore it appears that everyone has a duty for smart home security. When a manufacturer makes their products safer, the buyer feels more confident, which boosts sales and helps the manufacturer establish a solid reputation. On the users' side, when home owners contribute to making their smart home safer, they are in essence protecting their own privacy, secrets, and even life against any danger posed by technology.

References

- [1] Neeraj Sharma, Vijender Kumar Solanki, & Davim, J. P. (2019). Basics of the Internet of Things (IoT) and Its Future. In Vijender Kumar Solanki, Vicente García Díaz, & J. P. Davim (Eds.), *Handbook of IoT and Big Data* (1st ed.): CRC Press.
- [2] Subhas Chandra Mukhopadhyay, & Suryadevara, N. K. (2014). Internet of Things: Challenges and Opportunities. In S. C. Mukhopadhyay (Ed.), *Internet of Things: Challenges and Opportunities* (Vol. 9, pp. 1-17). Cham: Springer International Publishing.
- [3] Parvaneh Asghari, Amir Masoud Rahmani, & Javadi, H. H. S. (2019). Internet of Things applications: A systematic Review. *Computer Networks*, *148*, 241-261. doi:<https://doi.org/10.1016/j.comnet.2018.12.008>
- [4] Davit Marikyan, Savvas Papagiannidis, & Alamanos, E. (2019). A systematic review of the smart home literature: A user perspective. *Technological Forecasting and Social Change*, *138*, 139-154. doi:<https://doi.org/10.1016/j.techfore.2018.08.015>
- [5] Francesca Meneghello, Matteo Calore, Daniel Zucchetto, Michele Polese, & Zanella, A. (2019). IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. *IEEE Internet of Things Journal*, *6*(5), 8182-8201. doi:10.1109/JIOT.2019.2935189

-
- [6] Haseeb Touqeer, Shakir Zaman, Rashid Amin, ., M. H., & Bilal, F. A.-T. M. (2021). Smart home security: challenges, issues and solutions at different IoT layers. *The Journal of Supercomputing*, 77, 14053–14089. doi:<https://doi.org/10.1007/s11227-021-03825-1>
- [7] Huichen Lin, & Bergmann, N. W. (2016). IoT Privacy and Security Challenges for Smart Home Environments. *Information*, 7(3). doi:<https://doi.org/10.3390/info7030044>
- [8] Binglaw, F. (2021). Security Issues In The Internet of Things: Requirements, Attacks And Countermeasures. (Master in IT Master of Science), Atilim University.
- [9] Ftayem Binglaw, Murat Koyuncu, & Pusatlı, T. (2021). *Security Requirements in IoT Environments*. Paper presented at the International Conference on Internet of Things as a Service, Sydney.
- [10] Bogdan-Cosmin Chifor, Ion Bica, Victor-Valeriu Patriciu, & Pop, F. (2018). A security authorization scheme for smart home Internet of Things devices. *Future Generation Computer Systems*, 86, 740-749. doi:<http://dx.doi.org/10.1016/j.future.2017.05.048>
- [11] Andreas Jacobsson, Martin Boldt, & Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems*, 56, 719-733. doi:<https://doi.org/10.1016/j.future.2015.09.003>

-
- [12] Nazmiye Balta-Ozkan, Rosemary Davidson, Martha Bicket, & Whitmarsh, L. (2013). Social barriers to the adoption of smart homes. *Energy Policy*, 63, 363-374. doi:<https://doi.org/10.1016/j.enpol.2013.08.043>
- [13] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, & Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal*, 4(5), 1250-1258. doi:10.1109/JIOT.2017.2694844
- [14] Zahrah A. Almusaylim, & Zaman, N. (2019). A review on smart home present state and challenges: linked to context-awareness internet of things (IoT). *Wireless Networks*, 25, 3193-3204. doi:<https://doi.org/10.1007/s11276-018-1712-5>
- [15] Mussab Alaa, A.A. Zaidan, B.B. Zaidan, Mohammed Talal, & Kiah, M. L. M. (2017). A review of smart home applications based on Internet of Things. *Journal of Network and Computer Applications*, 97, 48-65. doi:<https://doi.org/10.1016/j.jnca.2017.08.017>
- [16] Dimitris Geneiatakis, Ioannis Kounelis, Ricardo Neisse, Igor Nai-Fovino, Gary Steri, & Baldini, G. (2017). *Security and privacy issues for an IoT based smart home*. Paper presented at the 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia.
- [17] Brittany D. Davis, Janelle C. Mason, & Anwar, M. (2020). Vulnerability Studies and Security Postures of IoT Devices: A

- Smart Home Case Study. *IEEE Internet of Things Journal*, 7(10), 10102 - 10110. doi:10.1109/JIOT.2020.2983983
- [18] Jordi Mongay Batalla, Athanasios Vasilakos, & Gajewski, M. (2018). Secure Smart Homes: Opportunities and Challenges. *ACM Computing Surveys*, 50(5). doi:<https://doi.org/10.1145/3122816>
- [19] Won Min Kang, Seo Yeon Moon, & Park, J. H. (2017). An enhanced security framework for home appliances in smart home. *Human-centric Computing and Information Sciences*, 7. doi:10.1186/s13673-017-0087-4
- [20] Eirini Anthi, Lowri Williams, Małgorzata Słowińska, George Theodorakopoulos, & Burnap, P. (2019). A Supervised Intrusion Detection System for Smart Home IoT Devices. *IEEE Internet of Things Journal*, 6(5), 9042-9053. doi:10.1109/JIOT.2019.2926365
- [21] Geong Sen Poh, Prosanta Gope, & Ning, J. (2021). PrivHome: Privacy-Preserving Authenticated Communication in Smart Home Environment. *IEEE Transactions on Dependable and Secure Computing*, 18(3), 1095-1107. doi:10.1109/TDSC.2019.2914911
- [22] Yan Meng, Zhang, W., Haojin Zhu, & Shen, X. S. (2018). Securing Consumer IoT in the Smart Home: Architecture, Challenges, and Countermeasures. *IEEE Wireless Communications*, 25(6), 53-59.

-
- [23] Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, & Zualkernan, I. (2015). *Internet of things (IoT) security: Current status, challenges and prospective measures*. Paper presented at the 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK.
- [24] David Barnard-Wills, Louis Marinos, & Portesi, S. (2014). *Threat Landscape and Good Practice Guide for Smart Home and Converged Media*. Retrieved from
- [25] Joseph Bugeja, Andreas Jacobsson, & Davidsson, P. (2016). *On Privacy and Security Challenges in Smart Connected Homes*. Paper presented at the European Intelligence and Security Informatics Conference (EISIC), Uppsala, Sweden.
- [26] Omar Alrawi, Chaz Lever, Manos Antonakakis, & Monrose, F. (2019). *SoK: Security Evaluation of Home-Based IoT Deployments*. Paper presented at the IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA.
- [27] Changmin Lee, Luca Zappaterra, Kwanghee Choi, & Choi, H.-A. (2014). *Securing smart home: Technologies, security challenges, and security requirements*. Paper presented at the IEEE Conference on Communications and Network Security, San Francisco, CA, USA.
- [28] Utkarsh Saxena, J. S. Sodhi, & Singh, Y. (2017). *Analysis of security attacks in a smart home networks*. Paper presented at the 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence, Noida, India.


- [29] Mirza Abdur Razzaq, Sajid Habib Gill, Muhammad Ali Qureshi, & Ullah, S. (2017). Security Issues in the Internet of Things (IoT): A Comprehensive Study. *International Journal of Advanced Computer Science and Applications*, 8(6), 383-388. doi:10.14569/IJACSA.2017.080650
- [30] Cypfer. (2020). Cyber Security in the Era of the Smart Home Devices. Retrieved from <https://cypfer.com/cyber-security-and-smart-devices/>
- [31] Chang, Z. (2019). Inside the Smart Home: IoT Device Threats and Attack Scenarios. Retrieved from <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/inside-the-smart-home-iot-device-threats-and-attack-scenarios>
- [32] Earlence Fernandes, Amir Rahmati, Jaeyeon Jung, & Prakash, A. (2017). Security Implications of Permission Models in Smart-Home Application Frameworks. *IEEE Security & Privacy*, 15(2), 24-30. doi:10.1109/MSP.2017.43
- [33] Keyur K Patel, & Patel, S. M. (2016). Internet of Things-IoT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. *International Journal of Engineering Science and Computing*, 6(5), 6122-6131.
- [34] Mohammed Talal, A. A. Zaidan, B. B. Zaidan, A. S. Albahri, A. H. Alamoodi, O. S. Albahri, . . . Mohammed , K. I. (2019). Smart Home-based IoT for Real-time and Secure Remote Health Monitoring of Triage and Priority System using Body

- Sensors: Multi-driven Systematic Review. *Journal of Medical Systems*, 43. doi:<https://doi.org/10.1007/s10916-019-1158-z>
- [35] Nisha Panwar, Shantanu Sharma, Sharad Mehrotra, Łukasz Krzywiecki, & Venkatasubramanian, N. (2019). Smart Home Survey on Security and Privacy. *arXiv:1904.05476*. doi:<https://doi.org/10.48550/arXiv.1904.05476>
- [36] Seokung Yoon, Haeryong Park, & Yoo, H. S. (2015). Security Issues on Smarthome in IoT Environment. In James J. (Jong Hyuk) Park, Ivan Stojmenovic, Hwa Young Jeong, & G. Yi (Eds.), *Computer Science and its Applications* (pp. 691-696): Springer.
- [37] Avast. (2019). Two out of Five Digital Households Worldwide at Cyber Risk, Avast Reveals [Press release]. Retrieved from <https://press.avast.com/two-out-of-five-digital-households-worldwide-at-cyber-risk-avast-reveals>
- [38] Ali, M. H. (2022). Smart Home Security: Security and Vulnerabilities. *IoT Foundation Series*. Retrieved from <https://www.wevolver.com/article/smart-home-security-security-and-vulnerabilities>
- [39] Michael J. Fagan, Katerina N. Megas, Karen Scarfone, & Smith, M. (2020). *Foundational Cybersecurity Activities for IoT Device Manufacturers* (NISTIR 8259). Retrieved from
- [40] Ali, W., Dustgeer, G., Awais, M., & Shah, M. A. (2017). *IoT based smart home: Security challenges, security requirements and solutions*. Paper presented at the 23rd International

- Conference on Automation and Computing (ICAC), Huddersfield.
- [41] Bogdan-Cosmin Chifor, Stefan-Ciprian Arseni, Ioana Matei, & Bica, I. (2019). *Security-Oriented Framework for Internet of Things Smart-Home Applications*. Paper presented at the 22nd International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania
- [42] Shahrouz Sotoudeh, Sattar Hashemi, & Garakani, H. G. (2020). *Security Framework of IoT-Based Smart Home*. Paper presented at the 10th International Symposium on Telecommunications (IST), Tehran, Iran.
- [43] Waseem Iqbal, Haider Abbas, Pan Deng, Jiafu Wan, Bilal Rauf, Yawar Abbas, & Rashid, I. (2021). ALAM: Anonymous Lightweight Authentication Mechanism for SDN-Enabled Smart Homes. *IEEE Internet of Things Journal*, 8(12), 9622 - 9633. doi:10.1109/JIOT.2020.3024058
- [44] Young-Pil Kim, Seehwan Yoo, & Yoo, C. (2015). *DAoT: Dynamic and energy-aware authentication for smart home appliances in Internet of Things*. Paper presented at the IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA.
- [45] DEVELCO Products. Security and Privacy. Retrieved from <https://www.develcoproducts.com/gateway/security-and-privacy/>

- [46] European Telecommunications Standards Institute Technical Committee Intelligent Transport Systems. (2019). ETSI TS 102 941 v1.3.1. France.
- [47] GDPR.eu. (2022). Complete guide to GDPR compliance. Retrieved from <https://gdpr.eu>
- [48] Sandeep Pirbhulal, Heye Zhang, Md Eshrat E Alahi, Hemant Ghayvat, Subhas Chandra Mukhopadhyay, Yuan-Ting Zhang, & Wanqing Wu. (2017). A Novel Secure IoT-Based Smart Home Automation System Using a Wireless Sensor Network. *Sensors*, 17(Sensors for Home Automation and Security). doi:<https://doi.org/10.3390/s17010069>
- [49] Yinxin Wan, Kuai Xu, Guoliang Xue, & Wang, F. (2020). *IoTArgos: A Multi-Layer Security Monitoring System for Internet-of-Things in Smart Homes*. Paper presented at the IEEE INFOCOM 2020 - IEEE Conference on Computer Communications, Toronto, ON, Canada.
- [50] Eric Zeng, Shrirang Mare, & Roesner, F. (2017). *End user security and privacy concerns with smart homes*. Paper presented at the 13th Symposium on Usable Privacy and Security (SOUPS 2017), Santa Clara, CA, USA.
- [51] Soteris Demetriou, Nan Zhang, Yeonjoon Lee, XiaoFeng Wang, Carl A. Gunter, Xiaoyong Zhou, & Grace, M. (2017). *HanGuard: SDN-driven protection of smart home WiFi devices from malicious mobile apps*. Paper presented at the WiSec '17: Proceedings of the 10th ACM Conference on

- Security and Privacy in Wireless and Mobile Networks, Boston, MA, USA.
- [52] Norton. (2022). Norton Secure VPN. Retrieved from <https://us.norton.com/products/norton-secure-vpn>
- [53] Vijay Sivaraman, Dominic Chan, Dylan Earl, & Boreli, R. (2016). *Smart-Phones Attacking Smart-Homes*. Paper presented at the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, Darmstadt, Germany.
- [54] Angrishi, K. (2017). Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets. *arXiv:1702.03681v1*.
doi:<https://doi.org/10.48550/arXiv.1702.03681>
- [55] Haddadi, H., Christophides, V., Teixeira, R., Cho, K., Suzuki, S., & Perrig, A. (2018). *SIOTOME: An Edge-ISP Collaborative Architecture for IoT Security*. Paper presented at the International Workshop on Security and Privacy for the Internet-of-Things (IoTSec), USA.
- [56] Vijay Sivaraman, Hassan Habibi Gharakheili, Arun Vishwanath, Roksana Boreli, & Mehani, O. (2015). *Network-level security and privacy control for smart-home IoT devices*. Paper presented at the 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Abu Dhabi, United Arab Emirates.



**DESIGN AND IMPLEMENTATION OF
A QUADRATURE HYBRID COUPLER
IN MICROWAVE CIRCUITS**

7

DESIGN AND IMPLEMENTATION OF A QUADRATURE HYBRID COUPLER IN MICROWAVE CIRCUITS

Alhasan Ali Almahroug
Faculty of Engineering, University of Zawia, Libya
Department of Electrical and Electronic Engineering
h.almahroug@zu.edu.ly

Basem Mustafa Amer
Faculty of Economics, University of Zawia, Libya
Department of Data Analysis
basim_Zawaghy@yahoo.com

Abdusamea I.A Omer
Faculty of Engineering, Sabratha University, Libya
abdusamea@gmail.com

Abstract

Microstrip antennas encounter gain-bandwidth limits when matched with passive matching networks. NGD-based non-Foster reactive networks have been proposed as a solution to overcome those restrictions. However, the NGD networks are inherently “lossy” structures due to the incorporation of parasitic elements in their design, leading to poor quality at microwave frequencies. This paper aims to develop a suitable method to compensate for the losses of the NGD networks. The proposed scheme involves three main

components to realise a loss-compensated non-Foster network. It combines NGD networks with a reflection amplifier in a balanced structure using a Lange coupler. One crucial step in implementing the compensation technique is designing a quadrature hybrid coupler. In this paper, a Lange coupler is employed to demonstrate the principle. By passing the signal through the NGDs twice in a balanced structure, the Lange coupler effectively doubles the effect of the NGDs' behavior. The paper presents a systematic design methodology for the Lange coupler and includes simulation and experimental results.

Keywords: Lange coupler-Non-Foster-reactive elements, NGD networks, compensation techniques.

1. Introduction

A new technique to compensate for the inherent losses of the reflection-mode NGD networks was firstly presented in references (Almahroug et al., 2016, Almahroug et al., 2017, Almahroug et al., 2021). The concept of the proposed loss compensation technique is demonstrated in Figure 1. It is realised by combining two “lossy” reflection-type NGD networks and a negative resistance reflection amplifier with a Lange coupler in a balanced structure. The merit of this new design is that the overall NGD response is provided by passive circuits which should make it easier to achieve stable behaviour. A Lange coupler is used to double the effect of the NGDs’

behaviour as a result of sending the signal through them twice in a balanced structure. The reflection amplifier is connected to one of the ports of the coupler to provide the required gain that compensates the losses. The proposed technique can be very attractive in antenna-matching applications where both transmit and receive capabilities are required

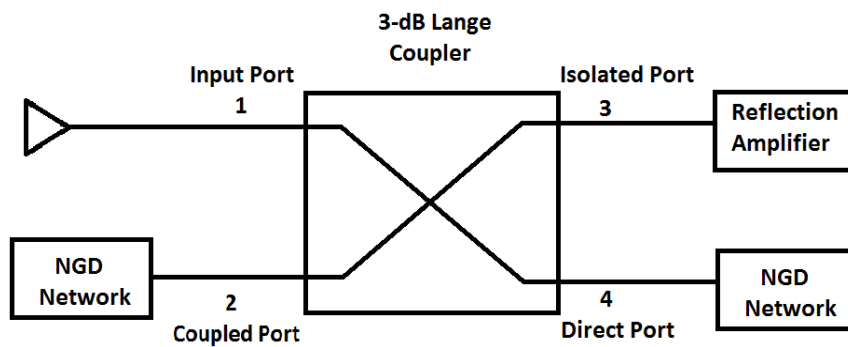


Figure 1: The structure of the proposed loss compensation technique (Almahroug et al., 2016)

Equation 1, presents the concept of the proposed loss compensation technique demonstrated in Figure 1.

$$T_{in} = -T_{RA} T_{NGD}^2 \quad (1)$$

Where,

The reflection coefficient of the received signal at the input port is a result of the reflection coefficients of the reflection amplifier in addition to the two NGD networks. Moreover, the effect of the NGD

behaviour of the realised NGD-based non-foster circuit is the double effect of the NGD devices as a result of sending the signal through them twice in a balanced structure. The direct and coupled ports of the coupler are both connected to reflection-type NGD networks. The reflected signals passing back into the coupler recombine at the isolation port and are amplified by the FET reflection amplifier. The amplified signals pass back into the coupler, reflecting again from the NGD devices, finally recombining at the coupler input port (Almahroug et al., 2016)

To make the combining effect work, as the coupling ratio is low and the structure is reciprocal, then the vast majority of the reflected signal from the output ports goes to the isolated port (port 3) because there is no cancellation of the direct reflection and the magnitude S_{41} is much smaller than the S_{21} magnitude. If the hybrid coupler can achieve a coupling factor of 3 dB then the two reflected signals from the NGDs would be 180° out of phase and will cancel each other. If the coupling ratio is not 3 dB then the reflected signal from ports 2 and 4 are not equal. Therefore, they won't perfectly cancel out. In this work, a 3-dB hybrid coupler is designed and experimental tested.

2. Lange Coupler Design and Experiment

One important key step in the proposed loss-compensation technique is the design of a quadrature hybrid coupler. In this work, a Lange coupler is used to demonstrate the principle. It is used to double the

effect of the NGDs' response as a result of sending the RF signal through them twice in a balanced structure. Other forms of quadrature hybrid couplers could be used, such as multilayer couplers or branch-line couplers, as appropriate in the chosen circuit medium. The Lange coupler is a four-port interdigitated structure which constitutes a quadrature hybrid with a 3-dB coupling ratio and a 90-degree phase shift difference between the output ports. To demonstrate the physics of the Lange coupler concept, the AWR Microwave Office circuit schematic simulator is used. This simulation tool gives results with good accuracy and fast execution times. A circuit schematic of an ideal Lange coupler is shown in Figure 2.

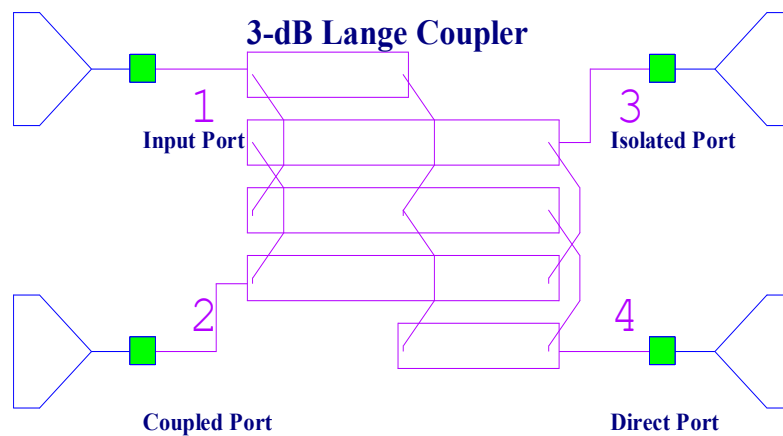


Figure 2: Ideal Lange coupler schematic layout

3. Problem Statement

The symmetry of the proposed Lange coupler's structure is beneficial, as any port could be used as an input port, and the isolated port is on the same side as the input port. In addition, the output ports are on the other side of the junction from the input port. An even-odd mode characteristic impedance technique is used to design and analyse the operation of the proposed Lange coupler. For more details, and examples of this scheme, readers are referred to reference (Pozar., 2012). For such a microstrip coupled line, a design graph shown in Figure 3 is used to determine the width of the strips and the gap spacing between them: for a given dielectric constant and characteristic impedances, there is a set of even-mode (Z_{0e}) and odd-mode (Z_{0o}) impedances. The implementation described here uses Taconic substrate type RF_35_0600_C1/C1. To design a 3-dB hybrid Lange coupler with a centre frequency of 3 GHz, we need to calculate the even-mode and odd-mode line impedances. To do that, firstly we determine the coupling (C) using the following equation (Pozar., 2012)

$$C = 10^{\frac{\text{coupling coefficient}}{20}} \quad (1.1)$$

$$C = 10^{\frac{-3dB}{20}} = 0.707$$

Thus, even mode characteristic impedance (Z_{0e}) can be determined using this equation:

$$Z_{0e} = \frac{4C - 3 + \sqrt{9 - 8C^2}}{2C\sqrt{(1 - C)/(1 + C)}} Z_0 \quad (1.2)$$

$$Z_{0e} = \left[\frac{(4 \times 0.0707) - 3 + \sqrt{9 - (8 \times 0.0707^2)}}{2 \times 0.0707 \times \sqrt{(1 - 0.0707)/(1 + 0.0707)}} \right] \times 50$$

$$Z_{0e} = \frac{2.828 - 3 + 2.236}{2 \times 0.0707 \times 0.414} = 176 \Omega$$

To find the odd-mode characteristic impedance (Z_{0o}), the following equation is used:

$$Z_{0o} = \frac{4C + 3 - \sqrt{9 - 8C^2}}{2C\sqrt{(1 + C)/(1 - C)}} Z_0 \quad (1.3)$$

$$Z_{0o} = \left[\frac{(4 \times 0.0707) + 3 - \sqrt{9 - (8 \times 0.0707^2)}}{2 \times 0.0707 \times \sqrt{(1 + 0.707)/(1 - 0.707)}} \right] \times 50$$

$$Z_{0o} = \frac{2.828 + 3 - 2.236}{2 \times 0.0707 \times 2.414} = 52.6 \Omega$$

Plotting (Z_{0e}) and (Z_{0o}) on the even-odd mode characteristic impedance design data coupled microstrip lines graph as depicted in Figure 3, we can approximately read the values of the width (W) of the tracks and the gap (S) between them.

$$\frac{S}{d} \cong 0.075$$

Where d is the height of the substrate which is 1.52 mm.

Therefore,

$$\frac{S}{1.52} \cong 0.075, \text{ thus } S = 0.114 \text{ mm}$$

Also,

$$\frac{W}{d} \cong 0.8$$

and d is the height of the substrate which is 1.52 mm.

Therefore,

$$\frac{W}{1.52} \cong 0.8, \text{ thus, } W = 1.216 \text{ mm}$$

Now, we determine the quarter wavelength of the Lange coupler's fingers by using the following equations:

$$V = \frac{c}{\sqrt{\epsilon_r}}$$

Where c is the speed of light in a vacuum, then

$$V = \frac{c}{\sqrt{3.5}} = 0.54c$$

$$\lambda = \frac{V}{f}$$

Where V is the speed of light and f is the frequency of the design which is 3 GHz.

$$\lambda = \frac{0.54 \times 3 \times 10^8}{3 \times 10^9}$$

$$\lambda = 54 \text{ mm}$$

The quarter wavelength of the fingers l is determined as follows:

$$l = \frac{\lambda}{4} = \frac{54}{4} = 13.5 \text{ mm}$$

$$l = 13.5 \text{ mm}$$

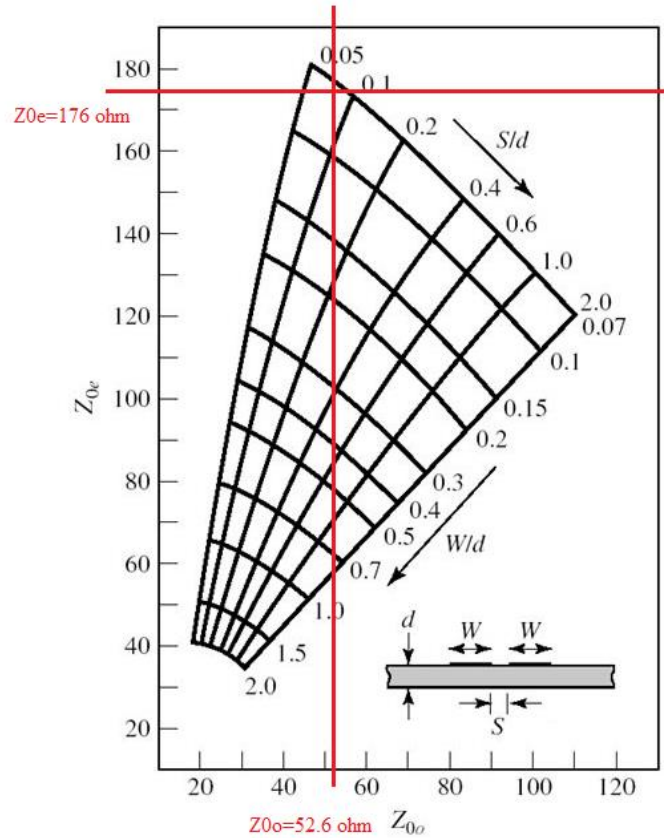


Figure 2: Even- and odd-mode characteristic impedance design data for coupled microstrip line (Pozar., 2012). This implementation uses a substrate with a dielectric constant of 3.5.

4. Coupler Assessment

To choose the most suitable hybrid coupler to comply with the loss-compensated non-Foster circuit requirement, an assessment was made between the proposed realistic Lange coupler, an ideal Lange coupler, commercial surface mount couplers, and a branch line

coupler. It should be noted that the commercial couplers were assessed using their S-parameters which were downloaded from the corresponding companies' websites. The datasheets for the commercial couplers are not included in this paper. All the couplers were used as four-port sub-circuits, where three ports were short circuits and one port was 50Ω . Figure 4 shows the simulated group delay and reflection coefficient magnitude obtained from the used couplers. In the frequency range of interest, the proposed Lange coupler was the most suitable for use because it generated less positive group delay and had a lower loss. Consequently, this proposed structure was fabricated and experimentally validated.

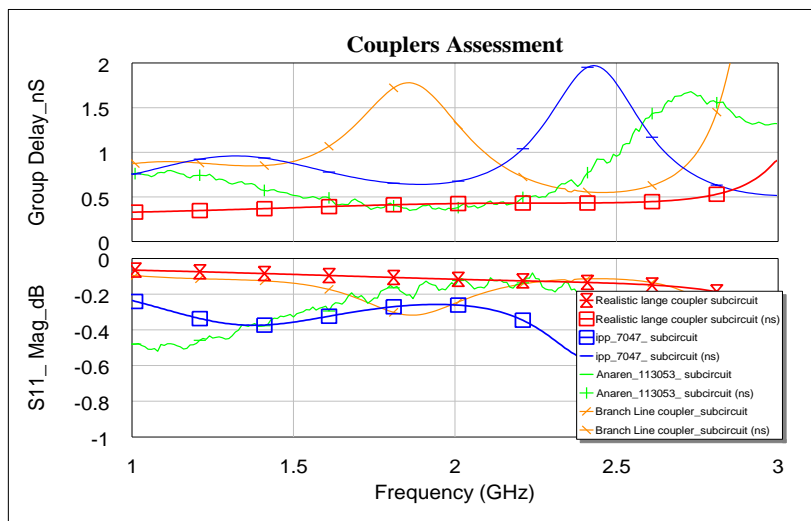


Figure 4: Group delay and S11 magnitude obtained from the assessed couplers

In this work, a realistic Lange coupler is designed using NI AWR Microwave Office and then tested. Due to the compact size of the design, the four ports of the coupler were folded in a way that can be manufactured. The circuit schematic and its associated layout of the proposed design are shown in Figures 5 and 6 respectively. It should be noted that extra 10 mm transmission lines are added to connect the four ports of the coupler with the measurement ports of the network analyser, to measure its S-parameters. They will be de-embedded later when the coupler is used in the implementation of the final design of the reactive non-Foster element.

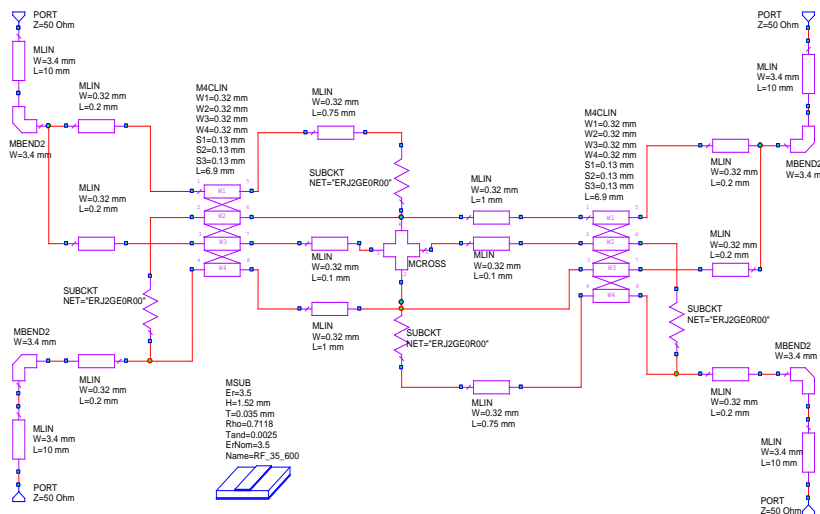


Figure 5: Realistic Lange coupler schematic layout

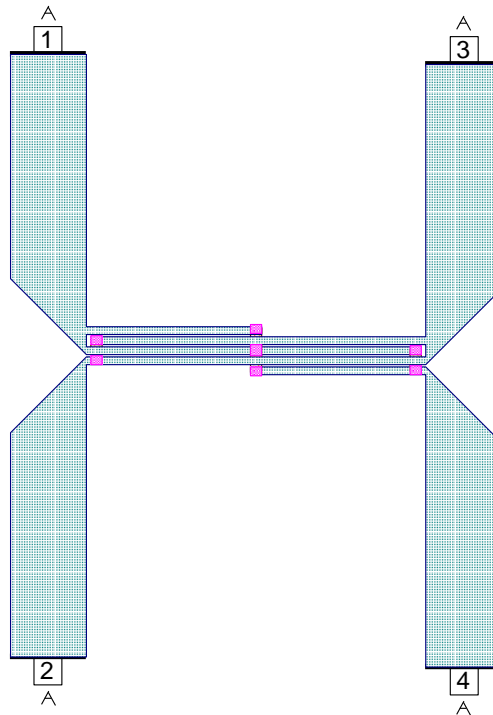


Figure 6: Structure layout of the realistic Lange coupler

5. The Fabrication Procedure

The circuit has been fabricated and manufactured on a double-sided printed circuit board (PCB) where the rear side was a full copper ground plane. The test board was printed on Taconic substrate type RF_35_0600_C1/C1. The challenging feature for manufacturing the prototype on a PCB board in the laboratory was the (0.13 mm) gap between the tracks of the coupler and assembling (0603) surface

mount resistors, amongst the other parts on it. Fortunately, we were able to wire bond the tracks of the coupler. Some bond wires were needed to form air bridges and connect the strips of the prototype. The wire bonding was achieved using an ultrasonic ball bonder. An electrostatic spark melted the tip of some gold wire forming a small ball, hanging from the wire. A ceramic bonding tool then pushed the ball down onto the bonding site and vibrated at ultrasonic frequencies to form the bond. The attached wire was then pulled over to the second bonding site where the wire was wedge bonded by smearing the wire across the copper, detaching the wire from the bonding machine and completing the bridged connection. Due to the wire's small diameter, this forms a robust link between the two tracks.

An image of the fabricated circuit is depicted in Figure 7. Four SMA connectors were carefully soldered to test the circuit. It is to be noted that all ports are 50 ohms. A photograph of the prototype, when it was connected with a two-port vector network analyser in the lab to measure its S-parameters, is depicted in Figure 8.

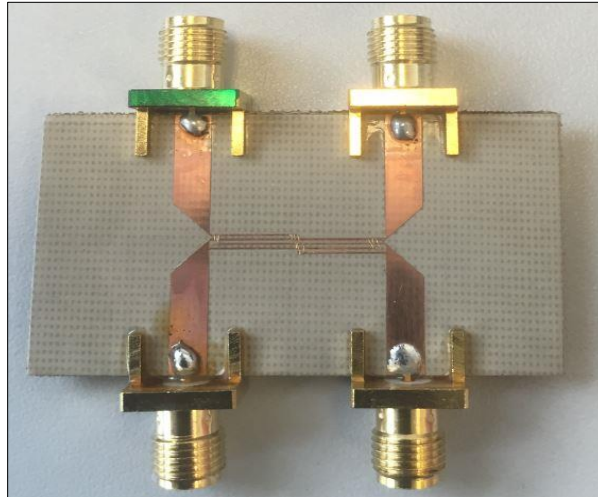


Figure 7: Image of the fabricated circuit board

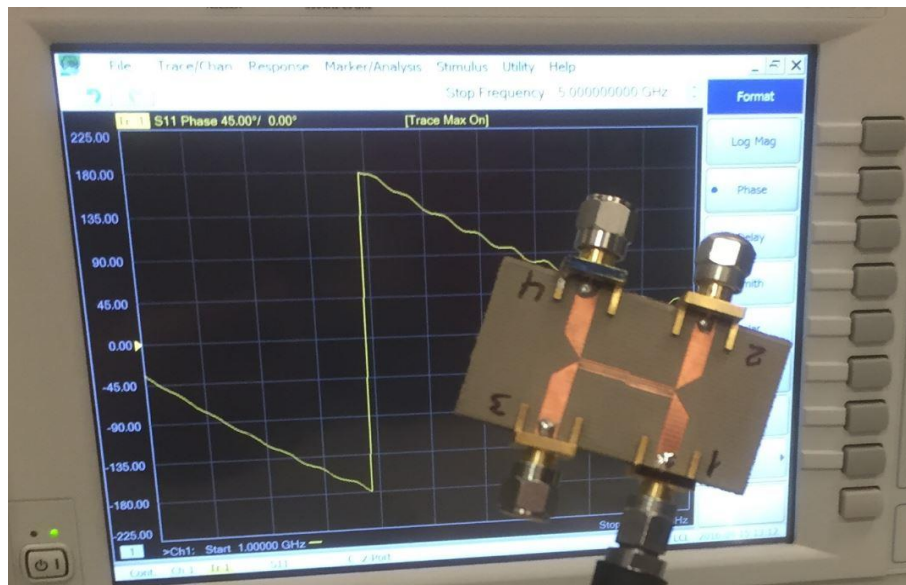


Figure 83: Photograph of the measured S11 phase response of the fabricated circuit board in the test station

6. Lange Coupler Simulated and Measured Performance

Fine-tuning and optimization were carried out to refine the design which can be integrated with the other components, forming the final synthesized non-Foster reactive element. Figure 9 compares the measured and simulated coupling results between outputs 2 and 4 of the Lange coupler. The design frequency was 3 GHz and the frequency range of interest was ± 2.0 GHz for a total range of 1.0 to 5.0 GHz. At the frequency range from 2.0 to 4.0 GHz, the coupling factors obtained from simulation and measurement are approximately -3.5 dB and -5.0 dB respectively. It is observed that the simulated S21 and S41 are approximately 3.5 dB. Furthermore, at the frequency range of interest, the measured S41 closely follows that of those simulated at almost -3 dB. However, the measured S21 shows an approximate 1.5 dB below the same simulations at the same bandwidth. This implies that the coupled port receives less power than the direct port and is possibly due to dimensional inaccuracy in the coupler fabrication.

Furthermore, the output balance plot is depicted in Figure 10. This graph shows the characteristics of the output ports. The amplitude balance and the phase balance achieved from the simulation are ± 0.8 dB and ± 2 degrees; whereas, the measured magnitude and phase balances' responses are ± 3 dB and ± 5 degrees. The

difference in phase angle between the two output ports obtained is close to 90^0 with respect to the input.

The return loss at port 1 and the isolation at port 3 are depicted in Figures 11 and 12 separately. The input and isolated ports obtained from the simulation results receive signals that are down by more than 14 and 17 dB individually; whereas, the magnitudes of the S_{11} and S_{31} obtained from the measurement are down by more than 10 dB and 11 dB separately. This implies that the manufactured prototype is not well-matched and isolated compared to the simulated model. This can be attributed to the mechanical implementation difficulties of the design. Moreover, changes in any of the design parameters could affect all of the S-parameters.

An important consideration in the choice and design of the hybrid coupler is the amount of positive group delay that it contributes. Simulated and measured group delays that are contributed by the proposed Lange coupler are plotted in Figure 13. As seen from the graph, the proposed coupler is generating an approximately $0.2 nS$ positive group delay at the frequency of interest. It should be clarified that as a drawback, this undesirable amount of positive group delay reduces the value of the NGD; thus, it has an impact on the performance of the final reactive non-Foster element. Table 1 shows the electrical specifications of the simulated and measured Lange coupler.

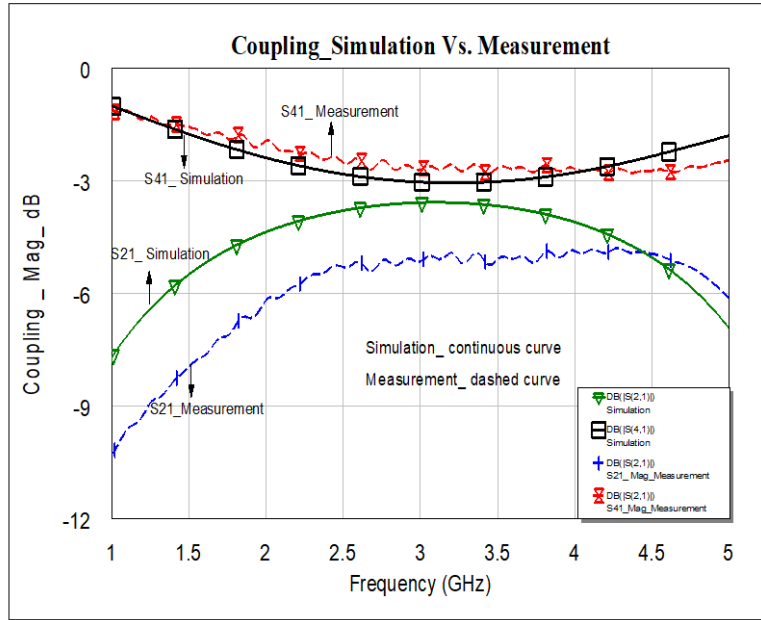


Figure 9: Coupling simulation and measurement results obtained from the Lange coupler

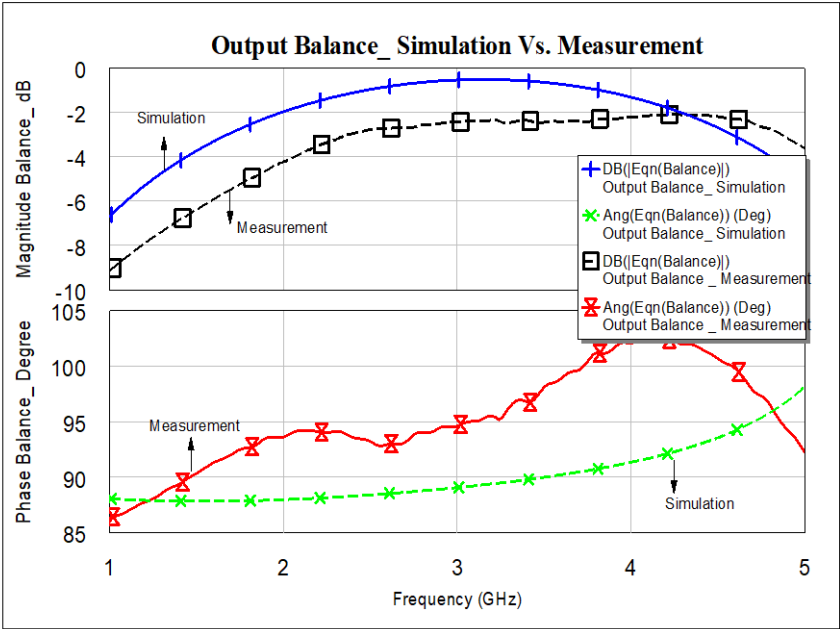


Figure 10: Output balance at ports 2 and 4 obtained from simulation and measurement

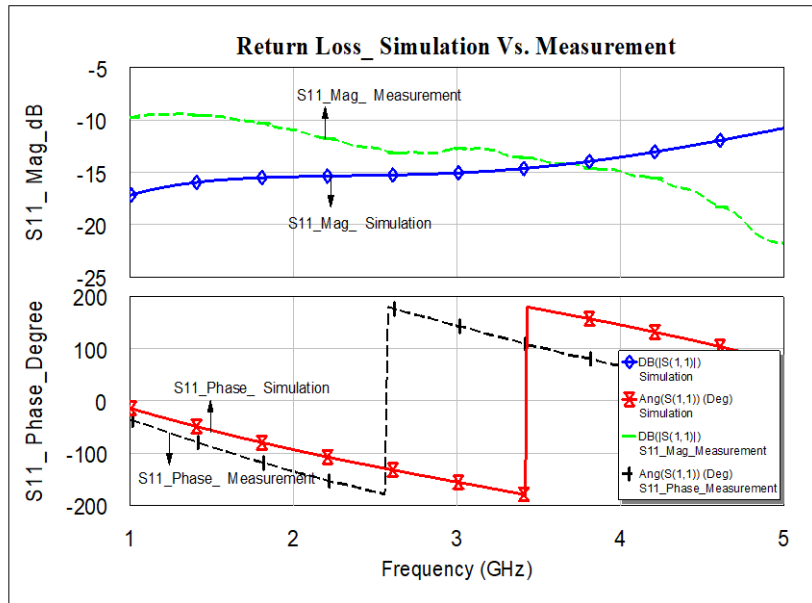


Figure 11: Return loss simulation and measurement results obtained from the Lange coupler

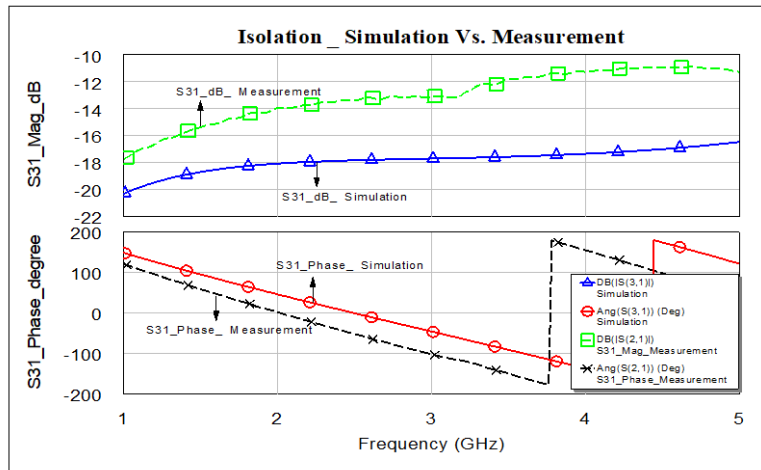


Figure 12: Isolation simulation and measurement results obtained from the Lange coupler

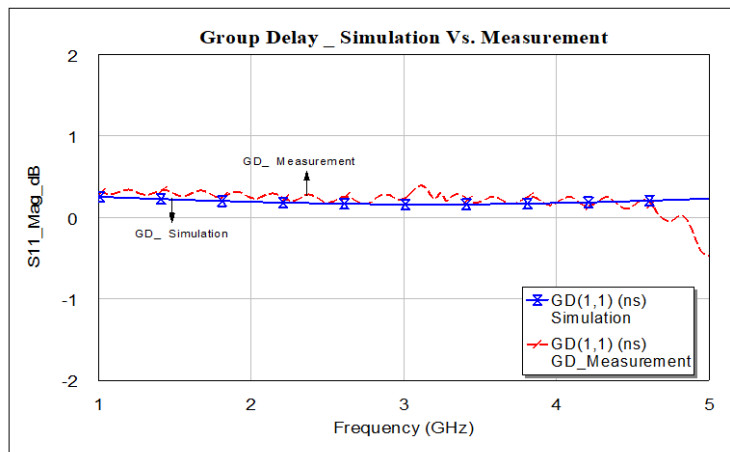


Figure 13: Group delay simulation and measurement results obtained from the Lange coupler

Table 1: Electrical specifications of the designed Lange coupler

Parameter	Frequency Range (GHz)	Simulation	Measurement
Coupling	2.0 to 4.0	3 ± 0.5 dB	3 ± 2 dB
Isolation		< -17 dB	< -11 dB
Return loss		< -14 dB	< -10 dB
Phase balance		90 ± 2 degrees	90 ± 5 degrees
Amplitude balance		± 0.8 dB	± 3 dB
Group delay		< 0.2 nS	< 0.2 nS

7. Conclusion

A systematic design methodology which starts by characterising the parasitic elements like the Lange coupler has been presented. Knowing how much positive group delay these components produce is necessary at the beginning. This helps in designing the NGD network using the method developed by (Almahroug., 2016), with a sufficient amount of negative group delay to overcompensate for the unwanted positive group delay produced by the parasitic elements. This systematic approach will provide a new route for synthesising networks with non-Foster behaviour over a limited frequency range.

8. Acknowledgement

The authors would like to acknowledge the help provided by Cadence in making available the AWR Design Environment used in the circuit simulations reported in this paper.

References

- [1] ALMAHROUG, A., FERESIDIS, A. & GARDNER, P. Non-Foster antenna matching networks using reflection-mode negative-group-delay networks. 2016 Loughborough Antennas & Propagation Conference (LAPC), 2016. IEEE, 1-4.
- [2] ALMAHROUG, A., FERESIDIS, A. & GARDNER, P. Antenna matching network using new class of non-Foster reactive elements. 2017 International Workshop on Electromagnetics: Applications and Student Innovation Competition, 2017. IEEE, 180-182.
- [3] Almahroug, A.A., Amer, B.M., Fheleboom, Z.H., Rehan, S., Omer, A.I. and Elgaber, A.D., 2021. Designing a reflection-type NGD network using open and short shunt stubs for wideband electrically small antennas. Scientific Journal of Applied Sciences of Sabratha University, pp.61-75.
- [4] D. M. Pozar, Microwave Engineering, 4th ed. New York, NY, USA: Wiley, 2012.

