ISSN: 2791-9293 Volume: 5 Issue: 1 Year: 2025

JOMCOM

Journal of Millimeterwave Communication, Optimization and Modelling

editor in chief

Assoc. Prof. M. Tahir GUNESER

CONTENT

Content i

About the Journal ii

Editor in Chief ii

Publisher ii

Aims & Scope iii

1. A Hybrid Security Approach to Nuclear Power Plants

Ebutalha Camadan, Beste Desticioğlu Taşdemir, Fikret Baykalı *1-6*

2. A Secure Lightweight Authentication Scheme for RFID Systems in IoT Environment

Md. Monzur Morshed , Hongnian Yu, Anthony S. Atkins *7-15*

3. Performance Of Grape Leaves Extract As Green Inhibitor On Corrosion Inhibition Of Mild Steel In Acidic Media

Noor Qasim Atiyah Alsaedi, Ali Al-Hashim, Hussien K.Abdul Zahra, Elaf Qasim Atiyah Alsaedi, Qasim Jaber Yousif *16-19*

4. The classification of pen ink aging by machine learning and deep learning technique using Raman spectrum

Kübra GÜRBÜZ GÖÇMEN, Mustafa Cem KASAPBAŞI, Sinan BOSNA *20-24*

5. A GaN-based Power Amplifier Module Design for 5G Base Stations

Burak Berk Türk, Furkan Hürcan, Hüseyin Şerif Savcı, Hakan Doğan, Serkan Şimşek *25-28*

About the Journal

Journal of Millimeterwave Communication, Optimization and Modelling (JOMCOM) published its first issue in 2021 and has been publishing since 2021. In JOMCOM two issues were published annually in June and December between 2021-2023, after 2024 the frequency is kept two times in a year but changed the publication times as February and August. Manuscripts in JOMCOM Journal reviewed of at least two referees among the referees who have at least doctorate level in their field. Uploading and publishing articles is free.

Journal of Millimeterwave Communication, Optimization and Modelling (JOMCOM) is an international online journal that is published 2 times in a year in English.

The purpose of JOMCOM is publishing the scientific research in various fields of communication. All kinds of transactions and the application about the journal can be made from **https://jomcom.org**
The scientific responsibility of articles belongs to the authors.
No fee is charged from the authors during the submission, evaluation and publication process.
ISSN: 2791-9293

Editor in Chief:

Communication Theory Section Editor

Artificial Intelligence Applications Section Editor

Proofreading Editor

PUBLISHER

Assoc. Prof. Muhammet Tahir GÜNEŞER

Aims & Scope

JOMCOM publishes original research and review articles in Communication Technologies, Innovative Technologies, and Systems within the broad field of Information and Communication Technology. The purpose of JOMCOM is to create value in the field by publishing original studies that contribute to the literature on wireless communication sciences and serve as a resource for both academia and industrial applications worldwide.

Communication Technologies: Journal of Millimeter-wave Communication, Optimization and Modelling (JOMCOM) publishes original research and review articles in Communication Technologies, Innovative Technologies, and Systems in the broad field of Information-Communication Technology. Purpose of JOMCOM; To create value in the field by publishing original studies that will contribute to the literature in wireless communication sciences and be a resource for academia and industrial application whole over the world. Besides, JOMCOM aims to bring the valuable work of researchers working in Communication studies to a broader audience all over the world. Readership of JOMCOM; valuable representatives of the wireless communication area, especially those who do academic studies in it, and those who do academic studies about modelling and system design and other interested parties. Since JOMCOM will appeal to a broader audience in article submissions, it prioritizes studies prepared in English.

Optimization and Modelling: Journal of Millimeter-wave Communication, Optimization and Modelling (JOMCOM), within the scope of Wireless Communication Sciences, publishes articles on communication theory and techniques, systems and networks, applications, development and regulatory policies, standards, and management techniques. It also reports experiences and experiments, best practices and solutions, lessons learned, and case studies. Additional studies on System Design, Modelling and Optimization. Subject areas of interest covered in the journal include the following but are not limited to:

5G-6G Technologies

Antenna Design

Circuits for Optical Communication Systems

Innovative Designs for Communications

Integrated Circuits for Communications

Optimization Methods on Engineering

RF Circuits

System Design

Wireless Communication

Realization of Microwave, Radar, and Sonar Systems

Realization of Antenna Systems

Communication Design Materials

Visible Light Communication

Fiber Optic Communication

A Hybrid Security Approach to Nuclear Power Plants

Received: 24 January 2024; Accepted: 8 March 2023 *Research Article*

Ebutalha CAMADAN
National Defence University
Ankara, Türkiye
ecamadan@kho.msu.edu.tr
ORCID: 0000-0001-7669-5601

Beste DESTİCİOĞLU TAŞDEMİR
National Defence University
Ankara, Türkiye
bdesticioglu@kho.msu.edu.tr
ORCID: 0000-0001-8321-4554

Fikret BAYKALI
National Defence University
Ankara, Türkiye
fbaykali@kho.msu.edu.tr
ORCID: 0000-0001-7518-8851

***Abstract*— It has recently been observed that the energy crisis in the countries has become more severe as a result of the experienced global crises. Similarly, in response to the rising demand for energy, countries have started to use alternative energy sources. Nuclear power plants are regarded as one of the best alternatives for producing energy, in part due to their high energy output and low carbon emissions. However, there are significant adverse effects on both human and environmental health from a potential radioactive leak. Hence, in order to produce nuclear energy safely, the necessary safety precautions should be taken. Providing cyber security has grown in importance as a result of the advancement of technology, both in nuclear power plants and other areas. The 2010 STUXNET attack is an illustration of how challenging and crucial it is to implement the necessary security measures against cyberattacks in nuclear power plants. It has been determined from studies in the literature that there are studies that look at environmental, occupational health and safety, and cyber security concerns separately in nuclear power plants, but that there isn't a study that appears at these issues simultaneously and comprehensively. In order to follow the studies on environmental safety, occupational health and safety, and cyber security in nuclear power plants in an integrated manner, a hybrid safety and security unit approach has been proposed in this study. Additionally, this research will examine the precautions that should be taken in a nuclear power plant for environmental safety, occupational health and safety, and especially cyber security.**

Keywords—cyber security, occupational health safety, nuclear security, nuclear power plants

I. INTRODUCTION

Traditional fossil fuel use is still widespread throughout the world [1]. One of the most important energy-political issues in almost all countries is the lack of environmentally friendly and green energy sources. These concerns are a crucial component of interstate competition and can also be addressed within the context of energy security. Another issue with shifting to alternative energy sources is energy efficiency. Reducing carbon emissions is one of the green movement's global effects. In this context, nuclear energy is being used as an alternative energy source by both developed and developing countries. Reducing carbon emissions is one of the green movement's global effects. In this context, nuclear energy is being utilized as an alternative energy source by both developed and developing countries. In fact, studies carried out in these countries have discovered a strong correlation between the use of nuclear power and the intention to reduce carbon emissions [2]. Traditional fossil fuels now make up a larger portion of the energy supply, which has ensured the establishment of certain standards for both cost and safety precautions. On the other hand, it is challenging to compile accurate statistics on this topic because nuclear accidents and nuclear attacks are extremely rare occurrences. Nuclear safety is a complex issue, even though investments in nuclear energy have emerged as sustainable investments in terms of lowering carbon emission rates and environmental costs. In order to assess the problem in an integrated framework, a hybrid security model can be applied to the safety of nuclear power plants to test the long-term viability of investments and security. The top 10 countries account for 84.6% of the world's nuclear energy use [3] and use generated electricity by nuclear power plants. There are significant flaws in the global supply of nuclear energy in terms of energy diversity. Competition between nations with nuclear energy and countries seeking access to it is triggered by this circumstance. Europe is a crucial region for competition. After the conflict between Russia and Ukraine in February 2022, there were serious issues with Europe's energy supply [4]. It has been noted that after this war, efforts to diversify the energy supply, particularly in Europe, have increased [5]. Nuclear investments in the Middle East are another source of international tension, in addition to Europe. Particularly, Israel and the United States view Iran's nuclear energy projects as a danger. As an example of a cyberattack on critical infrastructures, the STUXNET attack has also been cited in the literature [6]. The study will discuss the requirements of a common security architecture after discussing the issues of cyber security, environmental and occupational safety in nuclear power plants.

II. CYBER SECURITY

A. Cyberattack Types and Their Effects

The integrity of our information systems and communication infrastructures has historically and now being endangered by a variety of cyberattacks. Human life may not be affected by the exposure of institutions and organizations working in different areas to these cyberattacks. When this issue is considered in the context of nuclear power plants, it is found that it will have a significant negative impact on both human life and international security. We discuss cyber dangers and possible defenses against nuclear power facilities throughout our study. Within this data, if we want to bring together the basic components as a result of our literature research;

- Malware: This malicious software can be used to steal, change, corrupt, or delete data in information systems or communication infrastructures [7]. Typically, it is transferred between systems using USB or external

memory. Viruses and Trojans are the most harmful varieties of malware. The addition of viruses to applications or files allows them to replicate within the system, slowing it down and erasing data when activated by intended users. Trojans are frequently disseminated among systems by social engineering. It seeks to steal sensitive information while corrupting and destroying the systems it has infected.

- Ransomware: This kind of hack demands a ransom in exchange for decrypting the passwords and encrypting the data of the relevant systems [8].
- Social Engineering: Hackers aim to obtain confidential data by manipulating the emotions of company employees or target persons through emotional contact or persuasion [9].
- Phishing: Although it is an e-mail-based attack, it aims to capture the sensitive data of the target people with the links it publishes on e-mail attachments with the social engineering technique [10].
- DdoS: It prevents the relevant server or system from serving by subjecting a server or system serving on the network to data transmission over the capacity limits [11].
- Man-in-Middle Attack (MITM): It is a type of attack that allows obtaining or changing various data by listening to communications on the network [12].
- Password Attacks: It is the type of attack intended to enter the relevant system by guessing the passwords of users with full or limited authority on the system [13].
- Inside Threats: This type of threat refers to the data, system integrity or confidentiality of institutions or organizations; It includes the types of actions that can be done intentionally or unintentionally by the person authorized in the relevant system.

B. SCADA Systems in Nuclear Power Plants

These systems are used for data monitoring and control of industrial processes such as electricity networks, water networks, space stations and nuclear systems [14]. SCADA systems have used open access networks rather than closed access networks at some points to facilitate efficiency and business process monitoring. These types of networks have been exposed to a series of cyber-attacks over time. Intentional cyber-attacks by malicious personnel working in Nuclear Power Plants or unintentional cyber-attacks by an authorized personnel in the system working in these plants may cause a nuclear reactor to malfunction. In addition, this situation should not be considered as “inside threats” on the basis of personnel only. When we look at the world history, some cyber-attacks have been made on SCADA systems. These attacks are mentioned in the following articles.

- In 2010, SCADA systems of global oil, energy and petrochemical companies were targeted with a series of cyber attacks.
- In 2012, malware attacks were carried out on SCADA systems of Saudi Aramco, one of the largest energy systems [15].
- In 2013, a cyber-attack was carried out by Iranian hackers on a dam in New York [15].
- In the security report published by the German government in 2014, the SCADA systems of the German Steel Factory were the target of cyber-attacks [16].
- Due to the cyber-attack on electricity grids in Ukraine in 2015, approximately 250,000 people were left without electricity for a long time [17].
- According to FBI and Homeland Security reports, cyber-attacks were carried out on Nuclear Power Plants across the USA [14-18].

The most prominent cyber-attack against Nuclear Energy Stations worldwide and the most important cyber-attack against critical infrastructures has taken its place in the literature as STUXNET [6]. It was assumed that this attack damaged up to one-fifth of Iran's Nuclear Power Centrifuges. This attack can be considered as a cybersecurity wake-up call for SCADA systems.

STUXNET is a malicious computer worm created for the purpose of cyber-attack on Iranian nuclear facilities [19]. The main target of this worm is devices connected to centrifuges managed by PCLs via a USB stick connected to the SCADA system. STUXNET targets to listen to all nodes in the network by infecting Siemens SIMATIC Spen7 programs and tries to communicate with control servers by sending data in encrypted form [20]. As a result of communicating with the control servers, it disrupts the operation of the centrifuges.

C. Grouping of Cyber Attacks Against Nuclear Power Plants

The types of cyber threats mentioned in the Cyber Attack Types and Effects section of our study are based on two different points. These are internal and external sources. We think that threats from outside the institution are less likely to occur due to the fact that the SCADA systems used in the nuclear power station operate in closed networks and that the main factor is the unintentional intermediation of the personnel working in the institution. Moreover, it is difficult to state that personnel security and data security are separate structures. When we look at it from both perspectives, it will provide an important indicator in terms of reliability and testability that the unit inspecting these two units should look from a third perspective. Specifically, the variety of attacks on nuclear power plants in the face of a cyber incident can be examined under 5 different headings. The classification of cyber events and attack types that may occur in nuclear power plants is shown in Figure 1.

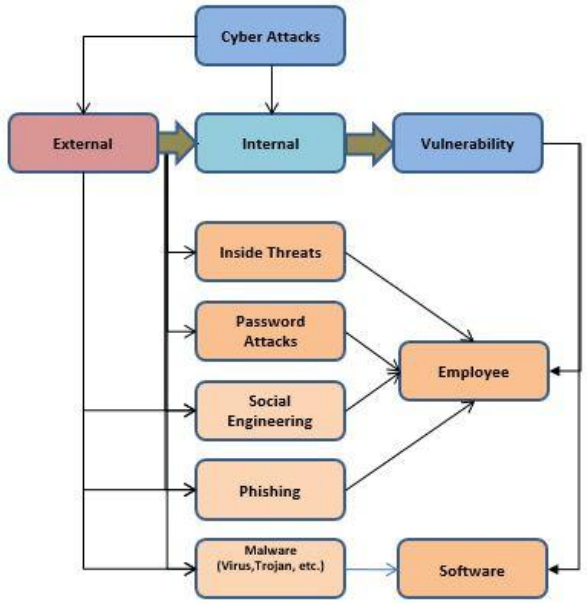

Fig. 1. Cyber Attack Types Reasons

III. Environmental and Occupational Safety in Nuclear Power Plants

The International Atomic Energy Agency emphasizes that nuclear energy obtained from nuclear reactors has an indispensable place among the energy sources used today [21]. On the other hand, nuclear energy production is still a controversial issue since the production of nuclear energy involves great risk [22]. There is a risk that a leak or an accident that may occur in nuclear power plants will affect large masses, primarily those working at the plant, including those living in the vicinity of the plant. An accident that may occur at a nuclear power plant can affect not only that country but also the surrounding countries . For example, the radiation emerged as a result of the Chernobyl Nuclear Power Plant accident that occurred in 1986 affected Ukraine, Belarus, Russia and Turkey as well [23].

When the accidents in nuclear power plants are examined, it is seen that most of them occur due to lack of safety precautions and human errors [24]. Therefore, in order to ensure both employee safety and environmental safety, it is necessary to take measures to prevent accidents in nuclear power plants. Proactive measures taken before an accident occurs are both more humane and cheaper [24]. Therefore, employers operating nuclear power plants should also take the necessary safety measures to prevent accidents. When it comes to measures to ensure environmental safety, the measures taken to prevent pollution of the air and water and the measures taken to prevent the destruction of the environment come to mind. However, an accident that may occur in nuclear power plants or any nuclear leakage that may occur in the power plant affects not only the personnel working at the power plant, but also the people living in the region where the nuclear power plant is located. Therefore, in addition to occupational health and safety measures in nuclear power plants, environmental safety measures should be taken to protect the personnel living in the region where the power plant is located. Some of the measures taken to ensure the occupational safety of employees in nuclear power plants are also effective in ensuring environmental safety.

IV. Security Unit Proposal of Nuclear Power Plants: Main Security Unit

The "Security Units" phases we recommend for the control and management of cyber-attacks against Nuclear Power Plants or physical and digital threats at the power plants are shown in Table I.

TABLE I. SCOPE OF UNITS

Phase	Units	Scope
1	Cyber Security	All digital devices at facility/ on network or not
2	Human Security	Ensuring the occupational health and safety of the employee and accident prevention
3	Environmental Security	Preventing the negative effects of nuclear materials on humans and the environment

A. Cyber Security Unit

This proposed security unit is responsible for the cyber security and policies of all digital devices in the Nuclear Power Plant, with or without access to the network at the power plant, operating in the power generation process at the plant. This unit performs the duties listed in the following items, respectively:

- Creating and managing the policy, strategy and training plans regarding the cyber security of the facility,
- To determine the cyber criticality level of the devices connected to the SCADA system in the facility and to follow up the authorization of the user personnel.
- To follow the records of the devices and storage units in the facility, to do the security tests and to follow the process,
- To provide training to the personnel working at the facility on the measures that can be taken against phishing and social engineering attacks,
- Creating password awareness by informing the personnel working at the facility about dictionary attacks and brute force attacks within the scope of password attacks,
- Within the scope of today's technology, viruses, Trojans, worms, etc. to follow the latest versions of malware types, to perform security tests on the devices on the independent closed network to be created of these versions, and to make a demo application by explaining the process to the personnel working in the facility,
- Identifying potential damage to occupational health and safety/environmental safety in case of a security weakness that may occur in the cyber security dimension and coordinating with these units.

B. Human Security Unit

Human Security Unit is responsible for protecting the health and safety of those working at the nuclear power plant. Therefore, employees should take the necessary precautions to work in a safe environment. In addition, it should determine

the necessary preventive actions to prevent leaks or accidents that may occur.

In this section, firstly, the occupational health and safety measures to be taken by Human Security Unit in order to create a safe working place in nuclear power plants are discussed, then the issues that need to be taken into account in establishing environmental safety are specified and the measures that are effective in establishing both occupational health and safety and environmental safety are determined. The activities to be carried out by the Human Security Unit in terms of occupational health and safety are as follows.

In nuclear power plants, it is necessary to prevent the danger from the source. If the hazard cannot be avoided at its source, workers should be provided with appropriate personal protective equipment [25]. Protective armor should be made of suitable materials and of sufficient thickness between the source that emits radiation and the working environment. Materials such as concrete and soil can be used to make this armor. Preventing radiation from its source in this way is important in terms of ensuring the safety of both the employees at the power plant and those working in the region where the power plant is located. If the amount of radiation cannot be reduced sufficiently with this measure, appropriate personal protective equipment should be provided to the employees and employees should be provided to work using these personal protective equipment. In addition, employees should be informed about radiation exposure and limit values and the use of personal protective equipment [25]. Personal protective equipment to be used by employees should be available against any risk of radioactive leakage. In nuclear power plants, it is necessary to reduce the risk of radiation emission by installing the necessary ventilation systems in the irradiated areas.

Only personnel trained in these areas should be allowed to work in areas with radiation. In addition, there should be a sufficient number of expert personnel in the power plant. Employees should be given training on issues such as hazards in the workplace, occupational health and safety within the periods specified in the legislation. Periodic health examination of the personnel to be employed in the nuclear power plant should be carried out before and after the work starts, every year. In addition, exposure measurements should be made with dosimeters in order to determine the radiation exposure of employees [24].

A "Radiation Protection Program" should be established for each nuclear power plant in order to ensure the safety of employees in case of any leakage. This document should include information such as radiation exposure and limit values, protective measures, and personal protective equipment used.

C. Environmental Security Unit

Identifying potential damage to occupational health and safety/environmental safety in case of a security weakness that may occur in the cyber security dimension and coordinating with these units.

The Environmental Security Unit should carry out the necessary studies in order to prevent the damage that the nuclear power plant may cause to the environment. Since some of the measures taken on occupational health and safety are also effective in ensuring environmental safety, this unit should work together with the Human Security Unit. In this section, both the studies that should be carried out by the Environmental Security Unit and the studies that should be carried out jointly by the Environmental Security Unit and the Human Security Unit are included.

It should be ensured that the water used in nuclear power plants to reduce the temperature is given to the environment after the necessary treatments are made. This unit should carry out the necessary studies in this regard [20].

When nuclear power plants, nuclear waste storage facilities, nuclear fuel storage facilities, waste processing facilities do not take the necessary precautions, radioactive materials that will threaten the environment and human health pollute the environment. The main purpose of nuclear safety measures is to ensure that any radioactive leakage occurs inside the building (shelter/protection building), or to ensure that the radioactive release takes place under the allowable limits and in a controlled manner in case of an accident [27].

Therefore, in the event of a leak in nuclear power plants, necessary precautions should be taken to prevent the release of radioactive material to the environment. Starting from the establishment phase of nuclear power plants, risk analyzes should be carried out by taking into account the events and accidents that may occur, the causes and probabilities of these accidents. Necessary protective measures should be taken for activities with high risks. Risk analyzes should be updated considering the risks that may arise in any change in the materials used in the plant or in the production process [28]. In the prepared risk analysis, both risks related to environmental safety and occupational health and safety of the employee and the safety of the plant should be evaluated. The STUXNET attack that took place in Iran showed how important it is to ensure cyber security at nuclear power plants. Therefore, in the risk assessment, suggestions should be included in the evaluation of the risks for cyber attacks and the studies to be done to prevent these attacks. As a result, in the risk assessment of the nuclear power plant, risks related to cyber security should be included in addition to the risks related to the health and safety of the employee and environmental safety. In addition, an emergency plan should be prepared for nuclear power plants and an exercise should be carried out at least once a year [26].

D. Main Security Unit

This proposed security unit represents the main security unit responsible for cyber, human and environmental security sub-units. In scope, it plays a role in the main authority of security and policies for which sub-security units are responsible. The main security unit fulfills the responsibilities described in the following items:

TABLE II. RESPONSIBILITIES OF MAIN SECURITY UNIT

Security Units	Responsibilities
Main Security Unit	-To create and implement the policy, strategy and training plans of the cyber, human and environmental security units -Following the resolution process of the relevant units in case of security breaches that may occur in the facility and ensuring its implementation -To identify current security problems worldwide and to take precautions by informing the relevant units -To monitor the network and communication infrastructure and to audit the Cyber Security unit by performing cyber vulnerability tests -To identify the threats that may occur within the scope of occupational health and safety and to audit the Human Security unit by making risk analysis. -Identifying threats within the scope of environmental conditions and security and auditing the Environmental security unit by making risk analysis - Identifying common openings for Cyber, Human and Environmental units and analyzing the behavior of these units as feedback.

TABLE III. RESPONSIBILITIES OF MAIN SECURITY SUB-UNIT CYBER+HUMAN SECURITY

Main Security Sub-Unit	Responsibilities
Cyber+ Human Security	-Detecting and controlling the common threats to cyber infrastructure and human health in case of possible cyber security attacks -Identifying situations that may threaten the health of the personnel working in the facility and ensuring the sustainability of the cyber infrastructure that may be affected in this context, with personnel redundancy.

TABLE IV. RESPONSIBILITIES OF MAIN SECURITY SUB-UNIT CYBER+ENVIRONMENTAL SECURITY

Main Security Sub-Unit	Responsibilities
Cyber+ Environmental Security	-Detecting and controlling the common threats to cyber infrastructure and environmental health in case of possible cyber security attacks -To determine the harmful situations that may occur for the environmental health of the facility and to ensure the continuity of the cyber infrastructure that may be affected as a result of this situation.

TABLE V. RESPONSIBILITIES OF MAIN SECURITY SUB-UNIT HUMAN+ENVIRONMENTAL SECURITY

Main Security Sub-Unit	Responsibilities
Human+ Environmental Security	-Reducing radiation emission by covering the surrounding of the reactor with an absorbing material -Reducing the amount of radioactive material released to the environment by establishing appropriate ventilation installations -In the risk assessment prepared for the nuclear power plant, the assessment of the risks related to the environmental effects of an accident or nuclear release

V. CONCLUSION

In this study, the "Main Security" unit was proposed within the scope of possible violations and attacks in response to cyber, human and environmental threats faced by nuclear facilities, and the type of joint solutions to overcome these situations with coordination between units was investigated. We consider that in case of possible cyber, human and environmental attacks, only cyber infrastructure and communication deterioration, human health deterioration and environmental health deterioration will not be possible. Therefore, it will be possible to overcome the threats that may occur in the facility and the attacks against the facility by ensuring that these recommended units work together. Cyber security, environmental security and occupational health and safety at nuclear power plants are carried out by different departments. However, in nuclear power plants, cyber security, occupational health and safety and environmental safety are in interaction with each other, and it is seen that risks are prevented by taking common precautions. In this study, common measures taken to ensure cyber security, occupational health and safety and environmental security were examined. For this reason, it is thought that effective security measures will be taken by establishing a common security unit that deals with cyber security, occupational health and safety and environmental safety in nuclear power plants, and thus nuclear power plants will operate more safely. In the final analysis, the intricate nature of the security of nuclear power plants necessitates the security architecture to be provided with control units that monitor and balance each other. The control unit, which constitutes the basic proposition of the study, also describes a theoretical approach produced against this problematic.

The necessity for the security of nuclear power plants to be in a multidimensional and complex architecture is a natural consequence of nuclear competition. On the other hand, the fact that physical/virtual attacks such as nuclear terrorism have not yet been experienced shows that new studies will be needed on this subject.

REFERENCES

[1] M. Naimoğlu, “The impact of nuclear energy use, energy prices and energy imports on CO2 emissions: Evidence from energy importer emerging economies which use nuclear energy,” Journal of Cleaner Production, vol. 373, p. 133937, 2022.

[2] A. Azam, M. Rafiq, M. Shafique & J. Yuan, “Towards achieving environmental sustainability: the role of nuclear energy, renewable energy, and ICT in the top-five carbon emitting countries,” Frontiers in Energy Research, vol. 9, pp.1-11, 2022.

[3] M. Sadiq, R. Shinwari, F. Wen, M. Usman, S.T. Hassan & F. Taghizadeh-Hesary, “Do globalization and nuclear energy intensify the environmental costs in top nuclear energy-consuming countries?” Progress in Nuclear Energy, vol. 156, p.104533, 2023.

[4] M. Umar, Y. Riaz, & I. Yousaf, “Impact of Russian-Ukraine war on clean energy, conventional energy, and metal markets: Evidence from event study approach,” Resources Policy, vol. 79, p.102966, 2022.

[5] B. Steffen & A. Patt, “A historical turning point? Early evidence on how the Russia-Ukraine war changes public support for clean energy policies.” Energy Research & Social Science, vol. 91, p.102758, 2022.

[6] S.R. Ameli, H. Hosseini, & F. Noori, “Militarization of Cyberspace, Changing Aspects of War in the 21st Century: The Case of Stuxnet" Against Iran,” Iranian Review of Foreign Affairs, vol. 10(29), pp.99-136, 2019.

[7] Alanazi, M., Mahmood, A., & Chowdhury, M. J. M. (2022). SCADA vulnerabilities and attacks: A review of the state ‐ of ‐ the ‐ art and open issues. Computers & Security, 125, 103028.

[8] Zimba, A., Wang, Z., & Chen, H. (2018). Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. ICT Express, 4(1), 14–18.

[9] Upadhyay, D., & Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. Computers & Security, 89, 101666.

[10] Nazir, S., Patel, S., & Patel, D. R. (2017). Assessing and augmenting SCADA cyber security: A survey of techniques. Computers & Security, 70, 436–454.

[11] Polat, H., Turkoglu, M., Polat, O., & Sengur, A. (2022). A novel approach for accurate detection of the DDoS attacks in SDN-based SCADA systems based on deep recurrent neural networks. Expert Systems With Applications, 197, 116748.

[12] Rodofile, N. R., Radke, K., & Foo, E. (2019). Extending the cyber-attack landscape for SCADA-based critical infrastructure. International Journal of Critical Infrastructure Protection, 25, 14–35.

[13] Upadhyay, D., & Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. Computers & Security, 89, 101666.

[14] S. Ghosh, & S. Sampalli, "A Survey of Security in SCADA Networks: Current Issues and Future Challenges," IEEE Access, vol. 7, pp.135812–135831, 2019.

[15] Bronk, C., & Tikk-Ringas, E. (2013). The Cyber Attack on Saudi Aramco. In Survival (Vol. 55, Issue 2, pp. 81–96). Taylor & Francis.

[16] Lee, R. M., Assante, M. J., & Conway, T. (2014). German steel mill cyber attack. Industrial Control Systems, 30(62), 1-15.

[17] Case, D. U. (2016). Analysis of the cyber attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC), 388, 1-29

[18] Department of Homeland Security and The Federal Bureau of Investigation, Russian government cyber activity targeting energy and other critical infrastructure sectors, Tech. Rep. TA18-074A, Mar. 2018, pp. 1–18.

[19] Homay, A., Chrysoulas, C., Boudani, B. E., Da Cunha Sargedas De Sousa, M. J., & Wollschlaeger, M. (2020). A security and authentication layer for SCADA/DCS applications. Microprocessors and Microsystems, 103479.

[20] Z. Masood, R. Samar, & M.A.Z. Raja, "Design of a mathematical model for the Stuxnet virus in a network of critical control infrastructure," Computers &Amp; Security, vol.87, p.101565, 2019.

[21] World Nuclear Association, https://world-nuclear.org/ (10.01.2023)

[22] S. Gandhi & J. Kang, "Nuclear Safety and Nuclear Security Synergy," Annals of Nuclear Energy, vol.60, pp.357-361, 2013.

[23] W. Hallenbeck, Radiation Protection. Reported thus far are 237 cases of acute radiation sickness and 31 deaths. CRC Press. s. 15. 1994.

[24] Kahraman, Z. & Yürüten Özdemir, K. "Nükleer Enerjinin Riskleri ve Nükleer Santrallerde İş Sağlığı ve Güvenliği," Karaelmas Journal of Occupational Health and Safety, vol. 6(1), pp.53-65, 2022.

[25] B. Desticioğlu & B. Özyörük, "Türkiye'de Sektörel Bazda Gelecek Yıllar için İş Kazası Sayısı Tahmini," in Bilimsel Araştırmalar Kitabı 2022: İktisadi ve İdari Bilimler, Ed. A. Yalçın, Ankara: Akademisyen Yayınevi, 2018, pp.143-156.

[26] Resmi Gazete, "6331 Sayılı İş Sağlığı ve Güvenliği Kanunu," https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6331.pdf (10.01.2023).

[27] Türkiye Enerji Nükleer ve Maden Araştırma Kurumu TENMAK, https://www.tenmak.gov.tr/2016-06-09-00-43-55/135-gunumuzde-nukleer-enerji-rapor/835-bolum-05-nukleer-guvenlik.html (10.01.2023).

[28] H. George-Williams, M. Lee and E. Patelli, "Probabilistic Risk Assessment of Station Blackouts in Nuclear Power Plants," in IEEE Transactions on Reliability, vol. 67, no. 2, pp. 494-512, June 2018.

A Secure Lightweight Authentication Scheme for RFID Systems in IoT Environment

Received: 30 January 2023; Accepted: 10 March 2023 *Research Article*

Md. Monzur Morshed
Department of Computer Science and Engineering
Daffodil International Univerrsity
Dhaka, Bangladesh
monjur.morshed@diu.edu.bd

Hongnian Yu
School of Computing Engineering and the Built Environment
Edinburgh Napier University
Edinburgh, UK
hongnianyu@uic.edu.cn
0000-0003-2894-2086

Anthony S. Atkins
School of Computing and Digital Technologies Staffordshire University
Stafford, UK
a.s.atkins@staffs.ac.uk
0000-0002-8447-4822

***Abstract*— Radio Frequency Identification (RFID) technology is suitable for IoT applications. RFID is cheap and light weight and hence it is very popular in IoT technology. The concern of research community is the privacy and security issue of RFID system. Due to low storages of RID tag it a challenging research problem to ensure privacy and security such as data visibility, loss, modification, eavesdrop etc. In this paper we propose a new RFID authentication protocol for RFID system. It ensures privacy and security in IOT environment in a more efficient way. To ensure better security we use a different password for each tag and it changes after each authentication process. It also can protect from an unexpected lack of synchronization in case an incomplete authentication is held for any unwanted problem in authentication phase. The proposed protocol shows some relatively superior performance in some aspects of computation and storages.**

Keywords*— *RFID security, IoT, privacy, recovery, authentication

I. INTRODUCTION (*HEADING 1*)

Various types of sensors and RFID technology are the essential component in the present deployment of IoT. RFID tags are used in many applications now a days. It is used in automation of automobiles, logistics management, toll collection in roads, animal tracking, etc [1][2]. The RFID tag is used as Electronic Product Code (EPC). It is standardized by EPCglobal Inc [3]. Due to thee small size and low-cost of the RFID tag it is used to identify items or objects automatically. An RFID system typically consists of three components. These are tag, reader and database in the back-end[4].

There are two types of RFID tags: active and passive. Typically passive tags are inexpensive where as active tag contains batteries to power their transmission. An RFID tag comprises a unique code as identity which can be used to identify any item or object. Using this unique code in an RFID tag it is possible to track the tag uniquely. Typically the code and information in RFID tags are transmitted in plaintext. In IoT environment the information in the tags may contain sensitive data. But without proper security protections this system may be less attractive for many practical applications [1]. The main challenge to ensure security is that, employment of traditional cryptography is not applicable in a low-cost, small size and lightweight passive RFID tags[5].

The paper aims the goal to develop a new scheme to solve these issues and to offer an efficient and secure protocol for RFID systems which can overcome from de-synchronization for any incomplete authentication and abnormal termination.

This paper aims to develop a new authentication scheme using a password that is changed after each authentication. The identifier and secret password are exchanged with lightweight encryption and light-weight hash function using random numbers so that the code and secret transmitted by the RFID systems are anonymous. In this way the scheme aims to ensure the privacy and security of RFID systems of the issues outlined above. It specially aims to ensure location privacy and recovery in case of desynchronization discussed above with less computation. The main contributions of the proposed scheme are:

(1) To develop a secure and light weight authentication scheme for RFID system

(2) Resist all known attacks like tracing, impersonation, information leakage etc.

(3) RFID tag identifier and secret password are always encrypted and hashed so that tag ID is never disclosed.

(4) To ensure less computation, storage and lower communication cost.

(5) To ensure synchronization in the case of communication failure.

The rest of the paper is organized as in following sections. In Section II the model for security and privacy for RFID systems and performance criteria are explained for the RFID systems. In Section III related works are outlined. Section IV presented the proposed protocol. In this Section the protocol is also explained together with a recovery example in the case of abnormal termination of the authentication. The performance, privacy and security of the scheme is evaluated in Section V. In Section VI the analysis and the result of simulation are outlined. The conclusion is placed finally in section VII.

II. PRIVACY AND SECURITY OBJECTIVES FOR RFID

To ensure privacy or security of the contents of the RFID tag there are several goals are identified. The objective of security protocols are to keep the data secret and to protect data during the transmission between the tag and the reader from tentative attacks.

- **Information leakage:** Every tag in an RFID system has a unique code and other data that are transmitted to the system. Due to this unique code it can be easily identified and the data may be leaked. To ensure the protection from the leakage of information of both identity and data, an RFID system requires security protection so that unauthorized person or adversary cannot access any information from the tag.
- **Traceability and Location privacy:** Sometimes it is enough to harm if any how it can be tracked or linked with any person to a tag. When a transmitter sends any fixed response to a receiver, an attacker may differentiate and identify the response. After this it may track the location of the user.
- **Mutual authentication**: Authentication of the tag and the reader with each other is done by transmitting their code and other secret with each other. If they are matched with their own information then they authenticate each other.
- **Impersonation and Forward security**: An adversary may collect the code and data during transmission between the tag and the reader. If any data can be identified it can be used to impersonate the tag to exploit in future.
- **Message Interception or denial of service (DoS):** An adversary sometimes may initiate to prevent communication between the tag and the reader. If the adversary is successful to interfere the transmission then it can cause de-synchronization between the server and the tag.

III. RELATED WORKS

There are different types of RFID authentication schemes to ensure privacy and security in an RFID system. Many schemes work with static code and few other work with varying code or secret.

In [6, 7, 8] the authors proposed various protocols that work with static codes to ensure security or privacy. The advantage of these schemes in pervasive computing environment is that it is easy to work and manage since it does not face any synchronization challenges. Molnar et al. [6] presented a novel authentication scheme to implement in a library system. To ensure anonymity and privacy it utilizes a pseudorandom number and secret key shared by the tag and the reader. In this scheme the code and the secret are fixed and the random number transmitted in plain text which can be a cause to break the privacy of the tag by the adversary.

In [7] Rhee et al. also outlines a mutual RFID authentication protocol (CRAP). This protocol also used fixed code or identifier suitable in IoT pervasive computing. However, hash functions computations makes the scheme inefficient for a large number of tags in pervasive computing of IoT.

In [8] Choi et al. presented another protocol with static identifier which is hash based low-cost and sized authentication scheme. It is also suitable for pervasive environment like IoT. This scheme is not appropriate to protect from impersonation attack and traceability attack for its counter parameter used in the scheme [9].

Ohkubo et al. [10] presented a privacy scheme for RFID system using a hash chain (HC) method. The method utilized two one-way hash functions to ensure privacy and security. However, it is not suitable in practical situation due to the uses of a large number of hash chains in back-end database.

To ensure the privacy and security of the RFID systems in an effective manner varying coder or secrets are used in some authentication schemes. This paper listed few of the schemes using varying codes and secret for the authentication process presented as follows:

Few of early researchers have also proposed authentication schemes to ensure privacy and security of RFID systems using varying codes or secrets [11, 12, 13, 14]. These are protected against many attacks. Due to varying codes they include the recovery process for accidental de-synchronization or incomplete authentication process. However, the hash function is used from the identifier only. If any authentication phase is incomplete, an unauthorized user can take the responses for the next phase to break the security. Hence the unauthorized user can intentionally use the collected information to use for man-in-the middle attack and it can also be a threat for location privacy.

Chien and Chen [11] presented a mutual authentication protocol to ensure protection from a replay attack. To ensure synchronization this protocol uses a database to store new and previous key values of the tag which can prevent from a DoS attack. The authentication key and access keys are always updated and hence prevent a traceability. However, this protocol is vulnerable to forward and backward traceability. If an adversary can capture the information from a tag it can trace the previous interactions of the tag from previous transmission and the identifier of the tag. By using the immediate previous transaction and identifier it may be possible to recognise any transaction in future.

Another hash-based identifier variation scheme (HIDV) is presented by Henrici et al. [12] which utilizes a hash function to prevent location privacy by altering the identifier after each successful session. However, if any session is terminated incompletely an adversary can use the same hashed response for which it may open the risk for impersonation attack say spoofing.

Lee et al. [13] also proposed an authentication scheme that improves and simplifies the HIDV scheme in security and efficiency. It also has the same limitation as in HIDV scheme that a tag always uses the same hashed response before the next authentication allows tracking the tag.

Dimitriou [15] introduced an RFID authentication scheme to protect the privacy and security. It also protects against cloning of the tag. This scheme also uses the hash function of the id to a reader and it maintains scalability at the server. The back-end server replies the message with the altered new identifier to the tag after receiving the response from the tag. This scheme also has the problem of tracking due to the fact that between valid sessions, the tag id remains the same.

Song and Mitchell [14] presented an authentication scheme for RFID system and also introduced a protocol for an ownership transfer [16] to prevent from all attacks. These protocols show better efficiency in terms of storage and computation. However these are vulnerable to impersonation attack for both the tag side and reader side.

Hoque et al. [17] introduced an authentication protocol that also supports both security, privacy and recovery of id in RFID systems. The protocol also can synchronize the value of tags and readers and thus ensures robustness. This protocol is expensive in as it requires a large number of hash functions and computations.

Cai et al. [18] presented an enhanced version of authentication protocol described in [8] to overcome the limitations by retaining all the security and privacy protections. The modified protocol also uses almost similar storage and computation requirements as in the previous protocol.

Shafiq et al.[19] proposed a new protocol for varying identifier, random number and low-cost operation like XOR, Rot and new function Rank to guarantee privacy and security for the RFID tag and reader. However, the IDS information is transmitted in plaintext which may be tracked by an unauthorized user.

Peris-Lopez et al. in [20–22] proposed various lightweight protocols RFID systems to ensure privacy and security. The protocols outlined in these papers are LMAP, *M*2AP, and EMAP. The protocols are efficient and utilized low-cost operations like bitwise OR, XOR, and *sum mod* operations. However, these protocols are also vulnerable at security attack and de-synchronization [23, 24].

In LPCP [25], an enhanced security scheme of RAPP [26] is proposed to overcome the weakness in security. To improve security performance, the protocol also uses a mechanism of secret key backup. However, the RAPP protocol is still insecure against de-synchronization attacks.

In [27], another new authentication scheme for RFID is proposed. The Ultra-lightweight protocol SLAP uses simple bitwise XOR, rotate with left circular Rot$(\cdot,\cdot)$ and $Con(\cdot,\cdot)$ for conversion operations. For implementation of these operations the inexpensive passive tags were appropriate. However, the protocol is vulnerable against various attacks like traceability, de-synchronization and replay attacks.

Liu et al. [28] utilizes Shamir's (2, n) ultra lightweight scheme UMAPSS for RFID authentication. The scheme can protect the system from the known security problem efficiently.

In [29], a lightweight authentication protocol IOLAS for passive RFID tags is introduced. The scheme can ensure all known security protection efficiently.

In [30] Xiao et al. presented a block cipher-based RFID authentication protocol named LRSAS. The author claimed The protocol guarantees all known security protection efficiently but Trinh et al. [31] reported that the protocol is susceptible to de-synchronization and secret disclosure attacks.

Some other schemes [32][33][34],[35] and [36] use almost similar lightweight encryption and showed relatively better performance but with a cost of compromising few security protections.

An essential research objective is to formulate a security scheme for RFID technology in IoT environment that addresses the issues and solve these problems efficiently with limited capability in computation and storage of an RFID tag.

IV. Our Contribution: A Secure Lightweight Authentication Scheme (SLAS)

In this section, a new scheme (SLAS) is proposed. The notations used in this protocol are as follows:

Notations

h hash function
l The length
r_1 First Random number
r_2 Second Random number
ID Tag Code / Identifier
X variable Secret
S Secret number
$A = A_L || A_R$
$B = B_L || B_R$
$\oplus$ Bitwise XOR
$\|$ Concatenation
$\leftarrow$ Assignment

Tag Initialization

Tag: Each tag contains three fields:
ID: Tag Code/ Identifier
X: Variable Secret
S: Helping Secret

Reader: Reader contains no field. It uses the data from database.

Database Initialization: The database has four fields:

ID: Tag Code/ identifier
X: Variable Secret
S: Helping Secret
X_{prev}: *X* in previous phase

Operations in SLAS Scheme

If a tag approaches within the range of any reader, the session of authentication scheme is initiated. The scheme is outlined in Fig.1. The steps in the scheme are as follows.

Step 1: A reader generates the first random number (r_1) and transmits a request with it to the tag.

Step 2: With the response from the reader the tag generates second random number (r_2).

It then computes

$$A \leftarrow h(ID \| r_1 \| r_2)$$
$$C \leftarrow X \oplus r_2$$
$$P \leftarrow S \oplus C$$

Step 3: The tag replies with the values A_L, *C* and *P* to the targeted reader.

The reader transmits this data to its database.

Step 4. The database side then computes

$$P' \leftarrow S \oplus C \quad \text{for all S}$$
$$if \quad P = P' \quad Computes$$

$r_2 \leftarrow X \oplus C$ and $A' \leftarrow h(ID \| r_1 \| r_2)$

if $A'_L = A_L$

ID of *the* tag is authenticated.

For next session

$X_{prev} \leftarrow X$ *and*

$X \leftarrow h(X, r_2)$.

$B \leftarrow h(ID \| X \| r_1 \| r_2)$

else *if* $A'_L \neq A_L$

Computes

$r_2 \leftarrow X_{prev} \oplus C$ and $A' \leftarrow h(ID \| r_1 \| r_2)$

if $A'_L = A_L$

ID of *the* tag is authenticated.

For next session

$X_{prev} \leftarrow X_{prev}$ *and*

$X \leftarrow h(X_{prev}, r_2)$

$B \leftarrow h(ID \| X \| r_1 \| r_2)$

else ignore the message and

Computes $B \leftarrow unknown$

Step 5. The reader replies with B_R to its tag.

6. *T*he tag then performs the following operations:

$XT \leftarrow h(X, r_2)$ $B' \leftarrow h(ID \| XT \| r_1 \| r_2)$

if $B'_R = B_R$ the tag authenticates and updates

$X \leftarrow XT$

Database *ID, S, X, X_{prev}*		Reader		Tag *ID, X, S*
			Request, r_1 →	
Computes for all S $P' \leftarrow S \oplus C$ *if* $P = P'$ *Computes* $r_2 \leftarrow X \oplus C$ and $A' \leftarrow h(ID \| r_1 \| r_2)$	A_L, C, P ←		A_L, C, P ←	Generate random number r_2 $A \leftarrow h(ID \| r_1 \| r_2)$ $C \leftarrow X \oplus r_2$ $P \leftarrow S \oplus C$
if $A'_L = A_L$ *ID* of *the* tag is authenticated. For next session $X_{prev} \leftarrow X$ *and* $X \leftarrow h(X, r_2)$. $B \leftarrow h(ID \| X \| r_1 \| r_2)$ else *if* $A'_L \neq A_L$ Computes $r_2 \leftarrow X_{prev} \oplus C$ and $A' \leftarrow h(ID \| r_1 \| r_2)$ *if* $A'_L = A_L$ *ID* of *the* tag is authenticated. For next session $X_{prev} \leftarrow X_{prev}$ *and* $X \leftarrow h(X_{prev}, r_2)$ $B \leftarrow h(ID \| X \| r_1 \| r_2)$ else ignore the message and Computes $B \leftarrow unknown$	B_R →		B_R →	$XT \leftarrow h(X, r_2)$ $B' \leftarrow h(ID \| XT \| r_1 \| r_2)$ *if* $B'_R = B_R$ then the tag authenticates and perform $X \leftarrow XT$

Fig. 2. Proposed SLAS Scheme

V. ANALYSIS AND EVALUATION

In the process of evaluation of the proposed scheme the privacy, security and efficiency are considered for analysis. It was a challenging task to select various existing authentication schemes to compare performance with tour proposed SLAS scheme. The proposed scheme SLAS has been compared with various existing and relatively recent protocols having good performance ultra-lightweight RFID authentication schemes. These selected scheme are URASP [8], ESRAS[19], IOLAS [29], RSAS [30], RAPP [31],RAPLT [32], SLAP [38], LMAP [41], *M*2AP [42], EMAP [43], LPCP [44], David–Prasad [54], RRAP [56], and URMAP [58]. Most of these protocols require relatively lower cost and storage in comparison to other protocols those are not selected.

A. ANALYSIS OF PRIVACY AND SECURITY

To evaluate the privacy and security we selected the threats [19] discussed in section II. It is shown in TABLE II.

Information leakage: In this protocol the information is either transmitted in a hash function. Without knowing the value of ID, X, S an adversary cannot authenticate. The value of ID is always hashed with a function when transmitted.

$$A \leftarrow h(ID \parallel r_1 \parallel r_2)$$
$$C \leftarrow X \oplus r_2$$
$$P \leftarrow S \oplus C$$

The value of X and S are transmitted using XOR but the value of X is updated by a hash function after every authentication phase.

$$X \leftarrow h(X, r_2)$$

The combination of r1 and r2 with X, S and ID produces an unpredictable response so that the adversary cannot access any information. In can only guess with a costly computation with negligible probability $\frac{1}{2^l}$.

Mutual authentication: In the proposed mutual authentication with the tag and reader is done by a very strict privacy and security mechanism. The reader server authenticate by the secure transmitted message part by comparing the expression $A'_L \neq A_L$

The tag also authenticate by the secure transmitted message part by comparing the expression $B'_R = B_R$

In this way the mutual authentication is established in the tag and the reader in a secure way.

Location privacy: The information transmitted by A cannot be tracked with any targeted tag. Two new random numbers r1, r2 are generated in every authentication process and the value of X also updated by using random number and hash function as follows:

$$A \leftarrow h(ID \parallel r_1 \parallel r_2)$$
$$C \leftarrow X \oplus r_2$$
$$P \leftarrow S \oplus C$$
$$X \leftarrow h(X, r_2)$$

In a simulation program the anonymity of the response are tested and found the tracking and location privacy breaking is not possible. Even if an adversary sends the same random number r1 many times it ensures anonymity in each session by transmitting new values of r2 and X.

Impersonation and Forward security: The scheme follows a complete challenge-response method using mutual authentication. Without accessing the value of tag code (ID), two secrets X and S an adversary cannot impersonate.

$$A \leftarrow h(ID \parallel r_1 \parallel r_2)$$

In each session the tag and reader generates new responses of A and B using two fresh random numbers. These are fully indistinguishable from other response in other sessions hence he impersonation are not possible and forward security is ensured.

$$B' \leftarrow h(ID \parallel XT \parallel r_1 \parallel r_2)$$

Message interception: The scheme can recover from the abnormal interruption can be synchronized automatically. If the last transmission is interrupted then in the subsequent authentication session the database side can use the older value Xprev using random numbers to authenticate and synchronous the system.

$$X \leftarrow h(X_{prev}, r_2)$$
$$B \leftarrow h(ID \parallel X \parallel r_1 \parallel r_2)$$

Forward security: The proposed protocol uses varying secret in each successful new session. So the scheme ensures the privacy and security of the past communications in case the tag is compromised by an unauthorized reader. It cannot discover previous secret and random number. Moreover the ID is never transmitted in plain text. Also the adversary cannot get access of future data and secret.

B. EFFICIENCY ANALYSIS

In this paper the communication cost, computation cost and storage cost were chosen for analysis of efficiency. The low-cost small sized tag has very limited computational and communication ability. The objective of the scheme is to minimize storage and computational and communication capacity requirements. By considering these issues the proposed SLAS scheme gives the performance as in Table II.

Computation cost: The proposed scheme does not use CRC, traditional high cost encryptions or decryptions. It uses simple bitwise XOR and lightweight hash function.

Communication cost: Another objective of the RFID authentication scheme is to reduce the communication cost sent by the tag. It denotes the number of transmitted data from the tag side in each authentication phase. It is assumed that all the field have same length of L. In our proposed scheme the communication cost from tag is 2.5L.

Storage Costs: For identification and authentication purpose the tag stores ID, secret and some other shared information. The objective is to optimize the memory space in tag by ensuring all the security issues discussed. The proposed scheme requires a total three parameters including its ID and two secrets X and S. So the storage size requirement in the tag is 3L.Tt requires relatively less storage in tag and in database side than some schemes and offers protection from

all threats discussed in section II. The storage cost in the database side is 4L.

TABLE I. SECURITY AND PRIVACY COMPARISON AUTHENTICATION SCHEMES.

Scheme	Mutual authentication	Forward Security	Tracking Prevention	Synchronization	Leakage Protection	Diffusion function Security
URASP [8]	*Yes*	X	*Yes*	*Yes*	*Yes*	*Yes*
IOLAS [29]	*Yes*	*Yes*	X	*Yes*	X	X
LRSAS [30]	*Yes*	*Yes*	*No*	*Yes*	X	X
RAPP [31]	*N*	*Yes*	*No*	*N*	*Yes*	*Yes*
RAPLT [32]	*N*	*Yes*	*No*	*No*	*Yes*	X
SLAP [38]	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
LAMP [41]	X	*No*	*No*	*No*	*No*	X
M^2AP [42]	X	*No*	*No*	*No*	*No*	X
EMAP [43]	X	*No*	*No*	*No*	*No*	X
LPCP [44]	*Yes*	X	*Yes*	*No*	*Yes*	X
David-Prasad [54]	X	*N*	*N*	X	*N*	X
R^2AP [56]	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*N*
URMAP [58]	*Yes*	X	*Yes*	X	*Yes*	*Yes*
ESRAS[19]	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
SLAS(Proposed)	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*

Database computation and complexity: The scheme requires less hash function computations in database. It does not computes hash unnecessarily to match the ID rather it initially checks the secret and then verify the hash function.

VI. SIMULATION RESULTS

The following simulations were conducted to verify few aspects of the security.

Scyther Simulation

To test the idea in a simulated environment Scyther Simulation tool is used. It is a GUI-based tool to verify security performance of the protocols [37]. For the experiment Scyther Simulation tool is installed in a Desktop computer in Windows 10 platform. It is suitable for challenge-response authentication system. The language used here is called Security Protocol Description language(SPDL). The basic requirements for this authentication protocol such as random number generation, encryption, hash functions, send response, verifications can be performed. For example a random number can be generated using fresh declaration. In our simulation r1 and r2 and fresh type. For one-way encryption process hash function can be used. Other necessary encryption function can be declared using special predefined type Function. Some popular events are

send to send response
recv to receive response
claim to specify role to model intended security property.

Some predefined claims are

Alive to check if it is alive
Secret Secrecy of a parameter is checked
Niagree Non-injective agreement
Nisynch Non-injective synchronisation
Weakagree Weak agreement
match to match pattern

Other than this a macro can be used to simplify and or abbreviation of complex term.

The result of the simulation is given in Fig.3. From the result it is shown that all the status are OK which means under the assumptions of the scheme and the protocol the SLAS is secure from the attacks and it resist all the active and passive threats.

VII. CONCLUSION

In case of a RFID system the security and privacy issue is very a challenging issue due to small memory size and computation capability of the low-cost tag. A novel authentication scheme SLAS has been proposed to protect privacy and security for RFID systems. Several security issues such as information leakage, eavesdrop, tampering, replay attack, modification and tracking are most concerns. Our proposed protocol works on these issue to protect the system using low cost and lightweight RFID. The protocol uses lightweight hash function for computation of identifier and secret using two random numbers. So the transmitted signal is fully protected from information leakage and tracking. It is secured from message interception and location privacy and ensures forward security by changing the secret number after each authentication process. The proposed scheme requires three one-way hash computations and one bitwise XOR function which makes it highly efficient for a large range of security protection in RFID system. The storage requirement for the tag is reasonably less for the overall security protection from all threats. The performance analysis shows that the SLAS scheme is both secure and relatively efficient in comparison to the selected schemes.

```
const XOR:Function;
hashfunction h;

protocol Myproposed(Tag, Reader)
{
   //SPDL part for Tag role
   role Tag
    {
        const  ID,X,X',AL,B,BR,B'R,XT, r1;
        fresh r2:Nonce;
         recv_!1(Reader, Tag, r1);
         macro A=h(ID, r1,r2);
         macro C=XOR(X,r2);
         send_!2(Tag, Reader, AL,C,r2);
         recv_!3(Reader, Tag, BR);
               macro XT=h(X,r2);
               macro B'=h(ID,XT,r1,r2);
               match(B'R,BR);
               claim(Tag, Secret, ID);
               claim(Tag, Secret, X);
               claim(Tag, Secret, r2);
               claim(Tag, Niagree);
               claim(Tag, Nisynch);
               claim(Tag, Nisynch);
               claim(Tag, Alive);
               claim(Tag, Weakagree);
         }

      //SPDL part for Reader role
        role Reader
          {
              const ID, X,Xprev,r2,AL,A'L,BL,BR;
               fresh r1:Nonce;
               send_!1( Reader,Tag, r1);
               recv_!2(Tag,Reader, AL,C,r2);
               macro r2=XOR(X,C);
               macro A'=h(ID, r1,r2);
               match(A'L,AL);
               macro Xprev=X;
               macro X=h(X,r2);
               macro B=h(ID,X,r1,r2);
               send_!3( Reader,Tag,BR);
               claim(Reader, Secret, ID);
               claim(Reader, Secret,X);
               claim(Reader, Secret, r2);
               claim(Reader, Niagree);
               claim(Reader, Nisynch);
               claim(Reader, Alive);
               claim(Reader, Weakagree);
          }
    }
```

Fig. 3. SPDL for the Tag and the Reader

TABLE II. PERFORMANCE COMPARISON AMONG VARIOUS AUTHENTICATION SCHEMES.

Criteria / Scheme	Number of messages (Total)	Communication messages (Tag)	Storage cost (Tag)
URASP [8]	**4*L***	**1.5*L***	**4*L***
IOLAS [29]	**4*L***	**2*L***	**5*L***
LRSAS [30]	**5*L***	**2*L***	**3*L***
RAPP [31]	**5*L***	**2*L***	**5*L***
RAPLT [32]	**4*L***	**3*L***	**5*L***
SLAP [38]	**4*L***	**1.5*L***	**7*L***
LAMP [41]	**4*L***	**2*L***	**6*L***
M^2AP [42]	**4*L***	**3*L***	**6*L***
EMAP [43]	**4*L***	**3*L***	**6*L***
LPCP [44]	**5*L***	**2*L***	**5*L***
David-Prasad [54]	**5*L***	**3*L***	**5*L***
R^2AP [56]	**5*L***	**2*L***	**5*L***
URMAP [58]	**4*L***	**2*L***	**5*L***
ESRAS	**5*L***	**1.5*L***	**5*L***
SLAS(Proposed)	**3L**	**2.5L**	**3L**

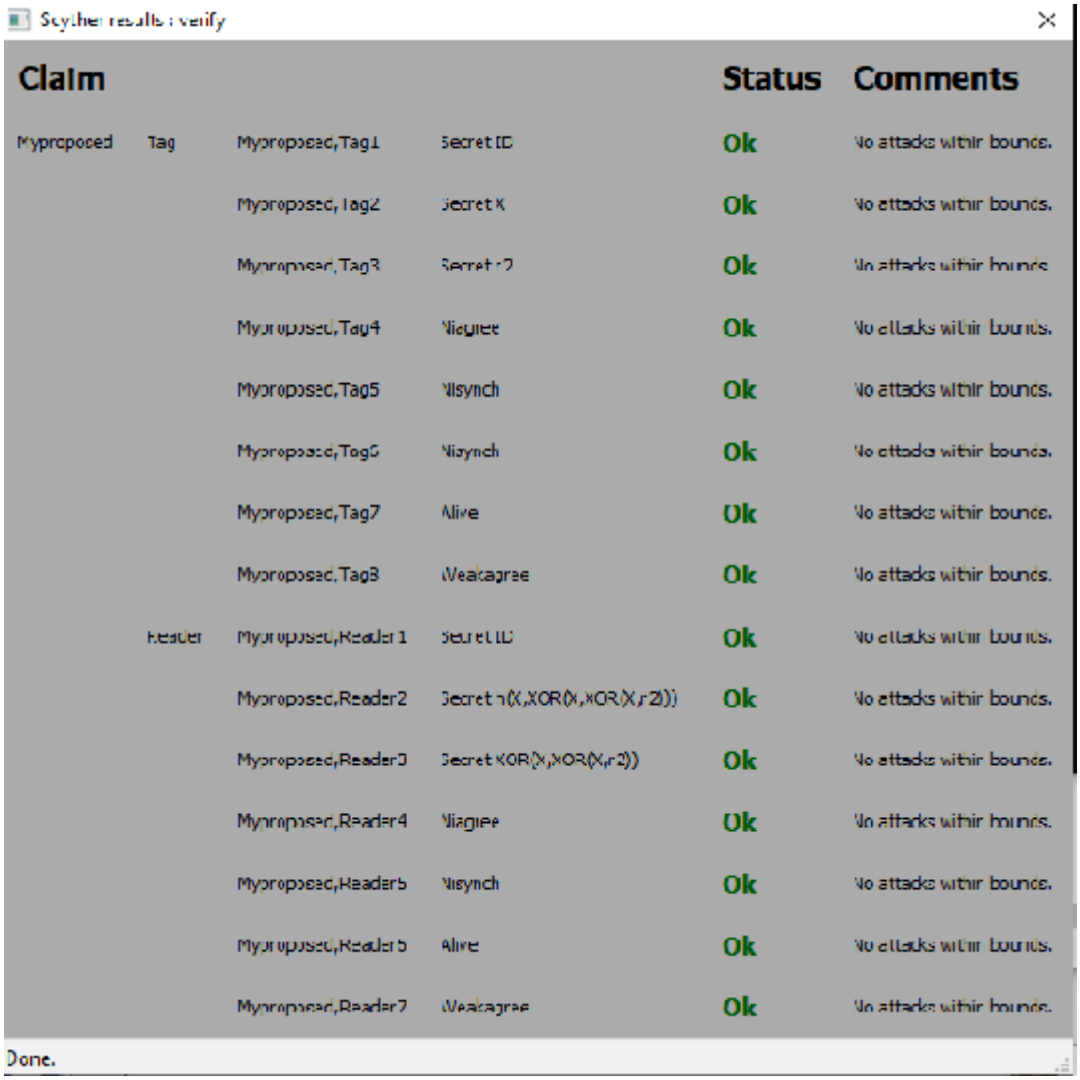

Fig. 4. Scyther Simulation Result for proposed SLAS

.

REFERENCES

[1] A. Jules,S. Garfinkel, and R. Pappu, "RFID privacy: an overview of problems and proposed solutions," IEEE Security and Privacy. 3(3): 34-43, May/June 2005.

[2] A. Jules, "RFID security and privacy: A research survey," IEEE Journal on Selected Areas in Communication, 24(2), February 2006.

[3] EPCglobal Web site, 2005. Referenced 2005 at http://www.EPCglobalinc.org.

[4] R. Want,"An Introduction to RFID Technilogy," IEEE Pervasive Computing, vol. 5, pp. 25 – 33, 2005.

[5] B. S. Prabhu, X. Su, H. Ramamurthy, C. Chu, R. Gadh, "WinRFID – A Middleware for the enablement of Radio Frequency Identification (RFID) based Applications," UCLA - Wireless Internet for the Mobile Enterprise Consortium (WINMEC)420 Westwood Pl., Los Angeles CA 90095.

[6] D. Molnar and D. Wagner, "Privacy and security in library RFID: Issues, practices, and architectures," In B. Pfitzmann and P. Liu, editors, Conference on Computer and Communications Security - ACM CCS, pages 210–219, Washington, DC, USA, October 2004. ACM Press.

[7] K. Rhee, J. Kwak, S. Kim and D. Won, "Challenge-Response Based RFID Authentication Protocol for Distributed Database Environmnet," SPC 2005, LNCS 3450, pp. 70-84, 2005.

[8] E.Y. Choi, S.M. Lee, D.H. Lee, "Efficient RFID Authentication Protocol for Ubiquitous Computing Environment," Embedded and Ubiquitous Computing, vol.3832, pp.945-954, 2005.

[9] J. Zhi-Wei , S. Xiao-yan, H. Lee and Z. Tao, "A Revised One-way Hash based Low-cost Authentication Protocol In RFID System," Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09. 5th International Conference, Page(s): 1 – 4.

[10] M. Ohkubo, K. Suzki, and S. Kinoshita, "Cryptographic approach to "privacy-friendly" tags.," In RFID Privacy Workshop, MIT, MA, USA, November 2003. http://www.rfidprivacy.us/2003/agenda.php.

[11] H. Chien and C. Chen, "Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards," Computer Standards & Interfaces, 29(2):254–259, February 2007.

[12] D. Henrici and P. Muller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers," In R. Sandhu and R. Thomas, editors, International Workshop on Pervasive Computing and Communication Security - PerSec 2004, pages 149–153, Orlando, Florida, USA, March 2004. IEEE Computer Society.

[13] S.M. Lee, Y.J. Hwang, D.H. Lee and J.I. Lim, "Efficient Authentication for Low-Cost RFID systems," ICCSA05, vol. 3480 LNCS, pp.619-629, Springer-Verlag, 2005.

[14] B. Song and C. J. Mitchell, "RFID authentication protocol for low-cost tags," In WISEC, pages 140-147, 2008.

[15] T. Dimitriou, "A lightweight RFID protocol to protect against traceability and cloning attacks," In Conference on Security and Privacy for Emerging Areas in Communication Networks - SecureComm, pages 59–66, Athens, Greece, September 2005. IEEE.

[16] B. Song, "RFID Tag Ownership Transfer," In 4thWorkshop on RFID Security (RFIDsec 08), Budaperst, Hungary, July 2008.

[17] M.E. Hoque,F. Rahman, S.I. Ahamed, "Supporting Recovery, Privacy and Security in RFID Systems Using A Robust Authentication Protocol," Proceedings of the 2009 ACM symposium on Applied Computing, SAC'09, Honlulu, Hawaii,USA. pp.1062-1066.

[18] S. Cai, Y. Li, T. Li, R. H. Deng, "Attacks and Improvements to an RFID Mutual Authentication Protocol and its Extensions," WiSec'09, March 16–18, 2009, Zurich, Switzerland.

[19] M. Shafiq, K. Shingh, C. Lal, M. Conti, T. Khan, ESRAS: An efficient and secure ultra-lightweight RFID authentication scheme for low-cost tags. Computer Networks, 217(2022), pp. 1-11.

[20] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M Estévez-Tapiador, Arturo Ribagorda, LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags, in: Proc. of 2nd Workshop on RFID Security, Vol. 6, 2006.

[21] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M Estevez-Tapiador, Arturo Ribagorda, *M*2AP: a minimalist mutual-authentication protocol for lowcost RFID tags, in: International Conference on Ubiquitous Intelligence and Computing, Springer, 2006, pp. 912–923.

[22] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M Estevez-Tapiador, Arturo Ribagorda, EMAP: An efficient mutual-authentication protocol for lowcost RFID tags, in: OTM Confederated International Conferences ''on the Move to Meaningful Internet Systems'', Springer, 2006, pp. 352–361.

[23] Ticyan Li, Guilin Wang, Security analysis of two ultra-lightweight RFID authentication protocols, in: IFIP International Information Security Conference, Springer, 2007, pp. 109–120.

[24] Tieyan Li, Robert Deng, Vulnerability analysis of EMAP-an efficient RFID mutual authentication protocol, in: The Second International Conference on Availability, Reliability and Security (ARES'07), IEEE, 2007, pp. 238–245.

[25] Lijun Gao, Maode Ma, Yantai Shu, Yuhua Wei, An ultralightweight RFID authentication protocol with CRC and permutation, J. Netw. Comput. Appl. 41 (2014) 37–46.

[26] Yun Tian, Gongliang Chen, Jianhua Li, A new ultralightweight RFID authentication protocol with permutation, IEEE Commun. Lett. 16 (5) (2012) 702–705.

[27] Hanguang Luo, Guangjun Wen, Jian Su, Zhong Huang, SLAP: Succinct and lightweight authentication protocol for low-cost RFID system, Wirel. Netw. 24 (1) (2018) 69–78.

[28] Yali Liu, Martianus Frederic Ezerman, Huaxiong Wang, Double verification protocol via secret sharing for low-cost RFID tags, Future Gener. Comput. Syst. 90 (2019) 118–128.

[29] Yali Liu, Xinchun Yin, Yongquan Dong, Keke Huang, Lightweight authentication scheme with inverse operation on passive rfid tags, J. Chin. Inst. Eng. 42 (1) (2019) 74–79.

[30] Liang Xiao, He Xu, Feng Zhu, Ruchuan Wang, Peng Li, SKINNY-based RFID lightweight authentication protocol, Sensors 20 (5) (2020) 1366.

[31] Cuong Trinh, Bao Huynh, Jan Lansky, Stanislava Mildeova, Masoumeh Safkhani, Nasour Bagheri, Saru Kumari, Mehdi Hosseinzadeh, A novel lightweight block cipher-based mutual authentication protocol for constrained environments, IEEE Access 8 (2020) 165536–165550.

[32] Mohd Shariq, Karan Singh, Pramod Kumar Maurya, Ali Ahmadian, Muhammad Rezal Kamel Ariffin, URASP: An ultralightweight RFID authentication scheme using permutation operation, Peer-to-Peer Netw. Appl. 14 (6) (2021) 3737–3757.

[33] Il-Soo Jeon, Eun-Jun Yoon, A new ultra-lightweight RFID authentication protocol using merge and separation operations, Int. J. Math. Anal. 7 (52) (2013) 2583–2593.

[34] Mathieu David, Neeli R. Prasad, Providing strong security and high privacy in low-cost RFID networks, in: International Conference on Security and Privacy in Mobile Information and Communication Systems, Springer, 2009, pp. 172–179.

[35] Xu Zhuang, Yan Zhu, Chin-Chen Chang, A new ultralightweight RFID protocol for low-cost tags: *R*2AP, Wirel. Pers. Commun. 79 (3) (2014) 1787–1802.

[36] Madiha Khalid, Umar Mujahid, M Najam-ul Islam, Hongsik Choi, Imtiaz Alam, Shahzad Sarwar, Ultralightweight resilient mutual authentication protocol for IoT based edge networks, J. Ambient Intell. Humaniz. Comput. (2021) 1–12.

[37] C. Cremers, Scyther tool, 2021, http://www.cs.ox.ac.uk/people/cas.cremers/scyther/. [Online; Accessed on March 10, 2021].

Performance Of Grape Leaves Extract As Green Inhibitor On Corrosion Inhibition Of Mild Steel In Acidic Media

Received: 12 January 2023; Accepted: 8 March 2023 ***Research Article***

Noor Qasim Atiyah Alsaedi
Department of Electrical Power Techniques Engineering
Alamara University college
Missan, Iraq
noor.qassim@alamarahuc.edu.iq

Ali Al-Hashim
Department of Medical Instrumentation Techniques Engineering
Alamara University college
Missan, Iraq
ali.abdalkarim@alamarahuc.edu.iq

Hussien K.Abdul Zahra
Department of Mechanical Engineering
Missan oil institute
Missan, Iraq
hussein.kareem.abdulzahra@gmail.com

Elaf Qasim Atiyah Alsaedi
Department of petroluem engineering
Alamara University college
Missan, Iraq
noorqasimat@gmail.com

Qasim jaber yousif
Department of Mechinaical Engineering
Missan oil institute
Missan, Iraq
Qasimjaber30@gmail.com

***Abstract*— The inhibitive effect of grape leaves Extract (GLE) on mild steel in acidic Media with different temperatures polarization measures and weight loss have been used to investigate. The study obtained that the corrosion rate increases with increasing of acid concentration and the used green inhibitor (GLE) inhibited the electrochemical reaction to its lowest levels. Temperature and extract concentration both increase corrosion inhibition effectiveness. Grape leaf extract was adsorbed according to the Langmuir adsorption isotherm. According to the thermodynamic characteristics, there was an exothermic, spontaneous adsorption process with a rise in entropy. Polarization curves demonstrated the mixed-type inhibitory properties of grape leaves extract.**

Keywords— corrosion; mild steel; green inhibitor; grape leaves extract; acidic corrosion.

I. INTRODUCTION

Mild steel is widely used in oil industry equipment's, Metallic corrosion Causing financial costs for oil industry and with time the metallic constructions corroded due to different reasons such as acidic media. In several oil industry processes, such as industrial acid cleaning, acid descaling, acid pickling, and oil well acidizing, acidic solutions are used.[1]. To eliminate the metals aggressive green inhibitors are used, which considered an excellent type of inhibitors to reduce the rate of corrosion in acidic media. One of the most effective and affordable ways to prevent mild steel corrosion in acidic medium is to employ green inhibitors. As green inhibitors, the researchers used a variety of plant leaf extracts, including those from Cola acuminata and Camellia sinensis.[2], Tithonia diversifolia [3], Newbouldia leavis [4], Euphorbia hirta [5], Carica Papaya and Camellia Sinensis[6], Vernonia Amygdalina [7,8]. According to the results of all these investigations, plant extracts contain organic compounds that have molecules of N, S, and O that can be used to create a protective coating on mild steel surfaces and so improve inhibitory effectiveness. The objective of the current work is to get high inhibitory effectiveness (I.E.) of grape leaf extract as a mild steel inhibitor in acidic solution. Ease of Use. The Corrosion is a global phenomenon that happens because of Chemical reactions between metals and the environment Metal corrosion can be controlled in a variety of ways. Methods are noteworthy, and among many methods of regulating cathodic protection. The imprinted current method and the sacrificial anode method are two types of metal cathodic protection. Both methods deal with the transfer of electrons either from or to the metal or the atmosphere. Its offered model is extremely important which accessible energy Renewable source and operates it to secure buried steel pipelines against corrosion. It is intended to use the capacitive coupler of the Cathodic Protection by Impressed Current Device at a minor level to increase the growth of this system to a greater degree, which may be agreed with the protection process of lengthy subversive pipelines in distant areas. Impressed Current Cathodic Safety in combination with capacitive couplings indicates that there are several potential solutions to inhibit corrosion in underground. The batteries can be considered one of the electrical sources. They are applied in many applications. However, most of the batteries charging process achieved by using of power harmonies. The concept of power transfer wireless was first expressed and established by Nikola Tesla 1900's [9]. The magnets that we use to design the system ready to transfer power through the small and large air gaps. Capacitance coupling is the principle of CPT systems. The application of WPT systems is found in many fields such as transportation [10], roadway lighting [11], consumer electronics [12], and high-power transmission [13]. The statistical details showed health problems, sensitivity and depression that resulted from electromagnetic field and capacitance coupling [14]. The magnetic fields properties are forced to form closed loops from pole to pole and all of them have equal strength. So, any electronics placed in magnetic fields vicinity exposed to the above effect resulting an electromagnetic Interference (EMI) issues and because the present of EMI, extra protection would need for the electronics in the environment and pass-through difficult testing of electromagnetic compatibility. the track looks of smallest reluctance between reverse poles and effort to make a closed loop between pair of poles is another property of magnetic fields [15].

II. FUNDAMENTALS OF CORROSION

Corrosion reaction can be achieved by formatting an electrochemical corrosion cell which is consists of Anode (corroded terminal), cathode (protected terminal) metallic path and electrolyte as shown in table 1. The electrical circuit is completed with the help of all these components, which permits electrons to flow. The positive side of the control source is attached to the inert anode in the Impressed Current Cathodic Protection technique (such as Graphite). Graphite can be considered as great conductor for power and upgrades moo values of current thickness, gives tall surface per unit weight with moo temperate Fetched moreover gives moo resistance to the electrolyte due to its tall surface-to-weight proportion. The Graphite Levels consumption is about 0.25 kilogram per Year which makes it a favorable among the different materials of anode available.

A. Mild steel Samples preparation

0.5 and 1M HCl solution , different amount (0.1, 0.25, 0.5, 0.75, 1 g/lit) of grape leaves extract were used as working media and immersion time was 24 hours. Solutions temperature was (30,40,50 °C).

B. Materials and Solutions Grape Leaves Extract preparation

0.5 and 1M HCl solution, different amount (0.1, 0.25, 0.5, 0.75, 1 g/lit) of grape leaves extract were used as working media and immersion time was 24 hours. Solutions temperature was (30,40,50 °C).

C. Grape Leaves Extract preparation

grape leaves was dried by sun light under temperature range (40 -50 °C) for three days then grinded and sifted. The resulted powder was used as an inhibitor for mild steel in different temperature and different concentration of HCl.

III. WEIGHT LOSS MEASUREMENT

A total of 40 experiments for weight loss measurements were achieved to study the corrosion rate of mild steel in different concentration of (GLE) and HCl for 24 hours as an immersion time. The results were presented in Table I ,Table II & Table III . The results can be demonstrated that the corrosion rate rose with increasing of acid concentration and (GLE) inhibits the electrochemical reaction and decreasing the rate of corrosion with increasing of HCl and temperature. It can be shown that the amount of acid present is directly proportional to the corrosion rate. The inhibition efficiency I.E. was calculated as the follow:-

$$IE\% = (Wo - Wi)/Wo \times 10 \quad (1)$$

Where, W_O and W_i are, respectively, the weight loss of the coupon in the normal and inhibited acid solutions. The I. E. increases with the (GLE) concentration as shown in TABLE I . [9].

A. Adsorption isotherm and thermodynamic parameters

adsorption isotherm calculations were performed to study the inhibition mechanism of grape extracting leaves, on the surface of mild steel, it was found best agreement with Adsorption isotherm of Langmuir. For both chemical and physical adsorption, the Langmuir adsorption isotherm is regarded as the ideal isotherm [10, 11]. moreover, it might be portrayed as:

$$Cinh/\Theta = 1/Kads + Cinh \quad (2)$$

Where, Kads is the adsorption constant and Cinh is the amount of an inhibitor. The surface coverage values θ (θ =Wo− Wi / Wo) computed from the weight-loss I. E. percentage. According to equation (2) it can be observed a linear relationship when Cinh/Θ was plotted against Cinh as seem from fig (1-3) therefore the adsorption of (GLE) on the mild steel surface in (0.5 ,1M) HCl solution by the Langmuir isotherm. The standard Gibs free energy of adsorption is related to the adsorption constant. ΔG°ads as follows [12]:-

$$\Delta G°ads = -RT \ln (55.5\ Kads) \quad (3)$$

Where, R is the universal gas constant, T is the absolute temperature and the value 55.5 is the molar concentration of water in the working solution [13,14]. The results showed negative value of ΔG°ads ranges from -13.656 to -14.921 kJ /mol and this values approved physical and spontaneous adsorption (physisorption) of grape leaves extract molecules on the metal surface [15].

Vant Hoff equation as follows below used to calculate the adsorption heat ΔH°ads of inhibitor molecules by plotting (ln Kads) against 1/T and the slope of the resultant straight line is representing ΔH°ads /R[16]:

$$\ln Kads = (-\Delta H°ads)/RT + constant \quad (4)$$

TABLE I. WEIGHT LOSS PARAMETERS FOR THE CORROSION OF MILD STEEL IN THE PRESENCE AND ABSENCE OF (GLE) AT 30 °C.

HCl Conc.(M)	**0.5 M**		**1M**	
Inhibitor Conc.(g/lit)	***Corrosion rate (mg /m² .d)***	***IE%***	***Corrosion rate (mg /m² .d)***	***IE%***
Blank	572.90		680.55	
0.1	121.3617	78.816	144.6098	78.75
0.25	85.87843	85.009	120.90782	82.23
0.5	79.25366	86.166	109.7458	83.87
0.75	62.31448	89.122	87.92488	87.08
1	56.31993	90.169	67.29465	90.11

TABLE II. WEIGHT LOSS PARAMETERS FOR THE CORROSION OF MILD STEEL IN THE PRESENCE AND ABSENCE OF (GLE) AT 40 °C.

HCl Conc.(M)	**0.5 M**		**1M**	
Inhibitor Conc.(g/lit)	***Corrosion rate (mg /m² .d)***	***IE%***	***Corrosion rate (mg /m² .d)***	***IE%***
Blank	692.14	0	731.37	
0.1	134.69	80.54006	137.40	81.21
0.25	95.47	86.20655	97.29	86.69
0.5	85.53	87.64267	82.43	88.72
0.75	62.75	90.93392	64.12	91.23
1	55.36	92.00162	56.20	92.315

TABLE III. WEIGHT LOSS PARAMETERS FOR THE CORROSION OF MILD STEEL IN THE PRESENCE AND ABSENCE OF (GLE) AT 50 °C.

Hcl Conc.(M)	**0.5 M**		**1M**	
Inhibitor Conc.(g/lit)	***Corrosion rate (mg /m² .d)***	***IE%***	***Corrosion rate (mg /m² .d)***	***IE%***
Blank	772.24		830.93	
0.1	103.8415	86.55	104.2845	87.449
0.25	85.05064	88.98	103.251	87.57
0.5	72.29537	90.63	78.65764	90.53
0.75	68.46623	91.13	60.85994	92.67
1	59.07047	92.35	54.84422	93.39

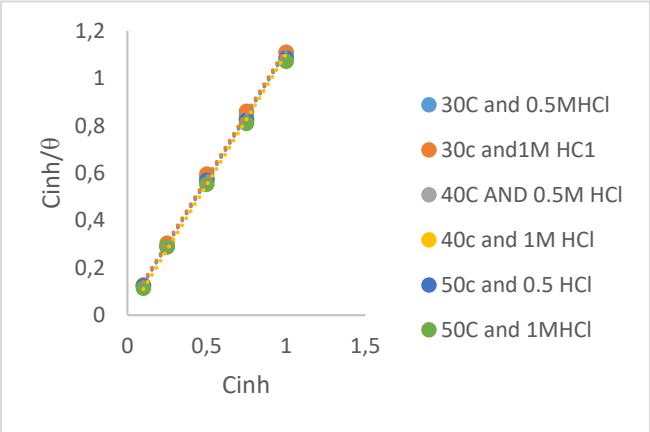

Fig. 1. Langmuir adsorption isotherm for grape leaves extract at 30 ,40 and 50 °C.

B. *Adsorption Entropy*

Table IV showed all the Adsorption thermodynamic parameters. Spontaneous adsorption of the grape leaves extract on mild steel surface proved by the negative value of ΔG°ads which concluded that physical Adsorption occurred by the extract on the mild steel surface .The negative value of ΔH°ads suggest that the process of adsorption of inhibitor on mild steel surface is exothermic. It can be assume that the increase in temperature leads to the increase in desorption of the adsorbed inhibitor molecule from the mild steel surface and can be calculated as:

$$\Delta G°_{ADS} = \Delta H°_{ADS} - T\,\Delta S \qquad (5)$$

TABLE IV. ADSORPTION THERMODYNAMIC PARAMETERS FOR THE GRAPE LEAVES EXTRACT ON MILD STEEL SURFACE

Temperature (°C)	**Hcl Conc.(M)**	**Kads kJmol⁻¹**	**ΔG° k J mole⁻¹**	**ΔH° k J mole⁻¹**	**ΔS° J mole⁻¹**
30	*0.5*	*32.894*	*-8.8*	*26.189*	*115.475*
	1		*-8.8*		*115.475*
40	*0.5*	*32.894*	*-9.09*		*115.30*
	1	*62.631*	*-10.31*		*115.30*
50	*0.5*	*32.894*	*-9.38*		*115.876*
	1	*62.631*	*-10.64*		*114.021*

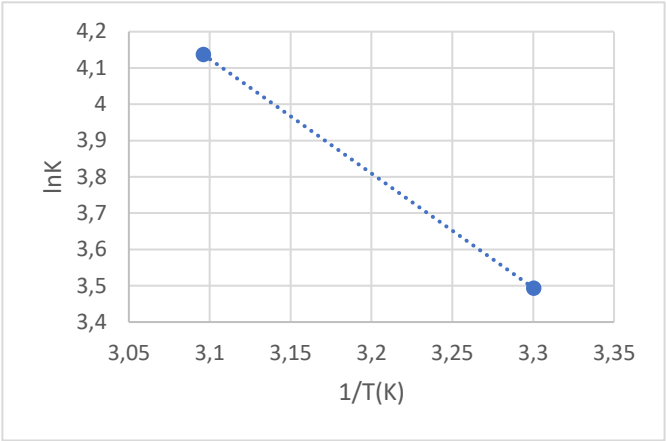

Fig. 2. Von't Hoff plot for grape leaves extract at 30 ,40 and 50 °C.

V. CONCLUSIONS

In this research, the effect of grape leaf extract was studied as an inhibitor of corrosion reaction in acidic media and different conditions of temperature, exposure time and concentration using two methods, the first is calculating weight loss, which is a chemical method, and the second is using the polarization method, which is an electrochemical method. The research revealed that the corrosion rate increased as the temperature and acid concentration increased, but that the grape leaf extract was able to lower it to the lowest levels, and that the effectiveness of the inhibitory effect increased as the extract's concentration and temperature increased. It was found that the corrosion inhibition process is subject to the Langmuir adsorption curves, and that the inhibition process is spontaneous, accompanied by the release of thermal energy and the inhibitor.

It may be used for another purpose in the future, Like vine leaves or fig leaves and to get the best results and prevent corrosion that occurs in metals.

REFERENCES

[1] Ahanotu, C. C., Onyeachu, I. B., Solomon, M. M., Chikwe, I. S., Chikwe, O. B., & Eziukwu, C. A. (2020). Pterocarpus santalinoides leaves extract as a sustainable and potent inhibitor for low carbon steel in a simulated pickling medium. Sustainable Chemistry and Pharmacy, 15, 100196.

[2] Samiee, R., Ramezanzadeh, B., Mahdavian, M., Alibakhshi, E., & Bahlakeh, G. (2019). Graphene oxide nano-sheets loading with praseodymium cations: Adsorption-desorption study, quantum mechanics calculations and dual active-barrier effect for smart coatings fabrication. Journal of industrial and engineering chemistry, 78, 143-154.

[3] Fawzy, A., Abdallah, M., Zaafarany, I. A., Ahmed, S. A., & Althagafi, I. I. (2018). Thermodynamic, kinetic and mechanistic approach to the corrosion inhibition of carbon steel by new synthesized amino acids-based surfactants as green inhibitors in neutral and alkaline aqueous media. Journal of Molecular Liquids, 265, 276-291

[4] Zeino, A., Abdulazeez, I., Khaled, M., Jawich, M. W., & Obot, I. B. (2018). Mechanistic study of polyaspartic acid (PASP) as eco-friendly corrosion inhibitor on mild steel in 3% NaCl aerated solution. Journal of Molecular Liquids, 250, 50-62.

[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Wang, L., Wu, W., Sun, W., Yang, Z., Wang, S., & Liu, G. (2019). Partially dehydrated zinc hydroxide sulfate nanoplates reinforced coating for corrosion protection. Chemical Engineering Journal, 373, 8-22.

[7] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE

Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[8] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[9] Ahmed, R.K., Zhang, S. (2019): Alchemilla Vulgaris Extract as Green Inhibitor of Copper Corrosion in Hydrochloric Acid, International Journal of Electrochemical Science, 14, 10657-10669. DOI: 10.20964/2019.11.43

[10] Alibakhshi, E., Ramezanzadeh, M., Haddadi, S.A., Bahlakeh, G., Ramezanzadeh, B., Mahdavian, M. (2018.): Persian Liquorice extract as a highly efficient sustainable corrosion inhibitor for mild steel in sodium chloride solution, Journal of Cleaner Production, 210, 660-670. DOI: 10.1016/j.jclepro.2018.11.053

[11] Bouammali, H., Ousslim, A., Bekkouch, K., Bouammali, B., Aouniti, A., Al-Deyab, S.S., Jama, C., Bentiss, F., Hammouti, B. (2013): The Anti-Corrosion Behavior of Lavandula dentata Aqueous Extract on Mild Steel in 1M HCl, International Journal of Electrochemical Science, 8, 6005-6013.

[12] Bouammali, H., Ousslim, A., Bekkouch, K., Bouammali, B., Aouniti, A., Al-Deyab, S.S., Jama, C., Bentiss, F., Hammouti, B. (2013): The Anti-Corrosion Behavior of Lavandula dentata Aqueous Extract on Mild Steel in 1M HCl, International Journal of Electrochemical Science, 8, 6005-6013. B

[13] Bozorg, M., Farahani, T.S., Neshati, J., Chaghazardi, Z., Ziarani, G.M. (2014): Myrtus Communis as Green Inhibitor of Copper Corrosion in Sulfuric Acid, Industrial & Engineering Chemistry Research, 53, 4295-4303. DOI: 10.1021/ ie404056w

[14] Cech, M., Davis, P., Guijt, W., Haskamp, A., Huidobro Barrio, I. (2021): Performance of European cross-country oil pipelines Statistical summary of reported spillages in 2019 and since 1971, Report. Brussels, 4/21

[15] Cordeiro, R.F.B., Belati, A.J.S., Perrone, D., D'elia, E (2018): Coffee Husk as Corrosion Inhibitor for Mild Steel in HCl Media, International Journal of Electrochemical Science, 13, 12188-12207. DOI: 10.20964/2018.12.29

[16] Da Rocha, J.C., Ponciano Gomes, J.A.C., D'elia, E., Gil Cruz, A.P., Cabral, L.M.C., Torres, A.G., Monteiro, M.V.C. (2012): Grape Pomace Extracts as Green Corrosion Inhibitors for Carbon Steel in Hydrochloric Acid Solutions, International Journal of Electrochemical Science, 7, 11941- 11956.

The classification of pen ink aging by machine learning and deep learning technique using Raman spectrum

Received: 26 January 2023; Accepted: 8 March 2023 *Research Article*

Kübra GÜRBÜZ GÖÇMEN
Engineering Faculty
Istanbul Ticaret University
Istanbul/Turkey
kubra.gocmen@istanbulticaret.edu.tr

Mustafa Cem KASAPBAŞI
Engineering Faculty
Istanbul Ticaret University
Istanbul/Turkey
mckasapbasi@ticaret.edu.tr

Sinan BOSNA
Physics Engineer
Tübitak Bilgem
Kocaeli/Turkey
sinan.bosna@tubitak.gov.tr

Abstract—Forgery of valuable documents generally constitutes falsification methods based on altering a previously written document by using similar or identical ink. In the event of the aforementioned situation, forensic science experts conduct various technical examinations on the relevant document using different devices. One of the main purposes of these examinations is to determine the differences in the aging levels of the inks relative to each other. Raman Spectra, which is also used for different purposes in forensic sciences, is one of the methods that can be used in this field. The Raman spectrometer provides information about molecules' vibration energy levels and presents the analyzed region's spectral signature values. Experts can observe the time-dependent changes that occur in the substances in the region under investigation relative to each other and in the substance content through the information obtained. Utilizing this information, sample data were created at different times using the same pen on A4 paper in our study. These data were divided into two groups old and new data. Raman spectra were taken with a 785 nm laser on both sample data. Sequential Keras model, KNN, and SVM algorithms were used to detect ink aging on paper. The k-fold cross-validation method was used to determine the classification performance more accurately. The results showed that the classification performance was 98.71% for the neural network and 100% for the KNN and SVM.

Keywords—Raman spectroscopy, pen ink, machine learning ,deep learning

I. INTRODUCTION

Any modification to a forensic document is regarded as document forgery because it does not accurately reflect the facts. There are falsification methods such as changes, additions and scribbling on the document. When a suspicious document is encountered, it is handled as a forensic case and examined by a document examiner. A document examiner is a person who specializes in studying and researching to uncover the facts about documents. The document "examiner" should not only specialize in handwriting, typewriting and printer printouts, but also in forgery, paper and ink analysis, falsified documents and all technical devices and methods used in document preparation [1]. Forged documents differ from the originals in a number of ways (print quality, paper structure, dimensions, typeface, characteristic features in numbers and patterns) [2]. Document review devices have been developed to detect these differences.

Raman scattering is a type of inelastic scattering. The spectrometric analysis of these scatterings, which occur as a result of the change in the vibration energy modes of molecules as a result of the interaction of matter and light, provides information about the bonds and structures of molecules. In order to obtain the Raman spectrum, a laser source, a spectrophotometer and optical elements that will optically block the laser source in the spectrophotometer and focus the laser source on the sample.

Raman spectroscopy is used in many fields to identify unknown substances, verify samples in quality assurance, analyze the chemical composition of samples or monitor changes. In addition, in recent years, Raman spectra have been used in applications such as classification and separation of certain analytes, disease detection from blood serum, etc [3] [4]. In this study, it is aimed to discriminate whether the pen ink is freshly written or not by taking Raman spectra over the ink sample. For this purpose, data were collected from different people using the same pen on white A4 paper with an interval of approximately 5 years. The spectrum of the ink on the data obtained was taken using Raman spectroscopy. The peaks of the spectra were equalized using min-max normalization and baseline correction. Raman spectra have a strong background fluorescence so that baseline correction is important. There are many methods for minimizing the fluorescence background signal. Various methods were evaluated and morphology based baseline correction method was used [5]. Machine learning algorithms KNN and SVM were used. Sequential model was used using Keras library, one of the deep learning algorithms. The results obtained from machine learning algorithms were more successful than neural network. [6]

II. METARIALS AND METHODS

A. Preparation of Working Area

Raman spectra were performed using Ocean Insight Raman QE Pro High spectrometer, 785 nanometer (40 mW) laser and optical probe. Samples were placed at the focal length of the probe (10 mm) and recorded in the dark environment with 500 ms integration time and 5 averages. The papers were fixed to the floor with the help of weights during the measurement to avoid focal length changes.

B. Data acquisition

About five years ago, data were collected from different people using a Schneider Xtra 8053 pilot pen on A4 paper. The data collection sheet consists of nine sections. The first section contains the name, surname, age, hand direction and date of the person from whom we collected data. In the second section, numbers between 0-9 were printed. In the third

section, the phone number, in the fourth section, the name and surname information was written again, in the sixth section, the alphabet was written with upper and lower case letters, and in the other sections, Fig. 1 in order of priority. These data were collected extensively to be used for future studies. For this study, Raman spectroscopy measurements were taken in the dark using the upper right corner of the drawn arrow shape.

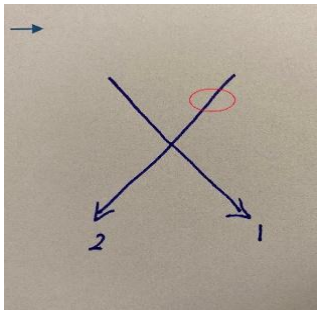

Fig. 1: Measurement sample data

The current data were collected using the same format and including similar or different people who wrote the experiment papers taken about five years ago. The pen used five years ago was the same pen used for the new data collection. The experimental pen was kept throughout the process. The data collected five years ago were kept in files in a cabinet in the office environment. When Raman spectroscopy measurements were taken with the data left on the desk for five years in the office environment, spectral differences were observed compared to the measurements taken from the papers kept in the cabinet for five years. It was observed that ink aging was visibly different on the papers kept outside. Sample data was generated on A4 paper with the current Schneider Xltra 8053 pilot pen. Raman spectra were taken of the data generated from the pilot pen used five years ago and the newly purchased pilot pen. When the spectra were plotted, it was observed that the spectra of the old and new pen were similar.

C. Classification

A total of 155 data, old and new, were collected from different people. Raman measurements were taken at the same location on each paper and spectrum data were obtained. There were negative values in the spectrum data. For each data, spectrum values corresponding to the same wavelength were deleted. Min-max normalization was performed to bring the peaks of the spectral values to the same point. Min-Max normalization is used to scale values in the range (0,1). It sums the data between (0,1) while preserving the values of the original data.

$$x_s = \frac{x - x_{min}}{x_{max} - x_{min}} \quad \textbf{(1)}$$

III. THEORY

Supervised machine learning methods are often used for classification and regression problems. Supervised machine learning involves labeled data that gives information about what is in the dataset. Since it is known what the data corresponds to, the algorithm can give the appropriate output when a similar test data is presented. In unsupervised machine learning, it makes inferences based on the similarity of the datasets to each other.

Deep learning is a type of machine learning that uses an artificial neural network model to learn on large and complex data. It can analyze complexity in text, audio and image data. It is frequently used in problems such as translating audio files into text, extracting meaning from images, and detecting writing characteristics.

A. Support Vector Machines (SVM's)

SVM is a supervised learning method and is often used for classification and regression problems. It separates two classes by a plane. The plane is determined according to the farthest separation of the two classes. One reasonable choice as the best hyperplane is the one that represents the largest separation, or margin, between the two classes. So we choose the hyperplane so that the distance from it to the nearest data point on each side is maximized [3].

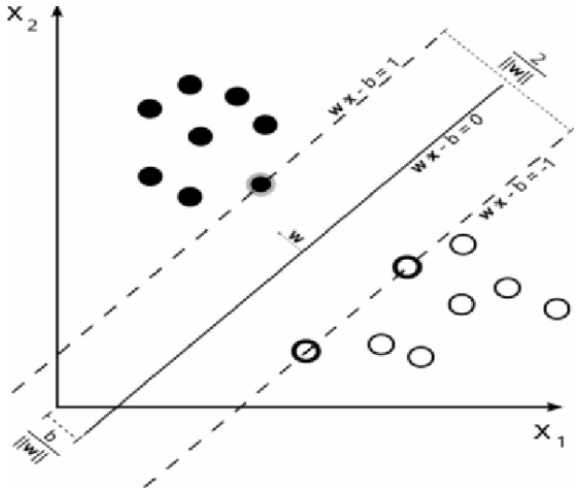

Fig. 2: Maximum-margin hyperplane and margins for an SVM trained with samples from two classes. Samples on the margin are called the support vectors [4]

B. K-nearest neighbors（KNN）

KNN is one of the most important supervised machine learning algorithms, often used for classification problems. Since the KNN algorithm is lazy learning, there is no training phase. To classify, this algorithm determines the class with the k closest classes as the class of the new data. Determining the value of k is important here. The k value may take a different optimum value for each problem. It uses the Euclidean distance calculation to find the distance of the point to be predicted to other points [5].

$$\sqrt{\sum_{i=1}^{n} (q_i - p_i)^2} \quad \textbf{(2)}$$

In our study, we used the optimal value of k as 7. While calculating the k value, we took the k value from 1 to 25 and examined the accuracy score values. We found that the k value is more successful when the accuracy score is 7.

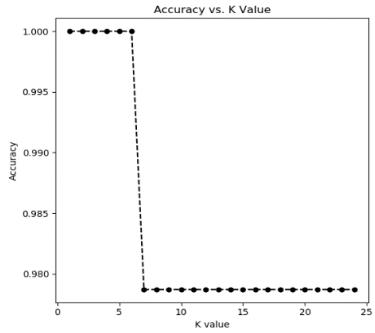

Fig. 3: Best fit k value

C. *Keras*

Keras is a deep learning library. Keras enables fast creation and training of deep learning models. When building deep learning models in Keras, the second layer understands the output of the first layer, so we don't need to specify the output each time in the input of the next layer. Keras is distributed under the permissive MIT license, which means it can be freely used in commercial projects. It's compatible with any version of Python from 2.7 to 3.6 (as of mid-2017). In the application to be made with Keras, we need to prepare the data, define the model and give the data as input to the layers, determine the activation functions and train the model with the fit function. Keras models are of two types: Sequential and Functional API. The most widely used model is the Sequential model. A Sequential model is appropriate for a plain stack of layers where each layer has exactly one input tensor and one output tensor [7]. Keras provides industry-strength performance and scalability: it is used by organizations and companies including NASA, YouTube, or Waymo [8].

D. *StratifiedKfold Cross-validation*

Once our model is trained, we move on to the validation phase. Sometimes, when the size of our data is small, we may have to test our model with a small number of data. When the validation process is with the same data, it is not very healthy. When we test with different data, we get different scores. StratifiedKfold cross validation is used for unbalanced data sets. It ensures that both groups of data are included in the test data. In the standard k-fold method, there is a possibility that both types of data may not be present. It divides the data into k parts and performs data training with the k-1 part and validation with the rest.

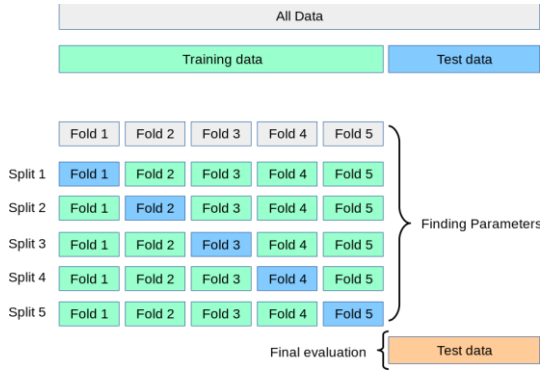

Fig. 4: Cross-validation [9]

Validation score is the average of the validation score of k parts. When building the models, the data is divided as 25% test and 75% training data. When the accuracy of the model is calculated with this split, the success rate may be higher than normal due to overfitting. StratifiedKfold cross validation prevents this situation. Since it validates with different test data, we get different validation scores. By averaging the validation scores, a more realistic score is obtained.

IV. Experimental Results

Raman spectra of four different paper types were obtained by min-max normalization and baseline correction and are shown in Fig. 5. The spectra show Brazilian A4, standard A4 and also diploma papers with different thicknesses. The differences in the types of these papers can be clearly recognized by the peaks in the Raman spectra. In the 1300 - 1500 cm-1 region, especially diploma papers and A4 papers show similar characteristics and can be distinguished from each other. The peak at approximately 1100 cm-1 raman shift value present in all papers comes from the structure of cellulose [6].

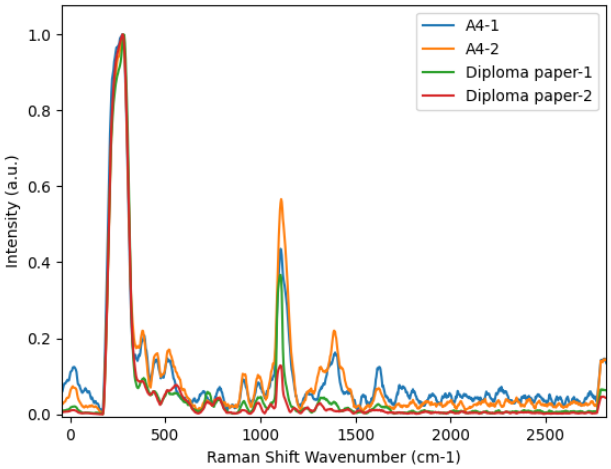

Fig. 5: Different Paper Raman Spectrum

Fig. 6, Old Pen 1 and Old Pen 2 are new samples taken from a Schneider Xtra 8053 pilot pen that was opened and used about 5 years ago and they differ in the way they are written. Old Pen-1 is the spectrum of the sample that is written thinly, without pressing down while writing. The Old Pen 2 is the spectrum of the data drawn thicker with pressure. New Pen-1 and New Pen 2 are samples taken using a newly purchased Schneider Xtra 8053 pilot pen of the same brand. New Pen 1 is the spectrum of the samples written thinner and New Pen 2 is the spectrum of the samples written thicker. Fig. 6 shows that there is no spectral difference between the old and new pen. Old Data 1 spectrum is the spectrum taken from A4 paper drawn about 5 years ago. Regardless of whether the pen is old or new, it is observed to be different from the old written data.

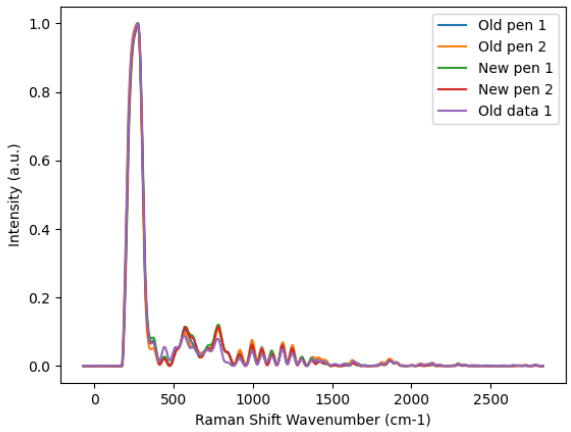

Fig. 6: Effects of Pen Thickness and Condition on Raman Spectrum

Fig. 7 shows the Raman Spectra of three samples written five years ago and three newly written samples. When the Raman Spectra of the old and new pencil samples are analyzed, no dominant change in the peaks is observed, but when the 300 - 1000 cm-1 region is analyzed in Fig. 8, when the 300 - 1000 cm-1 region is examined, the data of the old and newly written samples are separated within themselves, especially when examined in the 400-500 cm-1, 550-600 cm-1, 750-800 cm-1 regions. This separation is due to the changes in the molecular structure of the pen ink in the air environment over time. These changes are sufficient to solve the classification problem and the changes can be detected as features by machine learning algorithms.

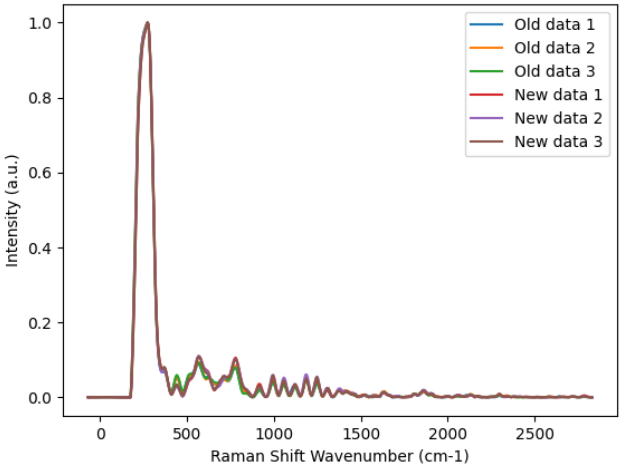

Fig 7: Effects Of Pencil Aging On Raman Spectrum

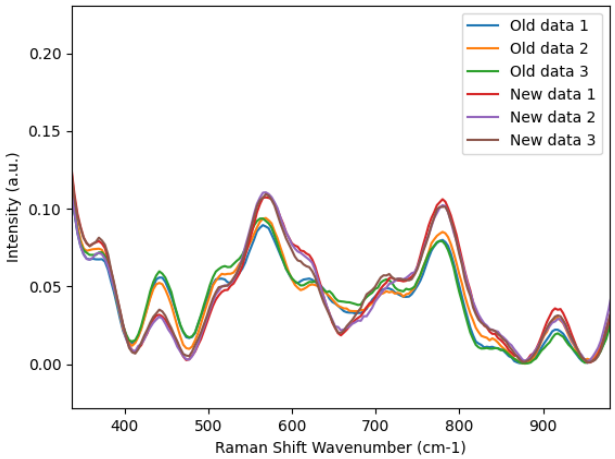

Fig. 8 : Effects Of Pencil Aging On Raman Spectrum (300-100 cm^{-1})

Python version 3.7.6 was used in our study. Spyder 4.0.1 IDE was used for code development environment. For the classification problem, we worked with SVM and KNN algorithms using Python Scikit-learn library. A neural network was developed using Tenserflow Keras library.

Data were collected from different people (men and women) at different times. 155 data were used in our study. Spectra of the collected data were measured using a Raman QE Pro High spectrometer. Min-max normalization was performed to fix the peaks of the spectrum data to 1. In our study, binary classification was performed to predict whether it was old or new writing. SVM, K-nearest neighbors (KNN) and Neural Network are the most common methods used for classification problems.

Data Type	Data Count
Old Data	84
New Data	71

Fig. 9: Number of data used

Support Vector Machine (SVM) and KNN are machine learning methods frequently used in classification problems. In SVM and KNN algorithms, 70% of the data is used for training and 30% for testing. In the KNN algorithm, the k value is taken as 7. It is concluded that the accuracy of both algorithms is 100%. When developing the Keras Sequential model, the hidden layers use the Rectified Linear Unit (ReLU) activation function. The sigmoid activation function is used in the output layer. ReLU activation function outputs between [0, $+\infty$]. Since ReLU takes numbers less than 0 as 0, it does not produce negative outputs and is only active for positive outputs. This affects the performance positively. Adam optimization function is used in our model. The input data size of our model is 1037. Our model consists of 3 Dense. The output activation function is Sigmoid. Sigmoid takes values between [0,1]. It is a non-linear function. StratifiedKFold cross validation divided into 5 parts. The success rate of the model was 98.71%. KNN and SVM had a higher accuracy score than Neural network.

V. CONCLUSION AND FUTURE WORK

Although the classification of pen ink aging using Raman spectra has been successful, it does not provide information about the molecular chemical structure of the ink due to the predominance of fluorescence signals in this region. Solutions can be evaluated by taking Raman spectra with a different wavelength laser source in order to take into account the cases where the writing is done with another pen. Since our current system is compatible with the 785nm laser source, we have not yet been able to perform this study. In addition, the evaluation of the samples written with FTIR (Fourier Transform Infrared Spectrospy) spectra is planned as our further studies. It is planned to collect data on different types of paper and conduct a similar study. Classification with CNN algorithm is also planned.

ACKNOWLEDGMENT

The data measurement phase of this study was completed using the devices and auxiliary instruments in TÜBİTAK BİLGEM Optics Laboratory. We would like to thank TÜBİTAK BİLGEM for their support.

REFERENCES

[1] İ. Birincioğlu ve E. Özkara, «Adli Belge İncelemelerinde Bilinmeyenler,Örneklerle Yazı ve İmza Analizi ile Islak İmza Kavramı,» *TBB Dergisi*, pp. 403-433, 2010.

[2] İ. Çakır ve H. Aslıyüksek, «Instruments and Methods in Forensic Document,» *Arşiv Dünyası,* pp. 16-17, 2014.

[3] A. T. Harris, A. Lungari, C. J. Needham, S. L. Smith, M. A. Lones, S. E. Fisher, X. B. Yang, N. Cooper, J. Kirkham, D. A. Smith, D. P. Martin-Hirsch ve A. S. High, «Potential for Raman spectroscopy to provide cancer screening,» *Head & Neck Oncology,* cilt 1, no. 1, p. 34, 2009.

[4] . A. Emin, A. Hushur ve T. Mamtimin, «Raman study of mixed solutions of methanol and ethanol,» *AIP Advances,* cilt 10, no. 6, p. 2020, 2020.

[5] R. Pueyo, M. Soneira ve S. Ruiz-moreno, «Morphology-Based Automated Baseline Removal for Raman Spectra of Artistic Pigments,» *Applied spectroscopy,* cilt 64, no. 10.1366/000370210791414281, pp. 595-600, 2010.

[6] U. Agarwal, «Analysis of Cellulose and Lignocellulose Materials by Raman Spectroscopy: A Review of the Current Status,» *Molecules,* cilt 1659, no. 10.3390/molecules24091659, p. 24, 2019.

[7] Y. Lin ve J. Wang, «Research on text classification based on SVM-KNN,» %1 içinde *2014 IEEE 5th International Conference on Software Engineering and Service Science*, Beijing, China, 2014.

[8] Y. Lin ve J. Wang, Artists, *Maximum-margin hyperplane and margins.* [Art]. IEEE.

[9] M. A. Lusiandro, S. M. Nasution ve C. Setianingsih, «Implementation of the Advanced Traffic Management System using k-Nearest Neighbor Algorithm,» %1 içinde *2020 International Conference on Information Technology Systems and Innovation*, Bandung, Indonesia, 2020.

[10] F. Chollet, DEEP LEARNING with PYTHON, United States of America: Manning Publications Co, 2018.

[11] F. Chollet, «The Sequential model,» 12 04 2020. [Çevrimiçi]. Available: https://keras.io/guides/sequential_model/.

[12] «About Keras,» 2015. [Çevrimiçi]. Available: https://keras.io/.

[13] «Cross-validation: evaluating estimator performance,» 19 10 2011. [Çevrimiçi]. Available: https://scikit-learn.org/.

A GaN-based Power Amplifier Module Design for 5G Base Stations

Received: 31 January 2023; Accepted: 4 March 2023 *Research Article*

Burak Berk Türk
Electronics and Comm. Eng. Dept.
İstanbul Technical University
İstanbul, Turkey

Furkan Hürcan
Electrical and Electronics Eng. Dept.
İstanbul Medipol University
İstanbul, Turkey

Hüseyin Şerif Savcı
Electrical and Electronics Eng. Dept.
İstanbul Medipol University
İstanbul, Turkey
hsavci@medipol.edu.tr

Hakan Doğan
Electrical and Electronics Eng. Dept.
İstanbul Medipol University
İstanbul, Turkey

Serkan Şimşek
Electronics and Communication Eng. Dept.
İstanbul Technical University
İstanbul, Turkey

***Abstract*—This paper presents a compact Power Amplifier Module (PAM) with class-AB topology designed for new-generation cellular base stations. The center frequency of 3.5GHz PAM is designed to target 5G New Radio (NR) and Long Term Evolution (LTE) bands. The module combines lumped element-based input, output matching networks, and a Gallium Nitride (GaN) High Mobility-Electron Transistor (HEMT) die, making it a hybrid design. The module was designed on a Rogers4003C laminate of 8.5 x 5.2 mm. Full-laminate layout electromagnetic analysis and vendor-supplied compact GaN device models are used in co-simulations to check the design's small signal and large signal behavior. The output power is tuned to 37.1 dBm with 39% power added efficiency(PAE). The transducer power gain is 12.4 dB, while the input and output return losses are -11.7 dB and -6.4 dB, respectively. Besides the small signal stability analysis, the large signal conditions are investigated to ensure unconditional stability up to the maximum oscillation frequency of the device.**

Keywords—Gallium nitride HEMT, LTE band 42, 5G n78, power amplifier module

I. INTRODUCTION

As the new generation of mobile services utilizes Multiple Input Multiple Output systems, the demand for power amplifiers is tremendously increased. There is a high demand for more power-efficient and cost-effective power amplifier modules. The increased data traffic and new frequency band additions require new cellular base stations to be more compact with higher performance. Moreover, the Microcells, Picocells, and Femtocells which are small-cell base stations, drew interest over macro cells as they emit less power, are more environmentally friendly, easier on thermal control, and smaller in size [1]. RF power amplifiers play an essential role in the transmitter design of cellular base stations. Since the microcells, picocells, and femtocells are smaller, their transmitter needs to be smaller and more efficient, which applies to power amplifiers.

GaN transistors have advantages over GaAs in the high energy band gap, allowing them to have higher power density and higher breakdown voltage [2]. As a result of higher breakdown voltage, GaN transistors can handle higher voltage swings and higher power outputs. In recent years there are many researches utilize the capabilities of the GaN transistor [3-5].In this work, class AB power amplifier module is designed with a GaN HEMT die transistor for compact base stations.

II. POWER AMPLIFIER DESIGN

This work aims to deliver 5W output power with a small module. The design goals are specified in Table (I). To achieve the design goals, the PAM's topology was selected as a hybrid module with a single die transistor and small discrete components on printed circuit board(PCB) laminate. The transistor selected Cree's CGH6008D GaN HEMT, a 0.8 x 0.9 mm die transistor. An 8W GaN HEMT was chosen for its capability of high power density, high breakdown voltage, broad bandwidth, and power output [6]. The mode of operation of PAM was chosen as class AB to balance the requirement of linearity and high power-added efficiency [7].

Furthermore, the non-linear transistor model of GaN HEMT CGH6008D was used to determine the bias point of operation. Fig. 1 shows the DC-IV curve of the chosen die HEMT. The bias point is selected as V_{gs}=-2.7V, which is the lower side of the load line. The chosen bias point of the PAM is supplied with V_{ds}=28V, which corresponds to the drain current of I_{ds}=0.134A. The GaN HEMT transistor model includes large signal characteristics, allowing harmonic balance simulations.

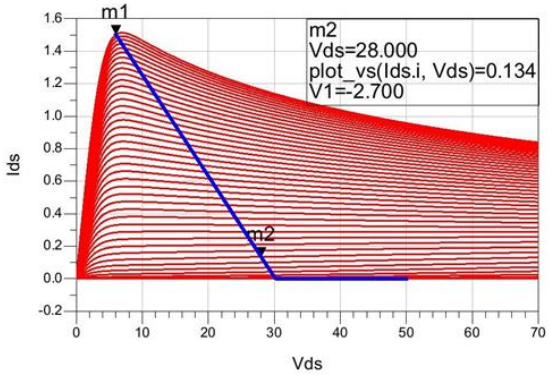

Fig. 1. DC-IV Curve of GaN HEMT CGH60008D.

TABLE I. DESIGN GOALS OF PAM

Design Goal	Value
Frequency	3.4-3.6 GHz
Output Power(dBm)	37
Power Added Efficiency	35%
Gain(dB)	12
Gain Compression(dB)	1
Module Size	10x6 mm

So, just like small-signal behavior, the load-pull simulations were done to develop the input and output matching networks based on the transistor's nonlinearity. The output matching network is designed using iterative load-pull and source-pull simulations to ensure optimum performance of the PAE and the 3rd order output Intercept Point (OIP3) for targeted power delivery [8]. The load-pull setup was prepared as shown in Fig. 2. Bias points were adjusted, as mentioned before. The source and load impedances for the maximum gain, the optimum OIP3 and the

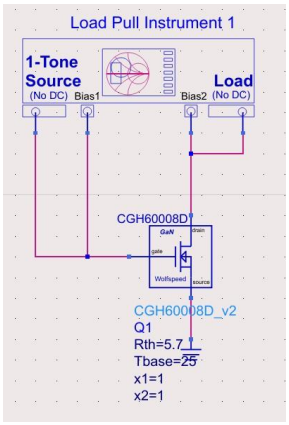

Fig. 2. Load Pull Setup for GaN HEMT Die Transistor

PAE for the transistor was found on the Smith Chart. At the optimum point selected in Fig 3, the source impedance is 0.58+j*5.92 Ω, and the load impedance is 18.68+j*28.19 Ω at the center frequency of the 3.4GHz-3.6GHz band for the 37 dBm output power. The contours indicate equal gain and matching PAE results. The marker was placed to gain contour to indicate an impedance value with the highest gain. This point gave a decent PAE result simultaneously, but it was not the highest PAE available. Typically, PAE has a peak value as the power approaches saturation value. However, one design goal was to gain compression to a maximum of 1 dB. So, the sweet spot was selected where both PAE and gain were satisfied.

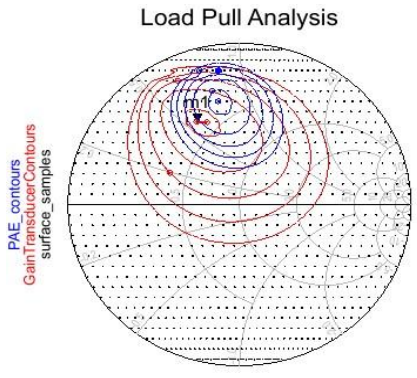

Fig. 3. Optimum Point on The Smith Chart from Load Pull Analysis

The HEMT die attached to the printed circuit board using the 25 µm gold bond wires for the gate and the drain connections. Bond wire effects were included in the design with the proper EM-based model where coupling among multiple wires and the ground plane and the mutual inductance are included [9]. Since the desired size is tiny for distributed elements at this frequency, the 0201 discrete lumped components were used for the power amplifier module design. The output matching was designed with a DC block capacitor and a low-pass LC network for harmonic suppression. The input matching network was built with a high pass T-network and stability network, and bond wire effects were included in the matching. The stability is ensured with a shunt RC at the gate of the transistor with a 100Ω.

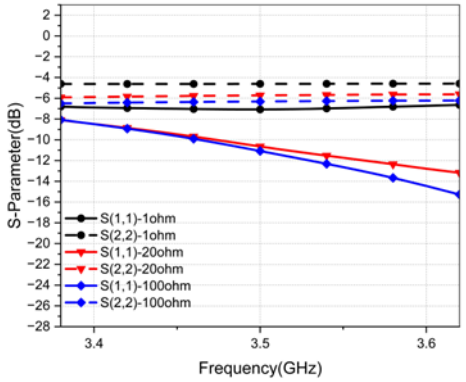

Fig. 4. Input and Output Return Loss Results for Altering Resistor Values

Different values of the resistor studied the determination of the resistor value. Fig. 4 indicates the input and output return loss values with the resistor change. Since the resistor value also modifies the matching network, a suitable value for the stability resistor was selected 100Ω for the better input and output return losses. After determining the stability resistor value, the layout was designed per the design goal of the total size. Fig. 5 shows the layout design of the PAM. 2-layer Rogers4003C laminate was selected for its high performance on high-frequency applications. Discrete lumped element packages and die transistor package was fit with careful floor planning, and conductor spaces were left for post-design optimization. The total size of the designed module is 8.5 x 5.2 mm.

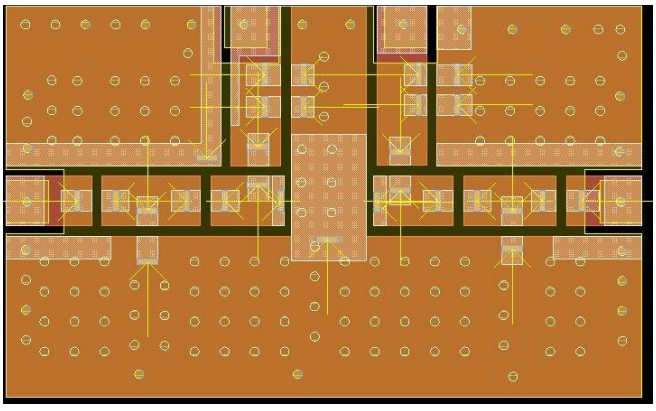

Fig. 5. . Designed Layout of PAM

Electromagnetic(EM) co-simulation of the designed layout was done with the real-life models of the discrete components, including the parasitic effects. Addition of layout parasitics and models of parts, matching networks were optimized, and the final circuit is shown in Fig. 6. Small signal and extensive signal simulations were performed after the design of the PAM.

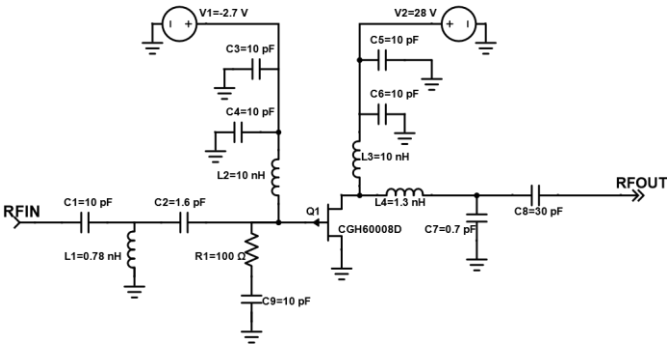

Fig. 6. Power Amplifier Module Schematic with Values

III. Simulation Results

A. Small Signal Simulation

The small signal of the PAM was analyzed. The input and output return losses were simulated with small signal gain. The power amplifier's input and output return losses are essential parameters since the amplified signal may damage the connected devices. Fig. 7 shows the S-parameter results of the designed PAM from DC-10 GHz. The simulated results of small signal gain are 13.8 dB, input return loss is -11.7 dB, and output return loss is -6.4 dB at 3.5 GHz. The frequency range of 3.4-3.6 GHz, as the design goal shows, the matching networks were designed appropriately.

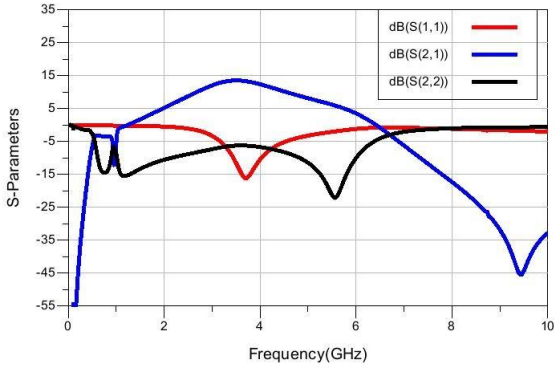

Fig. 7. Small Signal Results

As the maximum small signal gain and the desirable input-output return loss values, the small signal stability condition of the PAM was checked using μ and μ' stability criterion. The expected values of μ and μ' are above 1 for unconditional stability for a device. Fig. 8 indicates the small signal stability criteria μ and μ' from DC to 20 GHz. The chosen shunt resistor and capacitor values ensured the small-signal unconditional stability.

B. Large Signal Simulation

The power amplifiers are evaluated for their large-signal characteristics as they are used almost always under large-signal stimulation. The power amplifier; therefore, the large signal simulation was performed for the designed PAM. Fig. 9 shows the transducer power gain, PAE, and output power versus input power. Harmonic balance simulation results show that for the input power of 24.75 dBm, output power resulted in 37.1 dBm output power. PAE was 39%, and transducer power gain was 12.4 dB at the frequency of 3.5 GHz. The gain compression was around 1 dB.

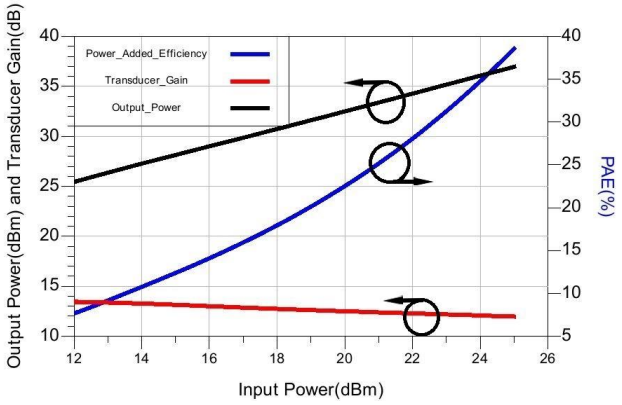

Fig. 9. Large Signal Results

Moreover, large-signal stability was checked. The large-signal stability was analyzed for an input power of 24.75 dBm. The loop gain is shown in (1). Considering an amplifier with an open loop gain of A, in real life, it has Feedback of β that comes from parasitic magnetic and electric couplings from the ground plane. The stability analysis can be made with the loop gain calculation [10].

$$A_f = \frac{A\beta}{1+A\beta} \quad (1)$$

The loop gain, $A\beta$, determines the stability with its value and phase. If the loop gain equals 1 with the phase of π degree, the system becomes unstable with the unrealistic A_f [11]. Loop gain was simulated for the PAM. For the output power of 5W, the loop gain simulation result is demonstrated in Fig. 10. Logarithmic result of loop gain was simulated for the drain and gate of the transistor. The maximum result of the logarithmic loop gain is around -18 dB from DC to 10 GHz, so the value of loop gain is lower than 1. This result ensures that large signal stability was granted.

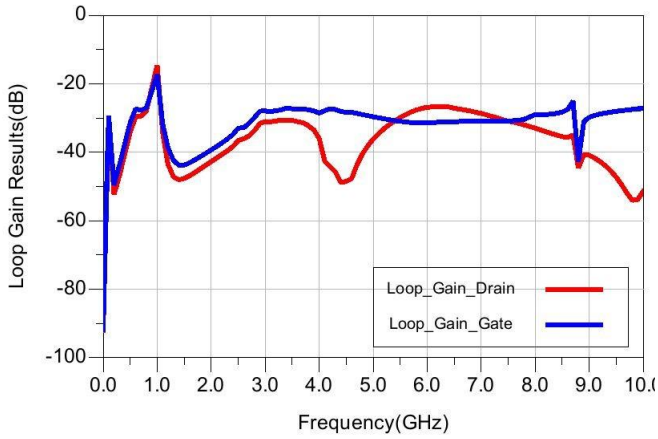

Fig. 10. Large Signal Loop Gain Result

TABLE II. PERFORMANCE COMPARISON OF RECENT GAN PAS

Ref.	Frequency(GHz)	Output Power(dBm)	Efficiency (%)	Size (mm^2)
[12]	3.6	40	40%	8x8
[13]	3.4–3.7	38.8	33 – 55%	4x2.5
[14]	3.0-3.6	34.2	45.9-50.2%	78x60
[15]	3.25	37.5	28%	3.5x2.8
This Work	3.4-3.6	37	39%	8.5x5.2

Table (II) shows a comparison of our work with the recent PAs.

IV. CONCLUSION

This work presents a compact hybrid power amplifier design with a GaN HEMT die, lumped, and distributed matching networks on a laminate. The amplifier is constructed as a class-AB single-stage topology with a low-pass output matching network and a high-pass input matching network in LC configuration. A shunt RC network is used at the input to increase stability. A parametric study of the resistor value is presented. The output power is simulated as 37.1 dBm with 39% PAE and 12.4 dB signal gain. The input return loss is -11.7 dB, and the output return loss is -6.4 dB at the center of the operating band, 3.5 GHz. The device is unconditionally stable across its working range. The design goals are achieved with a 1-stage 8.5 x 5.2 mm power amplifier module. The manufactured device prototype is being measured at the moment of this manuscript writing.

ACKNOWLEDGMENT

The authors would acknowledge Nero Industries Co. for funding this project.

REFERENCES

[1] Y. -C. Hsu, J. -Y. Li and L. -K. Wu," High reliable Doherty power amplifier module for LTE small cell base station," 2017 IEEE CPMT Symposium Japan (ICSJ), 2017, pp. 37-40, doi: 10.1109/ICSJ.2017.8240083.

[2] P. Colantonio, F. Giannini, and E. Limiti, Eds., "Power Amplifier Fundamentals," in High-Efficiency RF and Microwave Solid State Power Amplifiers. 2009, doi: 10.1002/9780470746547.ch1.

[3] V. Camarchia, R. Quaglia, A. Piacibello, D. P. Nguyen, H. Wang and A. -V. Pham, "A Review of Technologies and Design Techniques of Millimeter-Wave Power Amplifiers," in IEEE Transactions on Microwave Theory and Techniques, vol. 68, no. 7, pp. 2957-2983, July 2020, doi: 10.1109/TMTT.2020.2989792.

[4] R. S. Pengelly, S. M. Wood, J. W. Milligan, S. T. Sheppard and W. L. Pribble, "A Review of GaN on SiC High Electron-Mobility Power Transistors and MMICs," in IEEE Transactions on Microwave Theory and Techniques, vol. 60, no. 6, pp. 1764-1783, June 2012, doi: 10.1109/TMTT.2012.2187535.

[5] G. Lv, W. Chen, X. Liu and Z. Feng, "A Dual-Band GaN MMIC Power Amplifier With Hybrid Operating Modes for 5G Application," in IEEE Microwave and Wireless Components Letters, vol. 29, no. 3, pp. 228-230, March 2019, doi: 10.1109/LMWC.2019.2892837.

[6] CGH6008D Datasheet, Cree, Inc.

[7] G. Monprasert, P. Suebsombut, T. Pongthavornkamol, and S. Chalermwisutkul," 2.45 GHz GaN HEMT Class-AB RF power amplifier design for wireless communication systems," ECTI-CON2010: The 2010 ECTI International Conference on Electrical Engineering/Electronics, Computer, Telecommunications, and Information Technology, 2010, pp. 566-569.

[8] Y. Tao, R. Ishikawa, and K. Honjo," Optimum load impedance estimation for high-efficiency microwave power amplifier based on low-frequency active multi-harmonic load-pull measurement," 2015 Asia-Pacific Microwave Conference (APMC), 2015, pp. 1-3, doi: 10.1109/APMC.2015.7411814.

[9] Alexe L. Nazarian, et al., "A Physics-Based Causal Bond-Wire Model' for RF Applications," IEEE Transaction on Microwave Theory and Techniques, Vol. 60, No. 12, pp. 3683-3692, December 2012.

[10] B. Zhao, C. Sanabria, and T. Hon," A 2-Stage S-Band 2W CW GaN MMIC Power Amplifier in an Overmold QFN Package," 2022 IEEE Texas Symposium on Wireless and Microwave Circuits and Systems (WMCS), 2022, pp. 1-5, doi:10.1109/WMCS55582.2022.9866273.

[11] Sedra, A. S., Smith, K. C., Carusone, T. C., & Gaudet, V.," Feedback," in Microelectronic circuits. 2020, Oxford University Press.

[12] S. Inoue and K. Ebihara, "Broadband 2-stage GaN power amplifier in an 8×8mm package," 2016 11th European Microwave Integrated Circuits Conference (EuMIC), 2016, pp. 229-232, doi: 10.1109/EuMIC.2016.7777532.

[13] A. Seidel, J. Wagner and F. Ellinger, "3.6 GHz Asymmetric Doherty PA MMIC in 250 nm GaN for 5G Applications," 2020 German Microwave Conference (GeMiC), Cottbus, Germany, 2020, pp. 1-4.

[14] Y. Komatsuzaki, K. Nakatani, S. Shinjo, S. Miwa, R. Ma and K. Yamanaka, "3.0–3.6 GHz wideband, over 46% average efficiency GaN Doherty power amplifier with frequency dependency compensating circuits," 2017 IEEE Topical Conference on RF/Microwave Power Amplifiers for Radio and Wireless Applications (PAWR), 2017, pp. 22-24, doi: 10.1109/PAWR.2017.7875563.

[15] E. M. Suijker, M. Sudow, M. Fagerlind, N. Rorsman, A. P. de Hek and F. E. van Vliet, "GaN MMIC Power Amplifiers for S-band and X-band," 2008 38th European Microwave Conference, Amsterdam, Netherlands, 2008, pp. 297-300, doi: 10.1109/EUMC.2008.4751447.

.