مجلة جامعة البعث

سلسلة العلوم الهندسية الميكانيكية والكهربائية والمعلوماتية

مجلة علمية محكمة دورية

المجلد 43 . العدد 10

1442 هـ - 2021 م

تهدف المجلة إلى نشر البحوث العلمية الأصيلة، ويمكن للراغبين في طلبها الاتصال بالعنوان التالي:

رئيس تحرير مجلة جامعة البعث

سورية . حمص . جامعة البعث . الإدارة المركزية . ص . ب (77)

. هاتف / فاكس : 2138071 31 963 ++

. موقع الإنترنت : www.albaath-univ.edu.sy

. البريد الالكتروني : magazine@ albaath-univ.edu.sy

ISSN: 1022-467X

قيمة العدد الواحد : 100 ل.س داخل القطر العربي السوري

25 دولاراً أمريكياً خارج القطر العربي السوري

قيمة الاشتراك السنوي : 1000 ل.س للعموم

500 ل.س لأعضاء الهيئة التدريسية والطلاب

250 دولاراً أمريكياً خارج القطر العربي السوري

توجه الطلبات الخاصة بالاشتراك في المجلة إلى العنوان المبين أعلاه.

يرسل المبلغ المطلوب من خارج القطر بالدولارات الأمريكية بموجب شيكات باسم جامعة البعث.

تضاف نسبة 50% إذا كان الاشتراك أكثر من نسخة.

شروط النشر في مجلة جامعة البعث

الأوراق المطلوبة:

- 2 نسخة ورقية من البحث بدون اسم الباحث / الكلية / الجامعة) + CD / word من البحث منسق حسب شروط المجلة.
- طابع بحث علمي + طابع نقابة معلمين.
- **اذا كان الباحث طالب دراسات عليا:**

يجب إرفاق قرار تسجيل الدكتوراه / ماجستير + كتاب من الدكتور المشرف بموافقته على النشر في المجلة.

- **اذا كان الباحث عضو هيئة تدريسية:**

يجب إرفاق قرار المجلس المختص بإنجاز البحث أو قرار قسم بالموافقة على اعتماده حسب الحال.

- **اذا كان الباحث عضو هيئة تدريسية من خارج جامعة البعث :**

يجب إحضار كتاب من عمادة كليته تثبت أنه عضو بالهيئة التدريسية و على رأس عمله حتى تاريخه.

- **اذا كان الباحث عضواً في الهيئة الفنية :**

يجب إرفاق كتاب يحدد فيه مكان و زمان إجراء البحث ، وما يثبت صفته وأنه على رأس عمله.

- **يتم ترتيب البحث على النحو الآتي بالنسبة لكليات (العلوم الطبية والهندسية والأساسية والتطبيقية):**

عنوان البحث . . ملخص عربي و إنكليزي (كلمات مفتاحية في نهاية الملخصين).

1- مقدمة

2- هدف البحث

3- مواد وطرق البحث

4- النتائج ومناقشتها .

5- الاستنتاجات والتوصيات .

6- المراجع.

- **يتم ترتيب البحث على النحو الآتي بالنسبة لكليات (الآداب – الاقتصاد– التربية – الحقوق – السياحة – التربية الموسيقية وجميع العلوم الإنسانية):**
- عنوان البحث . . ملخص عربي و إنكليزي (كلمات مفتاحية في نهاية الملخصين).

1. مقدمة.
2. مشكلة البحث وأهميته والجديد فيه.
3. أهداف البحث و أسئلته.
4. فرضيات البحث و حدوده.
5. مصطلحات البحث و تعريفاته الإجرائية.
6. الإطار النظري و الدراسات السابقة.
7. منهج البحث و إجراءاته.
8. عرض البحث و المناقشة والتحليل
9. نتائج البحث.
10. مقترحات البحث إن وجدت.
11. قائمة المصادر والمراجع.

7- يجب اعتماد الإعدادات الآتية أثناء طباعة البحث على الكمبيوتر:

أ- قياس الورق 17.5×25 B5.

ب- هوامش الصفحة: أعلى 2.54- أسفل 2.54 – يمين 2.5- يسار 2.5 سم

ت- رأس الصفحة 1.6 / تذييل الصفحة 1.8

ث- نوع الخط وقياسه: العنوان . Monotype Koufi قياس 20

. كتابة النص Simplified Arabic قياس 13 عادي . العناوين الفرعية Simplified Arabic قياس 13 عريض.

ج . يجب مراعاة أن يكون قياس الصور والجداول المدرجة في البحث لا يتعدى 12سم.

8- في حال عدم إجراء البحث وفقاً لما ورد أعلاه من إشارات فإن البحث سيهمل ولا يرد البحث إلى صاحبه.

9- تقديم أي بحث للنشر في المجلة يدل ضمناً على عدم نشره في أي مكان آخر، وفي حال قبول البحث للنشر في مجلة جامعة البعث يجب عدم نشره في أي مجلة أخرى.

10- الناشر غير مسؤول عن محتوى ما ينشر من مادة الموضوعات التي تنشر في المجلة

11- تكتب المراجع ضمن النص على الشكل التالي: [1] ثم رقم الصفحة ويفضل استخدام التهميش الإلكتروني المعمول به في نظام وورد WORD حيث يشير الرقم إلى رقم المرجع الوارد في قائمة المراجع.

تكتب جميع المراجع باللغة الانكليزية (الأحرف الرومانية) وفق التالي:

آ . إذا كان المرجع أجنبياً:

الكنية بالأحرف الكبيرة . الحرف الأول من الاسم تتبعه فاصلة . سنة النشر . وتتبعها معترضة (–) عنوان الكتاب ويوضع تحته خط وتتبعه نقطة . دار النشر وتتبعها فاصلة . الطبعة (ثانية . ثالثة) . بلد النشر وتتبعها فاصلة . عدد صفحات الكتاب وتتبعها نقطة.

وفيما يلي مثال على ذلك:

–MAVRODEANUS, R1986– **Flame Spectroscopy**. Willy, New York, 373p.

ب . إذا كان المرجع بحثاً منشوراً في مجلة باللغة الأجنبية:

. بعد الكنية والاسم وسنة النشر يضاف عنوان البحث وتتبعه فاصلة، اسم المجلد ويوضع تحته خط وتتبعه فاصلة . المجلد والعدد (كتابة مختزلة) وبعدها فاصلة . أرقام الصفحات الخاصة بالبحث ضمن المجلة.

مثال على ذلك:

BUSSE,E 1980 Organic Brain Diseases **Clinical Psychiatry News** , Vol. 4. 20 – 60

ج. إذا كان المرجع أو البحث منشوراً باللغة العربية فيجب تحويله إلى اللغة الإنكليزية و التقيد

بالبنود (أ و ب) ويكتب في نهاية المراجع العربية: (المراجع In Arabic)

رسوم النشر في مجلة جامعة البعث

1. **دفع رسم نشر (20000) ل.س عشرون ألف ليرة سورية عن كل بحث لكل باحث يريد نشره في مجلة جامعة البعث.**
2. **دفع رسم نشر (50000) ل.س خمسون الف ليرة سورية عن كل بحث للباحثين من الجامعة الخاصة والافتراضية .**
3. **دفع رسم نشر (200) مئتا دولار أمريكي فقط للباحثين من خارج القطر العربي السوري .**
4. **دفع مبلغ (3000) ل.س ثلاثة آلاف ليرة سورية رسم موافقة على النشر من كافة الباحثين.**

المحتوى

دراسة سلسلة الكتل وإمكانية استخدامها في التحقق من ملكية المفتاح العام في إرسال رسائل معماة

طالب الماجستير: م .محمد خليل

المعهد العالي للعلوم التطبيقية والتكنولوجيا

اشراف الدكتور: محمد الشايطة + د. محمد عصورة

ملخص البحث:

نظرا لتزايد استخدام الشبكات في الوقت الحاضر والحاجة الكبيرة لنقل البيانات من خلالها، ظهرت العديد من التهديدات التي تواجه أمن وسلامة هذه التناقلات وبالمقابل أصبحت طرق التعمية القديمة أكثر هشاشة في مواجهة المخترقين وأبرزها البنية التحتية للمفاتيح العامة PKI التي تبنى عليها الكثير من تطبيقات الويب مثل(Https، S/MIME) وأبرز هذه المشاكل هي المركزية والبنية المعقدة في توزيع الشهادات، لذلك ظهرت الحاجة إلى البحث عن بدائل وآليات جديدة تلبي احتياجات المستخدمين لضمان الأمن والخصوصية.

تعد تقنية سلسلة الكتل من أكثر التقنيات الواعدة التي تتمتع بمزايا أمنية كبيرة ولامركزية في بنية الشبكة، ومن هنا قمنا بإنشاء نموذج بديل عن PKI بالاعتماد على تقنية سلسلة الكتل وخوارزميات التعمية غير المتناظرة وتوظيفها في تطبيق إرسال رسائل معماة بالمفتاح العام، حيث يقوم التطبيق بتسجيل مستخدمين جدد، وقبل إرسال أي رسالة يتم التحقق من ملكية المفتاح العام للمستقبل من سلسلة الكتل في شبكة Ethereum Blockchain، وتطرقنا أيضا إلى حل مشكلة الشهادات الملغاة مثلاً في Https التي تأخذ وقت طويل من أجل تعميم الشهادة الملغاة لكافة المستخدمين والمتصفحات، وذلك من خلال استخدام توابع الحذف في العقد الذكي المرفوع على سلسلة الكتل في

Ethereum والتي توفر لنا بيئة مناسبة لاختبار التطبيقات اللامركزية القائمة على سلسلة الكتل.

الكلمات المفتاحية: البنية التحتية للمفاتيح العامة، المرجع المصدق، سلسلة الكتل، خوارزمية التعمية غير المتناظرة.

Study of the blockchain and its potential use in verifying ownership of the public key in sending encrypted messages

Paper Research of Master Thesis

Eng. Mohammad khalil
Dr. Mohammed Alchaita
Dr. Mohammad Assoura

Abstract:

These days, the use of networks and the transfer of data is increasing, many threats of security and safety for these transmissions have appeared. On the other side, old encryption methods have become weaker for hackers. PKI (public key Infrastructure) is a technology used in web applications to make trust between parties. But there are some problems in the PKI like the central and the complex structure in the distributed certificates. Therefore, it became necessary searching for alternatives and new mechanisms ensure the users' security and privacy. Blockchain technology is one of the most promising technologies; it has terrific security advantages and decentralization network structure. Therefore, we created an alternative model for PKI based on blockchain technology, then employed it in an application for sending encrypted messages, which use asymmetric cryptography algorithms. The application registers new users and generates a public and private key for them, then before sending any message it verifies the owner of the receiver's public key from the Ethereum blockchain. We also worked on solving the problem of revoked certificates. For example, on Https, it takes a long time for publishing the revoked certificate to all users and browsers, we solved this issue by using the deletion methods in the smart contract which uploaded to the Ethereum blockchain. Then, we evaluated the security, functionality, and performance of our model, and compared the time between getting and revoking certificates in Https. The results showed a simple way of registering users,

ensuring that the public key is not either changed or stolen and canceled the central structure in PKI. We also got a speed in performance and solved the revoked certificates problems fast and efficiently during about 1 min.

Keywords: Public key infrastructure, certification authority, blockchain, asymmetric cryptography algorithm

1. مقدمة

في الوقت الحاضر، تعد المراسلة الإلكترونية أكثر تطبيقات الشبكة استخدامًا، لذلك لابد من تلبية المتطلبات الأمنية والخصوصية لأطراف المراسلة ومن أكثر الأساليب المستخدمة لذلك بروتوكولات تعمية البريد الإلكتروني S/MIME وبرنامج التعمية Pretty Good Privacy (PGP) التي توفر السرية مع التعمية والمصادقة عبر التوقيع وشبكة الثقة عبر التحقق من هوية أطراف المراسلة وتستخدم أيضاً بروتوكولات تعمية الاتصال بين الخادم والزبون SSL .

وتعتمد جميع هذه البروتوكولات والبرامج على البنية التحتية للمفتاح العام PKI، ولكنها في الواقع تواجه تهديدات أمنية متعددة، مثل هجوم MITM وهجوم EFAIL.

تعتبر البنية التحتية للمفتاح العام (PKI) مكونًا مهمًا لتأسيس المصادقة في الشبكات، وتوفر ضمانات للثقة في الشهادة الموقعة من المرجع المصدق (CA).

تصادق الشهادات على المفاتيح العامة وتسمح بإجراء عمليات التعمية مثل تعمية البيانات والتوقيع الرقمي، ولكن المصادقة والتحقق من الهوية مركزيان في البنية التحتية للمفتاح العام، مما يخلق إمكانية لفشل النقطة الواحدة.

سلسلة الكتل هي تقنية مبتكرة تتغلب على هذه التهديدات وتسمح بتطبيق اللامركزية على العمليات الحساسة مع الحفاظ على مستوى عال من الأمان، حيث يلغي الحاجة إلى وسطاء موثوق بهم، ويمكن لجميع عقد الشبكة الوصول إلى سلسلة الكتل وتتبع جميع المعاملات التي يتم إجراؤها.

سلسلة الكتل من شأنها أن تجعل المراسلات أكثر أمانا، ونقترح تصميم نموذج للمراسلة مع الحفاظ على أمن البيانات المسجلة على سلسلة الكتل، وذلك باستخدام عقد ذكي للتحقق من الهويات القائمة على نظام لا مركزي بالكامل يسمح للمستخدمين بتبادل الرسائل بأمان.

تم التصميم باستخدام تقنية سلسلة الكتل لجعل العملية أكثر وثوقية، وتعد تقنية سلسلة الكتل حلاً لتحقيق تكامل البيانات، وبالاعتماد على بنية الشبكة اللامركزية وآلية عمل سلسلة الكتل نحصل على مقاومة للتعديل والتزوير مما يحقق تناقل بيانات بشكل آمن وسليم.

إن تقنية سلسلة الكتل لامركزية، ولا يمكن لأي سلطة مركزية الموافقة على المعاملات بطريقة فردية، وإنما يجب أن تتوصل جميع العقد في الشبكة إلى إجماع للتحقق من صحة المعاملات بطريقة آمنة، ولا يمكن تغيير السجلات السابقة. وإذا أراد شخص ما تغيير السجلات السابقة يجب إنفاق تكلفة عالية جدًا حيث يتعين عليه الوصول إلى 51% من أجهزة الكمبيوتر في الشبكة التي تستضيف قاعدة بيانات سلسلة الكتل في نفس الوقت للتعامل معها، وهو أمر مستحيل عمليا[1].

تم إنشاء عملة البيتكوين (bitcoin) المعماة من قبل شخص غير معروف باستخدام الاسم المستعار Satoshi Nakamoto في عام 2008، تقوم Bitcoin بإنشاء

المعاملات وإرسالها إلى سلسلة الكتل بمجرد التحقق من صحة عملية النقل، يتم نشر المعاملات من خلال الشبكة وإضافتها إلى كتلة وبمجرد امتلاء الكتلة يتم إلحاق الكتلة بسلسلة الكتل عن طريق إجراء عملية تنقيب.

تحاول العقدة المنقبة حل لغز تعمية صعب عن طريق عملية تسمى Proof of Work (PoW)، وتضيف العقدة التي تحل اللغز أولاً الكتلة الجديدة إلى سلسلة الكتل، تعتمد Bitcoinعلى الثقة اللامركزية، ويتم تحقيق الثقة كخاصية ناتجة عن تفاعلات المشاركين المختلفين في نظام البيتكوين [2] ولا يمكن اختراق البيانات المخزنة على سلسلة الكتل أو تعديلها أو حذفها، ويكون ثبات البيانات في سلسلة الكتل أقوى عندما تكون السلسلة أطول[3].

2. الهدف من البحث

تدور مسألة البحث حول موضوع إيجاد بديل آمن وغير مركزي للبنية التحتية للمفتاح العام واستخدامها في إرسال الرسائل بطريقة آمنة بحيث نبحث عن آلية يتم فيها تسجيل المفتاح العام والتحقق منه بكل شفافية وأمان بالسرعة والأداء المطلوبين وذلك باستخدام تقنية سلسلة الكتل، بحيث نجيب عن الأسئلة التالية:

هل تستطيع تقنية سلسلة الكتل حل مشاكل PKI وأن تكون بديلة عنها في إرسال الرسائل؟

في سلسلة الكتل، البيانات المشتركة هي كل عملية نقل تمت على الشبكة، يتم تخزينها في دفتر الأستاذ الموزع في نسخ متعددة على شبكة من أجهزة الكمبيوتر تسمى العقد في كل مرة يقوم شخص ما بإرسال عملية نقل إلى دفتر الأستاذ، يتم التحقق من العقد للتأكد من صلاحية عملية النقل ويتم إنشاء عملية النقل في هيكل البيانات المتسلسل لسلسلة الكتل و تسجيل طابع زمني جديد في نفس الوقت، ولن يسمح بعد ذلك بأي تعديل لعملية نقل تمت من قبل.

كيف تستطيع تقنية سلسلة الكتل حل مشاكل PKI في إرسال الرسائل ؟

سوف نقوم بعمل تطبيق وبناء عقد ذكي على شبكة Ethereum public blockchain وندرس خصائص النموذج المقترح ومعاملاته وأدائه من حيث معالجته لمشاكل PKI ومدى وثوقيته لاعتماده كحل بديل عن المرجع المصدق(Certificate Authority) CA.

3. مساهمة البحث

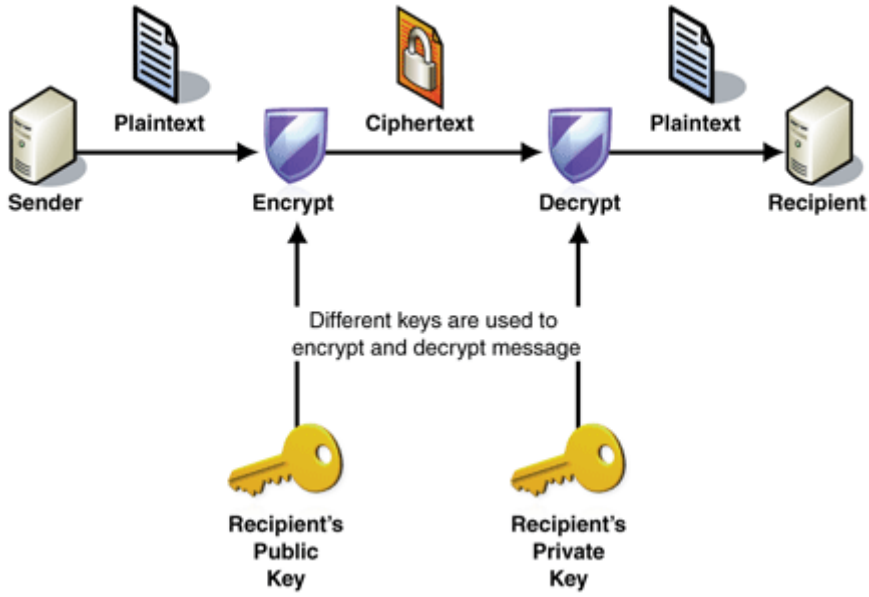
يمكننا تفنيد هذه المساهمة كما يلي:

- ❖ تصميم نموذج بديل عن PKI من حيث الوظيفة يستخدم الشبكات اللامركزية.
- ❖ تحقيق نسبة أمان عالية باستخدام سلسلة الكتل بالتحقق من ملكية المفتاح العام.
- ❖ دراسة وتصميم نموذج لتسجيل المفتاح العام للمستخدمين والتحقق منه بطريقة سريعة وباستخدام Ethereum blockchain.
- ❖ بناء تطبيق ارسال رسائل بطريقة معماة تستخدم سلسلة الكتل لتسجيل المفاتيح العامة والتحقق من ملكيتها.
- ❖ إيجاد حل سريع وفعال لإلغاء تسجيل المستخدم باستخدام سلسلة الكتل الموافق لإلغاء الشهادة في مقدمة عامة عن البنية التحتية للمفتاح العام (PKI).

4. مفهوم البنية التحتية للمفتاح العام (PKI)

PKI هو اختصار لـ Public Key Infrastructure هي تقنية لمصادقة المستخدمين والأجهزة في العالم الرقمي، والفكرة الأساسية هي أن يكون هناك طرف واحد أو أكثر من الأطراف الموثوقة يوقع رقميًا على المستندات التي تثبت أن مفتاح عام معين ينتمي إلى مستخدم أو جهاز معين، يمكن بعد ذلك استخدام المفتاح كهوية للمستخدم في الشبكات الرقمية.

وقد تم تطوير PKI لدعم تعمية المفتاح العام (غير المتناظر)، وفي هذا النوع من التعمية تتم تعمية الرسالة من قبل المرسل باستخدام المفتاح العام للمستقبل، ومن ثم يكون هذا المستقبل هو الوحيد الذي يمكنه فك تعمية هذه الرسالة باستخدام المفتاح الخاص به كما يوضح الشكل (4–1)، تم تقديم هذه الطريقة في التعمية منذ عام 1976 في [4] لحل مشكلة إدارة المفاتيح، باستخدام دليل يسمى الملف العام حيث تكون الإدخالات عبارة عن الاسم والرقم والمفتاح العام، يبحث المرسل عن المستلم في الملف العام باسمه للعثور على مفتاحه العام، وفقًا لهذا السيناريو لا يتمتع المرسل بالثقة الكاملة في أن المفتاح



الشكل (4-1) تعمية رسالة بالاعتماد على PKI

ينتمي حقًا إلى المستلم المطلوب، اقترح Kohnfelder في [5] حلاً عن طريق الشهادة أو التوقيع الرقمي على كل إدخال في "الملف العام"، بحيث يمكن توزيع الشهادات من خلال الشبكة بشكل آمن.

في الثمانينيات قرر الاتحاد الدولي للاتصالات (ITU) إنشاء دليل أكبر لتغطية جميع الأشخاص والأجهزة في جميع أنحاء العالم، وبالتالي كانت النتيجة معيارًا يسمى X.500 ويحدد [6] جميع خصائص هذا المعيار، تم اقتراح معيار آخر يسمى X.509 لأغراض المصادقة، ولا يمكن لأي شخص تغيير أي إدخال في الدليل إلا إذا كان لديه إذن، يحدد معيار X.509 تنسيق الشهادة حيث يربط هوية صاحب المفتاح بالمفتاح العام.

أدت جميع التطورات في مجال تعمية المفتاح العام إلى إنشاء بنية تحتية للمفتاح العام (PKI) حيث تلعب الشهادات الرقمية دورا جوهريا فيها، ولمزيد من الوثوقية تم تقديم المرجع المصدق (CA) [7]، وهو طرف موثوق به مسؤول عن التحقق من الشهادات

والتوقيع عليها لذلك ساعد PKI المرسل على استرداد المفتاح العام للمستلم المطلوب مع الثقة في أن هذا المفتاح هو بالفعل المفتاح العام للمستلم.

5. أبرز مشاكل PKI

لنفترض مثلاً أن مستخدم A يريد أن يرسل إلى B رسالة "دعنا نتحدث"، يتولد زوجين من مفاتيح التعمية غير المتناظرة خاصة PrA و PbA عامة.

يقول A: "مرحبا أنا A هذا هو مفتاحي العام، وهذه هي خوارزمية التعمية المتناظرة التي أعرفها"، ينشئ B مفتاحًا متماثلا S، يعميه بالمفتاح العام لـ A PbA(S) والآن لا يمكن فك تعمية S حتى بواسطة B، لأن A فقط يمكنه فك تعمية الرسالة بمفتاحه الخاص، في النهاية لدى B و A مفتاح متماثل لنقل موثوق للرسائل بينهما ومنع أي شخص من قراءة مراسلاتهما.

يتبين لدينا ثلاث وظائف رئيسية لبروتوكول SSL (المصادقة والتعمية والنزاهة)، والأهم هو المصادقة.

و لكن كيف ل A وB التأكد من عدم وجود شخص في المنتصف يمكنه قراءة رسائلهما بحيث ينشئ زوج المفاتيح الخاص به، ويعطي ل B مفتاحه على أنه المفترض من A، وينظم قناتين معماتين ويقرأ الرسائل.

يتم حل هذه المشكلة فقط بالإستعانة بطرف ثالث يسمى CA (Certificate Authority) يمكن أن يضمن أن مفتاح PbA ينتمي إلى A ويحتفظ بسجل المفاتيح العامة للجميع، يستطيع A أن يأخذ مفتاحه العام PbA ويسجله في CA، عندما يتلقىB المفتاح العام من A، يمكنه الذهاب إلى CA والتحقق من ملكية A للمفتاح إذا لم يتطابق المفتاح فهناك شخص في الوسط.

ولكن من غير المريح أن يذهب B إلى CA في كل مرة، لذلك يمكن إجراء المصادقة نفسها مع إدارة وسيطة تأخذ صلاحياتها من CA.

لدى المرجع المصدق (CA) زوج مفاتيح Pb0 وPr0 عندما يأتي A بمفتاحه العام تُصدر CA شيئًا مثل البطاقة التي تقول إنه A، وتحوي المفتاح العام PbA وبعض المعلومات الإضافية (مثل رقم الهوية) وتضيف حقلاً لتوقيعها.

يأخذ CA جميع المعلومات من البطاقة، ويجزئها، ويعميها بمفتاحه الخاص، ويطلق عليها توقيعًا رقميًا.

وتطلق CA الآن على هذه البطاقة شهادة، الآن يمكن ل A تبادل الرسائل مع B ليس فقط الاسم والمفتاح العام ولكن أيضًا شهادته.

سيضطر B للذهاب إلى CA مرة واحدة فقط، ويطلب منهم مفتاحهم العام، تعتبر أي معلومات يمكن لهذا المفتاح فك تعميتها بمثابة معلومات تمت تعميتها من قبل CA، والآن لا يمكن لشخص في المنتصف قراءة الرسائل إلا في حال التقاط المفتاح الخاص بالمرجع CA.

فيجب على كل مستخدم إضافة مفاتيح مراكز التصديق الأخرى إلى قائمته الموثوقة، ويبدأ بالاحتفاظ بسجله من المفاتيح العامة لمراكز التصديق، تصبح المنظمات التي توقع الشهادات كبيرة جدا يتم وصفها في تسلسل هرمي.

المرجع المصدق الجذري RCA لا يوقع على شهادات المستخدمين العاديين، ولكنه يوقع فقط على شهادات مراجع التصديق المتوسطة بعد التحقق منها [8]، يكفي أن يحتفظ B فقط بالمفاتيح العامة لمراكز التصديق، ولا يحصل من A على شهادته فحسب بل أيضًا على شهادات المراكز المتوسطة، بحيث يمكن فحصها حتى مركز الجذر.

مما سبق نجد أن النظام أصبح أكثر تعقيدًا ومركزية، ويكون أمام الشخص في المنتصف فرصة لقراءة الرسائل.

يكون لدى B قائمة صغيرة بمراكز تصديق الشهادات يحوي Windows حوالي 50 مركزًا لتصديق الشهادات أثناء التثبيت، وأيضاً من الصعب عليه اتباع سلسلة مراكز التصديق بأكملها في كل مرة.

يثق B في قائمته لمراكز التصديق بنسبة 99.9 في المائة، يمكن للشخص في المنتصف عن طريق استخدام إحدى الطرق (الهندسة الاجتماعية ، القرصنة ،الاختراق) تسجيل مركز تصديق شهادة مزيف خاص به في سجل B.

قد لا تكون سلطة الشخص في المنتصف كافية للتزوير من مراكز إصدار الشهادات الجذرية، ولكن يوجد طريقة أسهل حيث يذهب إلى مركز تصديق أدنى مستوى وفق التسلسل الهرمي لمراكز التصديق ، ويرشي الإدارة لتوقيع شهادته كشهادة وسيطة مصدقة، عندها يمكنه أن يرى حركة المرور والتعديل عليها، و لن يلاحظ المستخدم أي شيء، فالمتصفح لا يظهر أي تحذيرات.

ويوجد أيضا مشكلة معروفة إذا تم العثور على هذه الشهادات المزيفة ومراكز الوسط والجذر المخترقة، فيجب وضع علامة على هذه الشهادات على أنه تم إبطالها واختراقها (الشهادات المبطلة)، وتقوم بذلك سلطة التسجيل RA بشكل أساسي، وتكون RA مسؤولة عن قبول طلبات الشهادات الرقمية والتحقق من هوية الذي يقدم الطلب [9]،

هذا يعني أنه بالإضافة إلى تخزين شهادات الجذر، يحتاج المستخدم أيضًا إلى مزامنتها باستمرار مع قائمة الشهادات المبطلة عبر الإنترنت، يتم تنفيذ هذه الآلية من خلال بروتوكولات CRL (Certificate Revocation List)[10].

المشكلة في الشهادات الملغاة هي أن هناك بالفعل عددًا كبيرًا منها، في عام 2013 كان هناك حوالي 3 ملايين شهادة ملغاة [11]، و23000 شهادة ملغاة من سيمانتيك فقط في 2018 [12].

عطل Chrome الميزة الافتراضية للتحقق من صحة الشهادات الباطلة بالكامل قبل بضع سنوات [13] لزيادة سرعة تحميل الصفحات، ويتضح أنه إذا تم العثور على الشخص المهاجم لدينا، فإن عملية منع أفعاله ستكون طويلة ولن تكون ناجحة دائمًا.

مما سبق يتضح لدينا أبرز المشاكل لبنية PKI:

- يوجد مركزية في النظام من خلال مفهوم مراكز تصديق الشهادات CA.
- مراجع التصديق المتوسطة كثيرة وغير معروفة وبالتالي يمكن اختراقها.

- صعوبة معرفة وتمييز الشهادات الملغاة وطول المدة الزمنية لتعميمها.

6. حلول مقترحة لمشاكل PKI

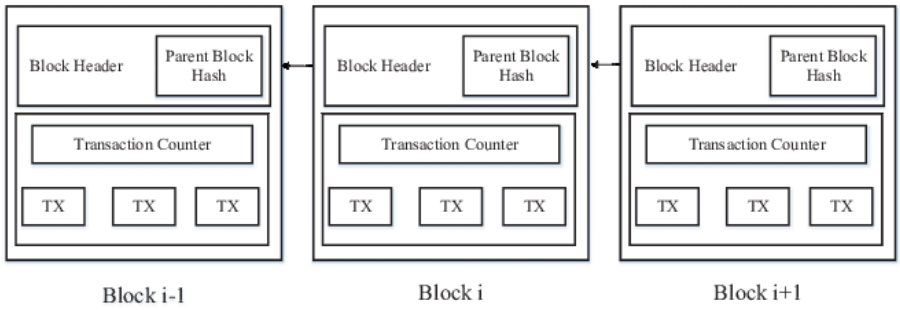
نقترح الإستفادة من تقنية سلسلة الكتل blockchain لما تتمتع من خصائص مميزة وأبرزها أنها لا مركزية، ولا يمكن لأي سلطة الموافقة على المعاملات بشكل فردي، ويجب أن تتوصل جميع العقد في الشبكة إلى إجماع للتحقق من صحة المعاملات بطريقة آمنة، ولا يمكن تغيير السجلات السابقة.

و إذا أراد شخص ما تغيير السجلات السابقة يجب إنفاق تكلفة عالية جدًا حيث يتعين على المهاجمين الوصول إلى 51% من العقد في الشبكة التي تستضيف قاعدة بيانات سلسلة الكتل في نفس الوقت للتعامل معها، وهو أمر مستحيل عمليا.

حيث أثبتت تقنية سلسلة الكتل نجاحا من خلال استخدامها في العملة الرقمية لBitcoin ونقترح في هذا البحث تصميم نموذج بديل عن PKI من خلال سلسلة الكتل وذلك بإنشاء نموذج نتمكن من خلاله من تسجيل وتأكيد هوية المفتاح العام بالتواصل مع شبكة سلسلة الكتل.

7. مفهوم سلسلة الكتل

قواعد بيانات موزعة تُنشئ قائمة مرتبة زمنيًا من السجلات وعمليات النقل المرتبطة ببعضها البعض بطريقة ثابتة عبر سلسلة من الكتل [14] تشكل هذه الكتل سلسلة خطية حيث تحتوي كل كتلة على قيمة تهشير الكتلة السابقة لإنتاج سلسلة من الكتل المترابطة الشكل (7−1)، وجميع سلاسل الكتل يتم الاحتفاظ بها في شبكة من العقد، تقوم كل عقدة بتنفيذ وتسجيل نفس المعاملات لديها وهي قادرة على قراءة أي معاملة تمر عبر الشبكة.



الشكل (7-1) بنية سلسلة الكتل

لا تعتبر سلسلة الكتل تقنية مستقلة، ولكنها تحتوي على تعمية ورياضيات وخوارزميات، تقوم شبكات الند للند بتجميع واستخدام خوارزميات المطابقة الموزعة لحل المشكلات التقليدية لمزامنة قواعد البيانات الموزعة فهي تعتبر بنية تحتية متكاملة ذات مجالات متعددة[15].

8. أهم ميزات سلسلة الكتل

تتمتع سلسلة الكتل بمزايا عديدة [16] أضافت نسبة عالية من الأمان والوثوقية للشبكات ومنها:

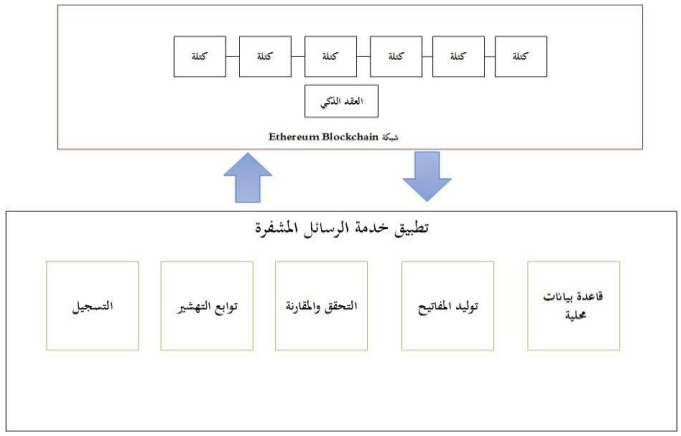
- لامركزية: لا تعتمد على عقدة أو سلطة مركزية واحدة للموافقة على عمليات النقل يمكن إنشاء البيانات وتخزينها وتحديثها بطريقة موزعة، ويجب على جميع المشاركين فيها الوصول إلى الإجماع لقبول عمليات النقل.
- شّفافة: جميع البيانات المخزنة في سلسلة الكتل شفافة لجميع العقد المشاركة، وشفافة أيضًا عند تحديث تلك البيانات، لذلك تعتبر سلسلة الكتل موثوقة.
- آمنة: يمكن توسيع قاعدة البيانات دون تغيير السجلات السابقة.

- التعمية: تستخدم سلسة الكتل مجموعة متنوعة من تقنيات التعمية ووظائف التهشير وأشجار Merkle التي سنتحدث عنها في الفقرة 4.2.2، وتقنية المفتاح العام والخاص [17].
- مفتوحة المصدر: معظم أنظمة سلسلة الكتل مفتوحة للجميع، لذلك يمكن التحقق منها بالعموم، ويمكن للمستخدمين استخدام تقنيات سلسلة الكتل لأي تطبيق يريدونه.
- مجهولة الهوية: تحل تقنية سلسلة الكتل مشاكل الثقة في شبكات الند للند، حيث يمكنها نقل البيانات وإرسالها إلى عنوان مجهول الهوية فقط بمعرفة عنوان المستقبل.
- ثابتة غير قابلة للتغيير: حيث يتم الاحتفاظ بأي تسجيل فيها إلى الأبد، ويمكن تغييره فقط في السيطرة على أكثر من 51٪ من العقد في نفس الوقت وهذا أمر شبه مستحيل.
- الإستقلال الذاتي: يمكن لأي عقدة في نظام سلسلة الكتل نقل البيانات وتحديثها بأمان بسبب وجود قواعد الإجماع.

9. النموذج المقترح

نستخدم بعض أجزاء النموذج المقترح في [18] لتصميم نموذج جديد حيث نضيف إليه التحسينات والوظائف التي سنذكرها لاحقاً في القسم العملي وذلك من أجل ضمان الوصول إلى شبكة آمنة محققة لخدمات السرية والخصوصية والسرعة باستخدام سلسلة الكتل.

يتألف النموذج المقترح من عدة أجزاء رئيسية أهمها شبكة Ethereum Blockchain، والعقد الذكي وتوابع التهشير المطبقة داخل تطبيق إرسال الرسائل كما يوضح الشكل (9-1).



الشكل (9–1) النموذج المقترح للتسجيل والتحقق من ملكية المفتاح العام

يقوم النموذج المقترح على تصميم آلية للتسجيل والتحقق من ملكية المفتاح العام، حيث يتم استخدام توابع التهشير للمفاتيح ثم تخزينها في سلسلة الكتل، ويتم التحقق من ملكية المفتاح العام للمستخدم في كل مرة يتم فيها التعامل معه.

نقدم فيمايلي نموذج يتم فيه توليد مفتاح عام وخاص ثم يحفظ تهشير المفتاح العام في سلسلة الكتل Ethereum ونقوم ببرمجة تطبيق يقوم بتسجيل المستخدمين وإرسال رسائل معماة بالمفتاح العام والتحقق من ملكية المستقبل للمفتاح بواسطة سلسلة الكتل قبل عملية الإرسال، ويؤمن آلية لإلغاء تسجيل المستخدم في حال أراد إلغاء التسجيل أو انتهت فترة الصلاحية، وذلك من أجل توظيف فكرة البحث والتحقق من إمكانية تطبيقها على أرض الواقع.

نتعرف فيما يلي على أجزاء النموذج المقترح مع تعريف بسيط عن كل جزء

1- شبكة Ethereum Blockchain

هي شبكة مبنية على تقنية سلسلة الكتل تتيح برمجة التطبيقات اللامركزية فيها عن طريق كتابة عقود ذكية بلغة solidity.

2- العقد الذكي

البرنامج الذي يستقبل وينفذ الطلبات داخل سلسلة الكتل في شبكة Blockchain Ethereum.

3- تطبيق ارسال الرسائل المعماة

يقدم بيئة تفاعلية للمستخدم للتسجيل وإلغاء التسجيل وإرسال الرسائل.

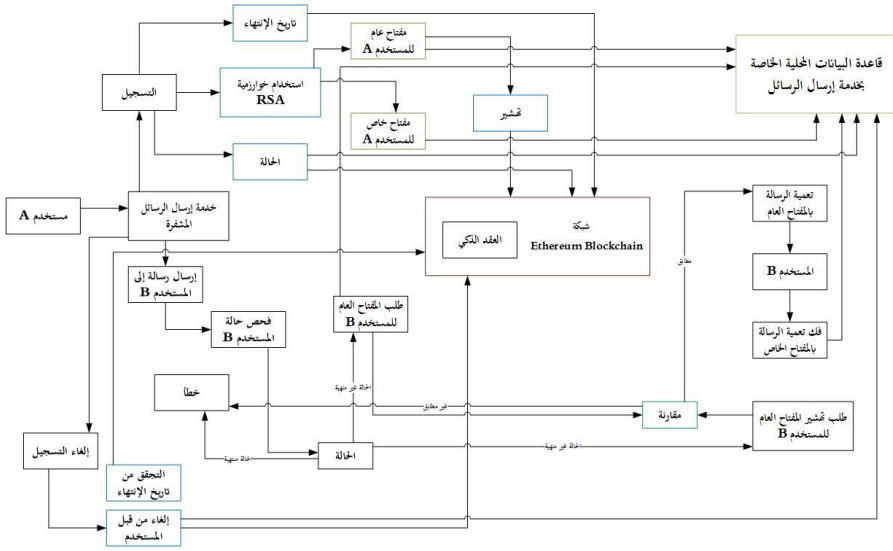
4- قاعدة بيانات محلية

يتم فيها تخزين المفاتيح العامة والخاصة للمستخدمين من أجل عمليات الإرسال والإستقبال.

5- خوارزمية RSA لتوليد المفاتيح

تقوم بتوليد مفتاحين لكل مستخدم من أجل تعمية وفك تعمية الرسائل المتبادلة.

يبين الشكل (9-2) الوظائف التي يقوم بها النموذج بشكل عام.



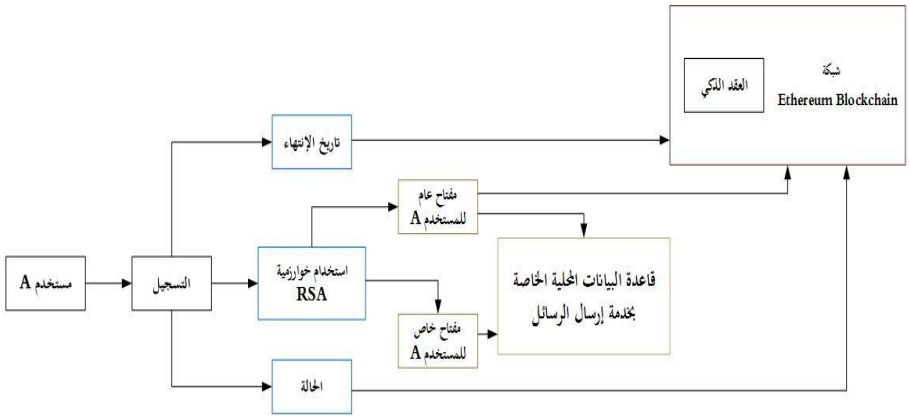
الشكل (9-2) وظائف النموذج المقترح

1.9. نموذج التسجيل لمستخدم

نقدم في الشكل (9–3) نموذج تسجيل لمستخدم جديد في التطبيق والمراحل التي يمر بها.

حيث يقوم المستخدم A بالتسجيل في التطبيق عبر الخطوات التالية:

- يدخل المستخدم معلوماته (الإسم ، الإيميل، اسم المستخدم، كلمة المرور).
- يتم توليد مفتاحين (مفتاح عام ومفتاح خاص) باستخدام خوارزمية التعمية غير المتناظرة (RSA).
- يتم حفظ المفتاح العام والخاص في قاعدة البيانات المحلية الخاصة بالتطبيق.
- يتم إرسال المعلومات التالية (تهشير المفتاح العام، تاريخ الانتهاء، الحالة) إلى داخل سلسلة الكتل وتخزينها.



الشكل (9–3) نموذج تسجيل مستخدم جديد

2.9. نموذج إرسال رسالة

نقدم في الشكل (9–4) نموذج عن كيفية تناقل الرسائل بين مستخدمين والمراحل التي تمر بها الرسالة وآلية التحقق عن طريق الخطوات التالية:

1– يقوم المستخدم A بالدخول إلى الحساب الخاص به في تطبيق إرسال الرسائل.

2– يحدد المستقبل المراد إرسال الرسالة له فرضاً المستخدم B.

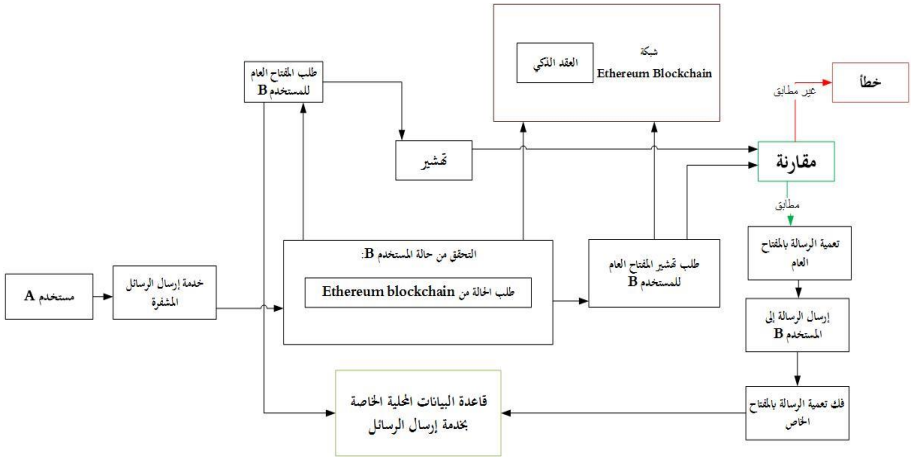
3- تتم آلية التحقق على مرحلتين:

- ❖ التحقق من حالة المستخدم B من سلسلة الكتل فتكون إما صالحة أو منتهية.
- ❖ مقارنة تهشير المفتاح العام للمستخدم B من سلسة الكتل مع الموجود في قاعدة البيانات المحلية الخاصة بالتطبيق.

4- في حال كانت الحالة منتهية حسب التاريخ أو المقارنة غير مطابقة تظهر رسالة خطأ.

وفي حال كانت المقارنة مطابقة تتم عملية تعمية الرسالة باستخدام المفتاح العام للمستخدم B ثم إرسالها له من خلال التطبيق.

5- يقوم المستخدم B بفك تعمية الرسالة باستخدام مفتاحه الخاص الموجود في قاعدة البيانات المحلية.



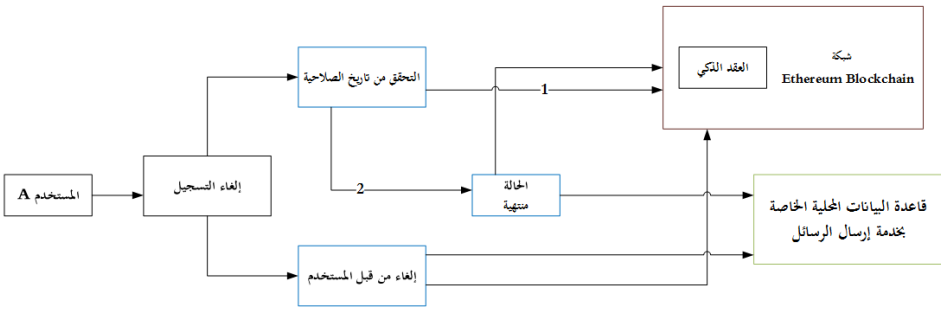
الشكل (9-4) نموذج إرسال رسالة

3.9. نموذج إلغاء التسجيل

نعرض في الشكل (9-5) نموذج إلغاء التسجيل لمستخدم ويشمل الحالتين:

- إنتهاء صلاحية التسجيل: حيث يقارن التاريخ الحالي مع تاريخ إنتهاء الصلاحية من سلسلة الكتل حيث يوضع في خانة الحالة منتهية في سلسلة الكتل وقاعدة البيانات المحلية ليتوقف التعامل معه ريثما يقوم بتجديد التسجيل.

- طلب المستخدم إلغاء التسجيل: حيث يتم حذف حساب المستخدم من سلسلة الكتل وقاعدة البيانات المحلية.



الشكل (9–5) نموذج إلغاء تسجيل المستخدم

10. القسم العملي

1.10. تقييم النموذج المقترح والنتائج العملية

بتطبيق بعض أجزاء النموذج المقترح في [18] وإضافة بعض المزايا تبين لدينا أنه يوجد بطء في النظام حيث كل عملية إرسال تحتاج إلى عملية تنقيب لإضافة المعاملة على سلسلة الكتل وهذا الأمر غير واقعي في حال إرسال الرسالة في كل مرة، فقمنا بإضافة بعض التعديلات على النموذج وإضافة بعض الوظائف والتي أدت إلى الحصول على النتائج المرجوة، وكان أبرز هذه التعديلات:

- إضافة معاملة على سلسلة الكتل فقط في حال إنشاء مستخدم جديد مما يعطي السرعة في الأداء لأن الإضافة تحتاج لعملية تنقيب وبالتالي زمن أكثر.
- جلب البيانات من سلسلة الكتل من أجل التحقق من ملكية المفتاح العام لا يتطلب زمن تنقيب.
- استخدام HashMap في عملية تخزين البيانات في سلسلة الكتل مما يعطي سرعة في البحث.
- إضافة نموذج إرسال للرسائل ونموذج حذف.

- تطبيق النماذج عمليا في Ethereum Blockchain وكتابة النتائج.

- **تقييم النموذج من الناحية الأمنية**

نقدم في الجدول (10-1) كيف يلبي نموذجنا المقترح المتطلبات الأمنية الأساسية.

المتطلب الأمني	كيفية تحقيق المتطلب الأمني
السرية	استخدام آلية التحقق من ملكية المفتاح العام للمستخدم ثم استخدام المفتاح العام في تعمية الرسائل
السلامة	تحوي كل كتلة على قيمة تهشير لكل محتوياتها في سلسلة الكتل ولكل مستخدم عنوانه الخاص في سلسلة الكتل يتم التعامل معه من خلاله
التوافرية	تقوم شبكة Ethereum Blockchain بمعالجة كافة الطلبات ولأن الشبكة مؤلفة من عدة عقد فعند توقف إحدى العقد لا تتأثر الخدمة

الجدول (10-1) المتطلبات الأمنية وكيفية تحقيقها في النموذج المقترح

- **تقييم النموذج من ناحية الوظائف والأداء**

تم توظيف بيئة تفاعلية تسمح بالتسجيل والتحقق من ملكية المفتاح العام بطريقة تضمن السرعة في الأداء والفاعلية وذلك بتحقيق الوظائف (التسجيل والصلاحية وإلغاء التسجيل)، وقمنا بإجراء الاختبارات عليه لنقوم بالإجابة عن مسألة البحث كالتالي:

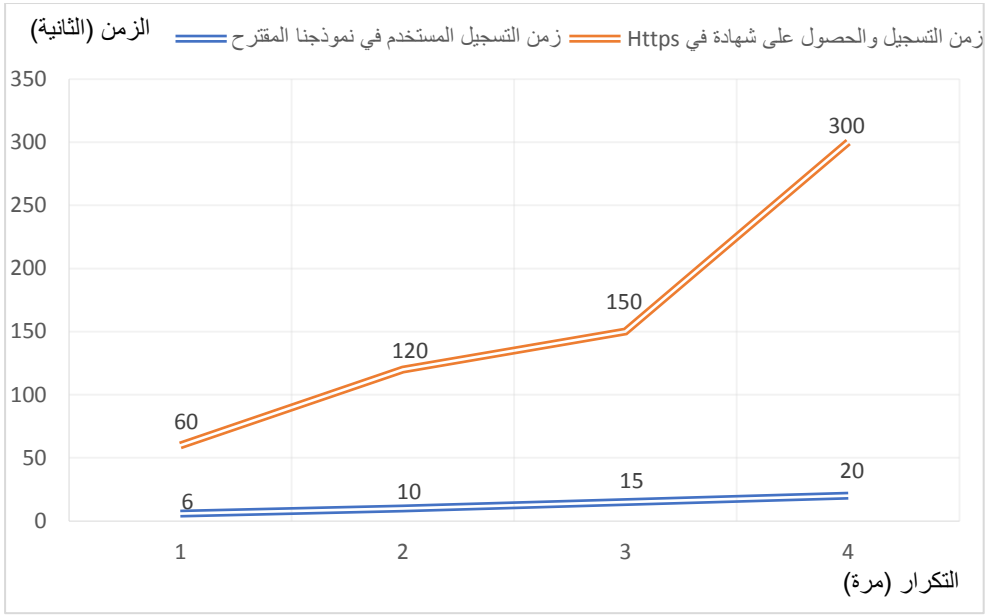
هل تستطيع تقنية سلسلة الكتل حل مشاكل PKI وأن تكون بديلة عنها في إرسال الرسائل ؟

نعم يمكن لشبكة سلسلة الكتل أن تحل مشاكل البنية التحتية للمفتاح العام PKI وأن تكون بديلة عنها حيث برهنا على ذلك من خلال تطبيق النموذج المقترح، عن طريق برمجة العقد الذكي والتخاطب معه وإضافة المفاتيح العامة على سلسلة الكتل حيث يتم حفظ تهشير المفتاح العام مع اسم المستخدم في سجل عام موزع على جميع عقد سلسلة الكتل في Ethereum Blockchain لنضمن بذلك عدم إمكانية التعديل على السجل، وتتم عملية إرسال رسالة إلى مستخدم ما مسجل في النظام بعد التحقق من ملكية المفتاح العام من خلال مقارنة التهشير المحفوظ في سلسلة الكتل مع الموجود في قاعدة البيانات المحلية باستخدام تطبيق الويب حيث كانت نتائج الوظائف للنموذج كما يلي:

- **عملية تسجيل المستخدم**

تمت العملية بنجاح حيث تم توليد مفاتيح التعمية غير المتناظرة وتخزينها في قاعدة البيانات، وتم استخدام توابع التهشير من أجل تهشير المفتاح العام وإرساله إلى سلسلة الكتل بسرعة عالية،

ومن ناحية الأداء يبين الشكل (10-1) مقارنة بين زمن تسجيل المستخدم في نموذجنا المقترح وزمن الحصول على الشهادة التي تستخدم PKI في برتوكول Https حسب موقع godaddy [19]و comodo [20].



الشكل (10-1) مقارنة زمن تسجيل المستخدم في نموذجنا المقترح وزمن الحصول على الشهادة في Https

نلاحظ من الشكل (10-1) أن زمن التسجيل في نموذجنا يأخذ حوالي (6-20 ثانية)، بينما الحصول على شهادة مصدقة من CA نحتاج إلى حوالي (1- 5 دقائق).

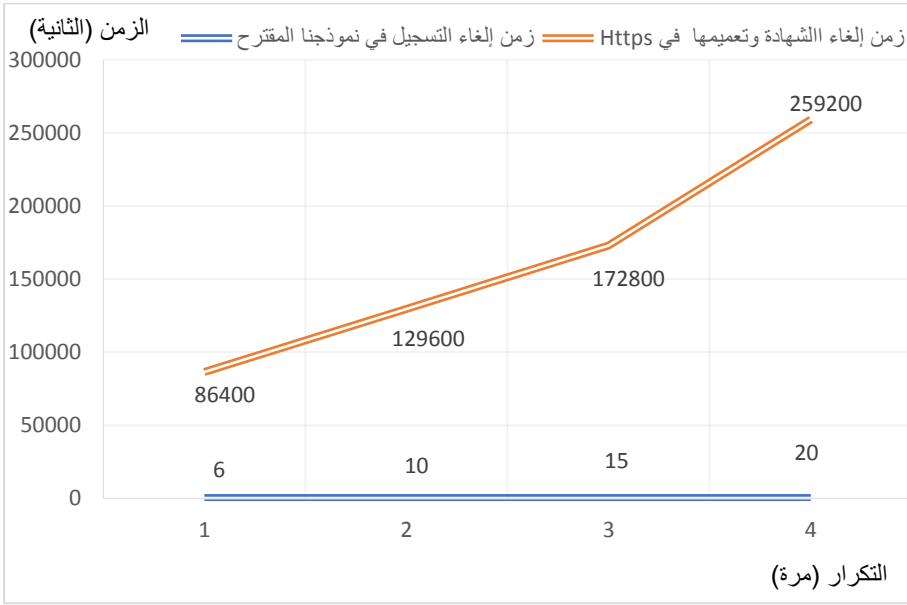
- **عملية الإرسال والمقارنة والاستقبال**

تتم العملية من خلال دخول المستخدم إلى حسابه ثم تحديد المستقبل الذي يريد الإرسال له، وبعدها تتم عملية التحقق من صلاحية المستخدم ومقارنة المفاتيح، وفي حال صحة العملية يتم تعمية الرسالة بالمفتاح العام للمستقبل وإرسالها له ليقوم بقراءة الرسالة باستخدام مفتاحه الخاص.

- **عملية إلغاء تسجيل المستخدم وحذفه**

تتم هذه العملية من خلال ضغط المستخدم على زر الحذف بحيث يتم حذف حساب المستخدم من قاعدة البيانات المحلية وسلسلة الكتل وبذلك يتم حل مشكلة الشهادات الملغاة بحيث تأخذ العملية عدة ثواني حتى يتم تعميم الإلغاء.

ومن ناحية الأداء يبين الشكل (10-2) مقارنة بين زمن إلغاء الشهادة في النموذج المقترح والآلية المطبقة في إلغاء الشهادات في PKI.



الشكل (10-2) مقارنة زمن إلغاء تسجيل مستخدم في نموذجنا مع زمن إلغاء الشهادة في PKI في Https

نلاحظ من الشكل (10-2) أن زمن إلغاء التسجيل في نموذجنا يأخذ حوالي (6 – 20 ثانية)، بينما في إلغاء شهادة مصدقة من CA نحتاج إلى حوالي (24 ساعة) حسب شركة godaddy [21] .

كيف تستطيع تقنية سلسلة الكتل حل مشاكل PKI وأن تكون بديلة عنها في إرسال الرسائل ؟

تمت عملية تصميم النظام من خلال استخدام سلسلة الكتل في Ethereum حيث تم إنشاء حساب تجريبي من أجل إضافة العقد الذكي والتخاطب معه، وتم ذلك بسهولة وبسرعة جيدة وذلك باستخدام توابع API وواجهات التخاطب وبيئات التطوير التي توفرها Ethereum.

11. الاستنتاجات والتوصيات

نستنتج مما سبق أن النموذج المقترح الذي قمنا بطرحه قد أعطى نتائج فعالة في بناء نموذج بديل عن PKI واستخدامها في إرسال الرسائل بطريقة آمنة تضمن السرية والخصوصية عن طريق التسجيل والتحقق من ملكية المفتاح العام وذلك من خلال استخدام سلسلة الكتل في Ethereum وهو الهدف الأساسي من بحثنا كما تقدم.

قدمنا في هذا البحث عرضا لتقنية سلسلة الكتل وقمنا بتوصيف البنية التحتية للمفتاح العام PKI وتحدثنا عن المشاكل التي تعاني منها، ثم قدمنا حلول مقترحة للتغلب على هذه المشاكل باستخدام تقنية سلسلة الكتل.

بعدها عرضنا النموذج المقترح من قبلنا لامكانية تطبيق بنية بديلة عن PKI واستخدامها في تطبيق إرسال الرسائل بطريقة آمنة عن طريق خوارزميات التعمية غير المتناظرة وبالاعتماد على سلسلة الكتل في Ethereum من خلال العقد الذكي.

وقد أثبت النموذج فاعليته في تسجيل المفتاح العام لمستخدم وضمان عدم تغييره وسرقته وإلغاء البنية المركزية التي تقوم عليها PKI، كما أثبت أيضا سرعة في الأداء وحل لمشاكل إلغاء الشهادات بطريقة سريعة وفعالة.

واستطاع النموذج المقترح إضافة العديد من الميزات على استخدام سلسلة الكتل في التحقق من المفتاح العام أهمها:

- سهولة تسجيل المستخدم.
- سرعة إجراء التحقق من ملكية المفتاح العام.
- سهولة إرسال الرسائل بطريقة معماة.
- سرعة إلغاء التسجيل لمستخدم وتعميمها على جميع عقد السلسلة.

ولا ننسى أيضاً أن بيئة Ethereum قد وسعت آفاق العمل على برمجة تطبيقات لامركزية تستفيد من ميزات سلسلة الكتل فيها، مما يقدم سهولة في تطوير تطبيقات تضمن السرعة والأمان لمستخدميها.

12. الأعمال المستقبلية

- دراسة كفاءة النظام في استخدام عدد كبير من المستخدمين.
- تطوير وظائف العقد الذكي.
- إضافة إمكانية تجديد الإشتراك في حال انتهاء الصلاحية.
- إضافة خيارات من أجل حالة المستخدم.

المراجع

[1] F.Schuermann, "Bitcoin and Beyond-A Technical Survey on Decentralized Digital Currencies,"*IEEE communication surveys and tutorials, 2016.*

[2] S.Bano,A.Sonnino,M.Bassam,S.Azouvi,P.McCorry,S.Meiklejohn,G. danezis, "SoK: Consensus in the Age of Blockchains," *1st ACM Conference on Advances in Financial Technologies, 2019.*

[3] C.Cachin,M.Vukoli, "Blockchain Consensus Protocols in the Wild," *IBM Research - Zürich, Rüschlikon, Switzerland, 2017.*

[4] W.Diffie. and M.E.Hellman, "New Directions in Cryptography," *IEEE Transactions On Information Theory, VOL. IT-22, NO. 6, november 1976.*

[5] L.M Kohnfelder, "Towards a Practical Public-key Cryptosystem," *Massachusetts Institute of Technology, Cambridge, 1978.*

[6] ITU-T, "The Directory Overview Of Concepts, Models And Service," *X.500 Series of Recommendations, International Telecommunications Union, Geneva, 1993.*

[7] M.S.Baum and W.Ford, "Public Key Infrastructure Interoperation," *IEEE Aerospace Conference, 21-28 March 1998.*

[8] Michael Alan Specter, "Understanding Certificate Authorities," *Massachusetts Institute of Technology, 2015.*

[9] "An Overview of Public Key Infrastructures (PKI)," *Techotopia. Retrieved March 26, 2015.*

[10] Jayanth Rajakumar and KN Subrahmanya , "Overview Of Tls Certificate Revocation Mechanisms, " *International Journal of Advanced Research in Computer Science; Udaipur, May 2019.*

[11] https://www.grc.com/revocation/crlsets.html

[12] https://searchsecurity.techtarget.com/news/252436120/23000-Symantec- certificates-revoked-following-leak-of-private-keys

[13] https://scotthelme.co.uk/certificate-revocation-google-chrome/

[14] A. Bahga and V. K. Madisetti, "Blockchain Platform For Industrial Internet Of Things," *eorgia Institute of Technology, Atlanta, GA, USA, 2016.*

[15] I. C. Lin and T. C. Liao, "A Survey Of Blockchain Security Issues And Challenges," *International. Journal of Network Security, 2017.*

[16] A. M. Antonopoulos, "Mastering Bitcoin: Unlocking Digital Cryptocurrencies," *O'Reilly Media, Inc Sebastopol in California, 2015.*

[17] Mauro Conti, E.Sandeep Kumar,Chhagan Lal and Sushmita Ruj, "A Survey on Security and Privacy Issues of Bitcoin," *IEEE 2017.*

[18] Kahina Khacef, Guy Pujolle, "Secure Peer-to-Peer communication based on Blockchain," *33rd International Conference on Advanced Information Networking and Applications (AINA-2019), Mar 2019.*

[19] https://www.godaddy.com/help/how-long-will-it-take-to-issue-my-certificate-858

[20] https://comodosslstore.com/ssl-validation-process/dv/how-long-to-issue-dv-certificate

[21] https://in.godaddy.com/help/uninstall-an-ssl-certificate-from-my-godaddy-hosting-31931

تصميم مضخّم (مكبر) قيادة راديوي عريض المجال يعمل عند المجال الترددي (100MHz -1800MHz) بالاعتماد على ترانزستورات InGap/GaAS HBT MMIC

عبده بللوق	فواز مفضي	سالم إبراهيم
طالب ماجستير في هندسة الاتصالات المتقدمة	أستاذ مساعد	دكتوراه
قسم هندسة الالكترونيات والاتصالات	قسم هندسة الالكترونيات والاتصالات	المعهد العالي للعلوم التطبيقية والتكنولوجيا
كلية الهندسة الميكانيكية والكهربائية	كلية الهندسة الميكانيكية والكهربائية	
جامعة دمشق	جامعة دمشق	دمشق

الملخص

يهدف البحث لتصميم عملي لمضخّم قيادة (Driver Amplifier) عريض المجال الترددي (100MHz -1800MHz) يستخدم كمضخّم أولي لقيادة مضخّم استطاعة عالية أو لتكبير الإشارات الراديوية ضمن المجالات الترددية (VHF/UHF/L) التي تعمل عندها أنظمة الاتصالات اللاسلكية، كما يمكن استخدام المضخّم في أنظمة التشويش والاعماء لتكبير إشارات التشويش الراديوية، إضافة إلى إمكانيته تكبير عدة إشارات ترددية مجمعة معاً ضمن مجال عمله الترددي، تم تصميم وتصنيع المضخّم عملياً بالاعتماد

على ترانزستورات (MMIC InGaP/GaAs HBT)، المضخّم يعتمد على مرحلتي تكبير، حيث تم استخدام ترانزستور استطاعة طراز (+5-ERA) مصنّع وموصف من شركة (Mini-Circuit) يعتمد تكنولوجيا (InGaP HBT) كمضخّم أولي وهو مستقر بدون شروط يعمل عند (DC-4GHz)، والترانزستور (SXA-289) من شركة (Sirenza Microdevices) يعتمد تكنولوجيا (GaAs HBT MMICs) كمضخّم ثانوي يعمل عند التردد (5-2000MHz)، أعطى المضخّم ربحاً للاستطاعة حوالي 39dB إلى 20dB عند المجال الترددي (100MHz-1900MHz) وذلك بحال استخدام موجة مستمرة (Continues Wave (CW) باستطاعة 0.03mW كإشارة دخل للمضخّم.

كلمات مفتاحية: InGaP/GaAs HBT– Wideband Amplifier- Broadband Amplifier– مضخّم استطاعة – RF Power Amplifier

Design A Wideband (100MHz -1800MHz) RF Driver Amplifier Based on InGaP/GaAs HBT MMIC

Abdo Ballouk
MSc Student in Advanced Communication Engineering.
Dept of Electronics and Communication Engineering, Faculty of Mechanical & Electrical Engineering Damascus University
Syria

Fawaz Mofdi
Prof Dr.
Dept of Electronics and Communication Engineering,
Faculty of Mechanical & Electrical Engineering
Damascus University
Syria

Salem Ibrahim
Dr.
Dept of Communication Engineering, Higher Institute for Applied Sciences and Technology,
Damascus,
Syria

Abstract

The research aims to design a practical wideband RF power Amplifier working at (100MHz-1800MHz), it used as a primary amplifier to drive a high power amplifier or to amplify radio signals within the (VHF / UHF / L) frequency bands in which wireless communication systems operate, and the amplifier can also be used in systems Jamming and blindness to amplify the radio jamming signals, in addition to its ability to amplify several frequency signals that combined within its frequency band, the amplifier was designed and manufactured practically based on (InGaP / GaAs HBT MMIC) transistors, the amplifier depends on two amplification stages, where the (ERA5+) power transistor was used, It was manufactured and specified by Mini-Circuit based on (InGaP HBT) technology as primary amplifier and it is stable unconditionally, operating at (DC-4GHz), Sirenza Microdevices (SXA-289) transistor based on (GaAs HBT MMICs) technology as secondary amplifier, that operating at (5-2000MHz). The amplifier has a gain about 39dB to 20dB at the frequency band (100MHz-1900MHz), in case of using Continues Wave (CW) with power of (0.03mW) as the input signal of the amplifier.

Keywords: InGaP/GaAs HBT - Wideband Amplifier - Broadband Amplifier - RF Power Amplifier

1- مقدمة:

InGaP: Indium Gallium Phosphide. **HBT:** Heterojunction Bipolar Tran
AlGaAs: Aluminium Gallium Arsenide. **MMIC:** Monolithic Microwave Int

يزداد الطلب على مضخّمات الاستطاعة عريضة المجال لتكبير الإشارات الراديوية ضمن المجالات (VHF/UHF/L) والتي تستخدم من قبل أجهزة الإرسال التلفزيوني، أنظمة (GSM900,GSM1800)وكذلك للاستخدام في تطبيقات الاتصالات العسكرية وحتى أنظمة الملاحة العالمية عبر الأقمار الصناعية مثل نظام (GPS Global Navigation System) الأمريكي، نظام (GLONASS) الروسي، (Galileo) الأوربي ونظام (Beidou) الصيني تعمل هذه الأنظمة جميعها عند المجال الترددي-1100MHz) (1610MHzوهي تطلب مضخّمات استطاعة عريضة المجال الترددي. بالنسبة لأجهزة الإرسال عريضة المجال تلعب مضخّمات الاستطاعة المستخدمة فيها دوراً مهماً في تحديد أداء هذه الأنظمة وذلك من خلال أداء وصفات هذه المضخّمات، مثل عرض المجال الترددي الكبير، ربحها المستوي على طول المجال الترددي، استطاعة الخرج المطلوبة، الخطية الجيدة، والكفاءة العالية، إلخ.

اكتسبت تكنولوجيا (Monolithic Microwave Integrated Circuit MMIC) قبولاً واسعاً بين كبار موردي معدات الاتصالات اللاسلكية عريضة المجال، باعتبارها التكنولوجيا المفضلة للتطبيقات التي تتطلب تردداً عالياً وأداءً وخطية عاليين. اعُتمدت هذه التكنولوجيا في مضخّمات الاستطاعة للهواتف الخلوية وأجهزة الكمبيوتر الشخصية (خدمات الاتصالات الشخصية)، ومضخّمات الاستطاعة للمحطات الأساسية الخليوية، بالإضافة إلى البث التلفزيوني ومضخّمات الخط المستخدمة في شبكات الألياف الضوئية [1,2]. توفر الأجهزة التي تعتمد تكنولوجيا (Heterojunction Bipolar Transistor (HBT)) وزرنيخ الغاليوم (Gallium Arsenide GaAs) عرض مجال ترددي واسع، وكسب تيار عالي، مما يسمح لهذهِ الأجهزة بتغطية مجموعة واسعة من التطبيقات. تعد (HBT) التي تستخدم (AlGaAs) كطبقة انبعاث التقنية الأكثر نضوجاً [3,4,5]. اكتسب نوع الترانزستور (InGaP/GaAs) الكثير من الاهتمام مؤخراً نظراً لمزاياها بالمقارنة

بترانزستورات (AlGaAs/GaAs). على سبيلِ المثال، تحتوي تكنولوجيا (InGaP/GaAs) على إزاحة فجوة بعرض مجال أكبر من المجال الموجود في تكنولوجيا (AlGaAs/GaAs) [6]، ولمادة (InGaP) قدرة تحفيز أكبر من التي موجودة في (GaAs) [8,7]، ويظهر سرعة إعادة تركيب سطح منخفضة. تسمح فجوة المجال العريضة لـ (InGaP) المستخدمة كطبقة باعثة بمستوٍ عالٍ من الانبعاث، مما ينتج عنه قيم مقاومة أساسية منخفضة وتردد تذبذب مرتفع. غالباً ما تتطلب أنظمة الاتصالات والدفاع الحديثة مضخّمات قيادة ذات كفاءة عالية وربح عالي وتتمتع بعرض مجال ترددي عريض وذلك لتقوم بقيادة مضخّمات استطاعة عالية [9]. في هذا العمل نستعرض تصميم دارة مضخّم استطاعة بالاعتماد على تقنية (MMIC) الخاصة بـ (HBT)، تم استخدام النتائج التجريبية لترنزستورات (InGaP/GaAs HBT)والموجودة في نشراتها الفنية وذلكَ لتصميم دارة مضخّم إشارة راديوية عريض المجال (VHF/UHF/L) وللتطبيقات عالية الحساسية التي تعمل من 100MHz إلى 1800MHz.

في وقتنا الحاضر ترانزستورات الاستطاعة المستخدمة للمجالات الترددية (VHF,UHF, L-Band) بشكل أساسي هي من شركات، مثل (Hittie, Triquint, Infenion, Fujitsu) أما في تصميمنا هذا تم اختيار ترانزستور طراز (+ERA-5) من شركة (Mini-Circuit) كمضخّم أولي، والترانزستور (SXA-289) من شركة (Sirenza Microdevices) كمضخّم ثانوي.

2- الدراسات المرجعية:

سوف نستعرض بشكل مُقْتَضَب بعض الدراسات المرجعية التي تهدف لتصميم مضخّمات استطاعة تعمل ضمن أو بالقرب من المجال الترددي لهذا البحث وذلك بهدف مقارنة أدائها مع أداء المضخّم المقترح.

1. نشّر كلاً من Xiangning Fan و Zhou Yu وزملائهم في مجلة IEEE عام 2015 مقالاً علمياً بعنوان " Design of a 0.7~1.5 GHz Wideband Power Amplifier in 0.18-µm CMOS"

حيث يعمل المضخّم المقترح ضمن المجال الترددي (700MHz-1500MHz) يقدم استطاعة خرج (16.6~21.4dBm) وبربح استطاعة 13dB.[15]

2. نشّر كلاً من A. Salleh و K. S. Yong وزملائهم في مجلة ScienceDirect عام 2013 مقالاً علمياً بعنوان:

" Design of Low Power Wideband Low Noise Amplifier for Software Defined Radio at 100 MHz to 1GHz"

يعرض تصميم مضخّم يعمل ضمن المجال الترددي (100MHz-1GHZ) بربح استطاعة حوالي 15dB.[16]

3. نشّر كلاً من Azwar Mudzakkir Ridwan و Eki Ahmad Zaki Hamidi وزملائهم في مجلة PhotonIcs & Electromagnetics Research Symposium عام 2019 مقالاً علمياً بعنوان:

" High Gain 2-stage Class-E RF Power Amplifier for Wireless Transfer Power"

يستعرض تصميم مضخّم استطاعة بالاعتماد على ترانزستورات MOSFET طراز IRF510 و IRF620 يعمل على المجال الترددي (1MHz-30MHz) بربح استطاعة 38dB. [17]

4. نشّر كلاً من Engin Çağdaş و Oğuzhan Kızılbey في مجلة IEEE عام 2018 مقالاً علمياً بعنوان:

"High Efficiency Wideband Power Amplifier with Class-J Configuration"

يستعرض تصميم مضخّم استطاعة بالاعتماد على ترانزستورات GaN HEMT طراز CGH400010F يعمل ضمن المجال الترددي (2500-3500MHz) بربح 10dB وباستطاعة إشارة خرج 39.84dBm عند تطبيق إشارة دخل باستطاعة 30dBm. [18]

5. نشّر كلاً من Philip Zurek و Tommaso Cappello في مجلة IEEE عام 2019 مقالاً علمياً بعنوان:

"A Concurrent 2.2/3.9-GHz Dual-Band GaN Power Amplifier"

يستعرض تصميم مضخّم استطاعة بالاعتماد على ترانزستورات GaN HEMT طراز (T2G6001528-SG) Qorvo يعمل عند الترددين (2.2/3.9GHz) بربح (13.9 dB و 9.37 dB). [19]

3- مواد وطرائق البحث:

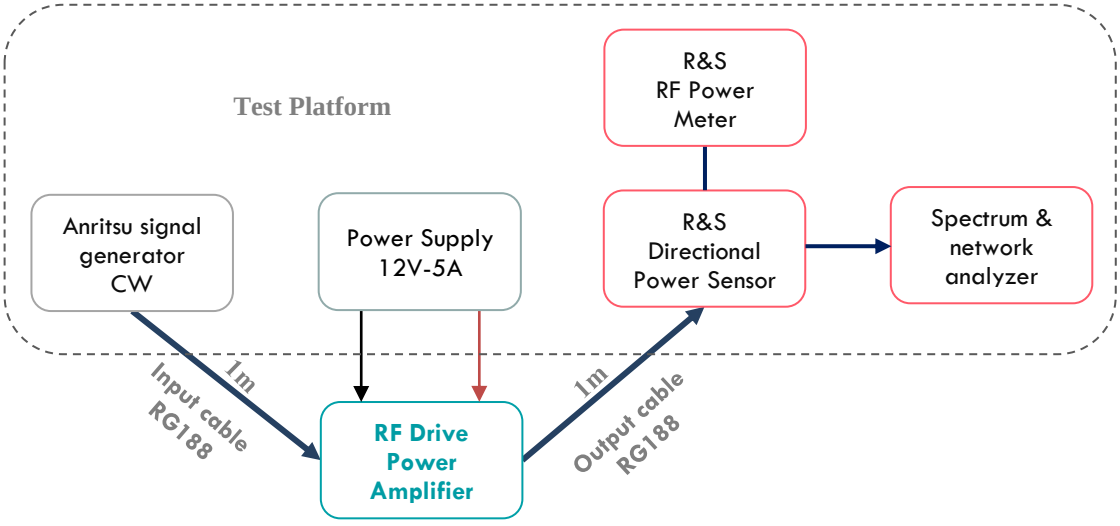
3-1- مواد البحث:

تم في هذا البحث تصميم وتصنيع بطاقة مضخّم استطاعة يعمل عند المجال الترددي 100MHz إلى 1800MHz حيث يعتمد على مرحلتي تكبير كل مرحلة تستخدم مضخّم خاص فيها حيث استخدام في المرحلة الأولى (Monolithic Amplifier) طراز (ERA-5+) وهو يعمل عند المجال الترددي DC-4GHz يقدم ربح استطاعة 18.5dB وله رقم ضجيج 3.5dB أما بالنسبة لمرحلة التكبير الثانية تم الاعتماد على (Medium Power GaAs HBT Amplifier) طراز (SXA-289) يعمل عند المجال الترددي (5- 2000MHz) يقدم ربح حوالي 15dB وله رقم ضجيج حوالي 5.5dB يمكن تلخيص مواد وتجهيزات البحث كالتالي:

- ترانزستور استطاعة طراز (Monolithic Amplifier ERA-5+).

- ترانزستور استطاعة طراز (Medium Power GaAs HBT Amplifier SXA-289).
- ركيزة نوع (FR4) بسماكة عازل 1.6mm وثابت عازلية Σ r = 4.5 وسماكة طبقة نحاس35µm.
- منصة اختبار مكونة من المكونات الأساسية التالية:
  - مولد إشارة طراز (Anritsu MG3692C) يعمل حتى التردد 20GHz.
  - محلل طيف ترددي طراز (ROHDE & SCHWARZ FSH8) يعمل عند المجال الترددي 100KHz-8GHz.
  - مقياس مع حساس استطاعة اتجاهي.
  - كابلات توصيل طراز (RG188) تعمل حتى التردد 20GHz.
  - وحدة تغذية 24VDC-5A.

الشكل (1) يظهر المخطط الصندوقي لمنصة الاختبار



الشكل (1) مخطط صندوقي لمنصة الاختبار

3-2- طرائق ومراحل إجراء البحث

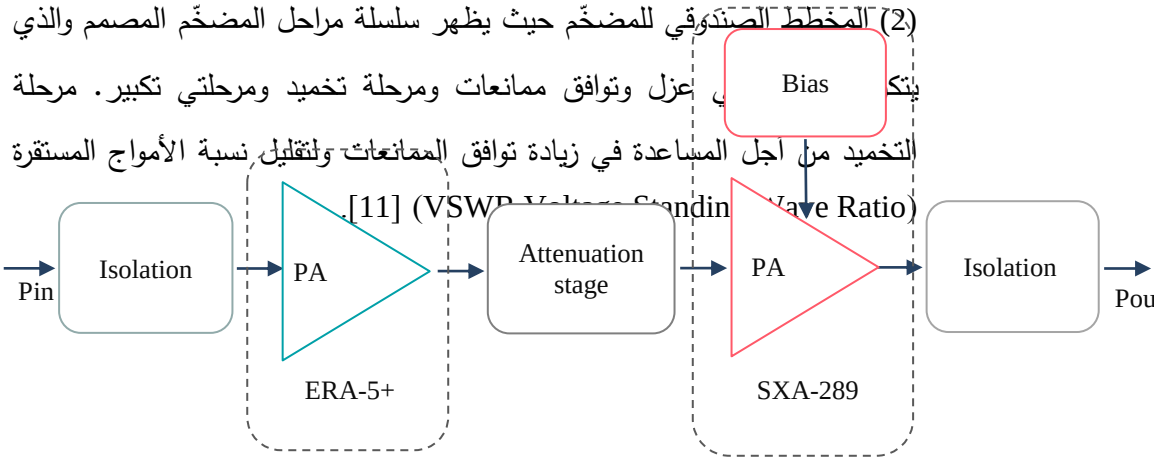
مراحل إجراء البحث:

3-2-1- دراسة النشرات الفنية (Datasheet) المعتمدة والموصّفة من قبل الشركات المصنّعة للترانزستورين (ERA-5+,SXA-289) المراد استخدامها في المضخّم المقترح:

تم دراسة النشرات الفنية لكلا الترانزستورين بالتفصيل، حيث قمنا بدراسة منحنيات عمل وأداء كل ترانزستور، وتم الاستفادة منها بمعرفة مجال عمل الترانزستورات ونسبة ربحها وجهد الانحياز اللازم لعمها، إضافةً لمعرفة الضجيج اللذان يضيفانه، وتم الاستفادة من مقترح الشركات المصنّعة لتصميم دارة تشغيل هذه الترانزستورات مع المحافظة على توافق الممانعات عند دخل وخرج كل ترانزستور.

3-2-2- وضع المخطط الصندوقي للمضخّم المقترح:

بناءً على الدراسة السابقة للنشرات الفنية، تم اقتراح مخطط صندوقي للمضخّم المراد تصميمه ليعمل عند المجال الترددي 100MHz إلى 1800MHz، يوضح الشكل (2) المخطط الصندوقي للمضخّم حيث يظهر سلسلة مراحل المضخّم المصمم والذي يتكـ[illegible]ي عزل وتوافق ممانعات ومرحلة تخميد ومرحلتي تكبير. مرحلة التخميد من أجل المساعدة في زيادة توافق الممانعات وتقليل نسبة الأمواج المستقرة (VSWR Voltage Standing Wave Ratio) [11].

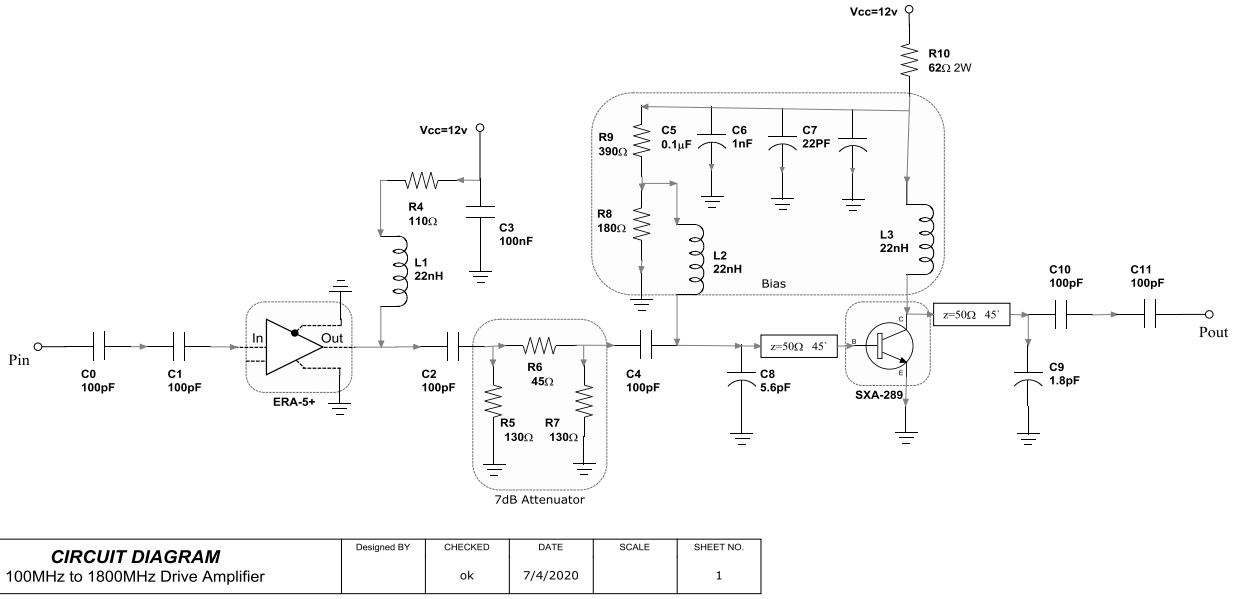


الشكل (2) مخطط صندوقي لبنية المضخّم

3-2-3- رسم مخطط الدارة للمضخّم المقترح:

يعد تصميم دارة انحياز المضخّم خطوة مهمة في تصميم مضخّم الاستطاعة، ويتمثل دورها في تأمين التيار المستمر (DC) اللازم للمضخّم مع الحماية من السحب الزائد للتيار. وهي أيضاً يجب أن تحافظ على درجة عالية من العزل بين الإشارة الميكروية واستطاعة التيار المستمر، وتقوم بتقليل فقد الإدخال (Insertion loss) إلى أقصى حد ممكن. إضافة المكثفات (0.1µF, 1nF, 22pF) والملف (22nH) إلى دارة الانحياز لتقليل التشويه ولتنعيم تيار الانحياز وذلك لغاية الحفاظ على استقرار عمل

المضخّم. لم نستخدم مرحلة توافق ممانعات بين ترانزستوري التكبير لانهما اختيرا على أساس أن لهما توافق ممانعات واحد عند (50Ω)، الشكل رقم (3) يظهر (schematic circuit) المخطط الكهربائي لبنية المضخّم.

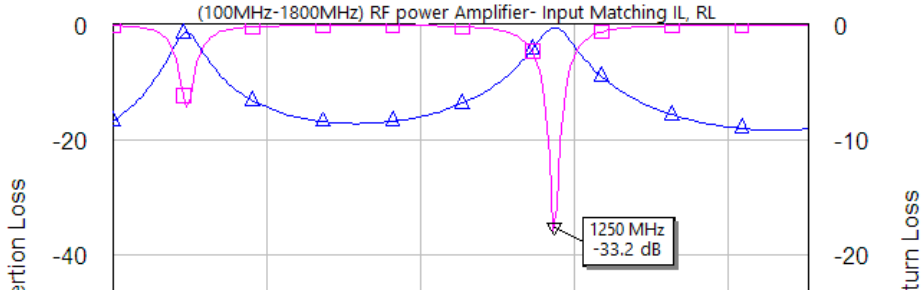


CIRCUIT DIAGRAM 100MHz to 1800MHz Drive Amplifier	Designed BY	CHECKED	DATE	SCALE	SHEET NO.
		ok	7/4/2020		1

الشكل (3) مخطط كهربائي لبنية المضخّم

3-2-4- محاكاة تصميم المضخّم المقترح:

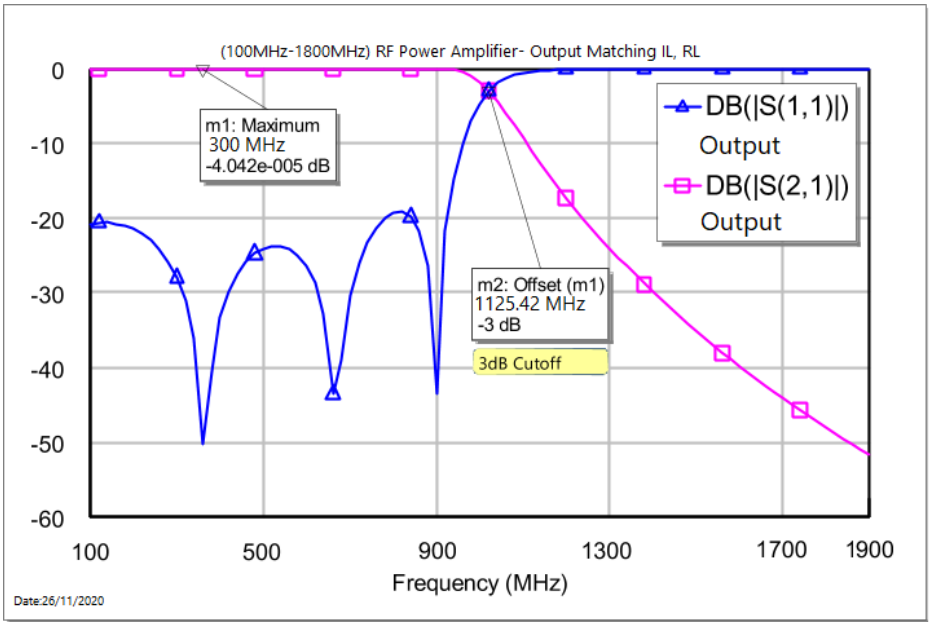
بالاعتماد على برنامج (MICROWAVE OFFICE) قمنا بإجراء محاكاة للمضخّم المقترح حيث تم دراسة توافق الممانعات بدراسة ضياع الإدخال (Insertion loss)



وضياع الإرجاع (Return loss) لكل من دخل وخرج المضخّم، يظهر الشكل (4) مخطط الاستجابة الترددية لدخل المضخّم.

الشكل (4) مخطط الاستجابة الترددية للدخل

نلاحظ من الشكل (4) الناتج عن المحاكاة أن (S11) والتي تعبر عن (Return loss) والتي تحدد درجة توافق الممانعات أنها وسطياً بين (dB 5-) إلى (dB 8-) على طول المجال الترددي حتى الوصول إلى فجوة عند التردد 1250MHz بلغت (0 dB) مع العلم أن (S11) كلما كان أقل على طول المجال الترددي كان توافق الممانعات أفضل. كما يظهر في الشكل (4) (S21) والذي يعبر عن (Insertion loss) ضياع الادخال أنه قليل على طول المجال الترددي إلا عند التردد 1250MHz حيث بلغ (33.2 dB)، انطلاقاً من هذه النتائج نلاحظ أن دخل المضخّم يحقق توافق ممانعات جيد على طول المجال الترددي باستثناء التردد 1250MHz.

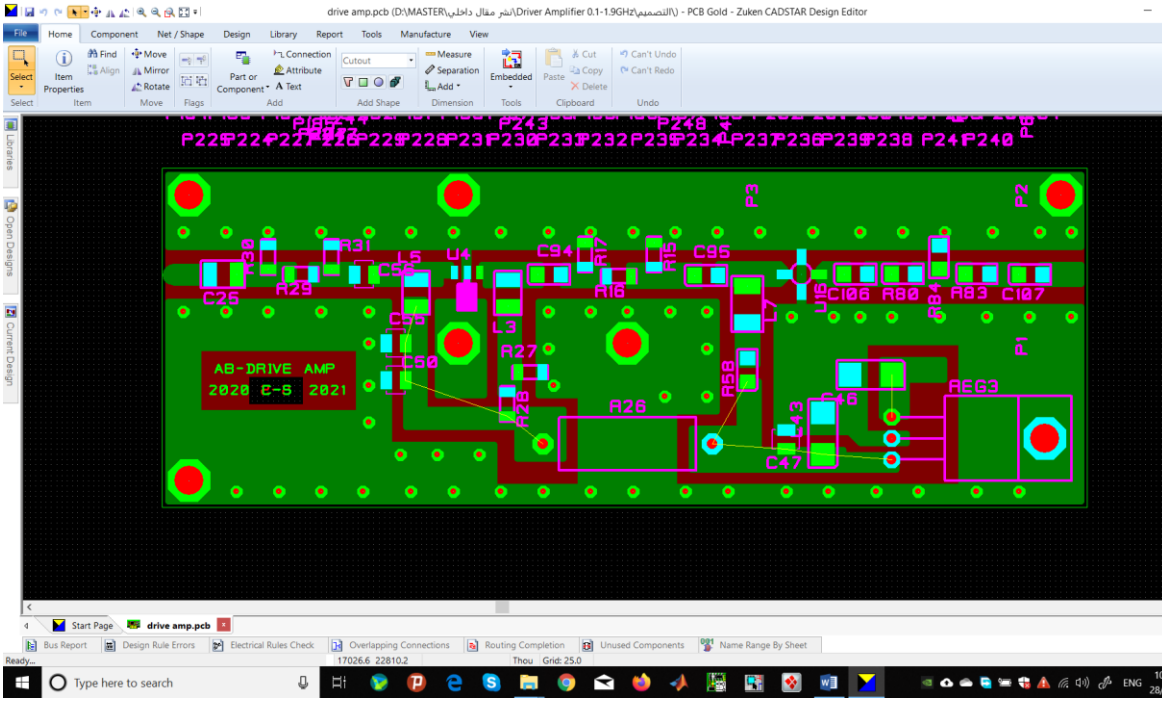


الشكل (5) مخطط الاستجابة الترددية للخرج

بالنسبة لخرج المضخّم نلاحظ من الشكل (5) الناتج أن خرج المضخّم يحقق فقد إرجاع (Return loss) صغير جداً ضمن المجال الترددي (100-900MHz)، لكن خارج هذا المجال يبدأ هذا الفقد (Loss) بالازدياد، أما بالنسبة لفقد الإدخال Insertion loss له قيم شبه صفرية على طول المجال الترددي (100-1000MHz) ويبدأ هذا الفقد بالازدياد خارج هذا المجال. نستنتج مما سبق أنا خرج المضخّم يحقق توافق ممانعات جيد عند التردد 100MHz حتى يصل إلى تردد القطع (1125.42MHz).

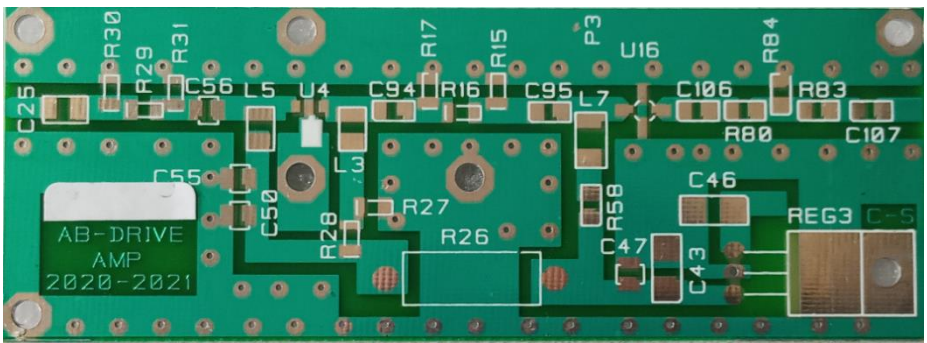
3-2-5- رسم الدارة المطبوعة PCB (Printed Circuit Board):

تم رسم الدارة المطبوعة بالاعتماد على برنامج (CADSTAR v16) من شركة (Zuken)، كما هو معلوم أن مواصفات الركيزة (Substrate) التي سوف تطبع عليها الدارة مهمة في تصميم الدارات الميكروية، لأنها تحدد أبعاد خطوط النقل للحفاظ على خط نقل بممانعة 50Ω (للحفاظ على توافق الممانعات)، لذا قمنا قبل التصميم بدراسة الركيزة المتوفرة حيث وجدت إمكانية الطباعة على ركيزة نوع (FR4) لها ثابت عازلية $\Sigma r =$



الشكل (6) مخطط الدارة المطبوعة PCB

كما يظهر الشكل (7) البطاقة الناتجة بأبعاد (11 X 4 cm).



الشكل (7) بطاقة PCB المصنّعة

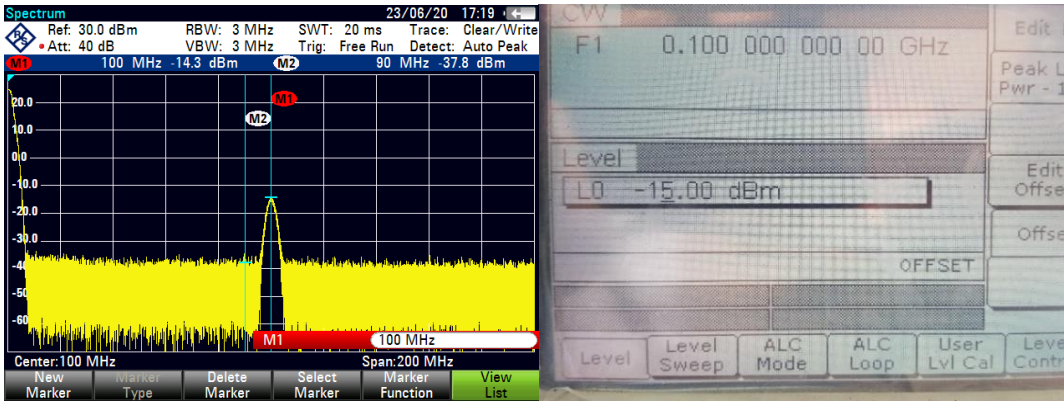
3-2-6- تجميع ولحام عناصر الدارة.

تم اختيار العناصر الغير فعالة للدارة نوع (SMD) بقياس 0805 وذلك لأنها لا تأخذ حيز كبير من الدارة، كما اخترنا نوع المأخذ لدخل وخرج المضخّم نوع (SMA Female) لها ممانعة (50Ω)، الشكل (8) يظهر دارة المضخّم بعدَّ تجميع العناصر

الشكل (8) بطاقة PCB المصنّعة بعد عملية تجميع العناصر

3-2-7- تهيئة منصّة الاختبار وإجراء القياسات المناسبة:

تم اجراء القياسات باستخدام منصّة الاختبار الموضحة في الشكل (1)، تم استخدام مولد الإشارة لتوليد إشارة (CW) حيث يمكن التحكم في ترددها ومستوى استطاعتها، الشكل



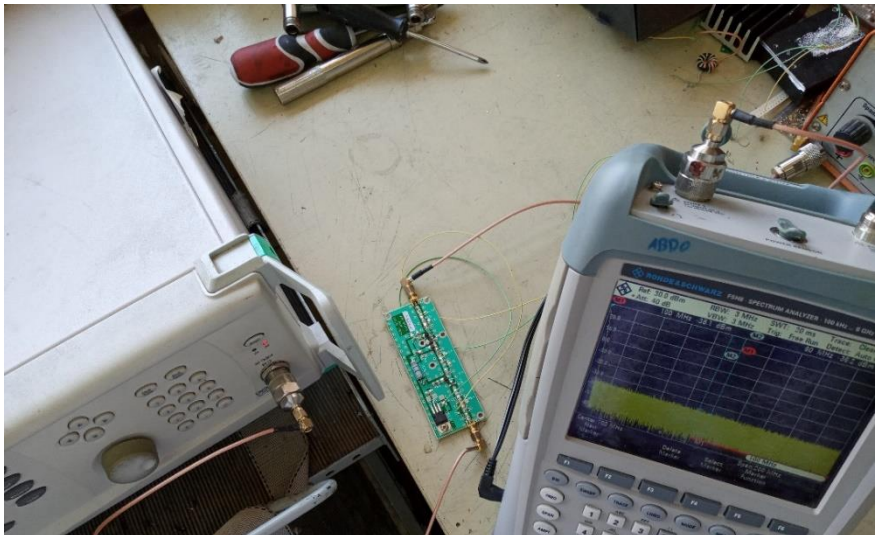
(أ) (ب)

الشكل(9): (أ) بارامترات الإشارة المولدة من مولد الإشارة، (ب) طيف إشارة دخل المضخّم

تم تهيئة منصّة الاختبار قبل اجراء الاختبارات والقياسات حيث تم قياس تخميد كابلات دخل وخرج المضخّم ووجد التالي:

- تخميد كابل إشارة الدخل 0.4dB عند التردد100MHz
- تخميد كابل إشارة الخرج 0.6dB عند التردد100MHz

كما تم وصل خرج المضخّم إلى مدخل البوابة الأولى من جهاز محلل الطيف والشبكة طراز (ROHDE & SCHWARZ FSH8) كما هو ظاهر في الشكل (10).



الشكل (10): مولد الإشارة مع المضخّم الموصول بمحلل الطيف

يعطي المضخّم الناتج استطاعة خرج حوالي 23dBm وذلك عندما يطبق على دخله إشارة موجة مستمرة (CW) باستطاعة (-15dBm).

4- النتائج ومناقشتها

تم تطبيق على دخل المضخّم إشارة ذات تردد متغيرة ضمن المجال الترددي 100MHz إلى1900MHz وباستطاعة (-15dB) (0.03mW)، أظّهرت النتائج أن استطاعة خرج المضخّم بلغت +22.1dBm وذلك عند التردد 100MHz تم قياس خرج المضخّم على طول المجال الترددي المطلوب، كما يمكن كتابة علاقة ربح المضخّم وفقا للتالي:

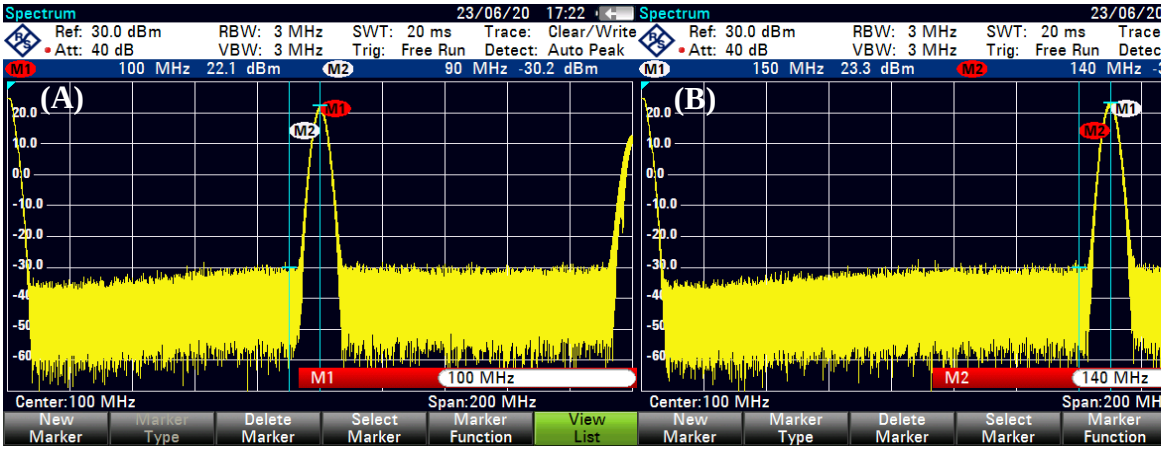
$$\mathrm{Gain_{PA}[dB]} = \mathrm{Pout[dBm]} - \mathrm{Pin[dBm]} + \mathrm{INCAB_{loss}[dB]} + \mathrm{OutCAB\ _{Loss}[dB]} \ldots (1)$$

حيث Pin: استطاعة إشارة الدخل، Pout: استطاعة إشارة الخرج، $InCABloss$: تخميد كبل دخل المضخّم،

$OutCABLoss$: تخميد كبل خرج المضخّم.

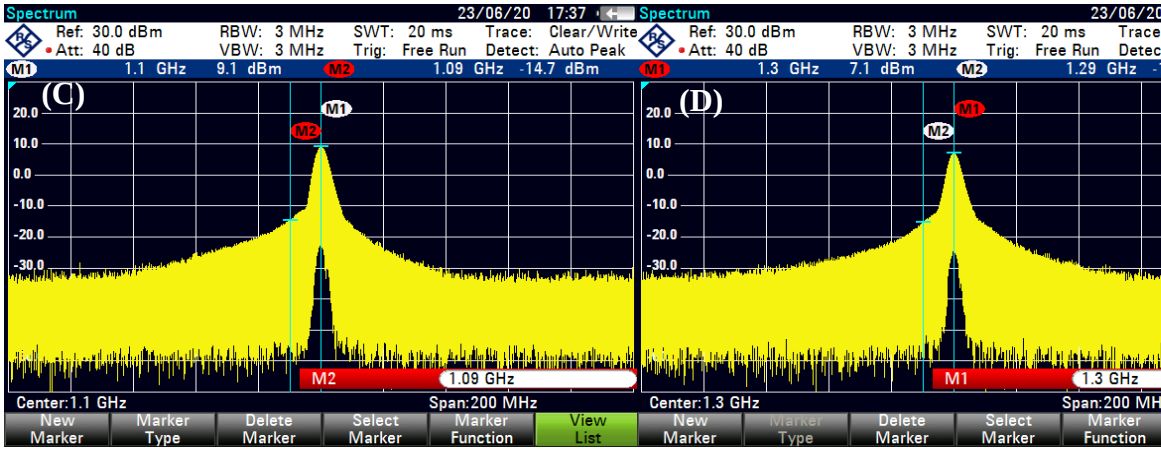
تصميم مضخّم (مكبر) قيادة راديوي عريض المجال يعمل عند المجال الترددي- (100MHz
1800MHz) بالاعتماد على ترانزستورات InGap/GaAS HBT MMIC

يظهر الشكل (11): (A) خرج المضخّم بحال طبق على دخله إشارة ترددها 100MHz باستطاعة (-15dBm) نجد أن استطاعة إشارة الخرج حوالي 22.1dBm أي حقق المضخّم ربحاً عند هذا التردد قرابة 37dB، أما (B) فهي خرج المضخّم بحال طبق على دخله إشارة ترددها 150MHz ولها نفس استطاعة وصفات إشارة الدخل السابقة نجد استطاعة الخرج حوالي 23.3dBm أي بربح 38dB.



الشكل (11): الطيف الترديد لإشارة خرج المضخّم عند الترددات (100MHz/140MHz)

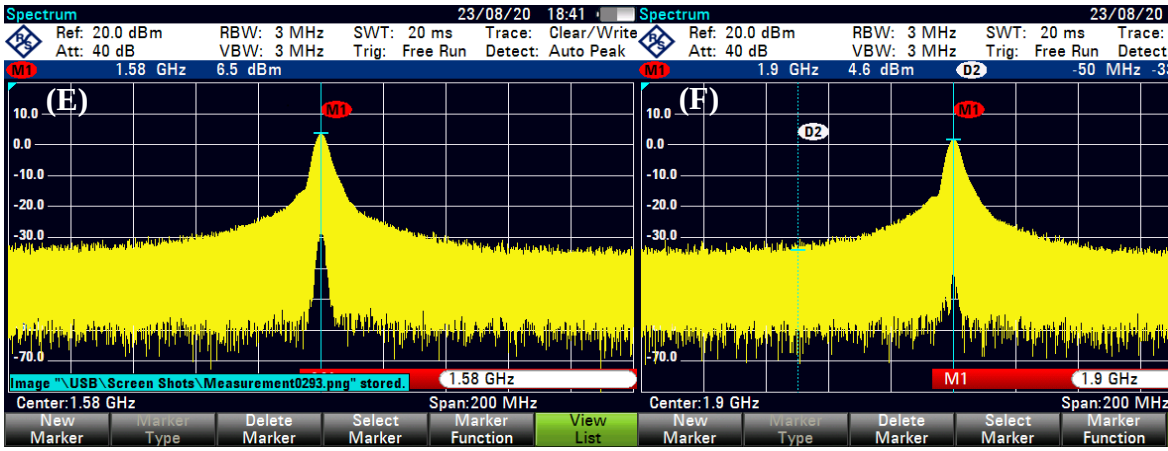
يظهر الشكل (12): (C) خرج المضخّم بحال طبق على دخله إشارة ترددها 1100MHz باستطاعة بنفس صفات إشارات الدخل السابقة نجد أن استطاعة إشارة الخرج حوالي 9.1dBm بربح قدره 24dB، أما (D) فهي خرج المضخّم بحال طبق على دخله إشارة ترددها 1300MHz نجد استطاعة الخرج حوالي 7.1dBm بربح 22dB.



الشكل (12): الطيف التردد لإشارة خرج المضخّم عند الترددات (1090MHz/1300MHz)

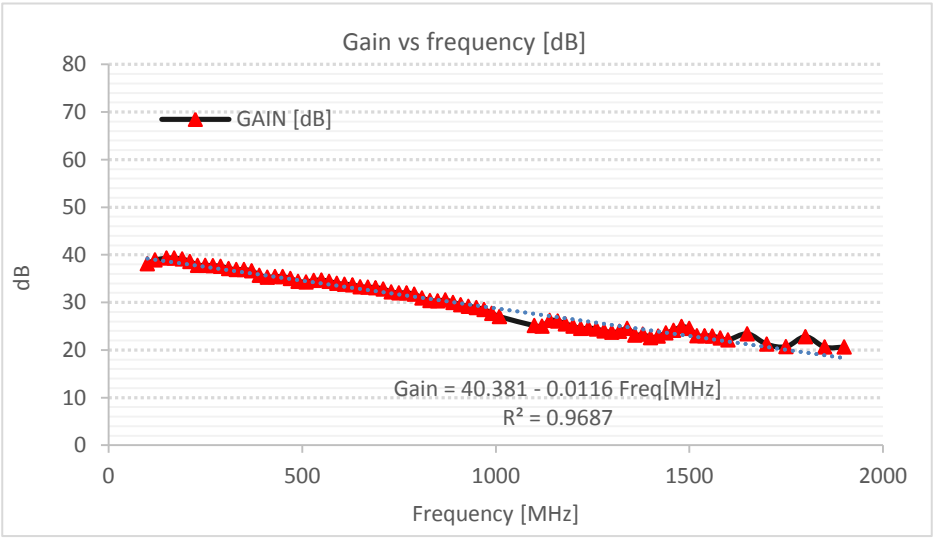
نلاحظ من هذه النتائج أن ربح المضخّم بدأ بالانخفاض بشكل ملحوظ بعد التردد 1100MHz هذا الانخفاض في الربح نتيجة زيادة فقد الإدخال (Insertion loss) وفقد الإرجاع (Return loss) لخرج المضخّم هذه النتائج قريبة نسبياً من نتائج المحاكاة السابقة التي حددت تردد قطع عند التردد 1125MHz والذي عنده ينخفض توافق الممانعات ويزداد الفقد.

يظهر الشكل (13): (E) خرج المضخّم بحال طبق على دخله إشارة ترددها 1580MHz نجد أن استطاعة إشارة الخرج حوالي 6.5dBm بربح قدره 21.5dB، و(F) الخرج عند التردد 1900MHz نجد استطاعة الخرج 4.6dBm بربح 19.6dB.



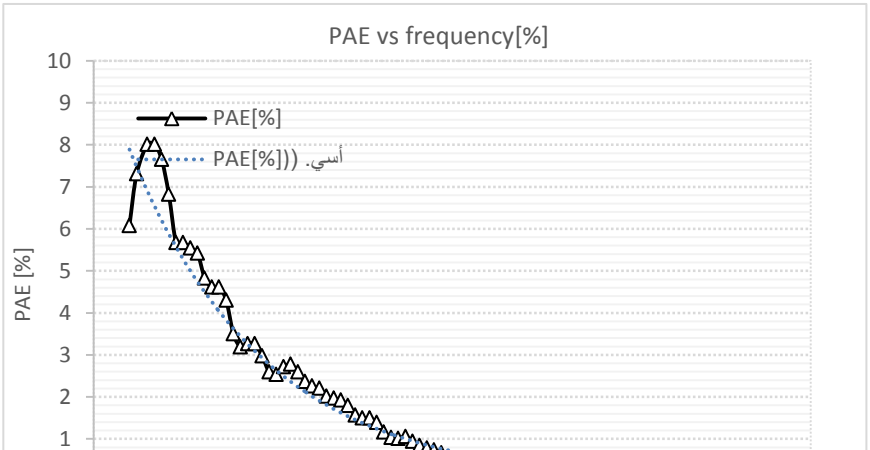
الشكل (13): الطيف التردد لإشارة خرج المضخّم عند الترددات (1580MHz/1900MHz)

وجد أن أعظم ربح يمكن أن يقدمها المضخّم هو 39.3dB وذلك عند المجال الترددي 150MHz-170MHz وهو ربح عالي، خارج هذا المجال بدأ ربح المضخّم بتناقص تدريجياً بشكل شبه خطي مع زيادة التردد حتى وصل إلى 20dB عند التردد 1800MHz، على الرغم من انخفاض الربح إلى أنه مازال يعتبر ربحاً عالياً الشكل (14)



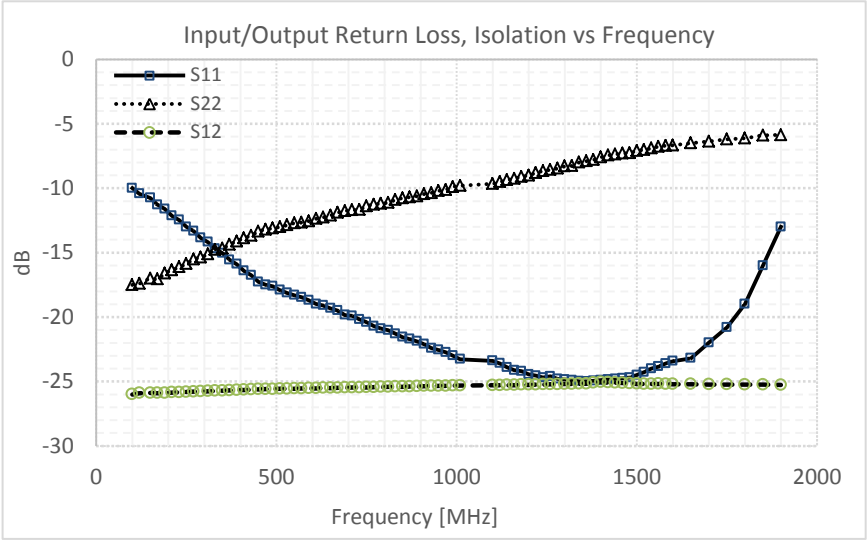
الشكل (14): ربح المضخّم كتابع للتردد

قدم المضخّم أفضل أداء له عند المجال الترددي 100-300MHz من حيث ربح المضخّم وكفاءة الاستطاعة المضافة (Power Added Efficiency (PAE)) حيث بلغت حوالي 8% ثم بدأت بالتناقص تدريجياً مع زيادة التردد، الشكل (15) يظهر تغيير (PAE) مع تغيير التردد.



الشكل (15): كفاءة الاستطاعة المضافة PAE كتابع للتردد

الشكل (16) يظهر معاملات التبعثر (S-parameters) الخاصة بالمضخّم حيث (S11) تعبّر عن ضياع الإرجاع لدخل المضخّم (input return loss) الذي يزداد مع زيادة التردد إلى أن يصل إلى التردد 1340MHz ليعاود بعدها الارتفاع، أما S22 تعبّر عن ضياع الإرجاع لخرج المضخّم (output return loss) الذي يزداد تدريجياً مع زيادة التردد



الشكل (16): معاملات التبعثر (S-parameters) الخاصة بالمضخّم

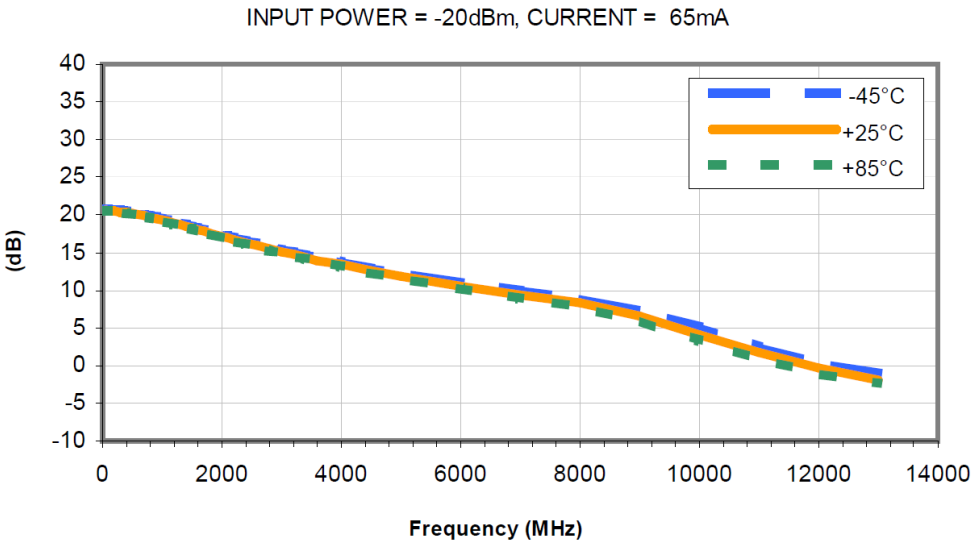
4-1 مقارنة أداء كل مضخّم على حدى مع المضخّم الناتج

- المضخم(ERA-5+): هو ترازستور استطاعة يعمل ضمن المجال الترددي DC- 4GHz وهو مضخّم يتحسس للإشارات الضعيفة بحدود 50dBm- إلى - 10dBmويعمل على تكبيرها بربح استطاعة (14-20dB)، الجدول (1) يظهر مواصفات هذا المضخم وفقاً للشركة المصنّعة.

الجدول (1): مواصفات المضخم ERA-5+ [20]

Parameter		Min.	Typ.	Max.	Units	Cpk
Frequency Range*		DC		4	GHz	
Gain	f=0.1GHz f=1 GHz f=2 GHz f=3 GHz f=4 GHz	19 — 16 12	20.2 19.5 18.5 16.7 14.3	22 19 16	dB	≥1.5
Magnitude of Gain Variation versus Temperature (values are negative)	f=0.1GHz f=1 GHz f=2 GHz f=3 GHz f=4 GHz		.0025 .0034 .0043 .0052 .0065	.005 .007 .0085 .0105 .013	dB/°C	
Input Return Loss	f=0.1 GHz f=2 GHz f=4 GHz		21 23 21		dB	
Output Return Loss	f=0.1 GHz f=2 GHz f=4 GHz		30 26 17		dB	
Reverse Isolation	f=2 GHz	19	22		dB	

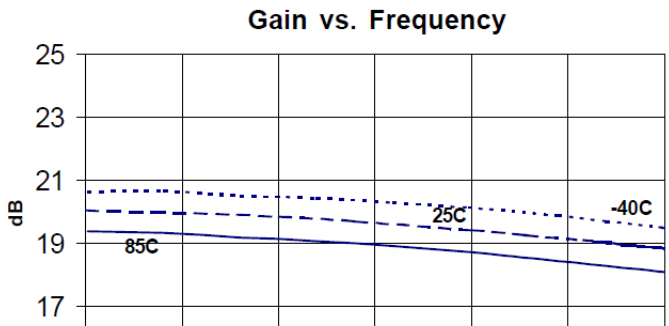
كما يظهر الشكل (17) ربح المضخّم كتابع للتردد، نلاحظ أن أعظم ربح للمضخّم يبلغ 20 dB ويتناقص هذا الربح تدريجياً بزيادة التردد.

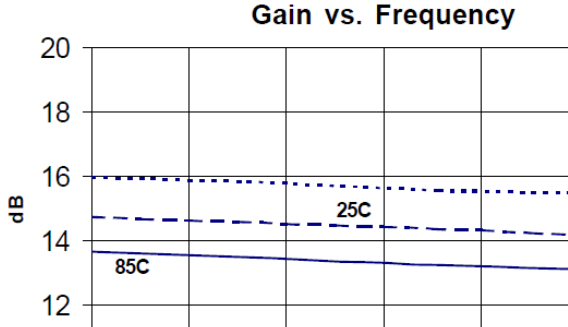


الشكل (17): يظهر منحني ربح المضخّم ERA كتابع مع التردد [20]

ERA-5+ هو مضخم جيد لتكبير الإشارات ذات الاستطلاعات المنخفضة الأقل من -10dBm لكن سيئته هو أن أعظم إشارة على خرجه لن تتجاوز (+10dBm ± 2dB) وذلك بحال قدم هذا المضخم ربح أعظمي مقداره 22dB، وضع عدة مراحل تكبير من مضخمات ERA لن يحسن مستوى الإشارة بشكل حقيقي بل سوف يكون له أثراً سلبياً بزيادة مستوى الضجيج الذي يتحسس له المضخم بشكل أكبر من الإشارة المفيدة وتدخل المضخّم في حالة التشبّع، لذا ظهرت الحاجة في هذا البحث لمرحلة تكبير ثانوية تستخدم مضخّم يمكنه رفع مستوى الاستطاعة إلى أكبر من +10dBm.

- المضخّم SXA-289: هو مضخّم استطاعة متوسط يعمل كمضخّم قيادة ضمن المجال الترددي 50MHz-1950MHz ويعطي ربح استطاعة (13dB-20)، الشكل (18) يظهر ربح المضخّم ضمن المجال الترددي (800-1990MHz).





الشكل (18): يظهر منحني ربح المضخّم SXA كتابع مع التردد [21]

يتحسس SXA-289 للإشارات ذات مستوى الاستطاعة (-10dB) إلى (+20dB) بربح أعظمي 20dB+، ويعطي استطاعة خرج أعظمية 23dB+، زيادة مستوى استطاعة الدخل لن تؤثر على استطاعة خرج المضخّم لأن المضخّم يدخل مرحلة التشبّع. يمكن استخدام مرحلتي تضخّيم SXA، لكن لـSXA رقم ضجيج 5.5dB وحسب علاقة Friis

$$F_{total} = F_1 + \frac{F_2 - 1}{G_1} + \frac{F_3 - 1}{G_1 G_2} + \cdots$$

حيث F1,F2,F3 عامل الضجيج لكل مرحلة، Ftotal عامل الضجيج الكلي و G1,G2,G3 عامل ربح الاستطاعة لكل مرحلة.

في حال استخدام مرحلتي SXA

لـSXA ، $F_1 = F_2 = 5.5dB$ $G_1 = 15dB$ فيكون رقم الضجيج لمرحلتي تكبير SXA

$$F_{total} = 5.8dB$$

أمـا للمضـخم المقتـرح ERA & SXA $F_2 = G_1 = 15dB$ $F_1 = 3.5dB$ $5.5dB$

$$F_{total} = 3.8dB$$

يعرض الجدول (2) أداء المضخّم المقترح بالمقارنة مع المضخِّمين السابقين:

الجدول (2): مقارنة أداء المضخّم المقترح مع المضخِّمين الجزئيين

	SXA-289	ERA-5+	المضخّم المقترح SXA+
رقم الضجيج	5.5dB	3.5dB	3.8dB
استطاعة الخرج	يقدم استطاعة خرج أكبر من (+23dB± 2dB)	استطاعة الخرج الأعظمية قرابة (+10dBm± 2dB)	يقدم استطاعة خرج تص (24.3dBm)
الربح Gain	من (+20dB) إلى (+15dB)	من (+20.2dB) إلى (+14.3dB)	من (+39.3dB) إلى (B

5- الاستنتاجات والتوصيات

تم تصـميم وتصـنّيع مضـخّم قيـادة عـريض المجـال (100-1800MHz) بالاعتمـاد علـى ترانزسـتورات(InGaP/GaAs HBT MMIC) ، قـدم اسـتطاعة خـرج (23dBm إلـى 5.6dBm) بـربح (39.3dB إلـى 20dB) وذلـك عند تكبيره لإشارة موجـة مستمرة (CW) مطبقة على دخله باستطاعة (-15dBm). قدم المضخّم كفاءة استطاعة مضافة (PAE) حوالي 8% عند مجال الترددات المنخفضة وذلك عند تطبيق جهد انحياز مصرف 12V. سيتم العمل علـى تحسين توافق الممانعات لخرج المضـخّم وتحسين (PAE) للمضـخّم باستخدام مكونات منخفضة الفقد وتحسين اللحام وتقليل طول أسلاك التوصيل.

6- المراجع (References)

[1] BROWNE.J, 2000 - **InGaP/GaAs provides high linearity HBTs Microwave & RF**.(2), 121P.

[2] FAZAL.A, July 1995 - Introduction to special Issue on Emerging comercial and Consumer Circuits Systems, and their Applications. **IEEE transactions on Microwave Theory and Techniques**, Vol. 43, N.7.

[3] SITCH.J, Oct 1997 - HBTs in Telecomunications. **Solid-State Electronics**, pp.1397-1405.

[4] BAYRAKTAROGLU. B, Oct (1997) - HBT power devices and circuits. pp. 1657-1665.

[5] KOBAYASHI.K.W, Jan 1998, An AlGaAs/GaAs PA-LNA transceiver MMIC chip for 1.9 GHz digital cordless telephones. **Microwave Journal**, pp. 94.

[6] KOBAYASHI.T,NAKAMURA.F, TAIRA.K, Taira and H. Kawai, in Inst. 1989 - Band Lineup for a GainP/GaAs p-n-p Heterojunction Bipolar Transistor. **Conf. Ser**, 106, ch.6,pp. 357-362.

[7] Hanson.A.W, Baillargeon.J.N, Stockman.S.A, Apostolakis.P.J. and Stillman.G.E, 1991 - presented at the 1991 Electron Material Conf., Bouder, Co.

[8] Lothian.J.R, Kuo.J.M, Ren. and Pearton.S, 1992 - Plasma and Wet Chemical Etching of In0.5Ga0.5P. **Journal of Electronic Materials**, vol. 21, N. 4.

[9] 3GPP TS 36.104 V15.0.0, "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception (Release 15)," September (2017). [Online]. Available:

https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2412;

[10] Mini-Circuit,2015-**Fixed attenuators help minimize impedance mismatches**, [Online]. Available: https://www.minicircuits.com/app/AN70-001.pdf ;

[11] RFcafe, **VSWR Reduction by Matched Attenuator**, [Online]. Available: http://www.rfcafe.com/references/electrical/vswr-reduction.htm;

[12] Teng.J and Wang.B, 2018- **Design of a Driver-stage Power Amplifier for Wireless Transmitter**. IEEE , 978-1-5386-9389-6/(2018 IEEE).

[13] Faiz.M, Earles.S, Hou.B and Zhang.S, 2012- **Design of a Two Watt Power Amplifier in InGaP/GaAs HPT Process for very High Linearity Wireless Application**. IEEE, 978-1-61284-1438-2/(2012 IEEE).

[14] Bansal.K, Chander.S, Gupta.S and Basu.A, 2020- **Design and development of (1.2-2.7) GHz GaN HEMT based broadband power amplifier**. IEEE , 978-1-7281-6368-0/(2020 IEEE).

[15] Fan.X, Yu.Z, Lu.J and Hua.Z, 2015- **Design of a 0.7~1.5 GHz Wideband Power Amplifier in 0.18-µm CMOS**. IEEE , (2015 IEEE).

[16] Yong.K, Salleh.A, Abd Aziz.M and Misran.M, 2013- **Design of Low Power Wideband Low Noise Amplifier for Software Defined Radio at 100 MHz to 1GHz**. ScienceDirect , Melaka, Malaysia.

[17] Ahmad Zaki Hamid.E, Mudzakkir Ridwan.A, 2019- **" High Gain 2-stage Class-E RF Power Amplifier for Wireless**

Power Transfer ". PhotonIcs & Electromagnetics Research Symposium , Rome, Italy.

[18] Çağdaş.E, Kızılbey.O, and Yazgı.M, 2018- **High Efficiency Wideband Power Amplifier with Class-J Configuration**. IEEE , 978-1-7132--0/(2018 IEEE).

[19] Zurek.P, Cappello.T, and Popovi´c.Z, 2019- **A Concurrent 2.2/3.9-GHz Dual-Band GaN Power Amplifier**. IEEE , 978-1-8386-5947-2/(2019 IEEE).

[20] Mini-Circuits, 2019- **Monolithic Amplifier ERA-5+**. Brooklyn, NY.

[21] Sirenza Microdevices, **GaAs HBT Amplifier SXA-289**. Almanor Ave, Sunnyvale.

طريقة جديدة للتحكم عن بعد بمزارع الرياح باستخدام SCADA-OPC وشبكات بتري الضبابية

الدكتور المهندس: مسعود الأتاسي

استاذ مساعد في قسم هندسة الميكاترونك – كلية الهمك – جامعة البعث.

الملخص

يعدُّ التحكم بالنظم الموزعة لتوليد الطاقة تحدٍ كبير نظراً لطبيعتها المعقدة، وقد استخدمت شبكات بتري Petri Net كأداة رسومية لنمذجة وتحليل الأنظمة المعقدة. وتعد شبكات بتري فعّالة في النظم التتابعية Sequential ذات الأحداث المتقطعة نظراً لأن شروط الانتقال بين الحالات المختلفة تكون حدية. هناك بعض النظم الصناعية المعقدة ذات طبيعة مستمرة وشروط الانتقال بين الحالات المختلفة للنظام يجب أن تكون عائمة Fuzzy. يمكن اعتبار نظم التوليد مثالاً للنظم المعقدة ذات الطبيعة المستمرة والتي تكون بعض مكوناتها عبارة عن نظم لا خطية، ومثالها العنفات الريحية التي يتأثر عملها بشكل كبير بالظروف المناخية المحيطة وخصوصاً سرعة الرياح، وعندما يكون لدينا عدة عنفات ريحية فإننا نحتاج إلى متحكم إشرافي ينظم أداء وحدات القياس البعيدة الفرعية (RTU - **R**emote **T**elemetry **U**nit) للوصول إلى الأداء الكلي الأمثل للنظام. ويشكل بحثنا مساهمة في تصميم نظام تحكم إشرافي يعتمد تقنيات التحكم العائم لإدارة نظام مزرعة ريحية موزعة. وقمنا بدمج متحكم إشرافي SCADA (**S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition) مع البروتوكول OPC (**O**pen **P**latform **C**ommunication) ليؤمن الإدارة المثلى لنظام توليد الطاقة من خلال استخدام متحكمات صغرية (Microcontrollers) ومنطقية (Programmable Logic Controllers).

ويقوم النظام المصمم بإدارة هذه المتحكمات من خلال مراقبة كل عنفة ريحية، والوسط المحيط بها والحمل الكهربائي، وذلك بأخذ عينات من بيانات التشغيل الرئيسة التي

توفرها المولدات للمحطات المختلفة. وترتبط هذه المتحكمات الفرعية عبر روابط الاتصالات الموزعة بعيدة المدى DNP (**D**istributed **N**etwork **P**rotocol) وتستخدم بيانات لتحديد وتشخيص المشاكل المحتملة وتقديم حل لها عن طريق التحكم باستطاعة مولدة العنفة الريحية للحفاظ على نقطة التشغيل العظمى للعنفة ذات الريش الثابتة من خلال التحكم بسرعة التوربين أو العنفة ذات الريش المتحركة من خلال التحكم بزاوية ميل الريش. وقد منح بروتوكول الـ OPC برمجيات سكادا القدرة على القيام بدور مدير للشبكة الصناعية، حيث سمح لهم بإدارة جميع التجهيزات الموصولة على الشبكة على اختلاف أنواعها واختلاف الشركات الصانعة لها.

الكلمات المفتاحية: المنطق العائم، شبكات بتري العائمة الملونة ، مزرعة ريحية، التحكم الإشرافي الموزع، منصة الاتصالات مفتوحة المصدر. بروتوكول شبكة الاتصالات الموزعة.

A new method for remote control of wind farms using the SCADA-OPC and fuzzy Petri networks

Dr. Massoud ATASSI. Associate Professor at Mecatronics Engineering Department – Al Baath University

Abstract

Controlling distributed power generation systems constitutes a major challenge due to its complex nature. Petri Nets are used as a graphical tool for modeling and analyzing complex systems. Petri Nets are effective in sequential systems with discontinuous events since the transmission conditions between different states are limited. There are number of complex industrial systems of a continuous nature as well as conditions of transition between the different states of the system that must be fuzzy. Generating systems can be considered as an example of complex systems of a continuous nature, some components of which are non-linear systems, for example wind turbines whose work is strongly affected by the surrounding climatic conditions, in particular, when we have multiple wind turbines, we

need a supervisory controller that regulates the performance of the Sub-RTUs (Remote Telemetry Units) to achieve optimal overall system performance. Our research constitutes a contribution to the design of a surveillance control system using fuzzy control techniques to manage a distributed wind farm system. We have successfully integrated the SCADA (supervisory control and data acquisition system) with the OPC (Open Platform Communication) protocol to ensure optimal management of the energy production system through the use of microcontrollers and programmable logic controllers (PLC).

The designed system operates these controllers through monitoring every wind turbine, the surrounding environment and the electrical load, by taking samples of the main operating data provided by the generators to the different stations. These sub-controllers which are connected via Distributed Network Protocol (DNP) employ data to identify and diagnose potential problems and provide a solution through monitoring the ability of a wind turbine to maintain the maximum operating point of the turbine at fixed blades by controlling the speed of the turbine or the moving blades by means of controlling the angle of inclination of the feathers. The OPC protocol has given the SCADA software the ability to act as an industrial network manager, allowing them to manage all the equipments connected to the network of different types and manufacturers.

Keywords: Fuzzy Logic (FL), (CFPN) Colored Fuzzy Petri Net, Aeolian,

Wind Farm, SCADA, OPC, DNP.

1. مقدمة

تُعرَّف مصادر الطاقات المتجددة بأنها المصادر التي تتولد بصورة طبيعية ومستدامة بحيث يمكن للإنسان الاستفادة منها دون إحداث ضرراً ملموساً على البيئة. تُعدُّ العنفات الريحية Wind Turbine ونظم الطاقة الكهرومائية، ونظم الطاقة الشمسية، أكثر النظم انتشاراً في مجال توليد الطاقة الكهربائية من المصادر المتجددة. وسوف نهتم بهذا المقال بمزرعة الرياح وهي مجموعة من عنفات الرياح موجودة في نفس الموقع تستخدم لإنتاج الطاقة الكهربائية. وتتكون مزرعة الرياح الكبيرة من عدة مئات من عنفات الرياح وتغطي مساحات واسعة. ويمكن بنائها سواء في البحر Offshore أو على اليابسة Onshore. [1]

الوظيفة الرئيسة من السكادا SCADA، هي الرقابة الإشرافية والحصول على البيانات من الأجهزة وتوفير التحكم الشامل عن بعد من منصة برمجيات المضيف سكادا SCADA Host software، التي توفر ميزات لعرض البيانات الرسومية والمنحنيات Trending والتنبيه Alarm & Event والتخزين التاريخي للبيانات History data base. تكون أفضل تطبيقات أنظمة السكادا في العمليات الموزعة على مساحات ومناطق جغرافية كبيرة ، وتكون سهلة المراقبة والتحكم وتتطلب تدخل متكرر أو منتظم أو عادي، والأمثلة كثيرة لتطبيقات أنظمة السكادا، مثل محطات إنتاج الغاز أو النفط وأنظمة الري التي تغطي مئات الأميال المربعة ويكون التحكم به عن طريق فتح وإغلاق صمامات بسيطة، وتتطلب جمع معلومات قياس لمستويات المياه. وكذلك محطات التوليد وأنظمة نقل القدرة الكهربائية، وتتمثل مهمة التحكم الإشرافي هنا بتأمين التغذية المستمرة للحمل الكهربائي عن طريق الإدارة المثلى لموارد النظام الكهربائي. [2]

2. هدف البحث

تصميم نظام تحكم إشرافي يعتمد تقنيات التحكم العائم لإدارة نظام مزرعة ريحية موزعة عن طريق دمج SCADA مع بروتوكول OPC للإدارة المثلى لنظام توليد الطاقة.

تم استخدام متحكمات فرعية مختلفة (PLCs /Microcontrollers) للسيطرة على العنفات الريحية من خلال مراقبة الطقس وأخذ عينات من بيانات التشغيل الرئيسة التي توفرها المولدات والمحطات المختلفة. ترتبط هذه الأنظمة عبر روابط الاتصالات الموزعة بعيدة المدى DNP. تستخدم هذه البيانات من قبل النظام SCADA-OPC لتحديد وتشخيص المشاكل المحتملة وتقديم حل لها وتخزين بياناتها التاريخية. استخدم أسلوب التحكم باستطاعة المولدة للعنفة الريحية وذلك عن طريق ملاحقة نقطة التشغيل العظمى للعنفة الريحية ذات الريش الثابتة أو ذات الريش المتحركة. ويمنح بروتوكول الـ OPC برمجيات سكادا إدارة جميع التجهيزات الموصولة على الشبكة، على اختلاف أنواعها واختلاف الشركات الصانعة لها.

3. مواد وطرق البحث

1.3 أدوات البحث

- **الحزمة البرمجية Lab VIEW:**

تعد لابفيو Lab VIEW لغة برمجة رسومية Graphical تستخدم الأيقونات عوضاً عن التعابير النصية لإنشاء التطبيقات البرمجية، وعلى نقيض لغات البرمجة التقليدية التي تستخدم التعابير النصية و تحدد التعليمات Instruction مراحل تنفيذ البرنامج. تستخدم لغة البرمجة لابفيو مفهوم تدفق البيانات Dataflow الذي يحدد تنفيذ البرنامج، حيث تستطيع لابفيو التعامل مع عدد هائل من بطاقات التحصيل وأجهزة القياس. يحتوي لابفيو على عدد كبير من المكتبات التي تضم توابع Functions لتطبيقات تحصيل البيانات، وتوليد الإشارة وقياسها، وتكييف الإشارة وتحليلها. يمتاز لابفيو بأنه أداة نمذجة وتطبيق في آن معاً، حيث يمكن من خلال الحزمة البرمجية إجراء نمذجة للتطبيق المراد اختباره، ويمكن بناء نماذج تجريبية فيها اعتماداً على مفهوم Hardware-in-the-loop ، وبعد ذلك القيام بتنفيذ التطبيق بشكل عملي.[4][3]

- **الأداة CPN TOOLS:**

الأداة البرمجية CPN TOOLS هي أداة رسومية مرتبطة بلغة برمجية عالية المستوى CPN ML (Markup Language)، وتستخدم لإنشاء شبكة بتري وتحريرها ومحاكتها وتحليلها. و يتم من خلالها إجراء محاكاة لكل جزء من أجزاء النموذج المدروس بهدف اختبار صحة كل جزء من أجزائه، والتوصل إلى التصميم الكامل للنموذج و مراقبته Monitoring. [5]

2.3 دراسة مرجعية

- في عام 2004 عمل كل من Seung Jun Lee و Poong Hyun Seong على إجراء نمذجة وتحليل لسلوك نظام التحكم والمراقبة وتشخيص الأعطال **باستخدام شبكات بتري العائمة الملونة** Fuzzy Colored Petri Nets وكان الهدف من ذلك إدارة مثلى لمحطة طاقة نووية Nuclear Power [6].
- في عام 2006 عمل الباحثين Xu Luo, Mladen Kezunovic على إجراء نمذجة لنظام التحكم بالقدرة الكهربائية والمراقبة وتشخيص الأعطال باستخدام (Continuous CFPN Fuzzy Petri Net) وكان الهدف من ذلك إدارة محطة طاقة كهربائية[7].
- طور أمين حاج زاده [8] استراتيجية تحكم لتدفق الطاقة الفعلية في نظام تخزين هجين مؤلف من بطاريات وخلايا وقود. تضمن المنهج المقترح **متحكم إشرافي متقدم** في الطبقة الأولى مهمته التقاط كافة أنماط التشغيل الممكنة وفي الطبقة الثانية تم تطوير متحكم عائم لفصل الطاقة Power Spilting بين البطارية وخلية الوقود. وفي الطبقة الثالثة يوجد متحكمات محلية لتنظيم النقاط المرجعية Set Points لكل نظام فرعي للوصول إلى الأداء الأفضل ومؤشرات تشغيل مقبولة. ولقد أظهرت نمذجة النتائج تحسينات في كفاءة تشغيل النظام الهجين.
- بحثت ماريا هرناديز [9] في تصميم متحكم هرمي، للتحكم بنظام هجين مؤلف من عنفة ريحية ولاقط كهروضوئي ومصفوفة بطاريات وحمل كهربائي، مع إمكانية وصل النظام إلى

الشبكة الكهربائية. يتكون نظام **التحكم الهرمي** المقترح من متحكمات محلية في المستوى الأدنى لكل وحدة توليد ووحدة تخزين.

- وصمم سبيروس وآخرون [10] **متحكم إشرافي** لنظام هجين مكون من لاقط كهروضوئي و**مولد ريحي** وبطاريات ومولد ديزل ومدخرات بالإضافة إلى مولد خلايا وقود. تم تصميم **متحكم هرمي** مكون من ثلاث طبقات : طبقة الحقل I/O Fields تضم الحساسات والمفعلات، والمستوى الثاني هو مستوى التشغيل Operation Level، والمستوى الثالث هو المستوى الإشرافي. نفذ النظام باستخدام الحزمة البرمجية SCADA. كانت مهمة المتحكم الإشرافي هي فصل/وصل **الأنظمة الفرعية**، في حين أن مهمة المستوى التشغيلي تنفيذ الإجراءات والأفعال التحكمية بناءً على القرارات المتخذة في المستوى الإشرافي.

- أما الشاطر [11] فقد ركَّزت على دراسة تدفق الطاقة بين مكونات نظام توليد طاقة هجين مؤلف من مولد كهروضوئي وعنفة ريحية وخلايا وقود، وناقشت تنظيم جهد الخرج المستمر باستخدام **متحكم عائم**. تم اختبار المتحكم من خلال النمذجة باستخدام بيانات أحد مواقع الرصد المناخية. وخلصت الدراسة إلى جدوى استخدام التحكم العائم **لتعقب نقطة التشغيل العظمى للاستطاعة** لكل من اللاقط الكهروضوئي والعنفة الريحية. بالإضافة إلى دقة تنظيم جهد الخرج DC

- حالياً نظام SCADA PcVue الذي يعمل كمركز عصبي لمزارع الرياح، يربط مختلف التوربينات والمحطات الفرعية ومحطات الطقس إلى غرفة التحكم المركزية لمراقبة سلوك جميع مزارع الرياح وتسجيل النشاطات على فترات زمنية منتظمة وتحديد التعديلات المطلوبة أو الإجراءات التصحيحية التي يجب اتخاذها. هذا النظام مستخدم ومحتكر من شركات ضخمة مثل Iberdrola Renewables [12].

- يحتوي كل توربين رياح على صندوق تحكم يحتوي على **PLC** ومحول طاقة **ولوحات تحكم** ووحدة إدخال / إخراج. تقوم مستشعرات سرعة الرياح واتجاهها، وسرعة دوران

المحور، والعديد من **الحساسات** الأخرى بجمع البيانات وإرسالها إلى PLC بحيث نظام التحكم يصبح قادراً على توجيه التوربين بالكامل في الاتجاه المطلوب لتوليد الطاقة الأمثل. جميع التوربينات متصلة **بشبكة محلية** ، وصندوق التحكم لكل توربين متصل بواسطة ناقل **إيثرنت** بقاعدة البرج، وهو نفسه متصل بالشبكة المحلية عن طريق وصلة ألياف ضوئية. ترتبط الشبكة المحلية بمحطة **تحكم عن بعد**، تدير وتجمع البيانات، وتعديل بارامترات التوربين، وتولد إنذارات ذكية مع توفير وظائف استكشاف الأخطاء وإصلاحها وإعداد التقارير من خلال مركز التحكم ومعالجة. [13]

بهذا البحث تم تصميم نظام تحكم إشرافي بالاستفادة من الدراسات المرجعية السابقة وبطريقة جديدة وذلك بالاعتماد على تقنيات التحكم العائم السابقة لإدارة نظام مزرعة ريحية موزعة عن طريق دمج SCADA مع بروتوكول OPC للإدارة المثلى لنظام توليد الطاقة على الشبكة على اختلاف أنواعها واختلاف الشركات الصانعة لها واستخدام بروتوكول الاتصال الموزع DNP للتحكم بمزارع الرياح عن بعد.

3.3 دراسة مزرعة الرياحWind farm

يتكون النظام الريحي WECS (Wind Energy Conversion Systems) من البرج Tower والعنفة الريحية المزودة بثلاث شفرات Blades على الأغلب، وألية ملاحقة الهواء Yaw، ونظام نقل الحركة Mechanical Gear ومن الصرة Hub إلى المولد الكهربائي Generator. كل عنفة مزودة بنظام تحكم يقوم بوظائف المراقبة والتشغيل والحماية. ونظام كبح يتدخل ليوقف العنفات عند سرعات عالية للرياح، وظيفة علبة السرعة هي زيادة السرعة على مدخل المولد الكهربائي (Multiplicator)، وتتكون من عدد من المسننات التي تعشق بشكل ألي حسب سرعة الرياح لتحافظ على سرعة دوران معينة على دخل المولد الكهربائي. [14]

يتم اختيار التصميم الأنسب للمزرعة الريحية باتباع الخطوات التالية:

1.3.3 دراسة الأحمال والاحتياجات: تُجرى دراسة تفصيلية للحمل الكهربائي من حيث طبيعته وقيمته ونمطه: مستمر أو متناوب، وتغيراته مع الزمن. ويُحدَّد مقدار فقد الحمل المسموح به باعتباره أحد البارامترات المهمة لتصميم النظام.

2.3.3 تحديد مكونات النظام : يتلخص منشأ حركة الرياح في الطبيعة نتيجة انتقال الهواء من منطقة الضغط المرتفع (إشعاع شمسي قليل) إلى منطقة الضغط المنخفض (إشعاع شمسي عالي) ، وذلك لمعادلة الضغط بين المنطقتين. تمتصُّ عناصر الجو وسطح الأرض أشعة الشمس، فعند سقوط الإشعاع الشمسي على منطقة ما، يتأثر الغلاف الجوي ويسخن الهواء مما يؤدي إلى ازديادٍ كبيرٍ في حجمه وانخفاضٍ في كثافته، وعندها يَقِلُّ الوزن الحجمي للهواء في تلك المنطقة، مما يؤدي إلى انخفاض الضغط الجوي، أما المناطق التي ينخفض فيها مقدار الإشعاع الشمسي، فإن الوزن الحجمي للهواء يزداد، ويزداد تبعاً لذلك الضغط الجوي على تلك المناطق، وهكذا ينتقل الهواء من منطقة الضغط المرتفع إلى منطقة الضغط المنخفض.

تعد تقانات العنفات الريحية أو ما يعرف بنظم تحويل طاقة الرياح Wind Energy Conversion System أكثر التقانات التي تسارع العمل فيها خلال العقد الأخير، وحققت قفزات نوعية من حيث الاستطاعات التي تم الوصول إليها، وكذلك من خلال منافستها لأسعار توليد الكهرباء من المصادر المختلفة.

هناك عددٌ من العوامل الرئيسة التي سرَّعت تطور تقانة استخدام العنفات الريحية لتوليد الكهرباء [15] : متانة وقوة مركبات الفايبرFiber لإنتاج ريش ذات أطوال كبيرة بكلفة منخفضة. انخفاض أسعار إلكترونيات القدرة. إمكانية التحكم بالسرعة المتغيرة للمولد

الكهربائي للحصول على أكبر استطاعة متاحة. تراكم الخبرات والتجارب العملية التي ساهمت في تحسين عامل السعة Capacity Factor.

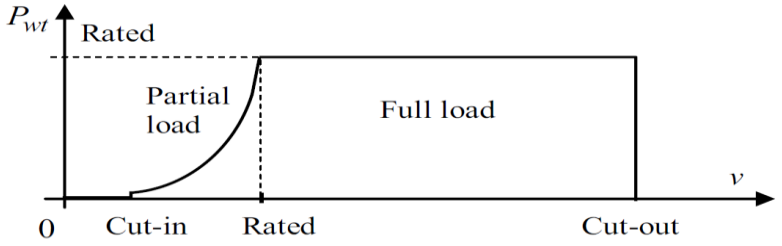
تُزوَّد العنفة بنظام تحكم كامل، يقوم بوظائف المراقبة والتشغيل والحماية. كما أن العنفة مزودة بأنظمة مساعدة كنظام الهيدروليك ونظام التبريد.

3.3.3 كيفية توليد الطاقة الكهربائية [16]:

تتلخص فكرة إنتاج الطاقة الكهربائية من العنفات الريحية على النحو التالي:

تعمل الطاقة الحركية للرياح على إدارة الريش المثبتة على صُرَّة Hub والتي ترتكز على محور الدوران الرئيسي الموصول بعلبة السرعة Gearbox التي تتولى مهمة رفع سرعة الدوران. ثم تنتقل الحركة إلى محور الدوران السريع High Speed Shaft فيقطع بدورانه مجال مغناطيسي داخل المولد، مما يؤدي إلى توليد الكهرباء. إذا زادت سرعة الرياح فإن الفرامل Brakes تمنع الريش من الدوران خوفاً من أن يؤدي دورانها بسرعة عالية إلى تحطمها، وتكسير الأجزاء الدّوارة. وتعد سرعة الرياح عالية إذا تجاوزت 25 متر/ثانية. لضمان توجيه ريش العنفات نحو اتجاه الريح، يوجد نظام توجيه خاص بالعنفة يعمل على توجيه العنفة في اتجاه الرياح، يمين و يسار.

تولد العنفة الريحية الكهرباء إذا زادت سرعة الرياح عن السرعة الدنيا التي تُعرَّف بسرعة القطع الصغرى V_{IN}، ويتزايد إنتاج الطاقة الكهربائية مع ازدياد سرعة الرياح، حتى تصل إلى السرعة الاسمية V_R، تكون عندها الاستطاعة المولدة مساوية للاستطاعة الاسمية للعنفة الريحية وتمثل أيضاً الاستطاعة العظمى. تستمر العنفة بإنتاج الطاقة الكهربائية مادامت سرعة الرياح دون السرعة القصوى V_O ، ويتم إيقاف العنفة الريحية متى تجاوزت سرعة الرياح السرعة القصوى. ويوضح الشكل (1) علاقة الطاقة الكهربائية المنتجة بسرعة الرياح.



الشكل (1): علاقة الطاقة الكهربائية المنتجة بسرعة الرياح.

تعطى الطاقة الريحية المتولدة عن العنفة الريحية **P** بدلالة السرعة وفق التالي:

$$\boldsymbol{P_{Wind} = \frac{1}{2} . \rho . \pi . r^2 . v^3} \qquad (0.3.3.3)$$

r: نصف قطر الدوار (m). $\boldsymbol{\rho}$: كثافة الهواء ($1.225\ kg/m^3$). $\boldsymbol{v}$: سرعة الرياح (m/s).

1.3.3.3 التحكم في العنفات الريحية:

يلعب التحكم بالعنفات الريحية دوراً هاماً ومحورياً في نظم العنفات الريحية الحديثة، لأنه يُحسِّن بشكل كبير من أدائها، باعتبارها تتعامل مع مصدر ريحي متغير بشكل كبير وتغيراته لا خطية وغير متنبأ بها. وأهم أنظمة التحكم في العنفات الريحية:

* **المتحكم الإشرافي:** يلعب التحكم الإشرافي دوراً رئيساً في الربط بين أنظمة التحكم المحلية ذات الدارة المغلقة، ويشرف على عمل النظام ككل، وهو المسؤول عن نقل العنفة الريحية من نمط تشغيل إلى آخر. يمكن أن تكون حالات التشغيل: التهيؤ Stand-by. الإقلاع Start-Up. إنتاج الطاقة Power Production. الإطفاء Shutdown. حالة الطوارئ Emergency. وعند الانتقال من حالة إلى أخرى، ينفذ المتحكم الإشرافي عدد من الإجراءات التحكمية على مراحل، ويتأكد المتحكم من إنجاز كل مرحلة بنجاح قبل الانتقال إلى المرحلة التالية، وفي حال فشل أية مرحلة، ينتقل المتحكم إلى نمط الإطفاء Shut-down Mode.

***المتحكمات ذات الدارة المغلقة Closed – Loop Controllers:** عبارة عن أنظمة جزئية مزودة ببرمجيات مهمتها ضبط حالة تشغيل العنفة الريحية ضمن حدود وخواص محددة. مثال على ذلك:

– التحكم في زاوية ميلان الريش: لتشغيل العنفة وفق منحني سرعة محدد أثناء بدء التشغيل أو الإطفاء.

– التحكم في عزم المولد: بهدف تنظيم السرعة الدورانية للعنفة ذات السرعة المتغيرة، والتحكم بمحركات نظام التوجيه Yaw لتخفيض خطأ التوجيه إلى الحد الأدنى.

***.نظام الحماية:** يعد نظام الحماية أساسياً في العنفات الريحية، ومهمته نقل العنفة الريحية في حال حدوث ظروف طارئة Emergency إلى حالة آمنة[17].

تتناسب الطاقة الميكانيكية المولدة من العنفة مع كثافة الهواء $\boldsymbol{\rho}$ والمكافئ الطاقي للدوار أو مكافئ الكفاءة (Coefficient or wind turbine) $\mathbf{Cp}$ ومكعب سرعة الرياح $\mathbf{V}$ ومع المساحة التي تمسحها الشفرات Swept Area $(\mathbf{A})$[14].

$$\mathbf{P_T = 0.5\, C_P(\lambda).\rho.A.V^3} \qquad (\mathbf{1.3.3.3})$$

تعتمد قيمة المكافئ الطاقي $\mathbf{C_P}$ على الخصائص الديناميكية للريش، وزاوية الريش، وسرعة الرياح، ويمكن التعبير عنها من خلال ما يعرف بـ Tip Speed Ratio ورمزه $\boldsymbol{\lambda}$ من خلال العلاقة:

$$\boldsymbol{\lambda} = \frac{\mathbf{RW_M}}{\mathbf{V}} \qquad (\mathbf{2.3.3.3})$$

حيث $\mathbf{R}$ طول الريشة و $\mathbf{W_M}$ السرعة الزاوية Angular Shaft Speed ويعطى عزم Torque العنفة الريحية وفق المعادلة:

$$\mathbf{T_T} = \frac{\mathbf{P_T}}{\mathbf{W_M}} = \frac{\mathbf{1}}{\mathbf{2}}\mathbf{C_T(\lambda).\rho.AV^2}$$
$$(\mathbf{3.3.3.3})$$

حيث أن

$$C_T(\lambda) = \frac{C_P(\lambda)}{\lambda}$$

$$(4.3.3.3)$$

وتعطى قيمة التيار الناتج عن العنفة الريحية على خرج المبدل DC/DC بالعلاقة:

$$I_W = \frac{\pi}{2\sqrt{3}}\sqrt{I_Q^2 + I_D^2}$$

$$(5.3.3.3)$$

حيث يمثل كل من I_Q و I_D قيمة التيار المتناوب وقيمة التيار المستمر، ويحسبان بالمعادلتين التاليتين:

$$I_Q = -\frac{R_S}{L}I_Q - W_E I_D + \frac{W_E \emptyset_M}{L} - \frac{\pi V_B I_Q}{3\sqrt{3}L\sqrt{I_Q^2+I_D^2}} \qquad (6.3.3.3)$$

$$I_D = -\frac{R_S}{L}I_D + W_E I_Q - \frac{\pi V_B I_D}{3\sqrt{3}L\sqrt{I_Q^2+I_D^2}} \qquad (7.3.3.3)$$

$$W_E = \frac{P}{2J}\left(T_T - \frac{3}{2}\frac{P}{2}\emptyset_M I_Q\right) \qquad (8.3.3.3)$$

أما الطاقة الكهربائية المولدة من العنفات الريحية فيمكن حسابها اعتماداً على النموذج الذي اعتمده يانغ [18] وفقاً للتالي:

$$P_W = \begin{cases} P_R \cdot \frac{V - V_{IN}}{V_R - V_{IN}} & (V_{IN} \le V \le V_R) \\ P_R & (V_R \le V \le V_O) \\ 0 & (V \le V_{IN} \text{ Or } V \ge V_O) \end{cases} \qquad (9.3.3.3)$$

4.3.3 ملاحقة نقطة التشغيل العظمى للعنفة الريحية[19]:

تعتمد طاقة الرياح بشكل رئيسي على الظروف المناخية وعلى الظروف الجغرافية، لذلك من الضروري بناء نظام توليد ريحي يكون قادر على توليد استطاعة عظمى في مختلف الظروف المناخية.

تستخدم هذه الأيام بشكل واسع عنفات ريحية متزامنة ذات مغناطيسية دائمة Permanent Magnet Synchronous Generator، ويشار إليها اختصاراً PMSG ، نظراً لمزاياها المتعددة والمتمثلة بأنها ذات موثوقية أفضل، ومتطلبات صيانة أقل وأكثر فعالية.

في الأماكن البعيدة عن الشبكة يتم عملياً استخدام عنفات ريحية ذات سرعة متغيرة، لجعل النظام أكثر استقراراً، ويتم عادةً إضافة نظام تخزين طاقة (بطاريات) مرافق للعنفة الريحية. إذا كانت الظروف المناخية وسرعة الرياح كافية، فإن العنفة الريحية تولد الطاقة اللازمة للحمل الكهربائي. إذا زادت الطاقة المولدة عن حاجة الحمل الكهربائي، تُخزَّن الطاقة الزائدة في نظام المدخرات. وفي حال أصبحت الطاقة المولدة من المولد الريحي غير كافية فإن البطاريات تقوم بتعويض النقص الحاصل في الطلب الكهربائي. تعطى الطاقة الحركية المتوفرة في الرياح بالعلاقة[19] :

$$\boldsymbol{P_{Wind} = \frac{1}{2}.\rho.\pi.r^2.v^3} \qquad \boldsymbol{(1.4.3.3)}$$

حيث أن:$\boldsymbol{\rho}$: كثافة الهواء. $\boldsymbol{v}$: سرعة الرياح (m/s). $\mathbf{r}$: نصف قطر الدوار أو طول الشيفرة (m).

لا يمكن استخراج كامل طاقة الرياح المتوفرة، بل يتم استخراج جزء فقط من هذه الطاقة وتحويله إلى طاقة ميكانيكية وفق المعادلة:

$$\boldsymbol{P_{Wind} = \frac{1}{2}.C_P.\rho.\pi.r^2.v^3} \qquad \boldsymbol{(2.4.3.3)}$$

يمثل $\boldsymbol{C_P}$ معامل الكفاءة، وتبلغ قيمته العظمى النظرية 0.59 وهو ما يعرف بحد بتز Bitz Limit، وتعتمد قيمة المعامل $\boldsymbol{C_P}$ على الخصائص الديناميكية للريش λ ، وزاوية الريش $\boldsymbol{\beta}$ وسرعة الرياح أي أنه تابع من الشكل :

$$\boldsymbol{C_P = f(\lambda, \beta)} \qquad \boldsymbol{(3.4.3.3)}$$

$$\boldsymbol{P_{Wind} = \frac{1}{2}.C_P.\rho.\pi.r^2.v^3} \qquad \boldsymbol{(4.4.3.3)}$$

إذا كانت $\mathbf{W_M}$ تعبر عن السرعة الزاوية لمحور الدوران Angular Shaft Speed فإننا نكتب:

$$\boldsymbol{\lambda = \frac{r \,.\, W_M}{v}} \qquad \mathbf{(5.4.3.3)}$$

. لنفرض أن سرعة الرياح ثابتة $\boldsymbol{v = const}$ عندها فإن λ تتغير متناسبة مع سرعة الدوران. القيمة العظمى لقيم $\boldsymbol{C_P}$ تتحقق عادةً عند قيم $\boldsymbol{\lambda}$ تتراوح بين 8 و 9 أي عندما تكون سرعة أخر نقطة في الريشة أسرع بثماني أو تسع مرات من سرعة الرياح. تُضبط زاوية انحراف الريش في العنفات الحديثة من خلال آلية تحكم خاصة.

إذا كان منحني $\boldsymbol{C_P - \lambda}$ معروف عند سرعة رياح معينة، فمن السهل حساب وإيجاد محني $\boldsymbol{C_P}$ تبعاً للعلاقة مع سرعة الدوران $\boldsymbol{\Omega}$ عند سرعة رياح معينة. وعند ضبط $\boldsymbol{\lambda}$ عند القيمة المثلى أي $\boldsymbol{\lambda = \lambda_{Opt}}$ فإن المكافئ الطاقي $\boldsymbol{C_P}$ يكون أعظم مايمكن

$$\boldsymbol{C_{PM} = C_P\,(\lambda_{Opt})} \qquad \mathbf{(6.4.3.3)}$$

وعندها يكون :

$$\boldsymbol{P_m^{Opt} = \frac{1}{2} . C_{PM} . \rho . \pi . r^2 . v^3} \qquad \mathbf{(7.4.3.3)}$$

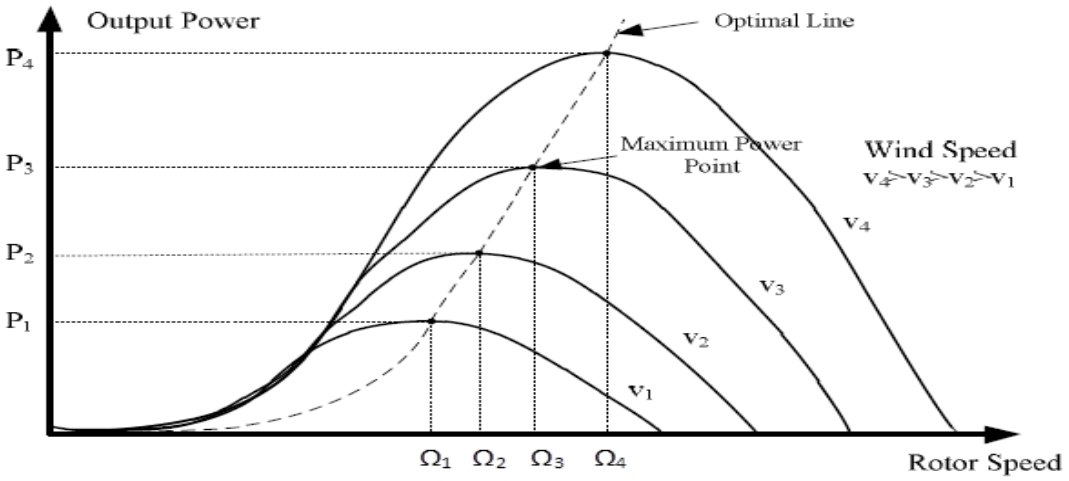
وتعطى سرعة الدوران المثلى بالعلاقة:

$$\boldsymbol{\Omega_{Opt} \frac{v.\lambda_{Opt}}{r}} \qquad \mathbf{(8.4.3.3)}$$

يبين الشكل (2) منحنيات الاستطاعة لعنفة ريحية عند سرعات رياح مختلفة [20]:

$$\boldsymbol{V_1 < V_2 < \cdots < V_n}$$

يبين المحور الأفقي سرعة دوران دوار العنفة الريحية ويبين المحور الشاقولي قيمة الاستطاعة المولدة من العنفة الريحية. لو ناقشنا أداء العنفة عند سرعة الرياح $\boldsymbol{V_1}$ ، نجد أن الاستطاعة المولدة تبدأ بالازدياد مع ازدياد قيمة $\boldsymbol{\Omega}$ حتى تصل إلى القيمة $\boldsymbol{\Omega_1}$ ، والتي تصبح عندها قيمة الطاقة المولدة هي $\mathbf{P_1}$، وبعد ذلك تعود قيمة الاستطاعة المولدة للتناقص بازدياد قيمة Ω .



الشكل (2): منحنيات الاستطاعة لعنفة ريحية عند سرعات رياح مختلفة

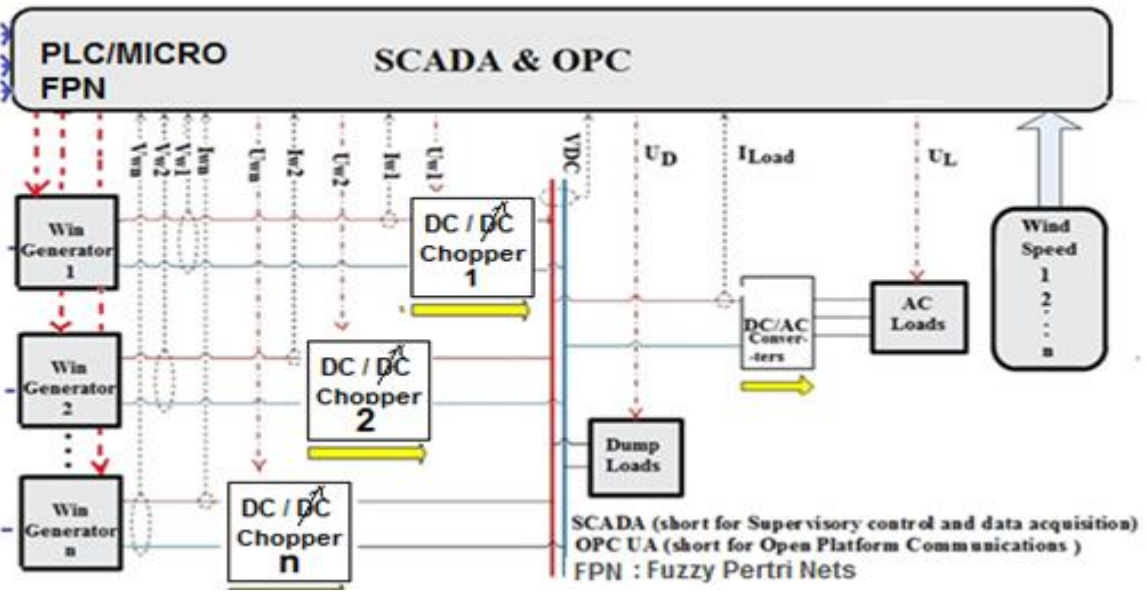
نطلق على سرعة الدوران $\boldsymbol{\Omega_1}$: السرعة المثالية لدوران العنفة الريحية لاستخراج الطاقة العظمى من الرياح التي تهب عند السرعة V_1، وبالمثل إذا أخذنا أداء العنفة الريحية عند سرعات رياح مختلفة $\boldsymbol{V_2, V_3, V_4, \ldots, V_n}$ نحصل على $\boldsymbol{\Omega_2, \Omega_3, \Omega_4, \ldots, \Omega_n}$ التي تمثل السرعات المثلى، التي تعطي أفضل طاقة مولدة من العنفة الريحية $\boldsymbol{P_2, P_3, P_4, \ldots, P_n}$، وبرسم المنحني الذي يمر بالنقاط العظمى للطاقة عند كل سرعة نحصل على المنحني الذي نطلق عليه اسم منحني الاستطاعة العظمى، وهو الخط المنقط في الشكل (2). بالعودة إلى الشكل السابق، نجد أن نقطة التشغيل العظمى والتي تكون عندها قيمة الاستطاعة المستفادة من الطاقة الحركية للرياح عظمى تتحقق عند:

$$\frac{\mathbf{dP}}{\mathbf{d\Omega}} = \mathbf{0} \qquad (\mathbf{9.4.3.3})$$

5.3.3 نمذجة ومحاكاة التحكم بمزرعة الرياح

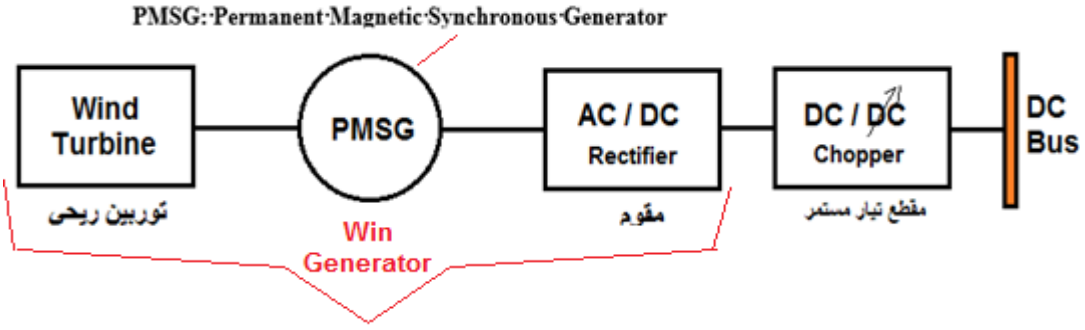
يبين الشكل (3) مكونات مزرعة الرياح والذي يتألف من عدة عنفات أو مولدات ريحية، بالإضافة إلى مبدلات(DC/DC (Chopper. يضاف حمل تخميد DC Dump مهمته

امتصاص الطاقة الزائدة على البار المشترك، بهدف ضمان عدم ارتفاع الجهد الكهربائي عن قيمته الاسمية. وتحصيل البيانات باستخدام شبكات بتري العائمة الملونة و بروتوكول منصة مفتوحة للاتصالات المتحدة البنية.



الشكل(3): مكونات مزرعة الرياح باستخدام SCADA-OPC وشبكات بيتري الضبابية

1.5.3.3 نمذجة العنفة الريحية: إن النموذج الذي سيتم استخدامه يعتمد على أن العنفة الريحية مربوطة إلى DC BUS عبر مقوم Rectifier مؤلف من جسر من الثنائيات وعن طريق مقطع تيار مستمر DC/DC Chopper كما هو موضح في. الشكل(4):



الشكل (4): نمذجة العنفة الريحية

هناك أسلوبين مختلفين لتصميم نظام تحكم لملاحقة نقطة التشغيل العظمى للعنفة الريحية. ففي حال كانت العنفة ذات ريش ثابتة، لا يمكن التحكم بزاوية ميلها، عندها يتم التحكم بمبدلات الاستطاعة Power Converter لتحقيق نقطة التشغيل العظمى، والأسلوب الثاني هو التحكم بزاوية ميل ريش الدوار بحيث تحافظ على سرعة زاوية Ω مثالية[19] . سنناقش هذين الأسلوبين بشيء من التفصيل في الفقرتين التاليتين:

2.5.3.3 ملاحقة الاستطاعة العظمى من خلال التحكم بالمبدلات:

يقوم مبدأ عمل خوارزمية التحكم على قياس سرعة الدوران الزاوية لمحور العنفة، وبناءً على منحني الخصائص المميزة يتم تحديد قيمة الاستطاعة المرجعية المثلى، ومقارنتها مع قيمة الاستطاعة الكهربائية المقاسة على الخرج، واستخدام إشارة الخطأ كدخل لدارة تحكم مهمتها تحديد قيمة دورة تشغيل D المقطع **DC/DC** ، الذي يحقق الاستجرار الأعظمي للطاقة من العنفة الريحية. من مساوئ هذه التقنية اعتمادها على معرفة منحني خصائص الطاقة الأمثلي. من مساوئ هذه الطريقة أيضاً عدم توفر منحني الخصائص بدرجة عالية من الدقة، وكذلك تغير منحني الخصائص مع مرور الوقت[3].

بالعودة إلى المعادلة $\frac{\mathbf{dP}}{\mathbf{d\Omega}} = \mathbf{0}$ التي تعبر عن نقطة التشغيل المثلى[19]، يمكن إعادة كتابتها وفقاً للتالي:

$$\frac{\mathbf{dP}}{\mathbf{d\Omega}} = \frac{\mathbf{dP}}{\mathbf{dD}} . \frac{\mathbf{dD}}{\mathbf{dV_{wG}}} . \frac{\mathbf{dV_{wG}}}{\mathbf{d\Omega_e}} . \frac{\mathbf{d\Omega_e}}{\mathbf{d\Omega}} = \mathbf{0} \qquad \mathbf{(1.5.3.3)}$$

حيث أن **D** : دور تشغيل المبدل. $\mathbf{V_{wG}}$: جهد خرج المبدل. $\mathbf{\Omega_e}$: السرعة الزاوية الكهربائية للمولد.

لنأخذ حالة كون المبدل من النمط الخافض للجهد في هذه الحالة فإن :

$$\mathbf{D} = \frac{\boldsymbol{V_o}}{\boldsymbol{V_{wG}}}$$

$$\frac{dD}{dV_{wG}} = -\frac{1}{V_{wG}^2}.V_o \neq 0 \qquad (2.5.3.3)$$

وكذلك فإن السرعة الزاوية الكهربائية للمولد ترتبط بالسرعة الزاوية لمحور الدوران وفق العلاقة التالية على اعتبار أن $\mathcal{P}$ يمثل عدد أزواج الأقطاب في المولد:

$$\Omega_e = \mathcal{P}\ .\ \Omega \qquad (3.5.3.3)$$

$$\frac{d\Omega_e}{d\Omega} = \mathcal{P}\ > 0 \qquad (4.5.3.3)$$

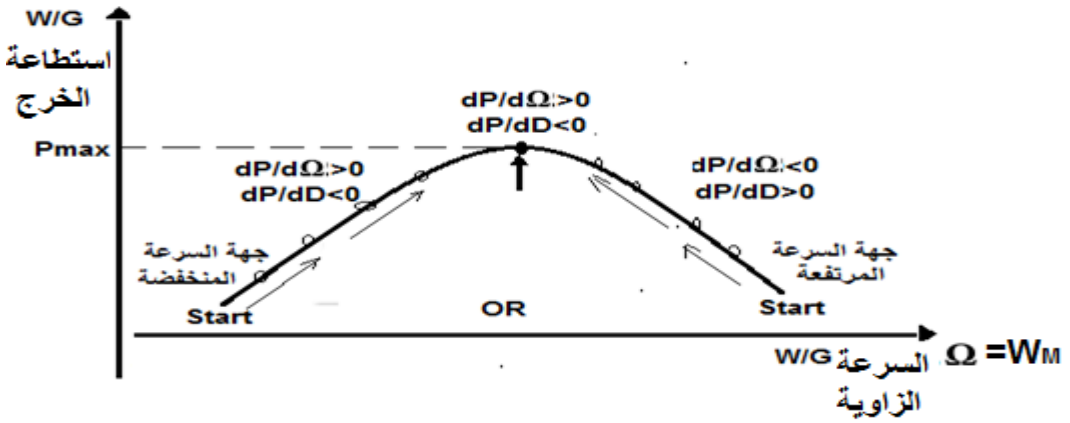
يتناسب جهد خرج المبدل مع جهد الطور للمولدة وبناءً على منحنيات العزم الكهربائي المرتبطة بجهد الطور للمولدة يمكن أن نكتب:

$$\frac{dV_{ph}}{d\Omega_e} > 0 \qquad (5.5.3.3)$$

$$\frac{dV_{wG}}{d\Omega_e} > 0 \qquad (6.5.3.3)$$

وبالعودة إلى المعادلة الأساسية نجد أن:

$$\frac{dP}{d\Omega} = 0 \quad \Leftrightarrow \quad \frac{dP}{dD} = 0 \qquad (7.5.3.3)$$



الشكل (5): منحني يوضح آلية تعقب الاستطاعة العظمى

يبين الشكل (5) توضيحاً لعملية تعقب نقطة التشغيل العظمى. حيث أنه في حال كانت قيمة سرعة الدوران في الجانب ذو السرعة المنخفضة Low Speed Side، يتم تخفيض قيمة دور التشغيل للمبدل، بحيث تتحقق زيادة قيمة سرعة الدوران، أما إذا كانت

نقطة التشغيل في الجانب الأيمن عن نقطة التشغيل العظمى، أي في الجانب ذو السرعة المرتفعة High Speed Side ، فإننا نقوم بزيادة قيمة دور التشغيل بحيث يتم تخفيض سرعة الدوران وإزاحتها باتجاه السرعة المثالية. يبين الشكل (6) مخطط خوارزمية عمل المستخدمة لتعقب نقطة التشغيل عند الاستطاعة العظمى.

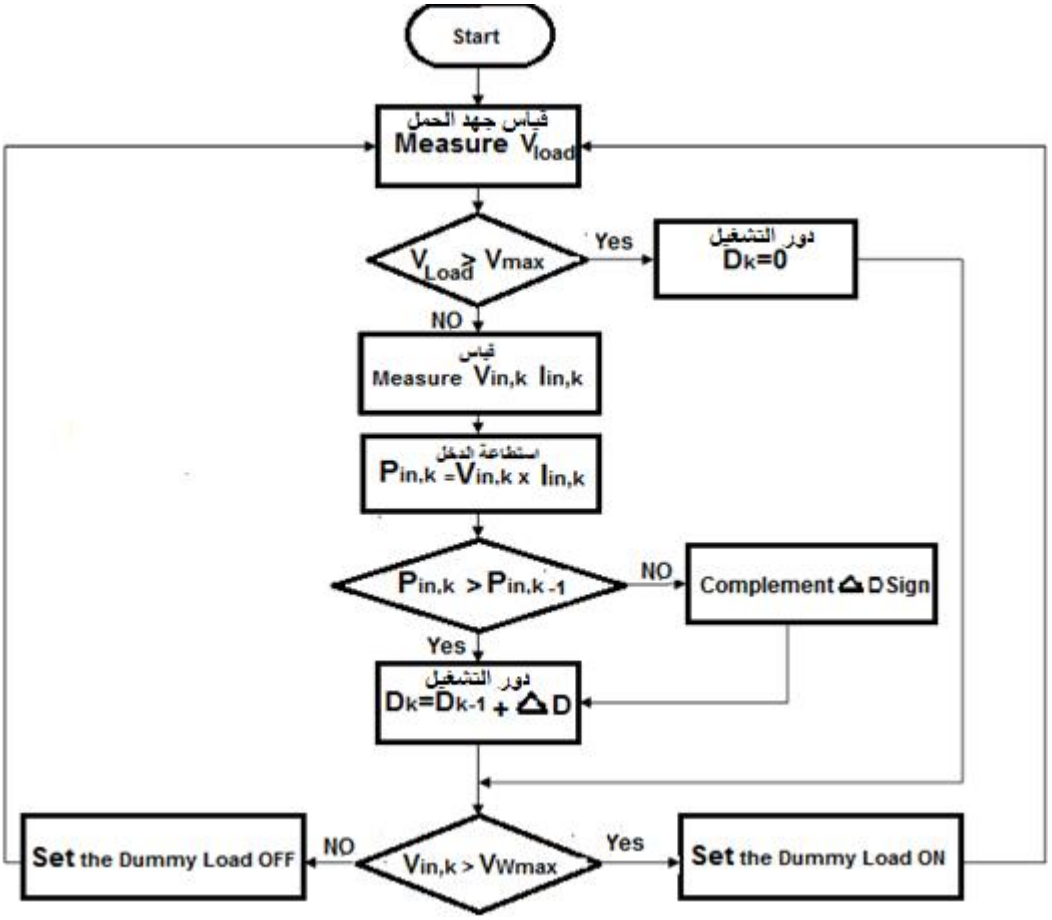
حيث أنه تم استخدام العلاقة التالية لتحديد قيمة دور التشغيلD :

$$\mathbf{D_k} = \mathbf{D_{k-1}} + \Delta\mathbf{D_{k-1}} \qquad \mathbf{(8.5.3.3)}$$

$$\Delta\mathbf{D_{k-1}} = \mathbf{C}\,.\,\boldsymbol{sign}(\Delta\mathbf{D_{k-2}}).\boldsymbol{sign}(\boldsymbol{P_{in,k-1}} - \boldsymbol{P_{in,k-2}})$$

حيث أن $\mathbf{C}$ ثابت يحدد سرعة ودقة تحقيق خوارزمية الأمثلة و التابع $\boldsymbol{sign}$:

$$\boldsymbol{sign}(\mathbf{x}) = \begin{cases} \mathbf{1}, & \boldsymbol{x} \geq \mathbf{0} \\ \mathbf{-1}, & \boldsymbol{x} < \mathbf{0} \end{cases} \qquad \mathbf{(9.5.3.3)}$$

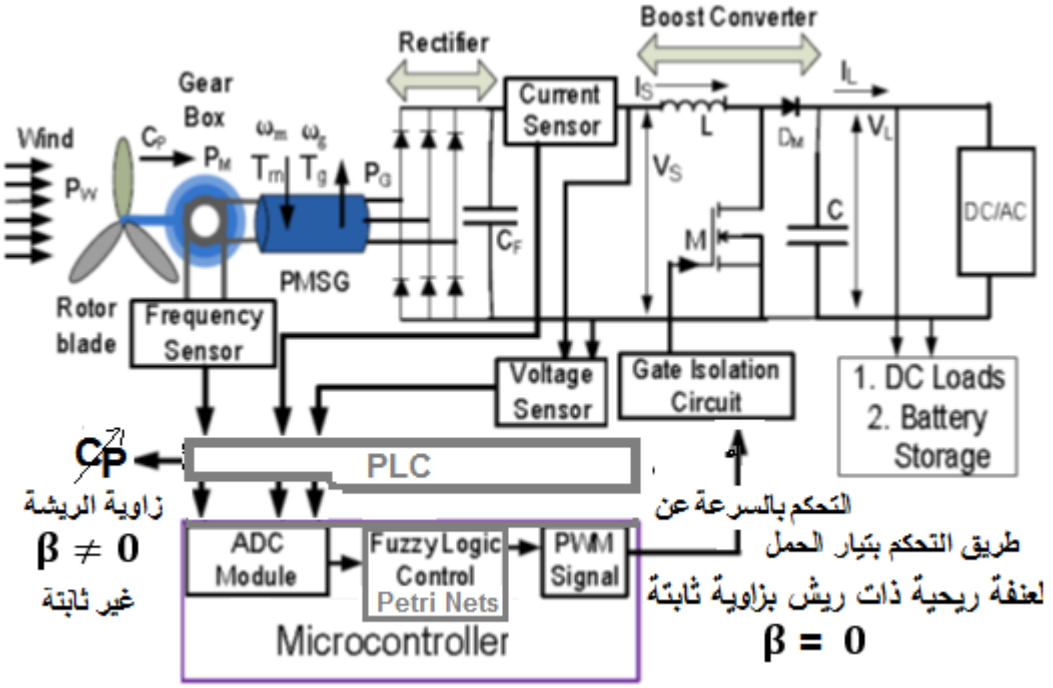


الشكل (6): خوارزمية محاكاة تعقب الاستطاعة العظمى[21]

سنناقش الآن أحد أساليب التحكم لضمان ملاحقة نقطة التشغيل العظمى لعنفة ريحية ذات ريش بزاوية ثابتة. يبين الشكل (7): مخطط دارة التحكم، حيث نلاحظ وجود كل من الحساسات: حساس التردد **Frequency Sensor** لقراءة السرعة الزاوية، وحساس تيار **Current Sensor** لقياس تيار الخرج للمقوم **Rectifier**، وحساس جهد لقياس جهد خرج المبدل.

كما أوضحنا سابقاً أنه للحصول على الطاقة العظمى من العنفة الريحية لابد من التحكم وضبط سرعة دوران العنفة الريحية بناءً على سرعة الرياح. ونظراً لكون الدوار غير

متحكم به نلجأ للتحكم بالعزم، حيث أنه من خلال التحكم بالعزم يمكن تغيير سرعة دوران العنفة الريحية وتشغيلها عند السرعة المثالية. وطالما أن العزم متناسب مع تيار الحمل على خرج المولدة أي يمكن من خلال التحكم بتيار الحمل على خرج المولدة أن نتحكم بسرعة دوران العنفة الريحية.



الشكل (7): ملاحقة الاستطاعة العظمى باستخدام التحكم العائم بزاوية ثابتة وغير ثابتة[21]

يقوم مبدأ عمل دارة الشكل (7) على قراءة سرعة دوران الدوار Ω ومن خلال منحني مميزة العزم – سرعة الدوران، يمكن الحصول على قيمة العزم $\mathbf{T_G}$ ، وتتم قراءة قيمة جهد خرج المبدل $\mathbf{V_d}$ ، ومنه نحسب قيمة التيار المرجعي وفق العلاقة والمرجع [21]:

$$\mathbf{I_{Ref}} = \frac{\mathbf{T_G} \cdot \Omega}{\mathbf{V_d}} \qquad \mathbf{(10.5.3.3)}$$

وبمقارنة قيمة تيار خرج المبدل المقاسة $\mathbf{I_d}$ مع قيمة التيار المرجعي $\mathbf{I_{Ref}}$ نحصل على إشارة الخطأ E التي تمثل دخل المتحكم:

$$\mathbf{E = I_{Ref} - I_d} \qquad \mathbf{(11.5.3.3)}$$

بناءً على إشارة الخطأ وبناءً على المتحكم المستخدم، نحصل على إشارة خرج تحدد قيمة دور التشغيل D الخاصة بالتحكم بتشغيل المبدل، للتحكم بزيادة أو إنقاص جهد التشغيل.

3.5.3.3 ملاحقة الاستطاعة العظمى من خلال التحكم بزاوية ميل الريش:

ناقشنا في الفقرة السابقة آلية ملاحقة نقطة التشغيل العظمى لعنفة ريحية ذات ريش ثابتة غير متحكم بميل الريش، والتي يطلق عليها Fixed-Pitch Variable Speed Wind Turbine، أي أن زاوية ميل ريش الدوار تبقى ثابتة $\boldsymbol{\beta = 0}$. وسنستعرض الآن آليةً أخرى، تقوم على مبدأ تنظيم سرعة دوران الدوار Rotor Speed على السرعة المثلى من خلال التحكم بزاوية ميل الريش $\boldsymbol{\beta \neq 0}$. في نظام التحكم بالريش، يتم قياس قيمة طاقة خرج نظام العنفة الريحية، فإذا زاد عن حدٍ معين (قيمة مرجعية) فإن نظام التحكم يزيد من زاوية ميل الريش، بحيث تقل مواجهة الريش للرياح. وعند انخفاض قيمة استطاعة خرج العنفة عن القيمة الإسمية، يتولى نظام التحكم تحقيق زاوية مثلى بحيث نحصل على سرعة الدوار المثلى التي تعطي أعظم استطاعة. لدينا هنا نوعان من العنفات الريحية: عنفات ريحية ثابتة السرعة متحكم بزاوية ريشها Variable-Pitch Fixed Speed Wind Turbine أو متغيرة السرعة متحكم بزاوية ريشها Variable-Pitch Variable Speed Wind Turbine.

بالعودة إلى علاقة المكافئ الطاقي $\mathbf{C_P = C_P(\lambda, \beta)}$ ، نجد أنه في هذه الحالة أن $\mathbf{C_P}$ ترتبط بشكل كبير بالزاوية $\boldsymbol{\beta}$ ، وتعتمد قيمة هذا المكافئ $\boldsymbol{C_P}$ على الخصائص الديناميكية للريش $\boldsymbol{\lambda}$ ، وزاوية الريش $\boldsymbol{\beta}$ وسرعة الرياح ويعطى وفقاً للمعادلة التالية[3]:

$$\boldsymbol{C_P = C_P(\lambda, \beta) = C_1 \cdot (C_2\lambda_i - C_3\beta - C_4) \cdot e^{-C_5\lambda_i} + C_6\lambda} \qquad \mathbf{(12.5.3.3)}$$

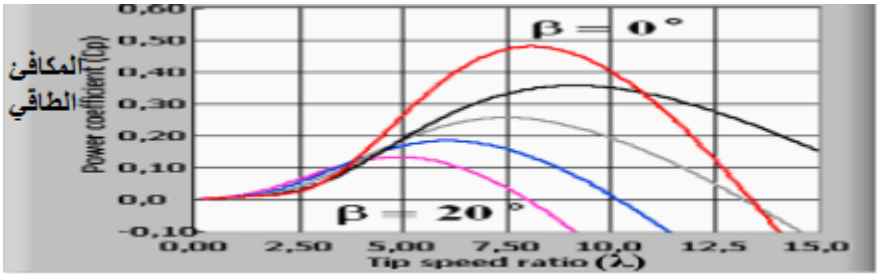
حيث أن :

$$\lambda_i = \frac{1}{\lambda + 0.08 \cdot \beta} - \frac{0.035}{\beta^3 + 1} \qquad (13.5.3.3)$$

إذا أخذنا القيم التالية :

$$C_1 = 0.5175,\ C_2 = 116, C_3 = 0.4, C_4 = 5, C_5 = 21, C_6 = 0.0068$$

نحصل باستخدام **Lab VIEW** على الشكل (8):



الشكل (8): مخطط يوضح العلاقة $C_P = C_P(\lambda, \beta)$

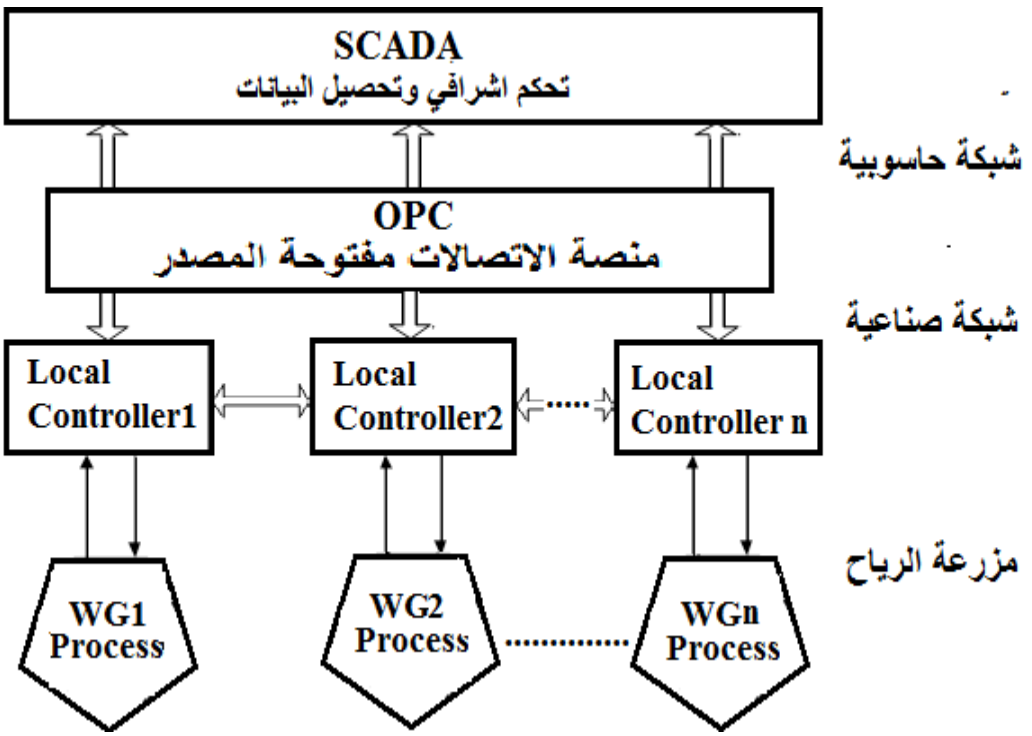
نلاحظ أن المكافئ الطاقي C_P يتعلق بقيم λ (Tip Speed Ratio) وقيم زاوية الريشة β . والطاقة الكهربائية المولدة من العنفات الريحية تزداد عنما يزداد المكافئ الطاقي C_P كما في المعادلة $(1.3.3.3)$ ولكن من أجل Cp(λ, β) ومن أجل قيم صغيرة لزاوية الريشة وقيم محددة لλ .

6.3.3 دور SCADA :

يستفيد المتحكم الإشرافي وتحصيل البيانات (SCADA) من المعطيات المتوفرة، لوصف السلوك الحالي للنظام، وتعديل المتحكمات المحلية، للوصول إلى المواصفات المطلوبة، يعمل المتحكم الإشرافي على تحصيل المعلومات من النظم الجزئية، ومكاملة هذه المعلومات ومعالجتها للوصول لعملية اتخاذ القرار الذي يسهم في تحسين الأداء ويؤدي إلى نوع من الاستقرار.

يوجد عدة متحكمات فرعية يرتبط كل منها بعدد من العناصر الحقلية يشرف عليها ويتحكم بها، وترتبط جميع المتحكمات الفرعية بمتحكم مركزي، يتولى التنسيق والإشراف على أداء المتحكمات الفرعية. تدعى هذه البنية بالتحكم الهرمي. من أهم مزايا هذه البنية:

خفض مشاكل تطوير البرمجيات، والسماح بالعمل بمعايير زمنية مختلفة، وأزمنة استجابة أسرع. ومن مساوئها زيادة حجم الاتصالات، وصعوبة إجراء تعديلات مستقبلية بين المتحكم المركزي والمتحكمات الفرعية. وإمكانية التخاطب بين المتحكمات الفرعية كما يبينها الشكل (10) وتتمتع باستقلالية ذاتية.



الشكل (10): بنية تحكمية تراتبية هرمية المعتمدة في هذا البحث

1.6.3.3 التحكم الهرمي: يمكن معالجة مشكلة التحكم بالنظم المعقدة من خلال تجزئة عملية_التحكم إلى عدة مستويات، لكل مستوى منها أغراض تحكمية معينة، يتم تحقيقها من خلال متحكمات مختلفة مهمتها المحافظة على تحقيق الأغراض التحكمية المناطة بها ضمن الشروط النظامية[22 ,3].

يختلف عدد المستويات في البنية التراتبية الهرمية تبعاً لدرجة تعقيد النظام وحجمه، والوظائف التحكمية التي ينفذها. وتختلف متطلبات الزمن لتنفيذ المهمة من مستوى لآخر،

ففي المستويات الدنيا تكون الاستجابة الزمنية من مرتبة أجزاء الثانية، في حين أنه في المستويات الأعلى تكون من مرتبة الدقائق، وفي المستويات العليا في بعض الأنظمة الكبيرة إلى مرتبة الساعات والأيام.

نظام SCADA يتضمن نظام التحكم والحصول على البيانات وجميع المكونات المطلوبة لجمع البيانات والمراقبة عن بُعد والتحكم في مزارع الرياح. المرونة التي يوفرها نظام SCADA تجعل من الممكن تلبية أصعب متطلبات مشغلي شبكة الطاقة ومزارع الرياح. ويشكل الخادم SERVER الوحدة المركزية لنظام SCADA. ويرتبط هذا بكل توربينات الرياح عبر شبكة الألياف الضوئية. تقوم بالعديد من المهام المتعلقة بالاتصال وتسجيل البيانات ومراقبة مزرعة الرياح. وتتوفر العديد من واجهات اتصال متنوعة لتبادل البيانات مع نظام SCADA لمزرعة الرياح.

يدعم بروتوكول(SCADA –OPC) المعتمد في بحثنا، واجهة طرفية بعيدة والقائمة على الأجهزة (RTU-I) التي تستند إلى Ethernet-TCP و RTU - DNP3. ونظام الطقس METEO متاح في SCADA لدمج معلومات الأرصاد الجوية من مصادر خارجية . لذلك يسمح نظام SCADA للمشغل بتحديد التعديلات الضرورية أو الإجراءات التصحيحية التي يجب اتخاذها بمراقبة الأداء لكل عملية ومراقبة العواصف الرعدية القريبة لتنبيه الفنيين إلى المخاطر المحتملة في المواقع. يحتوي كل توربين رياح على صندوق تحكم يحتوي على PLC ومحول طاقة ولوحات تحكم ووحدة إدخال/إخراج. من خلال استشعار اتجاه الرياح، فإن نظام التحكم قادر على التحكم في نظام التوجيه لتوجيه التوربين بأكمله في الاتجاه الأمثل ولإنتاج الاستطاعة القصوى والحصول على نقطة التشغيل العظمى. جميع التوربينات متصلة بشبكة محلية، وصندوق التحكم لكل توربين متصل بواسطة وصلة إيثرنت بقاعدة البرج، وهو نفسه متصل بالشبكة المحلية بواسطة وصلة ألياف بصرية. يتم توصيل الشبكة المحلية بمحطة تحكم عن بعد، تدير وتجمع البيانات،

وتعديل معاملات التوربين، وتولد إنذارات ذكية، وتمكن من استكشاف الأخطاء وإصلاحها ووظائف الإبلاغ من خلال مركز التحكم والمعالجة. لذلك نظام SCADA يعمل كمركز عصبي لمزارع الرياح ويربط التوربينات المختلفة والمحطات الفرعية ومحطات الطقس ورادار الكشف عن الطيور بغرفة التحكم المركزية. الميزة الرئيسة لنظام SCADA هي أنه غير مرتبط بأي مورد لأجهزة التحكم المنطقية القابلة للبرمجة ، مما يسمح باستخدامه مع أي نوع من التوربينات باستخدام بروتوكولOPC.

تجمع مزرعة الرياح، الممثلة بعدد من الوحدات الطرفية البعيدة (RTUs) ، البيانات المحلية وترسلها إلى المحطة الرئيسة، حيث تقوم بعرض البيانات المحصلة وعمليات التحكم عن البعيد. وجود البيانات ودقة التوقيت تجعل عمليات سكادا ذات كفاءة وموثوقية عالية والأهم من ذلك سلامة العنفات الريحية، كل هذا ينتج تكاليف عمليات أقل على المدى الطويل مقارنة بالأنظمة غير المؤتمتة.[23]

- **تنظيم المحطات والـ RTUs** : الـ RTU (والتي يشار إليها أحياناً بوحدات القياس البعيدة) هي وحدة تحصيل بيانات وتحكم مستقلة قائمة بحد ذاتها، عادة مبينة على أساس المعالجات الصغرية Microcontrollers أو المتحكمات المنطقية القابلة للبرمجة PLC، تقوم بمراقبة والتحكم بالأجهزة المختلفة في المحطات البعيدة، مهمتها الأساسية هي نقل هذه البيانات الناتجة عن القياس والتحكم إلى المحطة الرئيسة. فضلاً على قدرتها على التواصل مع المحطة الرئيسة فإنها أحياناً قادرة على التواصل مع بعضها البعض، فيمكن لوحدة RTU أن تعمل كمحطة ترحيل (Store & Forward Relay Station) لوحدة RTU أخرى قد لا تكون قابلة للولوج من المحطة الرئيسة[1].
- **نظام الاتصالات** : نظام الاتصال مهم جداً لتأمين الأداة التي يمكن بها نقل البيانات بين المحطة الرئيسة والـ RTUs، ويكون الوسيط هو إما كابل أو التلفون أو الراديو.

إن استخدام الكابلات المحورية جيد لمصنع محلي، وليس عملي للأنظمة التي تغطي مساحات واسعة بسبب الكلفة الاقتصادية العالية للكابلات. ويمكن استخدام الخط الهاتفي

لكونه اكثر اقتصادي عند تغطية مساحات أوسع بقليل، ويصبح مكلفاً عند الحاجة للعديد من الخطوط مع كل محطة طرفية للعنفات الريحية، لذلك برزت الحاجة لاستخدام نوع أفضل وهو الإشارات الراديوية الاقتصادية جداً.

تاريخياً كانت شبكات السكادا هي شبكات مخصصة، ولكن مع الانتشار الواسع لشبكات الـ LAN والـ WAN، أصبح هناك إمكانية لدمج شبكات السكادا مع الشبكات الحاسوبية واسعة النطاق وبرز مفهوم تحكم واسع النطاق. إن نظم السكادا هي النظم المستخدمة لتحصيل المعطيات والتحكم بالنظم واسعة النطاق، فهي تكامل بين أنظمة تحصيل المعطيات وأنظمة إرسال المعطيات أوالأوامر وبرمجيات التخاطب بين الانسان والآلة (HMI) لإنتاج نظام تحكم ومراقبة مركزي يسمح للمشغل بمراقبة النظام والتحكم به كاملاً في الزمن الحقيقي من مركز رئيسي، وذلك عبر بنية هرمية موزّعة مكونة من جزء عتادي وجزئ برمجي، حيث يتضمن العتاد مخدم السكادا الرئيسي SCADA Server أو ما يسمى بالوحدة الطرفية الرئيسة MTU الذي بدوره يتصل مع وحدات التحكم الطرفية RTU عبر شبكة اتصال واسعة النطاق متزامنة من خلال الأقمار الصناعية GPS وتعتمد على النقل الضوئي (غالباً) أو النقل اللاسلكي أو الكابلات (هاتف، مؤجر، كهرباء) ...الخ، وتتصل وحدات التحكم الطرفية مع الأجهزة الحقلية الأخرى IEDs المتمثلة بالحساسات والمشغلات. يمكن ذكر بعض برتوكولات الاتصال المستخدمة في نظام السكادا وهي: بروتوكول Modbus، بروتوكولCAN، بروتوكولPROFI Bus، بروتوكول ASI Bus، بروتوكول Ethernet، بروتوكول DNP3 و بروتوكول OPC.

من الأمثلة على نظم التحكم، هناك نظام التحكم بالشبكة الكهربائية وشبكة مياه الشرب وشبكة مياه الصرف الصحي وشبكة السكك الحديدية.

- **DNP3**: بروتوكول الاتصال الموزع هو بروتوكول يمكننا من تحقيق الاتصال بين عدة محطات "سيد" multi masters ومجموعة من وحدات Remote Telemetry Units (RTUs) وأيضاً أجهزة أخرى الكترونية تعرف بـ Intelligent Electronic Devices (IDEs)، تمّ تطويره لتحقيق الاتصال بين النظم للمحطات الخاصة بتوليد الطاقة الكهربائية

وأيضا ضمن حقول النفط والغاز ومؤسسات المياه والمجال الأمني. صمم هذا البروتوكول خصيصاً لتطبيقات الـ SCADA (Supervisory Control And Data Acquisition). أهم مزايا هذا البروتوكول هو أنه بروتوكول مفتوح وقد اعتمد من قبل العديد من الشركات المصنعة للمعدات ويتميز بوجود توافق بين الأجهزة من مختلف الصانعين حيث تم اعتماده عبر عدد كبير من أنظمة RTUs و SCADA والعديد من الأجهزة الالكترونية المختلفة. صمّم هذا البروتوكول للاتصالات الموثوقة في أوساط إرسال سيّئة وللتغلّب على التشويه، وهو بروتوكول مؤلف من 3 طبقات: الطبقة السابعة (تطبيق) والطبقة الثانية (بيانات ترتبط) والطبقة الفيزيائية Physical layer. تقسيم الرسالة المرسلة ببرتوكول DNP3 إلى مجموعة من الأطر frames لتوفير التحكم الأمثل وسهولة كشف الخطأ عن طريق (CRCs) و يدعم رسائل البث العام. يمكن عنونة مايزيد عن 65000 جهاز على الوصلة الواحدة.[24]

- **[Open Platform Communication] : OPC**

أو [OLE (Object Linked Embedding) for Processing Control]

أي ربط النظم وتضمينها للتحكم بالعمليات. وهو برتوكول ومعيار اتصال البيانات الموحد والمدعوم من شركة ميكروسوفت. بدأ تطويره من عام 1990، معتمد من جميع شركات الأتمتة، مفتوح المصدر، مكتوب بلغة C++ ولغة VB. يمكن أن نمثل OPC بأنه طبقة "التجريد" "أي طبقة غير محسوسة " والتي تقع بين مصدر البيانات ووجهة البيانات، مما يتيح لهم تبادل البيانات دون معرفة أي شيء عن بعضهم البعض. أي يعمل بروتوكول OPC في الطبقة التي تفصل بين المتحكمات والتحكم الإشرافي. قائم على طبقة COM و DCOM من شركة مايكروسوفت يعتمد على بنية Server/Client. التعديل والتطوير سهل جداً، يَسمح بالاستفادة من مزايا كل الشركات، الصيانة ممكنة، التعقيد في النظام أقل وتكلفة بناء النظام أقل.

في بروتوكول OPC يمكن تبديل مصادر البيانات، والتبادل، أو التحديث دون الحاجة إلى تحديث برامج التشغيل الخاصة المستخدمة من قبل كل تطبيق (وجهة بيانات) المتصلة مع مصادر البيانات عبر مخدم OPC.

يملك OPC ثلاثة فئات من البيانات وهي :(OPC DA) وتستخدم لنقل البيانات في الوقت الحقيقي. (OPC HDA) وتستخدم لنقل البيانات التاريخية. (OPC A & E) وتستخدم لنقل المعلومات الانذارات المثيرة للقلق. يعد بروتوكول OPC ثنائي الاتجاه، هذا يعني أن خوادم OPC تستطيع القراءة او الكتابة من وإلى مصدر البيانات [22].

مخدم الـOPC: هو جزء من البروتوكول المسؤول عن تحقيق الاتصال بالمتحكمات وتحصيل البيانات منها أو التعديل عليها، ويقوم بتلبية جميع طلبات الزبائن OPC المتصلة معه.

يخاطب الـ OPC Server المتحكم المتصل معه وفق بروتوكول محدد مدعوم من قبل المتحكم، ومن ثم يقوم بجلب البيانات المطلوبة من المتحكم ويترجمها لمعيار الـ OPC، غالبا ما يكون الـ OPC Server من انتاج الشركة المصنعة للتجهيزات الصناعية (PLCs) ويمكن أيضاً أن يكون من انتاج شركات برمجية ربحية خاصة. ويمكن لـ OPC Server واحد أن يُخدّم أكثر من زبون بنفس الوقت.

يخزن الـOPC Server البيانات التي قام بجلبها من المتحكمات المتصلة معه في قاعدة بيانات خاصة به ويقوم بتحديث القيم المخزنة فيها بشكل دوري، قاعدة البيانات هذه قد تكون عبارة عن ملف Access أو أي نوع أخر من أنواع قواعد البيانات المعروفة. تقوم جميع الـ OPC Clients المتصلة مع المخدم بتحديث قيم عناصرها من قاعدة البيانات السابقة[25].

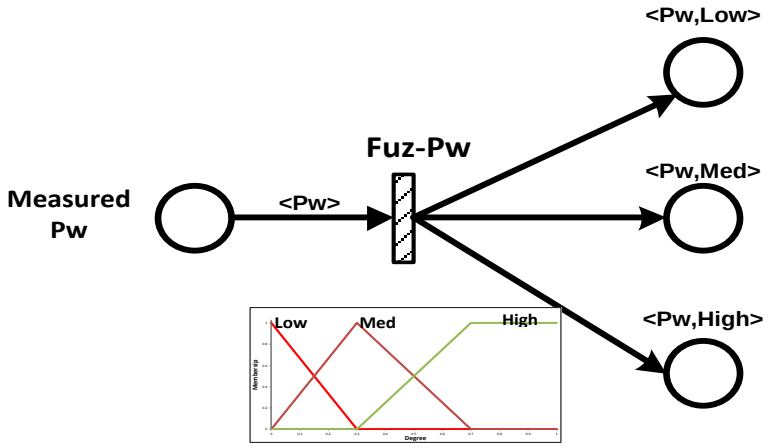
7.3.3 تصميم نموذج شبكة بتري عائمة لإدارة العنفة الريحية

في التحليل الوظيفي للمتحكم الإشرافي لنظام إدارة الطاقة في مزرعة الرياح، يتم نمذجة جزء من المتحكم من خلال شبكة بتري العائمة الخاصة بإدارة المولد الريحي، وفق نموذج الطبقات الخمس.

الطبقة الأولى : مرحلة التعويم

في عملية التعويم Fuzzification، يمثل دخل Measured Pw قياس قيمة الاستطاعة المولدة من العنفة الريحية، و يمثل العبور Fuz-Pw بتابع رياضي يحقق عملية التعويم الخاصة بحالة توليد الاستطاعة، وخرج العبور مرتبط بثلاثة أماكن خرج <Pw,Low> و < Pw,Med> <Pw,High>.

يتم عند قدح العبور، وبناءً على تابع الانتماء، حساب القيمة التي يجب إسنادها إلى كل مكان من أماكن الخرج الثلاثة. تمثل ΔP إشارة فرق الاستطاعة، وتتمثل في هذه الطبقة من خلال مكان دخل، وعبور Fuz- ΔP، وخرج العبور مرتبط بخمسة أماكن خرج <ΔP,NB> و<ΔP,NM> و<ΔP,Z> و<ΔP,PM> و <ΔP,PB>.



الشكل (11): جزء من شبكة بتري العائمة لتعويم القيمة Pw

الطبقة الثانية: مرحلة مضاعفة الأماكن

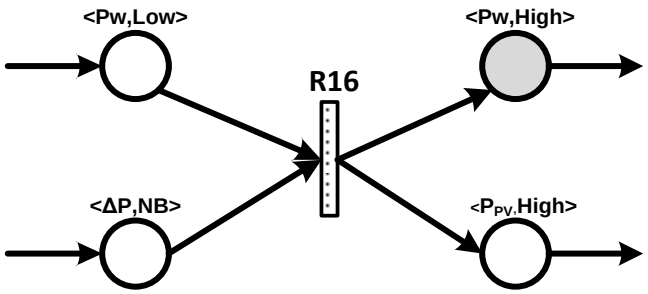
تمثل الطبقة الثانية طبقة العبورات المُضاعِفة، يرتبط كل مكان خرج من أماكن الخرج في الطبقة الأولى <Pw,Low> و <Pw,Med > و <Pw,High > بعبورٍ مُضاعِف يرتبط خرجه كون مرتبط بخمسة أماكن خرج، وعدد أماكن الخرج المرتبطة بكل عبور من العبورات الخمسة المرتبطة بالأماكن <ΔP,NB> و<ΔP,NM> و<ΔP,Z> و<ΔP,PM>

و <ΔP,PB> هو ثلاثة أماكن خرج. وظيفة العبور في هذه المرحلة نقل القيمة الموجودة في مكان الدخل إلى عدد أكبر من أماكن الخرج.

الطبقة الثالثة: تحقيق القواعد

تمثل الطبقة الثالثة طبقة إيجاد العلاقات Rules بين المتغيرات المختلفة. يمثل العبور في هذه الطبقة تابع Minimum يختار القيمة الصغرى المتواجدة في أماكن الدخل المرتبطة بهذا العبور، وإسناد هذه القيمة إلى مكاني الخرج المرتبطين به. يبين الشكل (12) جزء من شبكة بتري العائمة التي تمثل القاعدة التالية:

IF *ΔP* IS *NB* AND *Pw* IS *LOW* THEN *Pw_Ref* IS *High* ALSO *Ppv_Ref* IS *High*



الشكل (12): تمثيل القواعد في شبكة بتري العائمة

يوجد مكان دخل له الفرضية <Pw,Low> وتسند له قيمة تمثل قيمة تابع الانتماء لقيمة الاستطاعة المولدة من المولد الريحي $\mu_{Low}(Pw)$، وهي تمثل جزء الشرط IF *Pw* IS *LOW* . ومكان دخل له الفرضية <ΔP,NB> والذي يمثل قيمة تابع الانتماء لقيمة فرق الاستطاعة $\mu_{NB}(\Delta P)$ والتي تمثل جزء الشرط IF *ΔP* IS *NB* .

عند قدح العبور يتم اختيار القيمة الصغرى من مكاني الدخل Minimum ($\mu_{Low}(Pw)$, $\mu_{NB}(\Delta P)$) وإسناد خرج التابع إلى مكاني الخرج، الأول له الفرضية < Pw,High> والذي يرتبط بقيمة إشارة التحكم الخاصة بقيمة الاستطاعة المطلوبة من المولد

الريحي، ومكان الخرج الثاني له الفرضية <P_{PV},High>. يبين الجدول (1) تمثيل الطبقة الثالثة حيث يمثل العمود الأيسر العبورات والبالغ عددها 15 عبور{R16,R17,…,R30}، ويمثل العمود الثاني حصول الأحداث، ويمثل العمود الثالث الشروط المختلفة.

الجدول (1): توضيح تمثيل الطبقة الثالثة لشبكة بتري العائمة للمولد الريحي

Rule	Events		Condition	State P_{W_Ref}
R16	Pw is *Low*	ΔP is *NB*	C6 & C1	High
R17	Pw is *Low*	ΔP is *NM*	C6 & C2	High
R18	Pw is *Low*	ΔP is *Z*	C6 & C3	Low
R19	Pw is *Low*	ΔP is *PM*	C6 & C4	Low
R20	Pw is *Low*	ΔP is *PB*	C6 & C5	Low
R21	*Pw* is *Med*	ΔP is *NB*	C7 & C1	High
R22	*Pw* is *Med*	ΔP is *NM*	C7 & C2	High
R23	*Pw* is *Med*	ΔP is *Z*	C7 & C3	Med
R24	*Pw* is *Med*	ΔP is *PM*	C7 & C4	Low
R25	*Pw* is *Med*	ΔP is *PB*	C7 & C5	Low
R26	*Pw is High*	ΔP is *NB*	C8 & C1	High
R27	*Pw is High*	ΔP is *NM*	C8 & C2	High
R28	*Pw is High*	ΔP is *Z*	C8 & C3	High
R29	*Pw is High*	ΔP is *PM*	C8 & C4	Med
R30	*Pw is High*	ΔP is *PB*	C8 & C5	Low

الجدول (2): الشروط المختلفة الواردة في الجدول السابق

C1:	IF	ΔP	IS	*NB*	THEN ……
C2:	IF	ΔP	IS	*NM*	THEN ……
C3:	IF	ΔP	IS	*Z*	THEN ……
C4:	IF	ΔP	IS	*PM*	THEN ……
C5:	IF	ΔP	IS	*PB*	THEN ……
C6:	IF	*Pw*	IS	*Low*	THEN ……
C7:	IF	*Pw*	IS	*Med*	THEN ……
C8:	IF	*Pw*	IS	*High*	THEN ……

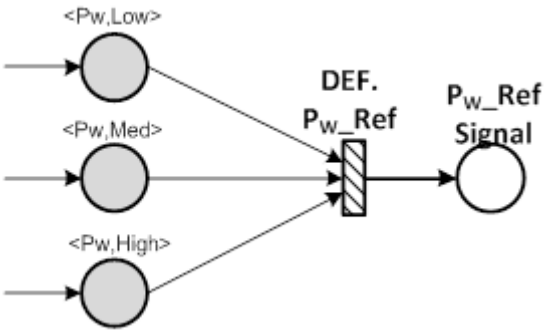
الطبقة الرابعة: طبقة العبورات التجميعية

يرتبط كل عبور بعدد من أماكن الدخل التي لها الفرضية نفسها NB أو NM أو Z أو PM أو PB. يمثل العبور في هذه الطبقة تابع Maximum ، وعند قدح العبور يتم اختيار القيمة العظمى من قيم أماكن الدخل المرتبطة به وإسناد هذه القيمة إلى مكان الخرج المرتبط به.

الطبقة الخامسة: طبقة فك التعويم

تمثل الطبقة الخامسة في شبكة بتري العائمة عملية فك التعويم Difuzzification كما هو موضح في الشكل (13)، يوجد في هذه الطبقة ثلاث أماكن دخل وعبور وحيد DEF Pw-Ref، ومكان خرج وحيد يمثل إشارة التحكم بطاقة العنفة Pw-Ref Signal . يمثل

العبور تابع رياضي يحقق عملية فك التعويم. يتم عند قدح العبور DEF. Pw-Ref وبناءً على تابع الانتماء لإشارة التحكم بطاقة العنفة يتم حساب إشارة التحكم اللازمة.



الشكل (13): طبقة فك التعويم في شبكة بتري العائمة

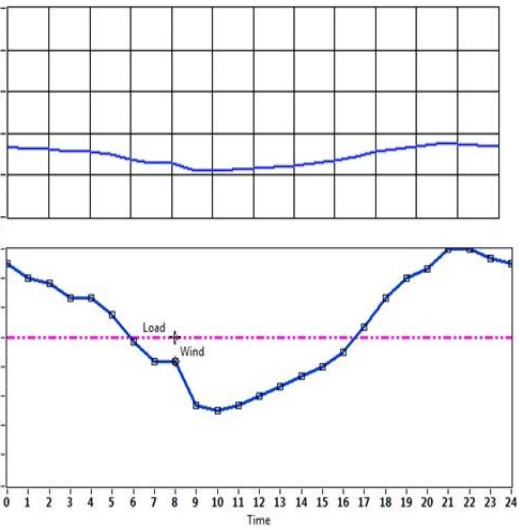
4.3 النتائج ومناقشتها

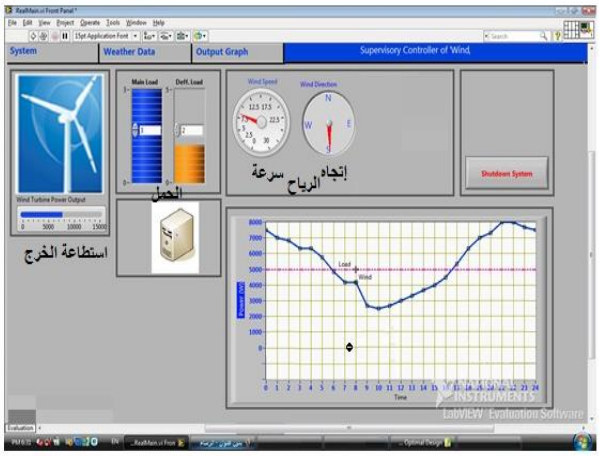
أنشأنا محاكة لعنفة ريحية باستخدام الحزمة البرمجية Lab VIEW واستخدمنا Fuzzy System Designer لصياغة المتحكم الإشرافي العائم والأداة CPN tools لإدارة العنفات الريحية.

- **محاكاة باستخدام الحزمة البرمجية Lab VIEW لملاحقة نقطة التشغيل العظمى للعنفة**

اختبرنا أداء النظام على عددٍ من حالات التشغيل المختلفة لثلاث عنفات ريحية وعند أحمال كهربائية مختلفة: حمل كهربائي منخفض 3KW واسمي 6KW وعالي 11KW.

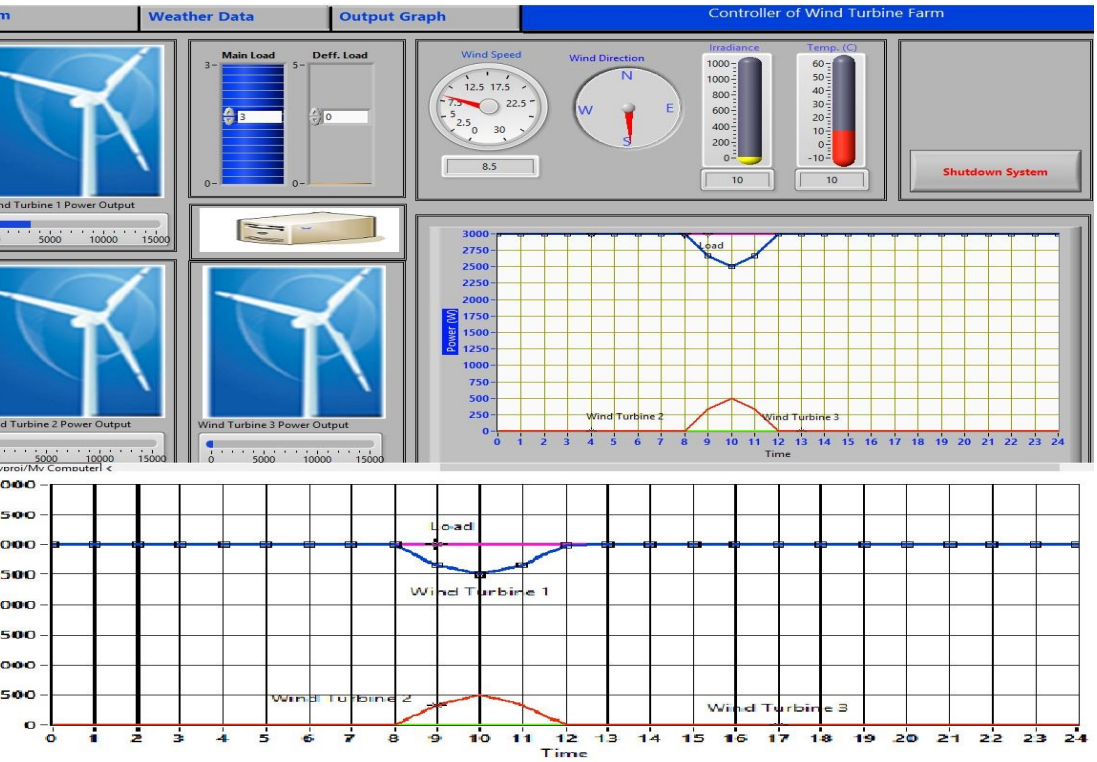
يبين الشكل(14) تغيرات الاستطاعة المنتجة بواسطة عنفة ريحية حسب سرعة الرياح وخلال 24 ساعة بالنسبة للحمل الكهربائي. علماً أن الاستطاعة الاسمية للعنفة هي 6000 واط.



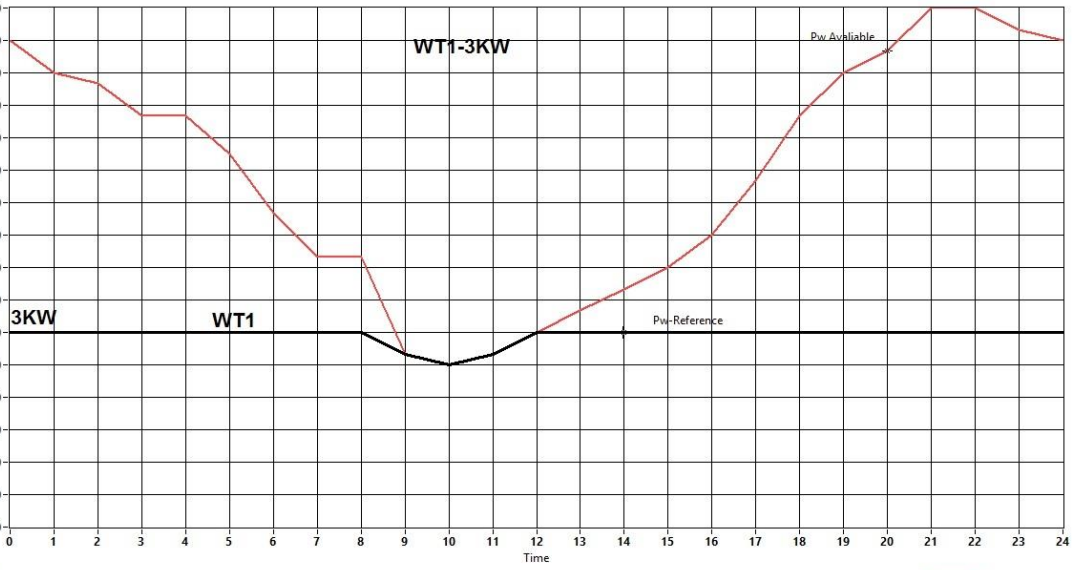


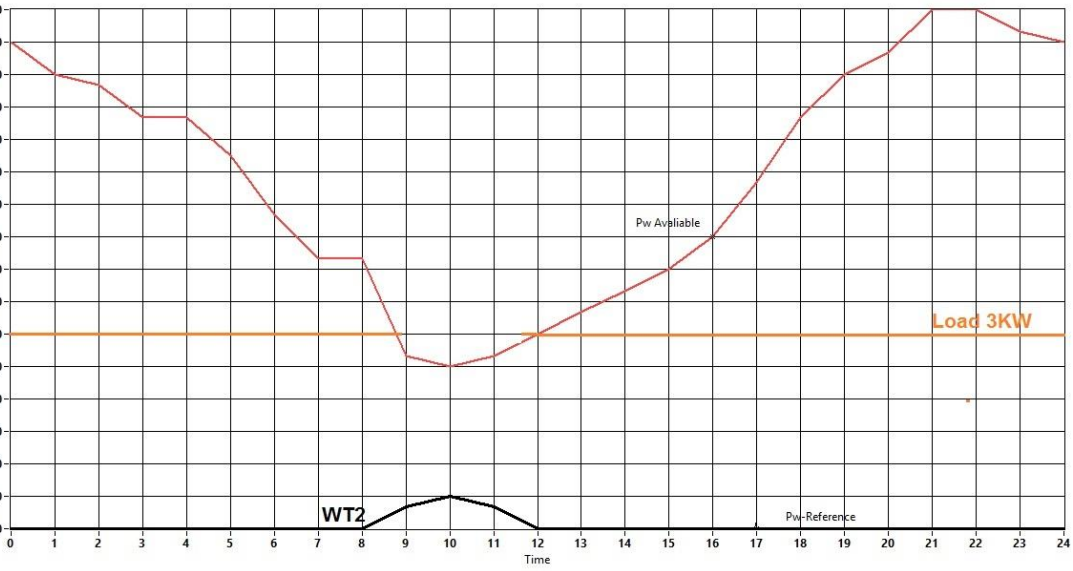
الشكل (14): الواجهة الرئيسة وتغير الاستطاعة للعنفة الواحدة WT حسب سرعة الرياح خلال 24 ساعة

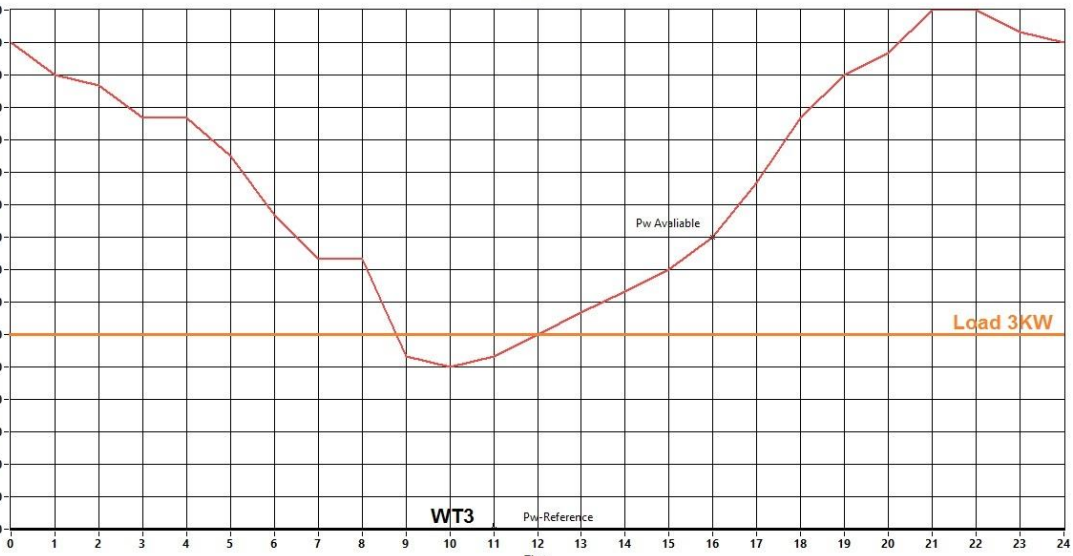
الاختبارات:



الشكل (15): الواجهة الرئيسة وتعويض الاستطاعة بواسطة عنفة واحدة WT


WT1-3KW
Pw Avaliable
3KW
WT1
Pw-Reference
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Time


Pw Avaliable
Load 3KW
WT2
Pw-Reference
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Time

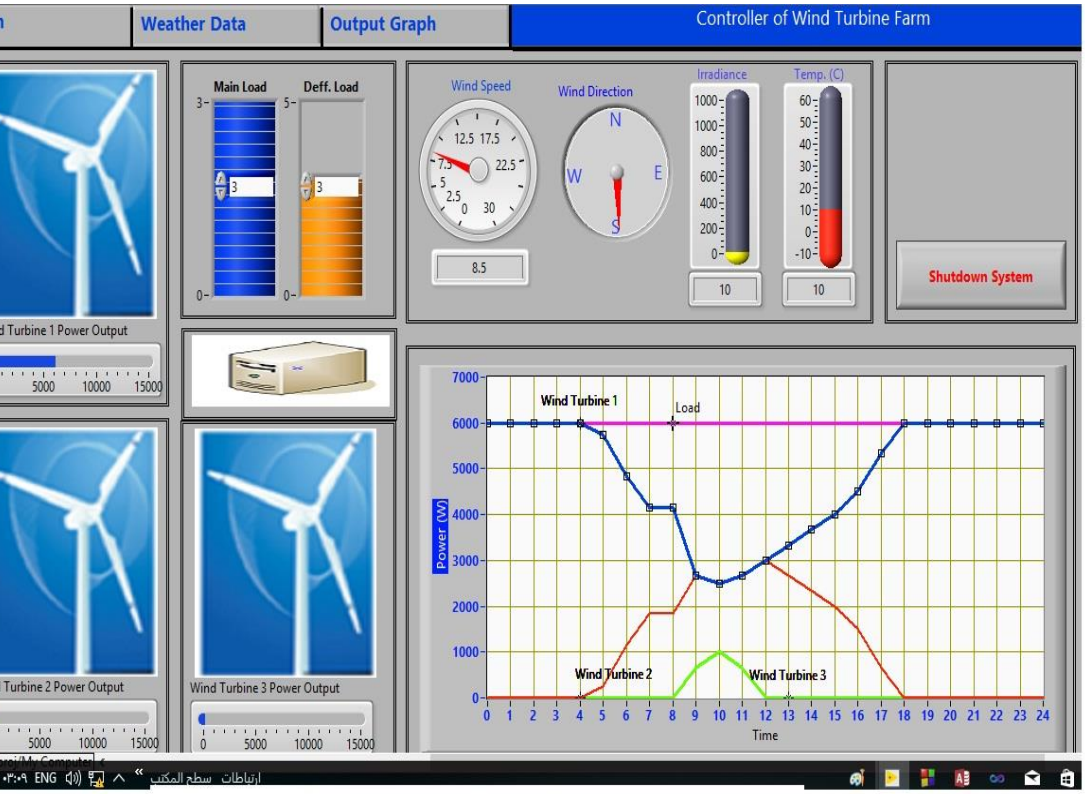

Pw Avaliable
Load 3KW
WT3
Pw-Reference
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

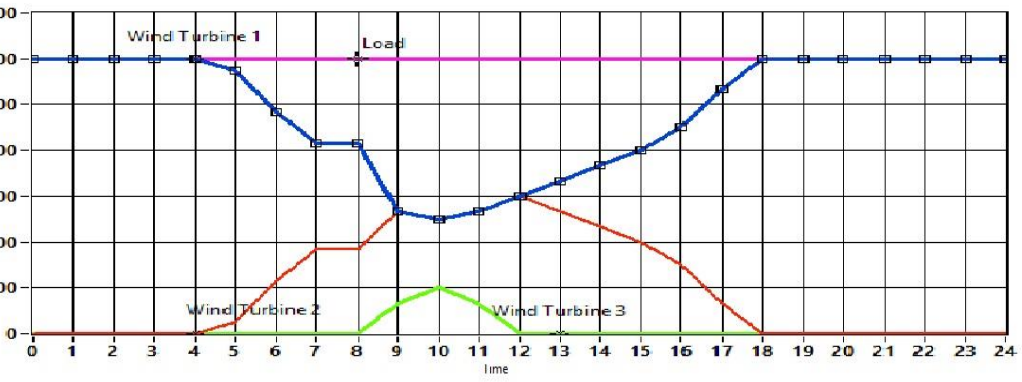
الشكل (16): تعويض انخفاض الاستطاعة بواسطة العنفة WT2 وعدم الحاجة للعنفةWT3`

حسب الاستطاعة المطلوبة $P_{availab-ref}$

المناقشة:

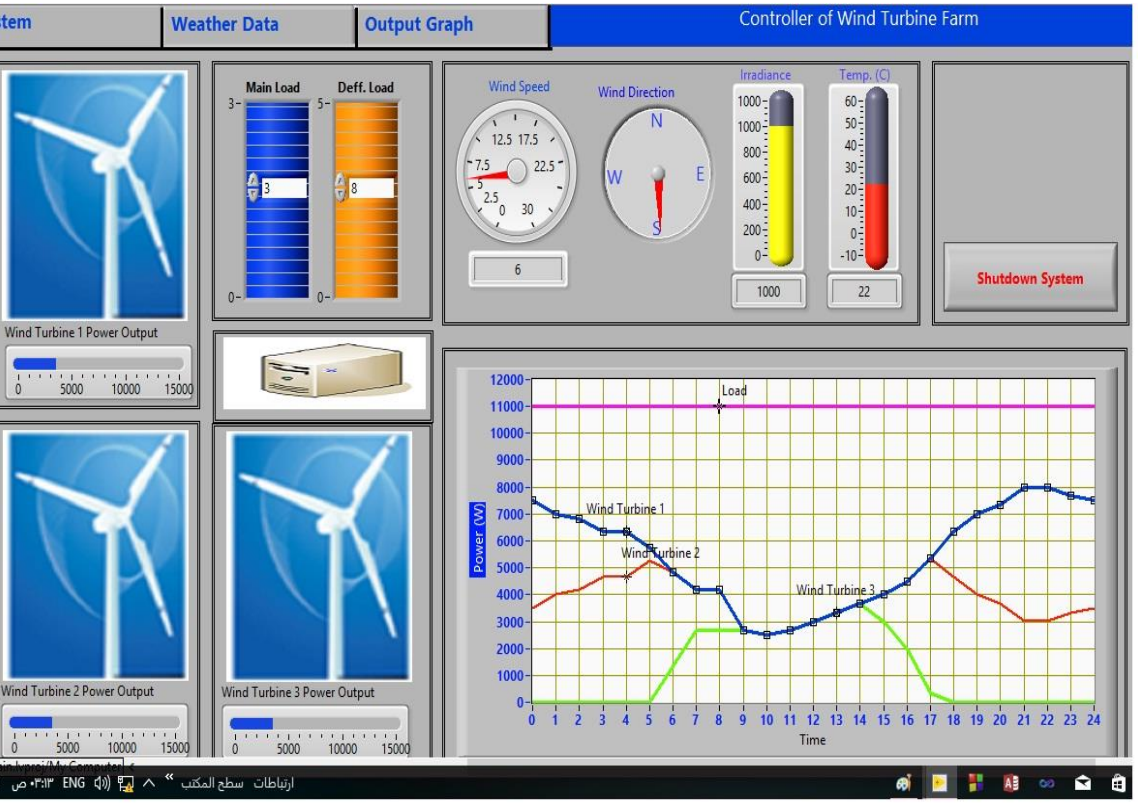
يبين الشكلان 15 و16 أنه بانخفاض سرعة الرياح أثناء النهار انخفضت الاستطاعة الكلية المتاحة وانخفضت معها الاستطاعة التي يقدمها المولد الريحي WT1 وصارت أقل بكثير من الاستطاعة الحمل 3KW، رغم ملاحقة نقطة التشغيل العظمى للعنفة الريحية بواسطة المتحكم الإشرافي العائم. بهذه الحالة عنفة واحدة غير كافية لتغذية الحمل الكهربائي. لذلك الحل هو زيادة عدد العنفات الريحية (أي مزرعة ريحية) لتغذية الحمل الكهربائي بشكل مستمر وبدون انقطاع وتعويض انخفاض الاستطاعة وهنا يكفي استخدام عنفة واحدةWT2 وليس بحاجة للعنفةWT3`.وذلك حسب الاستطاعة المطلوبة.

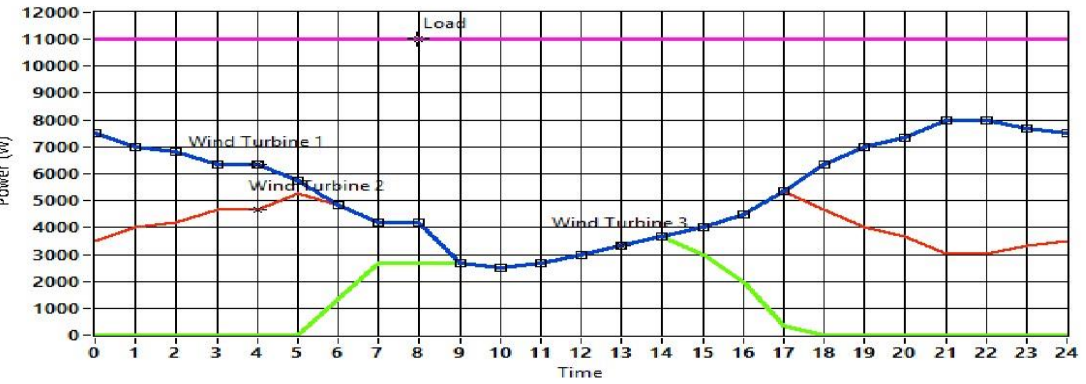




الشكل (17): تعويض انخفاض الاستطاعة بواسطة العنفة WT2 وبسيط بواسطة العنفةWT3`

حسب الاستطاعة المطلوبة $P_{availab-ref}$ بالنسبة للحمل





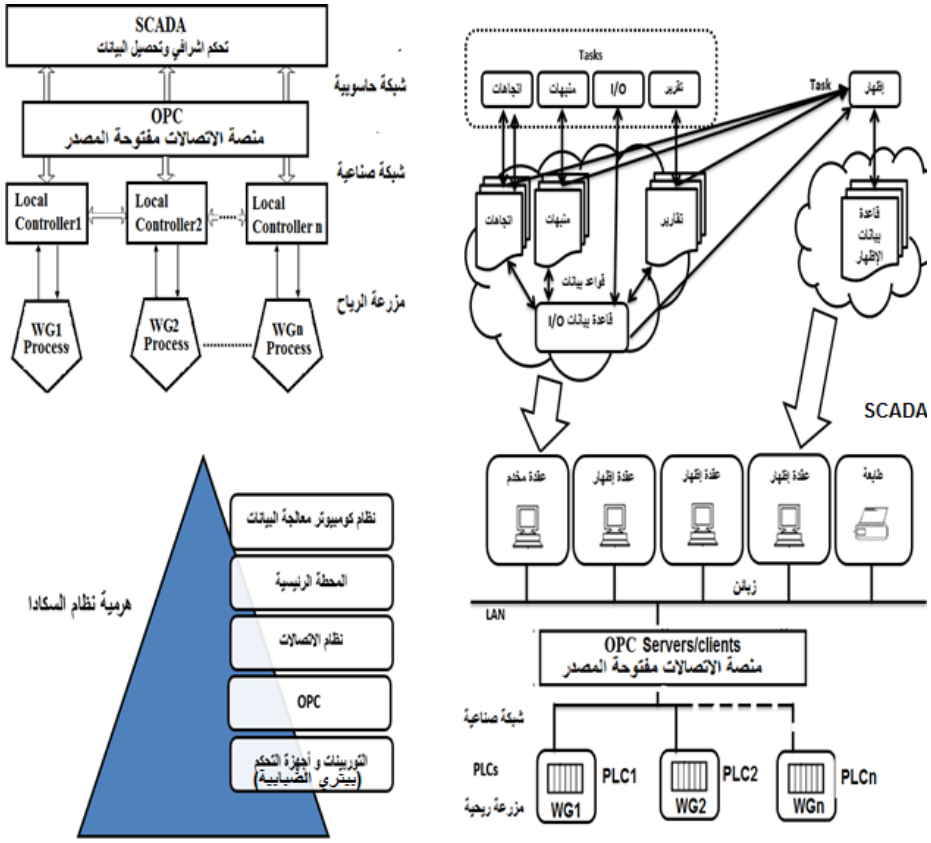
الشكل (18): تعويض انخفاض الاستطاعة بواسطة العنفة WT2 و العنفةWT3` حسب الاستطاعة المطلوبة بالنسبة للحمل

نلاحظ أنه كلما زاد الحمل الكهربائي ونقصت سرعة الرياح، كلما كان الحاجة لإشراك عنفات اضافية بحيث تغذي الحمل الكهربائي باستمرار دون انقطاع للتيار الكهربائي وهي

الغاية الاساسية من مزرعة الرياح. الشكل(18) يبين تدخل العنفةً WT2 بشكل كبير و WT3 بشكل أقل. أما من أجل حمل كهربائي أكبر من الاستطاعة الاسمية فإن العنفتان WT3 و WT3 تساعدان العنفة بشكل ملحوظ. يمكن تطوير الدراسة من أجل استطاعات ضخمة وعندها نحتاج الى مزرعة رياح ومتابعة باستخدام نظام SCAD-OPC لجمع البيانات والمراقبة عن بُعد والتحكم في مزارع الرياح.OPC بروتوكول OPC يسمح لبرمجيات المراقبة والتحكم SCADA بالنفاذ إلى بيانات المتحكمات وبروتوكولاتها على اختلاف أنواعها واختلاف الشركات الصانعة لها.

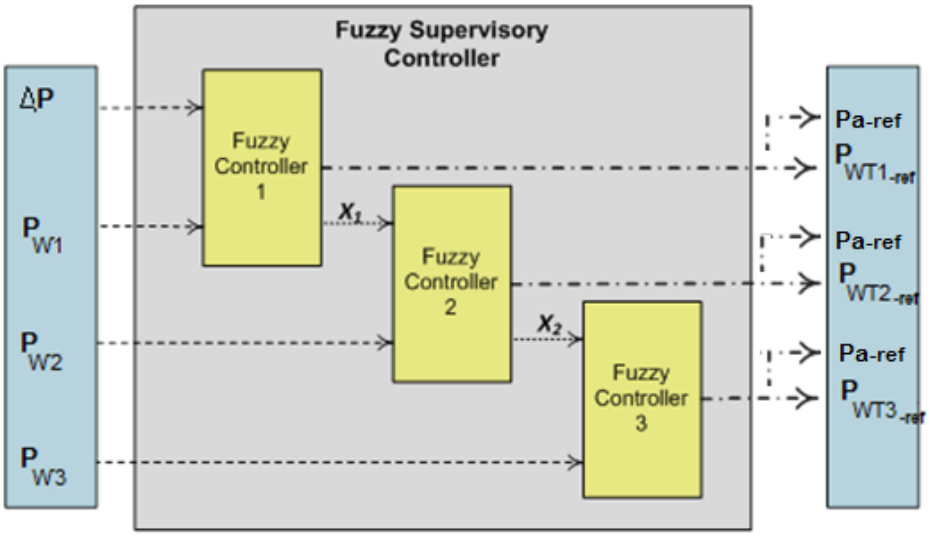
- **تصميم المتحكم العائم الإشرافي SCAD-OPC ذو البنية الهرمية لإدارة مزرعة ريحية**

تم تصميم متحكم إشرافي عائم SCAD-OPC ذو بنية هرمية للتحكم بمزرعة ريحية كما هو موضح في **خطأ! لم يتم العثور على مصدر المرجع.**



الشكل (19): نظام SCAD-OPC ذو البنية الهرمية للتحكم بمزرعة ريحية

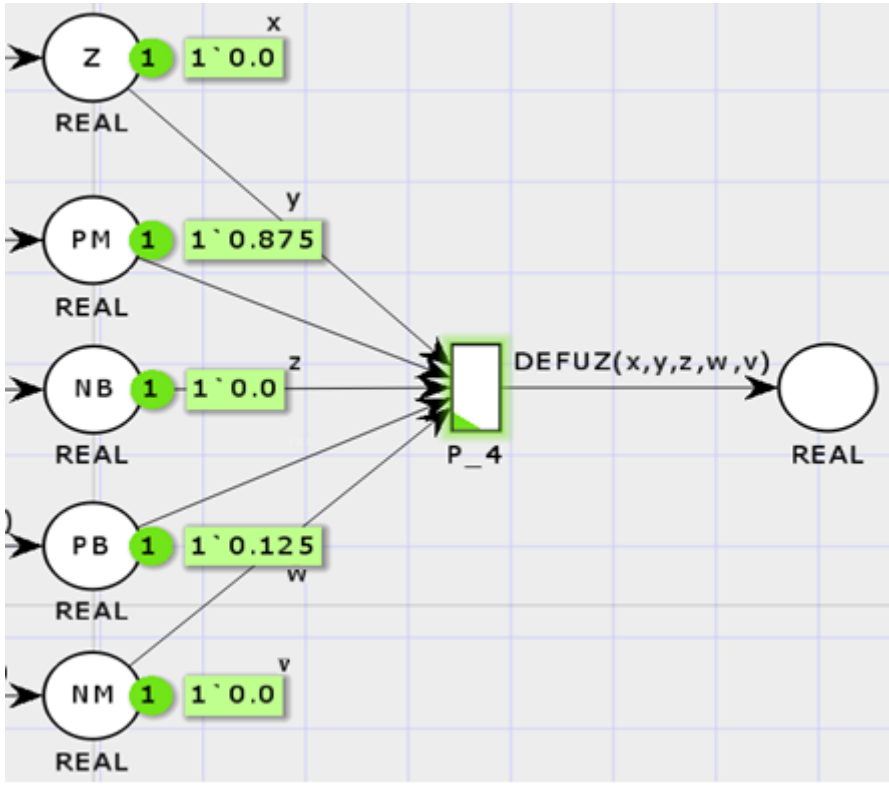
حيث يتم في المرحلة الأولى تصميم متحكم عائم Local Fuzzy Controller1 مهمته اتخاذ القرار بالاستطاعة التي يجب أن تقدمها العنفة الريحية الأولى بالنسبة للحمل. وبعد ذلك يتم الانتقال إلى المتحكم الثاني Local Fuzzy Controller 2 والمتحكم الثالث Local Fuzzy Controller 3 لتحديد الاستطاعة التي يجب أن تقدمها العنفة الريحية الثانية والثالثة لمساعدة العنفة الأولى لتعويض النقص في الحمل الكهربائي. كما هو موضح بالشكل (20).



الشكل (20): المخطط الصندوقي للمتحكم العائم الاشرافي

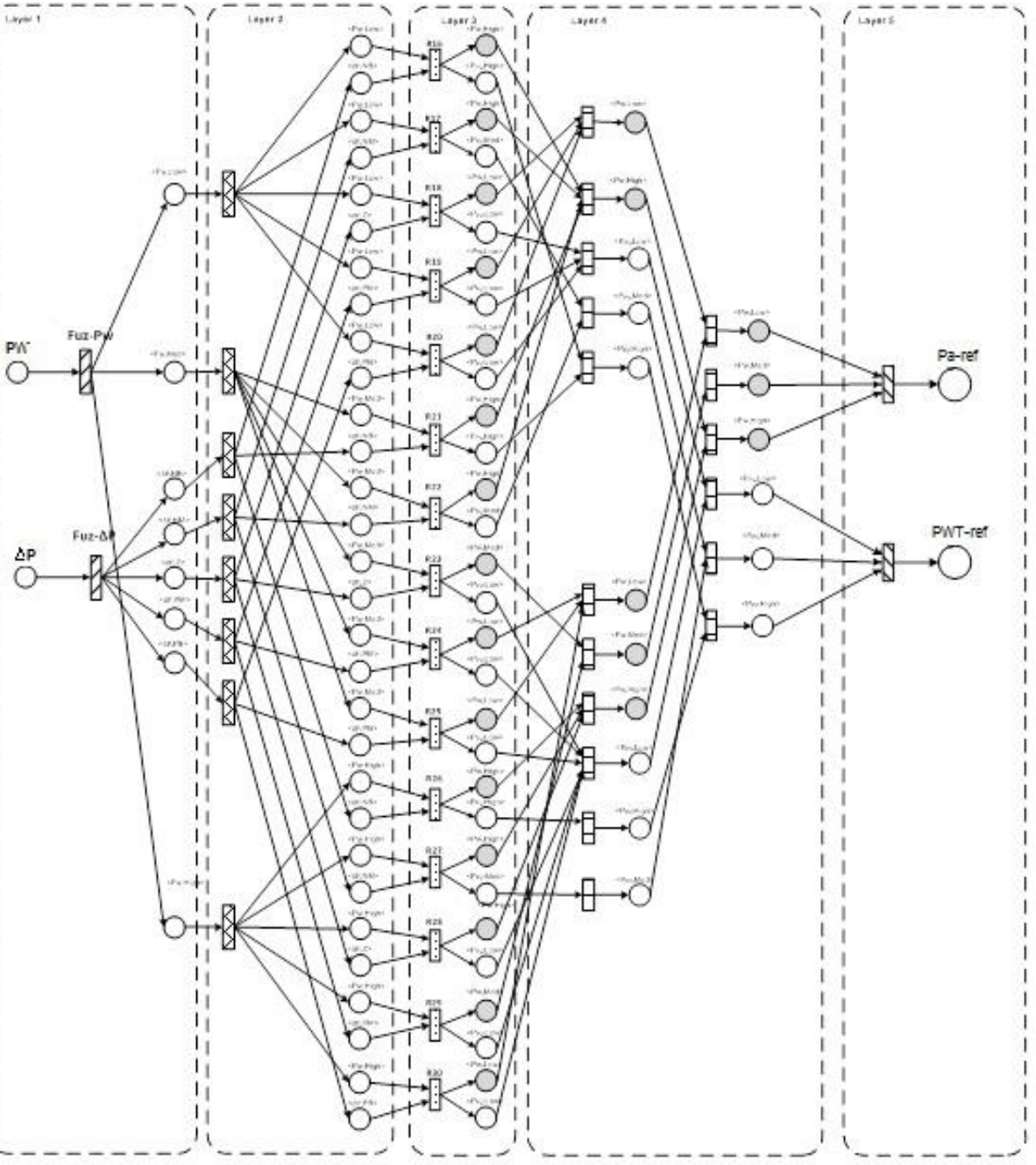
ويبين الشكلخطأ! **لا يوجد نص من النمط المعين في المستند.**(21) نموذج شبكة بتري لطبقة فك التعويم، يسند تابع ينفذ عملية فك التعويم fun DEFUZ(x,y,z,w,v) إلى خرج العبور. نضيف الجزء البرمجي التالي إلى منطقة التعريفات:

fun DEFUZ(x,y,z,w,v) = ((0.0 *x) + (0.875 *y) + ((~0.0)*z) + (0.125 * w) + ((~0.0)*v)))/(x+y+z+w+v)



الشكلخطأ! لا يوجد نص من النمط المعين في المستند.**(21): جزء من محاكاة مرحلة فك التعويم في شبكة بتري العائمة**

ويبين الشكل (22) مخطط شبكة بتري العائمة النهائي المصمم بطبقاتها الخمس لإدارة عنفة ريحية المشروحة سابقا بالتفصيل وهي: طبقة التعويم ، مرحلة مضاعفة الأماكن، طبقة إيجاد العلاقات Rules بين المتغيرات المختلفة، طبقة العبورات التجميعية لاختيار القيمة العظمى المطلوبة $P_{available}$ من قيم أماكن الدخل المرتبطة به (NB أو NM أو Z أو PM أو PB) وإسناد هذه القيمة إلى مكان الخرج PWT-Ref Signall. وأخيراً طبقة فك التعويم وتمثل بواسطة تابع رياضي يحقق هذه المرحلة. عند قدح العبور DEF. PW-Ref تحسب إشارة التحكم بطاقة العنفة الريحية بناءً على تابع الانتماء لإشارة التحكم بالطاقة.



الشكل (22): شبكة بتري عائمة لإدارة استطاعة عنفة ريحية PWT بالنسبة لقيمة استطاعة مطلوبة

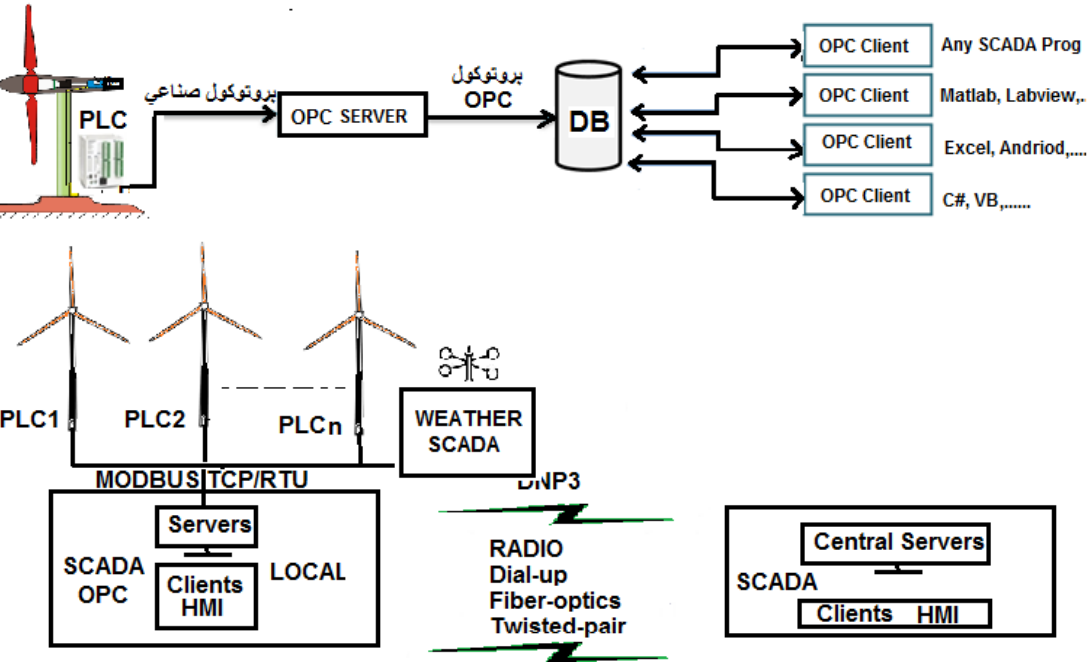
$P_{available}$

❖ **مخططات تنفيذ بروتوكولات الـ OPC وDNP3**

إن أغلب استخدامات بروتوكول الـ OPC تكون بغرض السماح لبرمجيات المراقبة والتحكم SCADA بالنفاذ إلى بيانات المتحكمات المنطقية القابلة للبرمجة PLCs وأمثالها، سنقوم هنا بتوضيح الاعدادات اللازمة لتوظيف بروتوكول الـ OPC بشقيه المخدم والزبون في تطبيق المزرعة الريحية.

سنستخدم في هذا التطبيق العملي الـ OPC الكلاسيكي نظرا لانتشاره الكبير واستحواذه على أغلب منتجات سوق الأتمتة وذلك بالرغم من صدور نسخة الجيل الثاني من البروتوكول (OPC UA).

لبدء مشروع تحكم يربط بين متحكم منطقي ما وبرمجية تحكم ومراقبة SCADA باستخدام بروتوكول الـ OPC يلزم شقين من العمل، الأول عتادي عملي و الآخر برمجي. الشكل (23) يبين البنية العامة التي لنظام SCADA-OPC.



الشكل(23): البنية العامة التي لنظام SCADA-OPC

في البداية وبشكل مختصر، فإن وظيفة الـ OPC Server تنحصر في مخاطبة المتحكمات المنطقية القابلة للبرمجة PLCn بهدف القراءة منه والكتابة فيه، حيث يقوم بالاتصال بالمتحكم وفقا لبروتكول محدد يفهمه المتحكم ويجعل البيانات التي قام بجلبها متاحة لأي OPC Client متصل معه.

يقوم OPC Client بتحديد المخدّم المطلوب ومن ثم ينشأ اتصال معه، فيستطيع عندها الزبون الاطلاع على جميع البيانات المُعرّفة ضمن المخدم وتحديد أي من هذه البيانات مطلوبة له ليُعرفها كمتحولات ضمن بنيته البرمجية (تضمين عناصر المخدم ضمن الزبون).

بعد نجاح الاتصال بينهما، يقوم الزبون بالإرسال إلى المخدم طالبا تحديث البيانات التي قام باختيارها، يُصطلح على تسمية هذه البيانات بالعناصر Items، ليقوم المخدم عند استقبال الطلب من الزبون بالاستجابة له وتحديث البيانات التي طلبها وفقاً لقيم كان المخدم قد قام مسبقاً بتحصيلها من المتحكم المنطقي.

يقوم الزبون بعدها بعرض البيانات المُحدّثة للمستخدم بأي شكل يريده (شكل رسومي Graphics – على شكل إنذارات Alarms –على شكل منحنيات بيانية Trends ... الخ) ويمكنه أيضاً تخزينها للاستفادة منها لاحقا (SCADA- OPC H**istorical** D**ata Access)**. من الجدير بالذكر أنه لا يمكن للـ OPC Client أن يطلب بيانات غير مُعرّفة مسبقاً ضمن الـ OPC Server.

يتبادل الـ OPC Client البيانات مع الـ OPC Server وفق معيار الـ OPC، أما الـ OPC Server فهو يخاطب المتحكم المنطقي وفق بروتكول صناعي يدعمه المتحكم مثل (Modbus, PROFI Bus ,CAN ..).

من ذلك نستنتج أن إنشاء وبرمجة OPC Server يتطلب دراية ببنية البروتوكول الذي يعمل عليه المتحكم و امتلاك صلاحية النفاذ إليه و معرفة بمواقع الذاكرة فيه، وهو أمر غير متاح غالباً، لذلك نجد أن أغلب مزودي OPC Server هم ذات الشركات المصنعة للمتحكمات، وهو أيضاً سبب في كون الـ OPC Server غير متوفر بشكل مجاني. والبرنامج الذي لدنيا يعمل لوقت محدد.

يجب التذكر دوماً منعاً للالتباس، أن الجانب المتعلق باتصال الـ OPC Server مع المتحكمات لا يخضع لبروتوكول الـ OPC، أما اتصال OPC Client مع الـ OPC Server فهو معياري يخضع لقواعد ومتطلبات لبروتوكول الـ OPC.

4.3.5الآفاق المستقبلية

- في هذا البحث تم إجراء اختبارات الأداء على بروتوكول OPC النافذ إلى البيانات (OPC DA) كونه هو السائد حتى الآن في السوق العالمية. مستقبلاً ، يمكن إجراء اختبارات مشابهة للاختبارات التي تم إجراؤها في هذه الدراسة لكن على إصدار الجيل الثاني من بروتوكول الـ OPC وهو OPC UA. والذي يتميز بالخصائص الأتية: منصة الاتصال مستقلة عن نوع نظام التشغيل، قابلية التوسع والأداء العالي أثناء الاتصال، دعم الإنترنت والجُدران النارية، الأمان وإمكانية التحكم بالوصول، إمكانية العمل والتشغيل بين الشركات المختلفة، إمكانية بناء الـ OPC UA باستخدام لغات برمجية متعددة منها (ANSI C، Java، NET) ، مخدم الـ OPC UA يمكن له وفق البنية الجديدة أن يكون متضمن داخل المتحكم وهي ميزة أعطت مرونة كبيرة للمعيار، يدعم أيضاً اتصال آلة بآلة Machine To Machine بمعنى أنه يسمح بالاتصال المباشر بين المكونات الصناعية مع البرمجيات من أجل تحصيل البيانات والتحكم.
- تم تطوير نموذج شبكة بتري عالية المستوى بخمس طبقات نقترح أن يتم البحث عن إمكانية إلغاء طبقة مضاعفة الأماكن، أو اختصار عدد الأماكن في طبقة تحقيق

القواعد، لما له من انعكاس كبير على حجم شبكة بتري، والذي يؤدي إلى زيادة سهولة تصميم ومراجعة تحقيق شبكة بتري.

- يعتمد أداء العنفات الريحية على الظروف المناخية، لذلك نقترح أن يتم تطوير المتحكم الإشرافي ليتضمن خوارزميات تتعلق بالتنبؤ المستقبلي لتغيرات الطقس بما يحسن من أداء المتحكم الإشرافي.

المراجع العلمية

[1] علي عباس القره غول ، وهيب عيسى الناصر -2002 **"مبادئ الطاقة المتجددة وتطبيقاتها ".**

[2] Schneider Electric, March 2012- **"Telemetry & Remote SCADA Solutions".** White paper. SCADA Systems.

[3] SHETTY and KOLOK. 2011**. Hechatronics system design**

[4] Kurt. J, Lars .M. K, 2009- **"Colored Petri Net".** Thesis, Springer.

[5] http://www.cs.au.dk/CPNTools, **"CPN Tools"** homepage. [Online].

[6] Seung Jun Lee and and Poong Hyun Seong, **"Development of Automated Operating Procedure System Using Fuzzy Colored Petri Nets for Nuclear Power Plants,"** *Annals of Nuclear Energy*, vol. 31, pp. 849-869, May 2004.

[7] Xu. L, Kezunovic. M, November 2006 – **"Implementing Fuzzy Reasoning Petri-nets for Fault Section Estimation".** IEEE Transactions on Power Delivery, Vol.1, No1**.**

[8] Hajizadeh. A, Golkar. M. G, 2007- **"Intelligent Power Management Strategy of Hybrid Distributed Generation System,"** Electrical Power and Energy Systems, pp. 783 – 795.

[9] Hernández. M, 2007- **"Hierarchical Control OF Hybrid Power Systems".** University Of Puerto Rico, Mayaguez Campus, Ms.c Thesis.

[10] Voutetakis. Spyros, Chrysovalantou. Z, Dimitris Ipsakis. D, 2009**. "On Line Energy Management Strategy of an Off-Grid Hybrid Power Generation System".** International journal of hydrogen energy 34 (16), 7081-7095

[11] Thana. F. Al-Shatter. M. N, Eskander.N.M, Mohsen T. El-Hagry.M. T**,** 2006- **"Energy Flow and Management of a Hybrid Wind/PV/Fuel Cell Generation System".** Energy Conversion and Management, vol. 47, pp. 1264-1280.

[12] Price. J.J, Sanchez. C, 2006- **"Simplified wind turbine generator aerodynamic models for transient stability studies".** Iberdrola Renewables. IEEE PSCE 2006, PP. 986-992.

[13] Gonthier. J. R, 2011- **"Surveillance centralisé de fermes éoliennes".** Vogel Communications Group. MSM.

[14] M. ATASSI. M, 2017- "Increase Reliability of Aeolian using Fuzzy Smith Predictor Modeled by Colored Petri Nets" .A. Prof. Dep. of Mecatronics Engineering – FMEE- Al Baath University.Vol 39. N°43.

[15] Mukund R. P, 1999- **"Wind and Solar Power System".** CRC Press**.**

[16] Kaltschmitt. M Wolfgang. S, Wiese. A, 2007- **"Renewable Energy"** Technology, Economics and Environment. Germany: Springer, Eds.

[17] Munteanu. I, IBratcu. A, CutululisN.A, Ceanga. E, 2008- **"Optimal Control of Wind Energy Systems".** Springer.

[18] Hongxing. Y, Wei. Z, Chengzhi. L, 2009- **"Optimal Design and Techno-Economic Analysis of a Hybrid Solar–Wind Power,"** Applied Energy, pp. 163–169.

[19] Huynh. Q. M, Nollet. F, Essounbouli. N, 2011- **"Control of permanent magnet synchronous generator wind turbine for stand-alone system using fuzzy logic"** EUSFLAT-LFA 2011, pp. 720-727**.**

[20] Mehmet. D, Serefoglu. S, **"Design and Implementation Of a Microcontroller-based Wind Energy Conversion System"** Tubitak.

[21] Shakil. A. K, Ismail H, Jakir Hossain. M, June 2011- **"Fuzzy Logic Based Control Scheme for Power Optimization of a Small Wind Turbine System with DC-DC Converter"** International Journal of Electronics & Communication Technology, vol. 2, no. 2, pp. 18-21**.**

[22] STUART. B, 2004- **"Supervisory Control and Data Acquisition (SCADA)**" Instrument Society of America, Research Triangle, NC Systems.

[23] ATASSI. M, 2015- **"SCADA- OPC- FPN-Micro" - .** Al-Baath University. Mechatronics Dept. FMEE

[24] ATASSI. M 2016- **"Large-scale control".** Damascus Universities. Masters. Computer & automation Dept. FMEE.

[25] Zarour. O, 2018- **"Study a Hybrid Industrial Network Using OPC Protocol"** Master in control and automation engineering. Damascus Universities.

استخدام الشبكات العصبونية للكشف عن التطبيقات الخبيثة في نظام أندرويد

طالب الدراسات العليا: روعة طويلة

كلية: الهندسة المعلوماتية – جامعة: البعث

الدكتورة المشرفة: رانيا لطفي

ملخص البحث

يعتبر نظام الاندرويد من أكثر نظم التشغيل المنتشرة على الهواتف المحمولة ، لذلك فإن عدد التطبيقات الضارة تتزايد مع ازدياد عدد التطبيقات المنتشرة على المتاجر. هنالك العديد من الأدوات الموقعة إلكترونياً موجودة على المتاجر والتي تحد من انتشار وتوزيع التطبيقات الضارة ، إلا أن هناك العديد من الدراسات والأبحاث التي وجدت أن نظام الكشف التقليدي المعتمد على التوقيع يعمل بشكل جيد إلى حد ما لأن مطوري البرمجيات الضارة يستخدمون تقنيات عديدة للاحتيال على تلك الأدوات. ومن هنا أتت الحاجة لإيجاد نظام بديل للكشف عن البرمجيات الضارة وذلك لاستكمال وتصحيح النظام المعتمد على التوقيع الالكتروني.

ركزت الأبحاث الحديثة على خوارزميات التعليم الآلي والتعلم العميق التي تحلل الميزات المستخرجة من التطبيقات الضارة ، كما وتستخدم هذه الميزات لتصنيف واكتشاف التطبيقات الجديدة والغير معروفة.

تلخص هذه الدراسة كيفية استخدام الشبكات العصبونية للكشف عن البرمجيات الضارة في نظام أندرويد .وتبين النتائج التجريبية أن استخدام الشبكات العصبونية كان له أثر إيجابي في تحسين الكشف عن البرمجيات الضارة وذلك يتوقف على عدد الطبقات وعدد العصبونات المستخدمة لبناء الشبكة.

كلمات مفتاحية : تحليل البرمجيات الخبيثة ، نظام أندرويد ، حماية الأجهزة الذكية ، الشبكات العصبونية.

Using Artificial Neural Networks to Detect Malicious Applications in Android System

Eng. Rawaa Taweela Dr. Rania Lutfi

Abstract

Android OS is one of the widely used mobile Operating Systems. The number of malicious applications and adwares are increasing constantly on par with the number of mobile devices. A great number of commercial signature based tools are available on the market which

prevent to an extent the penetration and distribution of malicious applications. Numerous researches have been conducted which claims that traditional signature based detection system work well up to certain level and malware authors use numerous techniques to evade these tools. So given this state of affairs, there is an increasing need for an alternative, really tough malware detection system to complement and rectify the signature based system. Recent substantial research focused on machine learning algorithms that analyze features from malicious application and use those features to classify and detect unknown malicious applications. This study summarizes the evolution of malware detection techniques based on machine learning algorithms focused on the Android OS.

Keywords: malware analysis, android, Smartphone security , Neural Networks.

المقدمة :

وفقاً لبحث جرى في عام 2014(RiskIQ 2014) ازدادت التطبيقات الضارة في المتاجر بنسبة 388% بين عامي 2011 و 2013 .

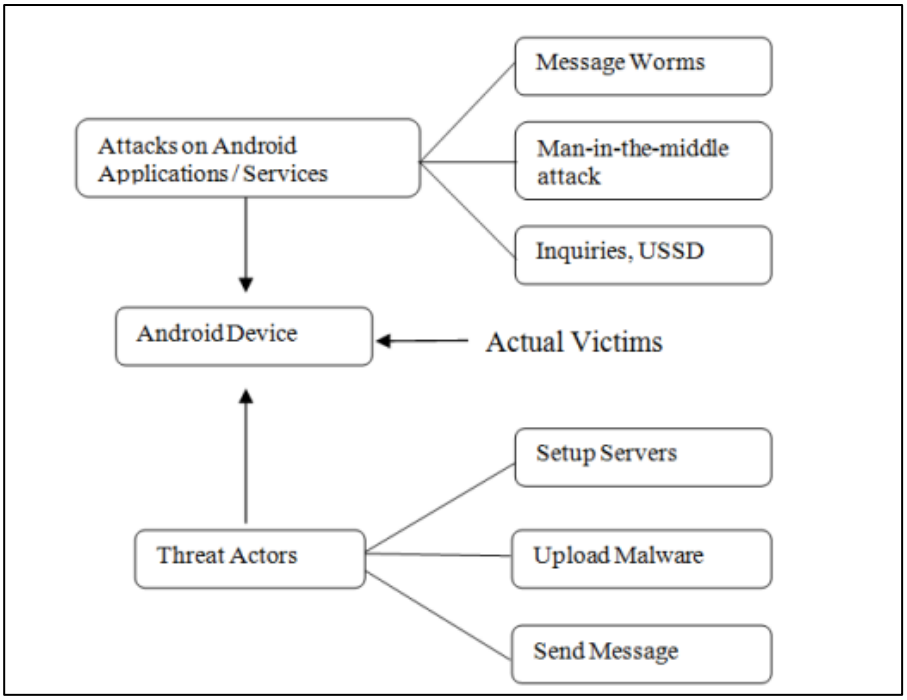
كجزء أساسي من بحثنا ، أجرينا دراسة شاملة حيث قمنا بتحليل المنهجيات الحالية المستخدمة في الكشف عن البرمجيات الضارة على نظام أندرويد باستخدام تقنيات التعلم الآلي.

الهدف العام من هذه الدراسة هو تحديد الأبحاث التي عملت على اكتشاف البرمجيات الضارة على نظام أندرويد باستخدام خوارزميات التعلم الآلي.

فمن خلال هذا التحليل يمكننا صياغة آلية للتصدي للهجمات المعدلة update attack التي يصعب الكشف عنها والقضاء عليها.

Update attack: يتم تعريفه على أنه تطبيق حميد مثبت على النظام يقوم بتحميل ملفات خبيثة أثناء تحديثه أو يحاول تنزيل تطبيقات ضارة وتثبيتها على النظام . من الصعب جداً تحديد هذا النوع من الهجوم لأن التطبيق الأساسي حميد، ولا يمكننا اكتشاف النشاط الضار ما لم نتتبع الإصدارات السابقة للتطبيق ومراقبة التطبيق بعد التحديث [2].

نهدف الى تقديم منهج مضاد لهذا الهجوم من خلال الاطلاع على الاتجاهات الحديثة في الكشف عن البرامج الضارة.



الشكل 1. لمحة عن الهجمات في نظام أندرويد [1]

هدف البحث :

تعتمد معظم أساليب الكشف عن التطبيقات الضارة على طرق تقليدية مثل دراسة التوقيع الالكتروني ، مراقبة استهلاك الطاقة في الجهاز ... الخ ، ولكن كل من الطرق السابقة لها العديد من السيئات ولم تعطِ النتائج المرغوبة.

هدفنا ايجاد حل لمعالجة التطبيق واستخراج الميزات ومحاولة كشف فيما اذا كان هذا التطبيق خبيثاً أو سليماً.

الحل البديل هو التحليل الستاتيكي أي دراسة الميزات واستخدام طرق الاستدلال التي تحاول الكشف عن البرمجيات الخبيثة من خلال مراقبة الميزات والخصائص

الاحصائية للأجهزة النقالة ، وأشهر هذه الطرق هي تحليل السماحيات التي يطلبها التطبيق عند تنصيبه مثل طلب الوصول إلى الشبكة – طلب تحديد موقع المستخدم .... الخ.

هذه الطريقة وحدها لم تكن كافية سليمة ، لذلك تم العمل على الناحية الديناميكية للتطبيقات مثل دراسة الاستدعاءات للتطبيق.

وتعتبر هذه الطريقة أكثر دقة من دراسة السماحيات فقط لأنها تلتقط التنفيذ الحالي (runtime)للتطبيق .

ومن هذا المنطلق كان الاقتراح لتصميم إطار لتحليل وتصنيف التطبيقات الخبيثة بالاعتماد على خوارزميات التنقيب في البيانات بما فيها تقنيات تعليم الآلة Machine Learning و تقنيات التعلم العميق Deep Learning .

وفيما يلي سنوضح احدى الطرق المستخدمة في هذه الدراسة ألا وهي الشبكات العصبونية الصنعية [4] :

الشبكة العصبونية – أو اختصاراً "الشبكات العصبونية " – هي تمثيل صنعي للدماغ البشري تحاول محاكاة عمليته الطبيعية للتعلم.

إن الشبكة العصبونية هي عبارة عن مجموعة من الأعصاب الصنعية المترابطة فيما بينها ، تستخدم نموذجاً رياضياً أو حسابياً لمعالجة المعلومات بالاعتماد على منهج ارتباط للحساب.

تحاكي الحواسيب العصبونية قدرات معالجة معينة في الدماغ البشري.

الحوسبة العصبونية هي نموذج لمعالجة المعلومات مستوحى من النظام البيولوجي ومركب من عدد كبير من عناصر المعالجة المترابطة فيما بينها بقوة (العصبونات) والتي تعمل بانسجام لحل مشكلة معينة.

على غرار البشر، فإن الشبكات العصبونية تتعلم من خلال الأمثلة.

تم تكوين الشبكات العصبونية بهدف تنفيذ تطبيقات معينة مثل تطبيقات التعرف على الأنماط ، تصنيف البيانات ، وكل ذلك يتم من خلال عملية التعلم.

تساعد الشبكات العصبونية في الحالات التي لا يمكن فيها صياغة خوارزمية معينة للحل ، أو عندما يمكننا الحصول على العديد من الأمثلة للسلوك الذي نطلبه.

إن الحواسيب المستخدمة تعتمد على بنية أساسية وهي "von neumann" تعتمد على عمليات المعالجة والتخزين بالذاكرة ، أما الشبكات العصبونية فتعتمد على البنية التفرعية للدماغ البيولوجي.

الشبكات العصبونية هي عبارة عن نظام حاسوبي متعدد المعالجات يتضمن:

عناصر معالجة بسيطة

درجة عالية من الارتباطات الداخلية

رسائل عددية بسيطة

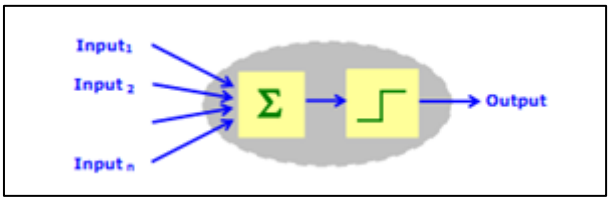
تفاعلات تكيفية بين العناصر

1.1 نموذج العصبون الصنعي:

العصبون الصنعي هو عبارة عن تابع رياضي يمثل نموذجاً مبسطاً من العصبون الحيوي الحقيقي.

- **نموذج McCulloch– pitts:**

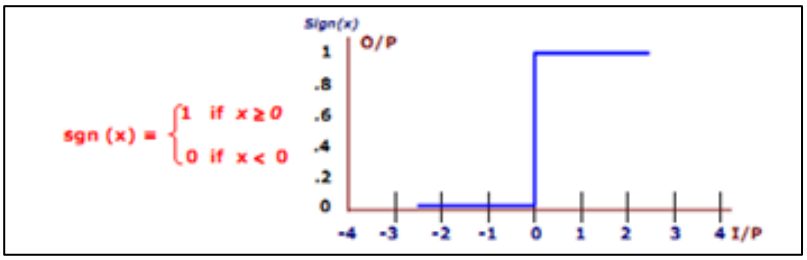
يدعى هذا النموذج وحدة منطق العتبة (threshold logic model)



- مجموعة من اتصالات الدخل مسؤولة عن إيصال أوامر التنشيط من العصبونات الأخرى.
- وحدة معالجة تقوم بجمع الدخل ثم تقوم بتطبيق تابع تنشيط غير خطي (مثل توابع squashing / transfer/threshold)
- خط خرج يوصل النتيجة إلى العصبونات الأخرى.

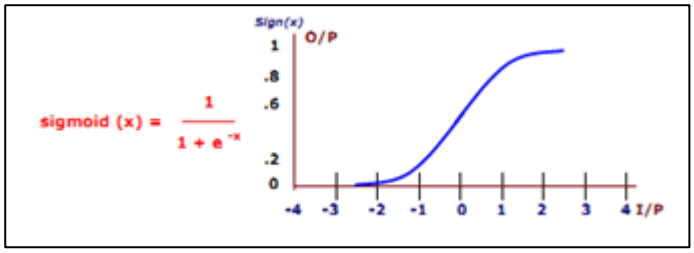
1.2 التوابع:

- Threshold or sign function: sgn (x) يعرف كالتالي



يأخذ التابع القيمة (1) إذا كانت المتحول موجبة او تساوي الصفر ويأخذ القيمة (0) إذا كانت سالبة

- Threshold or sign function: sigmoid(x) وهو يختلف عن السابق بأنه يضم تدرجاً وأنه قابل للاشتقاق



1. نماذج العصبون الصنعي :

a. نموذج McCulloch– Pitts:

والذي تم شرحه سابقاً

1– تكتب معادلة الخرج لعصبون McCulloch–Pitts كتابع لمدخلات عددها n –1 بالشكل التالي:

$$Output = sgn\left(\sum_{i=1}^{n} Input_i - \Phi\right)$$

عتبة تنشيط العصبون

وتطبق الشروط التالية:

$$If \sum_{i=1}^{n} Input_i \geq \Phi \quad then \quad Output = 1$$

$$If \sum_{i=1}^{n} Input_i < \Phi \quad then \quad Output = 0$$

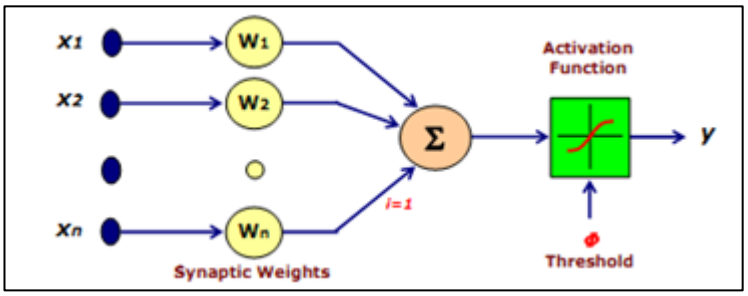
هذا النموذج يفتقر إلى الخصائص التالية:

- الدخل والخرج الغير ثنائي

- الجمع غير الخطي
- تنعيم العتبة
- العشوائية
- المعالجة الزمنية للبيانات

b. نموذج العصبون الصنعي (العناصر الأساسية):

يتكون العصبون من ثلاثة عناصر أساسية : الأوزان – العتبات – وتابع التنشيط



الشكل 2. العناصر الاساسية للعصبون الخطي الصنعي

- الأوزان W

لدينا شعاع الدخل(X) وشعاع من الأوزان (W)

تستخدم الأوزان (w1,w2,….,wn) لتحدد مدى أهمية كل دخل بالنسبة

للعصبون أو مدى قوة شعاع الدخل $X= [x1,x2,…..xn]^T$

كل دخل يضرب بالوزن الموافق له XT W

إذاً الدخل هو عبارة عن مجموع الجداء السلمي لعناصر الدخل بأوزانها

$$I = X^T.W = x_1 w_1 + x_2 w_2 + \ldots + x_n w_n = \sum_{i=1}^{n} x_i w_i$$

بعد ذلك يتم تطبيق أحد توابع التنشيط .

- العتبة Threshold:

العتبة الداخلية للعقدة هي قيمة حدية تؤثر على تنشيط الخرج (Y) لهذه العقدة

$$Y = f(I) = f\{\sum_{i=1}^{n} x_i w_i - \Phi\}$$

في النهاية يتم توليد الخرج (Y) من خلال تمرير المجموع السابق إلى تابع فلترة f يدعى تابع التنشيط أو تابع النقل الذي يعطي الخرج.

- تابع التنشيط (activation function):

يقوم التابع f بعمليات رياضية على إشارة الخرج

التوابع الأكثر شيوعاً:

- Linear function
- Threshold function
- Piecewise linear function
- Sigmoidal (S shaped) function
- Tangent hyperbolic function

يتم اختيار توابع التنشيط اعتماداً على نوع المسألة المطلوب حلها من قبل الشبكة العصبونية.

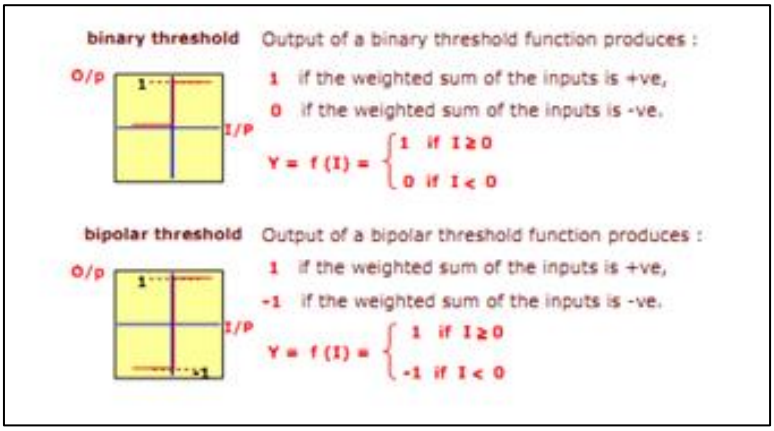
c. أنواع توابع التنشيط:

حاول الباحثون عبر السنوات إيجاد توابع لتحويل الدخل إلى خرج وفيما يلي أكثر هذه التوابع شيوعاً.

- I/P المحور الأفقي يمثل مجموع الدخل.
- O/P المحور العمودي يمثل القيمة التي يعيدها التابع (الخرج).

- **Threshold Function:**

يستخدم هذا التابع مبدأ القيمة الحدية ويكون إما من نوع ثنائي أو ثنائي القطب

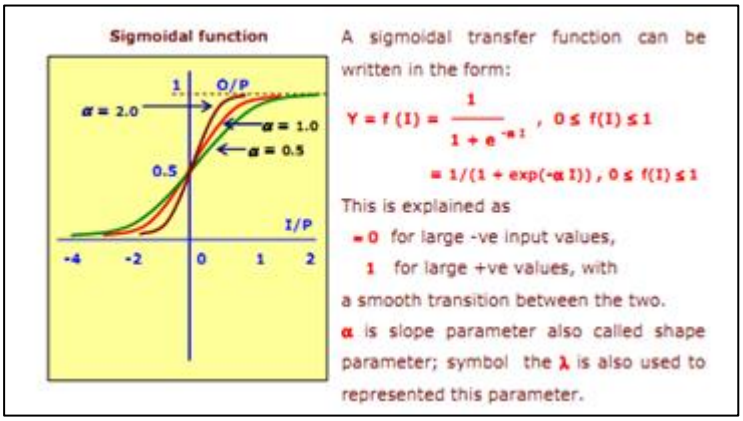


الشكل 3. تابع العتبة

- **Sigmoidal Function (S shaped)** :

تابع غير خطي وهو نوع شائع من توابع التنشيط يستخدم لبناء الشبكات.

وهو جيد رياضياً وقابل للتزايد بشكل كبير و differentiable



الشكل 4. تابع Sigmoid

2. دراسات مرجعية :

هناك منهجيتان أساسيتان لتحديد حالة البرنامج فيما اذا كان سليماً أم خبيثاً ، وهي التحليل الستاتيكي و التحليل الديناميكي .

في منهجيات التحليل الستاتيكي لا يتم تنفيذ التطبيق وإنما تعتمد على بعض الميزات التي نستخرجها من الملفات مثل (opcode frequency , strings , byte sequence , function length , API calls ....)

ومن ثم نطبق إحدى خوارزميات التصنيف لتحديد حالة البرنامج .

بينما في التحليل الديناميكي يتم تنفيذ البرنامج وخلال عمله نراقب سلوكه ونلتقط بعض البارمترات الهامة وتمثيلها كميزات تستخدم في خوارزمية التصنيف .

بالاضافة لذلك ، يوجد خوارزميات تستخدم ميزات مختلفة معتمدة على نوعي التحليل الستاتيكي والديناميكي وتسمى المنهجيات الهجينة.

Bilar[10] استخدم خاصية opcode frequency distribution لتحديد وجود تطبيقات خبيثة ، بينما Karim et al.[11] استخدم مسلسلات وتبديلات opcode كخاصية اساسية لخوارزمية التصنيف .

Ashu et al.[12] استخدم خاصيتين opcode frequency و file size وذلك بهدف زيادة دقة التصنيف مع أكثر من خوارزمية ، حيث وصلت الدقة لأكثر من 98% .

3. توصيف البيانات:

نظراً لأهمية النتائج التي أعطتها الشبكات العصبونية في المجالات العديدة التي طبقت فيها ، لذلك سنقوم ببناء شبكة وندربها لتكون بمثابة مصنف عملي يحدد حالة التطبيق سليم أم خبيث .

أولى خطواتنا تجهيز بيانات الدخل ، وهي عبارة عن تمثيل لتطبيقات الأندرويد المراد تحديد صنفها ، تتألف القاعدة من 100 سجل : 70 سجلاً لبيانات التدريب و 30 بيانات التجريب.

لذلك بعد درسة وبحث حددنا مجموعة من الخاصيات التي تميز تطبيق الأندرويد ، ومن خلالها سوف نقوم ببناء قاعدة البيانات وندرب الشبكة .

اسم الخاصية	قيمة الخاصية	توصيف
Category	Education Games MultiMedia And Video …	فئة التطبيق (فنية – رياضية – تعليمية ..)
Number of sensitive permissions	[1–10]	عدد السماحيات الحساسة في التطبيق
ask for sensitive data	Yes – no	هل يطلب التطبيق بيانات خاصة حتى يعمل
mature content	Yes – no	هل يتضمن التطبيق وجود محتوى جنسي
rating	1– عدم وجود التطبيق على متجر غوغل بلي [1–5]	تقييم التطبيق ضمن المتاجر الالكترونية
API Calls	[1–30]	عدد استدعاءات النظام التي يطلبها التطبيق
Signed Or Not	Yes – no	هل التطبيق موقع الكترونيا من هيئة معروفة
google play	Yes – no	هل التطبيق موجود على متجل google play الرسمي

الخرج هو نتيجة التصنيف هل التطبيق سليم أم خبيث .

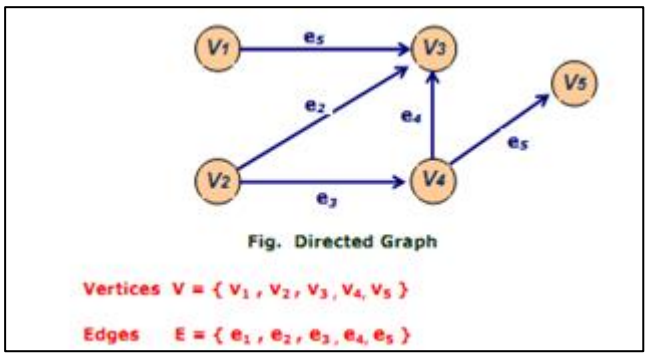
4. بنية الشبكات العصبونية:

الشبكة العصبونية هي نظام معالجة بيانات يتألف من عدد هائل من عناصر المعالجة المتصلة فيما بينها بشكل قوي ومتشابك.

يمكن تمثيل الشبكة العصبونية من خلال بيان موجه G يتضمن عدداً من الرؤوس V والوصلات E

كل رأس يمثل دخل أو خرج العصبونات والوصلات تمثل روابط المشابك

مثال:



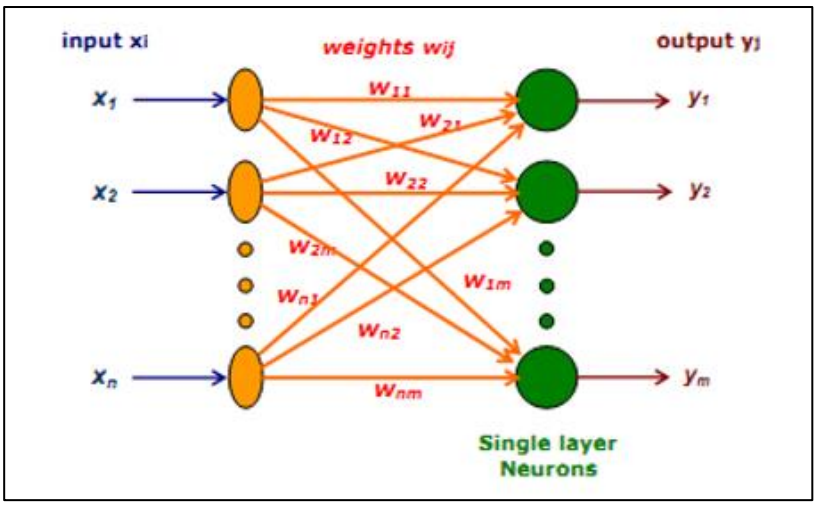
الشكل 5. بيان موجه

a. Single Layer Feed-Forward Network

تتكون هذه الهيكلية من طبقة واحدة فقط من العصبونات ، وتتصل نقاط الدخل مباشرة مع عصبونات الخرج حيث أن كل دخل يتصل مع جميع العصبونات في الخرج ، وكل اتصال يتمثل بوزن w_{ij} (وزن الدخل i مع العصبون j)

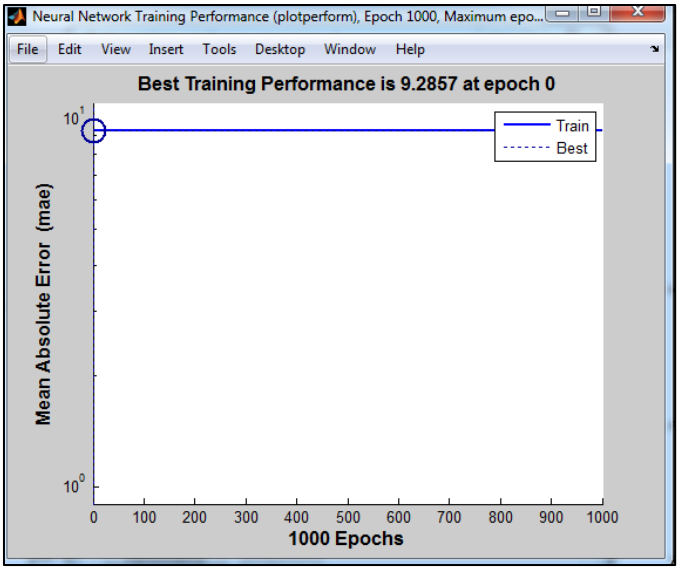
وكما تعتبر هذه الشبكة ذات تغذية متقدمة حيث كل الأسهم تتجه من الدخل نحو عصبونات الخرج ولا يوجد أسهم عائدة.

كل عصبون في طبقة الخرج يقوم بحساب مجموع أوزان الدخل القادمة إليه ، من ثم يقارن المجموع مع حد معين (عتبة) وعلى أساس ذلك يعطى الخرج المناسب 0 أو 1.



الشكل 6. شبكة من طبقة واحدة تغذية متقدمة

بالاختبار الأول سنقوم ببناء شبكة من النوع Perceptron تتألف من طبقة واحدة، وتدريب هذه الشبكة بالبيانات التي ذكرناها سابقاً ، ومن ثم استخراج ومعالجة النتائج ، فيكون الأداء كما يلي :



الشكل 7. أداء الشبكة

ونتيجة محاكاة الشبكة ظهرت كما يلي :

```
>> sim(network1,indata)

ans =

  Columns 1 through 9

    1     1     1     1     1     1     1     1     1

  Columns 10 through 18
```

الشكل 8. محاكاة الشبكة

مما سبق نلاحظ أن النتائج سيئة للغاية وأن الشبكة لا تتدرب والنتائج التي حصلنا عليها بعيدة كل البعد عن النتائج المتوقعة والمرغوبة ، لذلك نجد أن الشبكة المؤلفة من طبقة واحدة فقط لا تعطي خرجاً جيداً.

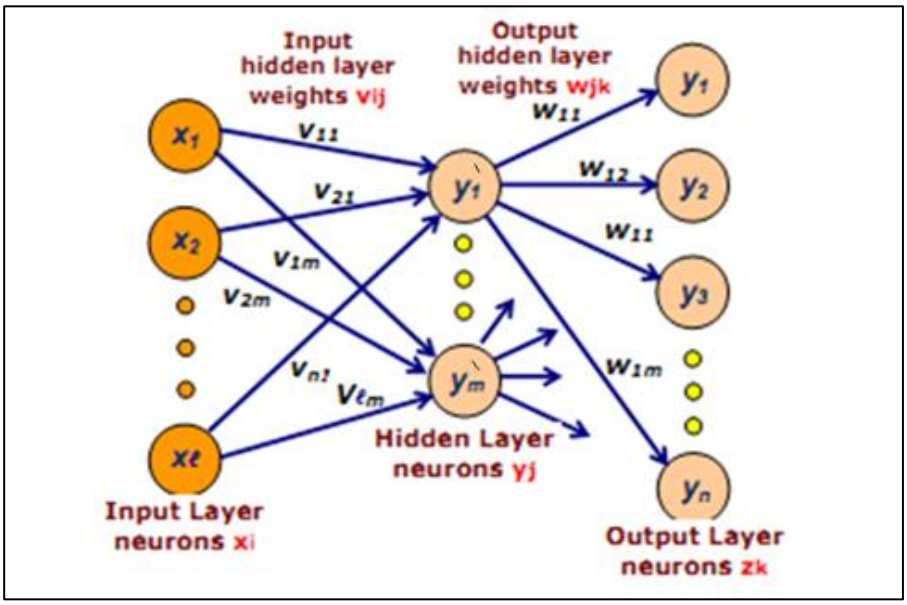
b. Multi Layer Feed-Forward Network

تتكون هذه الهيكلية من عدة طبقات ، طبقة الخرج ومجموعة من الطبقات المخفية (طبقة مخفية واحدة أو أكثر) [3]

ترتبط عناصر الدخل مع جميع عصبونات الطبقة المخفية ، وعصبونات الطبقة المخفية ترتبط مع جميع عصبونات طبقة الخرج .

أما بالنسبة للأوزان : الأوزان بين عناصر الدخل والطبقة المخفية vij (وزن الدخل i مع عصبون الطبقة المخفية j) ، و wjk تمثل الأوزان بين عصبونات الطبقة المخفية وعصبونات طبقة الدخل (وزن العصبون j من الطبقة المخفية مع العصبون k من طبقة الخرج)

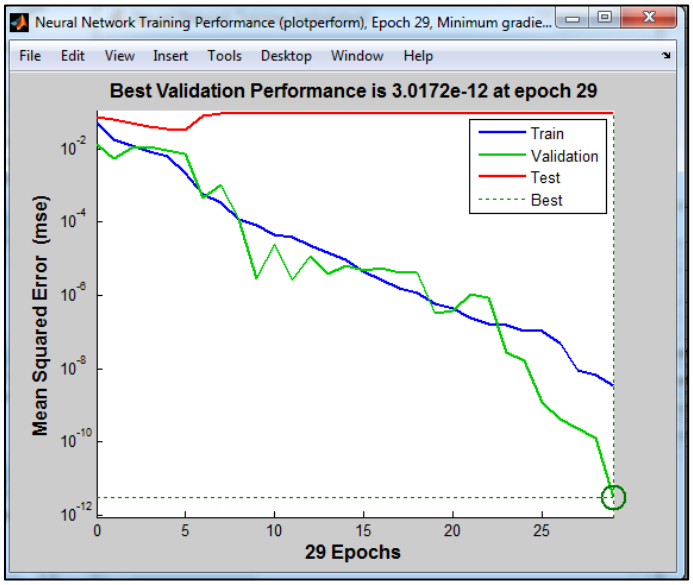
تتم في الطبقة المخفية العمليات الحسابية والمعالجات المرحلية (التكميم) اللازمة لإشارات الدخل قبل إرسالها إلى طبقة الخرج



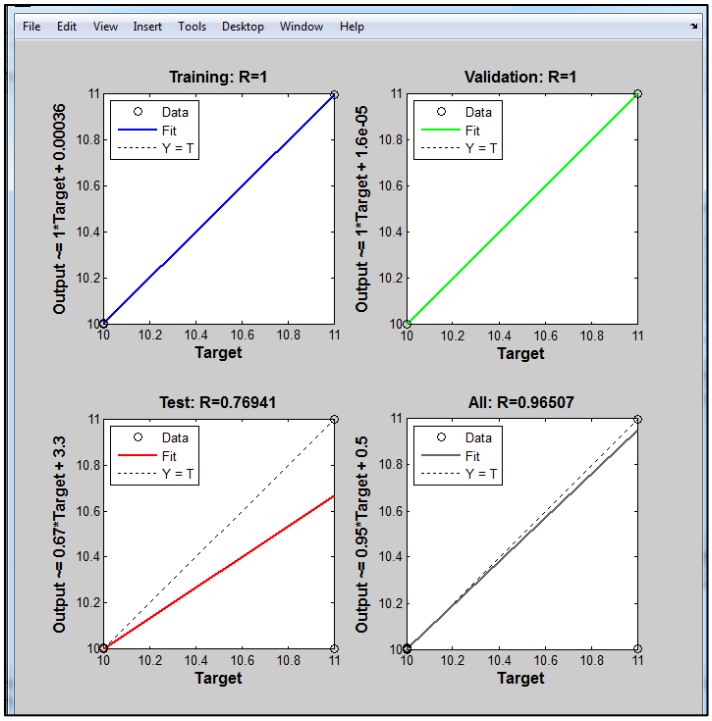
الشكل 9. شبكة من عدة طبقات بتغذية متقدمة

حاولنا أن نجري بعض التحسينات على الشبكة السابقة من خلال إنشاء شبكة جديدة من النوع feed–forward back prop مؤلفة من طبقتين مخفيتين تتألف كل منها من 10 عصبونات ونقوم بتدريب الشبكة على 1000 epochs

ويكون أداؤها:



الشكل 10. أداء الشبكة 2

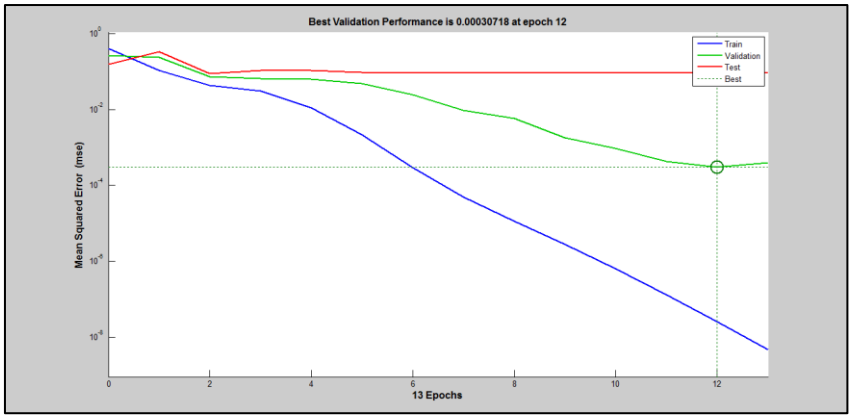


الشكل 11. Network2 Regression

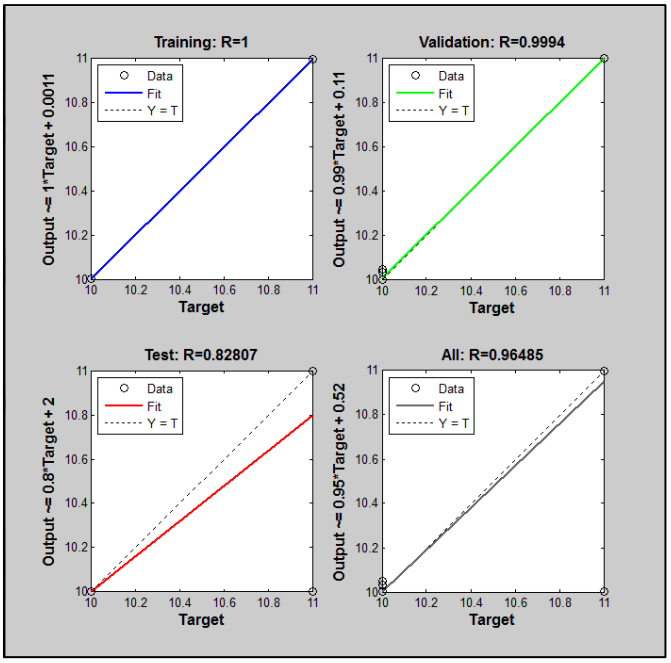
استغرق تعليم هذه epochs 29 بمدة 3 ثانية

بعد ذلك نقارن بين الخرج الذي أعطته الشبكة والخرج المطلوب لنلاحظ أن النتائج قريبة من النتائج الفعلية مع وجود خطأ مرتكب قيمته العظمى 0.0286

النتيجة جيدة ومقبولة ولكن سنحاول تحسين النتائج من خلال زيادة عدد العصبونات في الطبقات المخفية الى 30 عصبوناً في كل منها، لتكون النتائج كما يلي:



الشكل 12. أداء الشبكة 3



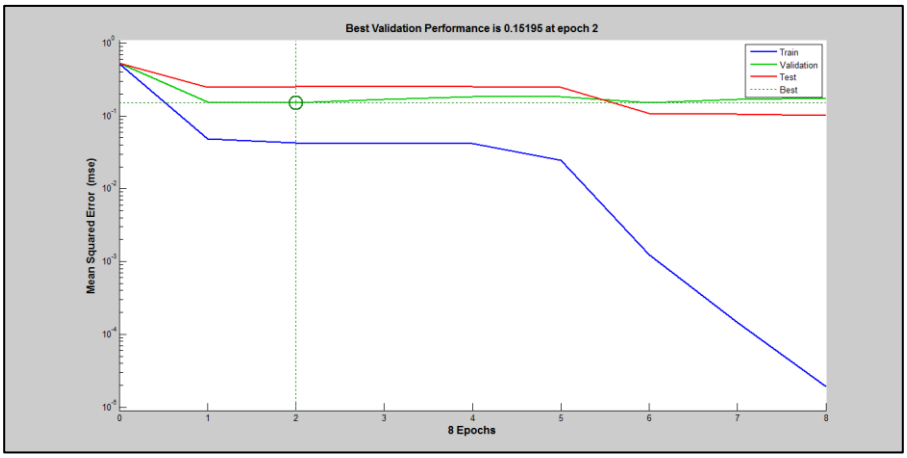
الشكل 13. Network3 Regression

انتهى تدريب شبكة بعد 13 epochs بمدة 6 ثواني ، وأعطت خطأ مرتكباً قيمته

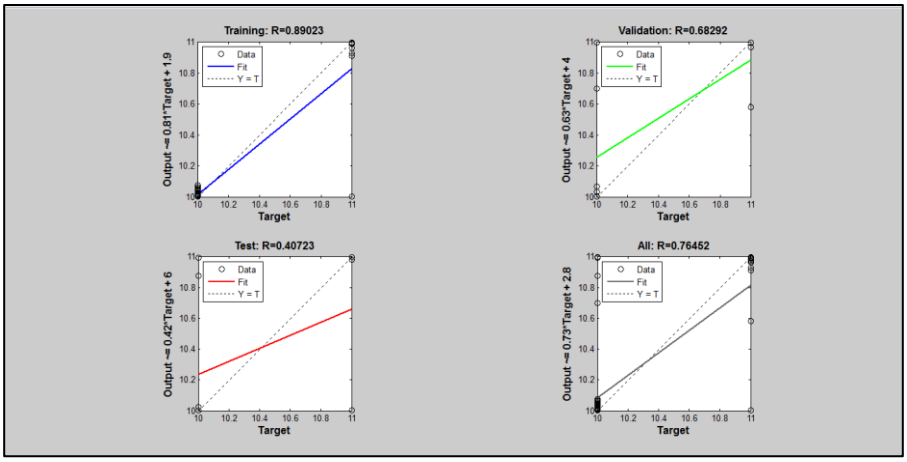
0.0130

النتائج في هذه التجربة جيدة جداً فقد تم تعليم الشبكة خلال زمن قياسي ، كما استطعنا أن نخفض قيمة الخطأ المرتكب وحصلنا على نتائج تصنيف مطابقة تقريباً للخرج المطلوب.

وفي المرحلة الأخيرة من التجريب سنعدل عدد العصبونات لنزيدها إلى 100 عصبون في كل طبقة ليكون الخرج كما يلي :



الشكل 14. أداء الشبكة 4



الشكل 15. Network4 Regression

نتيجة محاكاة تلك الشبكة ظهرت كما يلي :

```
sim(network4,testdata)
ans =
  Columns 1 through 5
   10.7601   11.0000   10.0010   10.0413   10.2834
  Columns 6 through 10
   10.0036   10.0077   10.0219   11.0000   10.0017
  Columns 11 through 15
   10.0011   10.0006   11.0000   10.0067   10.2780
  Columns 16 through 20
   10.0004   11.0000   11.0000   11.0000   11.0000
  Columns 21 through 25
   10.9994   11.0000   10.9999   10.9213   10.5260
  Columns 26 through 30
   10.9999   10.9976   11.0000   10.8404   10.9631
```

الشكل 16. محاكاة الشبكة 4

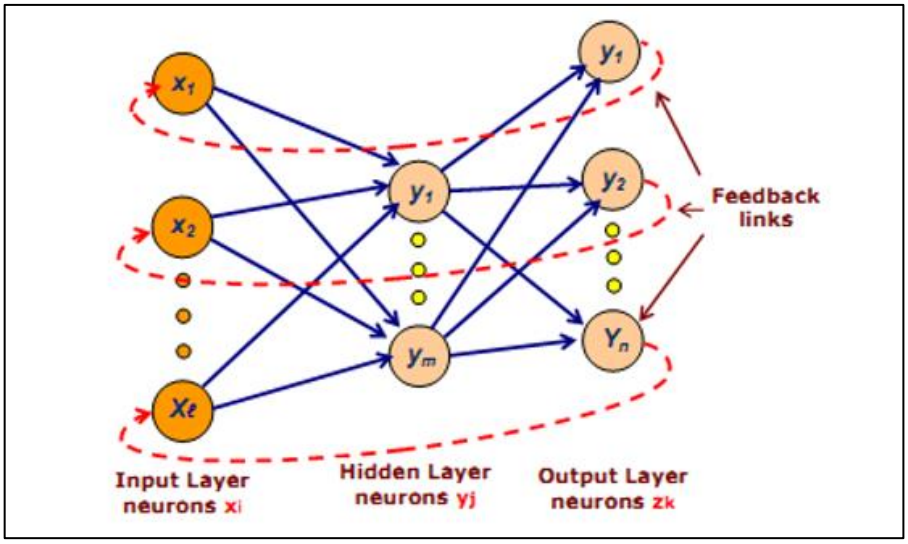
تمت عملية التعليم خلال ثانيتين و 8 epochs

الا أن قيمة الخطأ ازدادت في هذه التجربة فقد بلغت 0.482 ،لذلك نلاحظ أن خرج الشبكة قد ساء بالمقارنة مع الحالة السابقة، وبالتالي يمكننا أن نستنتج من ذلك أن زيادة عدد عصبونات الطبقة المخفية يمكن أن يحسن من النتائج ولكن لا يجب زيادة عددها إلى حد كبير لأنه قد ينعكس سلبيا على أداء الشبكة، لذلك حاولنا تحسين الشبكة من خلال زيادة عدد الطبقات المخفية إلى طبقتين كما وضحنا سابقاً وذلك لأن زيادة عدد الطبقات المخفية يساعد في زيادة كفاءة خاصية التحويل غير الخطي بين الدخل والخرج.

c. Recurrent Network

تتميز هذه الهيكلية عن سابقاتها بوجود اتصال من عصبونات طبقة الخرج إلى عناصر الدخل ما يسمى بالتغذية الراجعة أو العودية

يصعب تعليم الشبكة عند استخدام هذه الهيكلية ، لذا لها تطبيقات خاصة لاستخدامها.



الشكل 17. شبكة ذات تغذية راجعة

5. تعليم الشبكة :

يتمحور المفهوم الاساسي للشبكات العصبونية حول ألية تعليم الشبكة سواء بنماذج جديدة أو معروفة سابقاً.

تصنف طرق التعليم وفق 3 أنواع :

- التعلم بإشراف
- التعلم من غير إشراف
- التعلم بالتعزيز

5.1 التعلم بإشراف:

يعتمد هذا النمط على وجود معلم للشبكة ، يقدم نماذج الدخل للشبكة وكما يعطي نموذج الخرج المتوقع[3].

تستخدم نماذج الدخل لتعليم الشبكة ، وعملية التعليم تعتمد على المقارنة بين الخرج المتوقع والخرج الذي اعطته الشبكة وفقاً لنموذج الدخل ،ويتم حساب قيمة الخطأ المرتكب.

تتعدل قيم الأوزان وفقا للخطأ المرتكب الذي أعطته الشبكة وذلك بهدف تحسين النتائج.

هناك العديد من الدراسات التي اعتمدت هذا النهج منها : دراسة أعدت عام 2004 اعتمدت على استخدام خوارزمية Naïve Bayes[13] لاجراء التصنيف ، ودراسة أخرى تمت في عام 2013 اعتمدت على خورزمية Support Vector Machine[14] . إن الدراستين السابقتين اعتمدتا التحليل الديناميكي ، أما التحليل الستاتيكي اجريت دراسة عام 2016 اعتمدته وقام الباحثون باستخدام خورزمية Random Forest[15] لبناء المصنف .

عادة نستخدم التعلم بإشراف لتسريع أداء الشبكة لذا اعتمدناه في هذه الدراسة ، حيث قمنا بتجميع الميزات واستخدام خوارزمية اشجار القرار لتعليم الشبكة وإجراء التصنيف.

5.2 التعلم بدون إشراف:

في هذا النمط من التعلم لا يوجد معلم للشبكة ولا تعطى نماذج متوقعة للخرج ، وإنما تأخذ الشبكة الدخل المطلوب وتقوم بإيجاد علاقة بين العناصر المدخلة ومن خلالها تعطي الخرج الصحيح.

غالبية الطرق الشهيرة في استخراج الميزات تستخدم خوارزميات التعلم بدون إشراف ، وذلك لتمثيل الميزات أفضل ما يمكن.

ومن أهم طرق استخراج الميزات :

hierarchical, unary variable removal، Goodness evaluator, and Weighted Term Frequency.

5.3 التعلم بالتعزيز:

تعتمد هذه الطريقة على وجود معلم يعطي الشبكة نماذج الدخل ، ولكن دون إعطاء الخرج المتوقع ، وإنما يشير فقط للعصبون الذي أعطى الخرج الصحيح .

فتتم مكافأة العصبونات التي أعطت النتائج الأقرب للخرج الصحيح من خلال تعديل قيم أوزانها.

6. الخاتمة والتوصيات

لقد ناقشنا دراسة منهجية تستند إلى الدراسات الحديثة في الكشف عن التطبيقات الضارة لنظام أندرويد في المتاجر الرسمية والغير رسمية . لا تسلط هذه الدراسة الضوء على طرق و تقنيات الكشف المتنوعة سواء كانت ستاتيكية أو ديناميكية ، وإنما تناقش أيضاً التقنيات المختلفة التي لها القدرة على مواجهة الهجوم والأذى الذي

يتسبب التطبيق المشبوه من خلال الاعتماد على مجموعة من الميزات لبناء شبكة عصبونية تساعدنا في تحديد نوع وحالة التطبيق .

7. المراجع

[1] RIASAT, R2016-"A Survey on Android Malware Detection Techniques" .Institute of Software, Chinese Academy of Sciences, Beijing, China , 9p.

[2] Yajin ZHOU and Xuxian JIANG , 2012- "Dissecting android malware: Characterization and evolution In Security and Privacy (SP)" . 2012 IEEE Symposium on، pages 95-109.

[3] BENGIO, Y2009- "Learning deep architectures for ai. Foundations and trends in Machine Learning". 2(1):1-127p.

[4] SAXE and BERLIN , JK2015 – "Deep neural network based malware detection using two dimensional binary program features". In International Conference on Malicious and Unwanted Software (MALWARE), pages 11-20, Oct 2015.

[5] A. Sharma and S. K. Dash- "Mining api calls and permissions for android malware detection". In Cryptology and Network Security, pages 191-205. 2014.

[6] Kim, TaeGuen, et a- "A multimodal deep learning method for android malware detection using various features." IEEE Transactions on Information Forensics and Security 14.3 (2018): 773-788.

[7] Tobiyama, Shun, et al- "Malware detection with deep neural network using process behavior." 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC). Vol. 2. IEEE, 2016.

[8] Khan, Haider Adnan, et al- "Malware detection in embedded systems using neural network model for electromagnetic side-channel signals." Journal of Hardware and Systems Security 3.4 (2019): 305-318.

[9] HaddadPajouh, Hamed, et al- "A deep recurrent neural network based approach for internet of things malware threat hunting." Future Generation Computer Systems 85 (2018): 88-96.

[10] Daniel Bilar. ""Opcodes as predictor for malware". Int. J. Electron. Secur. Digit Forensic, 1(2):156–168, January 2007.

[11] Md. Enamul Karim, Andrew Walenstein, Arun Lakhotia, and Laxmi Parida. "Malware phylogeny generation using

permutations of code ". Journal in Computer Virology, 1:13–23, 2005

[12] Malicia project. http://malicia-project.com, 2012, Date last accessed 15-July-2014.

[13] Jeremy Z. Kolter and Marcus A. Maloof. "Learning to detect malicious executables in the wild". In Proceedings of the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD '04، pages 470–478, New York, NY, USA, 2004. ACM.

[14] Igor Santos, Felix Brezo, Xabier Ugarte-Pedrero, and Pablo G. Bringas." Opcode sequences as representation of executables for data-mining-based unknown malware detection ". Information Sciences, 231:64 – 82, 2013. Data Mining for Information Security.

[15] Ashu Sharma and Sanjay Kumar Sahay." An effective approach for classification of advanced malware with high accuracy". International Journal of Security and Its Applications, 10(4), 2016.