تحسين موثوقية شبكات ال OCDMA1اعتماداً على رموز الترابط المتبادل المعدوم ZCCC والبوابات المنطقية

طالـــب الدراســات العليــا: حنان حسان

كلية: الهمك – جامعة: دمشق

الدكتور المشرف: جمان أبو جيب + د. عبد الكريم السالم

ملخص

يتزايـد يومـاً بعـد يـوم أهميـة الأمـن فـي شـبكات الاتصـالات الضـوئية حيـث يمكـن للمتنصت اعتراض البيانات باستخدام المعدات المتطورة ويمكنه أيضاً الاستفادة من هذه البيانات. في هذه البحث، يتم تحسين الأمن من خلال دمج رموز ذات ارتباط متبادل معدوم مع بوابة EX–OR الضوئية المستخدمة في عملية التشفير. يتم ترميز البيانات المرسلة عبر شبكة OCDMA ثم تشفر لحمايتها من المتنصتين أو أي مهاجمين آخرين.

تم في هذا البحث دراسة أداء الشبكة قبل و بعد تعرضها للتنصت باستخدام برنامج ال optisystem17 وتم أيضاً تقييم أداء النظام المقترح من خلال معدل خطأ البت BER وعامل الجودة وشكل مخطط العين وذلك على مسافات إرسال مختلفة. وقد تبين من النتائج أن عملية الترميز باستخدام رموز ZCC تضمن جودة عالية وتحقق أداء أفضل بالمقارنة مع رموز أخرى ذات بعد واحد. بالإضافة إلى ضمان موثوقية تامة للمعلومات المرسلة من خلال استخدام بوابة EX–OR.

الكلمات المفتاحية: شبكات النفاذ المتعدد بتقسيم الرمز الضوئي(OCDMA)، بوابة EX–OR الضوئية، رموز ذات ترابط متبادل معدوم(ZCCC)، معدل خطأ البت(BER)، عامل الجودة.

Confidentiality Enhancement of OCDMA Networks Based on Zero-Cross Correlation Codes and Logic Gates

Eng. Hanan Hassan Dr. Jouman Abou Jeib Pro. Abdulkarim Assalem

Abstract

The importance of security in optical communications networks is increasing day by day since an eavesdropper can intercept data using advanced equipment and can also tap this data. In this paper, confidentiality has been improved by incorporating zero cross-correlation codes with an optical EX-OR gate using in the encryption process. The data in the OCDMA network is encoded and then encrypted to protect data from eavesdroppers and any others attackers.

In this work, the network performance before and after being eavesdropped using optisystem17 is analyzed , and evaluated in term of bit error rate (BER), quality factor and eye diagram at different transmission distances is also analyzed. The results showed that the encoding process using ZCC codes has higher quality and better performance compared to other 1D codes, in addition to ensuring the confidentiality of the transmitted data by using EX-OR gate.

Key Words: Optical Code Division Multiple Access Networks (OCDMA Networks), Optical EX-OR Gate, Zero Cross Correlation Code (ZCCC), Bit Error Rate (BER), Q-factor.

1- مقدمة:

توفر أنظمة النقل في شبكات الاتصالات خدمة نقل البيانات للعملاء والمشتركين، وتميز معاملات مثل الأداء والأمن والموثوقية نوعية خدمة النقل. أولت أنشطة البحث في شبكات الاتصالات الآمنة اهتماما ضئيلا للمقايضة بين متطلبات الأمن وغيرها من متطلبات جودة خدمات الاتصال، في حين أن الأمن يشكل مصدر قلق رئيسي في نظم الاتصالات الجماعية الآمنة سواء في الشبكات اللاسلكية أو الضوئية على حد سواء فإن آليات الأمن المستخدمة كثيراً ما تكون لها آثار ضمنية على أداء النظام[1] .

على الرغم من المزايا المهمة لنظام OCDMA، فإنه يعاني بعض القيود أيضًا، حيث يعاني الOCDMA من تداخل وصول متعدد Multiple Access Interference، يتم ضبط المستقبل المرغوب فقط للكشف عن إشارة البيانات الخاصة به مع الأخذ في الاعتبار الإشارات الأخرى كضجيج. يزيد MAI من معدل خطأ البت BER مع زيادة عدد المستخدمين. يمكن حل هذه القيود المفروضة على نظام OCDMA من خلال زيادة وزن وطول الرمز، وباستخدام الترامیز ذات الترابط المتبادل شبه المعدوم[2].

2-هدف البحث وأهميته:

يهدف هذا البحث إلى تحسين موثوقية المعلومات المرسلة في الشبكات الضوئية باستخدام النفاذ المتعدد بتقسيم الرمز من خلال الدمج بين بوابات EX-OR الضوئية التي تستخدم لعملية التشفير وفك التشفير ومرمزات ومفككات ترميزWDM لتوليد رموز ذات ترابط متبادل معدوم ZCC Code، بالإضافة إلى تحليل ودراسة أداء الطرق المستخدمة وأثرها على جودة البيانات المرسلة.

3-منهجية البحث وأدواته:

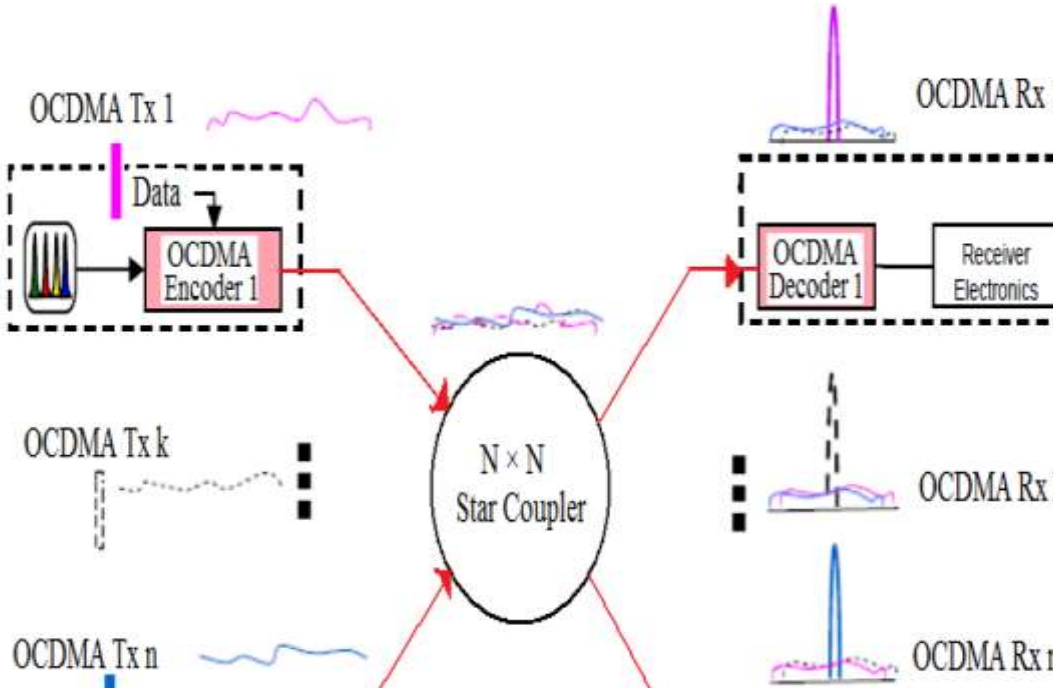
في برنامج المحاكاة Optisystem 17 تمت محاكاة التصميم الجديد من شبكات النفاذ المتعدد الضوئية بتقسيم الرمز، وتم التركيز في برنامج المحاكاة على تحليل مخطط العين ومعدل خطأ البت بالإضافة إلى عامل الجودة كمقاييس مهمة في التحليل والتنبؤ

عن مستوى احتمال تعرض التصميم الجديد للشبكة للأخطاء وبناءً على نتائج المحاكاة تم التوصل لإثبات الفرضيات والتأكد من صحتها.

4-الأساسيات النظرية:

4-1 النفاذ المتعدد بتقسيم الرمز الضوئي OCDMA:

الوصول المتعدد بتقسيم الرمز الضوئي OCDMA هي تقنية لتحقيق الإرسال المتعدد والوصول المتعدد عن طريق الترميز في المجال الضوئي الذي يدعم عمليات الإرسال المتزامنة وغير المتزامنة. لقد أصبحت تقنية واعدة لتنفيذ مختلف أنواع الاتصالات الضوئية التي تستخدم معالجة الإشارات الضوئية التي تجمع بشكل مباشر بين مزايا أجهزة معالجة الإشارات الضوئية والألياف الضوئية. يوضّح الشكل (1) البنية العامة لشبكة OCDMA. من بين المزايا الأخرى التي توفرها OCDMA إمكاناتها العالية لتعزيز أمن المعلومات. يتعامل الأمن مع البيانات المشفرة بطريقة يصعب فك تشفيرها بدون بعض المعلومات السرية، حتى لو كان شكل البيانات المشفر سهل القراءة .لذلك فقد حظي OCDMA باهتمام كبير في السنوات الأخيرة بسبب ميزاته المتعددة [4] .الفرق الرئيسي لأنظمة O-CDMA عن CDMA اللاسلكية هو بنية الرمز. يتم تعديل شدة الإشارة الضوئية بشكل أساسي، وبالتالي فإن الشرائح الموجودة في نظام O-CDMA تتبدل بين "1" و "0" بدلاً من "-1" و "+1".



الشكل (1): البنية العامة لشبكة OCDMA[3]

يمثل الشكل السابق بنية شبكة OCDMA التي تتألف من n مرسل و n مستقبل، تُجمع إشارات جميع المستخدمين باستخدام Star Coupler ثم ترسل عبر الليف الضوئي بعد ترميزها ياستخدام مرمز OCDMA، ليتم في جهة الاستقبال استقبالها و فك ترميزها ومن ثم تحويلها إلى إشارة كهربائية ليتم دراستها وتحليلها.

2-4 نظام OCDMA المتزامن وغير المتزامن :

يمكن تصنيف أنظمة OCDMA إلى فئتين: متزامن وغير متزامن. تتمتع الأنظمة المتزامنة بسعة أعلى ولكن على حساب كونها أنظمة أكثر تعقيدًا ، بينما تدعم الأنظمة غير المتزامنة عددًا محدودًا من المستخدمين ولكنها لا تتطلب أي نوع من المزامنة. من الجدير بالذكر أن عدم التزامن هو أحد أكثر الميزات إثارة للاهتمام في OCDMA.يمكن تطبيق أنظمة OCDMA غير المتزامنة على سيناريوهات مختلفة للشبكة على سبيل المثال، شبكة المنطقة المحلية وأنظمة الوسائط المتعددة ، ويمكن زيادة قدرة الأنظمة غير المتزامنة بمساعدة الرموز ثنائية الأبعاد وثلاثية الأبعاد. على

سبيل المثال، من الممكن استخدام مخططات ترميز ثنائية الأبعاد تعتمد على مزيج من الزمن أو القطاع الفضائي أو انتشار الطول الموجي لزيادة قدرة النظام[5].

4-3 نظام OCDMA المترابط وغير المترابط :

تصنف أنظمة OCDMA على أنها مترابطة وغير مترابطة حيث تعتمد الأنظمة غير المترابطة على تعديل الشدة والكشف المباشر، تجعل عملية الكشف المباشر الإجراء بسيطاً ويكون جهاز الاستقبال بسيطاً قليل التكلفة. يكتشف الكاشف الضوئي استطاعة الإشارة الضوئية ولا يكشف تغيرات الطور اللحظية للإشارة الضوئية وبالتالي يمكن استخدام تقنيات معالجة الإشارات غير المتماسكة لمعالجة تسلسلات الرموز المؤلفة من الأصفار والواحدات والتي تقيد نوع الرمز في أنظمة OCDMA[6].

في أنظمة OCDMA المترابطة، تعد معلومات الطور للحامل الضوئي أمراً بالغ الأهمية لعملية كشف الإشارة. نظراً لطبيعة النقل في الألياف الضوئية وتأثيراتها غير الخطية تصبح عملية تصميم المستقبل أكثر تعقيداً ومع ذلك يتفوق أداء النظام المترابط على غير المترابط لأنَّ المستقبل أكثر حساسية لنسبة الإشارة إلى الضجيج مما يجعل أداء النظام أفضل بشكل عام.

4-4 موثوقية البيانات:

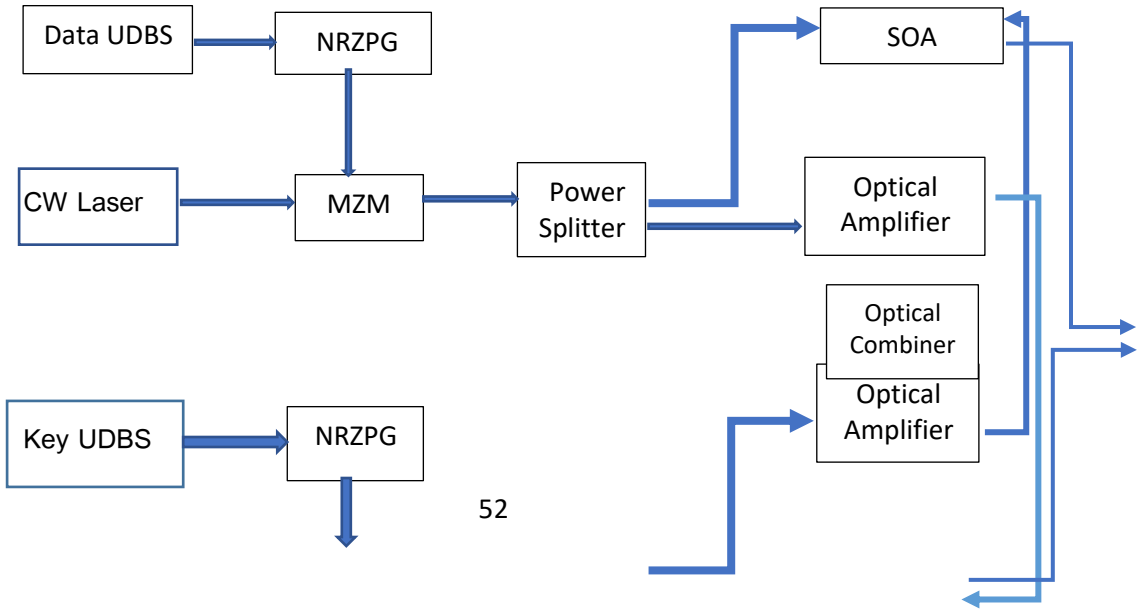
تكفل موثوقية البيانات عدم الكشف عن البيانات السرية للأشخاص غير المصرح لهم. وتكفل خصوصية البيانات أن لا تتوافر لهؤلاء الأشخاص غير المصرح لهم الوسائل التقنية للوصول إليها. تحمي تقنيات التشفير سرية نقل البيانات عن طريق تشفير البيانات الأصلية إلى نص تشفير. فإذ كان من المستحيل تقريباً قراءة البيانات، فإنها لم تعد مناسبة لأي مستمع (متنصت) . وقد تم اقتراح العديد من نُهُج التشفير بما في ذلك تشفير الإشارات الضوئية بأكملها على استخدام بوابات EX-OR الضوئية المستخدمة في هذا البحث أو مفاتيح التشفير المقطعة طيفياً [7].

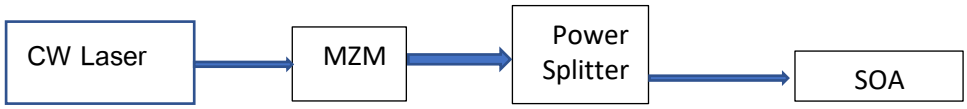
4-5 بوابة EX-OR :

تمّ تصميم بوابة EX-OR باستخدام المضخمات البصرية لأنصاف النواقل SOA والتي تؤدي الوظيفة المنطقية لهذه البوابة ويمكن أن تعمل مع سرعة بيانات تصل حتى 10 Gb/s. تتألف هذه البوابة من مدخلين فقط، عندما يتماثل المدخلين سواء (1) أو (0) سوف يكون خرج بوابة EX-OR مساوياً الصفر ومن ناحية أخرى إذا كان المدخلين مختلفين سنحصل على خرج يساوي الواحد، حيث كل من المدخلين عبارة عن سلسلة من بتات بيانات NRZ [8].

4-6 تصميم بوابة EX-OR باستخدام ال Optisystem:

يتم استخدام تسلسل بتات معرف من قبل المستخدم User Defined Bit Sequence تمثل تسلسل بيانات المستخدم وتسلسل المفتاح، يستخدم المعدل Mach Zender لتعديل تسلسل البتات وتحويلها إلى إشارة ضوئية، يتم استخدام SOA للحفاظ على الوظيفة المنطقية ويتم استخدام مضخم ضوئي لتصخيم الإشارة، كما هو موضّح بالشكل(2)[8].





الشكل(2): بنية بوابة EX–OR[8]

يوضّح الشكل السابق بنية بوابة EX–OR الضوئية التي تتألف من المكونات التالية:

مولد تسلسل بتات محدد من قبل المستخدم (Data User Defined Bit Sequence Data UDBS):

مولد نبضات مع عدم العودة إلى الصفر Non_Return_to_Zero Pulse Generator(NRZPG):

ليزر إشارة مستمرة لتوليد إشارة الحامل الضوئي (Continous Wave Laser CW Laser):

معدل ماك–زيندر (MZM): Mach-Zehender Modulation

مقسم ضوئي

Power Splitter :

مضخم ضوئي لأنصاف النواقل مسؤول عن الوظيفة المنطقية لبوابة EX–ORSemiconductor Optical Amplifier(SOA) :

مضخم ضوئي

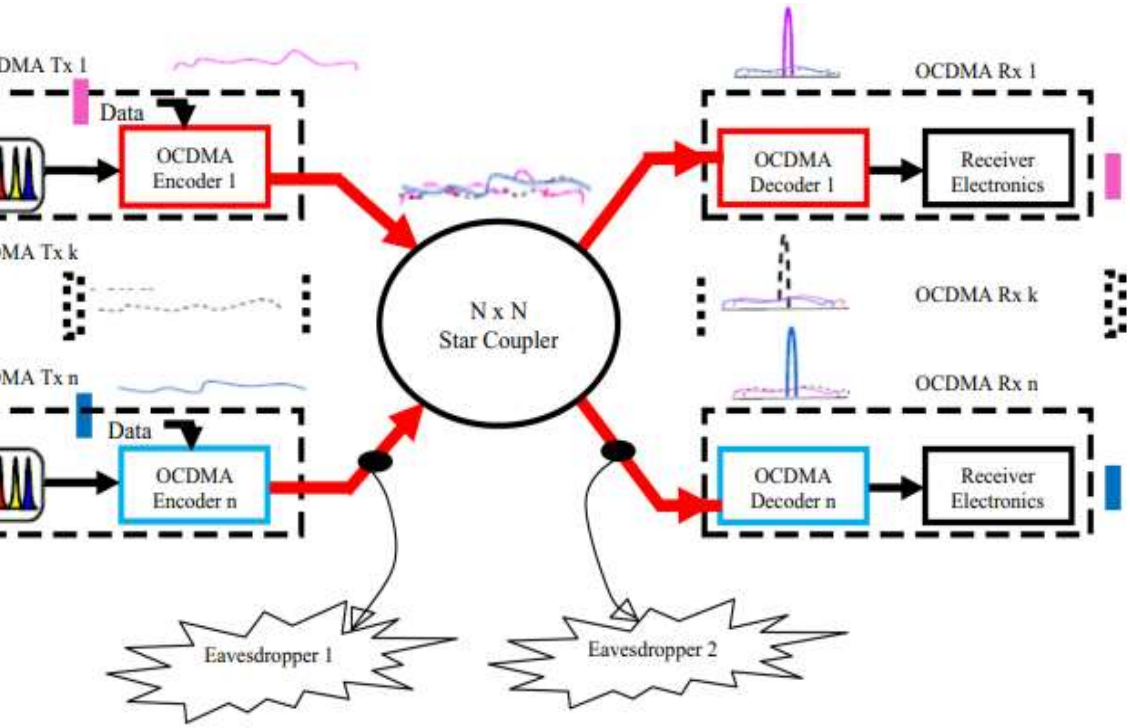
Optical Amplifier :

مولد تسلسل بتات محدد من قبل المستخدم لتوليد مفتاح التشفير: Key User Defined Bit Sequence(UDBS)

جامع ضوئي

Optical Combiner :

يمكن أن تتأثر درجة الأمن في أي تحقيق أمني تأثرا قويا بالعديد من الافتراضات. وتشمل هذه الافتراضات إجراء عمليات التنصت في المواقع المبينة في الشكل (3). والمهاجمون (المتسمعين أو المتنصتين) أذكياء تكنولوجياً مع معرفتهم للإشارات التي تنتقل في شبكات CDMA الضوئية (أي بنية الشبكات ، وأنواع الإشارات ، ومعدلات البيانات، ونوع الترميز ، وهيكل الرموز ، والتزامن، وما إلى ذلك)[1].



الشكل(3) شبكة OCDMA متعرضة للتنصت[9]

يوضّح الشكل السابق شبكة OCDMA تتعرض للهجوم من قبل المتنصتين وذلك بعد تجميع إشارات المستخدمين وإرسالها عبر الليف الضوئي.

4-7 التنصت في الشبكات الضوئية:

تُعد الشبكات الضوئية عرضة لعدة أنواع من الهجمات، التي تهدف عادة إلى تعطيل الخدمة أو الحصول على وصول غير مصرح به إلى البيانات المنقولة(التنصت)، وعلى الرغم من أن الألياف الضوئية محصنة ضد التداخل الكهرومغناطيسي ولا تشع إشارات تحمل إلى البيئة، فإن تعرض الشبكات الضوئية للتنصت يشكل تهديدا أمنيا كبيرا حيث يهدف التنصت بشكل عام إلى الوصول غير المصرح به إلى البيانات من أجل جمع أو تحليل حركة مرور البيانات والوصول إلى المعلومات.

توجد طريقة شائعة لتحقيق هجمات التنصت وهو الوصول مباشرة إلى القناة الضوئية عن طريق التنصت على الألياف، أجهزة التنصت التي يمكن وصلها على الألياف وتسبب الانحناءات الدقيقة لتسرب الإشارات ووصولها للمتنصت يمكن الوصول إليها بسهولة في السوق. وعلاوة على ذلك، أجهزة التنصت القائمة تسبب تخميداً أقل من 1dB ويمكن أن تحصل دون أن يتم الكشف عنها عادة من قبل أنظمة إدارة الشبكات ، ومن الواضح أن مثل هذه الاكتشافات تتطلب نظام مراقبة نشط يعمل عبر الشبكة.

هناك طريقة أخرى ممكنة للوصول إلى القناة عن طريق مراقبة المنافذ، والتي عادة ما تكون موجودة في مكونات الشبكة المختلفة مثل المضخمات، مفكك التجميع، المبدل الانتقائي لطول الموجة. يتم عكس الإشارة الضوئية بواسطة مقسم ضوئي للسماح باتصال أجهزة المراقبة دون انقطاع حركة تدفق البيانات. من خلال الوصول إلى الموقع، يمكن للمهاجم استخدام هذه المنافذ للاستماع إلى حركة البيانات المنقولة [10].

4-8 النقر على الألياف الضوئية:

على عكس التصور الشائع فإن الألياف الضوئية ليست آمنة بطبيعتها من التنصت أو التنصل. الكم الهائل من المعلومات الحساسة والهامة والمرحّلة عبر الألياف هذه الأيام معرّضة للاختراق من قبل المتنصت والتسمع بطرق مختلفة. إن التنصت على الألياف عبارة عن عملية يتم من خلالها تعريض أمن الألياف الضوئية للخطر إما باستخراج أو حقن المعلومات (كالضوء). في الأساس التنصت على الألياف يمكن أن يكون تدخليا

وغير تدخلي. ويتطلب الأول قطع الألياف وإعادة توصيلها في آلية التنصت في حين يتحقق التنصت في النوع الثاني دون قطع الألياف أو التسبب في اضطراب الخدمة بصورة واضحة [11]. أوضحت الدراسات إن مجرد انحناء الألياف مع الحفاظ على سلامتها يكفي لتتبع تبادل المعلومات مع وجود فرصة ضئيلة أو معدومة للكشف عنها [12]، حيث تستطيع أجهزة التنصت بسهولة مراقبة الاتصالات من دون تغير ملحوظ في الإشارة التي في طريقها إلى المتلقي. وقد تم الإبلاغ عن عدد قليل فقط من حوادث التنصت على الألياف لأنه من الصعب جدا الكشف عن الألياف المستغلة في حين أن عملية التنصت نفسها بسيطة جدا.

5- أنظمة ترميز المطال الطيفي Spectral Amplitude(SAC-OCDMA) Coding:

يسمح OCDMA لعدة مستخدمين بنقل البيانات في وقت واحد عبر قناة اتصال بالليف الضوئي من خلال تخصيص عرض المجال الترددي المتوفر لكل مرسل في وقت واحد، يتم تخصيص تسلسل شريحة فريد لكل مرسل يتم توليده بواسطة مولد شبه عشوائي أو محدد من قبل المستخدم. يتم تجميع الإشارات المرمزة من أجهزة الإرسال المختلفة وإرسالها عبر الألياف الضوئية إلى المستقبل علماً أنه يتم استخدام وحدة فك الترميز لفك ترميز إشارة البيانات المطلوبة باستخدام نفس تسلسل الشريحة المستخدم من قبل المرسل المطلوب[13].

من أجل تنفيذ شبكة اتصالات بتقنية الOCDMA ، يلزم توفر طرق ترميز ذات أداء كافي. يتضمن الترميز ضرب بتات البيانات بتسلسل رمز إما في مجال الزمن أو في مجال الطول الموجي أو في مجال الفضاء الذي يشار إليه على أنه أحادي البعد. يمكن أيضًا استخدام مزيج من مجالي طول الموجة والفضاء ويشار إليه باسم ترميز ثنائي الأبعاد. يمكن أيضًا إجراء ترميز بثلاثة أبعاد وهو مجموعة من مجال الطول الموجي و الزمن و الفضاء أو مجال الطول الموجي و الزمن و الاستقطاب[14].

تعرف الرموز في هذه النوع من الترامیز بالمحددات الآتية (λ_c،W،L،N) حيث N هو عدد المستخدمين ، L طول الرمز ، W وزن الرمز، و λ_c هي قيمة الترابط المتبادل بالطور IPCC. طول الرمز (L) هو إجمالي عدد الشرائح المستخدمة من قبل كل مستخدم. الوزن (W) يمثل عدد الشرائح التي لها قيمة 1. يتم تعريف IPCC بين رمزين على أنه [15]:

$$\lambda_c = \frac{\sum_{j=1}^{L} a_j \cdot d_j}{} \quad (1)$$

لرموز اثنيين من المستخدمين $A = (a_1, a_2, a_3, \ldots . a_l)$ و $D = (d_1, d_2, d_3, \ldots . d_l)$ ، ذو طول (L) .

5-1 الرموز ذات الترابط المتبادل المعدوم ZCC codes:

يسمى الرمز بخاصية الترابط المتبادل المعدوم باسم Zero Cross-Correlation Code (ZCCC). لا يحتوي على أي تداخل في الأطوال الموجية بين أي مستخدمين. تم الإبلاغ عنه مع بناء الرمز ذو الوزن الثابت وأيضا مع الرمز متعدد الأقطار، ورمز الترابط المتبادل المعدوم المعدل بخاصية ZCC. يتم التخلص من MAI تمامًا باستخدام الرموز مع خاصية ZCC ولكن بمعدل طول رمز أطول يتطلب مصادر المجال العريض [15].

5-2 رمز الترابط المتبادل المعدوم ZCCC:

تتألف الرموز الضوئية من تسلسلات من الأصفار والواحدات ذات k مستخدم. نشير إلى القيمة العظمى للارتباط المتبادل بين رمزين ب λ_{max} و w وزن الرمز (عدد الواحدات في الرمز). مجموعة الرموز التي لها أقل ارتباط متبادل تدعم أكبر عدد من المستخدمين مع أصغر طول رمز وهذا يضمن جودة الخدمة المقدمة مع معدلات خطأ منخفضة لعدد محدد من المستخدمين. العقبة الرئيسية في التنفيذ الناجح لجميع الشبكات

الضوئية هي في الأساس MAI عندما يحاول جميع المستخدمين إرسال بياناتهم في وقت واحد. يمكن التغلب عليها عن طريق تصميم تسلسلات رموز تسبب أقل تداخل بين شرائح البيانات[16].

نأخذ تسلسلين مختلفين من الرموز: $A_i=\{A_0,A_1,A_2,\ldots\ldots,A_N\}$ و $B_i=\{B_0,B_1,B_2,\ldots\ldots,B_N\}$

وبالتالي يمكننا تعريف الترابط الذاتيauto correlation والترابط المتبادل cross correlation بالعلاقتين التاليتين على التوالي:

$$\lambda_a = \sum_{i=1}^{N} A_i \cdot A_{i+t} \qquad (2)$$

$$\lambda_c = \sum_{i=1}^{N} A_i \cdot B_{i+t} \qquad (3)$$

يمكن تعريف رمز ZCC من خلال هذه البارمترات: (L,W,C) حيث L يعبر عن طول الرمز W يعبر عن وزن الرمز وC تعبر عن سعة النظام.

العلاقة بين طول الرمز (L) وعدد المستخدمين (K) ومرتبة المصفوفة (N) يعطى بالعلاقة التالية:

عدد المستخدمين = مرتبة المصفوفة

طول الرمز = (مرتبة المصفوفة)^2 = (عدد المستخدمين)^2 وهذا يكافئ $L=N^2=K^2$

الخطوة الأولى: إنشاء مصفوفة مربعة A_N، حيث تمَ اقتراح (N=4) ينتج لدينا المصفوفة التالية:

$$A_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

الخطوة الثانية: تُطبق خاصية إزاحة الصفوف ول $N-1$ مرة ينتج لدينا الآتي:

$$A_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad A'_4 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

$$A''_4 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \qquad A'''_4 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

الخطوة الثالثة: تُكتب المصفوفة A_4 بالشكل التالي:

$$A_4 = \begin{bmatrix} r_1(A_4) \\ r_2(A_4) \\ r_3(A_4) \\ r_4(A_4) \end{bmatrix}$$

حيث $r_1(A_4)$, $r_2(A_4)$, $r_3(A_4)$, $r_4(A_4)$ تمثل السطر الأول والثاني والثالث والرابع في المصفوفة A_4 على التوالي وبالتالي يمكننا كتابة المصفوفات A'_4, A''_4, A'''_4 بالشكل الآتي:

$$A'_4 = \begin{bmatrix} r_1(A'_4) \\ r_2(A'_4) \\ r_3(A'_4) \\ r_4(A'_4) \end{bmatrix}, \quad A''_4 = \begin{bmatrix} r_1(A''_4) \\ r_2(A''_4) \\ r_3(A''_4) \\ r_4(A''_4) \end{bmatrix}, \quad A'''_4 = \begin{bmatrix} r_1(A'''_4) \\ r_2(A'''_4) \\ r_3(A'''_4) \\ r_4(A'''_4) \end{bmatrix}$$

الخطوة الرابعة: يُعاد تشكيل المصفوفات السابقة لمصفوفة ذات سطر واحد فينتج لدينا:

$$A_4 = [r_1(A_4) \ , \ r_2(A_4) \ , \ r_3(A_4) \ , \ r_4(A_4)]$$

$$A'_4 = [r_1(A'_4) \ , \ r_2(A'_4) \ , \ r_3(A'_4) \ , \ r_4(A'_4)]$$

$$A''_4 = [r_1(A''_4) \ , \ r_2(A''_4) \ , \ r_3(A''_4) \ , \ r_4(A''_4)]$$

$$A'''_4 = [r_1(A'''_4) \ , \ r_2(A'''_4) \ , \ r_3(A'''_4) \ , \ r_4(A'''_4)]$$

ينتج لدينا :

$$A_4 = [1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1]$$

$$A'_4 = [0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0]$$

$$A''_4 = [0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0]$$

$$A'''_4 =$$

$$[0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0]$$

الخطوة الخامسة: أخيرا من خلال الجمع بين هذه المصفوفات المعاد تشكيلها سنحصل على رمز ZCC الجديد:

$$ZCC = \begin{bmatrix} A_4 \\ A'_4 \\ A''_4 \\ A'''_4 \end{bmatrix}$$

ZCCC=

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Codewords ⟹

User1 = $lambda_1$, $lambda_6$, $lambda_{11}$, $lambda_{16}$

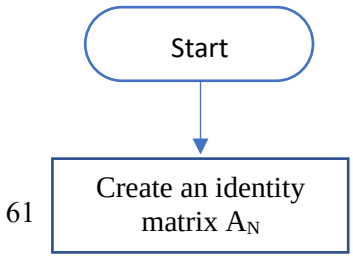
User2 = $lambda_2$, $lambda_7$, $lambda_{12}$, $lambda_{13}$

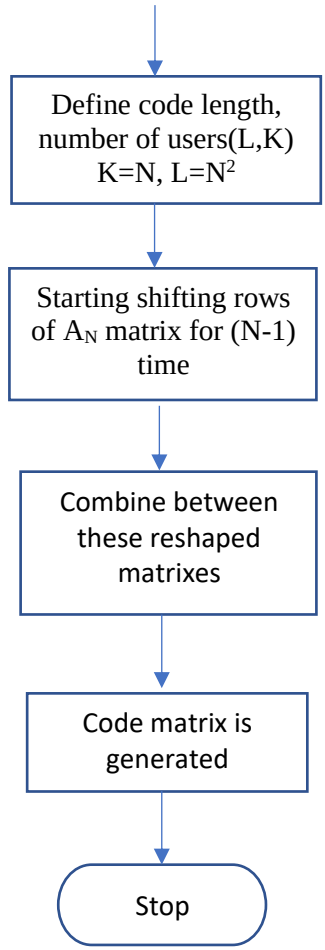
User3 = $lambda_3$, $lambda_8$, $lambda_9$, $lambda_{14}$

User4 = $lambda_4$, $lambda_5$, $lambda_{10}$, $lambda_{15}$

نلاحظ أنه من أجل 4 مستخدمين، قد حقق طول الرمز العلاقة السابقة $L=K^2=16$ [17]. وفقا للعلاقتين (1) و(2) وخصائص الرمز الناتج يتحقق لدينا: $\lambda_c = 0$.

يوضّح الشكل(4) المخطط الصندوقي للخوارزمية المتبعة لتوليد الرمز المبين في الخطوات السابقة.





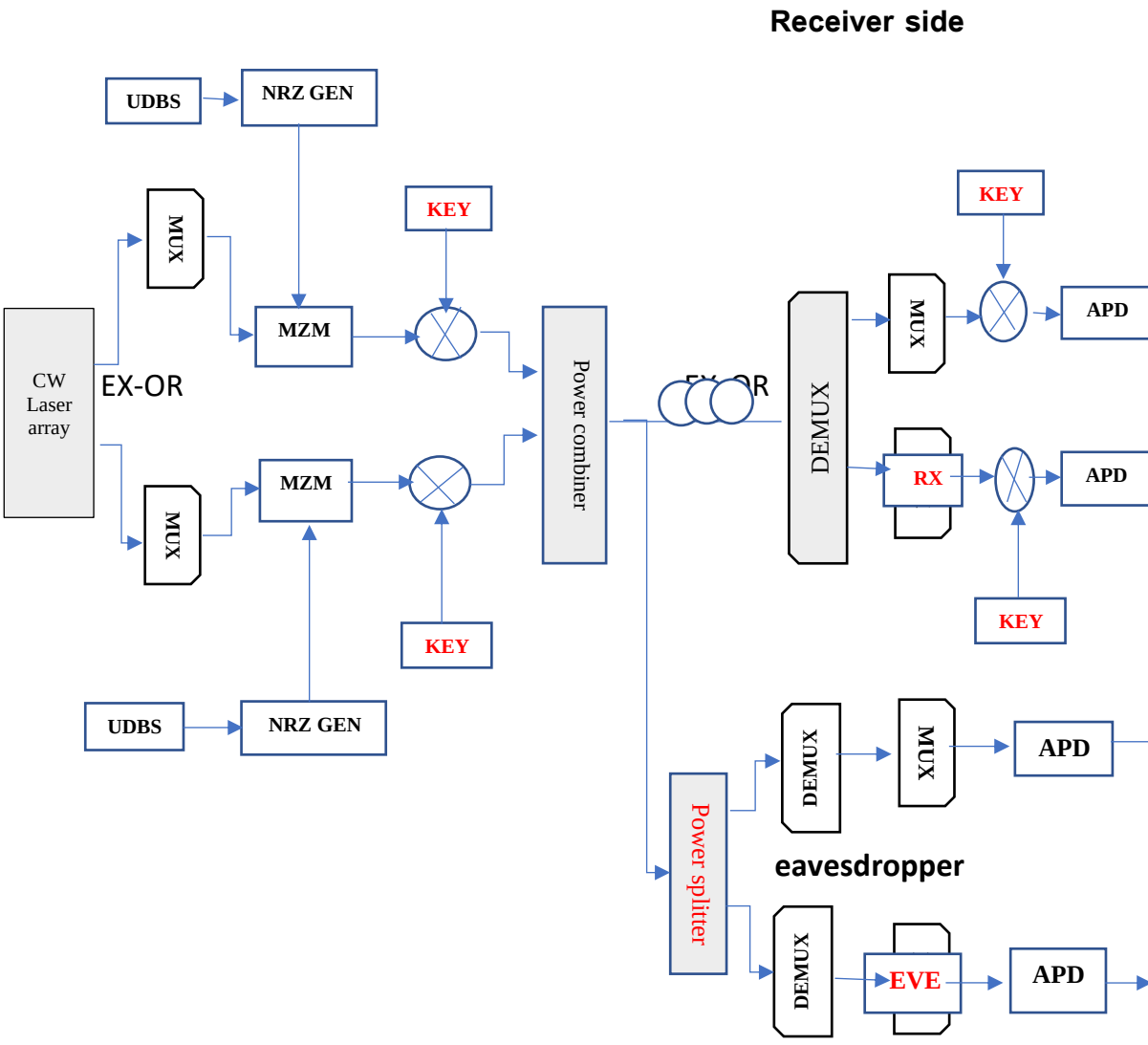
الشكل(4) المخطط الصندوقي لخوارزمية توليد الرمز

6- التطبيق العملي:

6-1 تصميم شبكة OCDMA:

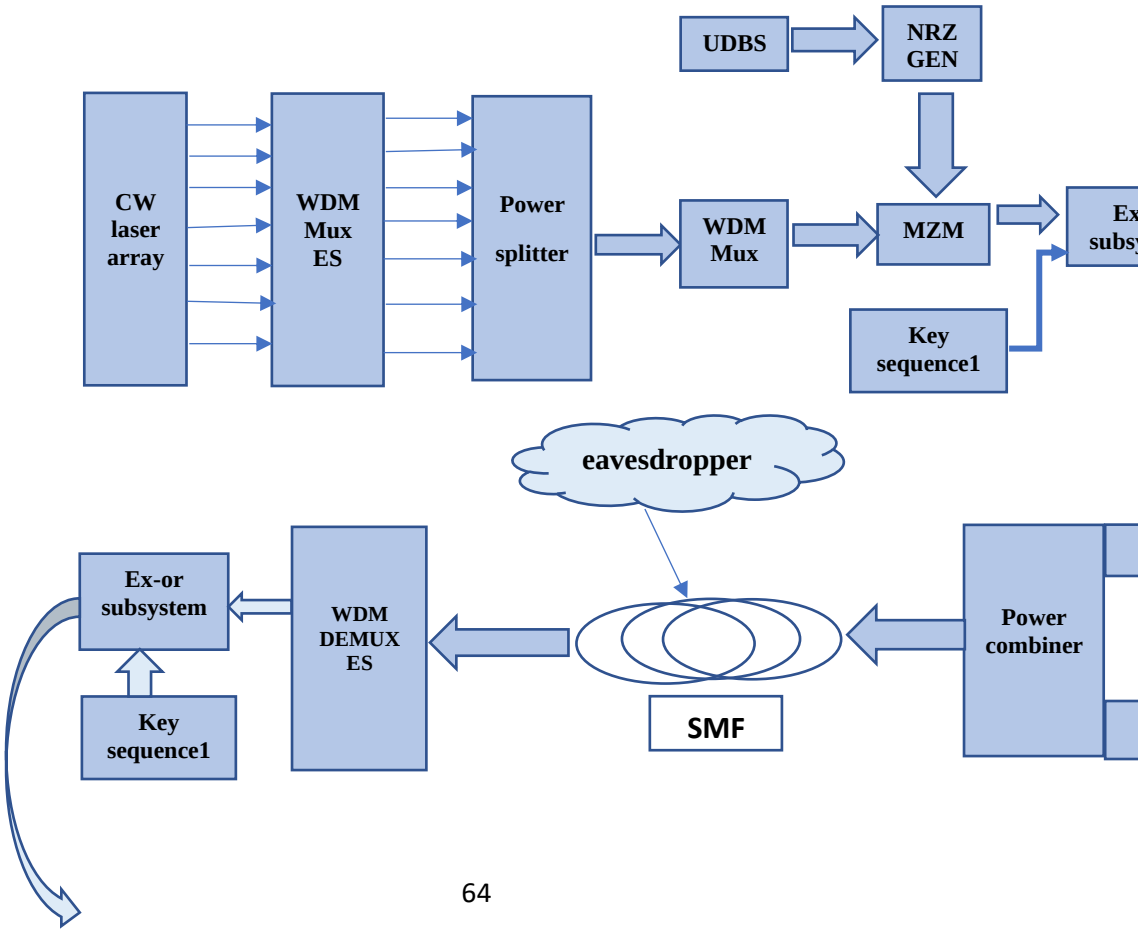
تم باستخدام المحاكاة الحاسوبية ضمن البرنامج الهندسي Optisystem ذو الإصدار 17 بناء شبكة OCDMA مكونة من 4 مستخدمين و16طول موجي، يستخدم WDM muxلتوليد الرمز الخاص بكل مستخدم، يتم تخصيص 4 أطوال موجية لكل مستخدم

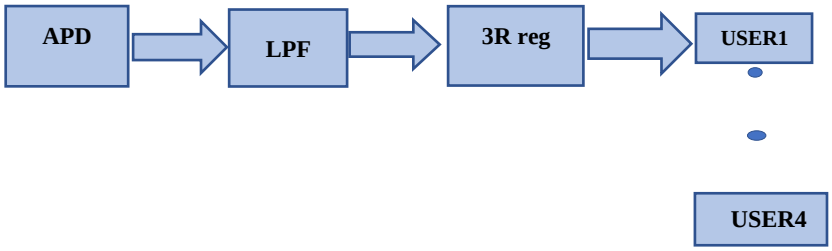
بناءً على رمز ZCC الوارد في الفقرة السابقة. يظهر الشكل (5) المخطط العام لشبكة OCDMA، ويظهر الشكل (6) المخطط التفصيلي لشبكة OCDMA. يتألف المخطط العام للنظام المقترح من ثلاثة أقسام، قسم المرسل وقسم المستقبل وقسم المتنصت، نلاحظ من المخطط كيف حاول المتنصت سرقة الإشارة من خلال النقر على الليف بعد قطع مسافة 50km .



الشكل(5) المخطط الصندوقي العام للنظام المقترح

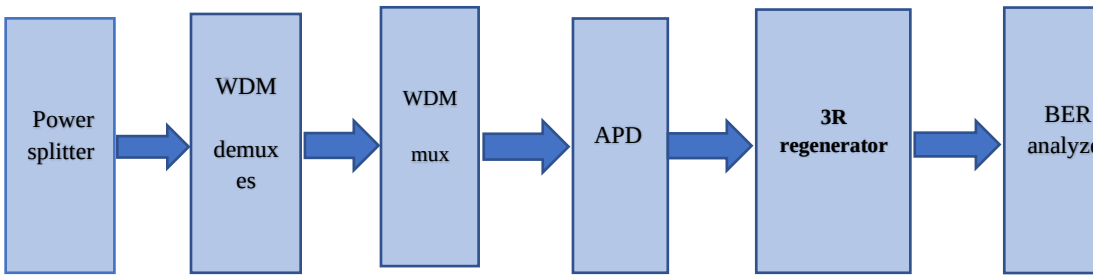
يوضح الشكل (6) المخطط التفصيلي للنظام المقترح، يستخدم هذا المخطط مولد بتات محدد UDBS لتوليد إشارة المستخدم التي يتم تعديلها بمعدل ماك-زيندر، بعد ذلك يتم استخدام بوابة EX-OR الضوئية لتشفير بيانات كل مستخدم بمفتاح تشفير مختلف بعد ترميزها باستخدام مرمز WDM ثم تجمع إشارات المستخدمين الأربع لترسل عبر ليف ضوئي وحيد النمط بتخامد 0.1dB/km لمسافة 100km لا تتطلب تضخيم والاكتفاء بطاقة الإشارة المولدة من المنبع الليزري CW laser array.





الشكل(6) المخطط التفصيلي لشبكة OCDMA المدروسة

في نهاية الليف يتم تفكيك الإشارة الضوئية الواردة باستخدام WDM DEMUX ES إلى أربع إشارات ليتم فك تشفيرها باستخدام بوابة EX–OR الضوئية وباستخدام نفس المفتاح الذي شفرت به ومن ثم عن طريق كاشف الضوء APD يتم تحويل الإشارة الضوئية إلى كهربائية ويتم ترشيحها باستخدام مرشح LPF ومن ثم يتم توليد تسلسل بتات البيانات الأصلية الخاصة بكل مستخدم من خلال 3R regenrator، لنحصل بعد ذلك على إشارة المستخدم في جهة الاستقبال. يوضح الشكل (7) البنية العامة للمتنصت، تتألف هذه البنية أولاً من مقسم ضوئي الذي يسمح بتوفير مسار لإشارة المتنصت إلى الليف الضوئي، ومن ثمَّ يتم تحليل الإشارة التي حصل عليها المتنصت إلى أربع إشارات باستخدام WDM DEMUX ES، يستخدم WDM MUX لإعادة توليد الرمز الخاص بكل مستخدم ومن ثم يتم تحويل الإشارة الضوئية إلى كهربائية وإعادة توليد بتات البيانات الأصلية من خلال 3R regenerator، ليتم أخيراَ تحليلها باستخدام BER analyzer.



الشكل(7) المخطط العام لبنية المتنصت

يظهر الجدول(1) العناصر المميزة لشبكة OCDMA ويبين الجدول (2) الأطوال الموجية وفقا لنمط الترميز ZCC حيث k=4.

الجدول (1) البارمترات الأساسية المميزة لشبكة OCDMA

بارمترات المحاكاة	القيمة
معدل البيانات	10 Gb/s
طول السلسلة	128 bits
المسافة الترددية	0.8 nm
طول الموجة المرجعي	1550 nm
طاقة المنبع الليزري	0 dB_m
عدد المستخدمين	4
نمط الترميز	ZCCC

حاكاة	القيمة
طول الليف الضوئي	100 km
ب	0.1 dB/km
تشتت الليف	16.75 Ps/nm/km
رة	NRZ
عدد الاطوال الموجية	16

يوضّح الجدول(2) الأطوال الموجية الخاصة بكل مستخدم وفقاً لنمط الترميز ZCCC.

الجدول (2) الأطوال الموجية وفقا لنمط الترميز ZCC حيث k=4

USER1	1550,1554,1558,1562nm
USER2	1550.8,1554.8,1558.8,1559nm
USER3	1551.6,1555.6,1556.4,1560.4nm
USER4	1552.4,1553.2,1557.2,1561.2nm

يوضّح الجدول(3) بيانات كل مستخدم بالإضافة إلى مفتاح التشفير.

الجدول(3) بيانات كل مستخدم ومفتاح التشفير

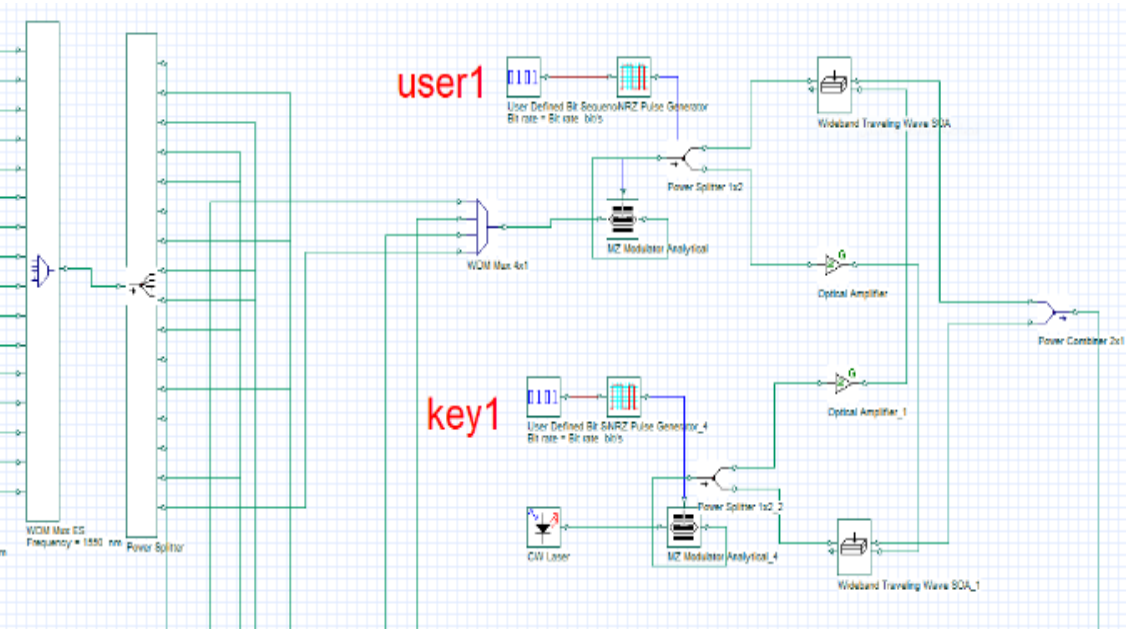
D1	100100111000	Key1	010010010110
D2	010110011011	Key2	110001110000
D3	101011100101	Key3	110011001110
D4	001001100111	Key4	110001011101

يفسر الجدول السابق بيانات كل مستخدم التي يتم توليدها باستخدام مولد بتات محدد من قبل المستخدم ومن ثم

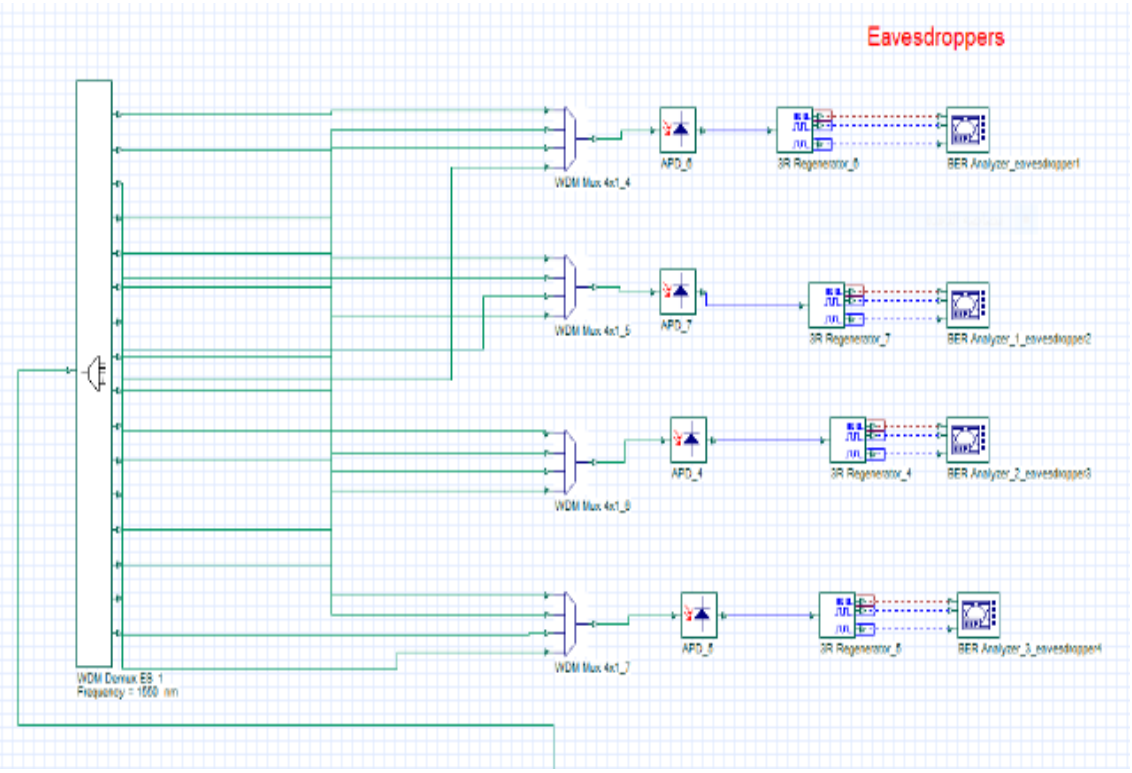
يتم ترميزها باستخدام رمز ZCCبالإضافة إلى مفتاح التشفير الذي يستخدم لتشفير بيانات كل مستخدم على حدى.

وفقا لمخطط الشبكة ولمميزات العناصر التي وردت سابقا تم بناء الشبكة باستخدام برنامج Optisystem17.

يبين الشكل (8) بنية مرسل واحد فقط باستخدام نمط الترميز ZCC، كذلك يوضح الشكل (9) قسم المتنصت.



الشكل(8) بنية مرسل واحد فقط باستخدام نمط الترميز (ZCC,K=4)

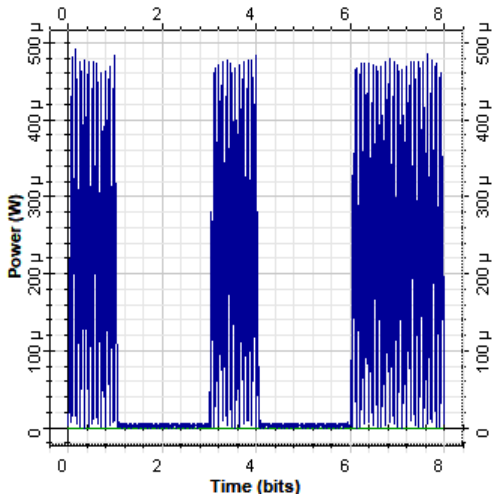


الشكل(9) بنية المتنصت

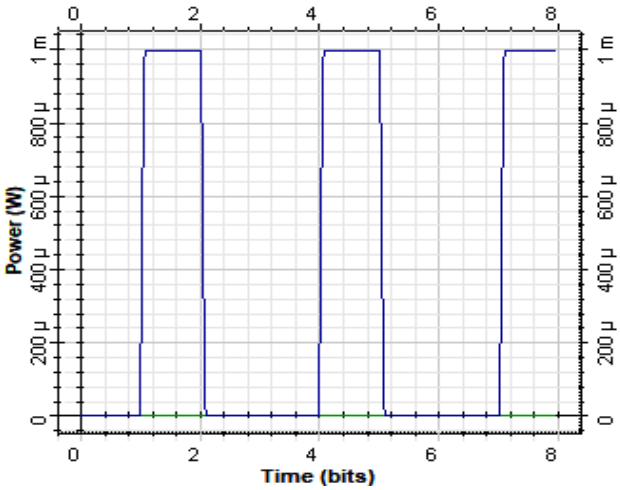
7- النتائج والمناقشة:

بعد تحديد مميزات شبكة OCDMA، تمت المحاكاة العملية وإظهار النتائج ومقارنتها، عملية المقارنة أُجريت اعتماداً على المحددات الأساسية من مخطط العين Eye Diagram وعامل الجودة Q Factor والأهم معدل خطأ البت BER.

بعد إجراء المحاكاة، تمّ استخلاص النتائج ومناقشتها على ثلاث أطوال للوصلات الضوئية المدروسة ابتداءً من مسافة 60km حتى مسافة 100km، تجدر الإشارة إلى أن القيم (BER=10^{-8}، Q Factor=6) تعد قيم الحد الأدنى المقبولة في أنظمة الشبكات الضوئية. يبين الشكل(10) بيانات كل مستخدم بعد عملية الترميز، ويبين الشكل(11) مفتاح التشفير الخاص بكل مستخدم،

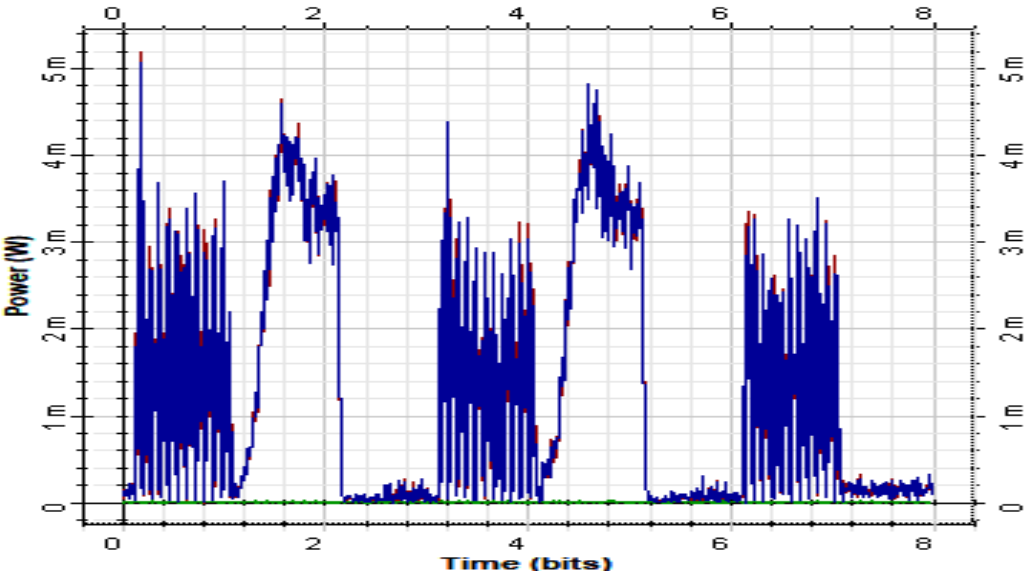


الشكل(10) إشارة بيانات المستخدم بعد الترميز



الشكل(11) مفتاح التشفير

وتظهر نتيجة بوابة EX-OR في الشكل(12).



الشكل(12) EX-OR لإشارة المستخدم ومفتاح التشفير

نلاحظ من الشكل (12) نتيجة تصميم بوابة EX-OR والتي تعطي قيمة مساوية للصفر عند تماثل المدخلين، وتعطي قيمة الواحد عند عدم تماثلهما.

يبين الجدول (4) معدل خطأ البت لكل مستخدم من المستخدمين الأربعة قبل عملية التنصت وبعدها، ونلاحظ زيادة معدل الخطأ في البت مع انخفاض عامل الجودة بعد محاولة التنصت عن قيمتها قبل عملية التنصت .

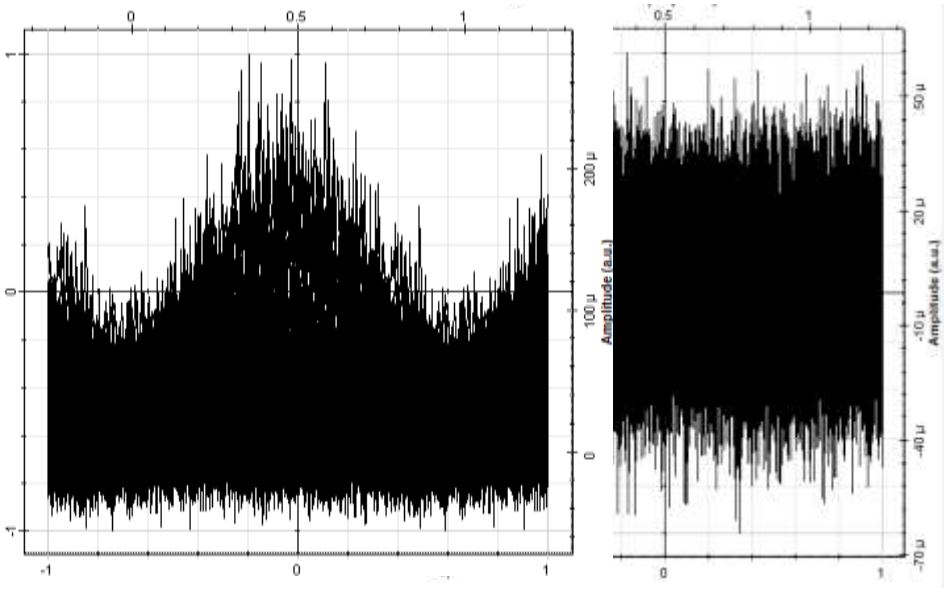
الجدول (4) معدل الخطأ في البت وعامل الجودة لكل مستخدم قبل التنصت وبعده

	قبل التنصت		بعد التنصت	
	Q-factor	**BER**	**Q-factor**	**BER**
المستخدم الأول	17.9	10^{-73}	9.9	10^{-24}
المستخدم	10.5	10^{-27}	7.7	10^{-15}

الثاني				
المستخدم الثالث	8.8	10^{-19}	6.5	10^{-11}
المستخدم الرابع	11.4	10^{-31}	6.8	10^{-12}

يفسر الجدول (4)محاولة المتنصت سرقة الإشارة من خلال النقر على الليف وذلك بسبب تغيُر جودة الإشارة بعد التنصت عن قيمتها قبله، حيث ازداد معدل خطأ البت وانخفض عامل الجودة .

يظهر الشكل(13) نماذج من أشكال العين للمتنصتين، وقد تمَ الاقتصار على نماذج محددة نتيجة الحصول على النتيجة ذاتها.



الشكل (13) نماذج من أشكال العين للمتنصتين

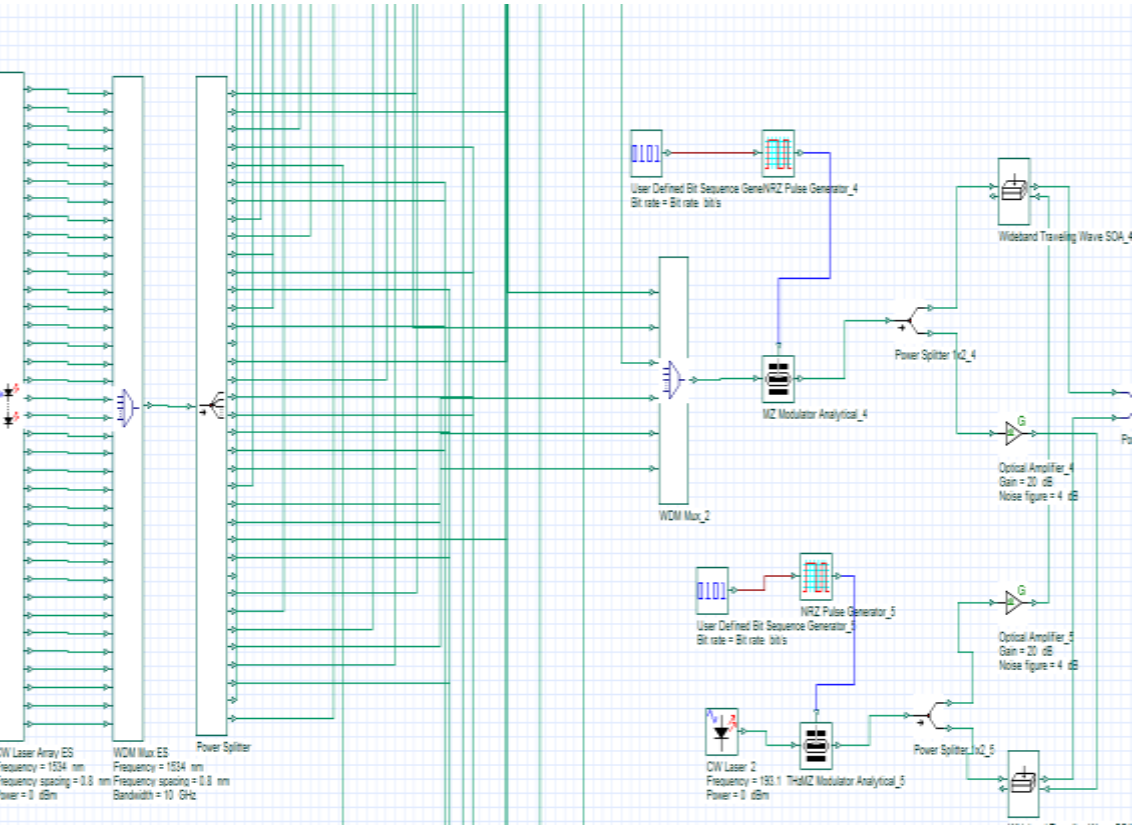
يبين الشكل (13)محاولة المتنصت في سرقة الإشارة قد باءت بالفشل لعدم إدراكه لوجود بوابة ex−or حيث حصلنا على (BER=1,Q−Factor=0) .

بعد محاكاة الشبكة بالنسبة لأربع مستخدمين باستخدام ترميز zcc تم دراسة أثر زيادة عدد المستخدمين على نمط الترميز المستخدم. مع زيادة عدد المستخدمين إلى 6 مستخدمين، يخصص لكل مستخدم 6 أطوال موجية يوضح الجدول(5) الأطوال الموجية المخصصة لكل مستخدم.

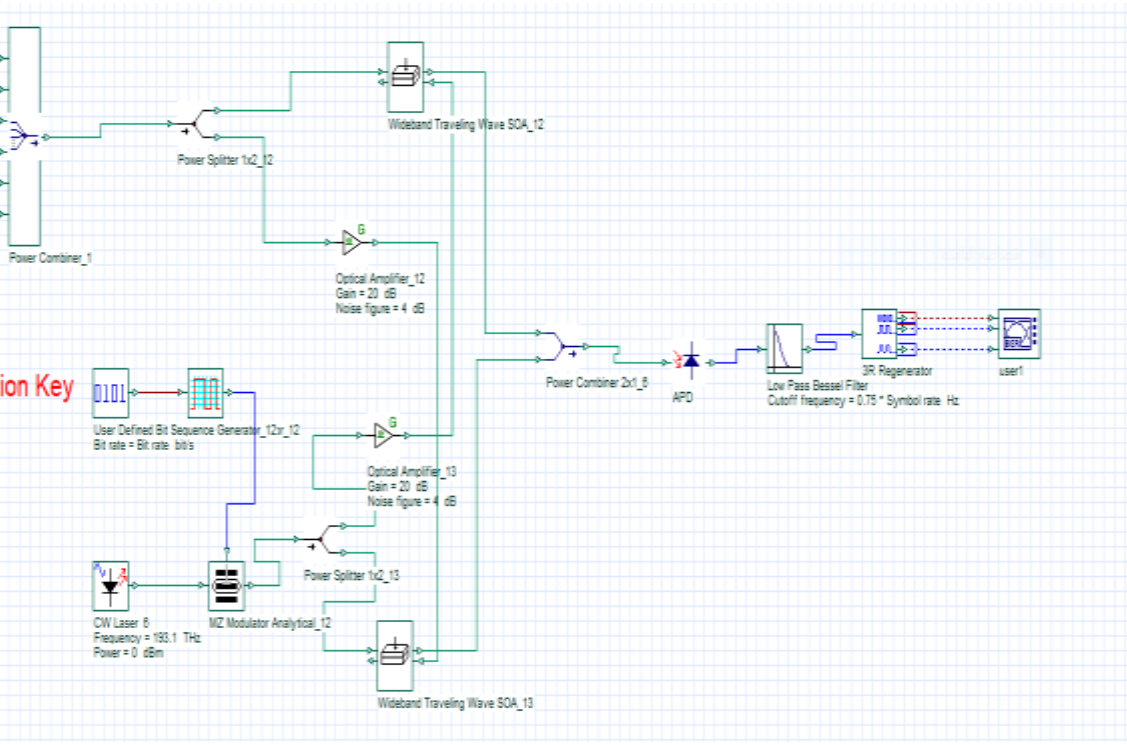
الجدول(5) الأطوال الموجية وفقاً لنمط الترميز ZCC حيث k=6

User1	λ_1 , λ_8 , λ_{15}, λ_{22} , λ_{29} , λ_{36}	1534,1539.6,1545.2,1550.8,1556.4,1562
User2	λ_2, λ_9 , λ_{16} , λ_{23} , λ_{30} , λ_{31}	1534.8,1540.4,1546,1551.6,1557.2,1558
User3	λ_3 , λ_{10} , λ_{17} , λ_{24} , λ_{25}, λ_{32}	1535.6,1541.2,1546.8,1552.4,1553.2,1558.8
User4	λ_4 , λ_{11}, λ_{18} , λ_{19} , λ_{26} , λ_{33}	1536.4,1542,1547.6,1548.4,1554,1559.6
User5	λ_5, λ_{12}, λ_{13} , λ_{20} , λ_{27}, λ_{34}	1537.2,1542.8,1543.6,1549.2,1554.8,1560.4
User6	λ_6 , λ_7 , λ_{14} , λ_{21} , λ_{28} , λ_{35}	1538,1538.8,1544.4,1550,1555.6,1561.2

يوضَح الشكل(14) والشكل (15) بنية مرسل واحد ومستقبل واحد على التوالي باستخدام نمط الترميز (ZCC,K=6).



الشكل(14) بنية المرسل باستخدام (ZCCC,K=6)



الشكل(15) بنية المستقبل باستخدام (ZCCC,K=6)

ثم قمنا بزيادة عدد المستخدمين إلى 6 مستخدمين وتمت المحاكاة على عدة أطوال للألياف الضوئية. يبين الجدول (6) معدل خطأ البت وعامل الجودة للمستخدمين الستة باستخدام ZCC على ثلاث مسافات 60km، 80km، 100km

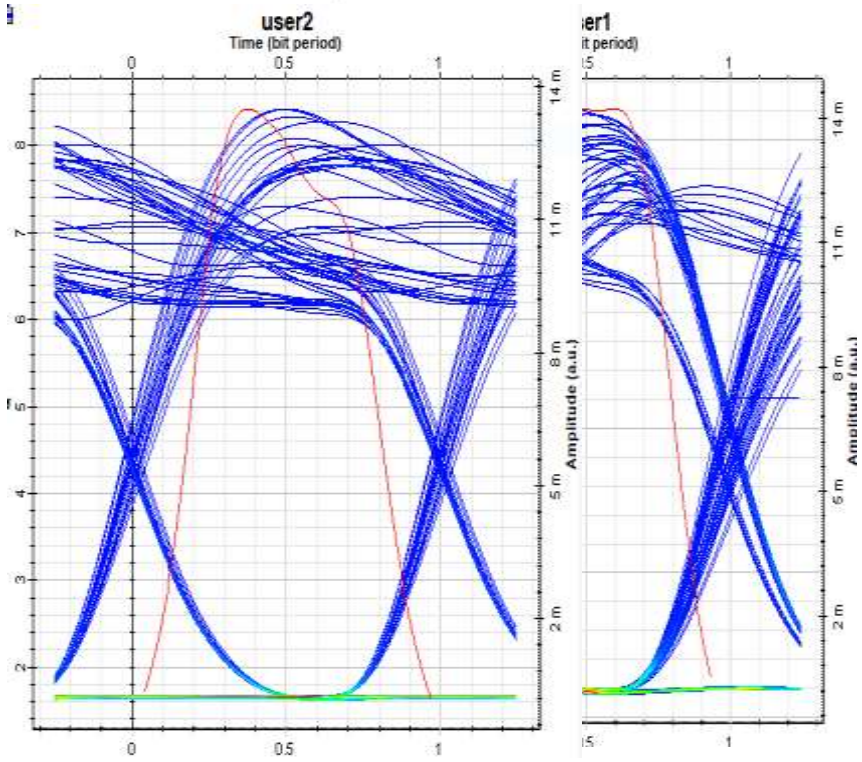
الجدول (6) معدل الخطأ في البت وعامل الجودة باستخدام ZCCC

Q-factor			BER			
100Km	80km	60km	100Km	80km	60km	
8.8	9	9.4	10^{-19}	10^{-20}	10^{-22}	User1
7.1	7.3	8.4	10^{-13}	10^{-14}	10^{-17}	User2
6.1	6.7	7.5	10^{-10}	10^{-12}	10^{-14}	User3

5.8	6	6.4	10^{-9}	10^{-9}	10^{-11}	User4
5.9	5.9	6	10^{-8}	10^{-8}	10^{-8}	User5
9.5	9.7	14.1	10^{-22}	10^{-23}	10^{-33}	User6

بالمقارنة بين النتائج السابقة نلاحظ أنه عند المسافات الثلاثة لم نحقق أي نتيجة أقل من الحد المقبول بالنسبة لمعدل خطأ البت، ويقل مع زيادة مسافة الإرسال وتحقق مسافة 60km النتيجة الأفضل وبالتالي تكون ذو إمكانية أكبر لزيادة عدد المستخدمين كذلك الأمر بالنسبة لعامل الجودة.

يبين الشكل(16) نماذج من أشكال العين على مسافة 60km باستخدام رمز ZCC.



الشكل(16) نماذج من أشكال العين باستخدام ZCCC على مسافة 60km

نلاحظ من المخططات السابقة اتساع فتحة العين وقلة عدد التداخلات للمستخدم الأول والثاني وهذا يتناسب مع ازياد عامل الجودة وانخفاض معدل خطأ البت وكذلك الأمر بالنسبة لباقي المستخدمين.

8-مقارنة النتائج مع الدراسات السابقة:

بهدف تقييم نتائج هذه الدراسة، تمت مقارنة نتائج نظام OCDMA المصمم في هذا البحث بنتائج الأبحاث السابقة كما هو موضَح في الجدول (7) .

الجدول(7) مقارنة بين الأبحاث المنشورة

	اسم الباحث وسنة النشر	دار النشر	الطريقة المقترحة	عدد المستخدمين	معدل الإرسال	مسافة الإرسال	Min. BER
البحث[18]	Sharma& Kummar 2020	Research-gate	Ex-OR subsystem & MDC	2	1Gbit/sec	100km	10^{-25}
البحث[8]	Chowdhury Uddin2019	AJSE	CMUX& CDEMUX	4	1.25Gb/sec	70km	10^{-15}
البحث [19]	Urmila bharji2022	springer	Encryption circuit+2D encoding	22	-1.25)Gb/s (10	-10)km (50	10^{-13}
الدراسة الحالية	-	-	EX-OR Optical Gate & ZCCC	6	10Gb/s	100km	10^{-22}

9-الاستنتاجات والتوصيات

تمَّ في هذا البحث اقتراح آليات مختلفة لحماية معلومات المستخدمين من التنصت أثناء الارسال عبر شبكة OCDMA وذلك بسبب الأهمية الكبيرة لهذه الشبكة حيث يعتبر النفاذ المتعدد بتقسيم الرمز الضوئي التطبيق الأفصل لشبكات الوصول إلى المنازل وغيرها من التطبيقات. فكان للبحث مخرجات ونتائج يمكن تلخيصها بالنقاط التالية:

- تمت حماية البيانات بشكل تام من السرقة أو الاختراق من قبل متنصتين .
- تم تحقيق أقصى معدل إرسال قدره 10 Giga bits/sec مع طول ليف 100km فكانت أقل قيمة لمعدل خطأ البت هو 10^{-22} .
- تم تحقيق معدل إرسال قدره 10Giga bits/sec بالنسبة ل 6 مستخدمين.

نعمل في المستقبل على زيادة أبعاد الرموز المستخدمة ومقارنة النتائج مع الرموز المستخدمة في هذا البحث.

المراجع

[1] Shukra, Mohamed Mansour, Arvind Kumar Jaiswal, and Mukesh Kumar. "Security Based Performance Analysis in Optical CDMA Network Systems." IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) 8.6 (2013): 70-74.

[2] Kaur, Gurjeet, and Simranjit Singh. "Review on Optical Code Division Multiple Access Systems." International Journal of Engineering Sciences 17 (2016).

[3] Fouli, Kerim, and Martin Maier. "Ocdma and optical coding: Principles, applications, and challenges [topics in optical

communications]." IEEE Communications Magazine 45.8 (2007): 27-34.

[4] Bharti, Manisha, Ajay k Sharma, and Manoj Kumar. "Simulative analysis of 2-code keying approach using Walsh Hadamard codes to enhance security and reduce dispersion in OCDMA system." 2014 International Conference on Data Mining and Intelligent Computing (ICDMIC). IEEE, 2014

[5] Mrabet, Hichem, et al. "A comparative study of asynchronous and synchronous OCDMA systems." IEEE Systems Journal (2020).

[6] Hooshang, G., & M, M.K." Optical CDMA Networks: Principles, Analysis and Application". Wiley-IEEE Press.(2012).

[7] Dahan, David, and Uri Mahlab. "Security threats and protection procedures for optical networks." IET Optoelectronics 11.5 (2017): 186-200.

[8] Chowdhury, T., & Uddin, M. N. (2019). OCDMA System Using Two Code Keying Encryption Introducing a SOA Based CMUX And CDEMUX Over a WDM System. AIUB Journal of Science and Engineering (AJSE), 18(1), 11-17.

[9] Bhanja, Urmila, and Sutikshna Singhdeo. "Novel encryption technique for security enhancement in optical code division multiple access." Photonic Network Communications 39.3 (2020): 195-222.

[10] Furdek, Marija, et al. "Vulnerabilities and security issues in optical networks." 2014 16th International Conference on Transparent Optical Networks (ICTON). IEEE, 2014.

[11] Iqbal, M. Zafar, Habib Fathallah, and Nezih Belhadj. . "Optical fiber tapping: Methods and precautions." 8th International

Conference on High-capacity Optical Networks and Emerging Technologies. IEEE, 2011.

[12] Everett, Bernard. "Tapping into fibre optic cables." Network Security 2007.5 (2007): 13-16.

[13] Abraham, Nelsa, and Ankit Parakh. "Various architecture for detection of information using SAC-OCDMA for FTTH system." 2016 International Conference on Next Generation Intelligent Systems (ICNGIS). IEEE, 2016.

[14] Rajesh Yadav, Dr. GurjitKaur. "Optical CDMA: Technique, Parameters and Applications." Proc. of Int. Conf. on Emerging Trends in Engineering and Technology, 2013.

[15] Kumawat, Soma, and M. Ravi Kumar. "A review on code families for sac–ocdma systems." Optical and Wireless Technologies. Springer, Singapore, 2020. 307-315.

[16] Rashid, C. B. M., et al. "New design of flexible cross correlation (FCC) code for SAC-OCDMA system." Procedia Engineering 53 (2013): 420-427.

[17] Alayedi, M., et al. "Performance improvement of multi access OCDMA system based on a new zero cross correlation code." IOP Conference Series : Material Science and Engineering. VOL. 767. NO. 1. IOP Publishing, 2020.

[18] Sharma, T., & Kumar, M. R." Novel Security Enhancement Technique for OCDMA and SAC OCDMA Against Eavesdropping Using Multi-diagonal Code and Gating Scheme". In Optical and Wireless Technologies (pp. 477-486). Springer, Singapore, 2020.

[19] Bhanja, U. "Design and Performance Analysis of an Encrypted Two-Dimensional Coding Technique for Optical

CDMA". In Optical and Wireless Technologies (pp. 573-583). Springer, Singapore, 2022.