Journal of Engineering Sciences and Information Technology (JESIT) • Vol 7, Issue 2 (2023) • P: 47 - 22
https://journals.ajsrp.com/index.php/jesit
ISSN: 2522-3321(Online) • ISSN: 2522-3321(Print)

Development of a data encryption algorithm to enhance security in D2D communications by secure key exchange

Eng. Essam Mohammad Asaad*[1], Prof. Abdulkarim Assalem[1]
[1] Faculty of Mechanical and Electrical Engineering | Al-Baath University | Syria

Received: 14/02/2023
Revised: 24/02/2023
Accepted: 09/03/2023
Published: 30/06/2023

* Corresponding author:
essam.ryha@gmail.com

Citation: Asaad, E. M., & Assalem., A. (2023). Development of a data encryption algorithm to enhance security in D2D communications by secure key exchange. *Journal of engineering sciences and information technology, 7(2),* 22 – 47.
https://doi.org/10.26389/AJSRP.U140223

Abstract: D2D (Device to Device) technology enables direct communication between devices and allows devices to act as a relay. It is one of the promising technologies, as it provides broader coverage and ensures an increase in cell capacity by increasing the capacity of users, as it allows devices to operate as eNB (eNodeB) or a small base station to form a small network in infrastructure or non-infrastructure mode, and these networks can be exposed to intrusions and threats Many of them: denial-of-service attacks, man-in-the-middle attacks, side channel attacks, and others.

In this research, the focus is on the need to protect data, whether from hacking or copying, and thus accessing its contents and influencing the information exchange parties, and one of the most important methods of protection is information encryption.

The importance of the research lies in the fact that it provides security protection for the D2D device-to-device communication system, by developing the key exchange protocol in the discovery stage based on the Diffi-Hellman key exchange algorithm, as well as proposing an encryption algorithm for the D2D communication technology based on the Logistic Map functions to secure the mixing process. Which is considered a first encryption stage because it depends on private keys in addition to balanced mixing equations for BBM blocks. Thus, the research aims to build an encryption system for D2D communication technology.

Keywords: Device-to-device communication, discovery protocols, cryptography, algorithms, block balance mixing.

تطوير خوارزمية لتشفير البيانات لتعزيز الأمن في اتصالات D2D عن طريق التبادل الآمن للمفاتيح

المهندس / عصام محمد اسعد*[1]، الأستاذ الدكتور / عبد الكريم السالم[1]
[1] كلية الهندسة الميكانيكية والكهربائية | جامعة البعث | سوريا

المستخلص: تتيح تقنية D2D (Device to Device) الاتصال المباشر بين الأجهزة كما تسمح للأجهزة بالعمل كمُرحّل. إنها إحدى التقنيات الواعدة بما توفره من تغطية أوسع وتضمن زيادة سعة الخلية وذلك بزيادة استيعاب المستخدمين حيث تسمح للأجهزة بالعمل مثل(eNodeB) eNB أو محطة أساسية صغيرة لتشكيل شبكة صغيرة في وضع البنية التحتية أو غير البنية التحتية، ويمكن أن تتعرض تلك الشبكات إلى اختراقات وتهديدات كثيرة منها: هجمات رفض الخدمة أو هجوم الرجل في المنتصف بالإضافة إلى هجمات القناة الجانبية وغيرها.

حيث يتم في هذا البحث التركيز على ضرورة حماية البيانات سواء من القرصنة أو النسخ وبالتالي الاطلاع على محتوياتها والتأثير على الأطراف المتبادلة للمعلومة، ومن أهم طرق الحماية هو تشفير المعلومات،

تكمن أهمية البحث في كونه يقدم حماية أمنية لنظام الاتصالات من جهاز إلى جهاز D2D ، وذلك بتطوير بروتوكول تبادل المفاتيح في مرحلة الاكتشاف بالاعتماد على خوارزمية تبادل المفاتيح Diffi-Hellman، كذلك اقتراح خوارزمية تشفير خاصة بتقنية الاتصالات D2Dاعتماداً على توابع Logistic Map لتأمين عملية الخلط ، والتي تعتبر مرحلة تشفير أولى لاعتمادها على مفاتيح خاصة بالإضافة إلى معادلات المزج المتوازن للكتل BBM وبذلك يهدف البحث إلى بناء منظومة تشفير خاصة بتقنية الاتصالات D2D .

الكلمات المفتاحية: الاتصالات جهاز إلى جهاز، بروتوكولات الاكتشاف، التشفير، الخوارزميات، المزج المتوازن للكتل.

1- مقدمة:

يترافق التطور السريع المتزايد لتقنيات الاتصالات النقالة والأجهزة الذكية، مع التزايد الكبير بحركة البيانات مما يستدعي استخدام أفضل لموارد الشبكة وزيادة سعتها، الأمر الذي يطرح تحديات ومتطلبات أعلى على موارد الشبكة المحدودة، وستؤدي حركة المرور المتزايدة للبيانات إلى ازدحام في الشبكة، يترافق بدوره بتدني جودة الخدمة، وانخفاض الكفاءة الطيفية.

ومع الانتشار الواسع لتقنية LTE –A، يتزايد التركيز والاهتمام بتقنيات من شأنها تحسين أداء الشبكة مثل اتصالات من جهاز إلى جهازD2D .

تسمح تقنية الاتصال من جهاز إلى جهازD2D للأجهزة الخليوية المتجاورة بالاتصال ببعضها البعض مباشرة باستخدام الموارد الراديوية تحت إدارة الشبكات الخلوية، ويتزايد الاهتمام بها نظراً لمقدرتها في تقديم حلول مناسبة للشبكة ودعم أفضل لجودة الخدمة.

2- مشكلة البحث

هناك العديد من الأسباب الكامنة وراء ضعف نظام الأمان في اتصالات D2D حيث لا توجد بنية تحتية للشبكة لرصد الأنشطة المشبوهة التي تقوم بها أجهزة المستخدمين [5] كما ان الاتصال D2D مثل كافة التطبيقات اللاسلكية معرضة لخطر العديد من التهديدات الأمنية مثل التنصت، تعديل البيانات، هجوم الإعادة، انتحال الهوية، هجوم رفض الخدمة، والتشويش [5].

ومن ثم ، فإن اتصالات D2D يمكن أن تتعرض لجميع التهديدات الأمنية للاتصالات اللاسلكية، فالأمن هو أحد أهم المسائل الرئيسية لاتصالات D2D التي يجب معالجتها قبل تنفيذها.

3- فرضيات البحث

تتم الدراسة على بروتوكولات اكتشاف الخدمة والجوار في اتصالات D2D ، حيث تمثل عملية الاكتشاف المهمة الأساسية لاتصال D2D وتبدأ قبل بدء الاتصال بين جهازي UE بالإضافة إلى ذلك، تتضمن آلية الاكتشاف عمليات اكتشاف الجوار والخدمة. تم تقديم سيناريوهات 3GPP لاتصالات D2D والسيناريو المختار لتصميم البروتوكولات وذلك بهدف تعزيز أمن الاتصالات D2D، وتصنف البروتوكولات المستخدمة في الاكتشاف إلى:

- البروتوكولات الاستباقية (Proactive protocol) حيث تقوم BS بالإعلان عن توافر الخدمات (Proximity Service) ProSe إلى أجهزة المستخدمين عن طريق إرسال رسائل متعددة بشكل دوري، فإذا قام UE بإرسال طلب خدمة D2D ، تقوم BS بالرد عليه بشأن طلب اكتشاف ProSe الخاص بها، ومن الممكن أن تقدم خدمة D2D لـ UEs بواسطة BSs مختلفة[6].
- البروتوكولات التفاعلية (Reactive protocol) حيث يبدأ UE ببروتوكول اكتشاف الخدمة عند الحاجة إلى إنشاء اتصال D2D مع أجهزة UEs أخرى في الشبكة.

ويكمن الاختلاف الرئيسي بين هذين البروتوكولين أنه عند استخدام البروتوكول التفاعلي، يبدأ UE دائمًا اتصال D2D مع عملية اكتشاف الخدمة والجوار، ويعني ذلك أن UE سيرسل رسالة طلب D2D عندما يحتاج إلى معلومات محددة من UEs المجاورة، من ناحية أخرى تكون BS هي المسؤولة عن بث رسائل إعلان الخدمة إذا تم استخدام البروتوكول الاستباقي حيث أنه "دائم التشغيل"، بينما البروتوكول التفاعلي يستخدم "حسب الطلب"[6].

4- هدف البحث

يهدف البحث إلى حماية الاتصالات الجهاز إلى الجهاز D2D وذلك عن طريق تعزيز بروتوكول اكتشاف الخدمة باستخدام خوارزمية تبادل المفاتيح Diffi-Hellman وذلك قبل البدء بالاتصال D2D وبعد السماح بإنشاء الاتصال D2D يتم تشفير وحماية البيانات التي يتم تبادلها بين أطراف الاتصال عن طريق خوارزمية مطورة تم تطويرها باستخدام توابع رياضية Logistic Map ومعادلات المزج المتوازن للكتل Balanced Block Mixing بحيث يصبح الاتصال D2D آمن و يحافظ على الشروط الأمنية (Confidentiality, Integrity, Authentication, Availability And accessibility) CIAAA ، أي السرية والنزاهة والمصادقة والتوافر وسهولة الوصول للمعلومات المرسلة عبر قناة D2D [5] ، حيث تمت محاكاة أداء بروتوكول الاكتشاف المعزز باستخدام برنامج MATLAB ، وتم تطوير خوارزمية تشفير وتنفيذها باستخدام لغة البرمجة C# .

5- أهمية البحث:

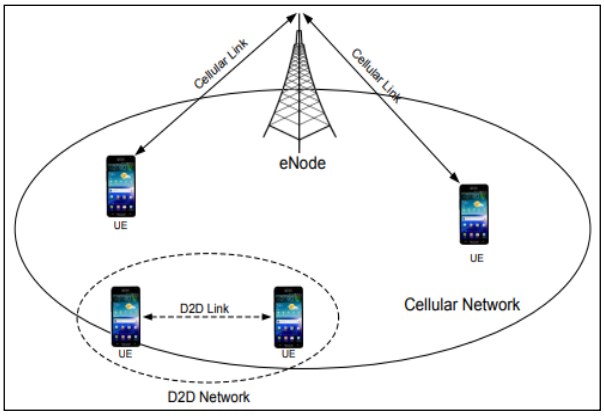
تنبع أهمية هذا البحث كم كونه يعالج ضرورة الحفاظ على سرية المعلومات في حالة الطوارئ بالإضافة أنه يقدم إجرائية لضمان عدم دخول أجهزة غير مرغوب بها ضمن شبكة الاتصال وبالتالي توفير موارد الخلية المسؤولة عن التغطية في المنطقة المستهدفة حيث يمكن للمستخدم المصرح له فقط الوصول إلى المعلومات، بما يضمن عدم تعديل المعلومات أثناء الإرسال من قبل أي مستخدم، في حين تسمح للمستخدم المصادق عليه فقط بالوصول إلى المعلومات، ويتيح للمستخدمين الشرعيين الوصول إلى المعلومات من أي مكان وفي أي وقت [8].

وهذا يضمن عدم تمكن المتطفل من الدخول إلى الاتصال D2D والقيام بكل ما يريد فعله بالرسائل التي يتم تبادلها عبره.

6- الاتصالات جهاز إلى جهاز D2D :

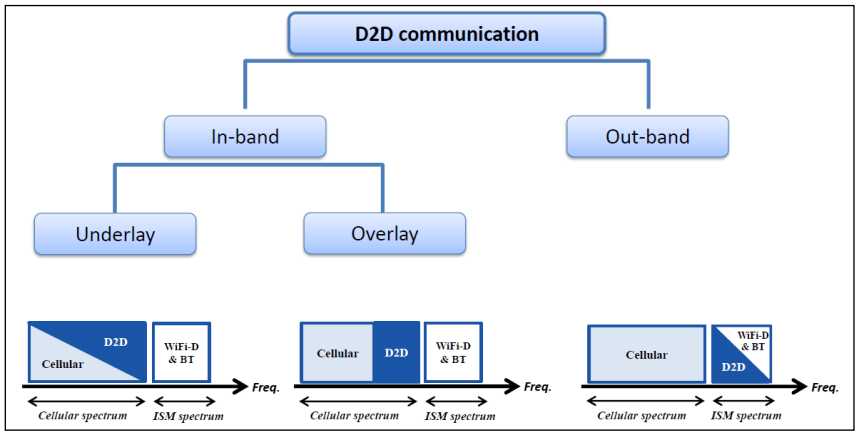
تعتبر الاتصالات D2D جزءاً أساسياً من البنية الرئيسية في شبكة 5G ، حيث يتم من خلال الاتصالات المباشرة تحسين إعادة استخدام الطيف والإنتاجية واستهلاك الطاقة والتغطية وتقليل أزمنة التأخير، مما دفع لتضمينها في شبكات 4G كونها ذات الانتشار الأوسع حالياً وتحتاج لهذه التقنية لتقليل الازدحام في نقل حركة البيانات المتزايدة أسياً، وتحسين جودة الخدمة عموماً.

ويبين الشكل (1) بنية اتصالات D2D .



الشكل (1) بنية الاتصالات D2D ضمن شبكة الاتصالات [1]

يقسم اتصال D2D في الشبكة الخلوية إلى نوعين: داخل المجال in-band وخارج المجال out-band ، كما هو موضح في الشكل (2) :



الشكل (2) تصنيف الاتصالات D2D [2]

- داخل المجال in-band : تعمل اتصالات D2D على طيف مرخص – طيف الاتصالات الخليوية نفسه- مما يشير إلى الحاجة إلى تحكم وإدارة للطيف الراديوي ، يتم تقسيم Inband D2D إلى أساسية Underlay و تراكب Overlay ، في اتصال D2D الأساسي.

تشترك الاتصالات الخلوية و D2D في نفس الموارد الراديوية، لكن روابط D2D في اتصالات التراكب تُمنح موارد خلوية مخصصة [4] .

- خارج المجال out-band : تعمل اتصالات D2D على الطيف غير المرخص ، والدافع وراء استخدام اتصال D2D خارج المجال هو حل مشكلة التداخل بين D2D والروابط الخلوية ، ويتطلب استخدام الطيف غير المرخص واجهة إضافية وعادة ما يعتمد شبكة لاسلكية أخرى ، مثل Wi-Fi Direct أو ZigBee أو Bluetooth ، ينقسم المجال الخارجي D2D أيضًا إلى اتصال متحكم به واتصال مستقل[3].

1-6- التحديات والتهديدات الأمنية في الاتصالات D2D

يتم وصف بعض التهديدات الأمنية التي قد تحدث في اتصال D2D [5] على النحو التالي:

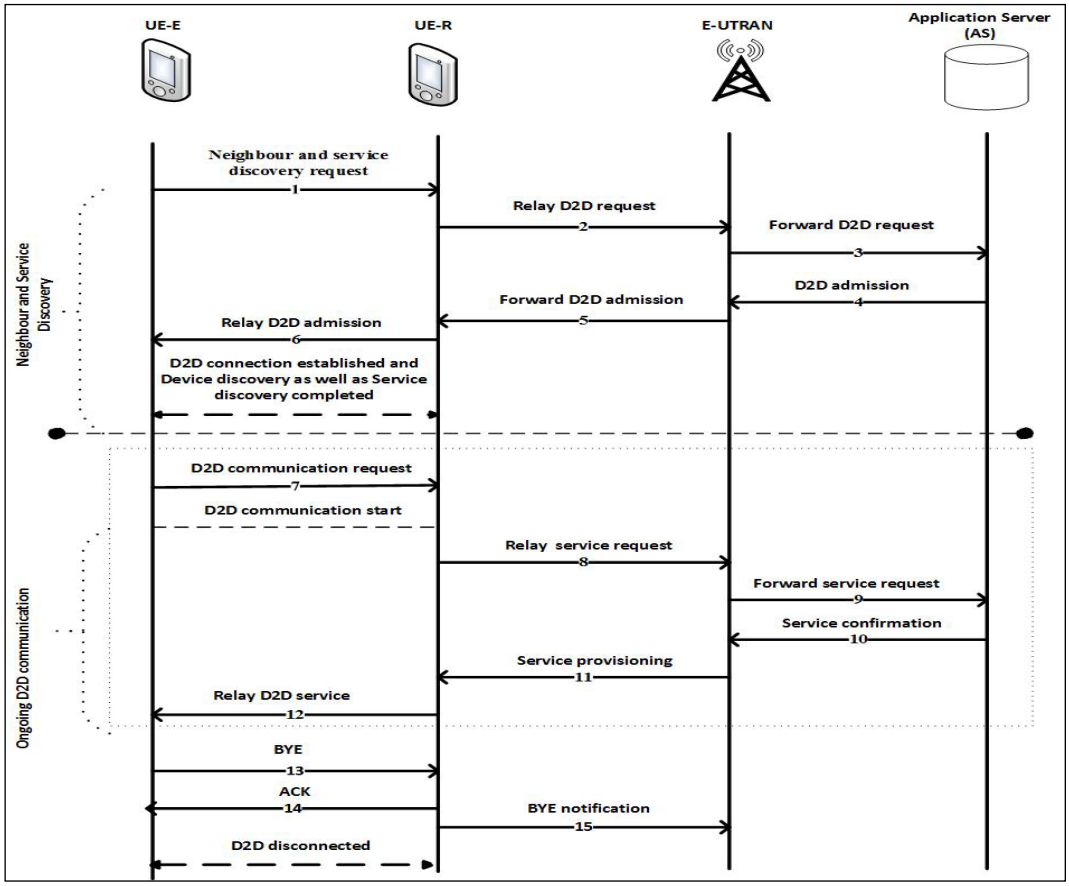
- هجوم الرجل في المنتصفMIM : يعتبر ارتباط D2D وضع اتصال غير آمن. لذلك، إذا لم يتم تطبيق الأمن المناسب قبل الإرسال، يمكن للمتطفل اعتراض الرسائل المرسلة عبر وصلة D2D وتعديلها وفقًا لمتطلباته وإرسالها إلى تجهيزات المستخدم الوجهة، يقوم الدخيل بإجراء اتصال منفصل مع كل من جهازي المستخدمين UEs حيث لا يكون لأي من الجهازين علم بالهجوم وتتم مواصلة الاتصال كما لو أن الرسائل صادرة عن مستخدم شرعي.
- هجوم الإعادة: في هجوم الإعادة، يقوم الدخيل بتسجيل الرسائل وإعادة إرسالها أو تكرارها بعد فترة زمنية معينة في نفس الشبكة أو في شبكات مختلفة. حيث يبدو أن الرسالة شرعية ومن الصعب تحديد أن الرسائل ليست من مستخدم شرعي.
- انتحال الهوية: في هجوم انتحال الهوية، ينتحل دخيل هوية UE المشروعة أو يستخدم أي هوية غير موجودة في شبكة معينة، تبدأ UEs المخادعة اتصال D2D وتستخدم ProSe الذي يوفره اتصال D2D على الرغم من أنها غير مؤهلة للاستخدام مما يؤدي إلى إساءة استخدام الموارد.
- رفض الخدمة DoS : في هجوم DoS ، يرسل واحد أو أكثر من UEs المتطفل طلب D2D إلى UE-R ونظرًا لقدرة UE-R المحدودة ، لا يمكنها متابعة جميع الطلبات المرسلة بواسطة UEs مما يتسبب في هجوم يسمى الحرمان من الخدمة DoS .

بالإضافة إلى ذلك، تستهلك حركة المرور الكثيفة في قناة D2D كمية كبيرة من الموارد، نظرًا لأن الموارد في اتصالات D2D محدودة، فإن هذا سيؤدي إلى عدم قدرة المستخدمين UEs الفعليين على الوصول إلى الخدمات التي تقدمها UE-R .

2-6- بروتوكولات اكتشاف الخدمة والجوار:

6-2-1 البروتوكول التفاعلي : يبدأ UE عملية الاكتشاف عن طريق إرسال رسالة اكتشاف إلى المرحل UE-R وتتضمن رسالة الاكتشاف هوية الجهاز ونوع الخدمة المطلوبة، حيث يكون الاتصال بينهما مباشر باستخدام البروتوكول التفاعلي ، وتبدأ عملية اكتشاف الجوار في اتصال D2D فقط عندما UE يطلب خدمة التقارب ProSe، حيث يلعب المرحل UE-R دور المناولة لإرسال جميع المعلومات التفصيلية حول جهاز المستخدم UE إلى المحطة القاعدية BS.

وفقًا للمعلومات التي يتم استلامها من المرحل UE-R، تتحقق BS وخادم التطبيق AS (Application Server) من صحة ومصادقة UE لاستخدام ProSe، لذلك لا يوجد أي دور ل BS في عملية اكتشاف D2D، إذا كان UE مستوفياً لجميع متطلبات ProSe ، فيجب الاستمرار في خطوات تقديم معلومات الخدمة، ويقسم البروتوكول كما هو موضح في الشكل (3) إلى مرحلتين، مرحلة اكتشاف الجوار والخدمة ProSe discovery ومرحلة الاتصال D2D .



الشكل (3) تسلسل مراحل عمل البروتوكول التفاعلي [6]

يتم وصف هاتين المرحلتين كما يلي كما يلي:

الخطوات من 1 حتى 6 تمثل مرحلة اكتشاف الجوار والخدمة:

- الخطوة 1: يرسل جهاز المستخدم UE "إشارة الاكتشاف" إلى المرحل UE-R، حيث تحتوي "إشارة الاكتشاف" على معرف المصدر، ومعرف الوجهة، ونوع الخدمة المطلوبة، وموقع UE.

- الخطوة 2: يحسب UE-R المسافة بين UE-R و UE والتأخير وجودة الإشارة و SINR والتداخل، يقوم UE-R بإعادة توجيه جميع هذه المعلومات إلى BS ويطلب الإذن لإنشاء اتصال D2D ولتوصيل الخدمات المطلوبة إلى UE.
- الخطوة 3: تقوم المحطة القاعدية BS بالتحقق وفحص وثوقية UE، إذا كان موثوقاً تطلب المحطة القاعدية BS من خادم التطبيقات AS توفير الخدمات، وإلا تكون استجابةBS سلبية على UE-R.
- الخطوة 4: يتحقق خادم التطبيقات AS من توافر الخدمات والاستجابات الإيجابية ، للخدمات المطلوبة من طرف UE وإلا فإنه يرسل استجابة سلبية إلى BS.
- الخطوة5: ترسل BS استجابة إيجابية لـ UE-R ، إذا تلقت استجابة إيجابية من AS.
- الخطوة 6: UE-R ترحّل استجابة BS إلى UE.
- الخطوة 7: يرسل UE "طلب الاتصال D2D" من أجل الوصول إلى الخدمات.

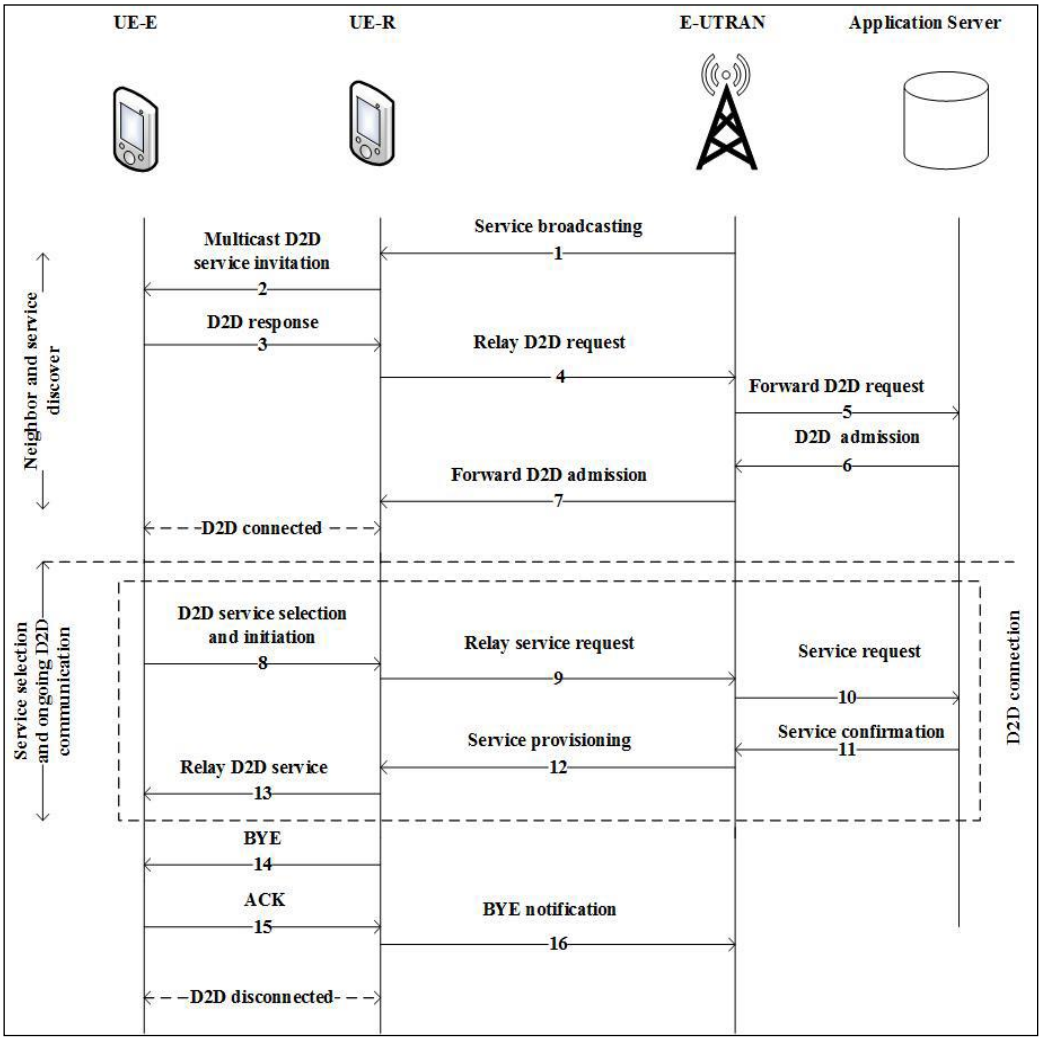
الخطوات من 8 حتى 12 تمثل مرحلة الاتصال D2D :

- الخطوة 8: يرسل UE-R "طلب خدمات المرحلات" إلى BS.
- الخطوة 9: تطلب BS من AS توفير الخدمات.
- الخطوة 10: توفر AS خدمات المعلومات إلى BS.
- الخطوة 11: تقوم BS بإعادة توجيه معلومات الخدمات إلى UE-R.
- الخطوة 12: تقوم UE-R بترحيل الخدمات المقدمة من BS، وتتكرر الخطوات من 9 إلى 12 حتى ينهي UE-R أو UE اتصال D2D.
- الخطوة 13: ترسل UE رسالة "BYE" إلى UE-R.
- الخطوة 14: يرسل UE-R "ACK" .
- الخطوة 15: تقوم UE-R بترحيل رسالة "BYE" إلى BS وعندها يتم قطع اتصال D2D.

2-2-6 البروتوكول الاستباقي: في البروتوكول الاستباقي، UE-R لا تنتظر UEs لبدء اتصال D2D كما هو الحال مع البروتوكول التفاعلي، تقوم UE-R بترحيل معلومات إعلانات الخدمات من BS، أي UEs المهتمة تقوم بالاستجابة لهذه الرسالة أثناء عملية اكتشاف الجهاز.

يكون نوع الاتصال بين UE-R و UEs هو الإرسال المتعدد، يتم بدء اتصال D2D بين UE-R و UE على الرغم من أن UE لم يطلب معلومات خدمة محددة.

يبين الشكل (4) إجرائية اكتشاف الخدمة والجوار باستخدام البروتوكول الاستباقي.



الشكل (4) تسلسل مراحل عمل البروتوكول الاستباقي[6]

يتم وصف الخطوات الرئيسية لعملية اكتشاف الخدمة والجوار كما يلي.

مرحلة اكتشاف الجوار والخدمة تمثل الخطوات من 1 حتى7:

- الخطوة 1: تقترح المحطة BS "إعلان الخدمة" على أجهزة المستخدمين في منطقة التغطية باستخدام رسالة إذاعية.
- الخطوة 2: يرسل UE-R كجهاز ترحيل "دعوة لخدمة D2D بالإرسال المتعدد" إلى UEs القريبة، تحتوي رسالة الإرسال المتعدد على معرفها ID ونوع معلومات الخدمة.
- الخطوة 3: تصدر عن UE استجابة برسائل منفردة "D2D response" إلى UE-R على أنها قبلت الدعوة للخدمة.
- الخطوة 4: يطلب UE-R من BS طلب إذن D2D بإرسال معلومات حول UE.

الخطوات 5 و 6 و 7: تمثل عمليات فحص D2D لـ UE، ترسل BS إلى AS طلبات D2D ، بعد ذلك ، تقوم AS بحفظ المعلومات حول UE في قاعدة البيانات الخاصة بها والتحقق من سعة وجودة القناة لذلك، بعد هذا الإجراء ، تقوم AS بالرد على طلب UE-R بإرسال رسالة "قبول D2D " عبر BS.

مرحلة الاتصال D2D تمثل الخطوات من 8 حتى 13:

- الخطوة 8: تختار UE خدمة محددة وتقوم بإرسال اقتراح واختيار خدمة D2D إلى UE-R.
- الخطوة 9: UE-R ترحل طلب الخدمة إلى BS.

- الخطوات 10 و 11 و 12: تمثل مرحلة توفير الخدمة من BS إلى UE-R، يتطلب ذلك فحص الخدمة وتأكيد من AS ، مع معالجة وتوزيع معلومات الخدمة المطلوبة.
- الخطوة 13: تقوم UE-R بتوصيل معلومات خدمة D2D عبر رسائل أحادية.
- الخطوة 14: ترسل UE رسالة "BYE" إلى UE-R.
- الخطوة 15: يرسل UE-R "ACK" .
- الخطوة 16: تقوم UE-R بترحيل رسالة "BYE" إلى BS وعندها يتم قطع اتصال D2D.

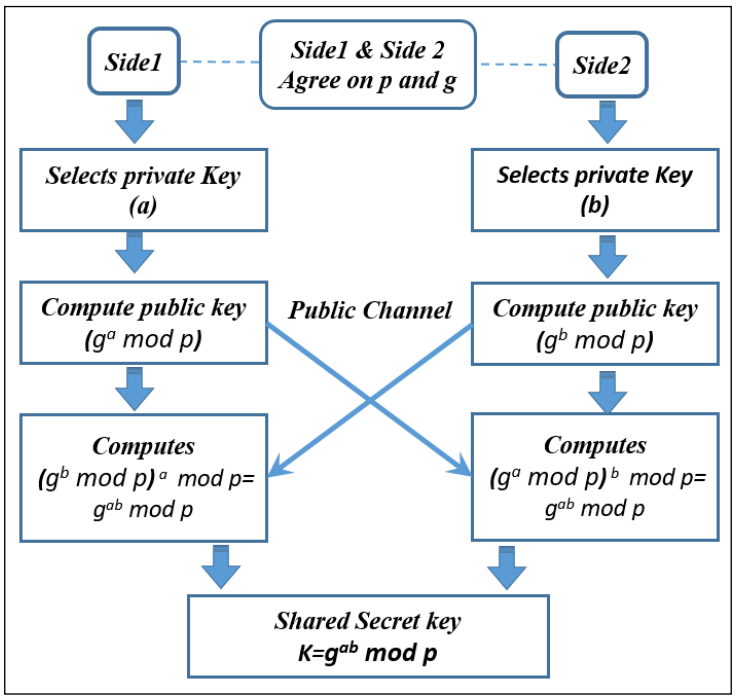
7- تطوير بروتوكول تحسين الأمان لمرحلة الاكتشاف

تم اقتراح بروتوكول تحسين الأمان للمصادقة المتبادلة لتجهيزات المستخدم (بين جهاز المستخدم UE الموجود خارج منطقة التغطية و جهاز المستخدم UE-R الذي يأخذ دور المرحّل) وإنشاء مفتاح سري مشترك استنادًا إلى خوارزمية تبادل المفاتيح Diffi-Hellman [7].

7-1- خوارزمية تبادل المفاتيح Diffi-Hellman :

7-1-1 تبادل مفتاح ديفي-هيلمان [7] D-H/ Diffie-Hellman key exchange : هو بروتوكول تشفير يسمح لجهتين ليس لديهما معرفة مسبقة ببعضهما بإنشاء مفتاح سري مشترك على قناة اتصال غير مؤمنة، هذا المفتاح يمكن استخدامه فيما بعد لتشفير المحادثات اللاحقة باستخدام خوارزمية تشفير بالمفتاح المتماثل.

يوضح الشكل (5) آلية عمل خوارزمية تبادل المفاتيح Diffi-Hellman بين الطرف 1 والطرف 2 .



الشكل (5) خوارزمية تبادل المفاتيح Diffi-Hellman [7]

ليكن لدينا طرفان يريدان التواصل، نرمز للطرفين A و B هذان الطرفان متصلان بشبكة ليست امنة ونفرض انه ليس بينها أي وسيلة اتصال آمنة، يريدان تشفير الرسائل وفكها بواسطة مفتاح سري مشترك أي فقط هما من يعرف هذا المفتاح. نفرض ان الطرفين يتعاملان بالأرقام وان الارقام تقع في مجال محدود منته.

إجرائية التبادل:

أولاً وقبل بدء الاتصال هناك قيمتان q عدد أولي, α جذر بدائي معروفتان لكل عنصر من الشبكة .

نفرض أن A و B يريدان تبادل مفتاح حيث أن القيمتان q و α معروفتان لهما .

1- يختار A عدداً عشوائياً $X_A < q$ ويحسب $Y_A = \alpha^{X_A} \ mod \ q$.

2- يختار B عدداً عشوائياً $X_B < q$ ويحسب $Y_B = \alpha^{X_B} \ mod \ q$.

3- يرسل A القيمة Y_A ويرسل B القيمة Y_B للطرف الآخر (القيمتين X_A و X_B سريتين) .

4- يحسب A : $K_A = {Y_B}^{X_A} \ mod \ q$.

5- يحسب B : $K_B = {Y_A}^{X_B} \ mod \ q$

المفتاح المشترك هو K_A أو K_B وذلك لأن :

$$K_A = {Y_B}^{X_A} \ mod \ q = {\alpha^{X_B}}^{X_A} \ mod \ q = {\alpha^{X_A}}^{X_B} \ mod \ q = {Y_A}^{X_B} \ mod \ q = K_B$$

في [16] تم التركيز على دراسة الهجمات الأمنية الرئيسية التي يمكن أن تتعرض لها الاتصالات D2D مثل هجمات رفض الخدمة وهجوم الرجل في الوسط بالإضافة إلى هجمات القناة الجانبية.

يسمح D2D باتصال قوي بين الأجهزة حيث يسمح للأجهزة بالعمل كمرحل. يحتوي هذا على مشكلات الأمان التي يمكن أن تؤدي إلى هجمات أمنية، يوفر هذا البحث فقط دراسة مقارنة للهجمات الرئيسية المحتملة التي يمكن القيام بها بينما يقترح في المستقبل إجراء الحل لمعالجة هذه الهجمات كمشروع بحث أعمق، وهذا ما سيقدمه بحثنا .

2-1-7 البروتوكول المقترح لتبادل المفاتيح في مرحلة الاكتشاف:

البروتوكول المقترح يطبق على كل من البروتوكولات الاستباقية والتفاعلية كما هو موضح في الشكل (6)

في حالة البروتوكول التفاعلي، يبدأ UE-R عملية التحقق كما هو مبين في الشكل(6) (a) .

وفي حالة البروتوكول الاستباقي يبدأ UE، عملية التحقق كما هو مبين في الشكل(6) (b) .

وفقًا لخوارزمية تبادل المفاتيح [8] Diffi-Hellamn، ينشئ كل من جهازي المستخدمين (UE,UE-R) مفتاحًا سريًا مشتركًا يمكن استخدامه كمفتاح سري لتشفير / فك تشفير الرسائل (كما هو موضح لاحقاً سيتم استخدام توابع المزج المتوازن للكتل BBM في عملية تشفير الرسائل) .

تعتبر أجهزة UEs نفسها مسؤولة عن إنشاء مفتاح سري لعدم توفر أي بنية أساسية للتوزيع [9].

بداية يولد UE الرقم السري A ويولد UE-R الرقم السري B ثم يتم توليد المفتاح العام Public Key – PubK كما يلي:

$$PubK_{UE} = g^A \ mod \ P \qquad (1)$$

$$PubK_{UE-R} = g^B \ mod \ P \qquad (2)$$

حيث:

g هو المولد العام .

P عدد أولي كبير.

$B \in (1,2,3, \dots . . P-1), A \in (1,2,3, \dots P-1)$

P و g معروفان لجميع تجهيزات المستخدمين في الشبكة

يولد UE-R القيمة Nj ثم يولد قيمة تجزئة Nj ويقوم بتشفيرها بالرقم السري B وإرفاقها بـ Nj

تسمى القيمة الناتجة التوقيع الرقمي DSigلـ UE-R والتي تعطى :

$$(DSig)_{UE-R} = \{Encrypt[Hash(N_j), B], N_j\} \qquad (3)$$

وبالمثل ، يولد UE-E القيمة Ni , ويولد قيمة تجزئة Ni المشفرة برقم سري A وإرفاقها بـ Ni تسمى القيمة الناتجة التوقيع الرقمي لـ UE-E والتي تعطى

$$(DSig)_{UE} = \{Encrypt[Hash(N_i), A], N_i\} \qquad (4)$$

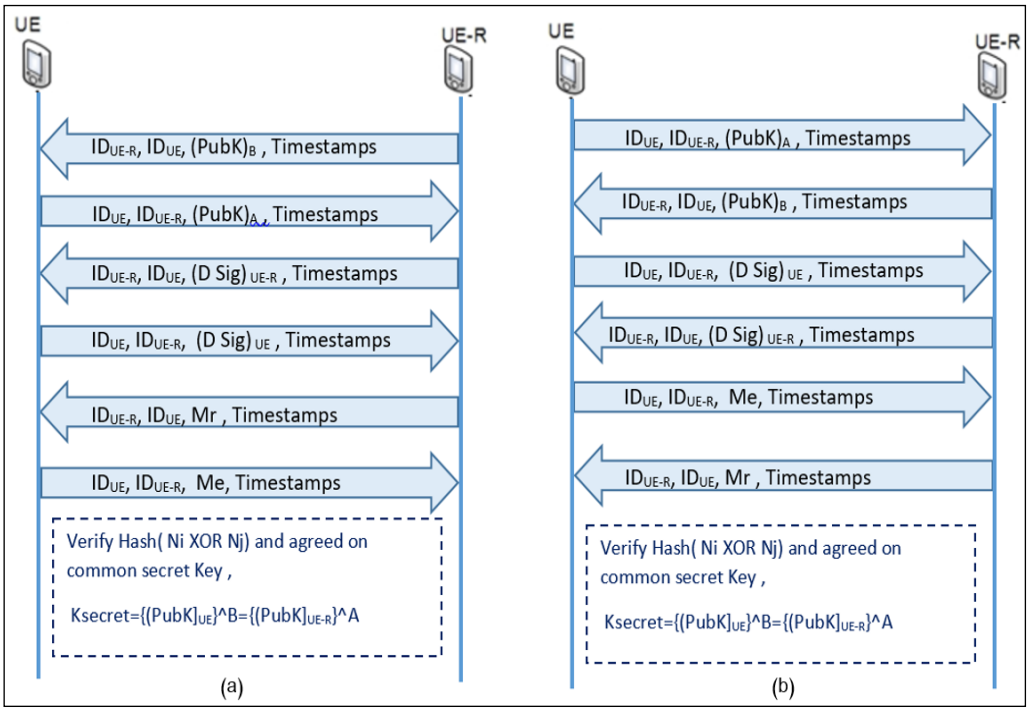
تقوم UE-R باستخراج Ni من التوقيع الرقمي وتحسب رسالة الإعلام:

$$M_r = Encrypt\{Hash(N_i \oplus N_j), (PubK)_{UE}\} \quad (5)$$

وبالمثل، فإن UE-E يستخرج Nj من التوقيع الرقمي ويحسب رسالة الإعلام

$$M_e = Encrypt\{Hash(N_j \oplus N_i), (PubK)_{UE-R}\} \quad (6)$$

يوضح الشكل (6) خطوات المصادقة المتبادلة وكذلك للاتفاق على مفتاح سري مشترك :



الشكل (6) تعزيز الأمن للبروتوكول للتفاعلي(a) و للبروتوكول اللاستباقي(b).

- الخطوة 1: بمجرد تلقي UE-R طلب اكتشاف من UE-E ، يرسل UE-R: $(PubK)_{UE-R}$ مع $(id)_{UE-R}, (id)_{UE}$ والطوابع الزمنية التي يتم إنشاء الرسالة عندها .
- الخطوة 2:يرسل UE-E : $(PubK)_{UE}$ جنبًا إلى جنب مع $(id)_{UE-R}, (id)_{UE}$ الطوابع الزمنية التي يتم إنشاء الرسالة عندها .
- الخطوة 3: يحسب UE-R التوقيع الرقمي $(DSig)_{UE-R}$ ويرسله مع الطابع الزمني الذي تم عنده انشاء التوقيع إلى UE-E
- الخطوة 4: يحسب UE-E التوقيع الرقمي $(DSig)_{UE}$ ويرسله مع الطابع الزمني الذي تم عنده انشاء التوقيع إلى UE-R
- الخطوة 5: UE-R يرسل ال Mr.
- الخطوة 6: UE-E يرسل ال Me.

يقوم كل من UE-E و UE-R بفك تشفير Me, Mr , بمفتاحهما الخاص والتحقق من التجزئة $(N_j \oplus N_i)$. بعد التحقق ، يتفق كل من UE-R & UE-E على إنشاء مفتاح سري ، يسمى K_{secret} المفتاح السري المشترك الذي يستخدم لتشفير / فك تشفير بقية الرسائل، يتم حساب K_{secret} كما يلي:

$$K_{secret} = ((PubK)_{UE-R})^A = ((PubK)_{UE})^B \quad (7)$$

7-1-3- طريقة عمل البروتوكول المحسّن

للحفاظ على صحة البيانات وتحقيقها للشروط الأمنية CIAAA ، من الضروري تشفير الرسائل والتوقيع عليها رقميًا باستخدام مفتاحها السري، والذي لا يمكن فك تشفيره والتحقق منه إلا لوحدات UE المصرح بها أو المصادق عليها [8]. هدفنا هو حماية الرسائل المتبادلة بين UEs من الدخلاء. لهذا الغرض، قمنا بتصميم بروتوكول مع تحسين الأمان، تكون قناة الاتصال بين أجهزة المستخدمين عامة، لذا من الممكن اعتراض الرسائل من قبل الدخيل. يجب التأكد من وجود وحدتين من أجهزة المستخدمين على اتصال مع تجهيزات UE شرعية. يمكن تحقيق ذلك من خلال عملية المصادقة المتبادلة، بشكل عام تعتمد آلية الأمن بين BS و UE على آلية الأمان القياسية الحالية التي يوفرها LTE-A [5] .

ومع ذلك ، نظرًا لعدم وجود بنية تحتية أمنية مركزية لاتصالات D2D ، يصبح الأمان غير مضمون. تم في هذا البحث التركيز على مصادقة اثنين من UEs وإنشاء مفتاح سري مشترك لا يعرفه سوى UEs المشاركة.

ينقسم بروتوكول الأمان المقترح إلى مرحلتين، مرحلة المصادقة المتبادلة ومرحلة الإعلام. أثناء مرحلة المصادقة المتبادلة، يتم استخدام التوقيع الرقمي للمصادقة على بعضها البعض، بينما في مرحلة الإعلام، تقوم وحدتان من تجهيزات المستعمل بإعلام بعضهما البعض بأنهما قد قاما بالتصديق على بعضهما البعض. في هذا البروتوكول، يتم إرسال كل الرسائل مع الطوابع الزمنية. يتم استخدام الطوابع الزمنية لمنع هجوم الإعادة. حيث أن هناك إمكانية لتسجيل الرسائل وإرسالها في فترة زمنية أخرى.

باستخدام الطوابع الزمنية Timestamps، يتحقق المستلم من الطوابع الزمنية الخاصة بالمرسل ويقارنها بالطوابع الزمنية الخاصة به التي تم استلام الرسالة عندها. في حال الاختلاف ، سيتم تجاهل الرسالة، بهذه الطريقة يمكن أن تمنع الطوابع الزمنية هجوم الإعادة، وبالمثل فإن كلاً من أجهزة المستخدمين تولد قيمة N بحيث لا يمكن استخدام المعلومات القديمة في هجوم إعادة التشغيل، N هو الرقم العشوائي الذي يتم استخدامه مرة واحدة فقط في اتصال التشفير.

يستخدم التوقيع الرقمي للتحقق من هوية المرسل وكذلك لسلامة البيانات [8]. يمكن لأي شخص في الشبكة التحقق من التوقيع الموقع رقميًا لأن جميع المستخدمين في الشبكة يعرفون المفتاح العام للمرسل ولكن المرسل فقط يمكنه توقيع الرسالة رقميًا لأن المرسل فقط لديه حق الوصول إلى المفتاح الخاص.

لذلك، فإن التحقق من التوقيع الرقمي يضمن شرعية أجهزة المستخدم الخاصة بالمرسل. في بروتوكول الأمان المقترح، يتم حساب قيمة التجزئة لـ N والتي يتم تشفيرها بعد ذلك بالرقم السري لـ UE الذي يسمى الشهادة. الشهادة مع N تسمى البيانات الموقعة رقمياً.

أثناء التحقق من التوقيع، يقوم المستقبل UE باستخراج رمز N والتوقيع. يحسب جهاز الاستقبال بعد ذلك القيمة N وكذلك فك تشفير التوقيع باستخدام المفتاح العام للمرسل واسترداد قيمة التجزئة لـ .N يقارن المتلقي الآن قيمة التجزئة المحسوبة وقيمة التجزئة المستردة للبيانات. إذا تطابقت قيمتا التجزئة، فإن المستلم يتحقق من أن المرسل حقيقي وشرعي وأن البيانات لا يتم العبث بها في طريقها. وبالتالي، فإنه يحافظ أيضًا على سلامة الرسائل.

بعد التأكيد المتبادل، ينبغي أن يبلغ كلا الجهازين بعضهما البعض بأنهما يقومان بالتصديق على بعضهما البعض. بالنسبة لعملية الإعلام، يحسب UE-R و UE رسالة الإعلام Mr و Me على التوالي. يقوم UE و UE-R بفك تشفير M_r و M_e على التوالي واستخراج التجزئة (Ni , Nj) يقارن كل من UE قيمة التجزئة المستلمة بقيمة التجزئة الخاصة بهما. إذا كانت قيمة التجزئة المحسوبة وقيمة التجزئة المستلمة متساوية، فإنهم يوافقون على إنشاء مفتاح سري مشترك يمكن استخدامه كمفتاح سري لعملية تشفير/ فك تشفير الرسائل.

8- تطوير خوارزمية لتشفير البيانات في الاتصالات D2D :

بعد مرحلة إنشاء المفتاح يتم التصريح ببدء الاتصال D2D وهنا يمكن تشفير البيانات حيث سيتم تصميم خوارزمية تشفير باستخدام توابع Logistic Map وتقنية المزج المتوازن للكتل BBM-Balanced Block Mixing.

تهدف هذه التقنية إلى تأمين عمل أجهزة محددة بتقنية الاتصالات D2D وذلك من أجل خدمات السلامة العامة وخاصة عندما يتطلب الأمر سرعة نقل عالية واستجابة سريعة أو لتجنب دخول أجهزة غير مرغوب بها على خطوط الاتصال، كما في حال الكوارث الطبيعية مما يستدعي دخول فرق معينة سواء لعمليات الحماية أو الإنقاذ وهنا يجب عدم السماح للأجهزة من خارج المجموعة بإنشاء اتصال D2D .

سنعتمد في هذا البحث على تطوير خوارزمية تشفير بيانات كتلية وكتل البيانات بطول 128-bit و طول المفتاح 128-bit.

وتركز عملية التطوير على بناء خوارزمية جديدة اعتماداً على توابع Logistic Map لتأمين عملية الخلط والتشفير لاعتمادها على مفاتيح خاصة وتوابع المزج المتوازن للكتل BBM لتكون مرحلة المزج والخلط ، حيث تمر البيانات بثلاث مراحل تشفير، وذلك كما يلي :

- طبقة حماية تسمى (Permutation) باستخدام مولد عشوائي يعتمد على معادلة Logistic Map بحيث يتم توليد مصفوفة قيم عشوائية تعتبر قاعدة معطيات لتنفيذ عملية الـ Permutation.
- طبقة المزج المتوازن للكتل(Balanced Block Mixing (BBM بما يمكن من بعثرة المعلومات وبالتالي تامين تشفير البيانات.
- المفاتيح المستخدمة في التشفير وفك التشفير هي كل من عنصر التحكم μ والقيمة الابتدائية x_n لمعادلة Logistic Map.
- الحصول على خوارزمية تشفير مكونة من مرحلتي Logistic Map ومرحلة Balanced Block Mixing ومفتاحين هما μ و x_n .

8-1- طبقة الحماية (Permutation) باستخدام مولد عشوائي يعتمد على معادلات Logistic Map

- بالاعتماد على معادلة الـ Logistic Map يتم إنشاء مصفوفة قيم عشوائية مكونة من 256-Byte تأخذ القيم من 0 حتى 255 وتتوزع على المصفوفة في مواقع عشوائية.
- معادلات Logistic Map هي جملة من المعادلات الرياضية والتي تعتمد لتوليد قيم عشوائية وسنعتمد منها Quadratic Recurrence Equation معادلة التكرار التربيعية[10] :

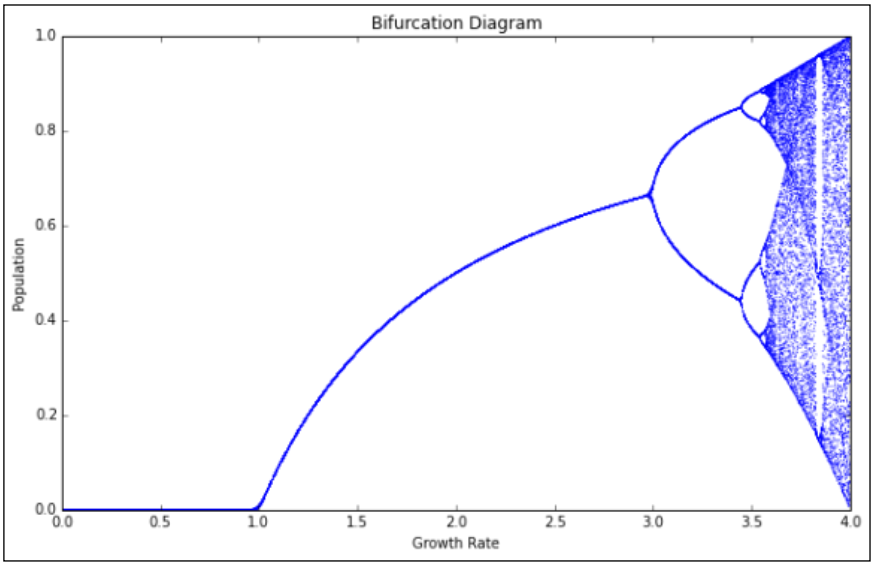
$$x_{n+1} = \mu\, x_n(1 - x_n) \qquad (8)$$

- وهي معادلة تعطي حلول عشوائية تبعاً لقيم بارامتر التحكم μ والذي يأخذ قيمه من المجال [1,4] وتتركز الحلول العشوائية حول القيمة (3.9) لبارامتر التحكم.

تعتبر x_n القيمة الابتدائية لحساب القيم والتي تعوض من المجال]0,1[.

وفي الدراسة التالية لمعادلات Logistic Map نوضح تغيرات المنطقة العشوائية تبعاً لتغيرات قيمة بارامتر التحكم μ ، مع اعتماد قيمة ابتدائية ثابتة وهي القيمة Xo=0.5 كما هو موضح في الشكل (7) [11] .

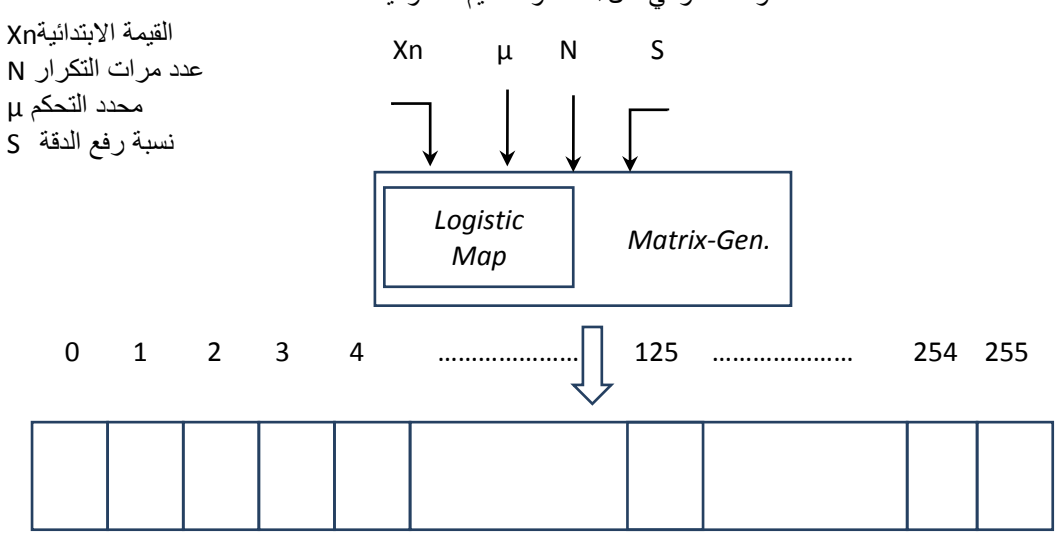
حيث نجد أن القيم المولدة بناءً على توابع Logistic Map تكون في أقصى العشوائية حول القيمة 3.9 لبارامتر التحكم.



الشكل (7) القيم العشوائية وفق تابع Logistic Map [11]

1-1-8 تصميم المولد العشوائي:

يتم توليد مصفوفة القيم العشوائية والتي تحوي صف و 256 عمود ما يؤمن 256 موقع ذاكري يعطى كل موقع Index من 0 حتى 255 كما هو موضح في الشكل (8) وهو عبارة عن مخطط يحاكي المولد البرمجي للمصفوفة والذي يتضمن محددات تابع Logistic Map بالإضافة إلى المحددات البرمجية المتعلقة بطول المصفوفة المقترحة :



الشكل(8) توليد مصفوفة القيم العشوائية وفق Logistic Map

إجرائية توليد مصفوفة القيم العشوائية:

1) Select Xn,μ,N,S // تحديد بارامترات طبقة الحماية
2) Xn= μXn(1-Xn)
Xn= Xn+1

الضرب بمعامل تغيير الدقة S ثم إيجاد باقي القسمة مع 256 لضمان أن فضاء القيم أقل من هذه القيمة أي بين 0 و 255وهي القيم التي نود وضعها في المصفوفة.

3) y=int(Xn+1*S)mod256
4) تخزين القيمة في مصفوفة القيم العشوائية إن لم تكن مكررة
5)1 زيادة موقع المصفوفة بمقدار
6) Go to 2

يقوم المولد العشوائي بالاعتماد على معادلة Logistic Map لتوليد قيم عشوائية وتخزينها في المصفوفة المكونة من صف و256 عمود وكل قيمة من هذه القيم ستأخذ موقع ذاكري ضمن المجال من 0 حتى 255.

- سيتم التعامل مع كتلة معطيات بطول 128-bit .
- تعتبر كتلة البيانات الحقيقية (النص الصريح) المكونة من 128-bitدخل طبقة الحماية بحيث تقابل قيم البيانات مع محتويات مصفوفة القيم العشوائية وتقابل كل قيمة(value) مع الموقع (index) الخاص بها وبالنتيجة نحصل على كتلة معطيات مكونة من قيم المواقع (index) المقابلة للقيم الحقيقية من مصفوفة القيم العشوائية.
- تعتبر مصفوفة القيم العشوائية بمثابة شيفرة سرية سيتم الاعتماد عليها من أجل عملية البعثرة Permutation وهذه العملية صعبة الكسر أو التوقع كونها تعتمد على مصفوفة يتم توليدها باستخدام معادلة غير عكوسه بالإضافة إلى أنها تعتمد على عدة بارامترات حيث يستخدم كل من بارامتر التحكم μ والقيمة الابتدائية x_n كمفاتيح تشفير وفك تشفير في الخوارزمية المقترحة.
- وهنا نجد أحد اعتبارات قوة الخوارزمية كون مرحلة البعثرة غير عكوسه أي لا يمكن اعتماد معادلات Logistic Map لإعادة توليد قيم الدخل بدءاً من قيم الخرج حيث نقوم بعملية العكس (تستخدم في فك التشفير) برمجياً وذلك بالاعتماد على محتوى مصفوفة القيم العشوائية ذاتها المستخدمة في البعثرة (تستخدم في عملية التشفير) كما سنرى في المثال التالي:

1-1-1-8 عملية البعثرة Permutation المستخدمة في عملية التشفير:

بفرض لدينا نص صريح يحتوي كتلة معطيات بطول 128-bit (16-Byte) كما يلي:

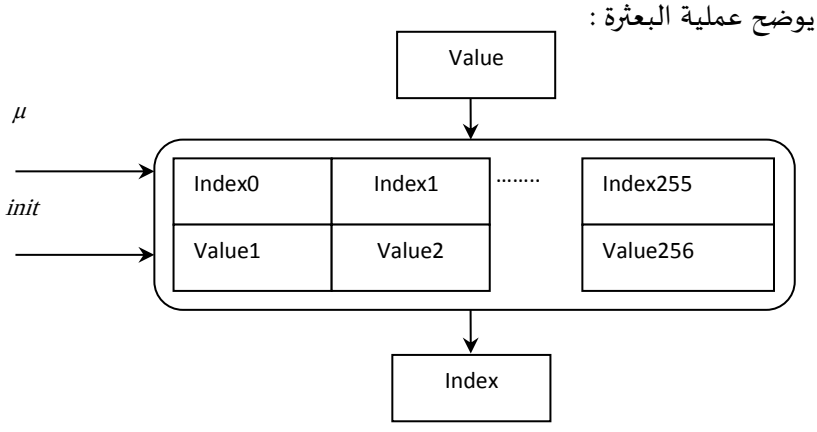
(value) 100, 22, 100, 77, ……, 33

تقارن القيم (value) مع محتويات مصفوفة القيم العشوائية بحيث نأخذ موقع(index).

نأخذ قيم المواقع لتصبح هي كتلة معطيات خرج مرحلة Logistic Map كما يلي :

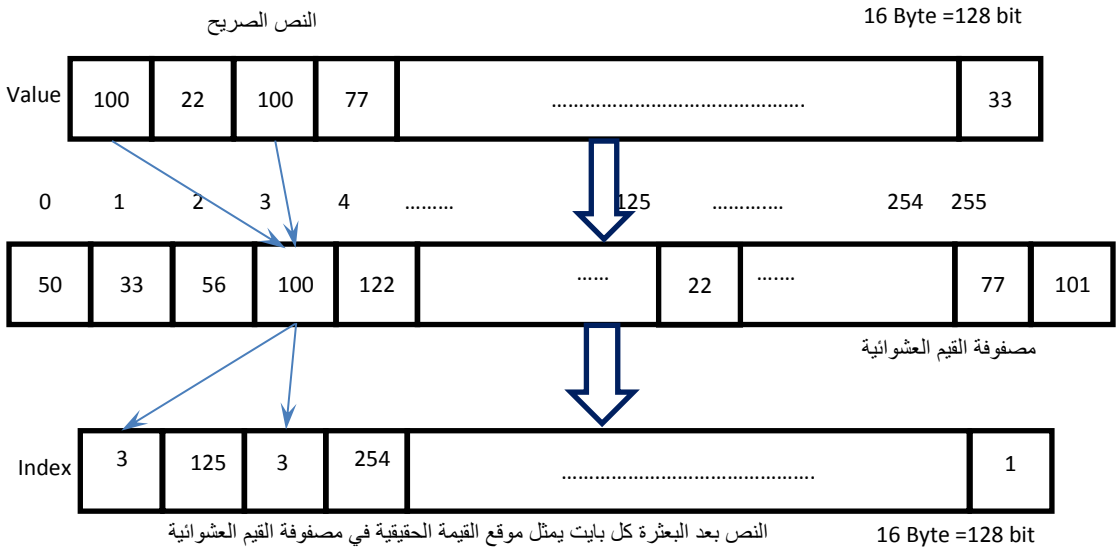
(index)3 , 125 , 3 , 254 , …….. , 1

الشكل (9) يوضح عملية البعثرة :



الشكل (9) المخطط الصندوقي لعملية البعثرة

وبشكل تفصيلي:



الشكل(10) إجرائية البعثرة للنص الصريح وفق مصفوفة القيم العشوائية

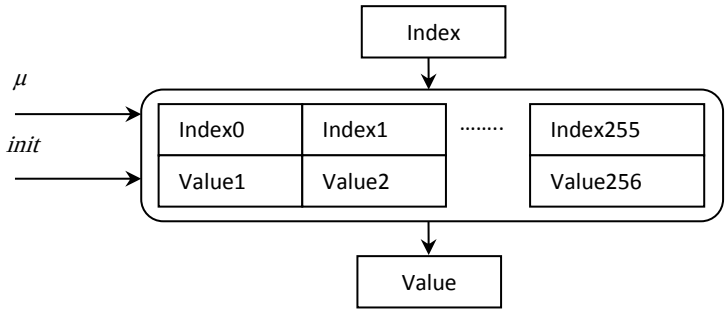
8-1-1-2- عملية عكس البعثرة Inverse-Permutation المستخدمة في عملية فك التشفير:

تكون كتلة البيانات هي عبارة عن قيم المواقع الذاكرية (خرج البعثرة في التشفير) .

تدخل كتلة البيانات1 , ... , 254 , 3 , 125 , 3(Index)

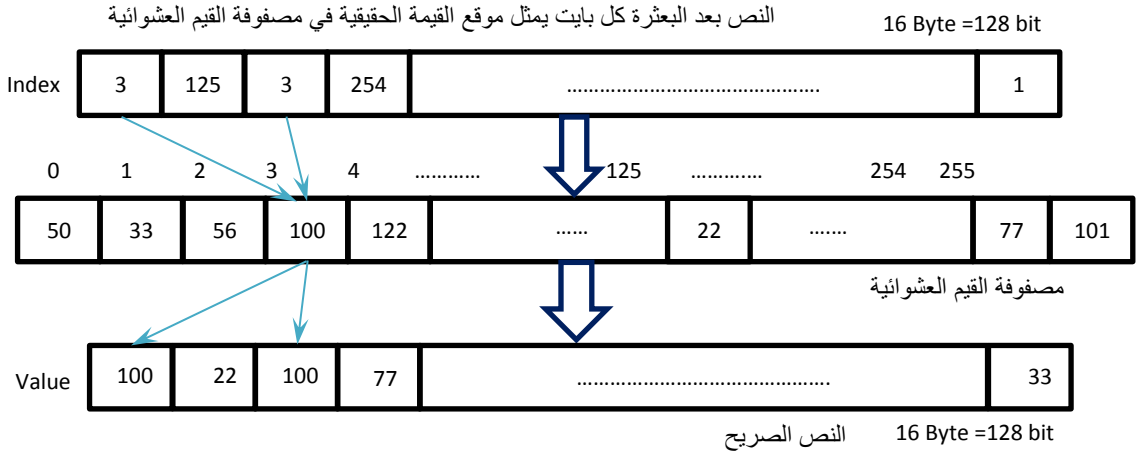
إلى طبقة الحماية وكل قيمة موقع تستخرج القيمة المخزنة المقابلة لها لنحصل على البيانات الصريحة 100, 22, 100, 77, ..., 33 (Value)

وهذا موضح في الشكل (11) .



الشكل (11) المخطط الصندوقي لعملية عكس البعثرة

وبشكل تفصيلي:



الشكل (12) إجرائية عكس البعثرة للنص المشفر وفق مصفوفة القيم العشوائية

إن عملية العكس تتم برمجياً دون إعادة توليد مصفوفة القيم العشوائية كون معادلات Logistic Mapغير عكوسه ، حيث تصبح المصفوفة المولدة من أجل عملية تشفير واحدة هي بمثابة قاعدة معطيات لكافة عمليات التشفير وفك التشفير المعتمدة على نفس المفاتيح.

- **مرحلة المزج المتوازن للكتل (Balanced Block Mixing (BBM**

- تتوضع طبقة الBBMبعد طبقة الحماية في مرحلة الدخل وبعدها في مرحلة الخرج بحيث يقسم ناتج عملية البعثرة إلى كتلتين كل منها 64-bit ويكون P بطول 65-bit [12] .
- ناتج طبقة المزج المتوازن هو كتلتين كل منهما 64-bit .
- معادلات المزج المتوازن هي معادلات عكوسة وبالتالي يمكن استخدامها في التشفير وفك التشفير[12].

معادلات الـ BBM

$$X,Y \longrightarrow A,B$$

$$A = 2X (+) 3Y \ mod(2) \ mod(p)$$

$$B = 3X (+) 2Y \ mod(2) \ mod(p)$$

المعادلات العكوسة لـ BBM

$$A,B \longrightarrow X,Y$$

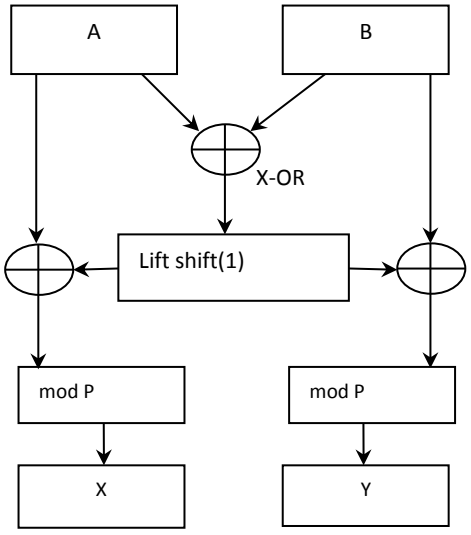
$$X = 2A (+) 3B \ mod(2) \ mod(p)$$

$$Y = 3A (+) 2B \ mod(2) \ mod(p)$$

حيث:

- ×2 هي إزاحة خانة لليسار
- ×3 هي ×2 ثم XOR مع X
- mod(2):عملية+هي exclusive-OR
- P هو عدد أولي يكون أكبر من X أو Y بمقدار خانة ليعيد ناتج أي عملية إلى فضاء القيم.

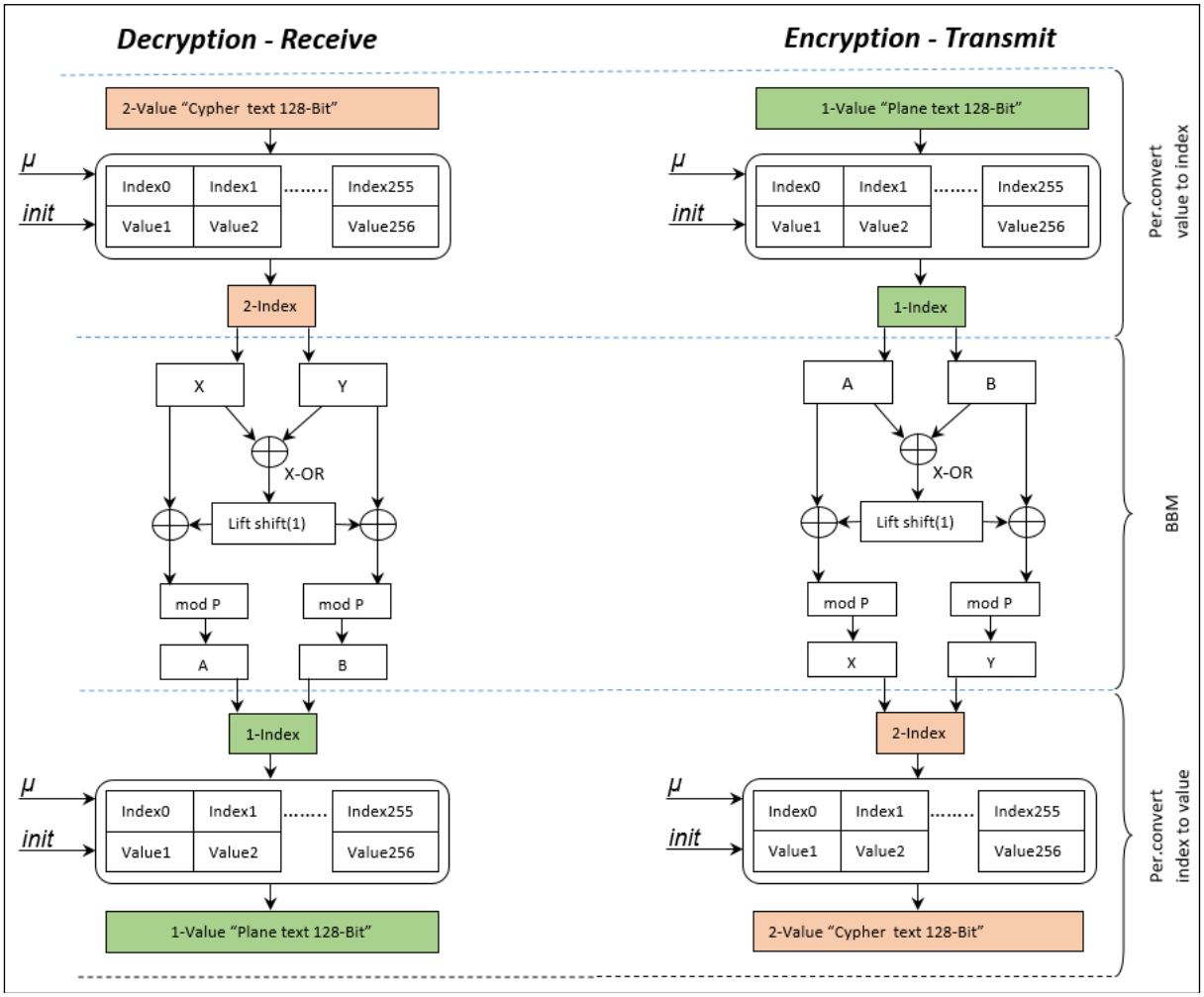
يوضح الشكل (13) المخطط الصندوقي لطبقة المزج :



الشكل (13) المخطط الصندوقي لطبقة المزج BBM

2-8 خوارزمية التشفير وفك التشفير المقترحة:

يوضح الشكل (14) بنية الخوارزمية المقترحة:



الشكل (14) المخطط الصندوقي لخوارزمية التشفير وفك التشفير المقترحة

حيث تبدأ عملية التشفير بدخول كتلة البيانات 128 bit إلى مرحلة الحماية أو البعثرة وهي تعتمد على معادلات Logistic Map لنحصل على بيانات تمثل مؤشرات مواقع البيانات الأصلية.

بعدها تتم عملية الخلط المتوازن لكتلة البيانات تلك بإدخالها إلى مرحلة المزج المتوازن للكتل بعد أن يتم تقسيمها إلى كتلتين كل منهما 64 bit.

خرج المرحلة السابقة يعاد إدخاله إلى مرحلة البعثرة ثانية وذلك بغرض إيجاد تسلسل عمل للخوارزمية في عملية التشفير يمكن عكسه عند عملية فك التشفير وكذلك نجد أن الخوارزمية مكونة من ثلاثة مراحل Rounds وهذا يعطيها قوة من حيث التشفير وممانعة أعلى في مواجهة الاختراق.

1-2-8 عملية التشفير وفك التشفير باستخدام الخوارزمية المقترحة:

يتم تنفيذ عملية التشفير حسب الخطوات التالية :

1- نأخذ كتل البيانات وهي القيم (Value) بطول 128-bit بحيث يتم دخولها إلى طبقة الحماية والخروج بكتلة معطيات بعد البعثرة مكونة من 128-bit وهي عبارة عن مواقع القيم (Index).

2- بعدها نجزئ خرج المرحلة السابقة إلى كتلتين كل منهما 64-bit لتكون دخل طبقة المزج المتوازن للكتل ونحصل بعد المزج على كتلة بطول 128-bit.

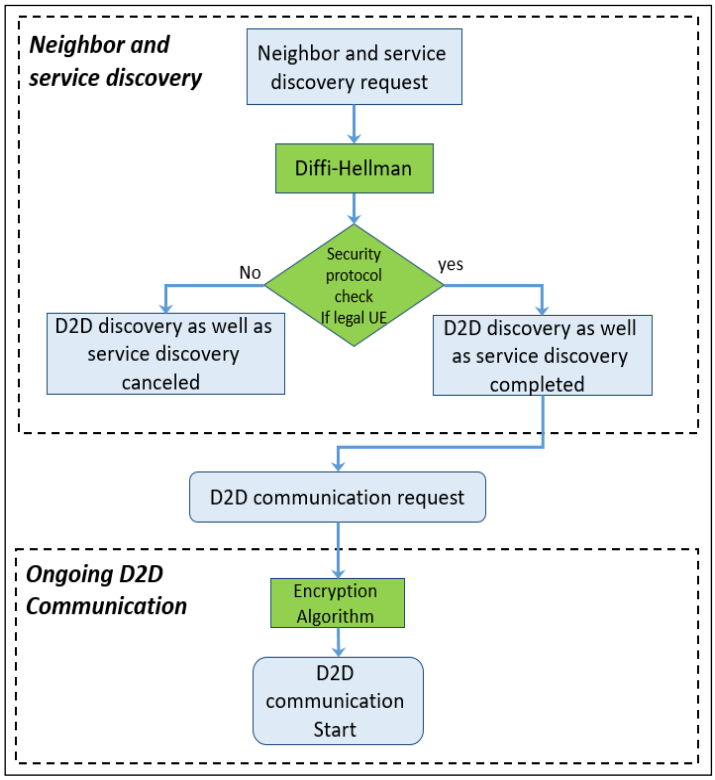
3- وبعدها يتم إدخالها إلى طبقة الحماية حيث نأخذ كتل البيانات وهي عبارة عن مواقع (Index) بطول 128-bit بحيث يتم إدخالها إلى طبقة الحماية والخروج بكتلة بيانات بعد البعثرة مكونة من 128-bit وهي عبارة عن القيم المقابلة (Value) ويكون الخرج هو النص المشفر.

في عملية فك التشفير يتم إدخال كتلة البيانات المشفرة لتمر بنفس مراحل عملية التشفير ونحصل في نهايتها على النص الصريح.

3-8 بروتوكولات الاكتشاف بعد تحسين الأمان المقترح.

تمت إضافة بروتوكول تحسين الأمان في تصميم بروتوكولات الاكتشاف المقترح، بالنسبة للبروتوكول التفاعلي.

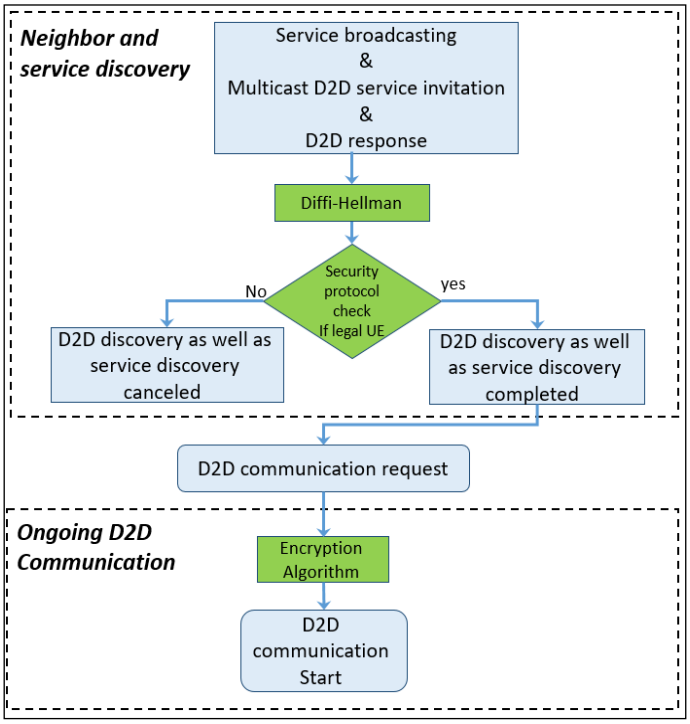
يبدأ UE-R بروتوكول تحسين الأمن بعد أن يتلقى طلب الجوار والاكتشاف من UE لا تنقل UE-R الطلب المرسل من UE إلى BS حتى تصادق UE كما هو مبين في الشكل (15) .



الشكل (15) تحسين الأمان المقترح في البروتوكول التفاعلي.

وتصبح عملية الحماية الأمنية الكاملة بإضافة البروتوكول الأمني المعزز وكذلك مرحلة تشفير البيانات التي يتم تبادلها بالاعتماد على تقنية المزج المتوازن للكتل .

بالنسبة للبروتوكول الاستباقي ، يبدأ UE بروتوكول تحسين الأمن بعد تلقيه دعوة خدمة الإرسال المتعدد D2D من UE-R كما في الشكل (16)



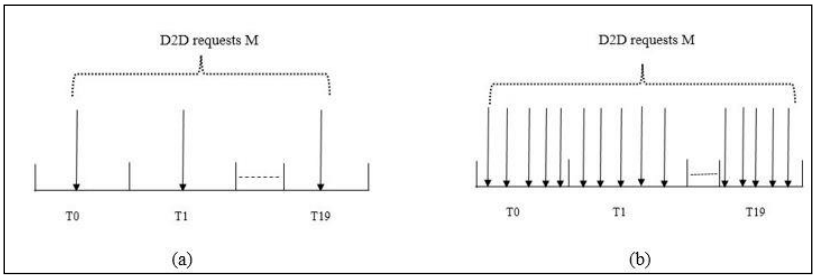
الشكل (16) تحسين الأمان المقترح في البروتوكول الاستباقي.

كذلك تصبح عملية الحماية الأمنية الكاملة بإضافة البروتوكول الأمني المعزز وكذلك مرحلة تشفير البيانات التي يتم تبادلها بالاعتماد على تقنية المزج المتوازن للكتل.

9- الدراسة العملية:

9-1 حساب حمل البروتوكولات حسب عدد الطلبات:

- الحالة 1: عدد الطلبات نفسه خلال الفترة الزمنية



الشكل (19) العدد الاجمالي لطلبات D2D في كل فترة زمنية (a) واحد (b) أكثر من واحد [13] .

نفترض في الحالة (b) أن عدد الطلبات D2D هو خمسة وتحسب نسبة حمل التأشير أو التحكم في البروتوكول الاستباقي والتفاعلي كما في المعادلتين.

$$CO_p = \frac{T' \times \left(2 + (14 \times M)\right) + \left(2 \times (T - T')\right)}{T} \qquad (14)$$

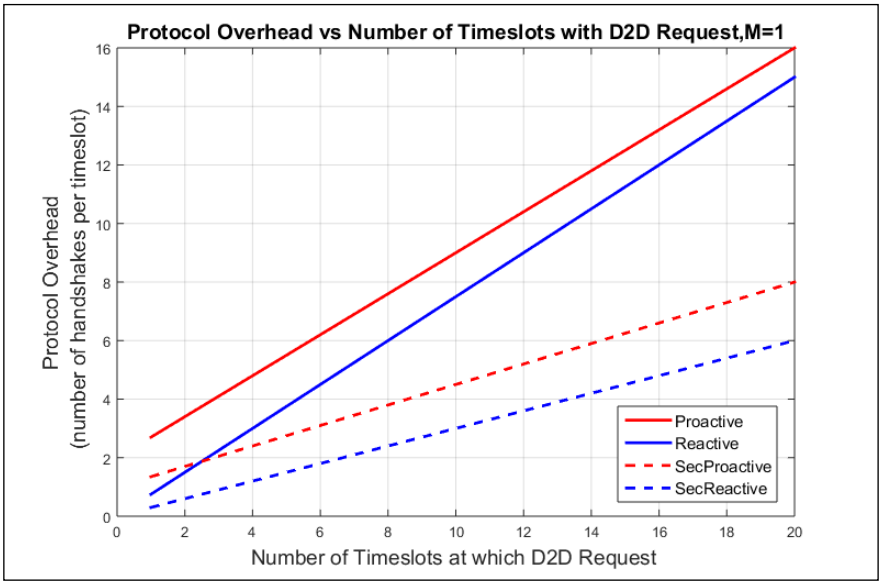
$$CO_r = \frac{T' \times 15 \times M}{T} \qquad (15)$$

يتم تحديد محددات الشبكة لحساب الحمل الزائد Overhead للبروتوكولات الاستباقية والتفاعلية قبل وبعد عملية تحقيق التعزيز الأمني كما في الجدول (1).

الجدول (1) قيم محددات الشبكة المعتمدة في حساب حمل البروتوكولات.

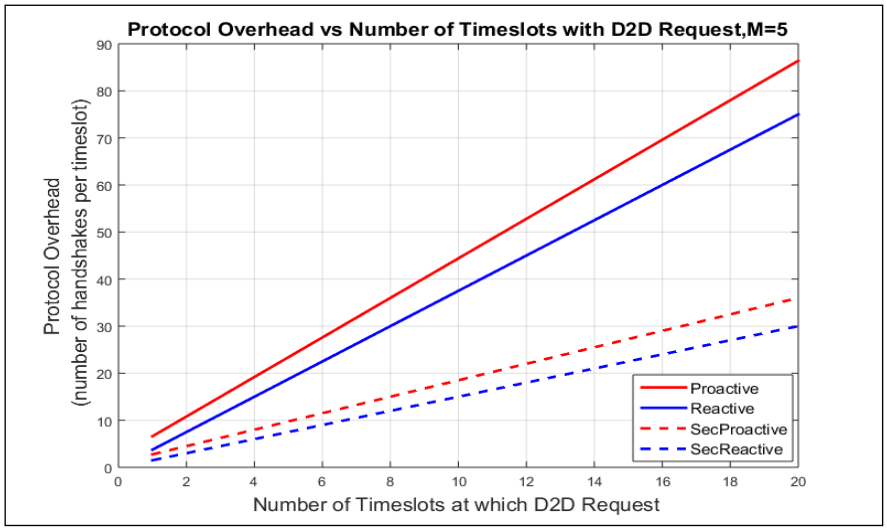
Parameters	Symbols	Values
العدد الإجمالي لوحداتUE	N	15
عدد UEs المشاركة في اتصالاتD2D	n	10
إجمالي الفترات الزمنية	T	20
الفترات الزمنية التي يحدث فيها طلبD2D	T′	1 to T
طلبات D2D في كل فترة زمنية	M	1 and 5

يوضح الشكل (20) الحمل Overhead للبروتوكولات، باعتبار ان عدد الطلبات في كل فترة زمنية هو M=1 ، حيث نلاحظ انخفاض الحمل في بروتوكولات الاكتشاف المعززة امنياً ، وذلك نتيجة البروتوكول الأمني الذي يجعل عمليات المصافحة بين الأجهزة مقتصرة فقط على الأجهزة التي يتم التعارف بينها ويتم رفض الأجهزة الغير مصرح لها بإنشاء الاتصال .



الشكل (20) حمل البروتوكولات تبعاً للفترة الزمنية حيث M=1

يوضح الشكل (21) الحمل الزائد Overhead للبروتوكولات، باعتبار ان عدد الطلبات في كل فترة زمنية هو M=5 ونلاحظ نفس النتائج في الحالة السابقة والتي تشير إلى انخفاض الحمل في البروتوكولات المعززة أمنياً عن البروتوكولات الغير معززة أمنياً .



الشكل (21) حمل البروتوكول تبعاً للفترة الزمنية حيث M=5

- الحالة 2 : حالة التوزيع الطبيعي لطلبات D2D

بافتراض أن N هو العدد الإجمالي لـ UEs التي تولد طلب D2D وأن M هو عدد الطلبات التي يتم توليدها في كل مرة - والتي تتبع التوزيع الطبيعي.

يُحسب تابع كثافة الاحتمال PDF لطلبات D2D المولدة بشكل طبيعي كما هو في المعادلة التالية [14].

$$PDF = \frac{1}{\sigma\sqrt{2\pi}} exp^{\frac{-(M-\mu)^2}{2\sigma^2}} \qquad (16)$$

حيث

μ هي القيمة المتوسطة لطلبات D2D الناتجة عن UEs

σ هي الانحراف المعياري للتوزيع الغاوسي العادي.

قيمة μ هي 2.14 وقيمة σ هي 3.8 ،و يُحسب مقدار الحمل للبروتوكولات الاستباقية والتفاعلية لطلبات D2D الموزعة بشكل طبيعي على النحو التالي:

$$CO_p = \frac{2 \times (T - T') + T' \times (2 + 14 \times M)}{T} \qquad (17)$$

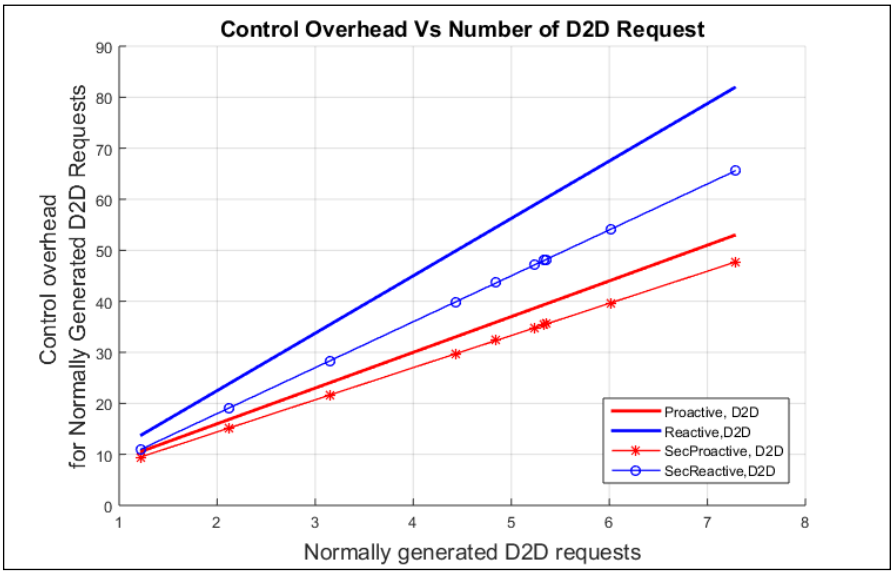
$$CO_r = \frac{T' \times 15 \times M}{T} \qquad (18)$$

حيث تشير COr إلى حمل التحكم Overhead في البروتوكول التفاعلي ويشير CO_P إلى حمل التحكم للبروتوكول الاستباقي.

الجدول (2) قيم محددات الشبكة المستخدمة في حساب حمل التحكم للبروتوكولات.

Parameters	Symbols	Values
العدد الإجمالي لوحداتUE	N	10
إجمالي الفترات الزمنية	T	20
الفترات الزمنية التي يحدث فيها طلبD2D	T′	T
طلبات D2D في كل فترة زمنية	M	0 to N

يوضح الشكل (22) حمل البروتوكول مقابل طلب D2D ذات التوزع الطبيعي.

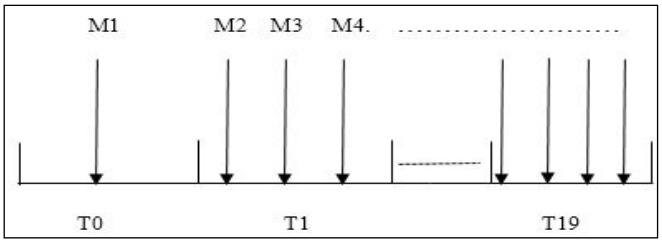


الشكل (22) حمل البروتوكولات مع عدد طلبات D2D الموزعة طبيعياً

حيث يظهر تزايد حمل البروتوكول التفاعلي مقارنة مع البروتوكول الاستباقي مع تزايد عدد طلبات D2D في كل فاصل، أي أنه مع تزايد عدد طلبات D2D والموزعة طبيعياً فإن البروتوكول الاستباقي يعطي نتائج أفضل بعد الفاصل الزمني الثاني أي مع بدء زيادة عدد الطلبات.

- الحالة 3 : التوزيع العشوائي لطلبات D2D.

يوضح الشكل (23) التوزع العشوائي لطلبات D2D في كل فاصل زمني حيث عدد طلبات D2D لكل غير ثابت.



الشكل (23) التوزع العشوائي لـ UEs [13]

ويتم حساب الحمل لكل من البروتوكول الاستباقي والتفاعلي على النحو التالي:

$$CO_p = \frac{T' \times (2 + (14 \times M)) + (2 \times (T - T'))}{T} \quad (19)$$

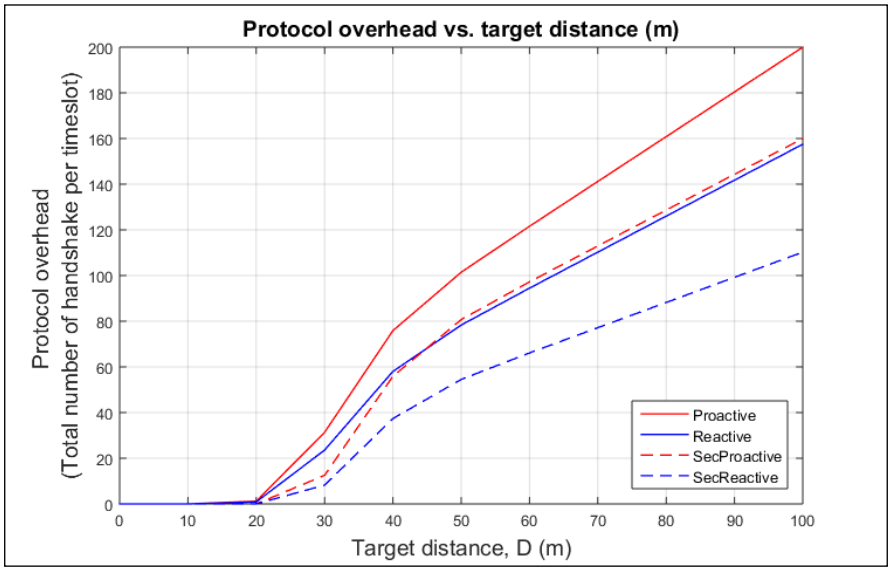
$$CO_r = \frac{(T' \times 15 \times M)}{T} \quad (20)$$

النتائج حسب الحالة 3

الجدول (3) محددات الشبكة لحساب مقدار الحمل حسب الحالة 3 .

Parameters	Symbols	Values
العدد الإجمالي لوحدات UE	N	15
عدد مستخدمي UE لخدمات التقارب من بين إجمالي المستخدمين N	n	10
إجمالي الفترات الزمنية	T	20
الفترات الزمنية التي يحدث فيها طلب D2D	T'	14
طلبات D2D في كل فترة زمنية وتأخذ قيم قيمة عشوائية	M	0 to n
المسافة المستهدفة	d	0 to 100 meter
المسافة القصوى بين UE-R و UE	D	100 m
نصف قطر خلية تغطية الشبكة	R	1000 m
المسافة بين حافة تغطية الشبكة وUE-R	h	m 20

يوضح الشكل (24) علاقة حمل البروتوكول تبعاً للمسافة بين المرحل والجهاز UE أي أنه مع ازدياد المسافة يزداد الحمل .



الشكل (24) حمل البروتوكول تبعاً للمسافة D(m)

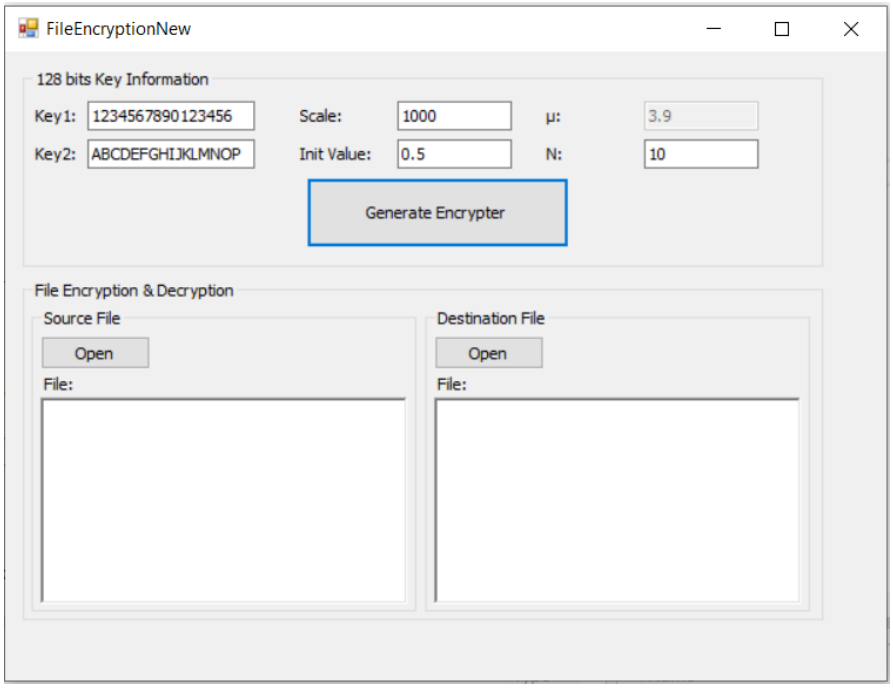
هنا يكون البروتوكول المعزز أمنياً أكثر فاعلية لأنه يولد مقداراً أقل من الحمل بالمقارنة مع البروتوكول الغير معزز.

وبالمقارنة نجد أن البروتوكول التفاعلي يكون خيار أفضل مع ازدياد المسافة كونه يحقق حملاً زائداً أقل عما هو عليه في البروتوكول الاستباقي.

2-9 تنفيذ خوارزمية التشفير المقترحة في لغة البرمجة C# :

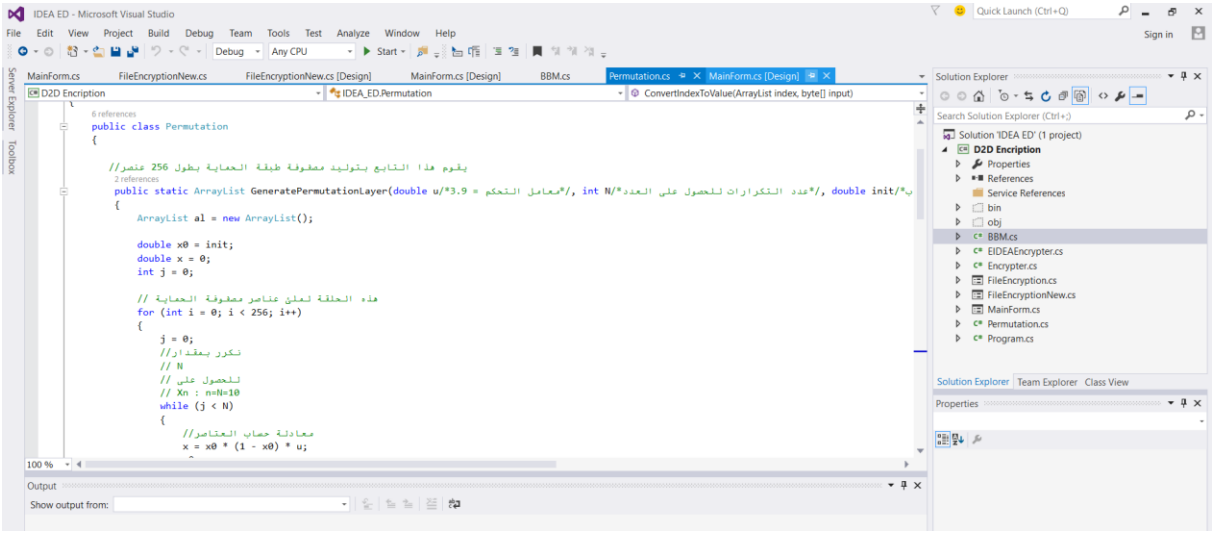
تم بناء برنامج ذو واجهة نوافذ وقد اقتصر تمثيل البيانات التي يتم تبادلها على ملفات نصية بحيث يتم بداية تحويلها إلى لغة ASCII ومن ثم تحول إلى الصيغة الرقمية binary ليتم تقسيم البيانات إلى كتل كل منها 128bits لتبدأ عملية التشفير عليها بدخولها في مراحل الخوارزمية المقترحة.

وقد تم برمجة محاكي لعملية التشفير القائمة على تابع Logistic Map وكذلك معادلات المزج المتوازن للكتل BBM ، حيث يوضح الشكل (25) واجهة عمل برنامج التشفير.



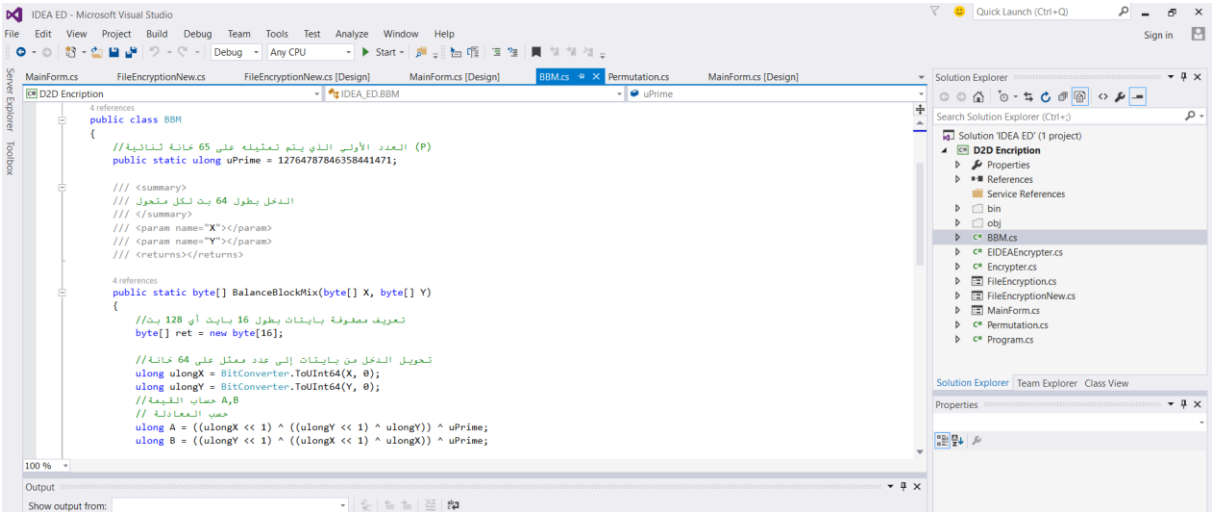
الشكل (25) واجهة تنفيذ عملية التشفير

يوضح الشكل (26) التابع Logistic Map وتنفيذ مرحلة التبديل Permutation في بيئة البرمجة C#



الشكل (26) مرحلة التبديل Permutation في بيئة البرمجة C#

يوضح الشكل (27) بناء معادلات BBM في بيئة البرمجة C#



الشكل (27) مرحلة المزج المتوازن للكتل BBM في بيئة البرمجة C#

10-النتائج:

توضح نتائج المحاكاة تحسن قيم الحمل لتصبح أقل وذلك نتيجة انخفاض عدد الأجهزة التي تدخل في إجرائية الاكتشاف وإقامة الخدمة بناء على اقتصار الاكتشاف على الأجهزة المصرح لها أمنياً ، حيث نجد انخفاض الحمل Overhead بنسب تتراوح من 30% إلى 50% .

ومن ناحية ثانية بناء برنامج تشفير يحاكي الخوارزمية التي تم تصميمها يعطي أمان وسرية للمعلومات التي يتم تبادلها بين الأجهزة، حيث أن التنفيذ العملي لخوارزمية التشفير أعطى نصوص مشفرة غير قابلة للفهم ولا يمكن إعادة توليدها بغياب محددات بناء الخوارزمية ومفاتيحها.

11-خلاصة البحث:

اقترح هذا البحث بروتوكول تحسين الأمان لبروتوكولات اكتشاف الجوار والخدمة، التفاعلية والاستباقية. وشرح التحديات الأمنية والتهديدات المحتملة للسيناريوهات المختارة لاتصالات D2D .

يعتمد بروتوكول تحسين الأمان المقترح على خوارزمية تبادل مفتاح .Diffi-Hellman يستخدم التوقيع الرقمي للمصادقة المتبادلة، يتم تبادل رسائل الإعلام لتأكيد التحقق، بعد عملية التحقق، اتفق UE و UE-R على المفتاح السري المشترك، والذي يمكن استخدامه لتشفير/ فك تشفير الرسائل المتبادلة بينهما. يبدأ بروتوكول تحسين الأمن في البروتوكول التفاعلي المقترح بعد أن يتلقى UE-R رسالة اكتشاف من UE .

من ناحية أخرى، في البروتوكول الاستباقي المقترح، يبدأ بروتوكول تحسين الأمن من قبل UE بعد تلقي رسالة "دعوة خدمة الإرسال المتعدد "D2D من UE-R .

كما تمت عملية تشفير البيانات بتصميم خوارزمية تشفير مبنية على توابع Logistic Map ومعادلات المزج المتوازن للكتل BBM وذلك استكمالاً لمرحلة بروتوكول الاكتشاف المعزز ، بما يضمن تبادل البيانات بشكل آمن .

12-التوصيات:

ركز البحث على الدراسة التصميمية والمحاكاة سواء من حيث بروتوكول الاكتشاف أو خوارزمية التشفير ، سيكون من المفيد والمقنع أكثر تنفيذ نتائج البحث عملياً عن طريق تصميمه كبرامج يمكن ان تحمل على الهواتف النقالة أو أن تفعل في شبكات الاتصالات بحيث يمكن الاستخدام الفعلي لهذه التصاميم واختبار نتائجها على أرض الواقع .

13- المراجع:

[1] F.J. Cintrón, D. W. Griffith, C. Liu, R. A. Rouil, Y. Sun, J. Wang, P. Liu, C. Shen, A. Ben Mosbah, S. Gamboa Quintiliani, 2021 "Study of 5G New Radio (NR) Support for Direct Mode Communications", Gaithersburg, MD, USA.

[2] P.K.Malik,D.S.Wadhwa,andJ.S.Khinda, ,2020 "Asurvey of device to device and cooperative communication for the future cellular networks," International Journal of Wireless Information Networks, pp.1–22.

[3] F.Jameel, Z.Hamid, F.Jabeen, S.Zeadally,andM.A.Javed, ,2018 "Asurvey of device-to-device communications: Research issue challenges," IEEE Communications Surveys &Tutorials,vol.20,no.3,pp.2133–2168.

[4] H. Esmat,M.M.Elmesalawy,andI.Ibrahim, ,2018 "Uplink resource allocation and power Control for d2d communications underlaying multi-cell mobile networks," AEU International Journal of Electronics and Communications, vol.93,pp.163–171.

[5] M. Alam, D. Yang, J. Rodriguez, and R. Abd-Alhameed, "Secure device-todevice communication in lte-a April 2014," Communications Magazine, IEEE, vol. 52, no. 4, pp. 66–73,.

[6] Anuradha Bista and Milka Radin May 26, 2015, " Neighbor and Service Discovery Protocols with Security Enhancement for Device-to-Device Communication in LTE"{LTE-A Cellular Networks .

[7] Sura Fahmy February 2021, "Secure voice cryptography based on Diffie-Hellman algorithm, University of Diyala" , Article in IOP Conference Series Materials Science and Engineering · DOI: 10.1088/1757-899X/1076/1/012057

[8] M. Stamp, Information security: principles and practice. John Wiley & Sons, 2011.

[9] W. Shen, W. Hong, X. Cao, B. Yin, D. Shila, and Y. Cheng, 2014 "Secure key establishment for device-to-device communications," in Global Communications Conference (GLOBECOM), IEEE, Dec 2014, pp. 336–340.

[10] Michelle Rudolph-Lilith *, Lyle E. Muller, (2014) On a representation of the Verhulst logistic map, UnitΘ de Neurosciences, Information et ComplexitΘ (UNIC) CNRS, 1 Ave de la Terrasse, 91198 Gif-sur-Yvette, France, Discrete Mathematics 324 19–27

[11] Viviana Costinela Preduna, 2012 "The logistic map of matrices " , Universitat Polit_ecnica de Val_encia,Valencia - September 13,

[12] Balanced Block Mixers for Block Cipher Cryptography Efficient, Flexible,Guaranteed Mixing- 1998-Terry Ritter-ritter@io.com -Ritter Software Engineering.

[13] Yue Wu, July 2016. "Advanced Technologies for Device-to-device Communications Underlaying Cellular Networks " , Department of Electronic and Eletrical Engineering University of Sheffield ,

[14] A. Papoulis and S. U. Pillai, , 2002 , " Probability, random variables, and stochastic processes" . Tata McGraw-Hill Education.

[15] J. W. Harris and H. St¨ocker, 1998," Handbook of mathematics and computational science" . Springer Science & Business Media.

[16] Yasir Javed, Adnan Shahid Khan; July 2019 " Major Security attacks in D2D Communication" ; Ubiquitous Computing and Communication Journal ·