مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (39) العدد (6) 2017
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (39) No. (6) 2017

Authentication Protocol in Device to Device in LTE Networks

Dr.Ahmad Saker Ahmad [*]
Amany Stiety**

(Received 31 / 8 / 2017. Accepted 2 / 11 / 2017)

□ ABSTRACT □

A constant need to increase the network capacity for meeting the growing demands of the subscribers has led to the evolution of cellular communication networks from the first generation (1G) to the fifth generation (5G). There will be billions of connected devices in the near future. Demanding higher data rates, lesser delays ،enhanced system capacity and superior throughput. The available spectrum resources are limited and need to be flexibly used by the mobile network operators (MNOs) to cope with the rising demands. The solution was the device-to-device connections.

Enabling Device to Device (D2D) communications over LTE-A networks (Long Term Evaluation-Advanced) can provide many benefits in terms of throughput ،energy consumption ،traffic load. It also enables new commercial services.

Such as location-based advertising. For these reasons ،D2D communications has become A hot topic in both the academic and industrial communities. However ،many research works are focused on node discovery ،radio resource management ،and other aspects ،while the issue of security is less addressed. In this article ،،we intend to provide an overview of the security architecture ،threads ،and requirements ،and authentication protocols.

Keywords: Authentication and Key Agreement in LTE-A Network ،security ، device-to-device connection.

[*] **Professor, Department of System and Networks Computing, Faculty of Informatics Engineering, Tishreen University, Lattakia, Syria**
****Postgraduate student,Department of System and Networks Computing, Faculty of Informatics Engineering,Tishreen University, Lattakia, Syria.**

مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (39) العدد (6) 2017
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (39) No. (6) 2017

بروتوكول المصادقة في اتصال جهاز إلى جهاز في شبكات LTE

الدكتور أحمد صقر احمد*

أماني ستيتي**

(تاريخ الإيداع 31 / 8 / 2017. قُبِل للنشر في 2/ 11 / 2017)

□ ملخّص □

الحاجة الماسة لزيادة قدرة الشبكة من أجل توفير المعلومات والمتطلبات للمشتركين أدى إلى تطوير شبكات الاتصال الخلوية من الجيل الأول إلى الجيل الخامس.

ففي المستقبل القريب سيكون هناك مليارات من الأجهزة المتصلة والتي تتطلب معدل بيانات أكبر، زمن تأخير أقل، قدرة نظام أعلى إضافة إلى انتاجية أفضل. ولكن الموارد المتاحة محدودة وتحتاج إلى استخدام مرن من قبل مشغلي الشبكات المتنقلة للتعامل مع المطالب المتزايدة، والحل كان بتقنية الاتصال جهاز إلى جهاز،

تفعيل اتصال جهاز إلى جهاز عبر الشبكات المتقدمة طويلة الأمد (Long Term Evaluation–Advanced) LTE–A يمكن أن يعود بالعديد من الفوائد من خلال الإنتاجية، استهلاك الطاقة، حمل حركة المرور وأيضا الخدمات التجارية الجديدة مثل الإعلانات المعتمدة على الموقع.

أصبح موضوع الاتصال جهاز إلى جهاز موضوع مهم سواء في الأوساط الأكاديمية والصناعية، والعديد من الأبحاث تركز على اكتشاف العقدة وإدارة الموارد الراديوية والجوانب الأخرى، في حين أن مسالة الأمن هي الأقل معالجة.

في هذا البحث، سوف نقدم لمحة عامة عن البنية الأمنية لاتصال جهاز إلى جهاز، التهديدات، المتطلبات، وبروتوكولات المصادقة.

الكلمات المفتاحية: المصادقة واتفاق المفتاح في شبكات LTE–A، الأمان، اتصال جهاز إلى جهاز.

*أستاذ– قسم النظم والشبكات الحاسوبية – كلية الهندسة المعلوماتية – جامعة تشرين – اللاذقية – سورية.

**طالبة دراسات عليا(دكتوراه)– قسم النظم والشبكات الحاسوبية – كلية الهندسة المعلوماتية – جامعة تشرين– اللاذقية– سورية.

مقدمة:

النمو الهائل في الطلب على بيانات من الشبكات اللاسلكية المتنقلة، أدى بشركات الاتصالات إلى إدخال معايير جديدة تمكن من توفير أعلى إنتاجية، انخفاض في استهلاك الطاقة وتحسين جودة الخدمة تحت هذه المتطلبات كان هناك اهتمام متزايد على تقنية الاتصال جهاز إلى جهاز (D2D).

هناك دوافع رئيسية لهذه التقنية:

أولا: إمكانية مشغلي الخلوي تخفيف الحمولة (حركة المرور) على الشبكة الرئيسية.

ثانيا: إطار لنموذج اتصال جديد يدعم خدمات جديدة مثل مشاركة المعلومات، الألعاب، الاعلانات المباشرة المتنقلة وخدمات البث.

الاتصال المباشر بين جهازين أو اتصال ad hoc موجود في التكنولوجية اللاسلكية بما في ذلك البلوتوث منذ سنوات، ولكنها بدون ترخيص والذي يسبب التداخل، مما يؤثر على الأداء. بينما استخدام تقنية جهاز إلى جهاز مرخص بها يجنب التداخلات.

بالإضافة لذلك فإن اتصالات LTE-A المعتمدة على تقنية D2D تعلن عن الموارد المتاحة محلياً والتي تُجنب المسح الأعمى وتقلل من استهلاك الطاقة للمستخدمين. وبالتالي فإن اتصالات D2D قادرة على توفير نوعية أفضل من الخدمات وتخفيض للطاقة من التكنولوجيا التقليدية التي تستخدم نطاقات غير مرخصة.

أهمية البحث وأهدافه:

يهدف البحث إلى رفع مستوى الأمن في اتصالات جهاز إلى جهاز في شبكات LTE-A من خلال بروتوكول المصادقة واتفاق المفتاح (Authentication and Agreement Key) والمحافظة على جودة الخدمة(QoS).

في الاتصالات التقليدية لا يسمح للجهاز الاتصال المباشر مع جهاز آخر، جميع الاتصالات تأخذ مكان من خلال المحطة القاعدية (BS(Base Station . من هنا تأتي أهمية البحث، فالتطور الهائل لأجهزة المحمول والتطبيقات ذات النطاق الترددي العالي مثل الفيديو وملفات الوسائط والتصوير ثلاثي الأبعاد، كل ذلك يتطلب معدل بيانات عالي وهذا يشكل تحدي كبير في الجيل الخامس. والحل الأفضل هو استخدام خدمات القرب proximity service(prose)، حيث يسمح لجهازين قريبين من بعضهما الاتصال وفق عرض النطاق الترددي المرخص في الشبكة الخلوية دون المحطة القاعدية BS أو بمشاركة محدودة.

لذا يمكن لاتصالات جهاز إلى جهاز أن تكون من الاستخدامات الحرجة في الكوارث الطبيعية (زلزال أو إعصار)، فإن شبكة الاتصال العاجلة يمكن إعدادها باستخدام خدمات القرب في فترة قصيرة لتحل محل شبكة الاتصال التالفة والبنية التحتية للإنترنت.

طرائق البحث ومواده:

سيتم بالبداية التعرف على هيكلية نظام الاتصال جهاز إلى جهاز وسيناريوهات هذا النموذج، إضافة إلى الأنواع الأربعة للاتصال، بعد ذلك سنبحث في البنية الأمنية للاتصالات الخلوية والعقد المضافة من أجل دعم الأمن في خدمات الاتصال المعتمدة على القرب.

دراسة بروتوكول المصادقة الأساسي وتطويره ليناسب نمط الاتصال الجديد من أجل أن يصادق كلاً من الجهازين الآخر.

وضع خطط لتشجيع المشتركين لاستخدام هذه التقنية على حساب مواردهم وطاقة أجهزتهم.

1- نظرة عن أجيال الشبكات الخلوية:[1]

- **الجيل الاول:**

استخدمت الهواتف الخلوية الاولى التقنية التماثلية لنقل أصوات المستخدمين وتستخدم تقنية النفاذ المتعدد بالتقسيم الترددي FDM .

- **الجيل الثاني:**

تم استخدام الاشارات الرقمية ،ومن أهم تقنيات الجيل الثاني:

1- GSM .

2- GPRS.

3- EDGE .

- **الجيل الثالث :**

أهم التقنيات تصل سرعة نقل البيانات إلى 2Mbps.

- **الجيل الرابع :**

تصل سرعة التدفق من 100 Mbps إلى 1 Gbps.

- **الجيل الخامس:**

التطوير المنتظر لشبكات الاتصالات خلال نهاية العقد الحالي في 2020.

في الاتصالات التقليدية لا يسمح للجهاز الاتصال المباشر مع جهاز أخر، جميع الاتصالات تأخذ مكان من خلال المحطة القاعدية BS.

2- نظام الاتصال جهاز إلى جهاز:

هناك مستويين للاتصال في الشبكة الخلوية:

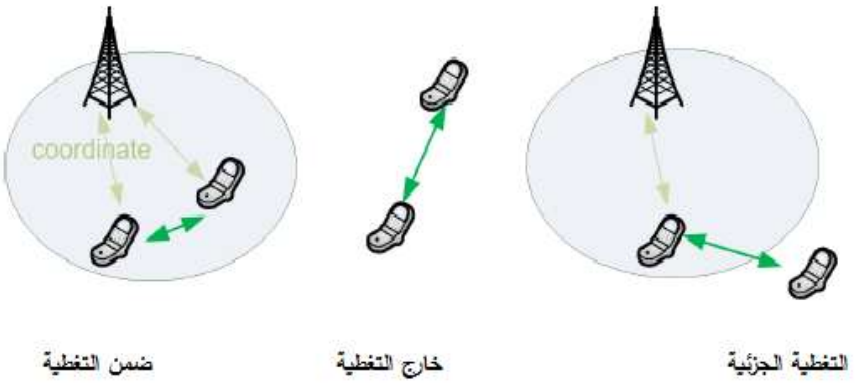
- مستوى الماكرو Macrocell tier (D 2 BS): في هذه التقنية بيانات المستخدم توجه من خلال المحطة القاعدة (BS) ومنها إلى الشبكة الرئيسية (core network).
- مستوى الجهاز Device tier (D 2 D): في هذه التقنية بيانات المستخدم توجه من خلال مستخدم أخر وبالتالي الحفاظ على الخصوصية أمر مهم للغاية.

2-1 سيناريو **النظام:[2]**

- سيناريو التغطية: تتحكم الشبكة في الموارد المستخدمة في اتصالات الخدمات القائمة على القرب (proximity service)prose ، ويجوز لها أن تخصص موارد محددة لأجهزة الارسال، وبهذه الطريقة فان التداخلات مع حركات المرور الخلوية يمكن تجنبها وبالتالي فإن الاتصال prose يكون الأمثل.

- سيناريو عدم التغطية: لا يمكن اجراء مثل هذا التحكم، بل يقوم تجهيز المستخدم UE باستخدام الموارد التي يتم تكوينها وحجزها مسبقا إما في جهاز الموبايل أو في شريحة الموبايل.
- سيناريو التغطية الجزئية: في هذا السيناريو يكون المشترك الخارج التغطية يستخدم الموارد المخصصة مسبقاً في حين المشترك ضمن التغطية يحصل على الموارد من المحطة eNB.

السيناريوهات موضحة ضمن الشكل (1)



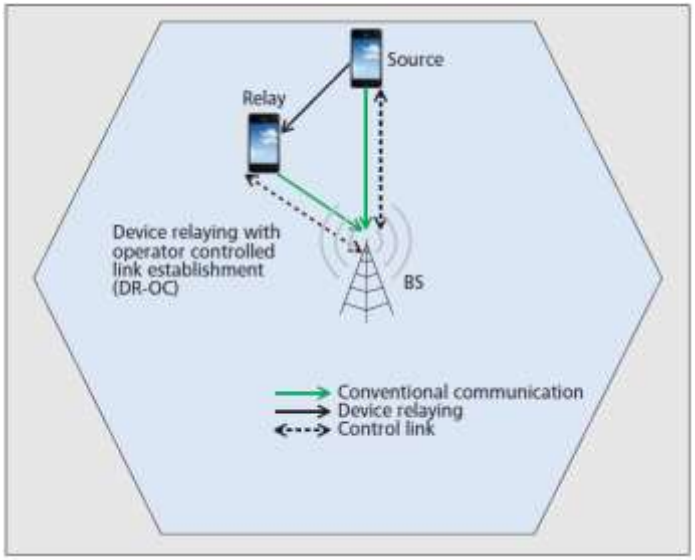
الشكل (1) سناريوهات نظام الاتصال D2D

من اجل تحقيق هذا النوع من الاتصال فان المشغل لديه أربع مستويات مختلفة من التحكم، إما تحكم كامل أو جزئي على الموارد المخصصة بين المصدر والهدف وأجهزة الترحيل أو ليس لديها أي سيطرة.

لذلك يمكننا تحديد أربع أنواع من اتصالات طبقة الجهاز:

❖ **Device relaying with operator controlled link establishment (DR-OC):[3]**

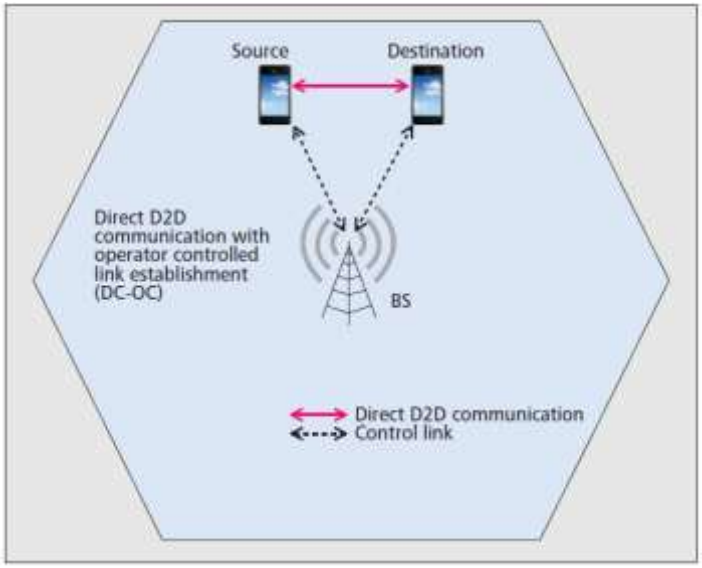
إن الجهاز في حافة الخلية أو في منطقة تغطية ضعيفة يستطيع الاتصال مع المحطة القاعدية من خلال ارسال المعلومات عبر جهاز أخر وهذا يسمح للجهاز بتحقيق جودة خدمة أفضل وحياة بطارية أكبر. المشغل يتصل مع جهاز الترحيل بتأسيس وصلة ذات تحكم كامل أو جزئي، الشكل(2)



الشكل(2) نمط الاتصال(DR-OC)

❖ **Direct D2D communication with operator controlled link establishment (DC-OC)**:

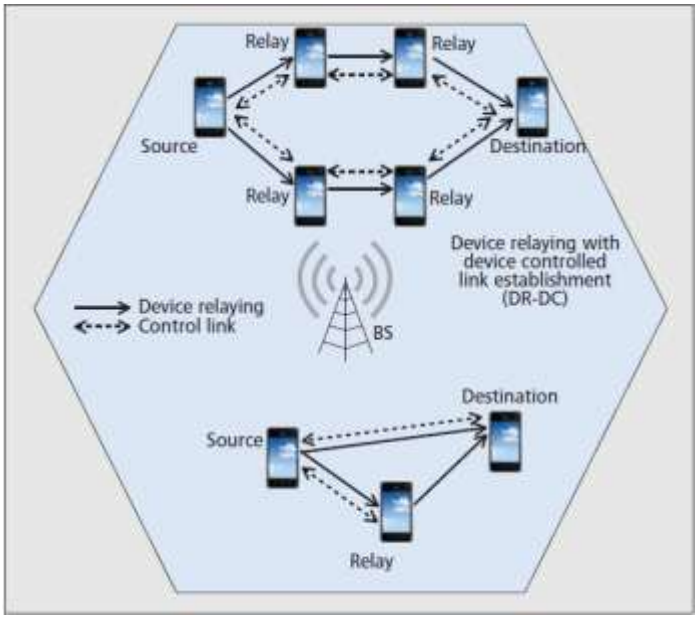
جهاز المرسل والمستقبل يتبادلون المعلومات دون الحاجة للمحطة القاعدية ولكن يحتاج إلى المشغل من اجل تأسيس الوصلة بينهما، الشكل(3).



الشكل(3) نمط الاتصال (DC-OC)

❖ **Device relaying with device controlled link establishment (DR-DC)**:[4]

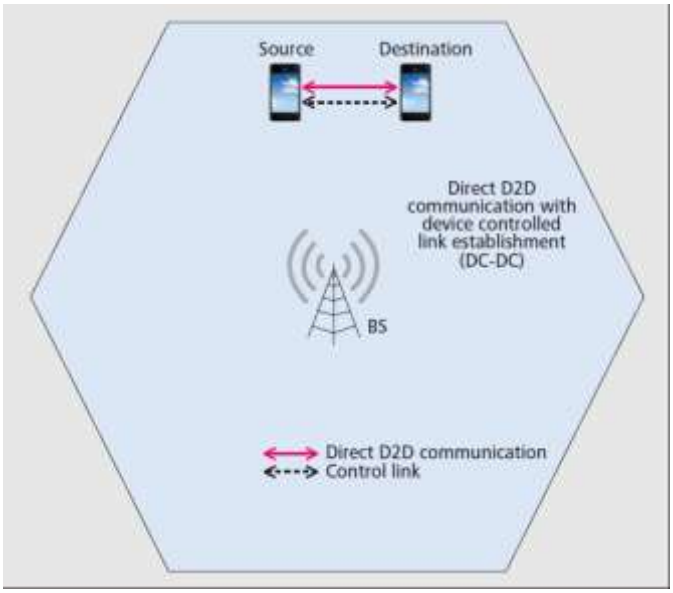
المشغل لا يشارك في عملية انشاء الارتباط ولذلك جهاز المرسل والمستقبل هما المسؤولان عن تنسيق الوصلة باستخدام أجهزة ترحيل بينهما، الشكل(4).



الشكل(4) نمط الاتصال(DR–DC)

❖ **Direct D2D communication with device controlled link establishment (DC-DC)**:

المصدر والهدف ليهما اتصال مباشر بدون تدخل المشغل وبالتالي يجب على المصدر والهدف استخدام الموارد بطريقة ما لضمان تداخل محدود مع الأجهزة الأخرى، الشكل(5).



الشكل(5) نمط الاتصال (DC–DC)

2–2 أهم استخدامات تقنية D2D:

افراغ الحمولة: يتم توجيه البيانات بين المستخدم الأول UE1 والمستخدم الثاني UE2 عبر المحطة eNB وبعدها إلى الشبكة الرئيسية (core network).

من خلال مراقبة الشبكة لحركات المرور بينهما تكتشف أنهما متصلين على نفس المحطة eNB فتطلب من الجهازين الذي يقع كل منهما ضمن تغطية الآخر بالاتصال المباشر وتحدد حامل مباشر لنقل البيانات بينهما، بالتالي تخفف من الضغط على مستوى الشبكة الرئيسية وتزيد من سرعة نقل البيانات بينهما.

انقاذ الكوارث: تسمح شبكات الاتصال لرجال الشرطة عند دخولهم إلى مناطق الكوارث حيث تكون المحطات eNB تم تدميرها بإقامة اتصال مباشر بينهم والاتصال مع أقرب شبكة متاحة.

الشبكات الاجتماعية: إذا كان المستخدم الأول UE1 والمستخدم الثاني UE2 أصدقاء، وكلاهما مسجل على أحد تطبيقات التواصل الاجتماعي وفي حال تفعيلهما لأمر "السماح بالاكتشاف" وكانا في منطقة prose فان الشبكة ترسل إخطاراً بذلك وتوفر اتصال مباشر بين هاتفيهما.

3- مقارنة بين تقنية D2D وwlan والبلوتوث:

سنقوم بالمقارنة بين التقنيات الثلاث وفق بعض الميزات كما في الجدول (1):

الجدول(1) مقارنة بين d2d وwlan والبلوتوث

المميزات	Bluetooth	Wlan	D2D
الاقتران	يتطلب اقتران يدوي	يتطلب اعدادات تعريف المستخدم لنقاط الوصول	محطة قاعدية مساعدة او جهاز مساعد
جودة الخدمة	لا يوجد ضمان لجودة الخدمة	لا يوجد ضمان لجودة الخدمة	يوفر ضمان لجودة الخدمة
الطيف	غير مرخص	غير مرخص	مرخص\غير مرخص
المعيار	Bluetooth	IEEE802.11	3GPP Release 12
الحد الأقصى لمعدلات البيانات	25 Mb/s	54Mb/s	5-10Gb/s
المسافة القصوى	10-100m	32m	500m
الطاقة القصوى	4dBm	15dBm	24dBm
السعر	مجاني	مجاني	المشغل يحدد السعر

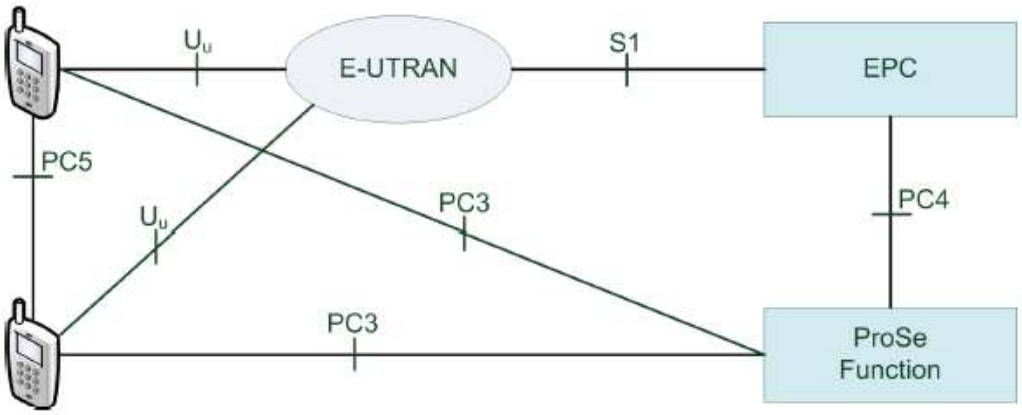
4- هيكلية النظام:[5]

تم ادخال عدة واجهات جديدة أهمها PC5، وهي الواجهة بين جهازي المشتركين، والواجهة PC3 وهي واجهة اتصال بين المشترك والوظيفة prose، مع العلم أنه يوجد وظيفة prose واحدة لكل مشغل شبكة وعنوان IP (Internet Protocol) الخاص بهذه الوظيفة يتم ضبطه مسبقا على الجهاز أو يتم البحث عنه بواسطة DNS، الشكل(6).

ويمكن توفير الخدمات القائمة على القرب (prose function) عندما تكون تجهيزات المستعمل قريبة من بعضها البعض.

هذه الخدمات تضم:

- الاكتشاف المباشر لخدمات القرب: تحدد هذه الخاصية أن اثنين من تجهيزات المستخدم قريبة من بعضها البعض، وبالنسبة لتجهيزات المستخدم ضمن التغطية يمكن استخدامها لأغراض تجارية.
- الاتصال المباشر لخدمات القرب: حيث يتم حجز الموارد من أجل هذا النوع من الاتصال.



الشكل(6) هيكلية نظام d2d

5- البنية الأمنية:

تتضمن البنية الأمنية:[6]

1-أمن الدخول للشبكة Network access security: تتم في هذا المجال بعض القضايا مثل: المصادقة وسرية هوية المستخدم وحماية البيانات المنقولة وغيرها من القضايا التي تتم مناقشتها في هذا المجال.

2-أمن نطاق الشبكة Network domain security: تمكن العقد المختلفة في مجال الشبكة من تبادل البيانات بشكل أمن وتحمي من المهاجمين على الشبكة اللاسلكية.

3-أمن نطاق المستخدم User domain security: تسمح بالوصول الأمن إلى المحطة المتنقلة.

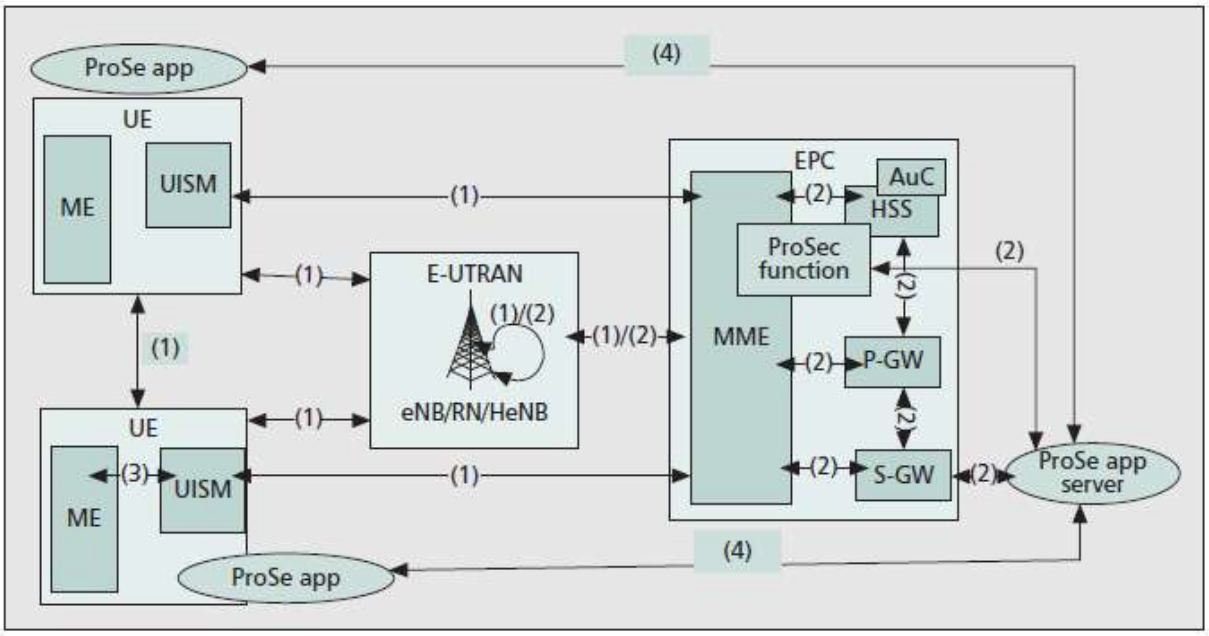
4-أمن نطاق التطبيقات Application domain security: تمكن التطبيقات في مجال المزود والمستخدم من تبادل الرسائل بشكل آمن وسري، كما هو موضح بالشكل(7).

سنسلط الضوء على التغييرات التي جلبتها خدمة القرب وهي:[7]

وظيفة الخدمة عن قرب prose function: وهي مجموعة من البرامج في الشبكة الرئيسية، يتعامل معها مخدم المشترك الرئيسي(HSS) وعنصر إدارة الموبايل (MME) ومخدم تطبيقات خدمة القرب، وهي مسؤولة عن ضبط تجهيز الموبايل واكتشاف العقد.

مخدم تطبيقات القرب وتطبيقات القرب prose apps server and apps: وهو مخدم لديه رابط منطقي مع تطبيقات المستخدم.

الوصلة الراديوية بين تجهيزي موبايلين radio link between two UEs: هذه الوصلة تقع في النطاق الترددي لشبكات LTE-A التي تديرها الشبكة (إذا مسموح) وتخصص اتصال مباشر بينهما.



الشكل(7) البنية الأمنية

5-1 التهديدات الأمنية:

يمكن للمهاجم اقتحام الشبكة الرئيسية وسرقة البيانات الخاصة بالمستخدم المسجلة في وظيفة prose او تعديلها، وقد يهاجم الرابط الراديوي بين المستخدمين، طالما أن طبيعة البث اللاسلكي تجعل من هذا الرابط عرضة للهجوم، وهذه التهديدات تشمل:

- التنصت: عقدة ضارة تتنصت على القناة الراديوية بين UE.
- هجوم انتحال الهوية: عقدة ضارة تتظاهر أنها جهاز شرعي أو عقدة eNB شرعية للوصول إلى حركة المرور.
- هجوم نشط على بيانات حركة المرور: تحاول العقدة الخبيثة تغيير بيانات حركة المرور.
- هجوم نشط على بيانات التحكم: عقدة خبيثة تحاول تغيير بيانات التحكم.

بما أن الوصلة الراديوية هي الأكثر ضعفا لذلك سنهتم بالجزء الأمني فيها.

5-2 تهيئة الاتصال:

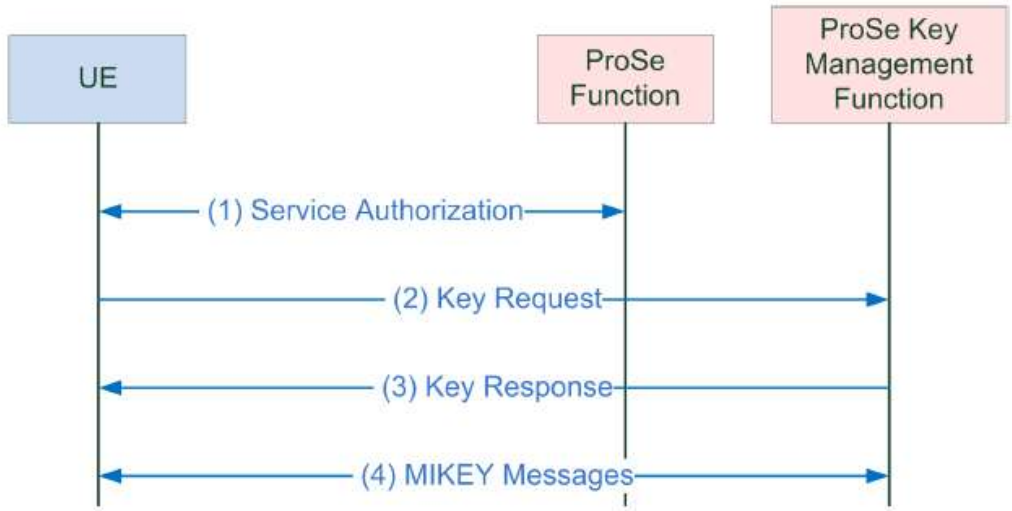
تزود بارامترات الأمن عن طريق عقدة في الشبكة تسمى إدارة مفاتيح خدمات القرب prose key management، يمكن أن تكون هذه العقدة جزء من وظيفة خدمات القرب prose function ويتم الاتصال مع هذه العقدة عن طريق الواجهة PC8 [8].

1-إذا لم يتم ضبط التهيئة مسبقاً في الشريحة فإن المشترك يجب أن يأخذ ترخيص من أجل الاتصالات عن قرب في وظيفة خدمات القرب prose function. يستقبل تجهيز المستخدم عنوان (IP) للمجموعات التي يريد الانضمام اليها وعنوان إدارة المفاتيح prose key management لاستخدامه في الخطوات اللاحقة.

2-من أجل حصول تجهيز المستخدم على المفاتيح للمجموعات المهتمة بها يرسل رسالة يطلب فيها عناوين المجموعات Group IP والقدرات الأمنية لتجهيز الموبايل.

3-تفحص إدارة المفاتيح prose key management من أجل كل مجموعة فيما إذا كان UE مرخص للاشتراك، وفيما إذا كانت قدراته الأمنية كافية من أجل الاتصال عن قرب، وبعد ذلك ترد على طلب UE والتي تتضمن عناوين أعضاء المجموعة Group Member ID وخوارزميات الأمان التي ستستخدمها، وتحوي أيضا مفتاح آخر مفتاح الوسائط المتعددة للإنترنت لخدمات الاتصال عن قرب Multimedia Internet Keying(PMIK) Prose، لاستخدامه في الخطوة الرابعة مع العنوان الخاص بالمفتاحPMIK ID ، إذا لم يتم ارسال PMIK ID يتم استخدام العنوان المرسل سابقاً.

4-في هذه الخطة تقوم إدارة المفاتيح للخدمات القريبة بإرسال مجموعة من PGK ID وPGK ومدة الصلاحية، كلا الطرفين يستخدم التشفير باستخدام المفتاح MIKEY، والشكل (8) يوضح الخطوات السابقة.



الشكل(8) تهيئة الاتصال في نظام d2d

5-3 بروتوكول نظام الحزم الاساسي standard AKA [9]

يتم تحقيق البروتوكول في مرحلتين:

1-توزيع أشعة المصادقة AV.

2-المصادقة واتفاق المفتاح.

5-3-1 توزيع اشعة المصادقة AV:

1-تطلب شبكة التخديم (SN) من المستخدم عنوان المعّرف Identity (ID) الخاص به.

2-يرسل المستخدم UE عنوان IMSI كرد على SN.

3-يرسل SN طلب للحصول على بيانات المصادقة الخاصة بالمشترك إلى الشبكة الرئيسية HN ويكون هذا الطلب محمل بعنوان المعرف الخاص بالمشترك وشبكة التخديم.

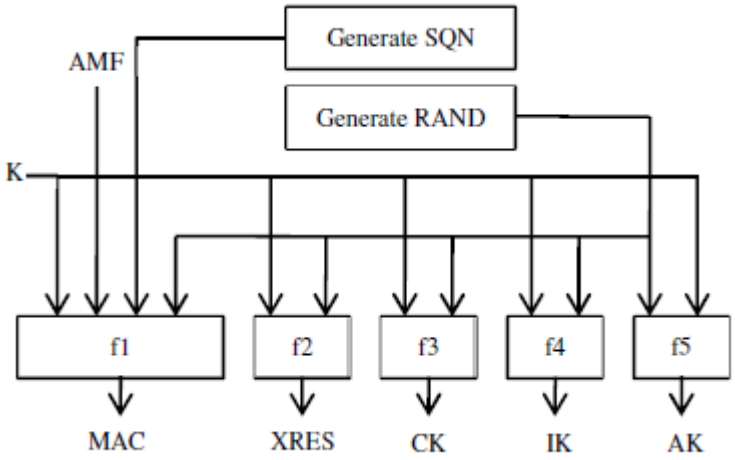
4-تقوم HN بتوليد اشعة مصادقة AVوترسلها إلى SN.

أشعة المصادقة المرسلة تخزن في SN لتستخدم في مصادقات لاحقة تخفيفاً من الحمل على الشبكة وازدحام الطلبات على HN.

بارامترات شعاع المصادقة:

- RAND قيمة عشوائية تولد في HN
- XRES (XResponse) قيمة الاجابة التي تتوقع SN استلامها من المشترك UE
- CK (Cypher Key) مفتاح التشفير
- IK (Integrity Key) مفتاح السلامة
- AUTN(Authentication Token) علّام المصادقة ومن خلاله يُصادق المشترك الشبكة ويتكون هذا البارامتر من ثلاث اجزاء:
  - SQN(Sequence Number) : رقم تسلسلي
  - AMF(Authentication Management Field) حقل ادارة المصادقة .يُستخدم لإدارة أغراض أمنية معينة.
  - MAC (Message Authentication Code) شيفرة رسالة التوثيق يتم التحقق منها في UE

يتم حساب البارامترات السابقة وفق الوظائف الأمنية (security functions) f1,f2,f3,f4,f5 كما في الشكل(9).[10]



الشكل(9) حساب بارامترات المصادقة بالوظائف الأمنية

5-3-2 المصادقة واتفاق المفتاح Authentication Key Agreement:

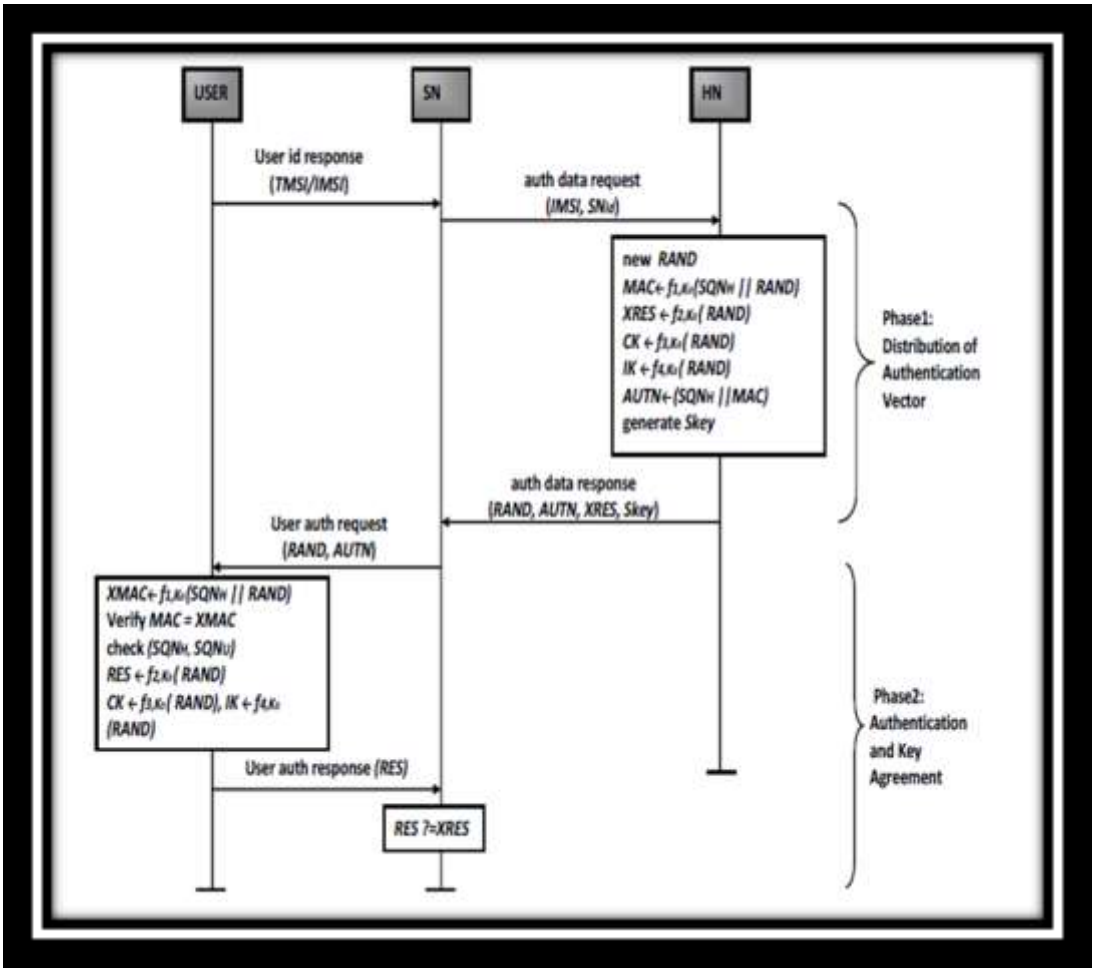
تتم وفق النقاط التالية:

1-بعد ان تستلم SN اشعة المصادقة ترسل البارامترين (RAND,AUTN) إلى المستخدم.

2-يقوم UE بحساب RES، XMAC ويتحقق من مطابقته لقيمة MAC المستقبلة من SN عبر AUTN، بذلك يكون UE قد تحقق من HN و SN ومصادقة الشبكة، وهو حل للشبكات ونقاط الوصول الوهمية. وبعد ذلك يتم

التحقق من SQNH و SQNU (الرقم التسلسلي الوارد من HN والرقم التسلسلي الموجود في UE) وذلك للتحقق من حداثة شعاع المصادقة. بعد التحقق من البارامترين السابقين يقوم UE بتوليد البارامتر RES ويرسله إلى SN.

3-يقارن SN البارامتر القادم من المستخدم ومن الشبكة الرئيسية ويتم مصادقة المستخدم إذا تساوت القيمتان، كما هو مبين في الشكل(10).



الشكل(10) بروتوكول المصادقة واتفاق لمفتاح AKA

5-4 بروتوكول المصادقة في D2D:

كما هو موضح بالشكل(11) تتم عملية المصادقة وفق التالي:

1) يرسل مخدم التطبيقات للتجهيزين UE1 و UE2المفتاح المشترك باستخدام تشفير يتم الاتفاق عليه مسبقاً.

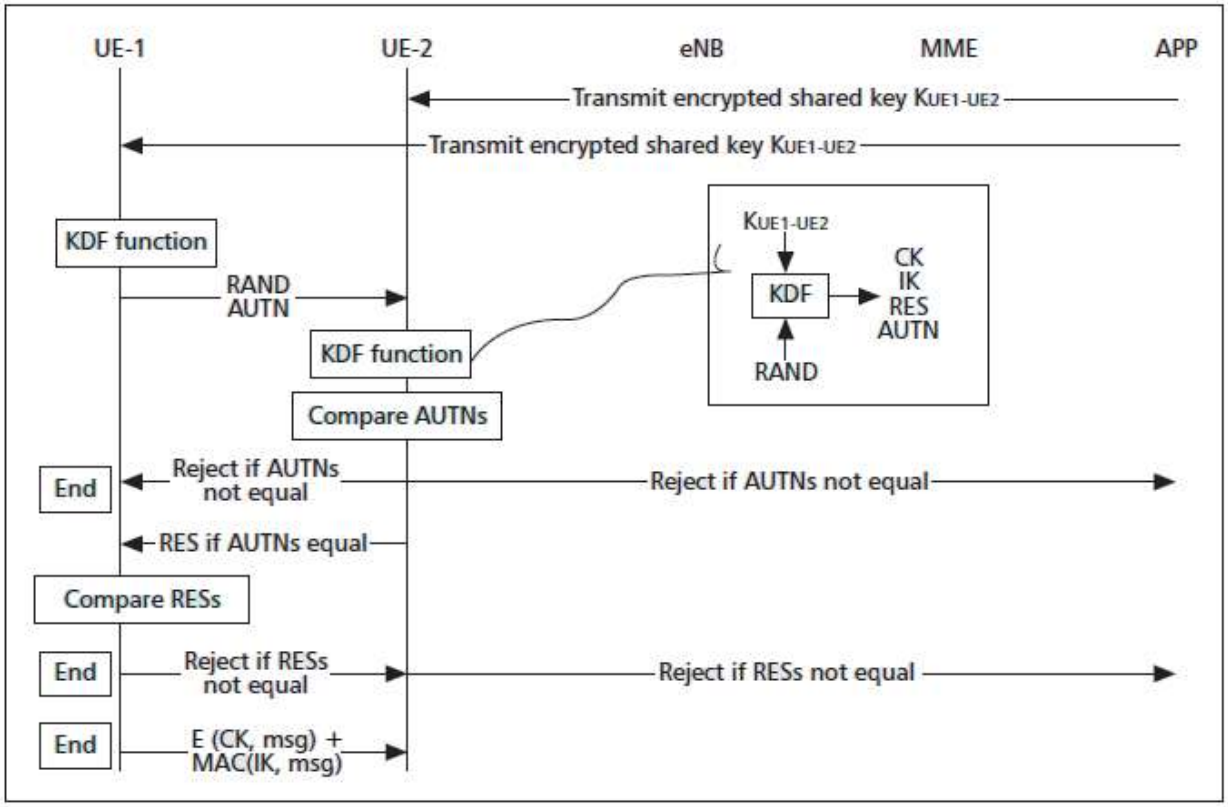
2) يفعّل التجهيز الأول UE1 الوظيفةKDF مستخدماً المفتاح المشترك ويولد القيمة العشوائية RAND ومفتاح التشفير CK ومفتاح السلامة IK والبارامترين AUTN وRES.

3) يرسل UE1 البارامترين AUTN وRAND إلى التجهيز الثاني UE2 عبر القناة التي تخصصها العقدة Enb.

4) يفعّل UE2 الوظيفة KDF مستخدما المفتاح المشترك والقيمة المستلمة RAND.

5) يقارن UE2القيمة المستلمة AUTN مع القيمة المولدة محليا في حال التطابق، يرسل القيمة RES إلى UE1، وإلا يلغي الطلب.

6) يقارنUE1 القيمة المستلمة RES مع القيمة المولدة محليا في حال عدم التطابق يلغي الاتصال وإلا يرسل رسالة تأكيد مشفرة باستخدام CK ويضمن البارامتر MAC باستخدام IK وبذلك تتم المصادقة، كما هو موضح بالشكل(11).



الشكل(11) بروتوكول المصادقة في D2D

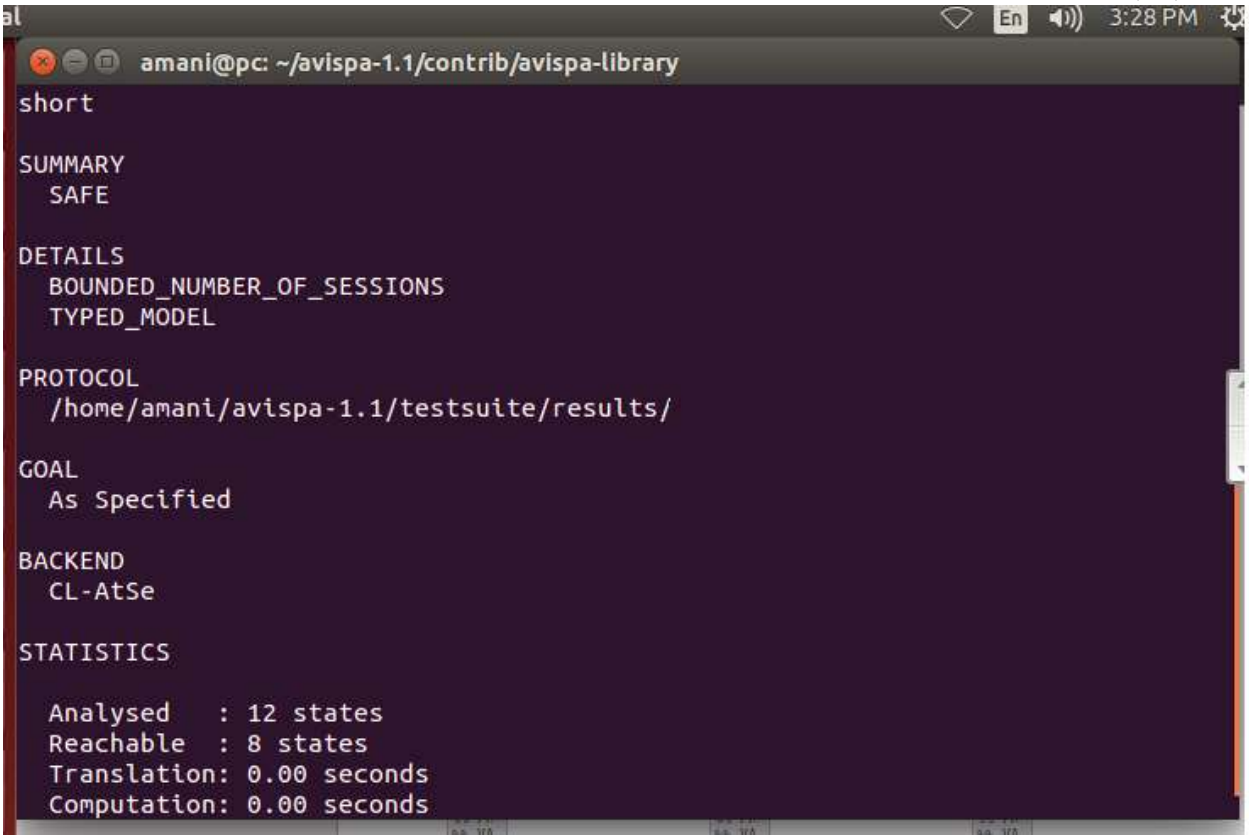
تمت نمذجة البروتوكول للتحقق من المستوى الأمني له باستخدام البرنامج AVISPA (Automated Validation of Internet Security Protocols and Application).

لمحة عن الأداة AVISPA:

يقوم هذا البرنامج بالتحليل الدقيق للبروتوكولات الأمنية عن طريق إيجاد العيوب وتصحيحها والبحث عن الثغرات والهجمات الأمنية لتغطيتها، من أهم مميزات الأداة AVISPA:

- تُستخدم لتحليل بروتوكولات أمن الإنترنت والتطبيقات.
- تعتمد على لغة البرمجة HLPSL (High-Level Protocol Specification Language) لغة توصيف البروتوكولات الرفيعة المستوى.
- يمكن تحميلها على سطح المكتب أو الوصول إليها مباشرة من المتصفح.
- متوافقة فقط مع بيئات ماكنتوش ولينكس.

بعد الفحص تبين أن بروتوكول المصادقة في D2D آمن من جميع التهديدات الأمنية المذكورة سابقا . والشكل(12) يبين ذلك.[11]



الشكل(12) اختبار بروتوكول المصادقة في D2D باستخدام AVISPA

التحدي الأساسي في هذا النموذج هو تشجع أجهزة الترحيل، طالما أنه يتم استخدام موارد المشترك (البطارية وعرض الحزمة) من أجل ترحيل المعلومات من جهاز إلى آخر.

لذلك لابد من وجود مغريات مادية أو حوافز أخرى لكي يتم تضمين هذا النوع من الاتصالات.

إحدى الاحتمالات الممكنة، ذلك أن المشغل يمكن أن يقدم عرض لبعض الحسومات على الفواتير الشهرية وذلك يعتمد على معدل البيانات التي يتم ترحيلها عبر أجهزتهم.

مثل هذه الحسومات مقبولة بالنسبة للمشغل لأن المشغل يستفيد من تقديم الخدمة لجهاز أخر مع تغطية أقل.

حافز أخر بدلاً من الحسومات على الفواتير الشهرية، يمكن للمشغل أن يقدم خدمات مجانية مقابل كمية البيانات المرحَلة.

الفائدة تعرف كالتالي:[12]

$$U_i = b_i \log_2 (1 + k_i\gamma_i) - Mb_ip_i + \tilde{b}_i \log_2 (1 + k_i\tilde{\gamma}_i),$$

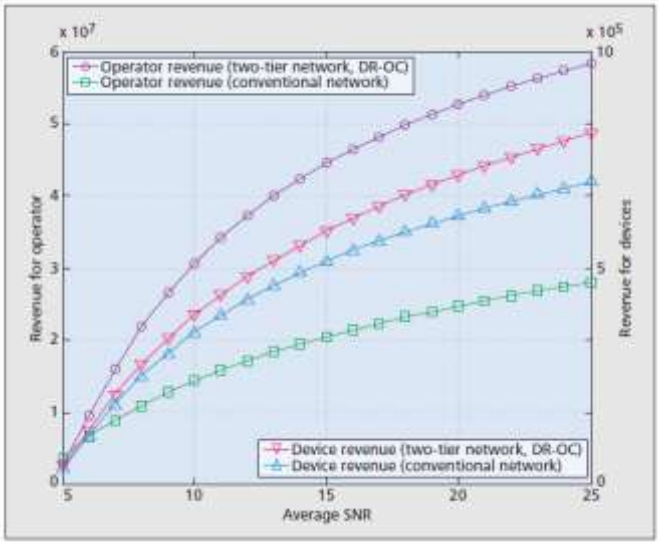
- حيث b_i: عرض حزمة القناة المستخدمة من الجهاز.
- الربح من هذا الاستخدام هو:

$$b_i \log_2 (1 + k_i\gamma_i)$$

- حيث $k_i = 1.5/\ln(0.2/\bar{BER}_{tar})$ يدل على كفاءة الطيف
- Y_i هو معدل نسبة الإشارة إلى الضجيجSNR للوصلة بين الجهاز و المحطة القاعدية
- BER هو معدل الخطأ
- M عدد القفزات بين المحطة القاعدة والجهاز عند ارسال البيانات
- مع العلم أن الجهاز يدفع $b_i p_i$ للمشغل على الاستخدام، حيث p_i هو وحدة سعر عرض الحزمة.
- الجزء الأخير من العلاقة يدل على مدى الربح للجهاز i من عرض الحزمة الممنوحة وهي من الحوافز التي تعطى من الشركة للجهاز للقيام بعملية ترحيل.
- $\ddot{Y}_i$ يدل على معدل SNR بين الجهاز والمحطة القاعدية خلال عملية ارسال البيانات الممنوحة .وبالتالي من اجل Nجهاز الربح للشبكة الخلوية يمكن ان تحسب كالتالي:

$$R = \sum_{i=1}^{N} Mb_i p_i - M\tilde{b}_i p_i .$$

الشكل (13) يبين إيرادات المشغل والمشترك بدون تقنيةD2D ومع وجود التقنية:



الشكل(13) إيرادات المشغل والمشترك مع وبدون تقنية D2D

نلاحظ أن إيرادات المشغل والمشترك تزداد بشكل ملحوظ باستخدام هذه التقنية من الاتصال.

تحليل النتائج:

وفقا" لتحليل أداء بروتوكول المصادقة في اتصال جهاز الى جهاز باستخدام الأداة AVISPA تبين أنه آمن وحقق المصادقة ثنائية الاتجاه وبالتالي تغلب على التهديدات الأمنية التي تم ذكرها سابقاً، إضافة انه لا يحتاج إلى عمليات حسابية معقدة مما يسرع في الأداء ولا يسبب حمل على الشبكة ويحقق مستوى أمني عالي بذلك يكون قد حقق جميع عناصر جودة الخدمة.

الاستنتاجات والتوصيات:

بالتركيز على أهمية الاتصال جهاز الى جهاز في الشبكات الخلوية، فهي تخفف من الضغط على مخدمات الشبكة الرئيسية، وتخفف من حركات المرور على الشبكة وبالتالي سرعة في الأداء، واستثمار أمثل للموارد المتاحة، تكلفة أقل مع تلبية المتطلبات المتزايدة على عرض الحزمة نتيجة التطور الهائل في أجهزة الموبايل.

إضافة لكونه الحل الأمثل في حال انهيار الشبكة عند الكوارث الطبيعية أو نتيجة خلل ما في الشبكة،

ويحقق إيرادات عالية على المشغل وعلى المشترك بهذه الخدمة ومع التنويه الى الضبط الأمني للاتصال من هذا النوع.

وفقاً لذلك كله ستكون كل التوجهات المستقبلية لإدراج هذه الخدمة ضمن مشغلات الخلوي لما لها من فوائد كبيرة.

المراجع:

[1]Raoush,R; Thompson; Willson ,C. *Comparison of Network Generation Techniques for Unconsolidated Porous Media*.ACSESS U.S.A, 2015 ,Vol. 67 No. 6, p. 1687-1700.

[2] FODOR,G. *Design Aspects of Network Assisted Device-to-Device Communications*. IEEE Commun. Mag., vol. 50, no. 3, Mar. 2016, pp. 170–77.

[3] LEIT,L.*Operator Controlled Device-to-Device Communications in LTE-Advanced Networks*. IEEE Wireless Commun,vol. 19, no. 3, June 2012, pp. 96–104.

[4] FENG,D.*Device-to-Device Communications Underlaying Cellular Networks*. IEEE Trans. Commun., vol. 61, no. 8, 2013, pp. 3541–51.

[5] 3GPP TS 23.303 V12.5.0, June 2015. *Technical Specification Group Services and System Aspects*. Proximity-based services

[6] 3GPP, TR 33.401, v. 12.9.0 .*Security Architecture*. Release 12, Sept. 2013.

[7] 3GPP, TR 23.703, v. 0.4.0 .*Study on Architecture Enhancements to Support Proximity Services (ProSe)*. Release 12, June 2013.

[8] 3GPP TS 33.303 V12.4.0, June 2015. Technical Specification Group Services and System Aspects; Proximity-based Services (ProSe); Security aspects

[9] FORSBERG,D;HORN,G;MOELLER,W. LTE Security, Second Edition.UK, Copyright © 2013 John Wiley & Sons, Ltd.

[10] BHUSAL,A.Is the Session Mix-up Attack on the UMTS/LTE AKA Protocol Practical. Norwegian University of Science and Technology,2013,96

[11] AVISPA Project, http://www.avispa-project.org/.

[12] Hossain,E; Niyato,D; Han,Z. Dynamic Spectrum Access and Management in Cognitive Radio Networks, Cambridge Univ. Press, 2009.

Email: amany.stiety@hotmail.com