مسح على الجوانب الأمنية ل شبكات LTE و LTE-A

جين كاو ، مود ما ، *عضو أول ، IEEE* هوي لي ، *عضو IEEE* ، ويويو تشانغ

***خلاصة*- مطالب عالية للاتصالات اللاسلكية المتنقلة ذات النطاق العريض-** يعزز الإصدار 10 من 3GPP LTE أنظمة LTE الحالية **الاتصالات وظهور الوسائط المتعددة اللاسلكية الجديدة** لدعم استخدام بيانات أعلى بكثير ، ووقت استجابة أقل وأفضل **تشكل التطبيقات الدافع لتطوير** الكفاءة الطيفية [2]. بالإضافة إلى ذلك ، فإن كلا من LTE و LTE- **تقنيات الوصول اللاسلكي واسع النطاق في السنوات الأخيرة. ال التطور طويل المدى / تطور بنية النظام (LTE / SAE)** ونظم دعم فلوريدا في الاتصال IP، البيني الكامل مع **تم تحديد النظام من قبل شراكة الجيل الثالث** شبكات الوصول اللاسلكية غير المتجانسة والعديد من الأنواع الجديدة **مشروع (3GPP) في طريقه نحو الجيل الرابع (4G)** من المحطات القاعدية مثل المحطات القاعدية بيكو / فيمتو والتتابع **الاتصالات الخلوية. من خلال تصميم وتحسين تقنيات الوصول إلى الراديو الجديدة والمزيد من التطور في المحمول لضمان احتفاظ 3GPP بهيمنة تقنيات**

أنظمة LTE ، تعمل 3GPP على تطوير مستقبل LTE-Advanced التحديات في تصميم البنيات الأمنية لـ **الإنترنت LTE-A و LTE GPPنظرًا لأن بنية 3 .3GPPلـ 3G الشبكات اللاسلكية كمعيار 4)LTE-A(في تصميم آليات الأمان. هذه الورقة تقدم عددا من المساهمات ل)IP(مصممة لدعم اتصال بروتوكول مع شبكات الوصول اللاسلكية غير المتجانسة ، فإن الميزات الفريدة الجديدة تجلب بعض التحديات الجديدة والعمل البيني الكامل**

الجوانب الأمنية لشبكات LTE و LTE-A. اولا نحنالهجمات [5] ، الجيل القادم من أنظمة الاتصالات المتنقلة **الحالية لهذه المشكلات بشكل كلاسيكي. أخيرًا ، نعرض قضايا البحث المحتملة لأعمال البحث المستقبلية. استكشاف الثغرات الأمنية الموجودة في بنية وتصميم شبكات LTE و LTE-A. ثالثًا ، تتم مراجعة الحلول تقديم نظرة عامة على وظائف الأمان لشبكات LTE و LTE-A. ثانيًا ، يتم

***الكلمات الدالة*—أمن LTE-A ، LTE ، أمان HeNB ، IMS الأمن ، أمن MTC.**

أنامقدمة

دبليو ألعاب تفاعلية وتلفاز محمول وفيديو وتدفق صوتي ، مع الشبكات اللاسلكية الأخرى الموجودة أنظمة الاتصالات [1]. نظام LTE-A المحدد بواسطة العالية ، وزمن وصول الوصول المنخفض ، وتشغيل النطاق الترددي المرنة والتكامل السلس عناصر شبكة أقل ، مما يحسن سعة النظام وتغطيته ، ويوفر أداءً عاليًا من حيث معدلات البيانات المتنقلة عريضة النطاق. تم تصميم نظام LTE ليكون نظامًا قائمًا على حزم يحتوي على 3GPP باعتبارها تقنيات الاتصالات المتنقلة الناشئة للجيل التالي من الشبكات اللاسلكية المحمول وتطبيقات الوسائط المتعددة الجديدة ، تم تحديد تقنيات LTE و LTE-A بواسطة وعمليات الوسائط المتعددة المتنقلة. من أجل استيعاب الاستخدام المتزايد لبيانات الهاتف المتنقلة إلى تلبية المتطلبات المختلفة لبيانات الهاتف المحمول وحسابات الهاتف المحمول تحتاج تكنولوجيا الاتصالات

تم استلام المخطوطة في 24 أغسطس 2012 ؛ تمت المراجعة في 27 يناير 2013.

يعمل J. Cao مع مختبر مفتاح الدولة لشبكة الخدمات المتكاملة ، جامعة شيديان ، شيان ، الصين (البريد الإلكتروني: caoj897@gmail.com).
هو في كلية الهندسة الكهربائية والإلكترونية ، نانيانغ M. Ma الجامعة التكنولوجية ، سنغافورة (بريد إلكتروني: Maode Ma@pmail.ntu.edu.sg).
مع مختبر مفتاح الدولة للخدمة المتكاملة Y. Zhang و H.Li الشبكة ، جامعة Xidian ، شيان ، الصين.

معرف الكائن الرقمي 10.1109 / SURV.2013.041513.00174

في شبكة خلوية كبيرة. نظرًا لإدخال الخصائص الجديدة ، فإنه يخضع للكثير من الأمان الجديد العقد

أنظمة LTE و LTE-A.

نظرًا لوجود الكثير من الثغرات الأمنية في الجامعة-)MitM(Man-in-the-Middle وهجمات المحطة القاعدية المارقة [4] ورفض الخدمة (DoS) آلية أمان نظام الاتصالات المتنقلة المتعدّد (UMTS) مثل هجمات]3[

وكيان إدارة التنقل (MME) من خلال شبكة الوصول إلى الراديو الأرضي العالمي المتطور- وظائف أمان أكثر من أنظمة UMTS. لتحقيق مصادقة متبادلة بين معدات المستخدم (UE) تحتاج إلى توفير

العمل (E-UTRAN) ، تعمل بنية SAE / LTE على تحسين اتفاقية المصادقة والمفتاح)UMTS-AKA(UMTS و بالإضافة إلى ذلك ، تم إدخال تسلسل هرمي جديد للمفاتيح وآلية إدارة مفتاح التسليم من أجل ، نظام الحزم المتطور)EPS AKA(AKA لتجنب الهجمات الموجودة في أنظمة UMTS. يقدم نهج أمان الوصول الجديد

ضمان أمن الوصول وعملية التنقل في

بعض الثغرات الأمنية في شبكات LTE-A / LTE الحالية ، والتي تحتاج إلى مزيد من التحليل. وحدد نقاط الضعف الأمنية المقابلة والمتطلبات والحلول [10] - [13]. ومع ذلك ، لا تزال هناك Machine Type Communication و]8[ )HeNB(Home eNodeB وعقد الترحيل [9] قوة أنظمة LTE ، أدخل نظام LTE-A بعض الكيانات والتطبيقات الجديدة مثل]7[ )MTC(

للوصول إلى الميكروويف (WiMAX) وأنظمة LTE. وأشارت إلى أن أنظمة الجيل الرابع في وظائف الأمان الحالية في شبكة WiFi ، وقابلية التشغيل البيني في جميع أنحاء العالم الضعف الأمنية في أنظمة 4G. بالإضافة إلى ذلك ، قدم الاستطلاع نقاط الضعف المحتملة أداة تحليل منهجية تستند إلى نموذج أمان Bell Labs المسمى X.805 القياسي لتحليل نقاط الأمن لنظام IP متعدد الوسائط الفرعي (IMS) وشبكات الجيل التالي (NGN) وتم اقتراح عن التهديدات الأمنية على شبكات 4G في [14]. في الاستطلاع ، تم التحقيق في معماريات عدد قليل من الاستطلاعات من أجل مراجعة الأعمال الحالية [14] - [18]. تم تقديم لمحة عامة اقتراح العديد من نتائج البحث حول وظائف الأمان لشبكات LTE / LTE-A. تم بالفعل نشر في الآونة الأخيرة ، تم

لم يتم التحقيق في الميزات الجديدة المقدمة في شبكات LTE / LTE-A مثل MTC و HeNB. دون تقديم جهود البحث الحالية والحلول قيد التقدم في موضوعات البحث. علاوة على ذلك ، السابقة بشكل أساسي على بنية الأمان ونقاط الضعف الأمنية ومتطلبات الأمان في أنظمة LTE في [18] لأنظمة الاتصالات المتنقلة من الجيل الرابع مع شبكات IPv6. ركزت الاستطلاعات 4G اللاسلكية. بالإضافة إلى ذلك ، تم اقتراح بعض الاستراتيجيات البناءة للدفاع عن الأمن من الجيل الرابع مع شبكات IPv6 والتحديات والقضايا الأمنية الموجودة في شبكات IPv6 4G اللاسلكية في طبقة التطبيق. في المسح، تم وصف خصائص أنظمة الاتصالات المتنقلة المحمولة وتتبع الموقع على طبقة MAC. ناقش الاستطلاع في [18] الجوانب الأمنية لأنظمة لهجمات DoS وهجمات سلامة البيانات والاستخدام غير القانوني لمعدات المستخدم والأجهزة الخدمة بسبب إدارة المفتاح الخاطئ. بالإضافة إلى ذلك ، فإن شبكات LTE معرضة أيضًا في طبقة MAC تحت هجمات DoS وهجمات التنصت وهجمات إعادة التشغيل وتدهور بأنظمة LTE و WiMAX. لقد أظهر أن نظام WiMAX يحتوي على بعض نقاط الضعف و LTE مع التركيز على مشكلات أمان طبقة MAC المحددة ونقاط الضعف المحتملة المرتبطة شبكات 4G اللاسلكية في [17]. في الاستطلاع ، تم تحديد معماريات الأمان لشبكات WiMAX المستخدم (UP) التشفير ، وما إلى ذلك. تم تقديم دراسة حول التطورات والتحديات الأمنية في على وظيفة اشتقاق المفتاح (KDF) ، والتعامل مع المفاتيح ، وتفعيل المستخدم لطبقة EPS الحالية التي يتعين معالجتها بسبب الطبيعة غير المتجانسة تمامًا لـ EPS ، مثل التفاوض 3GPP. لقد أشارت إلى أنه لا يزال هناك الكثير من المشكلات الموجودة في بنية أمان ذلك ، تم وصف معمارية أمن EPS وإجراءات الأمن التفصيلية المصممة بواسطة مواصفات البنية الشاملة لنظام الحزم المتطور (EPS) وتهديدات أمان EPS ومتطلبات الأمان. وبعد تم توفير ملخص موجز لوظائف وإجراءات أمان LTE في [16]. في الاستطلاع ، تمت مناقشة ليست شديدة على الأنظمة بينما معظمها يمكن أن يتسبب فقط في أضرار طفيفة للشبكات. من حيث الاتساع والعمق. لقد أظهر أن العديد من الهجمات الموجودة في أنظمة WiMAX لكل فئة من الهجمات. بالإضافة إلى ذلك ، تم تقييم الخاصية النوعية لكل نوع من الهجمات على عدد قليل من العوامل. وبعد ذلك ، تم تلخيص الإجراءات المضادة والعلاجات المقترحة أنظمة WiMAX المحددة بواسطة معايير IEEE 802.16 الموجودة في الأدبيات الحالية بناءً أنظمة WiMAX. في الاستطلاع ، تم فحص وتصنيف مجموعة متنوعة من الهجمات الضارة ضد الإنترنت. قدم الاستطلاع في [15] تصنيفًا شاملاً للهجمات الخبيثة والإجراءات المضادة في الخاصة ببروتوكول الإنترنت بسبب بنيتها المفتوحة غير المتجانسة والقائمة على بروتوكول سوف ترث جميع مشاكل الأمان لشبكات الوصول الأساسية ومعظم الثغرات الأمنية

LTE والجوانب الأمنية لـ الميزات الجديدة المقدمة في شبكات)3(، LTE-A مناقشة حول الأمنية في شبكات)2(، LTE / LTE-A تحليل المشكلات الأمنية ونقاط الضعف في شبكات / LTE. تشمل جهودنا ومساهماتنا في هذا العمل (1) نظرة عامة على البنى والوظائف في هذه الورقة ، نقدم مسحًا شاملاً لجوانب الأمان في شبكات LTE-A الضعف هذه ، و (4) استكشاف المجالات المحتملة واتجاهات البحث للعمل البحثي المستقبلي. الحلول الحالية للتغلب على نقاط

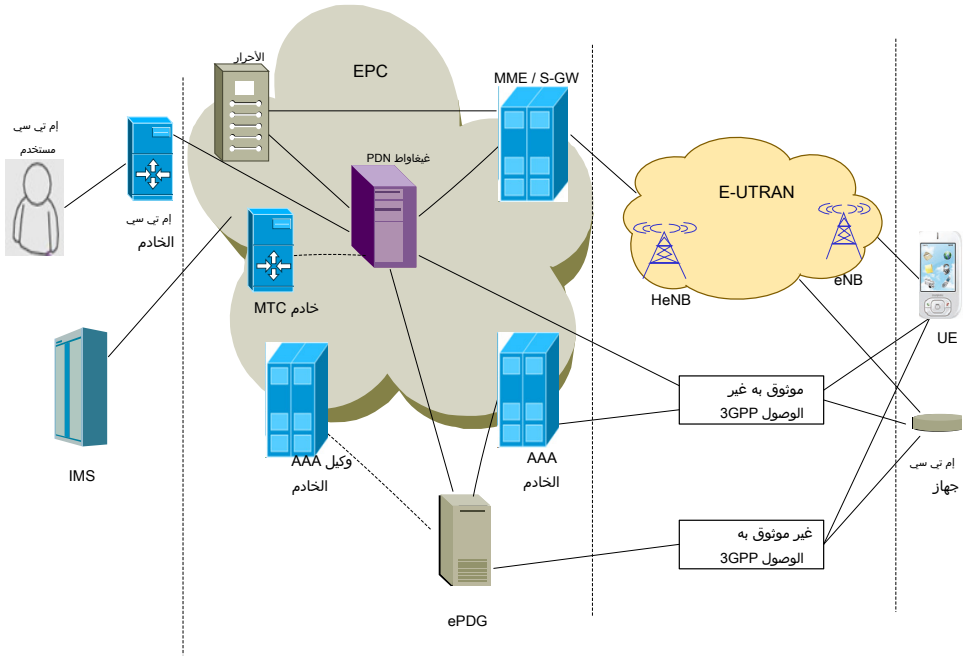
يتم تحديد قضايا البحث المفتوح وعرض خاتمة الورقة في القسم السادس والقسم السابع. الأمان لشبكات LTE / LTE-A. تتم مناقشة الحلول الحالية في القسم الخامس. وأخيرًا ، الأمان لشبكات LTE / LTE-A. في القسم الرابع ، تم استكشاف نقاط الضعف في وظائف على معمارية الأمن لشبكات LTE / LTE-A. في القسم الثالث ، تم تلخيص ميزات ووظائف تم تنظيم التذكير بهذه الورقة على النحو التالي. في القسم الثاني ، يتم تقديم نظرة عامة

ثانيًا. س ECURITY أهيكل ا نظرة عامة

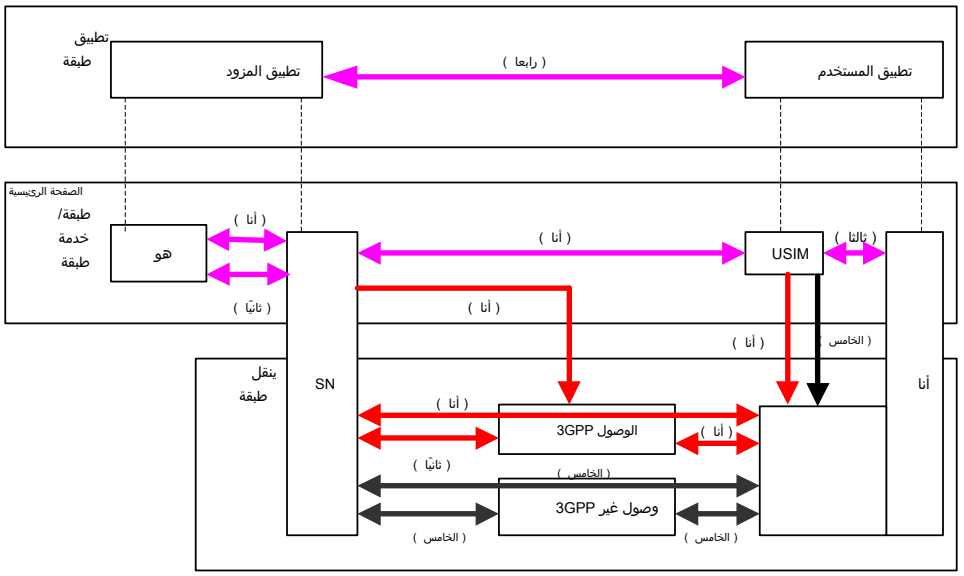
أ. هندسة شبكة LTE

الأرضي العالمي المتطور ، والتي تسمى)eNB(eNodeBs ، والتي تتواصل مع UEs. متبادلة مع تجهيزات المستعمل. يتضمن E-UTRAN المحطات الأساسية لشبكة النفاذ الراديوي (HSS). عندما يتصل تجهيزات المستعمل بـ EPC ، فإن MME تمثل EPC لإجراء مصادقة وبوابة الخدمة (SGW) ، وبوابة شبكة حزم البيانات (PDN GW) مع خادم المشترك المنزلي ، من خلال شبكة النظام الفرعي للوسائط المتعددة]19[ )IMS(IP. يتكون EPC من MME في أنظمة LTE. ستتم معالجة الخدمة الصوتية ، وهي خدمة شبكة ذات دارات كهربائية (CS) إن EPC عبارة عن شبكة أساسية تعمل بكامل بروتوكول الإنترنت وتحويل حزم البيانات (PS) مبين في الشكل 1 ، تتكون شبكة LTE من مركز الحزمة المتطور (EPC) وشبكة E-UTRAN. كما هو

لتشغيل عدد كبير من أجهزة MTC. خادم MTC متصل بشبكة LTE للتواصل مع MTCDs. خارج مجال مشغل الشبكة ، استخدام الخدمات التي يوفرها واحد أو أكثر من خوادم MTC في MTC ، مستخدم MTC وخادم MTC. يمكن لمستخدم MTC ، وهو شخص أو مركز تحكم دون أي شرط على أي شكل من أشكال التدخل البشري. هناك كيانان جديدان موجودان من اتصالات البيانات بين الكيانات ، يُسمى]7[MTC ، والتي يمكنها تبادل البيانات ومشاركتها الحزمة المتطورة الموثوقة (ePDG) المتصلة بـ)3(.EPC يدعم نظام LTE-A أيضًا نوعًا جديدًا وصول غير موثوق بها لا تعتمد على 3GPP ، تحتاج واجهة المستخدم إلى تمرير بوابة بيانات ليست سمة من سمات شبكات الوصول ، والتي تعتمد على قرار مشغلي الشبكة. بالنسبة لشبكة غير موثوقة لا تعتمد على]21[3GPP. ما إذا كانت شبكة الوصول غير 3GPP موثوقة أم لا لا تعتمد على 3GPP ، وهما شبكات نفاذ غير موثوق بها لا تعتمد على 3GPP وشبكات وصول بتقسيم الكود (CDMA) 2000 ، المتصلة بـ]20[EPC. هناك نوعان من شبكات الوصول التي مثل شبكات المنطقة المحلية اللاسلكية (WLAN) وأنظمة WiMAX وأنظمة الوصول المتعدد النطاق [8]. (2) بالإضافة إلى E-UTRAN ، يدعم نظام LTE-A شبكات الوصول غير 3GPP الصوت والبيانات عالية السرعة. يتم توصيله بـ EPC عبر الإنترنت عبر وصلة توصيل واسعة ويتم تثبيتها عادةً من قبل مشترك في المسكن أو مكتب صغير لزيادة التغطية الداخلية لخدمة HeNB ، لتحسين التغطية الداخلية وقدرة الشبكة. HeNB هي نقطة وصول منخفضة القدرة والكيانات الجديدة. (1) اقترحت لجنة 3GPP نوعًا جديدًا من المحطات القاعدية ، يُدعى بالمقارنة مع شبكات الجيل الثالث اللاسلكية ، تقدم شبكات LTE / LTE-A بعض الوظائف



الشكل 1. بنية شبكة LTE



الشكل 2. نظرة عامة على هندسة الأمن

لجهاز MTC الاتصال بخادم MTC والتحكم فيه بواسطة مستخدم MTC عبر خوادم MTC. نطاق. عندما يتصل جهاز MTC بشبكة LTE ، يمكن

B. هندسة أمان LTE

هناك خمسة مستويات أمان حددتها لجنة 3GPP]6[، والتي تم تحديدها على النحو التالي. كما هو مبين في الشكل 2 ،

بين USIM و)ME(Mobile Equipment و E-UTRAN والكيانات الموجودة في EPC. ارتباط الوصول (اللاسلكي). يحتوي هذا المستوى على آليات أمان مثل حماية التكامل والتشفير ميزات الأمان التي توفر وصولاً آمنًا لوحدات UE إلى EPC وتحميها من الهجمات المختلفة على أمان الوصول إلى الشبكة (I): مجموعة

أمان مجال الشبكة (II): مجموعة ميزات الأمان الخطوط السلكية ويمكّن العقد من تبادل بيانات التشوير وبيانات المستخدم بطريقة آمنة. يحمي من الهجمات في شبكات

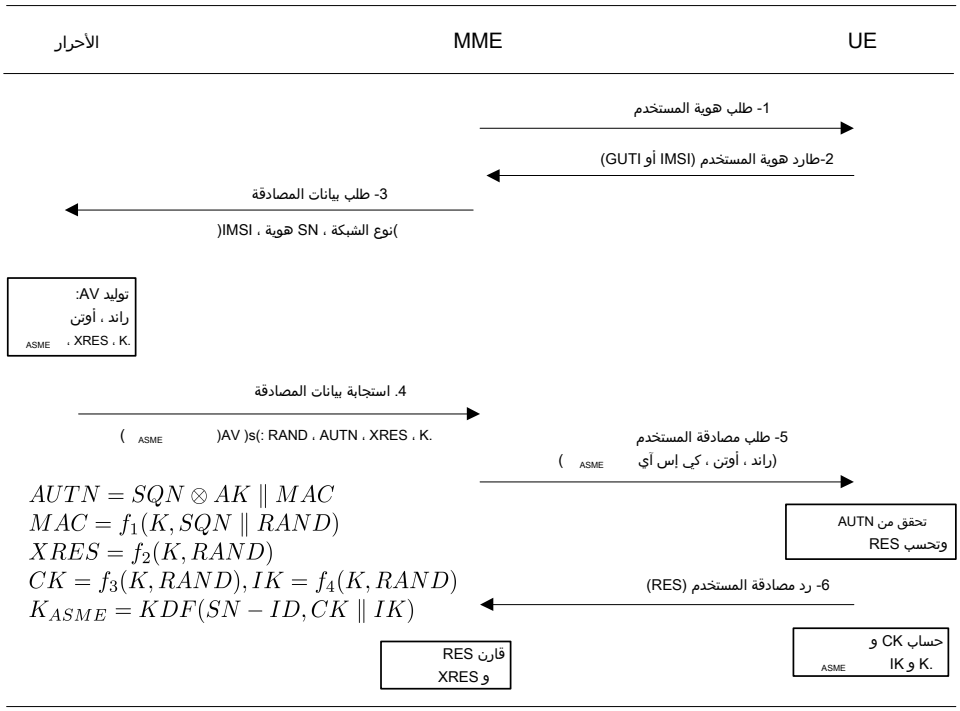
أمان مجال المستخدم (III): مجموعة ميزات الأمان التي توفر مصادقة متبادلة بين USIM و

.ME إلى USIM قبل وصول ME

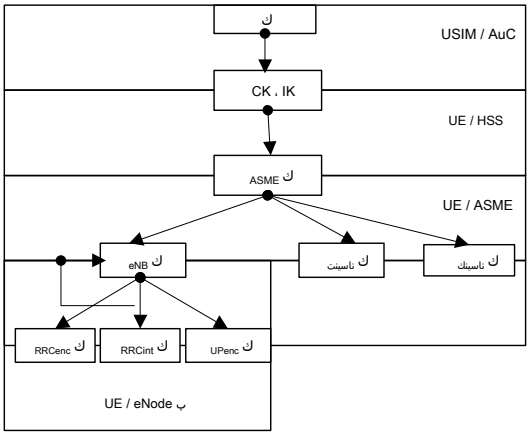
التطبيقات في تجهيزات المستعمل وفي مجال مزود الخدمة من تبادل الرسائل بأمان. أمن مجال التطبيق (IV): مجموعة ميزات الأمن التي تمكّن

EPC عبر شبكات الوصول غير 3GPP وتوفر الحماية الأمنية على ارتباط الوصول (الراديو). أمان المجال غير)V(3GPP: مجموعة الميزات التي تمكّن UEs من الوصول بأمان إلى

تم قبول هذه المقالة لتضمينها في عدد مقبل من هذه المجلة. المحتوى نهائي كما هو مقدم ، باستثناء ترقيم الصفحات.



الشكل 3. EPS AKA



الشكل 4. التسلسل الهرمي الرئيسي لـ LTE 3GPP

ثالثا. LTE إس ECURITY Fأكل و م ECHANISMS

أمان LTE-A / LTE في السنوات الأخيرة ، نركز على الجوانب الخمسة التالية لأمان LTE. الأمان للميزات الجديدة المقدمة في شبكات LTE-A. استنادًا إلى تقدم البحث حول ميزات LTE التي يمكنها تلبية متطلبات الأمان على مستوى أمان الوصول إلى الشبكة ، وتحديد جوانب في هذا القسم ، نفصل بشكل أساسي ميزات وإجراءات أمان

1) الأمن الخلوي LTE.
2) أمان تسليم LTE.
3) أمن IMS.
4) أمن HeNB.
5) أمن MTC.

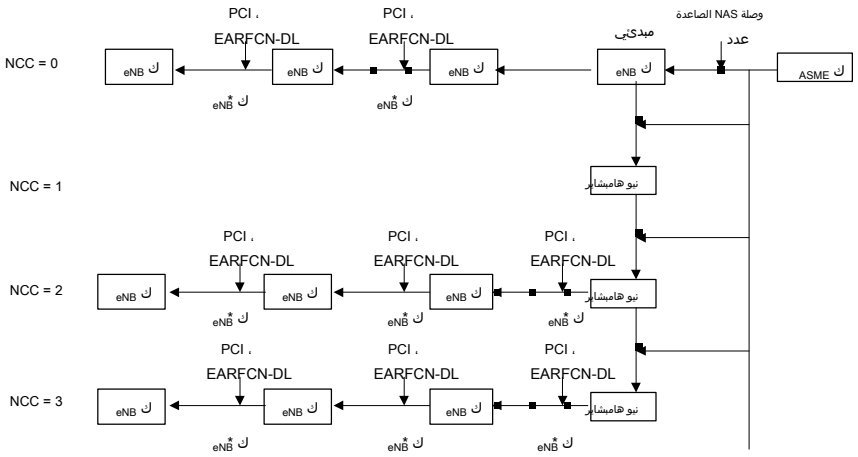
أ. الأمان في نظام LTE الخلوي

AKA المختلفة في بنية أمان LTE عند وصول UEs إلى EPC عبر شبكات وصول مميزة. للتشفير وحماية السلامة. نظرًا لدعم الوصول غير 3GPP ، يتم تنفيذ العديد من إجراءات وإنشاء مفتاح تشفير (CK) ومفتاح تكامل (IK) ، والتي تستخدم لاشتقاق مفاتيح جلسة مختلفة إطار أمان LTE. يستخدم نظام LTE إجراء AKA لتحقيق المصادقة المتبادلة بين UE و EPC تعد المصادقة المتبادلة بين UE و EPC أهم ميزة أمان في

مصادقة متبادلة مع UE بواسطة بروتوكول]6[EPS AKA كما هو مبين في الشكل. عندما يتصل تجهيزات المستعمل بـ EPC عبر E-UTRAN ، فإن MME تمثل EPC لإجراء

الهرمي الجديد للمفاتيح لحماية الإشارات وتوجيه بيانات المستخدم كما هو موضح في الشكل. 3. بالإضافة إلى ذلك ، تم إدخال التسلسل
وصول غير موثوق بها غير 3GP ، فإن UE و ePDG بحاجة إلى تنفيذ إنشاء نفق IPsec. المحسن (EAP-AKA ') لإنجاز مصادقة الوصول. نظرًا لأن UE يتصل بـ EPC عبر شبكة وخادم AAA سوف ينفذان بروتوكول المصادقة المتوسع-)EAP-AKA(AKA أو EAP-AKA شبكة النفاذ غير 3GPP غير موثوقة. بالنسبة لشبكة وصول موثوق بها غير 3GPP ، فإن UE هناك معلومات مُؤَمّنة مسبقًا في تجهيزات المستعمل ، يجب أن تعتبر تجهيزات المستعمل أن تأمين شبكات النفاذ غير الموثوقة غير]22[3GPP مسبقًا في تجهيزات المستعمل. إذا لم تكن AAA. سوف تمر إشارة المصادقة عبر خادم Proxy AAA في سيناريوهات التجوال. يمكن نفاذ غير 3GPP ، سيتم تنفيذ مصادقة الوصول غير 3GPP بين تجهيزات المستعمل وخادم 4. عندما يتصل جهاز UE بـ EPC عبر شبكات

تم قبول هذه المقالة لتضمينها في عدد مقبل من هذه المجلة. المحتوى نهائي كما هو مقدم ، باستثناء ترقيم الصفحات.



الشكل 5. تسليم مفتاح الإدارة

ب. الأمن في عمليات التسليم

الوصول غير]25[-]22[،]6 [3GPP ، والتي تم وصفها بالتفصيل على النحو التالي.
الأرضي)UTRAN(UMTS / شبكة الوصول اللاسلكي)GERAN(GSM EDGE / شبكات
الأمان المتعلقة بالتنقل داخل E-UTRAN وكذلك بين E-UTRAN وشبكة الوصول اللاسلكي
حددت لجنة 3GPP ميزات وإجراءات

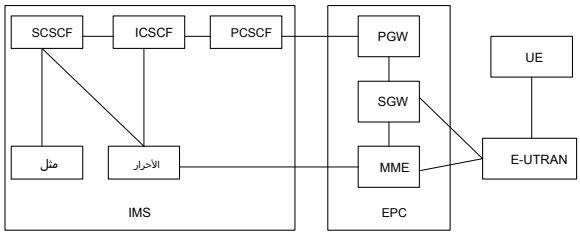
الأفقية [6] كما هو موضح في الشكل 5. إلى تحقيق اتصال آمن بين UE و MME ، eNB
على طرق مختلفة لاشتقاق مفاتيح eNB الجديدة بناءً على اشتقاقات المفاتيح الرأسية أو
تسليم آمن داخل E-UTRAN ، تستخدم شبكات LTE آلية جديدة لإدارة المفاتيح ، والتي تحتوي
(1) التنقل داخل]23[،]22[E-UTRAN. من أجل تحقيق

ويشتق UE أ*ك eNB* ومعلمة الخطوة التالية
من)NH(*ك* ، *ASME* تجهيزات المستعمل و MME بعد إجراء مصادقة أولية. A NH Chaining
وهي مشتقة من
العداد (NCC) مرتبط بكل منها *ك eNB* في عمليات التسليم ، ستكون مفاتيح الجلسة الجديدة
والمعلمة NH.
المستخدمة بين UE و eNB الهدف ، يسمى *ك* ، *eNB* سوف
أن تكون مشتقة من أي من النشطة حاليا *ك eNB* أو من معلمة NH.

بالنسبة للتسليم من E-UTRAN إلى UTRAN أو GERAN ، يجب أن تحدد UE و MME-
(2) التنقل بين E-UTRAN و]24[،]23[UTRAN / GERAN.

مزق CK "و IK" من *ك* [*ASME* 6]. عند الاستلام
CK ، *IK* || *ك* مع KSI من MME ، الخدمة المستهدفة
لاشتقاق خدمة حزم الراديو العامة (GPRS)]22[Kc. للتسليم من UTRAN / GERAN إلى
يجب أن تستخدم عقدة دعم)SGSN(GPRS و UE CK 'و IK'

المستهدف MME يجب اشتقاق ، E-UTRAN*ك* من CK *ASME*
تجهيزات المستعمل أيضاً أن تنفذ نفس الإجراء المذكور أعلاه الذي يمكن اشتقاقه من MME
و IK أو GPRS Kc المستلمة من SGSN. يتعين على
ك ، *ASME* ثم يتم اشتقاق MME المستهدف وتجهيز المستعمل
ك eNB NAS المقابلة وفقًا للتسلسل الهرمي الرئيسي لـ LTE كما هو موضح في الشكل 4.
ومفاتيح
لمواصفات]22[3GPP ، عندما تتنقل UE من شبكة وصول لاسلكي إلى أخرى ، فإن UE ،
عمليات نقل آمنة وسلسة بين شبكات الوصول E-UTRAN وشبكات الوصول غير 3GPP. وفقًا
الوصول غير]25[3GPP. اقترحت لجنة]25[3GPP العديد من مناهج التنقل لـ EPC لتحقيق
(3) التنقل بين شبكات النفاذ E-UTRAN وشبكات



الشكل 6. LTE و IMS بنية النظام المتكامل

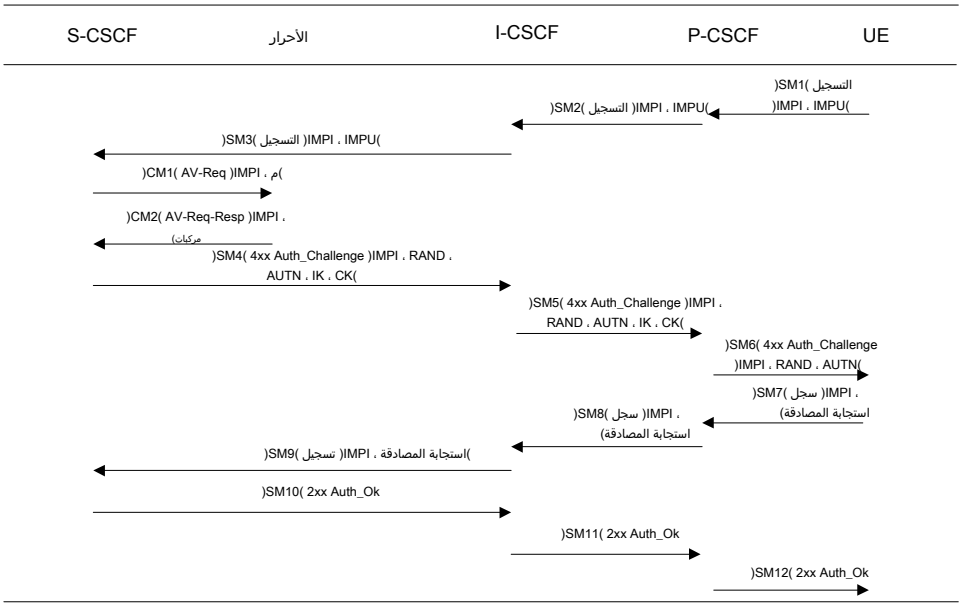
أو EAP-AKA 'عند التسليم إلى شبكات وصول غير موثوق بها لا تعتمد على 3GPP.
EAP-AKA 'عند التسليم إلى شبكات وصول موثوق بها غير 3GPP و IKEv2 مع EAP-AKA
في سيناريوهات تنقل مميزة ، مثل EPSAKA عند التسليم إلى E-UTRAN أو EAP-AKA أو
وسيقوم EPC بتنفيذ مصادقة وصول كاملة. سيتم تنفيذ إجراءات مصادقة الوصول المختلفة
شبكة الوصول المستهدفة

جيم الأمن في IMS

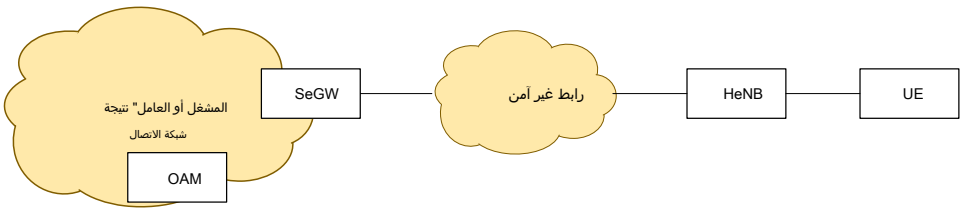
بخدمات الوسائط المتعددة مثل الصوت عبر)VoIP(IP ومؤتمرات الفيديو وما إلى ذلك.
، بواسطة IMS .]26[،]19[3GPP عبارة عن بنية متراكبة لتزويد شبكات LTE / LTE-A
عبارة عن معمارية تحكم في الخدمة قائمة على بروتوكول الإنترنت لا تعتمد على الوصول
شبكات LTE / LTE-A نحو جميع شبكات IP وشبكات PS بالكامل. تم تطوير IMS ، وهو
تتطور

و)S-CSCF(ServingCSCF. عندما يريد مستخدم المراسلة الفورية التواصل مع IMS ،
تقسيمها إلى ثلاثة كيانات ،)P-CSCF(ProxiesCSCF و)I-CSCF(Interrogating-CSCF
الاتصال (CSCF). يمكن معالجة جميع إشارات جلسة SIP بواسطة CSCFs ، والتي يمكن
المعمارية الرئيسية في IMS هي وكلاء SIP ، والمعروفة باسم وظائف التحكم في خدمة
نظرًا لاستخدام بروتوكول بدء الجلسة (SIP) للتحكم في الجلسات وإشاراتها ، فإن العناصر
بشبكات LTE ، يجب تخزين مفاتيح ووظائف مصادقة IMS على جانب المستخدم في ISIM.
المتكاملة العالمية (UICC). على غرار بطاقة)USIM(UMTS SIM ، التي تُستخدم للاتصال
المتعددة ، تحتاج UE إلى وحدة تعريف مشترك)ISIM(IMS موجودة داخل بطاقة الدوائر
الشكل 6 معمارية LTE والنظام المتكامل]27[IMS. من أجل الوصول إلى خدمات الوسائط
يصف

تم قبول هذه المقالة لتضمينها في عدد مقبل من هذه المجلة. المحتوى نهائي كما هو مقدم ، باستثناء ترقيم الصفحات.



الشكل 7. IMS AKA



الشكل 8. هندسة نظام HeNB

مستخدم المراسلة الفورية ويوفر التحكم بجلسة خدمات الوسائط المتعددة الخاصة به.

المنزلية (HN) للمصادقة والاتفاقية الرئيسية لنظام IMS كما هو موضح في الشكل. الوصول إلى خدمات الوسائط المتعددة. بعد ذلك ، يتم تنفيذ IMS AKA بين ISIM والشبكة وحدة IM UE أولاً إلى تحقيق المصادقة المتبادلة مع شبكة LTE بواسطة EPS-AKA قبل ، يجب مصادقة تجهيزات IM UE في كل من طبقة شبكة LTE وطبقة خدمة IMS. تحتاج المتعددة. وفقًا لمواصفات]27[3GPP ، من أجل الوصول إلى خدمات الوسائط المتعددة ، يلزم وجود ارتباط أمني منفصل بين IM UE و IMS قبل منح الوصول إلى خدمات الوسائط الوسائط المتعددة إلا بعد أن تنجح الوحدة في إنشاء ارتباط الأمن بالشبكة. بالإضافة إلى ذلك لن يتم توفير خدمات

نجاح مصادقة الشبكة ومصادقة IMS ، سيتم منح مشترك IM الوصول إلى خدمات الدردشة. 7. بمجرد

D. الأمن في HeNB

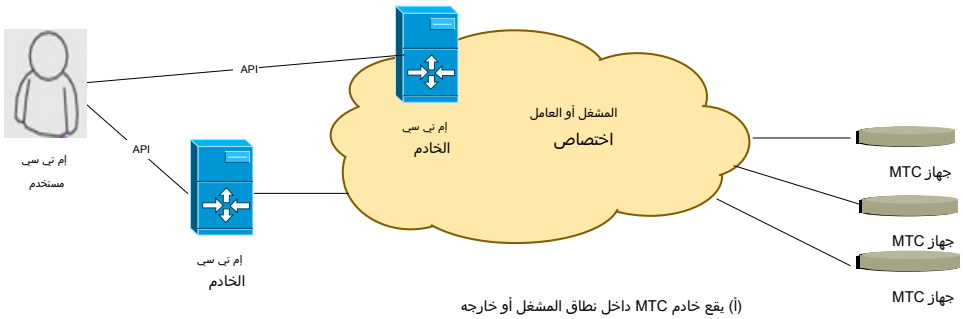
الداخلية لخدمة الصوت والبيانات عالية السرعة. يعتبر femtocell المعروف باسم A HeNB الطاقة. عادةً ما يتم تثبيته بواسطة مشترك في مساكن أو مكاتب صغيرة لزيادة التغطية والجودة العالية للخدمات. هناك ثلاثة أنواع من الوصول لـ HeNB هو نقطة وصول منخفضة [8] ، [12] ، HeNB جهازًا جذابًا للمشغلين لتقديم خدمات ممتدة مع مزايا التكلفة المنخفضة .أي الوصول المغلق والوصول الهجين والوصول المفتوح

8 ، يتصل HeNB بـ EPC عبر الإنترنت عبر وصلات التوصيل عريضة النطاق. الوصلة بين كما هو مبين في الشكل
، سيتم تنفيذ مصادقة الوصول الآمن بين تجهيزات المستعمل و MME بواسطة EPS AKA. المستهدف بناءً على قائمة مجموعة المشتركين المغلقة (CSG) المسموح بها. وبعد ذلك الشبكة عبر HeNB ، ستتحقق MME أولاً مما إذا كان UE مسموحًا له بالوصول إلى HeNB مؤمنًا ومصرحًا به من قبل التشغيل والإدارة والصيانة (OAM). عندما تريد UE الوصول إلى بواسطة IKEv2 مع EAPAKA أو مخطط قائم على الشهادات. A HeNB يحتاج إلى أن يكون وبوابة الأمان (SeGW) غير آمنين. يمثل SeGW EPC لإجراء مصادقة متبادلة مع HeNB قد يكون HeNB

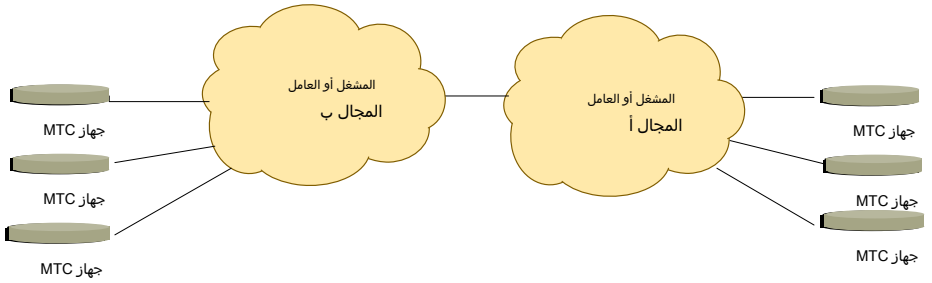
E. الأمن في MTC

المستقبلية. تختلف عن الاتصالات التقليدية من إنسان إلى إنسان (H2H) التي صممها الاتصال من آلة إلى آلة (M2M) ، على أنه إحدى التقنيات المتطورة التالية للاتصالات اللاسلكية يُنظر إلى MTC ، المعروف أيضًا باسم

يمكنها الاتصال بخادم MTC واحد أو أكثر عبر شبكة LTE. يمكن أن توجد خوادم MTC في أو 9 ، اقترحت لجنة 3GPP ثلاثة سيناريوهات لـ]7[MTC. يوضح الشكل 9 (أ) أن أجهزة MTC بشكل أساسي في جمع معلومات القياس وتسليمها تلقائيًا. كما هو مبين في الشكل من أشكال اتصال البيانات بين الكيانات التي لا تحتاج بالضرورة إلى تفاعل بشري. يتم استخدامه في الشبكات اللاسلكية الحالية ، تم تعريف MTC كشكل

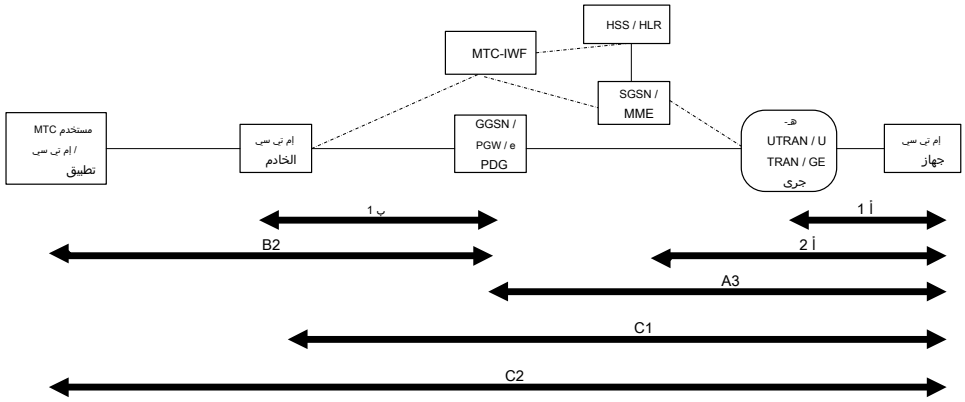


(أ) يقع خادم MTC داخل نطاق المشغل أو خارجه



(ب) أجهزة MTC تتواصل مباشرة مع بعضها البعض بدون خادم MTC وسيط

الشكل 9. سيناريوهات الاتصالات MTC



الشكل 10. هندسة الأمن MTC

المستوى محتملة لـ]10[MTC ، والتي تشمل ثلاث مناطق أمنية مختلفة موصوفة في الشكل. أجهزة MTC المقترحة في معيار 3GPP الحالي. وصفت اللجنة 3GPP معمارية أمنية عالية بالنسبة لسيناريوهات الاتصال في الشكل 9 (ب) ، لا يوجد نهج محدد لضمان الاتصال الآمن بين مع أجهزة MTC بواسطة EPS AKA لتمكين الاتصال الآمن بين أجهزة MTC وخادم MTC. (ب). بالنسبة لسيناريو الاتصال في الشكل 9 (أ) ، تمثل MME الشبكة لتنفيذ المصادقات المتبادلة التواصل مباشرة مع بعضها البعض دون مشاركة خوادم MTC كما هو موضح في الشكل 9 خارج مجال المشغل. بالإضافة إلى ذلك ، يمكن لأجهزة MTC

3GPP ، وأمان (B2) لـ MTC بين مستخدم MTC وتطبيق MTC وشبكة 3GPP. يمكن تقسيمها أيضًا إلى أمان الجوانب عندما يكون خادم MTC داخل وخارج شبكة

ب) إلى منطقتين فرعيتين ، (B1) أمان MTC بين خادم MTC وشبكة 3GPP ، والتي شبكة 3GPP وخادم MTC / مستخدم MTC ، تطبيق MTC ، والذي يمكن تقسيمه و MTCIWF للوصول إلى 3GPP / ePDG للوصول غير 3GPP. الأمان لـ MTC بين لـ MTC بين جهاز MTC

10.

MTC وشبكة الوصول اللاسلكي ،)A2(، EUTRAN / UTRAN / GERAN أمان MTC 3GPP ، والتي يمكن تقسيمها إلى ثلاث مناطق فرعية. (A1) أمان MTC بين جهاز أ) أمان MTC بين جهاز MTC وشبكة

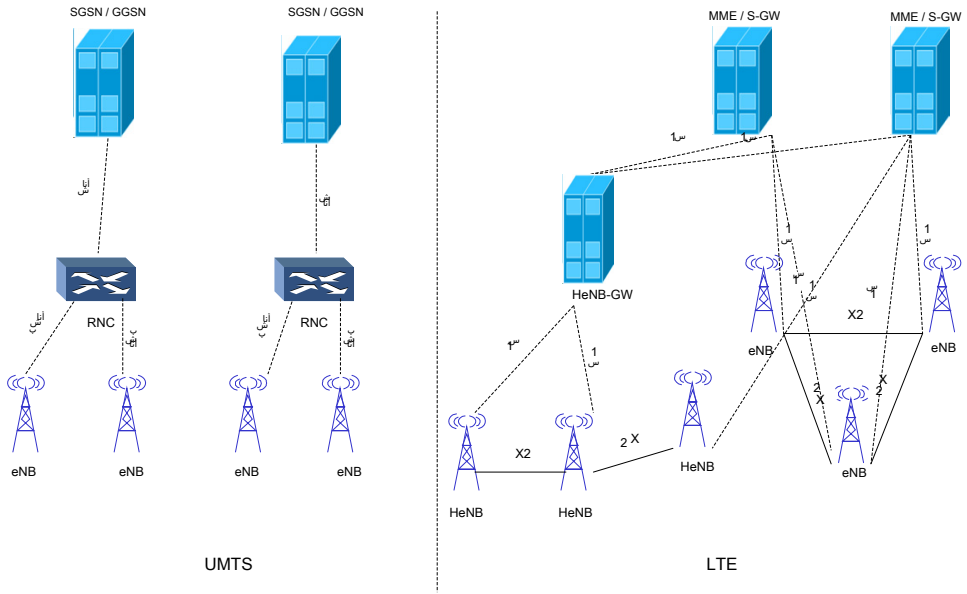
بين جهاز MTC و)A3(، MME متطلبات الأمان والميزات والتهديدات والحلول للمركز-

ج) ، MTC الأمان بالنسبة إلى MTC بين مستخدم MTC وتطبيق MTC وجهاز MTC. تقسيمه أيضًا إلى منطقتين فرعيتين ، (C1) أمان MTC بين خادم MTC وجهاز)C2(MTC بين خادم MTC / مستخدم MTC ، وتطبيق MTC ، وجهاز MTC ، والذي يمكن الأمان لـ

رابعا. الخامس في ULNERABILITIES إس LTE F ECURITY رامبورك

كما ذكرنا سابقًا ، حددت 3GPP الحماية الأمنية.

تم قبول هذه المقالة لتضمينها في عدد مقبل من هذه المجلة. المحتوى نهائي كما هو مقدم ، باستثناء ترقيم الصفحات.



الشكل 11. مقارنة بين بنية شبكة الوصول

نقاط الضعف هذه بالتفصيل في إطار عمل أمان LTE ، على وجه التحديد في طبقة MAC. الأمنية ومشاكل الأمان الموجودة في بنية أمان LTE الحالية. في هذا القسم ، نستكشف الاستجابة لمشاكل الأمان. ومع ذلك ، لا تزال هناك بعض الثغرات

أ. ضعف بنية نظام LTE

الميزات الفريدة لشبكات LTE بعض التحديات الأمنية الجديدة في تصميم آليات الأمان. at لدعم التشغيل البيني الكامل مع شبكات الوصول الراديوي غير المتجانسة. تجلب تم تصميم شبكة LTE من أجل all-IP-based architecture

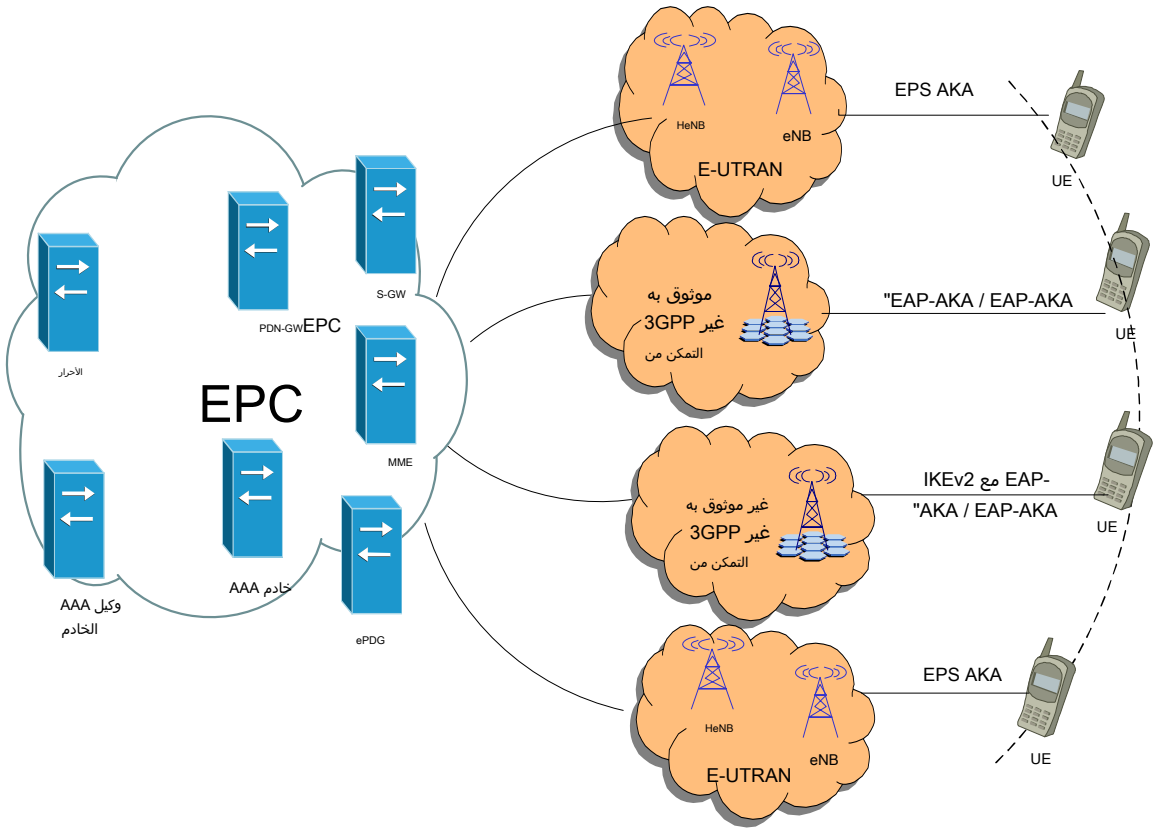
DoS والفيروسات والديدان ورسائل البريد العشوائي والمكالمات وما إلى ذلك [14]. عرضة للهجمات الضارة التقليدية الموجودة على الإنترنت مثل spoo ng لعنوان IP وهجمات أكثر من تلك الموجودة في شبكات GSM و] 29[،]28[UMTS. لقد وجد أن بنية LTE أكثر المزيد من المخاطر الأمنية مثل التعرض للحقن والتعديل وهجمات التنصت ومخاطر الخصوصية (1) تؤدي البنية القائمة على بروتوكول الإنترنت لشبكات 3GPP LTE إلى

في وقت واحد. باستخدام محطة قاعدة خادعة ، يمكن للمهاجم انتحال صفة قاعدة حقيقية يمكن للمهاجم إنشاء نسخته المارقة الخاصة المجهزة بوظائف محطة أساسية ومستخدم صغيرة ومنخفضة التكلفة ، HeNBs ، والتي يمكن للمهاجم الحصول عليها بسهولة ، وبالتالي للخطر بسبب طبيعة IP بالكامل لشبكات LTE. علاوة على ذلك ، نظرًا لإدخال محطات قاعدة بطريقة هرمية. بمجرد أن يهدد الخصم محطة أساسية ، يمكن أن يعرض الشبكة بأكملها تدير شبكة الخدمة في UMTS فقط زوجان من عناصر التحكم في شبكة الراديو (RNCs) الأساسية في شبكات LTE أكثر عرضة للهجمات مقارنة بتلك الموجودة في بنية UMTS ، حيث الشكل 11 ، نظرًا لأن MME تدير العديد من وحدات eNB في بنية at LTE ، فإن المحطات توفر شبكة all-IP مسارًا مباشرًا إلى المحطات الأساسية للمهاجمين الضارين. كما هو مبين في نقاط الضعف المحتملة الأخرى التي تسببها المحطات الأساسية الموجودة في أنظمة LTE. (2) هناك بعض

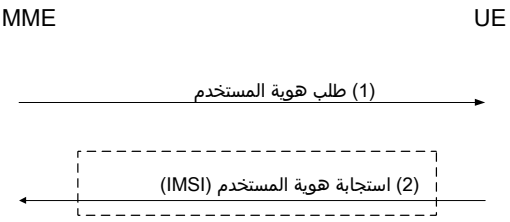
غير آمنة من الإنترنت ، والتي ستكون عرضة لعدد كبير من التهديدات بالاقتحام المادي [30]. اتصال بمحطة أساسية حقيقية. علاوة على ذلك ، نظرًا لأنه يمكن وضع HeNB في مناطق محطة لإغراء مستخدم شرعي. ويمكنه أيضًا إخفاء مستخدم شرعي لإنشاء

مصادقة التسليم. بسبب إدخال المحطة الأساسية البسيطة ، HeNB ، هناك العديد منها (3). قد ينتج عن بنية LTE بعض المشاكل الجديدة في إجراءات

إلى إجراءات مصادقة تسليم مميزة ، مما سيزيد من تعقيد النظام بأكمله. بالإضافة إلى، التجوال كما هو موضح في الشكل 12. بالإضافة إلى ذلك ، تحتاج سيناريوهات التنقل المختلفة الاتصال بالمصادقة ، والترخيص ، وخادم المحاسبة (AAA) أو خادم AAA الوكيل عندما يحدث الجديدة ، مما سيؤدي إلى تأخير تسليم أطول بسبب جولات متعددة من تبادل الرسائل مع مصادقة الوصول الكامل بين UE وشبكة الوصول المستهدفة قبل تسليم UE إلى شبكة الوصول بين E-UTRAN وشبكات الوصول غير]22[3GPP. لكنهم يحتاجون إلى الخضوع لإجراء اقترحت لجنة 3GPP العديد من مناهج مصادقة التسليم لتحقيق عمليات نقل آمنة وسلسة من التهديدات لأمن الشبكة ، خاصةً عندما يتم دعم التنقل بين أنظمة الوصول غير المتجانسة. قليلاً من أنظمة الوصول غير المتجانسة يمكن أن تتعايش في شبكات LTE ، فإنها تجلب المزيد MMEs مختلفة ، مما سيزيد من إجمالي تعقيد النظام. علاوة على ذلك ، نظرًا لأن عددًا ، وبين HeNB و eNB ، وعمليات التسليم بين MME عندما تدار المحطات الأساسية بواسطة المميزة مطلوبة في سيناريوهات مختلفة ، مثل عمليات التسليم بين eNBs ، وبين HeNBs نداءات التسليم ذات الصلة بالتفصيل [6] ، [23]. ومع ذلك ، فإن إجراءات مصادقة التسليم 3GPP عددًا قليلاً من سيناريوهات التنقل التي قد تحدث بين HeNB و eNB ، ووصفت تدفقات عن eNB / HeNB إلى HeNB / eNB جديد كما هو موضح في الشكل 11. اقترحت لجنة سيناريوهات التنقل المختلفة في شبكات LTE عندما يتحرك UE بعيدًا



الشكل 12. التسليم بين شبكة الوصول E-UTRAN و Non-3GPP



الشكل 13. عملية طلب IMSI في EPS AKA

الوصول الأخرى أو الشبكة الأساسية لاستنفاد موارد الشبكة ، حتى لشل الشبكات بأكملها. في شبكات LTE فحسب ، بل قد يتم استغلالها أيضًا من قبل المهاجمين لمهاجمة شبكات النظام بشكل عام. لن تجلب نقاط الضعف هذه الكثير من الصعوبة لدعم الاتصال المستمر آليات الإدارة ، والتي ستزيد أيضًا من تعقيد

ثغرة أمنية في إجراء الوصول إلى LTE

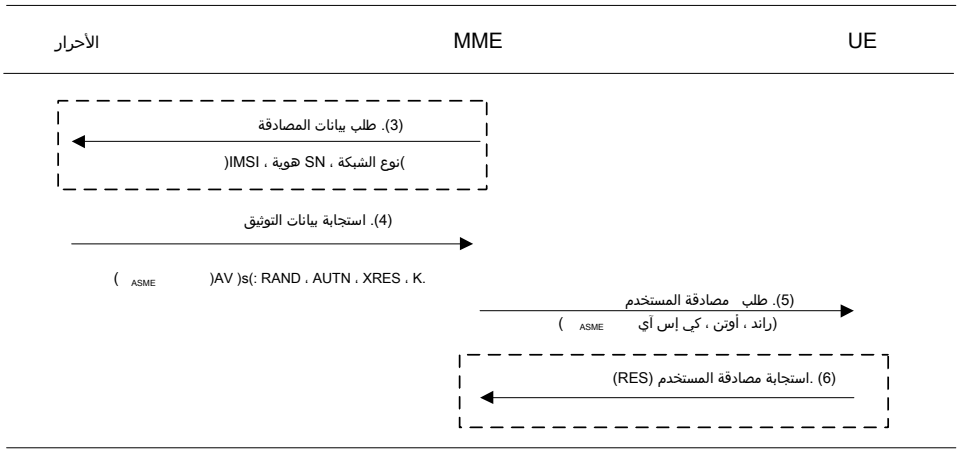
ومع ذلك ، لا تزال هناك بعض نقاط الضعف في آلية أمان الوصول إلى LTE الحالية. الضارة مثل هجمات إعادة التوجيه وهجمات المحطة الأساسية المارقة وهجمات MitM. يحتوي EPS AKA على بعض التحسينات على UMTS AKA بحيث يمكنه منع بعض الهجمات

بسبب فشل محتمل في المزامنة عندما يتجول إلى MME جديد أو MME الحالي أو الجديد UE في الشبكة للمرة الأولى ، أو لا يمكن الاتصال بـ MME الحالي أو لا يمكن استرداد IMSI هناك العديد من الحالات التي أدت إلى الكشف عن IMSI. على سبيل المثال ، عندما يسجل (1) يفتقر مخطط EPS AKA إلى حماية الخصوصية [32].

عن IMSI بواسطة مهاجم نشط ولا تستطيع آلية الأمان الحالية منع مثل هذه الهجمات النشطة. تم اقتراح نموذج هجوم نشط لسرقة IMSI في [32] والذي من خلاله يمكن الكشف بسهولة ثم إخفاء واجهة المستخدم الحقيقية وشن هجمات أخرى مثل هجمات DoS لتدمير الشبكة. للخصم الحصول على معلومات المشترك ومعلومات الموقع وحتى معلومات المحادثة ، ومن 13. قد يؤدي الكشف عن IMSI إلى مشاكل أمنية خطيرة. بمجرد الحصول على IMSI ، يمكن ، وبالتالي ، يجب على UE إرسال IMSI بنص عادي كما هو موضح في الرسالة (2) في الشكل تطلب MME IMSI الخاص بـ UE

(6) الشكل 14. بناءً على الشرطين المذكورين أعلاه ، يمكن للعدو شن هجمات DoS لـ MME أن تصدق على تجهيزات المستعمل إلا بعد استلام RES كما هو موضح في الرسالة المستعمل كما هو موضح في الرسالة (3) في الشكل 14. بالإضافة إلى ذلك ، لا يمكن MME طلبات تجهيزات المستعمل إلى HSS / AuC حتى قبل أن تصدق MME على تجهيزات (2) لا يمكن لمخطط EPS AKA منع هجمات]34[-]32[DoS. يجب أن ترسل

على العديد من هجمات DoS في إجراء NAS لزيادة التحميل على الكيانات في E-UTRAN. ذلك ، تمت الإشارة في [34] إلى أن إجراءات أمان NAS معرضة لهجمات DoS وقد تم العثور للغاية للحصول على استجابة شرعية أو خاطئة من تجهيزات المستعمل المقابلة. بالإضافة إلى أخرى ، يتعين على MME أن تستهلك المخزن المؤقت للذاكرة الخاص بها للانتظار لفترة طويلة HSS أن تستهلك قدرتها الحسابية لتوليد نواقل استيقان مفرطة لتجهيزات المستعمل. ومن ناحية مستخدم شرعية لإرسال IMSI مزيف باستمرار للتغلب على HSS / AuC. وبالتالي ، يتعين على إلى HSS / AuC و]33[،]32[MME. يمكن للخصم إخفاء واجهة



الشكل 14. طلب بيانات المصادقة وعملية المصادقة المتبادلة

عرض النطاق الترددي وإشارات المصادقة بين SN و HN واستهلاك التخزين في]35[SN. UE في SN لفترة طويلة وتستنفد مجموعتها من AVs للمصادقة ، مما يتسبب في استهلاك الشكل 14 ، يجب أن يعود SN إلى HN لطلب مجموعة أخرى من نواقل المصادقة عندما تظل (3). على غرار UMTS AKA ، في EPS-AKA كما هو موضح في الرسالة (3) و (4) في

فيما يتعلق بعملية المصادقة بين UE و SN ، والتي يمكن إرجاعها إلى تاريخها المتطور. ذلك ، يفتقر بروتوكول EPS-AKA إلى القدرة على المصادقة عبر الإنترنت لأن HN غير متصل الوصول الأخرى ، تبدو افتراضات الثقة الأصلية قديمة بين الشبكات غير المتجانسة. بالإضافة إلى يتطلب افتراضات ثقة قوية بين هؤلاء المشغلين. مع تزايد عدد شركاء التجوال وإدخال أنظمة جميع سلطات المصادقة تقريبًا من الشبكة المنزلية إلى الشبكة التي تمت زيارتها ، الأمر الذي EPS AKA ، مثل GSM AKA و UMTS AKA ، هو بروتوكول مفوض [36]. يتم تفويض (4). بروتوكول

هجمات MitM ، ونقص تزامن رقم التسلسل (SQN) ، واستهلاك إضافي للنطاق الترددي. EAP-AKA به العديد من أوجه القصور مثل الكشف عن هوية المستخدم ، والضعف أمام أو EAP-AKA لتوفير مصادقة وصول آمنة. تمت الإشارة في [37] إلى أن بروتوكول UE إلى EPC عبر شبكة وصول موثوقة غير 3GPP ، فإن بنية LTE تعيد استخدام EAP-AKA (5) عند وصول

ج. الثغرة الأمنية في إجراءات تسليم LTE

العثور على الكثير من الثغرات الأمنية في إجراءات إدارة التنقل LTE وآلية مفتاح التسليم. لمشاكل الأمان لدعم التنقل الآمن بين أنظمة الوصول غير المتجانسة. ومع ذلك ، لا يزال يتم من eNB إلى آخر. بالإضافة إلى ذلك ، حددت لجنة 3GPP متطلبات الأمان والتهديدات والحلول مخططًا جديدًا لإدارة مفتاح التسليم لتحديث المواد الرئيسية بين UE و eNB عندما تتنقل UE للتخفيف من التهديدات الأمنية التي تشكلها المحطات الأساسية الخبيثة ، توفر آلية أمان LTE

انعدام الأمن المتخلف [38]. نظرًا لأن آلية إدارة مفتاح LTE تستخدم بنية تسلسل المفاتيح ، (1)

eNB المحددة [38]. على سبيل المثال ، كما هو موضح في الشكل 15 ، يمكن لمصدر eNB مفاتيح جديدة للعديد من وحدات eNB المستهدفة من خلال ربط المفتاح الحالي بمعلمات قد يشتق eNB الحالي
اشتق مفتاح الجلسة الجديد *k eNB* بين الهدف eNB
و UE من المفتاح المعروف *k* .
*eNB*وكل منها
وبالتالي ، فشلت إدارة مفتاح التسليم في تحقيق الأمان المتخلف في شبكات LTE الحالية. الهدف. بمجرد قيام المهاجم بخرق مصدر eNB ، سيتم الحصول على مفاتيح الجلسة التالية. المعلمات

اشتقاق مفتاح التسليم الأفقي ، وبالتالي ستكون مفاتيح الجلسة المستقبلية عرضة للخطر. في هذه المناسبة ، تقوم eNBs المستهدفة بإلغاء مزامنة قيمة NCC ويمكنها فقط تنفيذ أو رسالة إقرار تبديل المسار S1 ، الموضحة في الشكل 15 ، من MME إلى a. الهدف eNB. قيمة NCC إما عن طريق معالجة رسالة طلب التسليم ، الموضحة في الشكل 15 ، بين eNBs بـ eNB القانوني أو ينشر eNB شخصيًا. بواسطة eNB المارقة ، يمكن للمهاجم تعطيل تحديث (2) قابلية التأثر بهجمات عدم التزامن [39]. افترض أن أحد الخصوم يخل

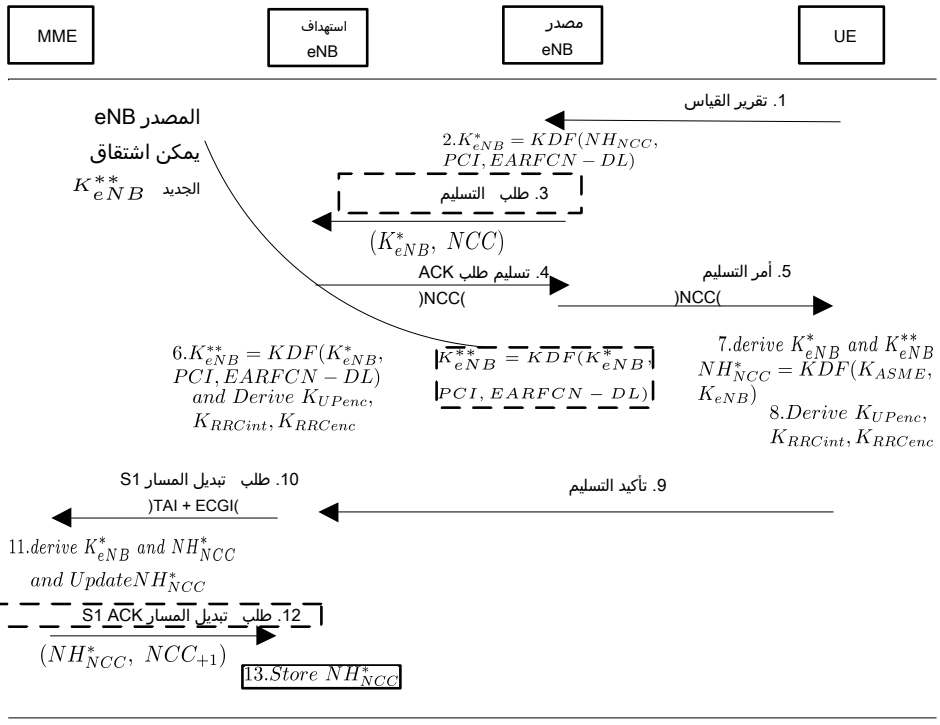
المجمعة بدلاً من الرسالة الشرعية إلى eNB المستهدف. ثم ، تحيات eNB المستهدفة عندما تريد UE الانتقال إلى eNB مستهدف ، يرسل الخصم رسائل طلب التسليم السابقة المهاجم رسالة طلب تسليم مشفرة ، كما هو مبين في الشكل 15 ، بين UE و eNB شرعي. الهجوم هو تدمير إنشاء الرابط الآمن بين تجهيزات المستعمل و eNB المستهدفة. أولاً ، يعترض (3) الضعف أمام هجمات الإعادة [39]. والغرض من هذا

المفتاح المستلم *k eNB* كمفتاح ارتباط ، ويرسل قيمة NCC في الرسالة السابقة مرة أخرى في الرسالة السابقة
إلى UE. عند استلام قيمة NCC من الهدف
القيمة المخزنة في تجهيزات المستعمل. نظرًا لأن قيمة NCC مما إذا كانت UE يتحقق ، eNB فشلًا. وبالتالي ، لن يتم إنشاء اتصال أمني بين تجهيزات المستعمل و NCC المستلمة تساوي أن تبدأ إجراء تسليم جديد eNB المستلمة تأتي من الرسالة السابقة ، فإن الفحص يكون .الهدف ويتعين على تجهيزات المستعمل

د. الضعف في آلية أمن IMS

بالإنترنت مباشرة ، فإن .IP و SIP يعمل على أساس ، IGPPالذي قدمته لجنة 3 IMS .عرضة لعدة أنواع من الهجمات IMS نظرًا لاتصاله

تم قبول هذه المقالة لتضمينها في عدد مقبل من هذه المجلة. المحتوى نهائي كما هو مقدم ، باستثناء ترقيم الصفحات.



الشكل 15. تسليم Inter-eNB

أمن IMS. ومع ذلك ، فإن آلية أمان IMS المحددة بواسطة 3GPP بها بعض الثغرات الأمنية. استخدمت لجنة 3GPP مخطط IMS AKA لضمان

المماثلة ، مما يزيد من تعقيد النظام بشكل عام ويؤدي إلى تدهور جودة الخدمة (QoS). UEs. بالإضافة إلى ذلك ، يشترك هذان الإجراءان من إجراءات AKA في العديد من العمليات يجلب استهلاكًا عاليًا للطاقة لتجهيزات UE محدودة الطاقة وبالتالي يقلل من عمر البطارية في EPS AKA ، AKA في مصادقة الوصول إلى LTE و IMS AKA في مصادقة IMS ، مما الطاقة في تجهيزات المستعمل وتعقيد النظام [40]. يحتاج IMS UE إلى تنفيذ بروتوكولين (1) أدى إجراء المصادقة في نظام IMS إلى زيادة استهلاك

الضعف لهجمات MitM ، ونقص تزامن SQN ، واستهلاك عرض النطاق الترددي الإضافي. EAP. وبالتالي ، على غرار EAP AKA ، فإن IMS AKA لديه العديد من أوجه القصور مثل (2) يعمل نظام IMS AKA على أساس مخطط]41[AKA

I-CSCF / S-CSCF عن طريق إرسال الحزم الصحيحة مع IMSI / IMPI غير صالح. (I-CSCF / SCSCF) لتنفيذ مصادقة الوصول. في هذا الإجراء ، يمكن للخصم أن يملأ HSS ، كما هو مبين في الشكل 7 ، يرسل PCSCF / MME الطلب إلى الشبكة الأساسية (HSS) لأنواع عديدة من هجمات]42[DoS. على سبيل المثال ، بعد تلقي طلب تسجيل من IMS UE (3) إن آلية أمن IMS عرضة

هـ. الضعف في آلية أمن HeNB

و EPC ، والتي تكون عرضة لأنواع عديدة من الهجمات لأن البيانات والمحادثات هي المحددة في [12] من الروابط اللاسلكية غير الآمنة بين UE و HeNB والوصلة بين HeNB بتوزيع التهديدات على HeNBs ومتطلبات أمن]12[HeNB. تنشأ معظم نقاط الضعف الأمنية قامت لجنة 3GPP

، فقد تم استكشاف أن مواصفات 3GPP الحالية لم تعالج بعد بعض متطلبات أمن HeNB. الضعف هذه ، تمت مناقشة الإجراءات المضادة المقابلة من قبل لجنة]12[3GPP. ومع ذلك عرضة للاعتراض والتنصت على هذه الروابط. للتغلب على نقاط

بشكل مستقل لأن الصدق بينهما غير صالح في الشبكة القائمة على بروتوكول الإنترنت. إلى ذلك ، لا يعتبر HeNB طرف ثقة مناسبًا إذا قامت الشبكة الأساسية و OAM بمصادقتها وصول المشتركين لأنها لا تحتوي على مصادقات متبادلة قوية بين UE و HeNB. بالإضافة المختلفة بما في ذلك هجمات التنصت وهجمات MitM وهجمات التنكر والإضرار بقائمة و HeNB. يُشار في [43] إلى أن آلية أمان HeNB الحالية لا يمكنها منع هجمات البروتوكول (1) عدم وجود مصادقة متبادلة بين تجهيزات المستعمل

العام ، فهي عرضة للعديد من الهجمات المستندة إلى الإنترنت ، وخاصة هجمات DoS. لمعدلات البيانات. ومع ذلك ، نظرًا لانكشاف نقاط الدخول للشبكة الأساسية على الإنترنت HeNBs ، والذي يمكن أن يتجنب الترقيات المكلفة للاتصالات الأساسية وتلبية الحاجة المتزايدة بتكلفة منخفضة ، فإنه يعد بديلاً جيدًا لمشغلي الهاتف المحمول لإجراء نشر واسع النطاق لـ DoS. تخضع بنية HeNB في شبكة LTE لهجمات]44[DoS. نظرًا لخصائص الحجم الصغير (2) قابلية التأثر بهجمات

و. الثغرات الأمنية في هندسة أمن MTC

من الأجهزة وعمليات نقل البيانات الصغيرة وغير المتكررة وسيناريوهات الخدمة المتميزة في شبكات 3GPP الحالية ، تتضمن MTC الكثير من الميزات الفريدة مثل العدد الهائل لا يزال إدخال MTC في أنظمة LTE في مهده. تختلف عن اتصالات H2H المصممة

الكامنة في MTC لم يتم استكشافها بشكل جيد من قبل لجنة 3GPP والباحثين الآخرين. الخدمة والعديد من تحسينات النظام لـ]48[،]7[MTC. ومع ذلك ، فإن القضايا الأمنية - [47] لمعالجة القضايا المذكورة أعلاه. وصفت لجنة 3GPP أيضًا معمارية MTC ومتطلبات من أجل تعزيز التطور السريع لـ MTC. في السنوات الأخيرة ، تم اقتراح الكثير من الحلول [45] من العقبات التقنية في بنية النظام ، والواجهة الجوية ، وإدارة الموارد الراديوية وجودة الخدمة مسبوقة لـ 3GPP لتحقيق توحيدها. وبالتالي ، تحتاج شبكة LTE الحالية إلى التغلب على الكثير وفرص أقل لإعادة شحن الأجهزة ، مما يجلب تحديات غير

، سيتم تحسين بنية نظام LTE ، مما قد يتسبب في بعض مشكلات الأمان الجديدة. هكذا، لضمان الاتصال الآمن بين أجهزة MTC. علاوة على ذلك ، من أجل دعم ميزات MTC المتنوعة وأجهزة MTC (مثل B2 ، A3 ، و C2 في الشكل 10). بالإضافة إلى ذلك ، لا توجد آلية محددة غير 3GPP ، و MTC بين تطبيقات MTC وشبكات 3GPP و MTC بين تطبيقات MTC على سبيل المثال ، تفتقر إلى آليات الأمان الخاصة بـ MTC بين جهاز MTC و ePDG للوصول ذلك ، لا تزال هناك العديد من المشكلات التي تحتاج إلى مزيد من التحسين لبنية أمان MTC. في الشكل 10 وناقشت بعض التهديدات والمتطلبات والحلول المقابلة لأمن]10[MTC. ومع قدمت لجنة 3GPP نظرة عامة على معمارية أمن MTC كما هو موضح

حمل زائد للتشوير بين HSS و MME عندما يطلبون في نفس الوقت الوصول إلى الشبكة. يشار في [50] إلى أن الاستيقان المتزامن لعدد كبير من أجهزة MTC يمكن أن يؤدي إلى منخفضة من حيث موارد الطاقة والحوسبة ، ويتم نشرها دون إشراف بشري لفترة طويلة. والهجمات على الشبكة الأساسية لأن أجهزة MTC هي مطلوب عادةً أن تكون القدرات لأنواع عديدة من الهجمات مثل الهجمات الجسدية واختراق بيانات الاعتماد وهجمات البروتوكول ، [50]. تم تحليل التهديدات الأمنية في MTC في [49] ووجدت أن أجهزة MTC معرضة بشدة هناك عدد قليل من الأدبيات حول أمن MTC التي تم تناولها في [49]

ضد OLUTIONS TO THE رمبتهج س ECURITY أناSSUES

القسم ، سنراجع الحلول الحالية لمعالجة نقاط الضعف المذكورة أعلاه في الأدبيات الحالية. في هذا

أ. بنية نظام LTE

الهدف. لذلك ، لديها عملية مصادقة بسيطة بدون إدارة مفاتيح معقدة ويمكن تحقيقها طويلة الأجل تم إنشاؤها بواسطة توقيعات الوكيل عندما تدخل UE في تغطية eNB أو HeNB eNB أو HeNB المستهدفين تحقيق مصادقة متبادلة مباشرة وإنشاء مفتاح جلسة بمفاتيح سرية بين وحدات eNB وعمليات التسليم فيما بين MME. من خلال المخطط ، يمكن لـ UE و في ذلك عمليات التسليم بين HeNBs وعمليات التسليم بين eNBs و HeNBs ، عمليات التسليم أساس توقيع الوكيل المحسن في [38] ، والذي يمكن تطبيقه على جميع سيناريوهات التنقل بما في بنية نظام LTE ، تم اقتراح مخطط مصادقة تسليم جديد بسيط وقوي على

ذات قيود الموارد. بالإضافة إلى ذلك ، قد يعانون من مشاكل متوافقة في شبكات LTE. المخططين الكثير من التكاليف الحسابية ونفاد البطارية ، وهو أمر غير ممكن للأجهزة المحمولة ذلك، نظرًا لاستخدام تقنية توقيع الوكيل والتشفير المستند إلى الهوية (IBC) ، فقد يتحمل كلا جميع سيناريوهات التنقل بين E-UTRAN وشبكات الوصول غير 3GPP في شبكات LTE. ومع ثالث. يمكن أن يوفر المخطط في [51] حماية أمنية قوية وكفاءة مثالية ويمكن تطبيقه على Key لاشتقاق مفتاح الجلسة المشتركة فقط من خلال 3 مصافحة بدون الاتصال بأي طرف عليها باستخدام مفاتيحهما طويلة الأجل التي تم إنشاؤها بواسطة)KGC(Generate Center عندما تنتقل UE إلى تغطية AP جديدة ، يمكن لـ UE و AP الجديدة تنفيذ اتفاقية مفتاح مصدق و ePDG لشبكات الوصول غير الموثوق بها non3GPP بشكل جماعي بنقاط الوصول (APs).]51[LTE. وفقًا للمخطط ، يُشار إلى E-UTRAN وشبكات الوصول الموثوقة غير 3GPP تسليم سريع وآمن لتحقيق عمليات تسليم سلسة بين أنظمة الوصول غير المتجانسة في شبكات الكفاءة المرغوبة. بعد ذلك ، تم اقتراح مخطط مصادقة

B. الأمان الخلوي LTE

أمان هوية المستخدم والرسالة المتبادلة مع استهلاك محدود للطاقة باستخدام Ellipse SE-EPS) القائمة على البنية التحتية للمفتاح العام اللاسلكي (WPKI) في [54]. يضمن النظام للطاقة باستخدام Ellipse تم اقتراح اتفاقية المصادقة المحسنة الأمنية واتفاقية المفتاح (AKA (WPKI) في [54]. يضمن النظام أمان هوية المستخدم والرسالة المتبادلة مع استهلاك محدود الأمنية واتفاقية المفتاح (SE-EPS AKA) القائمة على البنية التحتية للمفتاح العام اللاسلكي المتبادلة مع استهلاك محدود للطاقة باستخدام Ellipse تم اقتراح اتفاقية المصادقة المحسنة التحتية للمفتاح العام اللاسلكي (WPKI) في [54]. يضمن النظام أمان هوية المستخدم والرسالة اقتراح اتفاقية المصادقة المحسنة الأمنية واتفاقية المفتاح (SE-EPS AKA) القائمة على البنية السجل وإعادة المصادقة ومصادقة التسليم على التوالي لسيناريوهات المصادقة المختلفة. تم نظام 3G AKA. بالإضافة إلى ذلك ، تم تقديم ثلاثة بروتوكولات مصادقة بما في ذلك مصادقة لتجهيزات المستخدم لتحديد المحطة الأساسية الأصلية ، وبالتالي يتغلب على أوجه القصور في 4G اللاسلكية في [53]. ينشئ المخطط بروتوكول بث مفتاح عمومي يعتمد على طريقة احتمالية تم اقتراح مخطط مصادقة واتفاقية مفتاح يعتمد على مفتاح عام معتمد ذاتيًا (SPAKA) لأنظمة المرور بـ with ngerprint والمفتاح العام لتحقيق الاستيقان المتبادل بين UEs و HN عبر TMP. إلى الخدمات والبيانات الحساسة في أنظمة الجيل الرابع. بالإضافة إلى ذلك ، ترتبط كلمات التحتية للمفاتيح العمومية ، يمكن أن يوفر قوة كبيرة لمستخدمي الهواتف المحمولة للوصول 4G المتنقلة في [52]. من خلال المخطط ، نظرًا لاعتماد مفهوم الحوسبة الموثوقة والبنية تفويض يعتمد على)TMP(Trust Model Platform والبنية التحتية للمفتاح العام (PKI) لشبكات في النظام الخلوي LTE ، تم اقتراح مصادقة هجينة واتفاق رئيسي ومخطط

ذلك ، تم اقتراح مصادقة مصادقة مضمونة واتفاقية مفتاح (ECAKA) لتعزيز سرية المستخدم. عرضة للقوة الغاشمة وهجمات القوة الذكية وبالتالي لا يمكنه ضمان أمن هوية المستخدم. بعد الواردة في بروتوكول EAP-AKA. تمت الإشارة في [56] إلى أن بروتوكول SE-EPS AKA Elliptic Curve Dif e-Hellman مع نظام تشفير رئيسي متماثل للتغلب على نقاط الضعف وصول واتفاقيات رئيسية جديدة تستند إلى EAP-AKA. كلا المخططين يستخدمان)ECDH(التهديدات والهجمات في التشغيل البيني لشبكة 3G-WLAN واقترحت بروتوكولات مصادقة تشفير منحنى (ECC). قامت المخططات الواردة في [37] ، [55] بتحليل

تنفيذه لضمان الاتصال الآمن والأسباب التي تجعل مخطط J-PAKE يمكن أن يوفر أقوى وسيط الإرسال. ومع ذلك ، فقد تناول فقط استخدام J-PAKE في شبكات LTE دون إدخال كلمة المرور لتوفير إثبات المعرفة الصفرية باستخدام مفتاح مشترك لا يتم إرساله أبدًا عبر EPS AKA لتوفير حماية أمنية أقوى. إن]60[J-PAKE هو بروتوكول اتفاقية مفتاح مصادقة Juggling Password Authenticated Key في عملية المصادقة بدلاً من بروتوكول اقتراح استخدام تبادل مفتاح مصادقة كلمة المرور بواسطة بروتوكول)J-PAKE(Exchange ، بينما لا يمكن التغلب على مشكلات الأمان الموجودة في إجراء EPS-AKA. في [59] ، تم المركبات ذاتية القيادة في MME. بالإضافة إلى ذلك ، يمكنه فقط تعزيز كفاءة إجراء المصادقة / HSS. ومع ذلك ، فإن هذا المخطط قادر على زيادة عبء MME لأنه سيتم إنشاء الكثير من تبادل إشارات الاستيقان بين SN و HN ، وبالتالي يوفر استهلاك عرض النطاق الترددي في HN (AVs) من AVs الأصلية في HSS / HN. يمكن للنظام في [35] أن يقلل بشكل كبير من بسيط في SN. بالمخطط ، تقوم MME / SN بإنشاء وتخزين الكثير من نواقل المصادقة EPS AKA محسن في [35] لتحسين أداء إجراء المصادقة الحالي عن طريق زيادة حساب بالإضافة إلى ذلك ، لا يمكنها التغلب على الكشف عن هوية المستخدم. تم اقتراح بروتوكول لعدد كبير من حالات التأخير في الاتصال وبالتالي يتسبب في ازدحام الإشارات على HSS. الجديد. نظرًا لأن HSS يحتاج إلى المشاركة في كل إجراء مصادقة لكل UE ، فقد يتعرض الوصول. ومع ذلك ، قد يعاني من مشاكل متوافقة في شبكات LTE بسبب استخدام ESIM للتغلب على أوجه القصور في بروتوكول EPS-AKA فقط مع تعديلات طفيفة في بنية أمان ESIM بدلاً من USIM ويوفر مصادقة متبادلة مباشرة عبر الإنترنت بين ESIM و HSS / MME نسخة معدلة قليلاً من بروتوكول EPS-AKA في [36]. يقدم المخطط وحدة جديدة للمشتركين والذي لا يمكنه منع شبكة LTE من الكشف عن هوية المستخدم وهجمات spoo ng. تم تقديم إلى الشبكة. ومع ذلك ، يواجه هذا المخطط نفس نقاط الضعف مثل بروتوكول EPS AKA ، ، يمكن للنظام في [58] تحقيق مصادقة متبادلة واتفاق مفتاح بين المستخدمين وطبقة الوصول طريقة]58[EAPArchie لضمان أمان طبقة الوصول في شبكات LTE. باستخدام تشفير AES ، يبدو أن 3GPP مترددة في تفويض مثل هذه البنية التحتية الباهظة الثمن [57]. تم تقديم إلى تحمل عدد كبير من النفقات العامة للنشر لإنشاء البنية التحتية للمفتاح العام. في الواقع التحتية للمفتاح العام عبر جميع المشغلين باتفاقيات تجوال متبادلة. لذلك، تحتاج شبكة LTE المحدودة. بالإضافة إلى ذلك ، في بيئة الطبيعة المفتوحة لشبكة LTE ، يجب أن تمتد البنية كبير من التكاليف الحسابية وتكاليف التخزين وتكاليف الاتصال للأجهزة المحمولة ذات الموارد استخدام UE و / أو AuC / HSS لشهادات المفتاح العام. ومع ذلك ، سيؤدي ذلك إلى عدد يمكن تحقيق مصادقة متبادلة وضمان الأمن الاتصال بين UE و AuC / HSS عن طريق آليات الحماية القائمة على المفتاح العام للتغلب على عيوب بروتوكول EPS AKA ، وبالتالي الذين يتم تعقبهم. كل هذه المخططات المذكورة أعلاه في [37] ، [52] - [54] ، [56] تستخدم عن طريق التشفير ، والذي يمكن أن يمنع الكشف عن هوية المستخدمين والمستخدمين وفقًا للمخطط ، فإن جميع رسائل AKA محمية تمامًا من حيث التكامل

ذلك ، لا يمكنها معالجة مشكلة الأمان المقدمة في بروتوكول EPS AKA ، أي حماية الهوية. الأمن من EPS AKA. بالإضافة إلى

ج. أمان تسليم LTE

التسليم بين أنظمة WiMAX وشبكات WLAN في [65] ، والتي تتجنب الاتصال بالمصادقة ذلك. تم اقتراح خمسة بروتوكولات إعادة مصادقة سريعة وآمنة لمشتركي LTE لإجراء عمليات الكثير من المشكلات التي يجب معالجتها ، مثل الأمان والأداء والمشكلات المتوافقة ، وما إلى جيدة لتحقيق تنقل سلس بين شبكات 3GPP والشبكات غير 3GPP. ومع ذلك ، لا يزال هناك وشبكات WLAN في [65] ، والتي تتجنب الاتصال بالمصادقة يقترح المخطط في [64] فكرة إعادة مصادقة سريعة وآمنة لمشتركي LTE لإجراء عمليات التسليم بين أنظمة WiMAX ، مثل الأمان والأداء والمشكلات المتوافقة ، وما إلى ذلك. تم اقتراح خمسة بروتوكولات والشبكات غير 3GPP. ومع ذلك ، لا يزال هناك الكثير من المشكلات التي يجب معالجتها بالمصادقة يقترح المخطط في [64] فكرة جيدة لتحقيق تنقل سلس بين شبكات 3GPP لإجراء عمليات التسليم بين أنظمة WiMAX وشبكات WLAN في [65] ، والتي تتجنب الاتصال ، وما إلى ذلك. تم اقتراح خمسة بروتوكولات إعادة مصادقة سريعة وآمنة لمشتركي LTE يزال هناك الكثير من المشكلات التي يجب معالجتها ، مثل الأمان والأداء والمشكلات المتوافقة [64] فكرة جيدة لتحقيق تنقل سلس بين شبكات 3GPP والشبكات غير 3GPP. ومع ذلك ، لا الأساليب الحالية بما في ذلك نقل سياق الأمان وآلية المصادقة المسبقة ، يقترح المخطط في غير 3GPP لتقليل زمن انتقال التسليم دون المساس بمستوى الأمان . من خلال اعتماد الموثوقة غير 3GPP وآلية مصادقة مسبقة لعمليات التسليم بين 3GPP والشبكات غير الموثوقة بالمخطط ، تستخدم آلية نقل سياق الأمان لعمليات التسليم بين شبكات 3GPP والشبكات تسليم سريع محسّنة في [64] للتعامل مع عمليات التسليم بين 3GPP والشبكات غير 3GPP. بالإضافة إلى ذلك ، لم يتم تقديم عمليات تسليم من WLAN إلى 3GPP LTE. تم تقديم آلية يتطلب الكثير من تكاليف النشر والتغييرات في البنية الحالية وبالتالي زيادة تعقيد النظام بأكمله. (HIU) ، للعمل كمحطة ترحيل بين شبكة LTE والشبكة المحلية اللاسلكية ، الأمر الذي قد 3GPP. ومع ذلك ، من خلال هذا المخطط ، يجب نشر كيان جديد ، وحدة الترابط الهجين تحسين بروتوكول EAPAKA ويعتمد وحدة هجينة لتوفير التشغيل البيني الآمن LTE-WLAN لتأمين التشغيل البيني والتجوال من 3GPP LTE إلى WLAN في [63]. يعمل النظام على و UMTS في إجراءات التسليم والثغرات الأمنية. تم اقتراح بروتوكول جديد لإعادة المصادقة / LTE وشبكات الوصول الأخرى ، حيث تختلف أنظمة LTE-A / LTE-A كثيرًا عن نظام GSM مشكلات الأمان الموجودة في أنظمة GSM. لم تتم معالجة عمليات التسليم بين أنظمة LTE-A يركز هذا المخطط فقط على عمليات التسليم بين WiMAX / WiFi و GSM / UMTS ويغطي و WiFi و WiMAX دون الحاجة إلى اشتراك مسبق في الشبكات التي تمت زيارتها. ومع ذلك ، عالمي لتمكين التسليم الرأسي بين أنظمة الوصول غير المتجانسة بما في ذلك GSM و UMTS المختلفة في شبكات 4G اللاسلكية في [62]. يصمم المخطط في [62] بروتوكول مصادقة 4G اللاسلكية. تم اقتراح مخطط تجوال أمني وتسليم عمودي بين العديد من تقنيات الوصول التشفير العام ، وبالتالي يجلب الكثير من الصعوبة لدعم عمليات التسليم السلس في أنظمة ومع ذلك ، فقد يتسبب في الكثير من التكاليف الحسابية وتكاليف التخزين بسبب استخدام تحقيق مصادقة متبادلة بين تجهيزات المستعمل والشبكة الأجنبية (FN) دون استخدام شهادة. إلى ذلك ، من خلال اعتماد بروتوكول إذاعة المفتاح العام المصمم كجزء من المخطط ، يمكن [61] كلمة مرور ديناميكية بمفتاح عمومي لتوفير مصادقة خفيفة وخدمة عدم التنصل. بالإضافة لدعم التنقل العالمي والاتصالات الآمنة في أنظمة 4G اللاسلكية [61]. يربط المخطط في من أجل عمليات تسليم LTE الآمنة ، تم اقتراح مصادقة مختلطة ونظام اتفاقية مفتاح

في الاتصالات اللاسلكية متعددة القفزات وآليات الأمان لحماية رسائل القفزات المتعددة. أن يدعم سوى الاتصالات أحادية القفزة بين UE و)BS(AP / Base Station). يجب التحقيق العديد من ميزات الأمان بما في ذلك السرية الأمامية والخلفية. ومع ذلك ، لا يمكن للمخطط المرور وتأخير إعادة المصادقة مقارنة ببروتوكولات 3GPP القياسية الحالية ويمكن أن يوفر التعديلات. يمكن للنظام في [65] تحقيق أداء متميز من حيث إعادة المصادقة على إشارات ، والتي يمكن أن تتجنب مشاكل التشغيل البيني مع الخدمات الأخرى دون فقدان القدرات بسبب و INEA لها نفس تسلسل الرسائل كما هو الحال في EAP-AKA القياسي و INEA المصادقة في عمليات تسليم WiMAX-WLAN المستقبلية. النسخة المعدلة من EAP-AKA من WLAN إلى نظام WiMAX من خلال تضمين معلمات أمان إضافية ومفاتيح للسرعة زيادة نظام WiMAX إلى WLAN وبروتوكول مصادقة دخول الشبكة الأولية (INEA) لعمليات التسليم التسليم. من خلال هذه المخططات ، يمكن تحسين بروتوكول EAP-AKA لعمليات التسليم من الخوادم في شبكات LTE أثناء

أمر غير ممكن للأجهزة المحمولة ذات الموارد المحدودة. تم اقتراح آلية مصادقة ، ECC و IBC عليها في إجراء مصادقة الشبكة الأولى في مصادقة G-WLANمحسنة لشبكات IMS 3 وهو [72]. وفقًا للمخطط ، سيتم إعادة استخدام ناقلات المصادقة ومفاتيح التشفير التي تم الحصول طريق نقلها بأمان من IMS من خلال تشجيع إعادة استخدام مفتاح فعال لمستخدم متنقل في عندما ينتقل المستخدم من مجال .HSS عبر S-CSCF إلى)HAAA(Home AAA عن المطلوب لاشتقاق نواقل المصادقة وبالتالي تجنب النفقات الإضافية وتدهور جودة الخدمة متبادلة بين تجهيزات المستعمل و WLAN لذلك ، يمكن أن يقلل المخطط إلى حد كبير الوقت إجراء مصادقة S-CSCF إلى آخر دون تغيير البنية الحالية. ومع ذلك ، لا يمكن أن يوفر مصادقة .المقترح IMS في

E. HeNB الأمن

سيما فيما يتعلق باستراتيجية التحكم في الوصول. عندما يريد UE الوصول إلى الشبكة عبر في [73]. تقدم هذه الورقة لمحة عامة عن العمل الجاري بشأن توحيد HeNB في 3GPP ، لا بالنسبة لأنظمة HeNB ، تم تناول مسائل المصادقة والتحكم في الوصول لمستخدمي HeNB

D. أمن IMS

ذلك ، قد يتحمل المخطط الكثير من التكاليف الحسابية وتكاليف التخزين بسبب استخدام مصادقة المستخدمين بطريقة شخصية أثناء الوصول إلى الخدمات ويوفر حماية أمنية قوية. ومع و)ECC(Elliptic Curve Cryptography ، يسمح المخطط بتخصيص خدمات IMS من خلال جديد في [71] باستخدام IBC لتعزيز أمن عملية مصادقة IMS. من خلال اعتماد مفهوم IBC تم استخدام IMPI الوحيد لتحقيق مصادقة طبقة الشبكة. تم اقتراح مخطط مصادقة خدمة IMS ومع ذلك ، قد يتسبب المخطط في بعض المشكلات في استخدام خدمات الشبكة العادية لأنه تجنب التنفيذ المزدوج لبروتوكول AKA وبالتالي تقليل الحمل الزائد للإشارة إلى حد كبير. مع المستخدم في إجراء مصادقة طبقة IMS دون الاتصال بـ HSS. لذلك ، يمكن للنظام الحصول مباشرة على AV للمستخدم من MME لإنشاء مفاتيح تشفير وتكامل صالحة IMPI فقط بدون IMSI للمستخدمين. بعد نجاح مصادقة طبقة الشبكة ، يمكن لـ P-CSCF استهلاك الطاقة. من خلال المخطط ، يمكن تنفيذ طبقة الشبكة ومصادقة طبقة IMS باستخدام تمت معالجة بروتوكول المصادقة المحسن)I-AKA(AKA في [40] لشبكات LTE لتقليل الاحتيالي لخدمات IMS وهجمات التنصت وهجمات الخادم المزيفة وهجمات الغش المؤقتة. بإجراء المصادقة متعددة المرور. ومع ذلك ، فإن هذا النهج معرض بشكل كبير للاستخدام الأمنية بين UE و P-CSCF ، وبالتالي يمكن أن يقلل بشكل ملحوظ من عبء المصادقة مقارنة مصادقة المستخدم باستخدام زوج (IMSI ، IMPI) في مصادقة طبقة خدمة IMS دون الحماية المخطط ، يمكن تنفيذ ربط مفتاح الأمان بين المصادقة الأولية والمصادقة الثانية بحيث يمكن تم تقديم إجراء محسن لـ onepass AKA لشبكات الجيل التالي (NGN) في [70]. من خلال المصادقة ذات المسار الواحد في UMTS من أجل تقليل تكاليف تشوير الاستيقان [66] - [69]. فيما يتعلق بأمن IMS ، تم اقتراح العديد من مخططات

من إستراتيجية التحكم في الشبكة ، حيث يمكن للأجهزة المحمولة تحديد وقت التغيير ديناميكيًا إستراتيجية جديدة لحماية الهوية تسمى إستراتيجية تغيير المعرف التي يطلقها المستخدم بدلاً في الواجهة الهوائية من خلال تعيين المعرفات وتغييرها بناءً على السياق. يوفر هذا النهج بحثية جديدة تعالج بعض هذه التهديدات. قدمت الورقة حلاً لمسألة تتبع الهوية والموقع التهديدات الهامة لأمن وخصوصية شبكات LTE الممكّنة من HeNB في [44] مع توجيهات استخدام توقيع الوكيل ، مما يجعل النظام أكثر صعوبة في السيناريوهات الحقيقية. تمت مراجعة من التكاليف الحسابية وتكاليف التخزين ويتطلب العديد من التغييرات على البنية الحالية بسبب مثل التنكر لهجمات HeNB و MitM وهجمات DoS. ومع ذلك ، فإنه يتحمل قدرًا كبيرًا التوقيع بالوكالة نيابة عن OAM و CN. يمكن أن يمنع المخطط العديد من هجمات البروتوكول توقيعه الخاص إلى UE. أخيرًا ، يمكن تحقيق المصادقة المتبادلة بين UE و HeNB من خلال توقيع الوكيل إلى HeNB. كما يعيد CN تفويض قدرته على وضع العلامات إلى HeNB ويصدر من خلال إصدار توقيع وكيل لبعضهما البعض. بعد ذلك ، يعيد OAM تفويض قدرته على ، لدى OAM والشبكة الأساسية (CN) اتفاقية تعاقدية بشأن تركيب وتشغيل وإدارة HeNB في الوصول لضمان الاتصال الآمن لـ HeNB من خلال تكييف توقيع الوكيل [43]. بالمخطط HeNB بناءً على قائمة CSG المسموح بها. تم اقتراح آلية قوية للمصادقة المتبادلة والتحكم مع تجهيزات المستعمل ، تحتاج MME إلى التحقق مما إذا كان UE مسموحًا له بالوصول إلى كيانات اشتراك لـ UE في HSS وتقدم إلى MME للتحكم في الوصول. قبل الاستيقان المتبادل هوية CSG بهوية PLMN. يتم تخزين المعلومات الواردة في قائمة CSG المسموح بها UE المسماة بقائمة CSG المسموح بها التي تم الاشتراك فيها. يربط كل إدخال في القائمة من أجل إجراء التحكم في الوصول ، يتعين على CN الاحتفاظ وتحديث قائمة بهويات CSG أ- CN ، HeNB مسؤول بالإضافة إلى ذلك عن أداء التحكم في النفاذ لتجهيزات المستعمل.

مثل مزود خدمة الإنترنت (ISPs) يمكن أن تكون بمثابة حماية فعالة ضد هجمات DoS. LTE. تمت الإشارة إلى أن الحلول التي تعتمد على التعاون بين العديد من الكيانات المشاركة التنقل. بالإضافة إلى ذلك ، تم اقتراح آلية حماية ضد هجمات DoS مع نشر HeNB في بنية استنادًا إلى ملاحظاتهم الخاصة للمناطق المحيطة ، مثل كثافة العقدة وسرعة الجهاز ونمط المُحدِّدات

ام تي سي الأمن .F

تحقيق الاتصال الآمن بين جهازي MTC من خلال إنشاء شبكات مخصصة ضمن تغطية من آلة إلى آلة قائم على الأنظمة الخلوية من الجيل الرابع في [76] ، [77] ، حيث يمكن أن تكون جميع أجهزة MTCD مطلوبة لتجهيز كلا واجهتي الشبكة. تم تقديم نموذج اتصال بالإضافة الى، يتطلب المخطط أن تدعم الأجهزة اتصالات LTE و WiFi ، وهو أمر غير مرجح ذلك ، قد يجلب الكثير من التكاليف الحسابية بسبب استخدام توقيع ECDSA والتوقيع الكلي. ، ولكن يمكنه أيضًا تقليل حركة مرور الإشارات بشكل كبير وبالتالي تجنب ازدحام الشبكة. ومع مصادقة متبادلة واتفاقية رئيسية فقط بين كل MTCD في مجموعة و MME في نفس الوقت لمعلمات اتفاقية المفتاح المختلفة المرسلة من MTCDs الطالبة. لا يمكن للمخطط أن يحقق عبر قائد المجموعة. أخيرًا ، سيتم إنشاء مفتاح جلسة مميز بين كل MTCD و MME وفقًا في MME عن طريق التحقق من توقيع خوارزمية التوقيع الرقمي (ECDSA) من MME تم إنشاؤه بواسطة قائد المجموعة نيابة عن جميع أعضاء المجموعة. ثم تثق كل MTCD وقت واحد ، تقوم MME بمصادقة مجموعة MTC من خلال التحقق من التوقيع المجمع الذي قائد المجموعة. عندما تطلب عدة MTCDs في مجموعة MTC الوصول إلى الشبكة في في [75]. وفقًا للمخطط ، يتم تهيئة عدد كبير من MTCDs لتشكيل مجموعة MTC لاختيار الوصول. تم اقتراح نظام مصادقة جديد للوصول إلى الأجهزة على أساس التوقيع الكلي متعددة إلى SN في وقت واحد لأن كل جهاز لا يزال يتطلب 4 رسائل تشوير لإنجاز مصادقة ، لا تزال هناك بعض المشاكل مثل ازدحام شبكة الإشارات في عقد SN عندما تتنقل أجهزة محليًا دون مشاركة HN. يمكن أن يقلل المخطط من تكلفة الاتصال بين HN و SN. ومع ذلك استيقان كامل. وبالتالي ، عندما يزور أعضاء المجموعة الآخرون ، يمكن لـ SN المصادقة عليهم معلومات المصادقة لوحدة المستعمل والأعضاء الآخرين من HN المعنية عن طريق إجراء ، أن تشكل مجموعة. عندما يتنقل UE الأول في مجموعة إلى SN ، تحصل الشبكة SN على إلى SN في [50]. وفقًا للمخطط ، يمكن لتجهيزات متعددة الاستخدامات ، تنتمي إلى نفس HN الاستيقان والاتفاق على المفاتيح لمجموعة من تجهيزات المستعمل التي تتجول من نفس HN في ذلك المتماثل و التشفير غير المتماثل وفك التشفير مقارنة مع UICC الحالي. تم تقديم نهج أن توفر وظائف محمية أكثر قوة لمصادقة الوصول ودعم العديد من إمكانيات التشفير بما أنه يمكن تضمين بيئة الثقة (TrE) داخل أجهزة MTC لحماية أمان أجهزة MTC ، والتي يمكن تمت مناقشة التهديدات ومتطلبات الأمان والحلول المقابلة لأمن MTC في [74]. يُنصح في [74] في MTC ،

يؤدي إدخال الشبكات المخصصة إلى مزيد من المشكلات الأمنية التي سيكون لها تأثير كبير عليها الأخرى وتغطية شبكة LTE / LTEA لم يتم تناولها في النموذج المقترح. بالإضافة إلى ذلك ، قد حيثما أمكن ذلك. ومع ذلك ، فإن الحالة التي يكون فيها الجهاز في نطاق كل من الأجهزة / LTE. بخلاف ذلك ، فإنه يميل إلى الاتصال بالأجهزة القريبة ، حيث يشكلون شبكة مخصصة تغطية شبكة LTE-A / LTE ولكن بعيدًا عن الأجهزة الأخرى ، فسيستخدم موارد شبكة LTE-A قادرة على التواصل في كل من الوضعين الخلوي والمخصص. إذا كان MTCD موجودًا في أنظمة LTE. من خلال النموذج المقترح ، فإن MTCDs

من تعديلات الشبكة والتحسين لتحقيق أفضل دمج لاتصالات M2M في شبكات LTE-A / LTE. دمج البنية المخصصة في شبكات LTE / LTEA. يتطلب المزيد

السادس. اقلم جاف ر ESEARCH أناSSUES

وفقًا للتحليل أعلاه ، هناك الكثير من مشكلات الأمان لـ الواعدة حول أمان LTE مثل الأعمال المستقبلية المحتملة ، والتي تم وصفها على النحو التالي. قضايا بحث مفتوحة بدون دقة مثالية. في نهاية هذه الورقة ، نقترح بعض التوجيهات البحثية لا تزال شبكات LTE-A / LTE

لأمن MTC. تعد ميزات MTC التالية غير المكتشفة قضايا مهمة لعمل البحث في المستقبل. الأولى من التطوير. لا تزال هناك العديد من القضايا مثل التحديات المفتوحة للتنفيذ العملي للبحث المستقبلي لأمان LTE لأن إدخال MTC في شبكات 3GPP لا يزال في مرحلته (1) سيكون تصميم آليات أمان MTC في شبكات LTE-A / LTE هو العمل الرئيسي

1) آليات الأمان لضمان موثوقية عالية السرعة

للعلاجات المقابلة مسبقًا. إنه السيناريو الذي يتطلب اتصال موثوق عالي السرعة. هكذا، معلومات مباشرة عن الحالة الطبية للمريض إلى المستشفى مما يسمح للأطباء بالاستعداد وخادم تطبيق MTC عبر شبكات 3GPP. في حالات الطوارئ ، يلزم وجود جهاز MTC لتقديم أو ظهور المرض أو حالات الطوارئ ، وإرسال المعلومات التي تم جمعها إلى جهاز MTC عن التغييرات في معلومات الحياة أو الوفاة مثل العلامات الحيوية المرتبطة بالأمراض المزمنة يمكن لأجهزة الاستشعار الحيوية التي يرتديها المريض مراقبة الحالة الصحية للمريض والإبلاغ الصحية ، تتمثل إحدى الخدمات الأساسية في مراقبة المرضى عن بُعد وتوفير الرعاية لهم. مطلوب الاتصال للبيانات الحساسة. في صناعة الرعاية

2) التوازن بين التشفير والصغير

تخفيف النفقات العامة لعمليات التشفير لتحقيق مفاضلة بين وظائف الأمان والنفقات العامة. أكبر من تكلفة إرسال كمية صغيرة من حزم الحمولة. وبالتالي ، تحتاج شبكات LTE إلى تحتوي على ميزات نقل البيانات الصغيرة ، قد تكون تكلفة عمليات التحقق من التشفير والتكامل والحمولات من خلال عمليات التحقق من السلامة. ومع ذلك ، بالنسبة لأجهزة MTC التي المطلوبة. من خلال مخططات أمان LTE الحالية ، يجب تشفير كل من إشارات التحكم كمية نقل المعلومات

3) أنظمة مصادقة الوصول الجديدة للازدحام

لتوصيل الأجهزة الجماعية يمثل مشكلة رئيسية بالنسبة إلى MTC في شبكات LTE-A. الشبكة. لذلك ، لا يزال تصميم مخططات مصادقة وصول فعالة وآمنة قائم على المجموعة يمثل مشكلة رئيسية بالنسبة إلى MTC في شبكات LTE-A. وبالتالي لا يمكن تخفيف عبء تصميم مخططات مصادقة وصول فعالة وآمنة قائم على المجموعة لتوصيل الأجهزة الجماعية بالنسبة إلى MTC في شبكات LTE-A. وبالتالي لا يمكن تخفيف عبء الشبكة. لذلك ، لا يزال وصول فعالة وآمنة قائم على المجموعة لتوصيل الأجهزة الجماعية يمثل مشكلة رئيسية MTC ، وبالتالي لا يمكن تخفيف عبء الشبكة. لذلك ، لا يزال تصميم مخططات مصادقة والتوقيع الكلي ، يتعين على الشبكة إجراء الكثير من العمليات الحسابية لمصادقة مجموعة في نفس الوقت. في [75] ، نظرًا لاعتماد تقنية التشفير العام بما في ذلك توقيع ECDSA ، لا يمكن تجنب ازدحام الشبكة عند عقد SN عندما تتصل العديد من أجهزة MTC بالشبكة لأن كل جهاز لا يزال بحاجة إلى إرسال رسالة طلب مصادقة مستقلة إلى الشبكة بواسطة الحل مصادقة الوصول. ومع ذلك ، لا تزال هناك نقاط ضعف بسبب ميزاتها المتأصلة. في [50] ، نظرًا المخططات الحالية في [50] ، [75] استخدمت نهجًا قائمًا على المجموعة لتبسيط عملية ازدحام الإشارات عندما يتصل عدد كبير من أجهزة MTCD بالشبكة في نفس الوقت الوقت. الشبكة قبل أي اتصال ، فإن مصادقة الوصول الجديدة وخطط اتفاقية المفتاح مطلوبة لتجنب الأمان بينهما. نظرًا لأنه من الأهمية بمكان لمجموعة من MTCDs تنفيذ مصادقة وصول مع الشرطة القائمة على المجموعة والعنونة القائمة على المجموعة دون النظر في مخططات مجموعة MTC. ومع ذلك، لقد عالج فقط قضايا الاتصالات بين أجهزة MTC وخادم MTC مثل الحي ، أو تحمل نفس الميزات أو من نفس مستخدمي MTC. حددت لجنة 3GPP آلية لتشكيل بدلاً من الأجهزة الفردية الفوضوية. يمكن إنشاء مجموعة MTC بواسطة أجهزة متعددة في لتشكيل مجموعة MTC ومن ثم يمكن لشبكة LTE التعامل مع مجموعة MTC بشكل منظم لمستخدمي MTC بشكل خطير. هناك طريقة أخرى تتمثل في إنشاء عدد كبير من أجهزة MTC ، والتي لا يمكن تسليمها في الوقت المناسب بواسطة الشبكة ، وبالتالي ستتأثر جودة الخدمة أخرى. قد تحتوي الاتصالات المرفوضة من جهاز MTC معين على بعض الرسائل المهمة تتمثل في احتمال تعرض حركة مرور غير تابعة لشركة MTC أو حركة مرور من أجهزة MTC ذات الصلة قادرة على رفض طلبات الاتصال أو منعها. ستجلب هذه الطريقة مشكلة جديدة الازدحام ، هناك طريقتان اقترحتهما لجنة]10[3GPP. أولاً ، يجب أن تكون عقد الشبكة MME و HSS للتسبب في حظر الشبكة لتوفير الخدمات لأجهزة MTC هذه. من أجل مكافحة رسائل إلى الشبكة في نفس الوقت ، يمكن تشغيل الحمل الزائد والازدحام على الشبكة في أو في فترات زمنية متزامنة بدقة. في هذه الحالات ، نظرًا لأن عددًا كبيرًا من الأجهزة يرسل من أجهزة القياس أو المراقبة نشطة في نفس الوقت تقريبًا بعد فترة انقطاع التيار الكهربائي العديد من محطات الدفع عبر الهاتف المحمول نشطة في يوم عطلة عامة أو يصبح عددًا كبيرًا ، يجب دعم الكثير من تطبيقات MTC في وقت واحد. على سبيل المثال ، يمكن أن تصبح مطلوب تجنب المصادقة المتزامنة لأجهزة متعددة. في أنظمة 3GPP

4) يلزم وجود آليات تأمين شاملة خاصة بـ MTC.

المخططات الحالية في [76] ، [77] نموذج اتصال M2M من خلال الجمع بين شبكات LTE مع إلى إنشاء آليات آمنة من طرف إلى طرف للاتصالات الآلية (M2M) بين جهازي MTC. صممت الآمن بين أجهزة MTC بدون خادم MTC نموذج اتصال مهيمن. وبالتالي ، تحتاج شبكات LTE في المستقبل ، من المحتمل أن يصبح الاتصال

البروتوكولات والتوصيلات البينية لتحقيق أفضل دمج لاتصالات M2M في شبكات LTE-A / LTE. المزيد من التعديلات والتحسين على الشبكة لمواجهة التهديدات الجديدة في التكامل ولتحسين في بنية التكامل بسبب إدخال البنية المخصصة في شبكات LTE-A / LTE. لذلك ، يلزم إجراء شبكات مخصصة. ومع ذلك ، قد يجلب المزيد من التهديدات الموجودة

5) آليات آمنة لدعم تقييد الحركة و

متطلبات الخدمة للتنقلية المقيدة والتنقل عالي السرعة لأجهزة MTC. في حالة تقييد الحركة ، لأجهزة MTC ذات ميزات التنقل المنخفض في شبكات LTE في [48]. ومع ذلك ، لم يتم وصف الحركة عالية السرعة لأجهزة MTC مطلوبة. تمت مناقشة متطلبات وحلول الخدمة

وبالتالي ، فإن استهلاك الطاقة المنخفض للغاية لأجهزة MTC مطلوب في تصميم آليات الأمان. للطاقة لأنه يكاد يكون من المستحيل استبدال البطارية أو إعادة شحن البطارية لأجهزة MTC. تتبع الحيوانات بواسطة أجهزة MTC في العالم الطبيعي ذات الحركة العالية استهلاكًا منخفضًا MTC في شبكة LTE. في حالة التنقل عالي السرعة ، يتطلب تتبع بعض أجهزة MTC مثل إدارة الأصول وآلية حماية آمنة لمراقبة تغيير موقع أجهزة MTC وتجنب التنقل الخبيث لأجهزة على سبيل المثال ، يجب تصميم نظام مراقبة المبنى مع

من المشكلات التي يجب معالجتها ، والتي تحتاج إلى مزيد من البحث من أجل التحسينات. (2) فيما يتعلق بالجوانب الأخرى لأمان LTE ، لا يزال هناك الكثير

1) في بنية أمان LTE ، المزيد من آليات الأمان-

مثل عدم الكفاءة وعدم التوافق بسبب استخدام التشفير العام مثل توقيع الوكيل و IBC. المتجانسة في شبكات LTE قد تم اقتراحها في [38] ، [51] ، إلا أن هناك بعض نقاط الضعف من أن بعض بروتوكولات مصادقة التسليم بين HeNBs و eNBs وبين أنظمة الوصول غير بين HeNBs و eNBs وعمليات التسليم بين شبكات 3GPP والشبكات غير 3GPP. على الرغم هناك حاجة إلى تصميم معماريات مصادقة تسليم أكثر فاعلية لتحقيق عمليات تسليم سلسة آمنة من هجمات البروتوكول التقليدية والاختراقات المادية في شبكات LTE. بالإضافة إلى ذلك ، يجب تصميم anisms لحماية الاتصالات بين UEs و)HeNB(eNBs و EPC

2) فيما يتعلق بالأمان الخلوي LTE ، فإن مخطط EPS AKA بتنسيق

مصادقة وصول أكثر أمانًا عندما يصل تجهيزات المستعمل إلى EPC عبر شبكات غير 3GPP. الوصول في شبكات LTE بسبب نقاط الضعف الكامنة فيها. علاوة على ذلك ، يلزم تصميم آليات المخططات المحسنة الأخرى في [35] ، [36] ، [58] ، [59] ليست مناسبة لسيناريوهات [55] آلية المفتاح العام لتجنب نقاط الضعف المختلفة ، والتي تجلب الكثير من استهلاك الحساب. الضارة الأخرى مع تحسين أداء المصادقة. اعتمدت معظم الحلول الحالية في [36] ، [51] - مزيد من التعزيز لتكون قادرة على منع الكشف عن هوية المستخدم وهجمات DoS والهجمات تحتاج شبكات LTE إلى

3) على تسليم LTE الأمن ، وإدارة المفاتيح

بما في ذلك هجمات إلغاء التزامن وهجمات الرد. المخطط الحالي في [61] غير مناسب مصادقة التسليم إلى مزيد من التعزيز في شبكات LTE لمنع العديد من هجمات البروتوكول تحتاج آليات وإجراءات

تم قبول هذه المقالة لتضمينها في عدد مقبل من هذه المجلة. المحتوى نهائي كما هو مقدم ، باستثناء ترقيم الصفحات.

قد تجلب لنا بعض الإلهام للتصميم المستقبلي لأنظمة مصادقة التسليم الآمن في شبكات LTE. هذا النهج مصادقة تسليم خفيفة الوزن ويقاوم هجمات DDoS في أنظمة WiMAX ، والتي / HMAC السابق إلى BS الجديدة ، ثم تتحقق BS الجديدة من صلاحيتها. يمكن أن يحقق يتجول UE في محطة BS جديدة ، ترسل بوابة شبكة خدمات الوصول (CMAC (ASN GW المستند إلى التشفير (CMAC) كدليل على أن UE قد تم تسجيله بالفعل في الشبكات. عندما المعلومات المهملة مثل 64 بت العلوي من رمز مصادقة رسالة التجزئة (HMAC) / MAC التي قد تؤدي إلى هجمات DoS الموزعة (DDoS). من خلال النهج ، يمكن استخدام بعض في [15] طريقة مثيرة للاهتمام للتغلب على نقاط الضعف في أنظمة WiMAX المحمولة ومع ذلك ، لا يزال هناك الكثير من القضايا التي تحتاج إلى مزيد من التحقيق. ناقش الاستطلاع 3GPP وشبكات غير 3GPP في [64] ، وعمليات التسليم بين WiMAX و WLAN في [65]. / GSM في [62] ، والتسليم من LTE إلى WLAN في [63] ، عمليات التسليم بين شبكات بين أنظمة الوصول غير المتجانسة ، مثل عمليات التسليم بين WiFi / WiMAX و UMTS بعض بروتوكولات مصادقة التسليم الأخرى في [62] - [65] لبعض سيناريوهات التنقل المحددة التنقل في شبكات LTE بسبب استخدام تقنية التشفير العامة. بالإضافة إلى ذلك ، تم اقتراح سيناريوهات

4) على أمن IMS ، وصول سريع وقوي إلى IMS au-
الاحتيالي لخدمات IMS وهجمات الغش المؤقتة ونقص المصادقات المتبادلة وما إلى ذلك. الأمنية التي لم يتم حلها بواسطة هذه المخططات وتوجد نقاط ضعف مثل الاستخدام من الحلول [40] ، [70] - [72] لتعزيز أمن IMS. ومع ذلك ، لا تزال هناك بعض المشكلات المصادقة ومنع هجمات DoS والهجمات الضارة الأخرى في شبكات LTE. تم اقتراح الكثير يجب تصميم آليات المصادقة لتبسيط عملية

5) فيما يتعلق بأمن HeNB ، بسيط وقوي متبادل-
إلى استهلاك حسابي كبير وغير متوافق مع بنية LTE المحددة بواسطة معيار 3GPP الحالي. هجمات البروتوكول المختلفة. نظرًا لاستخدام توقيع الوكيل ، فإن الحل الحالي في [43] يحتاج يجب تصميم آليات التأشير بين UEs و HeNBs لمنع

سابعا. ج التضمين

المحتملة كاقتراح لأنشطة البحث المستقبلية حول أمان شبكات LTE-A / LTE اللاسلكية. الأمان في شبكات LTE-A / LTE الحالية. أخيرًا ، قمنا بتلخيص مشكلات البحث المفتوحة الأمنية في الأدبيات. اكتشف الاستطلاع الذي أجريناه أنه لا يزال هناك الكثير من مشكلات اللاسلكية LTE-A / LTE وراجعنا الحلول الحديثة المطابقة المقترحة للتغلب على تلك المشاكل معيار 3GPP. لقد ناقشنا بشكل مكثف نقاط الضعف الموجودة في البنية الأمنية للشبكات في شبكات LTE-A 4G / LTE اللاسلكية. لقد قدمنا أولاً بنيات وآليات الأمان التي حددها الوسائط المتعددة الجديدة. في هذه الورقة ، قمنا بإلقاء نظرة عامة على مشكلات الأمان لجنة 3GPP بتحفيز مشروع LTE من أجل تلبية متطلبات زيادة حركة البيانات المتنقلة وتطبيقات قامت

أالمعرفة

يدعم هذا العمل National Basic Research Pro 973-
2012CB316100. وهو مدعوم أيضًا من منحة مؤسسة العلوم الطبيعية الوطنية في الصين غرام من الصين منحة
B08038 وبرنامج علماء Changjiang وفريق البحث المبتكر في الجامعة (PCSIRT 1078). ، وصناديق البحوث الأساسية للجامعات المركزية K50511010001 ، والمشروع الوطني 111 61102056

أ PPENDIX أ
أBBREVIATION

AAA	المصادقة والترخيص و محاسبة
AP	نقطة دخول
AV	ناقل المصادقة
مثل	الوصول إلى الطبقة
سى دى ام ايه	مفتاح تشفير الوصول المتعدد بتقسيم الكود
CK	
CS	الدائرة الكهربية
CSCF	في الخدمة مجموعة المشتركين المغلقة
CSG	الاتصال بوظيفة التحكم
EAP-AKA	بروتوكول المصادقة الموسعة- اتفاقية المصادقة والمفتاح
EAP-AKA '	تحسين EAP-AKA
ECC	منحنى شفرات القطع الناقص
حافة	معدل البيانات المحسن لـ GSM Evolution eNodeB
eNB	
EPC	متطور حزمة الأساسية
ePDG	بوابة البيانات المتطورة
EPS AKA	مصادقة نظام الحزم المتطورة والاتفاقية الرئيسية
E-UTRAN	راديو أرضي عالمي متطور الوصول إلى الشبكة
FN	شبكة أجنبية
جيران	العالم النظام العالمي للاتصالات المتنقلة الرئيسية eNodeB
جي بي آر إس	GSM EDGE خدمة حزمة الراديو العامة الفريدة على مستوى
جوتي	شبكة الوصول اللاسلكي
GSM	
HeNB	
HN	شبكة منزلية
H2H	من إنسان إلى إنسان
IBC	التشفير القائم على الهوية
I-CSCF	استجواب- CSCF
IMPI	الهوية الخاصة لـ IM
IMS	النظام الفرعي للوسائط المتعددة IP
IK	مفتاح النزاهة
IKEv2	المشترك IMS من بروتوكول تبادل مفتاح الإنترنت الإصدار 2
ISIM	وحدة تعريف
KGC	مركز توليد المفتاح

تم قبول هذه المقالة لتضمينها في عدد مقبل من هذه المجلة. المحتوى نهائي كما هو مقدم ، باستثناء ترقيم الصفحات.

LTE / SAE	التطور طويل المدى / هندسة النظام تطور
LTE-A	متقدم LTE
أنا	معدات الجوال
MME	كيان إدارة التنقل
إم تي سي	نوع الجهاز الاتصالات
M2M	آلة إلى آلة
ناس	لا شيء وصول الطبقة
NCC	عداد سلسلة NH
NDS	أمان مجال الشبكة
NGN	شبكة الجيل القادم
نيو هامبشاير	القفزة التالية
P-CSCF	وكلاء- CSCF
غيغاواط PDN	البنية التحتية للمفتاح العام لبوابة شبكة البيانات PKI
ملاحظة	حزمة تبديل
RNC	التحكم في شبكة الراديو
S-CSCF	خدمة- CSCF
SGW	بوابة الخدمة
SeGW	بوابة الأمان
SGSN	خدمة GPRS بروتوكول بدء جلسة دعم العقدة رشفة
SN	خدمة الشبكة
معرف SN	خدمة هوية الشبكة
SQN	رقم التسلسل
تري	الثقة في البيئة
UE	معدات المستخدم
UICC	بطاقة دوائر متكاملة عالمية
UMTS	العالمية للاتصالات المتنقلة نظام المصادقة والمفتاح UMTS-AKA UMTS اتفاق
USIM	وحدة تعريف المشترك العالمية
UTRAN	شبكة الوصول إلى الراديو الأرضي UMTS
VoIP	الصوت عبر بروتوكول الإنترنت
واي ماكس	إمكانية التشغيل البيني في جميع أنحاء العالم لـ الوصول إلى الميكروويف
شبكة WLAN	شبكة الاتصال اللاسلكية المحلية
OAM	التشغيل والإدارة و اعمال صيانة
جودة الخدمة	جودة الخدمة

رالجرأة

[1] S. و ، D. Astely ، E. Dahlman ، A. Furuskar ، Y. Jading ، M. Lindstrom ، Parkvall ، "LTE: The Evolution of Mobile Broadband" ، IEEE Commun. 51-44 ، أبريل 2009 ، ص .ماج ، المجلد 47 ، العدد 4

[2] A. Ghosh، R. Ratasuk، B. Mondal، N. Mangalvedhe، and T. Thomas، "LTE-Advanced: الجيل التالي من تقنية النطاق العريض اللاسلكي" ، IEEE Wireless Commun. ، 22-10 .المجلد 17 ، رقم 3 ، يونيو 2010 ، ص

[3] S. Wetzel و U. Meyer ، "هجوم رجل في الوسط على UMTS" ، ورشة عمل ACM الأمن اللاسلكي .ص 90-97 ، October 2004 ، الثالثة حول

[4] Y. Fang ، "تحليل الأمان وتحسينات مصادقة GPP ، بروتوكول اتفاقية المفتاح IEEE Trans. .الاتصال اللاسلكي ، المجلد 4 ، العدد 2 ، مارس 2005 ، الصفحات 734-742 و M. Zhang

[5] DO Wu و C. Tang ، "مخطط مصادقة متنقلة فعال للشبكات اللاسلكية" ، IEEE Trans. 7 ، العدد 4 ، أبريل الاتصال اللاسلكي ، المجلد 2008 ، ص 1408-1416.

[6] Home Node B و V11.6.0 ، 3GPP TS 22.220 ،)Rel 11(HeNB( ) Home eNode B سبتمبر 2012. مشروع شراكة الجيل الثالث ؛ خدمات مجموعة المواصفات الفنية وجوانب النظام ؛ متطلبات الخدمة لـ)HNB(النظام ؛ متطلبات الخدمة للاتصالات من نوع الماكينة (الإصدار 12) ، V12.0.0 3GPP TS 22.368 سبتمبر 2012.

[7] 3GPP TS 33.401 ، سبتمبر 2012. مشروع شراكة الجيل الثالث ؛ خدمات مجموعة المواصفات الفنية وجوانب وجوانب النظام ؛)SAE(3GPP System Architecture Evolution ؛ معمارية الأمن (الإصدار 12) V12.5.0 مشروع شراكة الجيل الثالث. خدمة مجموعة المواصفات الفنية

[8]

[9] ؛ مزيد من التطورات لجوانب الطبقة المادية E-UTRA (الإصدار 9) ، V9.0.0 3GPP TR 36.814 مارس 2010. الثالث. شبكة النفاذ الراديوي لمجموعة المواصفات التقنية ؛ النفاذ الراديوي العالمي المتطور للأرض (E-UTRA) مشروع شراكة الجيل

[10] النظام ؛ الجوانب الأمنية لاتصالات نوع الماكينة (الإصدار 12) ، V0.10.0 3GPP TR 33.868 ، سبتمبر 2012. مشروع شراكة الجيل الثالث. خدمات مجموعة المواصفات الفنية وجوانب

[11] الفنية وجوانب النظام ؛ أمن H (ه) ملحوظة ؛ (الإصدار 8) ، V8.3.0 3GPP TR 33.820 نوفمبر 2009 مشروع شراكة الجيل الثالث. خدمة مجموعة المواصفات

[12] النظام ؛ دراسة جدوى حول أمان عقدة ترحيل LTE (الإصدار 10) ، V10.0.0 3GPP TR 33.816 مارس 2011. 3GPP TS 33.320 يونيو 2012. مشروع شراكة الجيل الثالث ؛ خدمات مجموعة المواصفات الفنية وجوانب وجوانب النظام ؛ أمان العقدة الرئيسية)HNB(B / العقدة B المطورة منزليًا (HeNB) (الإصدار 11) ، V11.6.0 مشروع شراكة الجيل الثالث. خدمات مجموعة المواصفات الفنية

[13]

[14] IEEE ورش عمل .Y. Park and T. Park، "A Survey of Security Threats on 4G Networks،" Proc. .نوفمبر 2007 ، الصفحات 1-6 ، Globecom

[15] المصادة على 802.16: التحليل والتقييم" ، استطلاعات ودروس اتصالات IEEE ، 2013 ، مطبعة IEEE. كولياس ، ج. كامبوراكيس ، وس. جريتزاليس ، "الهجمات والإجراءات

[16] في أنظمة 3GPP من الجيل التالي: برنامج تعليمي" ، IEEE Commun. ماج ، المجلد 47 ، العدد 2 ، فبراير سي بي سانكاران ، "أمان الوصول إلى الشبكة 2009 ، ص 84-91.

[17] JF Beaumont ، "التطورات الأمنية والتحديات في شبكات 4G ، N. Seddigh ، B. Nandy ، R. Makkar و أغسطس ،)PST(المؤتمر الدولي السنوي الثامن لأمن الخصوصية والثقة .Proc "، اللاسلكية

2010 ، ص 62 - 71.

[18] J. Zheng ، "بحث حول أمن نظام 4G Mobile في شبكة IPv6 "، 2012 ، ص 829-834 ، المجلد. 126 ، .التطورات الحديثة في علوم الكمبيوتر وهندسة المعلومات

[19] ؛ النظام الفرعي للوسائط المتعددة)IMS(IP ؛ (الإصدار 11) ، V11.6.0 3GPP TS 23.228 ، سبتمبر. 2012. مشروع شراكة الجيل الثالث. خدمات مجموعة المواصفات الفنية وجوانب النظام

[20] ؛ متطلبات الخدمة لنظام الحزم المتطور (EPS) (الإصدار 12) ، V12.1.0 3GPP TS 22.278 يونيو 2012. مشروع شراكة الجيل الثالث. خدمات مجموعة المواصفات الفنية وجوانب النظام

[21] 3GPP Evolved Packet عبر شبكات وصول غير 3GPP TS 24.302 V11.4.0 Sep ،)Rel 11(3GPP. الجيل الثالث. الشبكة الأساسية والمحطات الطرفية لمجموعة المواصفات الفنية ؛ الوصول إلى)EPC(Core مشروع شراكة 2012.

[22] ؛ الجوانب الأمنية لعمليات الوصول بخلاف 3GPP TS 33.402 V11.4.0 ،)Rel 11(3GPP ، يونيو 2012. الثالث. خدمة مجموعة المواصفات الفنية وجوانب النظام ؛)SAE(3GPP System Architecture Evolution مشروع شراكة الجيل

[23] العالمي المتطور (E-UTRAN) ؛ وصف العام؛ (الإصدار 11) ، V11.3.0 3GPP TS 36.300 سبتمبر 2012. المواصفات التقنية ؛ النفاذ الراديوي العالمي المتطور للأرض (E-UTRA) وشبكة النفاذ الراديوي الأرضي مشروع شراكة الجيل الثالث. شبكة النفاذ الراديوي لمجموعة

[24] الراديوي الأرضي العالمي المتطور (E-UTRAN) (Rel 11) ، V11.3.0 3GPP TS 23.401 سبتمبر 2012. المواصفات الفنية وجوانب النظام ؛ تحسينات خدمة حزم الراديو العامة (GPRS) للوصول إلى شبكة الوصول مشروع شراكة الجيل الثالث. خدمات مجموعة

[25] ؛ تحسينات معمارية لعمليات الوصول بخلاف 3GPP TS 23.402 V11.4.0 ،)Rel11(3GPP سبتمبر 2012. مشروع شراكة الجيل الثالث. خدمات مجموعة المواصفات الفنية وجوانب النظام

[26] لمجموعة المواصفات الفنية ؛ بروتوكول التحكم في مكالمات الوسائط المتعددة IP القائم على بروتوكول مشروع شراكة الجيل الثالث. الشبكة الأساسية والمحطات الطرفية

تم قبول هذه المقالة لتضمينها في عدد مقبل من هذه المجلة. المحتوى نهائي كما هو مقدم ، باستثناء ترقيم الصفحات.

الجلسة (SIP) وبروتوكول وصف الجلسة (SDP) ؛ (الإصدار 11) ، V11.5.0 3GPP TS 24.229 سبتمبر 2012. بشأن بروتوكول بدء

[27] الوصول للخدمات القائمة على بروتوكول الإنترنت ؛ (الإصدار 12) ، V12.1.0 3GPP TS 33.203 سبتمبر 2012. مشروع شراكة الجيل الثالث. خدمات مجموعة المواصفات الفنية وجوانب النظام ؛ 3G Security ؛ أمن

[28] الندوة الجنوبية الشرقية الحادية والأربعون حول نظرية النظام (SSST 2009) ، مارس 2009 ، ص 94-97. براون ، "خارطة طريق الانتقال الأمني إلى شبكات الجيل الرابع والشبكات اللاسلكية لأجيال المستقبل" ، بروك. محمد الحميجاني ، ود. دن ، ود.

[29] Rel(،)SAE(RAN / 3GPP System Architecture Evolution)LTE(Long Term Evolved) يونيو 2009. المواصفات الفنية وجوانب النظام ؛ الأساس المنطقي وتتبع قرارات الأمان في V9.0.0 3GPP TR 33.821 ، 9 السادس المتقدم للاتصالات (AICT) ، مايو 2010 ، ص 439-444. مشروع شراكة الجيل الثالث. خدمات مجموعة

[30] ، أ. لاسبياي ، ور. فان ، "توفير الأمن في أنظمة الجيل الرابع: كشف النقاب عن التحديات ،" بروك. المؤتمر الدولي م. عياش ، جي ماب

[31] الكمبيوتر ، المجلد. 33 ، رقم 16 ، أكتوبر 2010 ، ص 1907-1915 LTE تحليل إدارة مفتاح" ، D. Forsberg .مع سياق مفاتيح الجلسة" ، اتصالات

[32] "، 3GPP E-UTRAN. الاتصالات اللاسلكية الشخصية والداخلية والمتنقلة (PIMRC) ، سبتمبر 2007 ، ص 1-5. د. فورسبيرج ، إل هوانج ، ك. تسويوشي ، إس. ألانارا ، "تعزيز الأمن والخصوصية في واجهة راديو Proc

[33] توصيل الوصول غير Proc "، 3GPP. الذكاء في شبكات الجيل التالي (ICIN) ، October 2010 ، ص 1-6. ، د. بارانكانيرا ، س. أنطوان ، X. هوانغ ، هـ. دوفوسيل ، "التنقل بين الأنظمة في نظام الحزم المتطور (EPS): ت. أحمد

[34] والاتصالات والتطبيقات .Proc "، E-UTRAN هجوم طلب عدم الوصول إلى الطبقة في" ، W. Wen و D. Yu .يناير 2012 ، ص 48 - 53 ،)ComComAp(مؤتمر الحوسبة

[35] ، Proc. المؤتمر الدولي الثالث لـ IEEE حول برامج وشبكات الاتصال (ICCSN) ، مايو 2011 ، ص 557-563. وأ. صلاحي ، "المصادقة المحسّنة وإجراءات الاتفاقية الرئيسية للجيل القادم من شبكات المحمول المتطورة" إم. بورخياباني

[36] الدولي السابع للاتصالات اللاسلكية والحوسبة المتنقلة .Proc "، LTE مصادقة الكيانات المتبادلة لـ" ، GM Koien .يوليو 2011 ، ص 689-694 ،)IWCMC(المؤتمر

[37] H. Mun، K. Han، and K. Kim، "3G-WLAN Interworking: Security Analysis and New Authentication and Key Agreement Based on EAPAKA." Proc. ،)WTS(ندوة الاتصالات اللاسلكية أبريل 2009 ، ص 1-8.

[38] شبكات eNB و HeNB مصادقة تسليم بسيطة وقوية بين" ، C. Lai و Y. Zhang و M. Ma و H. Li و J. Cao .شبكات الكمبيوتر ، المجلد. 56 ، ع 8 ، مايو 2012 ، ص 2119-2131 "، LTE في

[39] العليا ، جامعة سونجكيونكوان ، 2011 ، "LTE-Advanced هان ، "تحليل الأمان والتحسينات في شبكات CH. http://hit.skku.edu/ hedwig / pds / ، دكتوراه. أطروحة ، قسم هندسة النظم المتنقلة ، كلية الدراسات dissertation.pdf.

[40] الاتصالات الأسترالية .Proc "، مصادقة خضراء وآمنة لشبكة الجوال من الجيل الرابع" ، MA Gregory و L. Gu .نوفمبر 2011 ، الصفحات من 1 إلى 7 ،)ATNAC(مؤتمر شبكات وتطبيقات

[41] المصادقة المتقدمة المستندة إلى" ، S. Gritzalis و G. Kormentzas و A. Rouskas و G. Kambourakis WLAN-3G للعمل البيني الآمن SSL / TLS ." Proc. IEE Communications، Vol.151، No.5، October 2004، pp.501-506.

[42] G. Kambourakis، C. Kolias، S. Gritzalis، and J. Park، "DoS Attacks Exploiting Signaling in UMTS and IMS." Computer Communications، Vol. 34 ، ص 226-235 ، ع 3 ، مارس 2011.

[43] Proc. IEEE ، "أكثر أمانًا مع توقيع وكيل محسّن Femtocell بناء" ، IH Kim و HK Choi و CK Han .الولايات المتحدة الأمريكية ، ديسمبر 2009 ، الصفحات 1-6 ، GLOBECOM 2009

[44] في شبكات الهاتف المحمول من الجيل التالي: LTE و Femtocells" ، ورشة عمل Femtocell ، يونيو 2010. إ. بيلوجريفيتش ، إم جادليوالا وجي بي. Hubaux ، "الأمان والخصوصية

[45] LTE- الاتصال من آلة إلى آلة في" ، W. Wang و Y. Chen أ ، "بروك. مؤتمر تكنولوجيا المركبات الخريف (VTC 2010 - خريف) ، سبتمبر 2010 ، ص 1-4.

[46] و ، N. Iwasaki ، A. Takeuchi ، N. Kato ، MM Fouda ، فضل الله ZM ، أبريل 2011 ، ص IEEE Commun. 60 ، "نحو اتصالات ذكية من آلة إلى آلة في الشبكة الذكية" ، Y. Nozaki -ماج ، المجلد 49 ، العدد 4 .65

[47] Y. Zhang، R. Yu، S. Xie، و W. Yao و Y. Xiao و M. Guizani ، "Home M2M Networks: Architectures، Standards and QoS Improvement." IEEE Commun. 52-44 ، ص 2011 ، أبريل 4 .ماج ، المجلد 49 ، العدد

[48] النظام ؛ تحسينات النظام للاتصالات من نوع الآلة (الإصدار 11) ، V11.0.0 3GPP TR 23.888 ، سبتمبر 2012. مشروع شراكة الجيل الثالث. خدمات مجموعة المواصفات الفنية وجوانب

[49] ، "الثقة في اتصالات IEEE "، M2M فيه. تكنول. ماج. ، المجلد 4 ، العدد 3 ، سبتمبر 2009 ، ص 69-75. تشا ، واي. شاه ، إيه يو شميد ، إيه ليشر ، وام في ميرشتاين

[50] المستندة إلى المجموعة" ، الاتصالات الشخصية اللاسلكية" ، CC Tseng و KH Chi و JT Wang و YW Chen ، اتفاقية المصادقة والمفتاح 2010 ، ص 1-15.

[51] IEEE "، GPP وغير E-UTRAN 3 مصادقة تسليم موحدة بين شبكات الوصول" ، J. Cao ، M. Ma ، and H. Li .الاتصال اللاسلكي ، المجلد. 11 ، ع 10 ، أكتوبر 2012 ، ص 3644-3650 Trans.

[52] Y. Zheng ، D. He ، X. Tang ، و H. Wang ، "AKA and Authorization Scheme for 4G Mobile Networks Based on Trusted Mobile Platform ،" Proc. 980-976 ، ص 2005 ، ومعالجة الإشارات .المؤتمر الدولي الخامس للمعلومات والاتصالات

[53] المستخدم على أساس مفتاح عام معتمد ذاتيًا لشبكة الجيل القادم اللاسلكية" ، Y. Zheng و J. Wang و D. He - أبريل 2008 ، ص 1 ،)ISBAST 2008(القياسات الحيوية وتقنيات الأمن .Proc "، مخطط مصادقة 8.

[54] المتنقلة .Proc "، LTE / SAE المصادقة المحسنة للأمان وبروتوكول اتفاقية المفتاح لشبكة" ، Y. Wang و X. Li .سبتمبر 2011 ، ص 1-4 ،)WiCOM(الاتصالات اللاسلكية والشبكات والحوسبة

[55] JV Franklin and K. Paramasivam ، "3 شبكات في الأمان لتحسين المصادقة المحسن LTE GPP وبروتوكول ICINT 2011(المؤتمر الدولي لتقنية المعلومات والشبكات .Proc "، 2011.

[56] EPS" ، بروك. شبكات النطاق العريض والإنترنت السريع (RELABIRA 2012) ، مايو 2012 ، الصفحات 73-77. ج. عبدو ، وخ. الشاوشي ، وم. عودة ، "تأكيد السرية المضمون وبروتوكول اتفاقية المفتاح لـ

[57] GM Kien ، "Entity Authentication and Personal Privacy in Future Cellular Systems" ، River .أكتوبر 2009 ، Publisher

[58] الاتصالات .Proc "، والمحاكاة LTE نهج الأمان متعدد الطبقات في" ، L. Huang و Z. Gao و Z. Ji و Z. Shi .أغسطس 2009 ، ص 171-173 ،)ASID 2009(مكافحة التزييف والأمن وتحديد الهوية في

[59] C.Vintila، V. Patriciu، and I. Bica، "Security Analysis of LTE Access Network"، Proc. للشبكات ICN(المؤتمر الدولي العاشر 2011) ، يناير 2011 ، ص 29 - 34.

[60] F. Hao و P. Ryan ، "J-PAKE: تبادل المفاتيح المصدق بدون PKI "، Trans. العلوم الحسابية XI، LNCS، Vol. 6480 ، 2010 ، ص 192 - 206.

[61] Y. Zheng، D. He، L. Xu، and X. Tang، "Security Scheme for 4G Wireless Systems،" Proc. .الاتصالات والدوائر والأنظمة ، مايو 2005 ، ص 397-401

[62] والنظام .Proc "، تأمين التجوال والتسليم الرأسي في شبكات الجيل الرابع" ، N. Boudriga و N. Krichene .الصفحات 225-231 ، October 2009 ،)NSS '09(أمن الشبكات

[63] شبكات Proc "، 3GPP LTE. المؤتمر الدولي الثالث للاتصالات والشبكات (ComNet) ، مارس 2012 ، ص 1-6. أ. بو عبيدي ، إ. دالي ، وف. زاري ، "بروتوكول التسليم الآمن في

[64] "، GPP وغير 3GPP الجوانب الأمنية للتنقل بين أنظمة الوصول بين شبكات 3" ، S. Choi و R. Rajavelsamy .برمجيات أنظمة الاتصالات والبرمجيات الوسيطة وورش العمل (كومسوير) ، يناير 2008 ، ص 209 - 213 Proc.

[65] أثناء تسليم GPP إعادة مصادقة سريعة وآمنة لمشتركي 3" ، VCM Leung و AA Al Shidhani .حساب آمن يمكن الاعتماد عليه ، المجلد 8 ، رقم 5 ، سبتمبر-أكتوبر IEEE Trans. "، WiMAX-WLAN 2011 ، ص 699-713.

[66] IEEE J. UMTS "، لمرة واحدة لـ IMS و GPRS إجراء مصادقة" ، L. Wu و M. Hsu و M. Chang و Y. Lin .بلدية المناطق ، المجلد 23 ، العدد 6 ، يونيو 2005 ، الصفحات 1233-1239 Sel.

[67] والفعالة IP مصادقة النظام الفرعي للوسائط المتعددة" ، L. Ping و R. Fan و J. Chen و C. Wu و J. Fu .يونيو 2010 ، ص 139-144 ،)ICNIT(الشبكات وتكنولوجيا المعلومات .Proc "، خفيفة الوزن الفعالة

[68] مصادقة النظام الفرعي متعدد الوسائط عبر بروتوكول الإنترنت المعزز بمرور واحد لـ" ، X. Long and J. Joshi مايو ،)ICC(الاتصالات .Proc "، UMTS بروتوكول 2010 ، ص 1-6.

[69] الاتصال .Proc "، UMTS بمرور واحد في IMS تحسين مصادقة" ، S. Devane و A. Vidhate و G. Sharma .مايو 2011 ، ص 244-248 ،)ICCSN(برامج وشبكات

[70] لاستقلالية المستخدمين في شبكات الجيل التالي" ، I. Stavrakakis و ، C. Xenakis و ، C. Ntantogian المعلومات والحوسبة ، ديسمبر 2007 ، ص 295-300 BioInspired نماذج .Proc "، All-IP المصادقة الفعالة .للشبكات ونظم

[71] الدولي السابع حول التطورات في الحوسبة المتنقلة والوسائط المتعددة (MoMM '09) ، 2009 ، ص 260-266. مصطفى ، و H. A ، "المصادقة القائمة على الهوية للوصول إلى الخدمات المستندة إلى Proc "، IMS. المؤتمر عابد ، سونغ سونغ ، حسن

[72] لشبكات IP 3 آلية مصادقة النظام الفرعي للوسائط المتعددة" ، VCM Leung و MJ Sharma -كوم Proc. "، IG-WLAN المحسنة

تم قبول هذه المقالة لتضمينها في عدد مقبل من هذه المجلة. المحتوى نهائي كما هو مقدم ، باستثناء ترقيم الصفحات.

ورش عمل اتصالات الكمبيوتر (INFOCOM WKSHPS) ، أبريل 2011 ، الصفحات 1000-1005.

[73] فى Femtocell إستراتيجية التحكم فى الوصول فى" ، LB Patanapongpibul مصطفى ، و M. A. Golaup .ماج ، المجلد 47 ، العدد 9 ، سبتمبر 2009 ، ص 117 - 123 .IEEE Commun ، LTE و UMTS"

[74] الأمان المضمّن في تطبيقات شبكة الهواتف المحمولة من آلة إلى آلة" ، Y. Shah و ، I. Cha ، Meyerstein والاتصالات المتنقلة ، المجلد. 17 ، 2009 ، ص 214 - 225 ، "M2M(الجوانب الأمنية للبطاقات الذكية مقابل .الأمان والخصوصية في أنظمة المعلومات

[75] فى شبكات MTC اتفاقية مصادقة ومفتاح قائمة على المجموعة لشركة" ، Hui Li و Maode Ma و Jin Cao LTE" ، Proc. IEEE GLOBECOM
2012 ، ديسمبر 2012 ، تم قبولها للنشر.

[76] M. Saedy و V. Mojtahed ، "Ad Hoc M2M Communications and Security Based on 4G Cellular .أبريل 2011 ، ص 1-5 ،)WTS(ندوة الاتصالات اللاسلكية .System ،"

[77] آلة في الأنظمة الخلوية ،" المجلة الدولية للاتصالات والشبكات متعددة التخصصات" ، V. Mojtahed و M. Saedy .المجلد. 3 ، عدد 2 ، 2011 ، ص 66-75 ،)IJITN(حلول الاتصالات والأمن من آلة إلى

جين كاو ، الصين. اهتماماته في الشبكات اللاسلكية - أمن العمل وشبكات LTE. يعمل حاليًا للحصول على درجة الدكتوراه. شهادة فى التشفير ، جامعة Xidian على بكالوريوس العلوم. درجة من جامعة Xidian ، الصين ، في عام 2008. حصل

هوي لي الرئيسين المشاركين للجنة الفنية في ISPEC 2009 و IAS 2009. ونظرية المعلومات وتشفير الشبكات. وهو مؤلف مشارك لكتابين. شغل منصب ، الصين. تتركز اهتماماته البحثية في مجالات التشفير وأمن الشبكات اللاسلكية 2005 ، كان أستاذًا في كلية هندسة الاتصالات ، جامعة Xidian ، Xi'an Shaanxi حصل على درجات علمية من جامعة Xidian في عامي 1993 و 1998. منذ يونيو على درجة البكالوريوس من جامعة فودان عام 1990 ، ماجستير. ودكتوراه. حصل على بكالوريوس العلوم. حاصل

يويو تشانغ أمن المعلومات وأمن شبكات الاتصالات المتنقلة من الجيل التالي. 2008. وهو أستاذ مشارك في كلية هندسة الاتصالات. يدور بحثه الحالي في مجال ودكتوراه. حصل على درجات علمية من جامعة Xidian في عامي 2005 و حصل على بكالوريوس العلوم. درجة من جامعة Xidian في 2005 ، ماجستير.

مود ما اللاسلكية وأمن الشبكات اللاسلكية والشبكات الضوئية وما إلى ذلك في سنغافورة. لديه اهتمامات بحثية واسعة النطاق بما في ذلك الشبكات أستاذ مشارك في كلية الهندسة الكهربائية والإلكترونية بجامعة نانيانغ التكنولوجية علوم الكمبيوتر من جامعة هونغ كونغ للعلوم والتكنولوجيا في عام 1999. وهو الكمبيوتر من جامعة تيانجين عام 1991 ، ودرجة الدكتوراه. حاصل على درجة في هندسة الكمبيوتر من جامعة تسينغهوا عام 1982 ، ودرجة الماجستير في هندسة حصل على درجة البكالوريوس في

لـ تكنولوجيا المركبات ، مجلة أنظمة الكمبيوتر والشبكات والاتصالات والمجلة الدولية للحوسبة وتكنولوجيا المعلومات. للاتصالات اللاسلكية والحوسبة المتنقلة ، ومجلة تطبيقات الشبكات والكمبيوتر ، وشبكات الأمن والاتصالات ، والمجلة الدولية IEEE ، ومحررًا لاستطلاعات IEEE Communications والدروس التعليمية ، ومحرر مشارك للمجلة الدولية أكاديميًا دوليًا حول الشبكات اللاسلكية والشبكات الضوئية. يعمل حاليًا كمحرر مشارك لـ Communications Letters رئيسًا للمسار الفني ، وكرسيًا تعليميًا ، ورئيسًا للنشر ، ورئيسًا للجلسة لأكثر من 50 مؤتمرًا دوليًا. نشر أكثر من 130 بحثًا عضو اللجنة الفنية للبرنامج لأكثر من 110 مؤتمر دولي. لقد كان