مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (41) العدد (1) 2019
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (41) No. (1) 2019

The new standard authentication protocol is EPS2-AKA

Dr. Ahmad Saker Ahmad*
Amane State**

(Received 17 / 9 / 2018. Accepted 24 / 1 / 2019)

□ ABSTRACT □

Long Term Evolution (LTE) networks are the latest cellular network technologies that provide high-speed mobile services, greater range, better spectrum efficiency, wider coverage and improved security architecture.
3GPP (Third Generation Partner Project) has proposed the Advanced Evolved Packet System Authentication Key Agreement (EPS) to meet the security requirements of the advanced LTE packet system, but this protocol still has some drawbacks in the process Authentication because of vulnerabilities inherited from previous protocols.
In this research, we propose the EPS2-AKA protocol development of the advanced EPS-AKA protocol system to enhance the security level and cover the vulnerabilities at no additional cost by fully hiding the International Mobile Subscriber Identity (IMSI) and testing the proposed protocol using the SPAN (Security Protocol ANIMATOR for AVISPA) Its security level, and compare it with the standard EPS-AKA protocol in terms of load on the network.

Keywords:LTE networks, IMSI ID, EPS-AKA protocol.

* **Professor, Faculty of information technology, Tishreen University, Lattakia, Syria.**
** **Postgraduate Student, Faculty of information technology, Tishreen University, Lattakia, Syria.**

مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (41) العدد (1) 2019
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (41) No. (1) 2019

بروتوكول مصادقة قياسي جديد EPS2-AKA

الدكتور أحمد صقر أحمد*

أماني ستيتي**

(تاريخ الإيداع 17 / 9 / 2018. قُبِل للنشر في 24/ 1 / 2019)

□ ملخّص □

تُعد الشبكات المتطورة طويلة الأمد Long Term Evolution(LTE) أحدث تقنيات الشبكات الخلوية، والتي توفر خدمات عالية السرعة للأجهزة المحمولة، نطاق أكبر ، كفاءة طيف أفضل، تغطية أوسع وبنية أمنية متطورة.

فقد اقترح مشروع شراكة الجيل الثالث 3GPP(Third Generation Partner Project) بروتوكول المصادقة نظام الحزم المتطور واتفاق المفتاح EPS-AKA(Evolved Packet System Authentication Key Agreement) لتحقيق المتطلبات الأمنية لنظام الحزم المتطور في شبكات LTE ، ولكن هذا البروتوكول لايزال لديه بعض العوائق في عملية المصادقة بسبب نقاط الضعف الموروثة من البروتوكولات السابقة.

نقترح في هذا البحث البروتوكول EPS2-AKA تطويراً لبروتوكول نظام الحزم المتطور EPS-AKA لتعزيز مستوى الأمن، وتغطية نقاط الضعف دون تكلفة إضافية عن طريق إخفاء كامل للمعرّف IMSI(International Mobile Subscriber Identity) مع اختبار للبروتوكول المقترح باستخدام الأدة SPAN (Security Protocol ANimator for AVISPA) للتحقق من مستواه الأمني، ومقارنته مع البروتوكول القياسي EPS-AKA من حيث الحمل على الشبكة.

الكلمات المفتاحية: شبكاتLTE ، المعرّف IMSI ، بروتوكول EPS-AKA.

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

** طالبة دكتوراه –قسم النظم والشبكات الحاسوبية – كلية الهندسة المعلوماتية – جامعة تشرين – اللاذقية – سورية

مقدمة:

اقترح مشروع شراكة الجيل الثالث 3GPP، شبكة التطور طويل الأمد LTE باعتبارها التكنولوجيا الواعدة لشبكات الاتصالات المتنقلة، والتي أضافت وظائف جديدة مقارنة مع شبكات الجيل الثالث اللاسلكية وهي [1] :

- نوع جديد من المحطات القاعدية تسمى العقدة المتطورة الأساسية HeNB (Home evolved Node B) وهي نقطة وصول منخفضة الطاقة ،تتوضع ضمن مناطق صغيرة المساحة لزيادة سرعة البيانات وتحسين التغطية الداخلية ورفع إنتاجية الشبكة.
- شبكة النفاذ الراديوي الأرضي العالمي المتطورE-UTRAN(Evolved Universal Terrestrial Radio Access Network) الذي يُحسّن طرائق الاتصال بمعدل بيانات مرتفع، كمون منخفض وعرض نطاق ترددي مرن.
- بروتوكول الإنترنت IP: الذي تم تشغيله في قسم تطوير الحزم الأساسي EPC(Evolved Packet Core)، ويقدم التوافق الكامل مع الشبكات اللاسلكية غير المتجانسة.
- نمط جديد من الاتصالات بين الكيانات والعقد يسمى MTC(Machine Type Communication) وهي قادرة على تبادل البيانات دون تدخل الإنسان ، مثل أجهزة الاستشعار.

تتّبع شبكة LTE السياسات الأمنية الموجودة مسبقاً في 3GPP ، مع إضافة تحسينات جديدة لزيادة الأمن ولتكون الشبكة أكثر موثوقية.مع العلم أنه تم تحقيق حماية الرسائل المتبادلة بين كيانات الشبكة من خلال بروتوكول IPsec.

ولكن على الرغم من الميزات الأمنية الموجودة في شبكات LTE إلا أن بروتوكول المصادقة EPS–AKA يرث بعض العيوب الأمنية من بروتوكول UMTS مثل اصطياد IMSI ، هجوم منع الخدمة (DOS) وهجوم الرجل في المنتصف .نقترح في هذا البحث تحسين للبروتوكول القياسي EPS–AKA وتغطية نقاط الضعف السابقة.

أهمية البحث وأهدافه:

يهدف البحث إلى تطوير بروتوكول المصادقة القياسي EPS–AKA في شبكات LTE، ليصبح اكثر أمناً ويغطي نقاط الضعف الموروثة من بروتوكولات المصادقة السابقة، وأهمها اصطياد هوية المشترك IMSI ، العقد الوهمية و هجوم الرجل في المنتصف .

تأتي أهمية البحث من أهمية ودور الشبكات الخلوية في حياتنا اليومية، كتحويل الأموال وغيرها من الخدمات المصرفية ودفع الفواتير والبيع والشراء عن طريق الإنترنت، ولكن لايمكن لهذه الشبكات تحقيق المرجو منها إلا بكسب وثوقية المشترك من خلال التأكد من المستوى الأمني لها وعدم وجود خروقات أمنية تهدد خصوصية وأمن المشترك.

طرائق البحث ومواده:

سنقدم في هذه البحث شرحاً عن آلية عمل بروتوكول المصادقة EPS–AKA و تحديد نقاط الضعف التي يعاني منها.ومن ثمة اقتراح البروتوكول EPS2–AKA كبروتوكول مطوّر عن البروتوكول القياسي، يلبي جميع الاحتياجات الأمنية ويغطي نقاط الضعف الموجودة في البروتوكول القياسي، والتحقق من ذلك باستخدام الأداة SPAN . وتمت مقارنة الحمل على مستوى الشبكة بين البروتوكول القياسي والبروتوكول المقترح في حالتي المصادقة الأولية وعمليات المصادقة اللاحقة.

1-البنية الأمنية لشبكات LTE:

يوجد خمس مستويات أمنية حددتها لجنة 3GPP [2]:

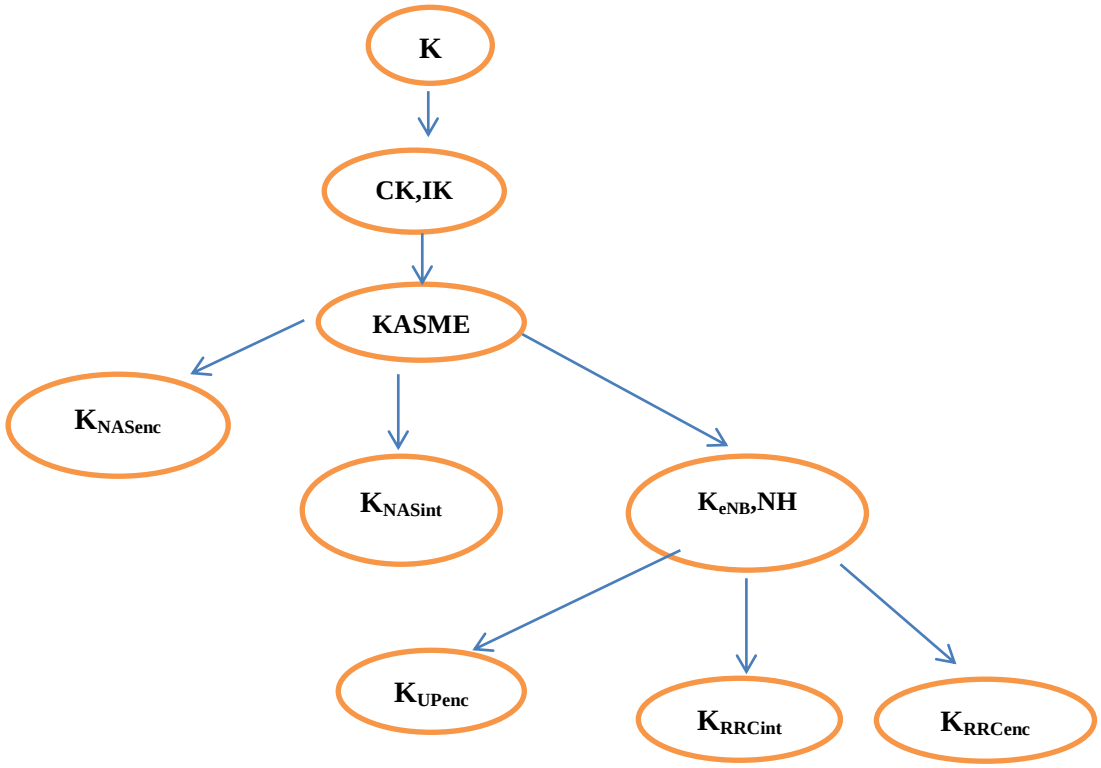
1. أمن الوصول إلى الشبكة: توفر الوصول الآمن إلى الشبكة، والحماية من الهجمات المحتملة على الوصلة الراديوية .
2. أمن مجال الشبكة: توفر مجموعة من الميزات الأمنية للحماية من الهجوم المحتمل على شبكة الخطوط السلكية وتُمكّن من تبادل البيانات بطريقة آمنة.
3. أمن مجال المستخدم: يتم اعتماد المصادقة المتبادلة بين جهاز الموبايل و الشريحة باستخدام رقم التعريف الشخصي السري PIN(Personal Identification Number).
4. أمن مجال التطبيقات : توفر مجموعة من الميزات الأمنية التي تمكن من تبادل البيانات بين التطبيقات لدى المستخدم و مزود الخدمة بشكل آمن.

2-هرمية توليد المفاتيح في بروتوكول EPS [3]:

في بروتوكول المصادقة EPS يتم اشتقاق كافة المفاتيح اللازمة من المفتاح الوسيط KASME (Key Access Security Management Entity) الذي يعد مفتاحاً رئيسياً محلياً للمشترك على عكس المفتاح الدائمK، يُخزن في كيان إدرة التنقل MME (Mobile Management Entity) بينما يتم تخزين المفتاح الدائم K في مركز المصادقة AUC(Authentication Center).

يحتوي التسلسل الهرمي على جذر واحد وهو المفتاح الدائم K وتليها مجموعة من المفاتيح كما في الشكل(1):

- جذر التسلسل الهرمي المفتاح الرئيسي K: وهو سلسلة بتات عشوائية خاصة بالمشترك مخزنة في الشريحة و مركز المصادقة.
- مفتاحي التشفير والسلامة CK(Ciphering Key) و IK(Integrity Key) : مشتقين من المفتاح K .
- المفتاح KASME : مشتق من المفتاحين CK وIK وهو يعمل كمفتاح أساسي محلي.
- المفتاح K_{eNB} : مشتق من المفتاحKASME يستخدم بين تجهيز المشتركUE (User Equipment) والعقدة eNB.
- المفتاح NH : مفتاح وسيط آخر مشق من KASME يستخدم في حالات التسليم Handover.
- المفاتيح K_{RRCENC}، K_{RRCINT} ، K_{UPENC} تستخدم من أجل التشفير والسلامة لمركز مراقبة الموارد الراديوية RRC(Radio Resource Control) وتجهيز المستخدم UE.
- المفتاحين K_{NASenc} و K_{NASint} يستخدامان من أجل التشفير والسلامة لحركات المرور في طبقة عدم الوصول.



الشكل(1) هرمية توليد المفاتيح في بروتوكول EPS–AKA

3- بروتوكول EPS-AKA

لابد من التعرف على المفاهيم الأساسية في المصادقة قبل البدء بشرح آلية عمل البروتوكول[4,5]:

1. هوية المستخدم:

تستخدم LTE نفس المعرّف الخاص بتحديد هوية المُستخدِم المُستخدَم في الشبكات السابقة وهوIMSI، ويتكون من ثلاثة أجزاء:

رمز البلد:MMC (Mobile Country Code).

رمز شبكة الجوال: MNC (Mobile Network Code).

رقم يعرّف المستخدم بشكل فريد: MSIN (Mobile Subscriber Identification Number).

2. سرية هوية المستخدم :

يحمي بروتوكول EPS سرية هوية المستخدم ضد الهجمات بنفس الطريقة التي تتبعها أنظمة GSM و UMTS ،حيث يتم تعيين هوية مؤقتة وتسمى GUTI(Globally Unique Temporary UE Identity) تختلف قليلاً عن TMSI(Temporary Mobile Subscriber Identity) المستخدمة في GSM و UMTS ويتم تخصيصها من قبل MME [6].

تتكون GUTI من عنصرين:

GUMMEI: يُعرّف الـ MME التي خصصت GUTI ويتكون من MNC، MCC، MMEid.

M-TMSI: يُعرّف تجهيز المستخدم ضمن MME التي خصصت GUTI.

3-1-آلية عمل بروتوكول EPS [7]:

تتم وفق الإجرائيتين الآتيتين:

- توليد أشعة المصادقة في الشبكة الرئيسية HSS(Home Subscribe Server).
- تحقيق المصادقة المتبادلة بين UE و MME.

توليد أشعة المصادقة:

وتتم وفق مايلي:

- تستدعي MME الإجرائية عن طريق طلب أشعة المصادقة من HSS ويتضمن الطلب المعرّف IMSI و هوية شبكة التخديم SNID التي سيتم استخدامها من أجل توليد المفتاح المحلي KASME.
- عند استلام الطلب يقوم HSS بتوليد أشعة المصادقة AV[1….n] ووضعها في مصفوفة مرتبة وإرسالها إلى MME .

وهنا نناقش حالتين :

1. اذا كان n>1 يتم توجيه أشعة المصادقة استناداً إلى الرقم التسلسلي.
2. توصي TS33.401[8] أن يكون n=1 بحيث يتم إرسال ناقل واحد للمصادقة في كل مرة يتم طلب المصادقة لأن الحاجة إلى الاتصال المتكرر مع HSS من أجل الحصول على أشعة المصادقة الجديدة تم تخفيضها في EPS من خلال استخدام المفتاح الرئيسي المحلي KASME، وهو غير مكشوف أو معرض للخطر مثل CK و IK في شبكات UMTS، بالنتيجة لايحتاج إلى التجديد في كثير من الأحيان. استناداً إلى المفتاح الرئيسي المحلي والمفاتيح المشتقة منه لم نعد بحاجة لاستخدام أشعة مصادقة محسوبة مسبقاً عندما ينتقل المستخدم إلى شبكة تخديم مختلفة لارتباط المفتاح KASME مع هوية شبكة التخديم.

يتكون شعاع المصادقة في UMTS من البارامترات الآتية:

- رقم عشوائي RAND.
- الاستجابة المتوقعة XRES(Expected Response).
- المفتاحان : مفتاح التشفير CK(Ciphering Key) و مفتاح السلامة IK(Integrity Key).
- رمز التوثيقAUTN(Authentication Token)

بينما يتكون شعاع المصادقة في LTE من البارامترات الآتية:

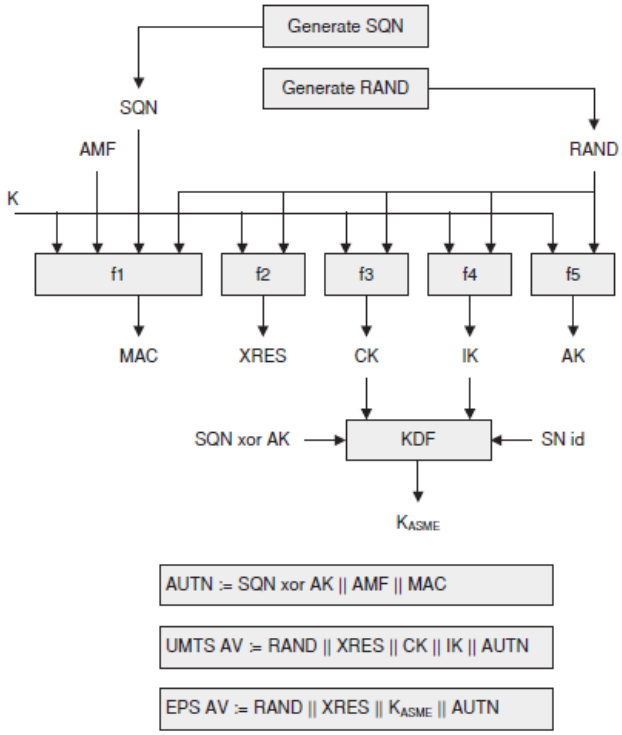
- رقم عشوائي RAND.
- الاستجابة المتوقعة XRES(Expected Response).
- المفتاح KASME(Key Access Security Management Entity).
- رمز التوثيقAUTN(Authentication Token).
- يبدأ AUC بتوليد رقم عشوائي RAND و رقم تسلسلي SQN ، مع العلم أنه يحتفظ كلاً من HSS و UE بالترابط بين SQN_{HE}(رقم تسلسلي يُخصّص لكل مستخدم في HSS) و SQN_{MS} (وهو أعلى رقم تسلسلي تم قبوله فيUE)، ويتم اخفاؤه باستخدام مفتاح إخفاء الهوية AK(Anonymity Key).

يتم حساب البارامترات الآتية كما هو موضح بالشكل(2)[9] :

- MAC=$f1_K$(SQN\\RAND\\AMF).
- XRES=$f2_K$(RAND).
- CK=$f3_k$(RAND).
- IK=$f4_k$(RAND).
- AK=$f5_k$(RAND).
- AUTN(SQN xor AK\\AMF\\MAC)

الخطوة الجديدة المختلفة عن شبكاتUMTS هو اشتقاق المفتاح KASME باستخدام تابع اشتقاق المفتاح KDF (Key Derivation Function) ويمكن بذلك الاستغناء عن المفتاحين CK و IK .

- KASME=KDF(SQN xor AK\\CK\\IK\\SNid)



الشكل(2) توليد أشعة المصادقة لبروتوكول UMTS وEPS

3-2-المصادقة المتبادلة بين MME وUE:

الهدف من هذا الإجراء هو:

- مصادقة المستخدم.
- إنشاء مفتاح رئيسي محلي بين MME و UE .
- التحقق من حداثة شعاع المصادقة.
- مصادقة الشبكة الرئيسية من قبل UE.

ويتم ذلك وفق الخطوات الآتية:

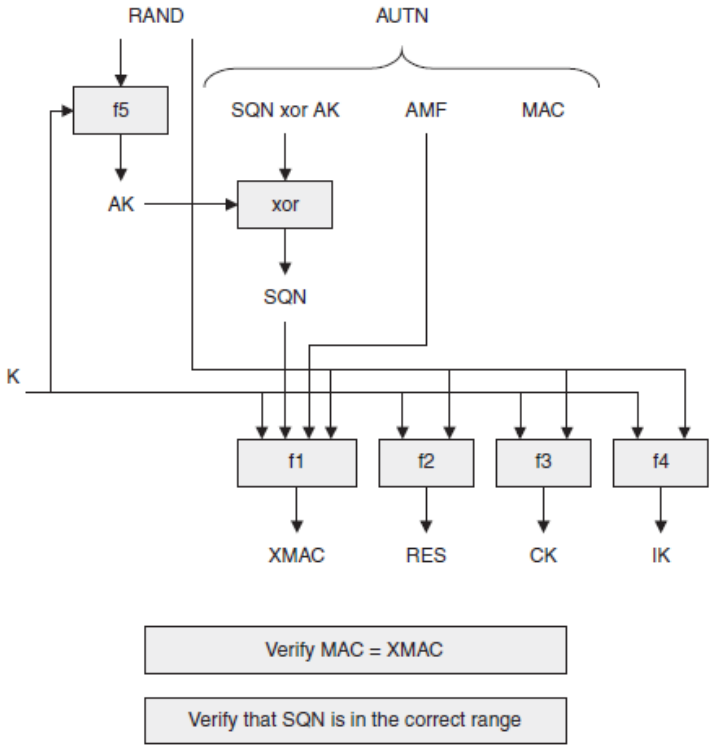
- تستدعي MME الإجرائية عن طريق تحديد شعاع المصادقة غير المستخدم التالي من مصفوفة الأشعة الموجودة في قاعدة بيانات MME، اذا لم يتواجد أي شعاع مصادقة تقوم بالطلب من HSS.

- ترسل MME البارامترين (RAND,AUTN) إلى UE.
- عند استلام UE للبارامترين السابقين يقوم بالعمليات الآتية:

- حساب قيمة المفتاح AK .
- استخلاص قيمة SQN .
- حساب قيمة XMAC .
- التحقق فيما إذا كان XMAC=MAC.
- التحقق من أن قيمة SQN ضمن المجال الصحيح.

بعد التحقق من الشرطين السابقين تتم مصادقة المستخدم للشبكة ويحسب قيمة RES ويرسلها إلى MME

- يقارن MME قيمة RES القادمة من UE مع قيمة XRES الموجودة في شعاع المصادقة في حال المطابقة تحصل المصادقة للمستخدم كما في الشكل(3).



الشكل(3) التحقق من المصادقة في شريحة المستخدم

3-3-أسباب فشل المصادقة:

I. فشل المطابقة بين MAC وXMAC.
II. فشل التزامن إذا كان الرقم التسلسلي ليس ضمن المجال الصحيح.
III. فشل المطابقة بين RES وXRES .

3-4-نقاط ضعف البروتوكول EPS-AKA:

❖ تفتقر آلية عمل البروتوكول EPS-AKA إلى حماية الخصوصية في الحالات التي يتم بها الإفصاح عن المعرّف IMSI وذلك عند التسجيل للمرة الأولى على الشبكة، ،في حال فقدان الترابط بين IMSI و GUTI وعندما

ينتقل إلى MME جديدة وليس لها اتصال مع MME القديمة، الأمر إلى يؤدي إلى مشاكل أمنية متعددة بمجرد التقاط IMSI من خلال العبث بالمعلومات الشخصية و تتبع لموقع المشترك .

❖ لايمكن لبروتوكول EPS منع حجب الخدمة DOS، والسبب بذلك أن MME تقوم بتوجيه طلب UE إلى HSS قبل أن يتم المصادقة عليه بواسطة MME ، ولا يمكن لـ MME مصادقته إلا بعد استلام البارمتر RES، بالنتيجة يمكن تنفيذ DOS (حجب الخدمة) بين HSS و MME .حيث يقوم المهاجم بإرسال معرّف IMSI مزيف باستمرار حتى ينهك المخدم HSS بسبب استهلاكه طاقة حسابية كبيرة لتوليد أشعة المصادقة ،وأيضاً تستهلك MME ذاكرتها لتخزين الأشعة المولدة حتى تنتظر الرد بالاستجابة من قبل UE.

❖ يتجاهل حماية هوية شبكة التخديم SNID سواء على الواجهة اللاسلكية أو السلكية حيث يتم تبادلها بشكل صريح والذي يُمكَن المهاجم من التنصت على SNID تشكيل عقدة وهمية والاحتيال على الشبكة.

❖ إمكانية تحقيق محطة قاعدية BTS وهمية لأن MS هو من يقوم باختيار العقدة للتواصل معها ممايسبب تحقيق هجوم الخلط (Mix Up Attack)[10].

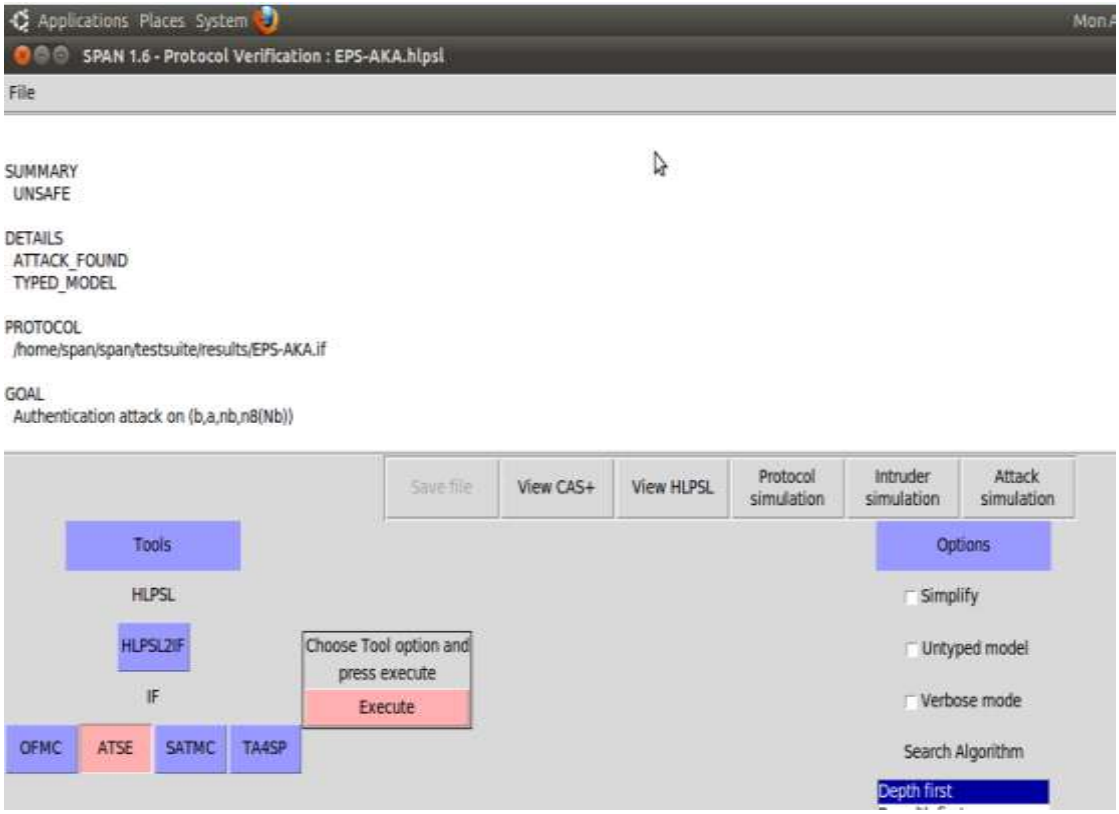
3-5-التحليل الأمني لبروتوكول EPS-AKA:

يتم الهجوم في بروتوكول EPS-AKA على مستويين:

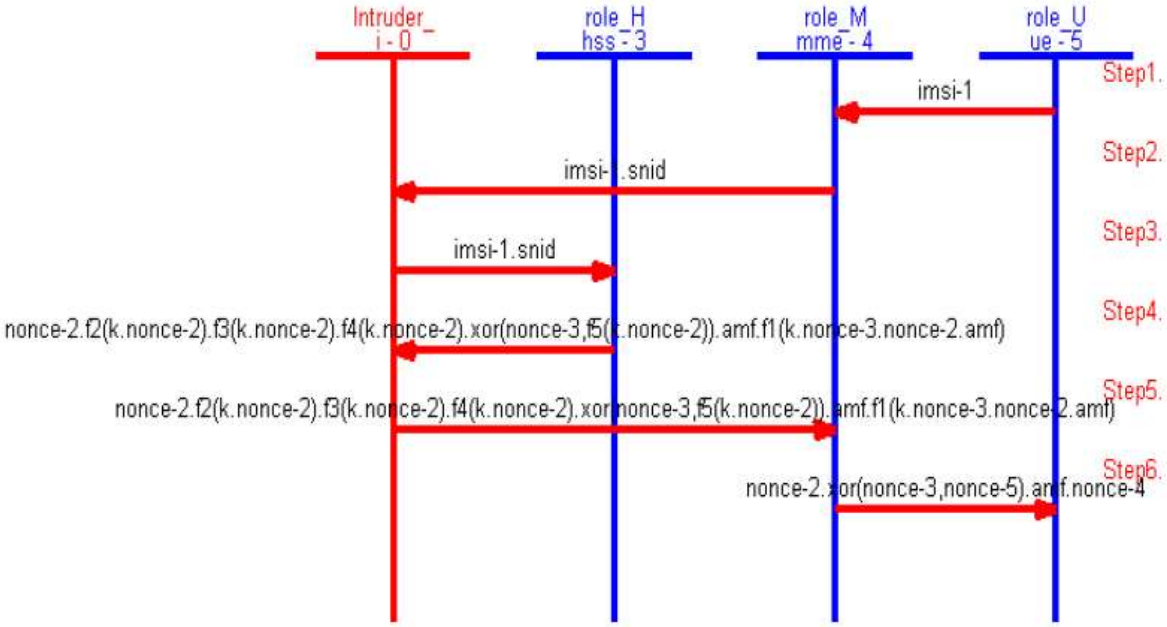
1. الهجوم السلبي (Passive Attack) : باصطياد المعّرف IMSI وخصوصاً في مواقع محددة مثل المطار و المشفى وغيرها.
2. الهجوم الفعال (Active Attack) : بتفعيل محطة قاعدية وهمية BTS للحصول على جميع المراسلات التي تتم بين المشترك والشبكة الرئيسية.

النمط الاول لا يحتاج إلى تجهيزات كثيرة ولكن فعاليته قليلة ،أمّا بالنسبة للنمط الثاني يتطلب استغلال أمن النقل بين HN و SN ,هو مكلف ولكن فعاليته عالية وخصوصاً إذا تمكّنت العقدة الوهمية من الحصول على المفتاح الخاص بالشبكة والحصول على ثقة الشبكة الرئيسية.

يبين الشكلين (4) و (5) سيناريو الهجوم على المستوى الثاني باستخدام الأداة SPAN المقترح من AVISPA[11,12].



الشكل(4) اختبار البروتوكول EPS–AKA باستخدام SPAN



الشكل(5) سيناريو الهجوم على بروتوكول EPS–AKA

يتم هذا الهجوم وفق الآتي حيث المتطفل (Intruder) يشكل محطة وهمية:

1. يتمكن المتطفل من الحصول على المعرَف المرسل من شبكة التخديم إلى الشبكة الرئيسية
2. يرسل المتطفل المعرّف إلى الشبكة الرئيسية.
3. ترسل الشبكة الرئيسية معلومات أشعة المصادقة إلى المتطفل عوضاً عن شبكة التخديم(MME).

4. يقوم المتطفل بإرسال المعلومات إلى شبكة التخديم التي بدورها ترسلها إلى المشترك.

هكذا تمكنت العقدة الوهمية من الحصول على جميع المعلومات الخاصة بالمشترك والتي يترتب عليها أمور عدة.

4-البروتوكول المقترح EPS2-AKA:

يقدم هذا البروتوكول تحسين للمستوى الأمني لبروتوكول EPS-AKA ودون تكلفة إضافية، وهو مشابه للبروتوكول القياسي من حيث أن كل خطوات المصادقة تُدار من قبل MME والذي له الإيجابيات الآتية:

- تخفيف العبء على الشبكة الرئيسية والضغط على المخدمات.
- سرعة المصادقة

يميز هذا البروتوكول بين أمرين:

1. المصادقة الأولية .
2. المصادقات اللاحقة.

4-1-المصادقة الأولية:

4-1-1-عمليات التهيئة:

- يولّد كلا" من UE وMME رقم فريد(TRID) وهو المعرّف الخاص بالمسار (Track Identity)، والذي يُستخدم ليحدد المسار الواصل بين UE و MME مروراً بالعقدة eNB ،ويتكون من المعرّف الخاص بـMME والمعرّف الخاص بـeNB :

$$(TRID=MMEID \oplus eNBID)$$

- توليد المعرّف الخاص بالمصادقة (Authentication Identity) وهي قيمة يتم تغييرها من قبل HSS في كل عملية تهيئة لمصادقة جديدة بالاعتماد على التابع RF، ويتم تشفيرها وفك تشفيرها باستخدام التابع الأمني f10:

$$AUTHID=f_{10}(K,IMSI)$$

- توليد الرقم العشوائي RAND :

$$RAND= f0()$$

- توليد مفتاح خاص بالمصادقة (Authentication Key) باستخدام الدالة KDF وهو معروف فقط من قبل HSS وUE.

$$AUTHK=KDF(IMSI,AUTHID)$$

4-1-2-آلية عمل البروتوكولEPS2-AKA:

الخطوة الاولى:

- يقوم جهاز المشترك UE بحساب البارامترات الآتية:
  - $TRID=MMEID \oplus eNBID$
  - $AUTHID=f_{10}(K,IMSI)$
  - $RAND=f_0()$
  - $AUTHK=KDF(IMSI,AUTHID)$
  - $MAC_U=f_1(AUTHK,IMSI,TRID,RAND)$
- يشفرUE القيمة RAND باستخدام التابع f6 كالتالي:
  - $XRAND=f_6(AUTHK,RAND)$
- يرسل UE رسالة طلب الاتصال A إلى MME والتي تتضمن:

$$A=\{AUTHID,XRAND,MAC\}$$

الخطوة الثانية:

- عند وصول الطلب إلى MME يستطيع أن يحدد المعرّف eNBID،ويحسب البارمتر(TRID)، هكذا فإن الـ HSS يستطيع مقارنة قيمة TRID الواردة من UE مع قيمة TRID الواردة من MME ليتم بذلك المصادقة على MME والكشف عن العقد الوهمية
- يمرر MME رسالة طلب الاتصال B إلى HSS ويلحق بها TRID:

B={A},TRID

الخطوة الثالثة:

- عند وصول الطلب إلى HSS يقوم باستخلاص القيمين (K،IMSI) من خلال البارامترات الواردة في طلب الاتصال وفق الخوارزمية التالية كما هو مبين بالشكل(6).
- يقوم HSS بحساب البارامتر AUTHK.
- فك تشفير XRAND باستخدام التابع *f6:

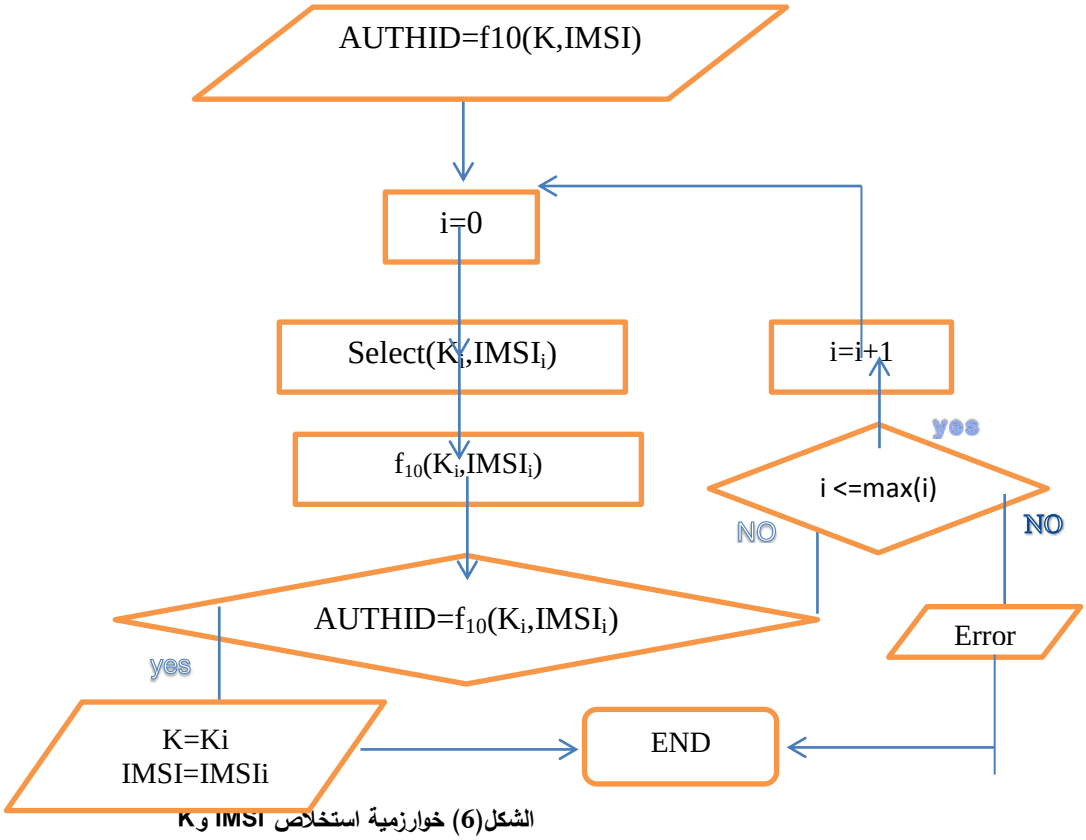
❖ $RAND=f_6^*(AUTHK,XRAND)$

- يحسب قيمة X-MAC ويقارنها مع قيمة MAC الممرة من MME في حال المطابقة تتم المصادقة على المشترك من قبل الشبكة، في هذه الحالة يتم التحقق من البارمترات IMSI ،eNBID،MMEID و RAND بشكل غير مباشر عند مطابقة MAC.
- يولد أشعة المصادقة ويعين رقم تسلسلي(SQN) من أجل كل شعاع مصادقة ويشفرها باستخدام التابع f_7:

❖ $XSQN=f_7(AUTHK,SQN)$

- يحسب البارامترات الآتية:

❖ MACH=f1(AUTHK,SQN,RAND)
❖ RES=f2(AUTHK,RAND)
❖ CK=f3(AUTHK,RAND)
❖ IK=f4(AUTHK,RAND)
❖ AK=f5(AUTHK,RAND)
❖ KASME=KDF(SQN,TRID,CK,IK)



الشكل(6) خوارزمية استخلاص IMSI و K

- يتكون كل شعاع مصادقة من البارامترات الآتية:

RES، KASME، AUTHID (يتم اخفاؤه باستخدام المفتاح AK) وAUTN (يتكون من XSQN و MAC-H).

- يغير من قيمة AUTHID باستخدام RF للحصول على قيمة جديدة NAUTHID.
- يحسب قيمة XAUTHID

❖ $XAUTHID=f_8(AUTHK,NAUTHID)$

- يرسل HSS رسالة الإجابة على طلب المصادقة C مع XAUTHID إلى MME.

$C=\{RES,KASME,AUTHID_{AK},AUTN\},XAUTHID$

الخطوة الرابعة:

- ترسل MME أول شعاع مصادقة يحوي AUTN و XAUTHID إلى UE من خلال eNB.

الخطوة الخامسة:

- يفك UE تشفير SQN من خلال f7* و ويحسب قيمة MAC_H
- للتحقق من حداثة شعاع المصادقة يفحص SQN و XMAC-H
- إذا لم يكن SQN ضمن المجال الصحيح أو لم تكن قيمة MAC_H التي تم حسابها مطابقة لقيمة MAC_H الواردة من MME يتم رفض رسالة المصادقة.
- بعد عملية المصادقة يقوم UE بفك شيفرة XAUTHID باستخدام f8* وخزينها من أجل عمليات التهيئة اللاحقة وتوليد المفاتيح CK، IK و KASME.

4-2-عمليات المصادقة اللاحقة:

تتم عمليات المصادقة اللاحقة بين UE و MME دون العودة لطلب أشعة المصادقة من HSS.

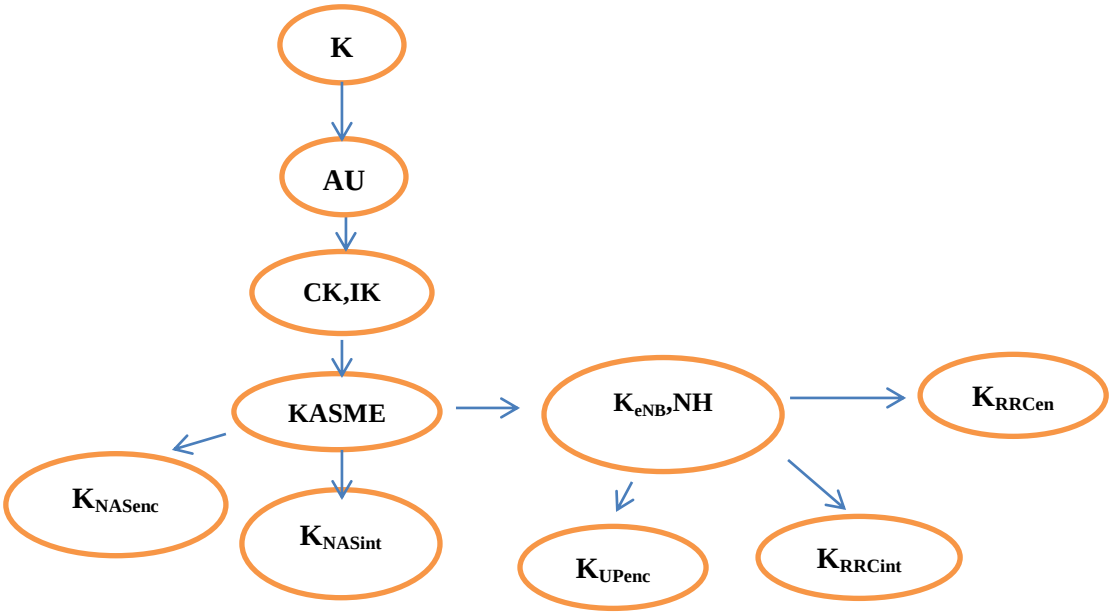
تتم المصادقة اللاحقة وفق مما يلي:

- يحسب UE قيمة XRES ويرسل طلب الاتصال إلى MME والذي يحوي AUTHID و XRES.
- عند وصول الطلب يتحقق MME من البارامتر XRES إذا كانت القيمة مطابقة يرسل AUTN إلى UE وإلا يرفض الطلب.
- يقوم UE بفك تشفير SQN وحساب MAC_H للتحقق من سلامة وحداثة شعاع المصادقة ليحسب بعد ذلك المفاتيح CK،IK، KASME.

4-3-هرمية توليد المفاتيح في بروتوكول EPS2:

تبقى هرمية توليد المفتاتيح مشابهة لبروتوكولEPS، باستثناء توليد مفتاح جديد AUTHK بالاعتماد على المفتاح الأساسي K الشكل(7). فمن أجل التقليل من مخاطر الحصول على المفتاح الاساسي لا يتم الاعتماد بشكل كامل عليه لتوليد المفاتيح الباقية وبدلاً من ذلك يتم استخدام المفتاح AUTHK وتغييره مع كل عملية تهيئة لمصادقة جديدة.

يجدد البروتوكول المقترح المفاتيح كلها من الأعلى إلى الأسفل من أجل كل عملية تهيئة لمصادقة جديدة ، وإذا اختُرِقَ مفتاح من المستوى الأدنى هذا لا يعني أنه سيتم الكشف عن باقي المفاتيح في المستويات الأعلى.



الشكل(7) هرمية توليد المفاتيح في بروتوكول EPS2-AKA

النتائج والمناقشة:

1- التحليل الأمني لبروتوكول EPS2-AKA:

يوجد ثلاث مستويات للمصادقة:

1. مصادقة HSS لـ UE عن طريق المطابقة بين XMAC-U و MAC-U.
2. مصادقة MME لـ UE عن طريق المطابقة بين RES=XRES.

3. مصادقة UE لـ MME عن طريق المطابقة بين MAC-H و XMAC-H.

مع التنويه على أن المصادقة تعتمد على حداثة ودقة البارامترات المدخلة إلى التوابع، لذلك عند نجاح عملية المصادقة يتم ضمنياً التحقق من البارامترات المدخلة للتوابع الأمنية .

3. حماية هوية المشترك IMSI والمفتاح الرئيسي K:

- في البروتوكول المقترح تم اخفاء هوية المشترك IMSI بالكامل باستخدام AUTHID ،ومن ثم يعاد تخصيص معرّف جديد من أجل عمليات المصادقة اللاحقة بذلك تم الاستغناء بالكامل عن استخدام IMSI من أجل تحقيق المصادقة وهذا حل لمشكلة اصطياد المعرّف أو إرساله بشكل صريح كما هو الحال في بروتوكول EPS.

- تم الاعتماد في البروتوكول المقترح على المفتاح K لإنشاء المفتاح AUTHK فقط، والذي يُستخدم بدوره لإنشاء المفتاح KASME الذي تُشتق منه باقي المفاتيح .والمفتاح AUTHK يتم تجديده بشكل دوري بكل عملية تهيئة للمصادقة، لذلك من الصعب اختراق المفتاح K عن طريق AUTHK. أما في البروتوكول EPS فإن كل المفاتيح تعتمد على المفتاح K لذلك فإنّ اختراقه يمكن للمهاجم إنشاء مفاتيح النظام بأكمله.

4. **الكشف عن العقد الوهمية:**

في بروتوكول EPS يمكن للمهاجم أن يحاكي العقدة eNB أو أن ينتحل شخصية UE لأن البارامتر SNID يتم تسليمه إلى HSS من MME فقط هكذا يمكن للمهاجم تشكيل عقدة وهمية والاتصال بالشبكة الرئيسية دون إمكانية الكشف عنها.

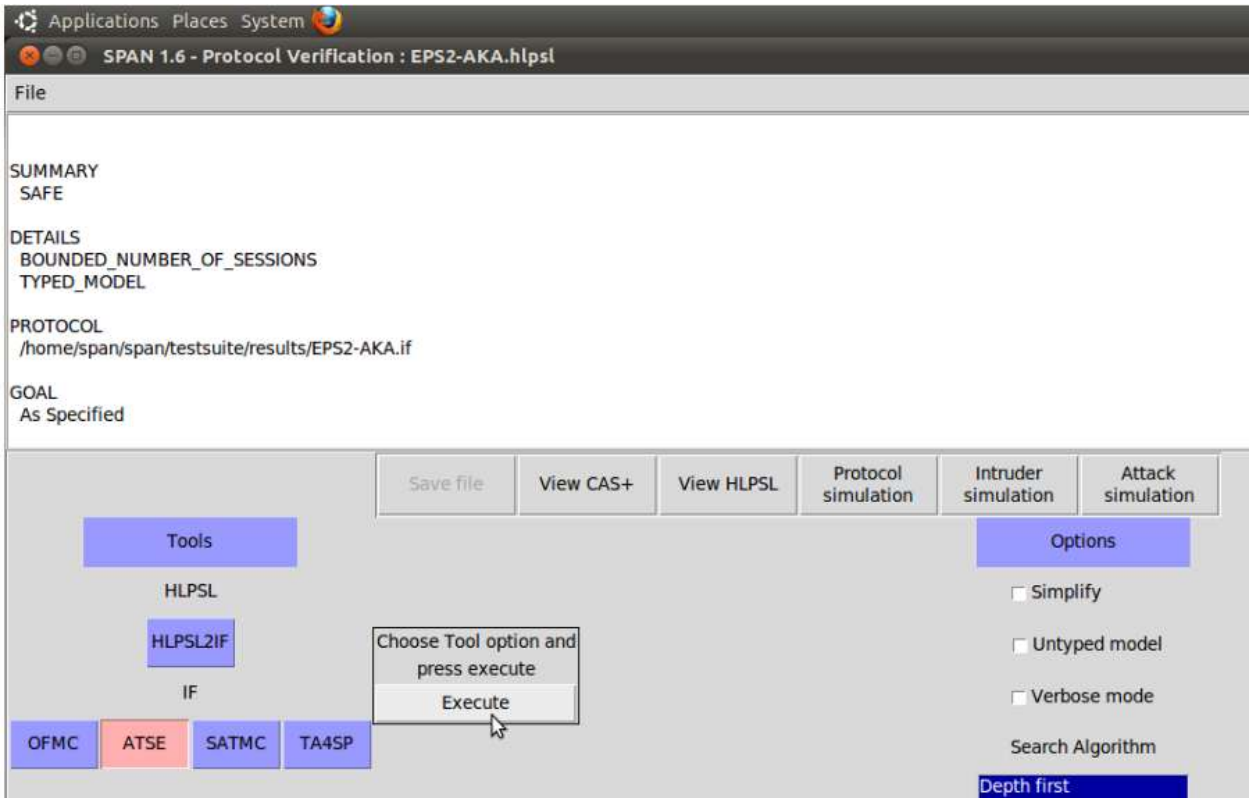
أما في البروتوكول المقترح يتم تسليم TRID إلى HSS من قبل UE وMME لذلك يمكن لـ HSS بسهولة التحقق من مدى وثوقية شبكة التخديم المتصلة معها.

5. الحماية من هجوم الرجل في المنتصف :

يعاني بروتوكول EPS من مشكلة الهجوم في الوسط، كما تبين لنا أعلاه عند اختبار البروتوكول باستخدام الاداة SPAN .

يمكن للبروتوكول المقترح التعامل مع المشكلة ببساطة نظرا لان هوية المشترك IMSI، مدرجة في رسالة طلب الاتصال كنص مشفر لا يمكن للمهاجم الحصول عليه.

وتم التأكد من تغطية البروتوكول المقترح للثغرات الامنية الموجودة في EPS-AKA باستخدام الاداة SPAN وتبين أنه آمن كما هو موضح بالشكل(8).



الشكل(8) اختبار البروتوكول EPS2-AKA باستخدام SPAN

2- الكلفة الإضافية:

التغييرات التي اقترحها البروتوكول EPS2 لا تتطلب استثمارات اضافية و بالتالي لا يوجد تجهيزات (hardware) إضافية أو أنظمة تشغيل إضافية. لذا فإن للبروتوكولين البروتوكولين نفس المستوى من التكلفة .

3- الحمل:

سيتم مقارنة البروتوكولين وفقاً لحركات المرور على الشبكة. الجدولين (1) و (2) يظهران حجم البارامترات الممرة لكل بروتوكول.

الجدول(1) حجم بارامترات البروتوكول EPS2-AKA

البارامتر	الحجم بالبت
AUTHID	64
RES	64
RAND	128
MAC	128
TRID	48
KASME	256
AUTN	128

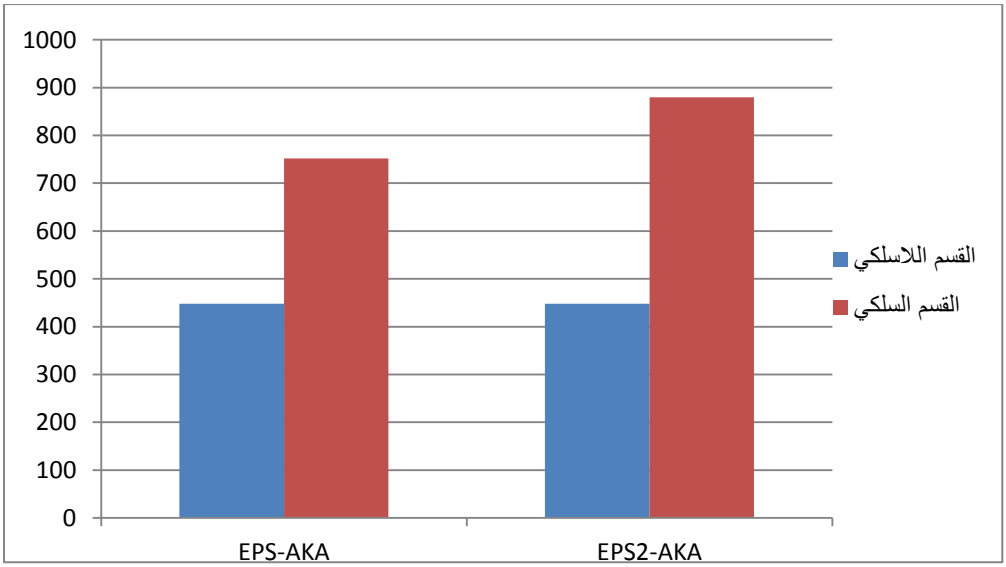
الجدول (2) حجم بارمترات البروتوكول EPS-AKA

البارامتر	الحجم بالبت
K	128
RAND	128
SQN	48
AK	48
AMF	16
AUTN	128
CK,IK	128
RES	128
KASME	256
MAC	64

وفقاً للرسائل الممررة على القسم السلكي واللاسلكي وحجم البارامترات لكل رسالة مع مراعاة المصادقة الأولية، والمصادقات اللاحقة، ومن أجل شعاع مصادقة واحد تظهر لدينا القيم في الجدوليين (3) و (4):

الجدول(3) الحمل على الشبكة وفقا للبارامترات المرسلة خلال عملية المصادقة الأولية

	بروتوكول EPS	بروتوكول EPS2
القسم اللاسلكي	448 بت	448 بت
القسم السلكي	752 بت	880 بت



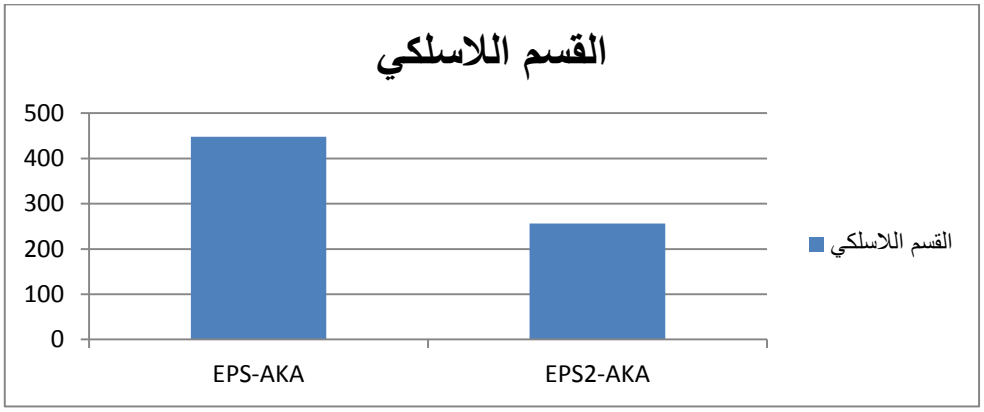
الشكل(9) مقارنة الحمل بين البروتوكولين EPS–AKA و EPS2–AKA عند المصادقة الأولية.

نلاحظ أن للبروتوكولين نفس الحمل على القسم اللاسلكي بينما يزيد حمل البروتوكول EPS2–AKA بنسبة قليلة ومقبولة مقارنة بالمستوى الأمني الذي حققه بتغطيه لنقاط الضعف السابقة.

يؤدي البروتوكول كامل عمله من خلال تقليل رسائل التوثيق ، وهذا يقلل من استهلاك النطاق الترددي بين بروتوكول EPS-AKA وبروتوكول EPS2-AKA.

جدول (4)الحمل على الشبكة وفقا للبارامترات المرسلة خلال عمليات المصادقة اللاحقة

	بروتوكول EPS	بروتوكول EPS2
القسم اللاسلكي	448 بت	256 بت



الشكل(10) مقارنة الحمل بين البروتوكولين EPS-AKA و EPS2-AKA عند المصادقات اللاحقة

نلاحظ أن البروتوكول المقترح لديه حمل أقل بمقدار النصف تقريباً بالمقارنة مع البروتوكول القياسي، مع العلم أن بروتوكول EPS2-AKA يقلل عدد رسائل التوثيق اللاحقة من ثلاث رسائل إلى رسالتين.

الاستنتاجات والتوصيات:

في هذا البحث ، اقترحنا البروتوكول EPS2-AKA لشبكة LTE لتعزيز مستوى الأمان لبروتوكولEPS-AKA . ، يوفر البروتوكول المقترح ميزات أمان قوية بما في ذلك إخفاء كامل لـ IMSI، ويزيد من صعوبة الحصول على بارامترات المصادقة لأن كل البارامترات يتم تشفيرها باستخدام الدالات الأمنية. يتم تغيير AUTHID بشكل دوري في كل جلسة مصادقة بواسطة HSS ويتم استخدامه لمنع إرسال IMSI ضمن رسائل طلب المصادقة.تم التاكد من تغطية البروتوكول الجديد لكل الثغرات الأمنية التي كانت موجودة في بروتوكول EPS-AKA باختباره بواسطة الأداة SPAN، ومن ثم تمت مناقشة تحليل أداء بروتوكول EPS2-AKA ،والذي بين انخفاض استهلاك النطاق الترددي بشكل كبير ، وانخفضت رسائل مصادقة الإرسال.

نُوصي بناءً على ما سبق باستخدامِ بروتوكول المصادقة المقترح EPS2-AKA بدلاً من البرتوكول القياسي في الشبكات الخلوية LTE.

المراجع:

1- ZUKANGK,S.*Overview of 3GPP LTE-advanced carrier aggregation for 4G wireless communications* IEEE Communications Magazine 50.2 (2012).

2- 3GPP TS 33.102 V11.5.0 (2012-12).*3rd Generation Partnership Project;Technical Specification Group Services and System Aspects; 3G Security; Security architecture* (Release 11). December 2012.

3- CAO,J. *A Survey on Security Aspects of LTE and LTE-A networks*,IEEE Communications Survey and Tutorial, Vol. 16, No 1, Frist Quarter 2014.

4- LI, XIEHUA, AND YONGJUN WANG. *Security enhanced authentication and key agreement protocol for LTE/SAE network.* Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on. IEEE, 2011.

5- د.أحمد،صقر،أحمد; ستيتي، أماني. *تقييم أداء بروتوكولات المصادقة في الشبكات الخلوية وفقاً لجودة الخدمة*. سلسلة العلوم الهندسية.(4)37;2016 Nov 21. ISSN: 2079-3081

6- CHOUDHARY,A;BHANDARIMR. *Analysis of UMTS (3G) Authentication and Key Agreement Protocol (AKA) for LTE (4G) Network*, International Journal on Recent and innovation Trend in Computing Communication, vol. 3, no. 4, pp. 2146-2149, 2015.

7-ALEZABI,K.*efficient authentication and key agreement protocol for 4G (LTE) networks*. Region 10 Symposium, 2014 IEEE. IEEE, 2014.

8- ETSI,T.*Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture* (3GPP TS 33.401 version 10.3. 0 Release 10) (2012).

9- [TR35.909], 3GPP, *3G Security: Specification of the MILENAGE algorithm set: an example algorithm set for the 3GPP authentication and key generation functions f1, f1∗, f2, f3, f4, f5 and f5∗*; Document 5: Summary and results of design and evaluation.2013..

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- GENET, T., *Span+ Avispa For Verifying Cryptographic Protocols*. 2017.