مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (37) العدد (4) 2015
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (37) No. (4) 2015

تقييم أداء بروتوكولات المصادقة في الشبكات الخلوية وفقاً لجودة الخدمة

الدكتور أحمد صقر احمد*
أماني ستيتي**

(تاريخ الإيداع 16 / 3 / 2015. قُبِل للنشر في 5/ 7 / 2015)

□ ملخّص □

نجحت شبكات LTE (Long Term Evolution) باعتبارها ذات انتاجية عالية أن تكون المظلة للشبكات اللاسلكية، مما دفع الباحثين بشدة الى دراسة وحل الثغرات الأمنية الموجودة. وكانت المصادقة المتبادلة التي اعتمدتها شبكات المحمول للتغلب على نقاط الضعف التي تُستغل لاصطياد المعرِّف الخاص بالمشترك IMSI (International Mobile Subscriber Identity) ، نجح تنفيذ المصادقة المتبادلة في نظام الحزم المطّور EPS AKA (Evolved Packet System) بتعزيز الأمن على الشبكة، لكنها فشلت في تغطية نقاط الضعف التي ورثت من UMTS .إحدى هذه النقاط هو اصطياد IMSI خلال اجراء تحديد هوية المشترك .على الشبكة. حاول العديد من الباحثين على مدى السنوات الماضية، اقتراح بدائل عن EPS–AKA قادرة على ضمان مستويات عالية من الأمن وتقديم أداء جودة خدمة مقبول.

في هذا البحث، سوف نقوم بتحليل SPAKA وPBKP الذي حل نقاط الضعف في EPS–AKA ، ثم سنقارن أداء جودة الخدمة لـ EC–AKA و EPS AKA .

البروتوكول المقترح "EC–AKA" هو المرشح الحقيقي ليحل محل المصادقة الحالية وبروتوكول اتفاق المفاتيح، لأدائه الممتاز في جميع البارامترات التي تمت دراستها.

الكلمات المفتاحية: الأمن في شبكات LTE ، اصطياد IMSI، المصادقة المتبادلة ، بروتوكول EC

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

مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (37) العدد (4) 2015
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (37) No. (4) 2015

Evaluate the performance of the authentication protocols in cellular networks according to the quality of service

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

(Received 16 / 3 / 2015. Accepted 5 / 7 / 2015)

□ ABSTRACT □

LTE's success as a high throughput, and umbrella technology for wireless networks is highly affected by the researchers' capability of solving its current security vulnerabilities. Mutual authentication was adopted by mobile networks to overcome vulnerabilities exploited by "IMSI catcher" and other active attacks. 3GPP's mutual authentication implementation in EPS AKA succeeded in enhancing the network's security, but failed to cover weaknesses inherited from its predecessor (UMTS). One of those vulnerabilities is the passive capturing of IMSIs during user identification in the Authentication and Key Agreement protocol. Many researchers tried over the past years, to propose an alternative for EPS AKA, able to ensure high levels of security and offer acceptable QoS performance. In this paper, we will crypt-analyze (SPAKA and PBKP) which was claimed to solve EPS AKA's privacy and mutual authentication weaknesses, then we will compare its QoS performance to EC-AKA and EPS AKA. Our proposed protocol "EC-AKA" is a real candidate to replace the current authentication and Key Agreement protocol, because of its excellent performance in all the studied parameters.

Keywords: LTE' Security , IMSI Catcher, Mutual authentication , EC protocol.

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

مقدمة:

الأمن في البيئة الشبكية السلكية التقليدية راسخ وقد تم بناؤه على أسس قوية، ودخول أي شخص يكون له دائماً حدود فيزيائية ملموسة ومحددة ولذا فإنه من الممكن تطبيق السيطرة الأمنية الصحيحة. إلا أنه في البيئة اللاسلكية وفي ظل وجود حدود لاسلكية مفتوحة في الهواء ، فإن مراقبة دخول غير المخولين بالوصول إلى المعلومات تكون أكثر صعوبة. وبالتالي لابد من تحقيق سياسات أمنية قوية وخصوصا في شبكات الخلوي بعد توسع استخدام هذه الشبكات في مجالات عديدة.

تحقيق مستوى عالي من الأمن هو دائما الهاجس الاول المرافق لتطور شبكات الاتصال الخلوي فهذا التطور يترافق دوما مع تطور الأودات المساعدة لتهديد أمن الشبكات.

في بداية الأمر كان تركيز العمل فقط على مصادقة المشترك من قبل الشبكة، وبعد ظهور مخاطر الأبراج والشبكات الوهمية، تطورت الأساليب لمصادقة المشترك والشبكة بنفس الوقت،مع الانتباه إلى ضرورة استخدام بروتوكولات على مستوى المشترك لمصادقته وتشفير البيانات المتدوالة ،وعلى مستوى عناصر الشبكة المرتبطة معاً ، لضرورة منع تعديل البيانات وكشف الهجوم،

إن وجد، مع محاولة عدم المخاطرة بين تحقيق جودة الخدمة Quality of Service(QoS) وتحقيق سرية عالية.

أهمية البحث وأهدافه:

يهدف البحث إلى رفع مستوى الأمن في الاتصالات الخلوية من خلال تحقيق المصادقة من قبل المشترك والشبكة في آن واحد من خلال استخدام بروتوكولات على مستوى المشترك ، وبين عناصر الشبكة الرئيسية لإدارة جلسة المفاتيح المتبادلة وتطوير بروتوكول المصادقة واتفاق المفتاح AKA (Authentication Key Agreement) مع المحافظة قدر المستطاع على جودة الخدمة.

تأتي أهمية هذا البحث نتيجة التوجه الكبير لإستخدام الموبايل للحصول على العديد من الخدمات الحياتية كتحويل الأموال وغيرها من الخدمات المصرفية ودفع الفواتير والبيع والشراء عن طريق الانترنت، وتزايد التهديدات والهجمات الامنية على انظمة المعلومات وشبكات الاتصالات ، وذلك من حيث حجمها وتنوعها وتعقيدها واستغلال نقاط الضعف في الشبكات الخلوية بالحصول على معِّرف المستخدم واستخدامه لتحديد موقع المشترك وبالتالي امكانية القيام بالأعمال الارهابية ، والاغتيال لذا لابد من العمل على تحقيق مستوى عالي من الأمن في هذه الشبكات للإستفادة منها بثقة .

طرائق البحث ومواده:

من أجل تحقيق الأهداف المذكورة سابقا سيتم في البداية التعرف على بروتوكول المصادقة واتفاق المفتاح وتحليله لتحديد نقاط الضعف المرافقة لتطور هذا البروتوكول مع تطور أجيال الشبكات الخلوية.

ثمّ تحقيق هجوم اصطياد معِّرف المشترك IMSI (International Mobile Subscriber Identity) بإستخدام برنامج AVISPA(Automated Validation of Internet Security Protocols and

(Applications) و بمقارنة عدة بروتوكولات مصادقة بالنسبة لجودة الخدمة (الأمن ،التكلفة ،الحمل) من أجل تحديد البروتوكول الأفضل لاستخدامه مستقبلا لتحسين الأمن في الشبكات الخلوية مع المحافظة على جودة الخدمة.

1 بروتوكول المصادقة واتفاق المفتاح AKA (Authentication and Key Agreement):[1] [2]

هو بروتوكول مصادقة بين الاطراف الثلاثة المستخدم (UE , USIM) و شبكة التخديم (VLR, MME) والشبكة الرئيسة HN(HLR\AUC, HSS\AUC).

يعتمد هذا البرتوكول على المفتاح السري k وهو مشترك بين UE(user equipment) و HN (Home Network) حيث يتم استخدامه من قبل HN لتوليد شعاع المصادقة AV(Authentication Vector) باستخدام الوظائف الأمنية .

اختلفت بارامترات شعاع المصادقة وفقا لتطور الشبكات الخلوية وزيادات التهديدات الأمنية :

1-1-بروتوكول المصادقة في شبكات GSM

في نظام GSM فان البروتوكول يعمل كالتالي:

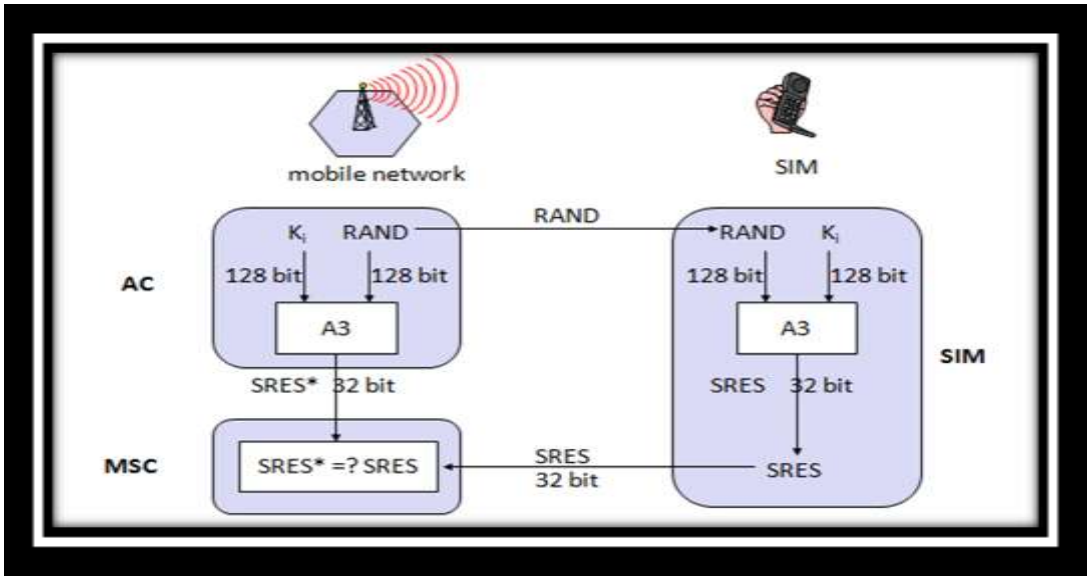
-عندما يريد UE الدخول الى الشبكة تطلب SN (serving network) عنوان IP الخاص بالمشترك

-يرسل UE عنوان IMSI أو TMSI(Temporary Mobile Subscriber Identity) الذي تمرره بدورها الى HN

-تقوم HN وفقاً لـ IMSI أو TMSI بالبحث في السجلات عن K الخاص به وتوليد رقم عشوائي RAND (Random) ، وتطبق F2(K,RAND) للحصول على قيمة SRES (SRESPONE)، وتقوم بإرساله مع RAND إلى SN

-يقوم UE بعد الحصول على القيمة العشوائية من SN بتوليد قيمة SRES وارسالها الى SN

تتم مقارنة قيمتي SRES في SN للحصول على المصادقة كما في الشكل (1).



الشكل(1) بروتوكول المصادقة واتفاق المفتاح في شبكات GSM

1-2-نقاط الضعف في شبكات GSM:

1. المصادقة تتم فقط من قبل الشبكة للمشترك وليس العكس،أدى ذلك لهجوم جديد وهو Base) BTS Transmit Station) للحصول على معلومات المشترك مثل IMSI

2. الحمل الزائد على الشبكة، ففي كل عملية مصادقة يتم تبادل الرسائل نفسها مع HN

يكمن الحل بوجود بارامترات جديدة في البروتوكول AKA لمصادقة الشبكة والمشترك معاً، وتوليد أشعة المصادقة (AV(authentication vector. وتم استخدامها في شبكات نظام الاتصالات المتنقلة العالمية UMTS (Universal mobile telecommunications system) و التطور الطويل الأجل (Long-term evolution LTE).

2 - **برتوكول المصادقةEPS AKA في شبكات UMTS و LTE: [3]**

3 - يتم تحقيق البروتوكول في مرحلتين:

1- توزيع AV.

2- المصادقة واتفاق المفتاح.

❖ **2-1- توزيع اشعة المصادقة AV:**

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

2 - يرسل المستخدم UE عنوان IMSI كرد على SN

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

4 - تقوم HN بتوليد اشعة مصادقة AV وترسلها الى SN .

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

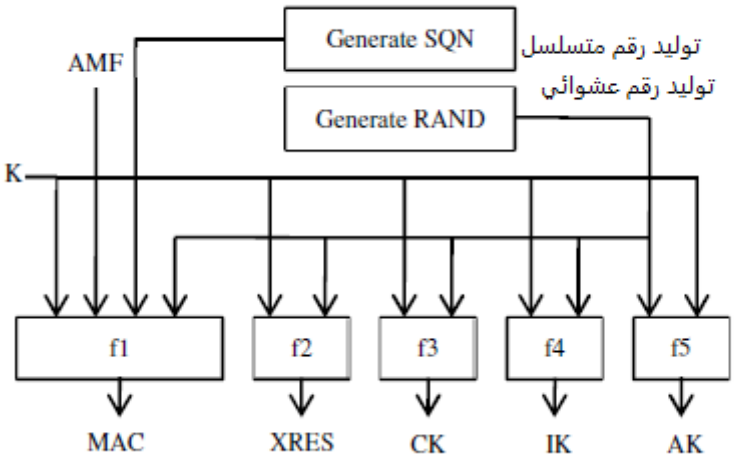
بارامترات شعاع المصادقة: [4]

- RAND قيمة عشوائية تولد في HN
- XRES (XResponse) قيمة الاجابة التي تتوقع SN استلامها من الشترك UE
- CK (Cypher Key) مفتاح التشفير
- IK (Integrity Key) مفتاح السلامة
- AUTN(Authentication Token) علامة المصادقة ومن خلاله يصادق المشترك الشبكة

ويتكون من ثلاث اجزاء:

- SQN(Sequence Number) : رقم تسلسلي
- AMF (Authentication Management Field) حقل ادارة المصادقة .يُستخدم لإدارة أغراض أمنية معينة.
- MAC (Message Authentication Code) شيفرة رسالة التوثيق يتم التحقق منها في UE

ويتم حسابهم وفق الوظائف الأمنية (security functions) f1,f2,f3,f4,f5 كما في الشكل (2):



الشكل (2) حساب بارامترات المصادقة بالوظائف الامنية

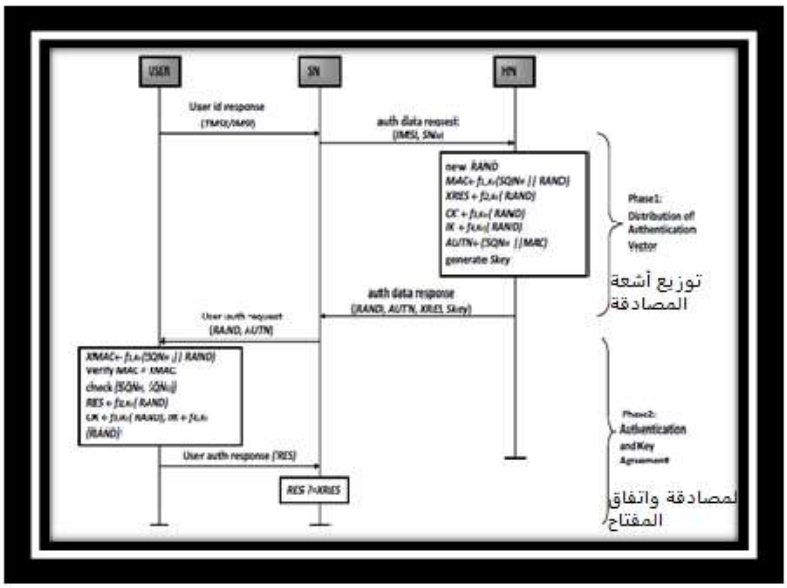
❖ **2-2- المصادقة واتفاق المفتاح Authentication Key Agreement: [5]**

تتم وفق الاجراء التالي:

1 بعد ان تستلم SN اشعة المصادقة ترسل البارامترين (RAND,AUTN) الى المستخدم

2 يقوم UE بحساب XMAC , RES ويتحقق من مطابقته لقيمة MAC المستقبلة من SN عبر AUTN، بذلك يكون UE قد تحقق من HN و SN ومصادقة الشبكة وهو حل للشبكات ونقاط الوصول الوهمية . وبعد ذلك يتم التحقق من SQNHو SQNU (الرقم التسلسلي الوارد من HN والرقم التسلسلي الموجود في UE) وذلك للتحقق من حداثة شعاع المصادقة . بعد التحقق من البارامترين السابقين يقوم UE بتوليد البارامتر RES ويرسله الى SN.

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



الشكل(3) خوارزمية عمل البروتوكول AKA

- من اجل تحديد هوية المشترك يتم استخدام إما هوية مؤقتة TMSI (temporary Mobile Subscriber Identity) او هوية دائمة IMSI (International Mobile Subscriber Identity) .
- يتم استخدام IMSI في حالتين :

1-عندما يشغل المشترك MS الخاص به

2-عندما تفقد الشبكة المراسلات بين IMSI و TMSI (مع العلم ان المراسلات تحفظ في SN ضمن VLR)

- في هاتين الحالتين يتم ارسال IMSI بشكل واضح وصريح عبر الوصلات اللاسلكية، وهذا يؤدي الى مخاطر جمة وخاصة اذا تم استخدام MS في حالة الدفع وتحويل الاموال باستخدام الشبكات، ويعتبر نقطة ضعف خطيرة في هذا البروتوكول. كما في الشكل (4)

الشكل(4) اجرائية الحصول على IMSI

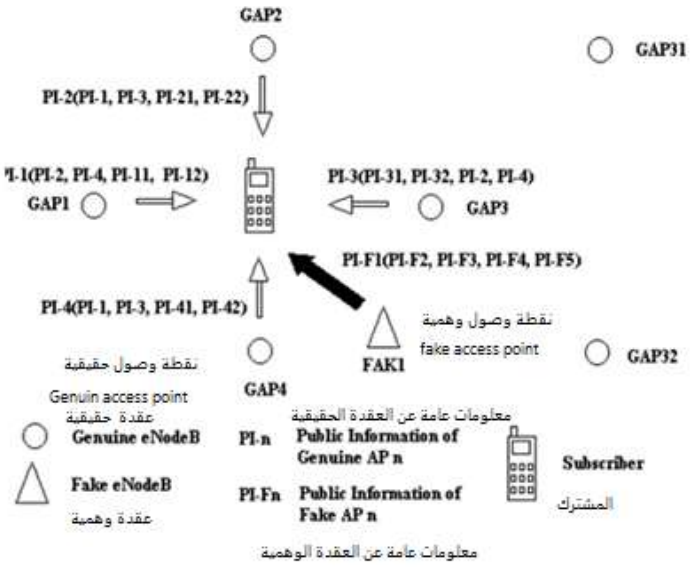
3-بروتوكول البث العام للمفاتيح العامة (PKBP) Public-Key Broadcast Protocol [6]:

تقوم كل عقدة او access point (AP) بارسال معلومات عامة عنها وعن جيرانها، وهذه المعلومات تحوي(المفتاح العام-المعرف- قوة الاشارة). يختار الموبايل العقدة وفقا لمعيارين :

- تكون قوة الاشارة فيها اكبر (POWER SIGNAL)
- تابعة للمجموعة الكبرى (BIGGEST GROUP)

بالتالي فان UE (User Equipment) سوف يتحقق من أن هذه العقدة أصلية وليست وهمية لأنها تابعة لأكبر عدد من العقد من نفس الشبكة، لأنّ العقد الأصلية دوما أكبر عدد من الوهمية نظرا للتكلفة الباهظة.

ليكن لدينا السيناريو التالي كماهو في الشكل (5):



الشكل(5) سيناريو الاتصال في PKBP

في هذا السيناريو لدينا أربع عقد حقيقية وعقدة وهمية (FAK1) ،تقوم كل عقدة بارسال البارامترات المذكورة سابقاًعنها وعن جيرانها فيتكون الجدول(1) وفقا للبيانات المستقبلة في جهاز الموبايل [4]

الجدول(1) البارامترات المستقبلة

AP ID معرف نقطة الوصول	Public Key المفتاح العام	Modulus المعامل	Power Signal قوة الاشارة	Group المجموعة
AP_1	PK_1	N_{AP1}	PS_1	1
AP_2	PK_2	N_{AP2}	PS_2	1
AP_3	PK_3	N_{AP3}	PS_3	1
AP_4	PK_4	N_{AP4}	PS_4	1
AP_{F1}	PK_{F1}	N_{APF1}	PS_{F1}	2

بالتالي فان الموبايل سيختار العقدة AP1 ليتصل معها لأنها تملك أقوى اشارة وتابعة لأكبر مجموعة ،حتى لو كانت العقدة APf1 صاحبة الاشارة الأقوى .

هذه الألية صحيحة في حال كانت العقدة الوهمية غير قادرة على بث اشارات متعددة منفصلة .

3-1-بروتوكول المصادق الذاتي على المفتاح العام SPAKA(Self- Certified Public-Key based Authentication):

يقوم بتحديد دور PKBP، فلنفرض وجود عقدة متطورة eNB (evolved Node B) تقوم بارسال البارمترات التالية:

[A1, BCH1 {PI-1, PI-2, PI-3, PI-4}] حيث:

A1: مدى التردد الواصل للموبايل من eNB

BCH1 : (Broadcast Chanel) البث العام من العقدة eNB تحوي معلومات عن العقدة وجيرانها.

بفرض لدينا أربع عقد حقيقية تغطي منطقة الموبايل فان UE سيتلقى الاشارات التالية:

A1 ×BCH1 {PI-1, PI-2, PI-3, PI-4}

A2×BCH2{PI-2, PI-1, PI-3, PI-4}

A3×BCH3{PI-3, PI-1, PI-2, PI-4}

A4×BCH4{PI-4, PI-1, PI-2, PI-3}

في حال قامت عقدة وهمية BTS بارسال اشارات متزامنة من BCH واشارات منفصلة ،فان كل منها تمثل عقدة مستقلة وهمية بالتالي تمكن BTS من التنكر بخمس عقد وهمية وسترسل الراسائل التالية:

AF1×BCHF1{PI-F1, PI-F2, PI-F3, PI-F4, PI-F5}+

(AF1×BCHF2{PI-F1, PI-F2, PI-F3, PI-F4, PI-F5})/2 +

(AF1×BCHF3{PI-F1, PI-F2, PI-F3, PI-F4, PI-F5})/2 +

(AF1×BCHF4{PI-F1, PI-F2, PI-F3, PI-F4, PI-F5})/2 +

(AF1×BCHF5{PI-F1, PI-F2, PI-F3, PI-F4, PI-F5})/2

وفقا للبيانات المستقبلة من العقد الشرعية والعقد الوهمية فان الموبايل سيشكل الجدول(2) المبين:

الجدول(2) البارمترات المستقبلة في حال الهجوم

AP ID	Public key	Group
AP_1	PK_1	1
AP_2	PK_2	1
AP_3	PK_3	1
AP_4	PK_4	1
AP_{F1}	PK_{F1}	2
AP_{F2}	PK_{F2}	2
AP_{F3}	PK_{F3}	2
AP_{F4}	PK_{F4}	2
AP_{F5}	PK_{F5}	2

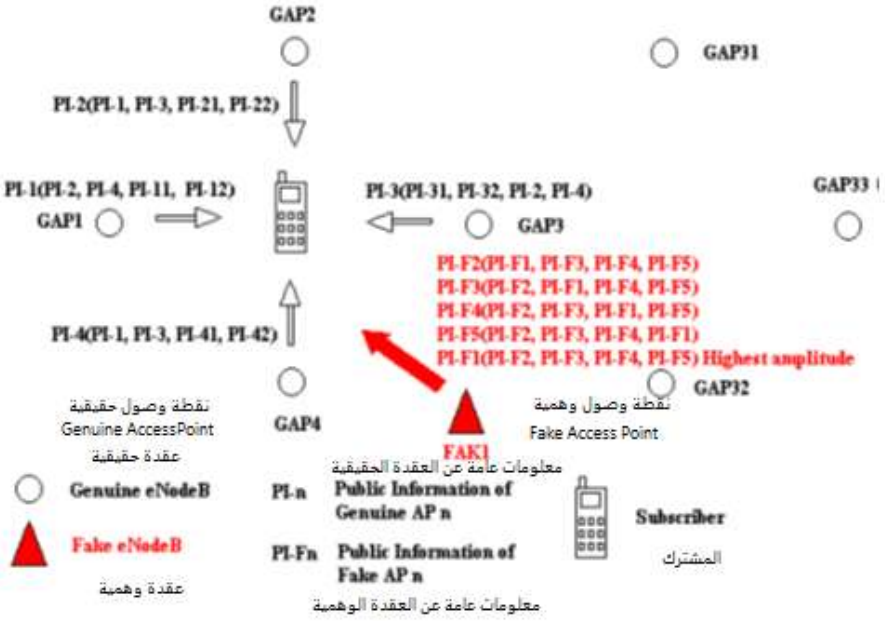
Physical AP
AP_1
AP_2
AP_3
AP_4
AP_{F1}
AP_{F1}
AP_{F1}
AP_{F1}
AP_{F1}

ويتم حساب قوة اشارة العقدة الوهمية وفق:

Link power budget = AF1 × (1 + ½ + ½+ ½+ ½) = 3× AF1

AF1 = Link power budget/3 [5].

ويتم السيناريو كما في الشكل (6):



الشكل(6) سيناريو الهجوم في PBKP

بالتالي سيختار الموبايل العقدة الوهمية حتى يتواصل معها وفي هذه الحالة سيقوم بارسال IMSI المشفرة باستخدام المفتاح العام الخاص بالعقدة الوهمية وبالتالي سيتم الحصول عليه .

يكمن الحل بجعل الشبكة الرئيسية HN مسؤولة عن تحديد SN لأنها تملك جميع المعلومات التي تجعلها أفضل من MS في اتخاذ القرار.

4-الهجوم في بروتوكول EPS AKA:[8] [7] [8]

نقاط الضعف في بروتوكول EPS:

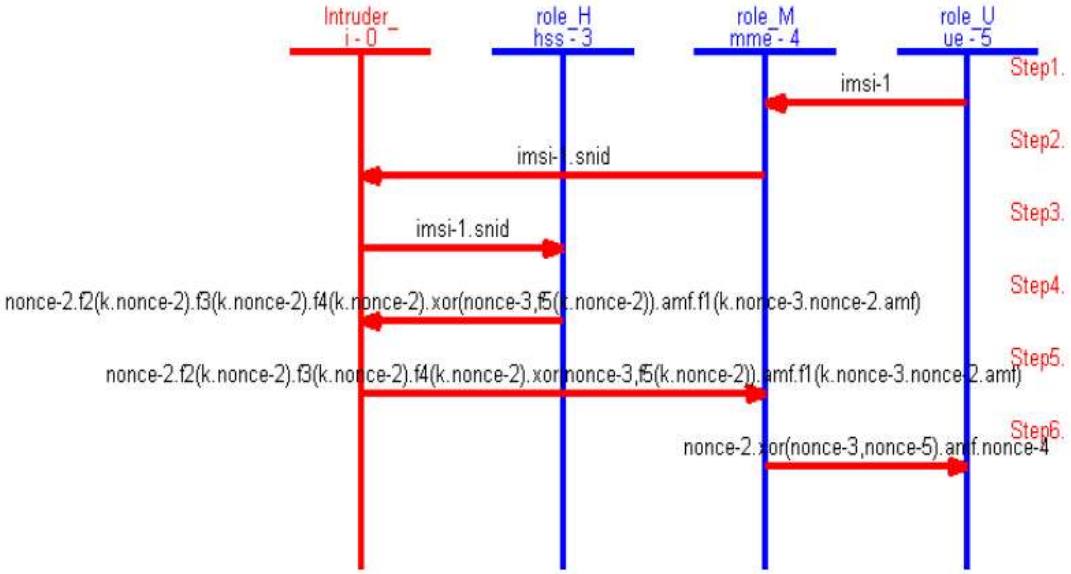
- BTS وهمية لأن MS هو من يقوم باختيار العقدة للتواصل معها .
- امكانية اصطياد IMSI

يتم الهجوم في مستويين:

1. الهجوم السلبي (Passive Attack) : باصطياد المعّرف IMSI وخصوصا 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 لايحتاج الى مواد كثيرة ولكن فعاليته قليلة ،أمّا بالنسبة للنمط الثاني فهو مكلف ولكن فعاليته عالية وخصوصا اذا تمكنت العقدة الوهمية من الحصول على ثقة الشبكة الرئيسية.

فيما يلي سيناريو الهجوم على المستوى الثاني باستخدام الأداة SPAN(Security Protocol ANimator) المقترح من AVISPA كما في الشكل (7) [9]



الشكل(7) الهجوم على المستوى الثاني باستخدام SPAN

يتم هذا الهجوم وفق التالي حيث المتطفل (intruder) يشكل محطة وهمية:

1. يتمكن المتطفل من الحصول على المعّرف المرسل من شبكة التخديم الى الشبكة الرئيسية
2. يرسل المتطفل المعّرف الى الشبكة الرئيسية
3. ترسل الشبكة الرئيسية معلومات أشعة المصادقة الى المتطفل عوضا عن شبكة التخديم (MME)
4. يقوم المتطفل بإرسال المعلومات الى شبكة التخديم التي بدورها ترسلها الى المشترك

بالتالي تمكنت العقدة الوهمية بالحصول على جميع المعلومات الخاصة بالمشترك والتي يترتب عليها أمور عدة.

5-بروتوكول السرية المضمونة EC-AKA Ensured Confidentiality:[10]

5-1-المفاهيم الاساسية في البروتوكول:

RandomEncKey (A random Encryption key) : مفتاح تشفير عشوائي يولد في UE ويستخدم قبل تبني CK RandomIntKey (A random Integrity key generated) : مفتاح وثوقية عشوائي يولد في UE ويستخدم قبل تبني المفتاح IK

IMSI’:الأرقام العشرة الأخيرة من IMSI

RandomUESecCapab1:رقم عشوائي يولد في UE ليسمح لكيان إدارة التجوال MME(Mobility Management Entity) بمشاركة امكانيات UE الأمنية المختارة

TIK = PIK|| RandomIntKey(Temporary Integrity Key) مفتاح الوثوقية المؤقت

PIK (Permanent pre-shared Integrity Key) : مفتاح سلامة دائم يتم مشاركته مسبقا بين UE و HSS ويتم توليده باستخدام hashing function من IMSI

EK=XOR(PEK, RandomEncKey)

PEK (Permanent pre-shared Encryption Key) : مفتاح تشفير دائم يتم مشاركته مسبقا ويحفظ في UE و HS

UESecCapabilities: قائمة من خوارزميات التشفير والسلامة المدعومة.

IntegritycheckTIK: نتيجة فحص وثوقية الرسالة باستخدام المفتاح TIK

PKH, PKM: المفتاح العام الخاص بـ HSS و SN

5-2-طريقة عمل البروتوكول :

يركز البروتوكول EC-AKA على تقوية التشفير والسلامة للقنوات المستخدمة في التراسل بالاضاقة لحماية المفاتيح المولدة و المتبادلة .

في هذا البروتوكول يتم استخدام التشفير المتناظر ابتداءً من الرسالة الرابعة، وهذا يقلل من التشفير الغير متناظر وبالتالي يقلل من التأخير، لأن خوارزميات التشفير المتناظر أسرع من التشفير غير المتناظر .

الرسائل المتبادلة تتم وفق :

1. UE → MME: NAS Attach Request: A={IMSI',RandomEncKey, RandomIntKey, UESecCapabilities, RandomUESecCapab1, IntegritycheckTIK}PKH , IDHSS

يرسل UE طلب اتصال الى MME ،حيث يولد UE ثلاث مفاتيح عشوائية :

RandomEncKey, RandomIntKey, and UESecCapabilities

ويتم التأكد من وثوقية الرسالة بتوليد البارامتر IntegritycheckTIK باستخدام خوارزمية يتم الاتفاق عليها وباستخدام TIK، وتشفر المحتويات السابقة باستخدام المفتاح العام الخاص بـ HSS بالإضافة لإرسال ID الخاص بـ HSS .

2 - MME → HSS: Authentication Data Request: A, {SNID}PKH

بعد وصول الطلب يقوم MME باستخلاص ID المعرف الخاص بالشبكة الرئيسية HSS ويضيف SNID (Serving Network Identity) ويشفرها باستخدام المفتاح الخاص بشبكة المستخدم ويرسلها مع الرسالة A الى HSS.

3. HSS → MME: Authentication Data Response {AV(1, …, n), UESecCap , EK, IntegrityCheck(AUTN(i), RAND(i), KSIASME)TIK, Integrity checkIIK }PKM

عند وصول طلب المصادقة الى HSS يقوم بفك التشفير بالمفتاح الخاص به ،وفقاً لـ IMSI تقوم الشبكة الرئيسية بجلب المفتاح الأساسي K المحفوظ في HN و SIM وأكثر دقة في UICC(Universal Integrated Circuit Card) ، يتم استخدام المفتاح K مع الرقم العشوائي RAND لتوليد مجموعة من المفاتيح .

يتم توليد عدد n من أشعة المصادقة للمستخدم AV ليتم استخدامها من MME لاحقا عند الحاجة بدلا من ارسال طلب جديد للحصول على المصادقة وهذا يزيد من التأخير في المشغل .

يتم توليد RandomIntKey ||PIK مع العلم أن المفتاح PIK يتم تبادله سابقا للحصول على TIK المطابق لـ TIK الموجود من جانب UE ، ويتم فحص وثوقية الرسالة. في حال عدم مطابقة قيمة IntegritycheckTIK يتم رفض الطلب والرد برسالة خطأ ، وإلا يولد EK = XOR(PEK, RandomEncKey) حيث PEK تمّ تبادله سابقاً و RandomEncKey يتم الحصول عليه من الرسالة المستقبلة A.

ويُحسب قيمة وثوقية الرسالة ويُشفر المحتويات باستخدام المفتاح العام الخاص بشبكة التخديم SN ويرد برسالة Authentication Data Response.

4. MME → UE: User authentication request : {RAND(i), AUTN, KSIASME, IntegrityCheck

(AUTN(i),RAND(i),KSIASME)TIK }

EK,XOR(RandomUESecCapab1,chosenUESecCapability

يتم فك تشفير الرسالة في MME باستخدام المفتاح الخاص بها وارسال AV(1) المتضمن RAND(1) AUTN, KSIASME, والتأكد من وثوقية البارامترات بحساب IntegrityCheck وتشفيرها باستخدام EK وفق خوارزمية يتم تحديدها بحساب XOR(RandomUESecCapab1,chosenUESecCapability.

5. UE → MME: User authentication response:{RES}EK.

بعد وصول الرسالة الىUE يتم تحديد خوارزمية التشفير وفق

(chosen algorithm's code+RandomUESecCapab1) – RandomUESecCapab1

عندئذ يستطيع UE فك التشفير باستخدام الخوارزمية والمفتاح الصحيحين ،من RAND(1), AUTN, KSIASME يستطيع UEالتحقق من وثوقية SN.

في حال تمت المصادقة على SNيتم حسابRES وتشفيرها بالخوارزمية والمفتاح المتفق عليهما.

6. MME → UE: NAS Sec Mode Command : {eKSI, [IMEISV request], [NONCEUE, NONCEMME]NASMAC}EK

بعد حساب RES ومطابقته مع XRES يتّم مصادقة المشترك من قبل الشبكة .في هذه اللحظة يبدأ الاتصال الآمن باستخدام المفاتيح المولدة من AKA . إن المعلومات بحاجة الى فحص وثوقية وتشفير باستخدام المفتاح EK علما ان خوارزميات التشفير والوثوقية يجب أن تكون ضمن لائحة الامكانيات الأمنية لـ UE.

7- UE → MME: NAS Security Mode Complete(IMEISV,] NAS-MAC)

يستلمUE الأمر ويرد برسالة اعلام NAS Security Mode Complete .

8- MME → eNB: Initial Context Setup (KeNB)

ان eNB عقدة تتصل بها UE مباشرة والتي تتصل بدورها بـ MME .

ترسل MME رسالة التهيئة أو الرسالة الأولية لـ eNB التي تحوي الخوارزميات والمفاتيح المستخدمة ليبدا الاتصال AS .

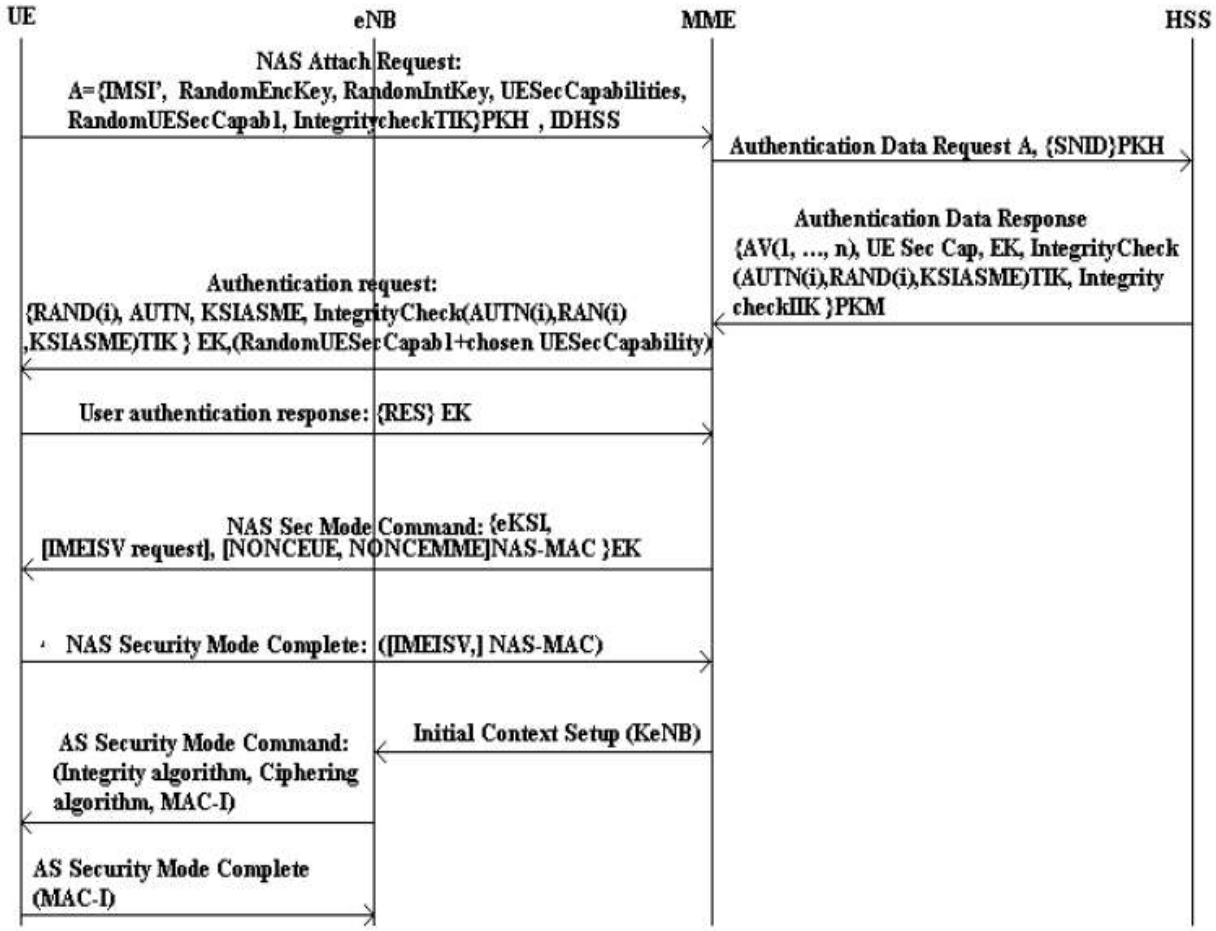
مع العلم ان الاتصال بين MME و eNB اتصال آمن باستخدام IPsec بالتالي ليس بحاجة للتشفير

9. eNB→ UE : AS Security Mode Command (Integrity algorithm, Ciphering algorithm, MAC-I)

يرسل eNB الامر بالبدء بالاتصال AS .

10- UE → eNB : AS Security Mode Complete (MAC-I)

يرد UE بارسال رسالة اعلام ACK ويبدأ بالاتصال الآمن والمشفر كما في الشكل(8).



الشكل(8) إجرائية البروتوكول EC-AKA

مما سبق نجد أن جميع رسائل AKA مشفرة حتى قبل تحديد الهوية مع أقل تكلفة واقل زمن.

النتائج والمناقشة:

تتفوق البروتوكولات عن بعضها بمدى قدرتها على عدم المخاطرة بجودة الخدمة مع تحقيق سرية عالية للبيانات المرسلة .

لذا لابد من تحليل أداء كل بروتوكول ومدى فقاليته وفقا لبرامترات الجودة(الأمن ، التكلفة،الحمل)

1 -الأمن(security):

وفقا لبنية البروتوكولات السابقة يتم ترتيبها تنازليا وفقا للأمن ووفقا لزيادة المخاطر

- EC-AKA
- (SP-AKA and PKBP)
- EPS AKA

2 - التكلفة(cost):

التغييرات التي اقترحها البروتوكول SPAKA و EC-AKA لا تتطلب استثمارت اضافية و بالتالي لايوجد تجهيزات (hardware)اضافية أو أنظمة تشغيل اضافية(software).

بالتالي البروتوكولين السابقين لهما نفس المستوى من التكلفة مقارنة بالبروتوكول EPS-AKA.

3 - الحمل overhead:

سيتم مقارنة البروتوكولات السابقة وفق حركات المرور على الشبكة

❖ الرسائل المحمّلة على الشبكة Upload message (Radio,Backhaul):

NAS Attach Request: 1024 (RSA) + 20 (HSS ID)

User Authentication Response: 128 (RES)

Upload Radio = Upload Backhaul = 1172 bits

❖ الرسائل المحمّلة عن الشبكة Download message(Radio. Backhaul):

Authentication Request: 128 (RAND) + 128 (AUTN) + 128 (Integrity check) + 3 ((RandomUESecCapab1 XOR chosen UESecCapability) + 4 (KSIASME) = 391 bits

❖ حركة المرور الأساسية(core traffic) :

Authentication Data Request: 2048

Authentication Data Response: ceiling ((n*688+396)/1024) *1024

Core traffic = 2048 + ceiling ((n*688+396)/1024) *1024 bits

الجدول(3) يظهر حركة المرور للبروتوكولات :

الجدول(3) الحمل على منافذ البروتوكولات

	الحمل الراديوي	حمل الوصلة	الحمل الراديوي	حمل الوصلة	الحركة الاساسية
	Upload Radio	*Upload Back-haul*	*Down-load Radio*	*Download Backhaul*	*Core Traffic*
EC-AKA	1172	1172	391	391	2048+ ceiling ((n*688+396) /1024)*1024
SP-AKA	1084	1024	120+x*(148+Z)	9216+Z	10240 +Z
EPS AKA	118	118	304	304	80 +n*688

حيث X :يمثل عدد نقاط الوصول المستخدمة AN (Access Node)

n:عدد أشعة المصادقة المرسلةAVs

Z: حجم كل من أشعة المصادقة المرسلة

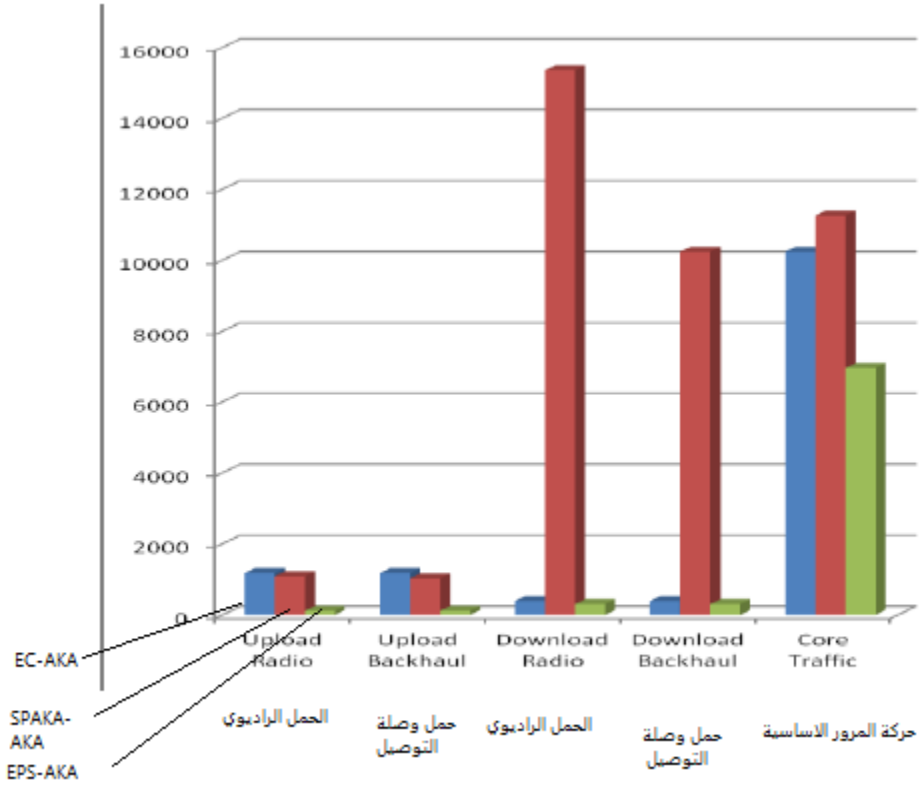
قيمة X عادة 13، وقيمة n هي 10 ،بينما قيمة Z تعتمد على الخوارزمية المستخدمة . في هذا البحث سوف نستخدم خوارزمية التشفير غير المتناظرةRSA بالتالي قيمة Z ستكون 1024

الجدول(4) التالي يبين القيم الفعلية للحمل على الشبكة بالمقارنة بين البروتوكولات EC-AKA,SPAKA,EPS-AKA

الجدول(4) مقارنة حمل البروتوكولات

	الحمل الراديو	حمل وصلة التوصيل	الحمل الراديوي	حمل وصلة التوصيل	الحركة الاساسية
	Upl-oad Radio	*Upload Back-haul*	*Down-load Radio*	*Down-load Backhaul*	*Core Traffic*
EC-AKA (bits)	1172	1172	391	391	10240
SPAKA (bits)	1084	1024	15356	10240	11264
EPS AKA (bits)	118	118	304	304	6960
SPAKA - EC-AKA (bits)	-88	-148	14965	9849	1024
SPAKA vs EC-AKA (%)	-8.12	-14.45	97.45	96.18	9.09
SPAKA - EPS AKA (bits)	966	906	15052	9936	4304
(SPAKA vs EPS AKA (%)	89.11	88.48	98.02	97.03	38.21

الجدول (4) يبين قيم الحمل وحركات المرور على الواجهات للبروتوكولات المدروسة ويتم تمثيلها بيانياً كما في الشكل(9)

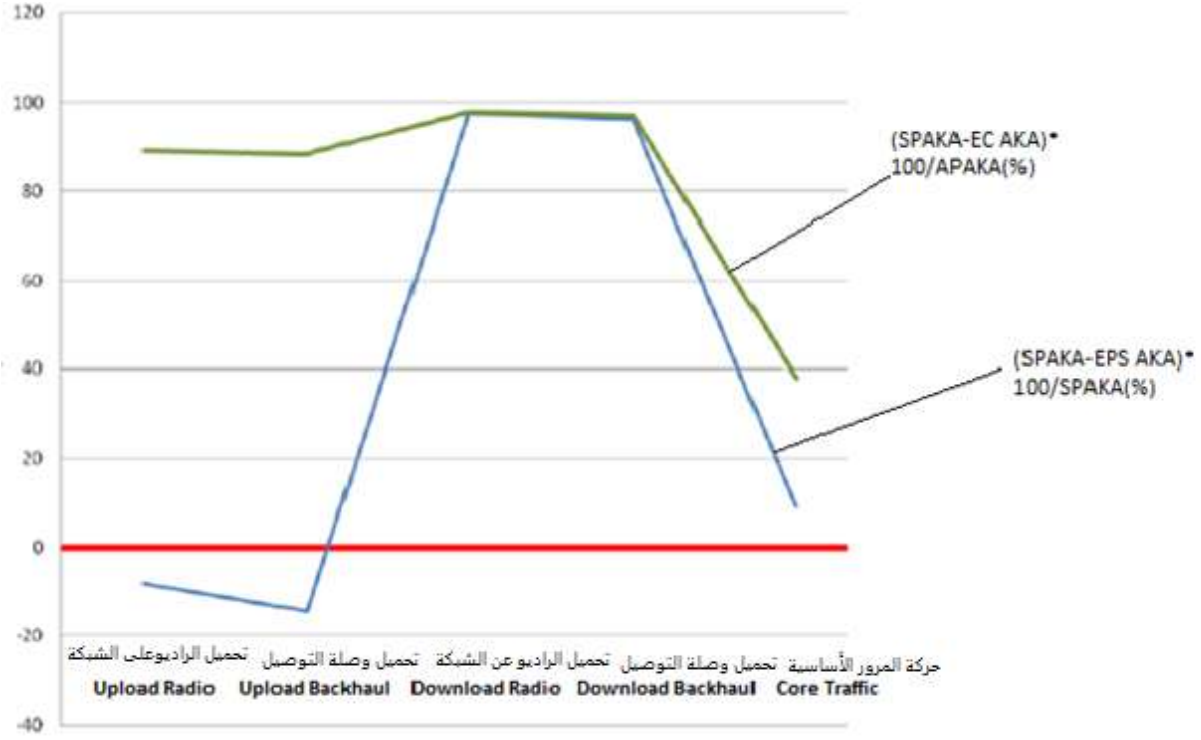


الشكل(9) الحمل على منافذ البروتوكولات

في الشكل (10) تتم مقارنة SPAKA نسبيا مع كلٍ من البروتوكولات وتظهر القيم بالنسبة المئوية.نستنتج من الشكل ترتيب البروتوكولات وفقا للحمل على الشبكة.

حيث يتم ترتيبها وفق التالي:

- EPS AKA
- EC-AKA
- (SP-AKA and PKBP)



الشكل(10) مقارنة نتائج الحمل بنسبة مئوية

تحليل النتائج:

نتيجة مقارنة البروتوكولات الثلاثة المدروسة يمكن تنظيم الجدول(5) .كما يمكن أن نرى، تفوق البروتوكول EC–AKA في جميع البارامترات المدروسة، وبالتالي نجحنا في اقتراح بروتوكول أفضل من (SPAKA و PKBP). على الرغم أن البرتوكول EPS AKA لديه أقل تكلفة مما يؤدي إلى أداء أسرع، لكنه فشل في ضمان مستوى الأمان المطلوبة من قبل شبكات الجيل الجديد. بالتالي بروتوكول السرية المضمونة EC–AKA Ensured (Confidentiality)هو البروتوكول الوحيد من الثلاثة المذكورة أعلاه قادر على تلبية احتياجات شبكات الأجيال اللاحقة NGN (Next Generation Network) من حيث الأمن، والتكلفة والأداء.

الجدول(5) نتائج مقارنة بارامترات QoS

	SPAKA	EPS AKA	EC-AKA
Security	2	3	1
Cost	1	1	1
Overhead	3	1	2

الاستنتاجات و التوصيات:

في هذه البحث تم تحليل البروتوكولين (SPAKA و PKBP) و أثبتنا أنه فشل في تغطية نقاط الضعف في البروتوكولEPS AKA ولقد تمكنا من إثبات أن البروتوكول المقترح " EC–AKA" هو الأفضل بين البروتوكولات

الثلاثة المدروسة من حيث الأمن و الحمل والتكلفة، علاوة على ذلك أننا نجحنا في تغطية كل نقاط الضعف المذكورة سابقا وتقديم حل لهجوم اصطياد المعّرف IMSI (International Mobile Subscriber Identity) معُرف المشترك العالمي وذلك باستخدام الاداة SPAN المحملة على المحاكي AVISPA.

المراجع:

1- KATARIA,J;BANSAL,A.*Exploration of GSM & UMTS security architecture with AKA protocol*. International Journal of Scientific and Research.Vol.3,No.2,2013,2250-3153.

2- TSAY,S; STIG, F. *A Vulnerability in the UMTS and LTE Authentication and Key Agreement Protocols*. Norwegian University,2010,12.

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

4- CARAGATA,D.*Confidential initial identification and other improvements for UMTS security*. Federico Santa Maria Technical University,UK,2013,10.

5- 3GPP TS 33.102 V11.5.0, 3rd Generation Partnership Project; *Technical Specification Group Services and System Aspects;3G Security ;Security architecture* (Release 11),2012,76.

6- DAKE,H; JIANDO.W; ZHING,Y.*User authentication scheme based on self-certified public-key for next generation wireless network* . IEEE, Security Technologies, ISBAST 2008, 23-24 April 2008,23.

7- 3GPP TR 33.821 V9.0.0 . *Rationale and track of security decisions in Long Term Evolved (LTE) RAN , 3GPP System Architecture Evolution* (SAE) .(Release 9),2009,56.

8- BOU ABDO,J;DEMERJIAN,H. *Security V/S Qos for LTE Authentication And Key Agreement Protocol*. International Journal of Network Security & Its Applications special issue on: "Communications Security & Information Assurance",Vol.4, No.5, September 2012,12.

9- AVISPA Project, http://www.avispa-project.org/.

10 - CHAOUCH,H;AOUDE,M. *Ensured Confidentiality Authentication and Key Agreement Protocol for EPS*. CNRS SAMOVAR, UMR 5751 ,Paris, France,2013,5.

Email:drahmad1961@gmail.com

Email:amany.stiety@hltmail.com