تأثير الشبكات الخاصة الافتراضية وخوارزمية التشفير AES و خوارزميات الترميز الصوتي على أداء بروتوكول VOIP (كلية الهندسة المعلوماتية – جامعة حمص أنموذجاً)

د.م يمان غازي[1]

الملخص

في ظل التحول الرقمي المتسارع، أصبحت الاتصالات الصوتية عبر شبكات البيانات جزءاً أساسياً من البنية التحتية الحديثة، حيث تعتمد العديد من المؤسسات على تقنيات VoIP لتوفير اتصالات مرنة وفعالة من حيث التكلفة. هذه التقنية تتيح نقل الصوت بجودة عالية عبر الإنترنت، لكنها تبقى عرضة لتحديات تتعلق بالأمان والأداء، خاصة في البيئات الأكاديمية والمؤسسية الحساسة. من بين الحلول المستخدمة لتعزيز خصوصية الاتصال، تبرز الشبكات الخاصة الافتراضية (VPN)كوسيلة فعالة لإنشاء قنوات اتصال آمنة بين الأطراف، مما يقلل من احتمالية التنصت أو التلاعب بالبيانات. إلا أن استخدام VPN قد يضيف عبئاً على الشبكة، يؤثر على جودة الخدمة المقدمة عبر VoIP . في السياق ذاته، يُعد التشفير باستخدام خوارزميةAES من أكثر الأساليب شيوعاً لحماية البيانات الصوتية أثناء النقل، لما يتمتع به من قوة أمنية وسرعة في التنفيذ. ومع ذلك، فإن تطبيقه في الزمن الحقيقي على بيانات VoIP قد يؤثر على مؤشرات الأداء مثل التأخير والتقطيع .كما أن خوارزميات ترميز الصوت تلعب دوراً محورياً في ضغط البيانات وتحسين استخدامها للموارد الشبكية، إلا أن أداءها يتفاوت عند دمجها مع تقنيات التشفير وVPN.

في هذا البحث، تم استخدام بيئة المحاكاة OPNET لنمذجة وتحليل تأثير كل من الشبكات الخاصة الافتراضية، وخوارزمية التشفيرAES، وثلاثة من خوارزميات ترميز الصوت (G.711, G.723.1, G.729) على أداء بروتوكولVoIP ، وأجريت الدراسة على نموذج شبكة كلية الهندسة المعلوماتية بجامعة حمص، بهدف تقييم مؤشرات جودة الخدمة مثل التأخيرمن النهاية الى النهاية، التقطيع، متوسط رأي المستخدم، والإنتاجية. أظهرت النتائج أن تطبيق تقنيات الشبكات الخاصة الافتراضية والتشفير باستخدام خوارزمية AES أدى إلى زيادة في التأخير من النهاية إلى

[1] أستاذ مساعد في قسم هندسة الشبكات والنظم الحاسوبية –كلية الهندسة المعلوماتية–جامعة حمص.

النهاية مقارنة بالسيناريوهات التي لم تُطبق فيها هذه التقنيات، وكان هذا التأثير أكثر وضوحاً مع خوارزمية ترميز G.711 . كذلك، لوحظ تأثير للتشفير على التقطيع، حيث حافظت خوارزمية G.729على استقرار نسبي في هذا الجانب مقارنة بالخوارزميات الأخرى. أما فيما يتعلق بجودة الصوت، فقد أظهرت خوارزمية G.729 أداءً أفضل في السيناريوهات غير المشفرة، بينما انخفض تقييم جودة الصوت عند تفعيل التشفير، خصوصاً مع خوارزمية G.723.1. كما أظهرت البيانات أن التشفير يضيف عبئاً على حجم البيانات المرسلة، مما يؤثر على كفاءة استخدام عرض النطاق الترددي، وخاصة مع خوارزمية G.711. بناءً على نتائج المحاكاة، يُعد ترميز G.729 الخيار الأمثل لشبكة كلية الهندسة المعلوماتية بجامعة حمص، نظراً لتوازنه الفعال بين جودة الصوت وكفاءة الأداء في بيئة مشفرة باستخدام VPN وAES.

الكلمات المفتاح: الشبكات الخاصة الإفتراضية، بروتوكول نقل الصوت عبر الانترنت، خوارزمية التشفير AES، المحاكي أوبنت، خوارزميات ترميز الصوت.

The Impact of Virtual Private Networks, AES Encryption Algorithm, and Voice Codec on VoIP Protocol Performance: A Case Study of the Faculty of Informatics Engineering – Homs University

Dr.Eng Yaman Ghazi*

ABSTRACT

Amid the rapid digital transformation, voice communications over data networks have become an essential component of modern infrastructure. Many institutions now rely on VoIP technologies to provide flexible and cost-effective communication solutions. This technology enables high-quality voice transmission over the Internet, yet remains vulnerable to challenges related to security and performance—particularly in sensitive academic and institutional environments. Among the solutions employed to enhance communication privacy, Virtual Private Networks (VPNs) stand out as an effective means of establishing secure communication channels between parties, reducing the risk of eavesdropping or data manipulation. However, the use of VPNs may introduce additional network overhead, potentially affecting the quality of service delivered via VoIP. In this context, encryption using the AES algorithm is one of the most widely adopted methods for securing voice data during transmission, due to its strong security and fast execution. Nevertheless, applying AES encryption in real-time VoIP traffic may impact performance indicators such as end-to-end delay and jitter.

Voice codecs also play a critical role in compressing data and optimizing network resource usage, though their performance varies when combined with encryption and VPN technologies.

In this study, the OPNET simulation environment was used to model and analyze the impact of VPNs, AES encryption, and three voice codecs (G.711, G.729, G.723.1) on VoIP protocol performance. The evaluation was conducted on a simulated network model of the Faculty of Informatics Engineering at Al-Baath University in Homs, with the aim of assessing key Quality of Service (QoS) metrics such as end-to-end delay, jitter, Mean Opinion Score (MOS), and throughput. The results showed that applying VPN and AES encryption led to an increase in end-to-end delay compared to scenarios without these technologies, with the effect being most pronounced when using the G.711 codec. Encryption also had a noticeable impact on jitter, while the G.729 codec maintained relatively stable

performance in this regard compared to other codecs. In terms of voice quality, G.729 demonstrated superior performance in unencrypted scenarios, whereas voice quality declined when encryption was enabled—particularly with the G.723.1 codec. Additionally, the data revealed that encryption adds overhead to the volume of transmitted data, affecting bandwidth efficiency, especially when using G.711.

Based on the simulation results, the G.729 codec is considered the optimal choice for the network of the Faculty of Informatics Engineering at Al-Baath University, due to its effective balance between voice quality and performance in encrypted environments using VPN and AES.

Keywords: OPNET Simulator, Voice over Internet Protocol, AES Algorithms, Voice Codec, Quality of Service.

*Associate Professor, Department of Systems and Computer Network, Faculty of Informatics Engineering, Homs University.

1. مقدمة:

شهدت تقنيات الاتصالات تطوراً ملحوظاً في العقود الأخيرة، حيث انتقلت من الأنظمة التقليدية المعتمدة على البنية التحتية الهاتفية إلى حلول أكثر مرونة تعتمد على شبكات البيانات. من بين هذه الحلول، يُعد بروتوكول نقل الصوت عبر الإنترنت من أبرز الابتكارات التي غيّرت جذرياً طريقة التواصل الصوتي، إذ يتيح نقل الإشارات الصوتية عبر شبكات الـ IP باستخدام تقنيات ضغط وتشفير متقدمة، مما يوفر بديلاً اقتصادياً وعملياً للاتصالات الهاتفية التقليدية [1].

تكمن أهمية VoIP في قدرته على دمج خدمات الصوت والبيانات ضمن بنية شبكية موحدة، مما يُسهم في تقليل التكاليف التشغيلية، وتبسيط إدارة الشبكات، وتوفير إمكانيات متقدمة مثل الاتصالات متعددة الأطراف، التكامل مع تطبيقات الأعمال، وتوسيع نطاق الوصول إلى خدمات الاتصال في المناطق ذات البنية التحتية المحدودة [2]. وقد أصبح هذا البروتوكول حجر الأساس في العديد من القطاعات، بما في ذلك التعليم، الصحة، والخدمات الحكومية، نظراً لما يقدمه من مرونة وسرعة في نشر الخدمات [3] .

ومع ذلك، فإن اعتماد VoIP لا يخلو من تحديات تقنية تؤثر على جودة الخدمة، خاصة في البيئات التي تتطلب اتصالات زمنية دقيقة مثل المؤتمرات الصوتية أو المكالمات الطارئة. من أبرز هذه التحديات: التأخير الزمني، التقطيع، فقدان الحزم، ومتوسط الرأي الشخصي. وتزداد هذه التحديات تعقيداً عند دمج VoIP مع تقنيات أمنية مثل التشفير باستخدام خوارزمية AES، أو عند تشغيله ضمن الشبكات الخاصة الافتراضية، حيث تؤثر هذه الإضافات على زمن المعالجة وحجم البيانات المنقولة [1].

تلعب خوارزميات ترميز الصوت مثلG.711 ، G.729، و G.723.1 دوراً محورياً في تحديد جودة المكالمة وكفاءة استخدام الموارد الشبكية. فكل خوارزمية تمتلك خصائص مختلفة من حيث معدل الضغط، التأخير الناتج، واستهلاك عرض الحزمة، مما يجعل اختيار الخوارزمية المناسبة عاملاً حاسماً في تصميم أنظمة VoIP فعالة وآمنة [2].

نظراً لتعدد هذه العوامل وتداخلها، تبرز الحاجة إلى دراسة تحليلية دقيقة تعتمد على أدوات محاكاة متقدمة مثل OPNET، والتي تتيح نمذجة الشبكات وتقييم أداء VoIP تحت ظروف مختلفة، بما في ذلك تغيير نوع الترميز، تفعيل التشفير، واستخدام VPN. ومن خلال هذه الدراسة، يمكن

الوصول إلى توصيات تقنية قابلة للتطبيق تُسهم في تحسين جودة الاتصال الصوتي، وتعزيز أمن البيانات، وتحقيق التوازن بين الأداء والكفاءة في بيئات الاتصالات الأكاديمية والمؤسسية [3] .

2. الهدف من البحث:

المساهمة الأساسية لهذا البحث تكمن في تقييم أداء بروتوكول نقل الصوت عبر الإنترنت (VoIP) عند دمج تقنية الشبكات الخاصة الافتراضية مع تشفير البيانات الصوتية باستخدام خوارزمية AES، وذلك بالتزامن مع استخدام ثلاثة من أشهر خوارزميات الترميز الصوتي في نموذج شبكة كلية الهندسة المعلوماتية بجامعة حمص. تم تنفيذ هذا التقييم عبر تضمين تأثير خوارزمية AES ضمن بنية محاكيOPNET ، اعتماداً على المنهجية الموضحة في الدراسة [4]، مع تفعيل الشبكات الخاصة الافتراضية، واختبار خوارزميات الترميزG.711 ، G.729، و G.723.1 في سيناريوهين: الأول مع تفعيل الشبكات الخاصة الافتراضية والتشفير، والثاني بدونهما. جرت المحاكاة ضمن سيناريو شبكي واقعي يعكس البنية التحتية الفعلية للشبكة، شاملاً توزيع العقد، وأنماط حركة البيانات، وتنوع أحمال الشبكة. يهدف هذا التصميم إلى تقديم تقييم دقيق لتأثير الشبكات الخاصة الافتراضية والتشفير على مؤشرات جودة الخدمة مثل التأخيرمن النهاية الى النهاية، التقطيع، متوسط تقييم المستخدم، والإنتاجية، ضمن بيئة محاكاة تعكس الواقع الأكاديمي والتطبيقي بدقة.

3. الشبكات الخاصة الإفتراضية (VPN):

تُعد الشبكات الخاصة الافتراضية (Virtual Private Networks – VPN) من أبرز تقنيات الأمان الشبكي المستخدمة في العصر الرقمي، حيث تتيح إنشاء قناة اتصال مشفّرة وآمنة بين طرفين عبر شبكة. تعتمد الـ VPNعلى إنشاء "نفق افتراضي" يتم من خلاله تمرير البيانات بشكل مشفّر باستخدام بروتوكولات مثل IPSec أوSSL/TLS ، مما يمنع الجهات الخارجية من اعتراض أو تحليل حركة البيانات أثناء انتقالها بين المستخدم والخادم.

تبرز أهمية الـ VPN في عدة جوانب حيوية، أبرزها حماية الخصوصية وتأمين الاتصالات في بيئات غير موثوقة، مثل شبكات Wi–Fi العامة أو الاتصالات عبر الإنترنت المفتوح. كما تُستخدم هذه التقنية على نطاق واسع في المؤسسات لتأمين الوصول عن بُعد إلى الموارد الداخلية، مما

يتيح للموظفين العمل من خارج الموقع دون تعريض بيانات الشركة للخطر. وتُعد الشبكات الخاصة الافتراضية أيضاً أداة فعالة لتجاوز القيود الجغرافية والوصول إلى المحتوى المحجوب، من خلال تغيير عنوان الـ IP الظاهري للمستخدم [4].

من الناحية التقنية، تختلف أنواع الـ VPN حسب طريقة التنفيذ والبروتوكولات المستخدمة، وتشمل : VPN من نوع Site-to-Site، و VPN Remote Access، و VPN Client-Based.

وتتنوع بروتوكولات التشفير بين PPTP، L2TP/IPSec، OpenVPN، و WireGuard، حيث تختلف في مستوى الأمان والأداء والمرونة [5].

في سياق تطبيقاتVOIP، يُمكن أن يؤثر استخدام VPN على جودة الخدمة (QoS) بسبب التأخير الناتج عن التشفير والتغليف، مما يستدعي دراسة دقيقة لتوازن الأمان مقابل الأداء، خاصة عند دمج VPN مع خوارزميات تشفير مثل AES وخوارزميات ترميز الصوت ذات معدلات ضغط مختلفة [6].

4. خوارزمية التشفير AES:

تُعد خوارزمية AES (معيار التشفير المتقدم) من أبرز خوارزميات التشفير الكتلي المتماثل، وقد تم اعتمادها رسمياً من قبل المعهد الوطني الأمريكي للمعايير والتكنولوجيا (NIST) عام 2001 ضمن الوثيقة FIPS PUB 197 ، لتكون بديلاً آمناً وفعالاً عن خوارزمية DES التي لم تعد قادرة على مقاومة الهجمات التحليلية الحديثة. تعتمد AES على معالجة البيانات ضمن كتل ثابتة بطول 128 بت، وتدعم مفاتيح بطول 128، 192، أو 256 بت، مما يتيح مرونة في اختيار مستوى الأمان حسب متطلبات النظام [1].

تتكون عملية التشفير في AES من عدة جولات (10، 12، أو 14 جولة حسب طول المفتاح)، وتُنفذ خلالها أربع عمليات أساسية: استبدال البايتات باستخدام جدول S-box، تدوير الصفوف لإعادة توزيع البيانات، خلط الأعمدة باستخدام عمليات رياضية في حقل غالوا، وأخيراً دمج المفتاح الفرعي عبر عملية XOR. هذه البنية تضمن تحقيق خاصيتي الانتشار والارتباك، مما يعزز مقاومة الخوارزمية للهجمات التفاضلية والخطية [7].

في تطبيقات الزمن الحقيقي مثل نقل الصوت عبر بروتوكول الإنترنت (VoIP)، يُعد دمجAES تحدياً تقنياً يتطلب دراسة دقيقة لتأثير التشفير على مؤشرات جودة الخدمة . فبينما توفر AES

حماية قوية للبيانات الصوتية، فإن عمليات التشفير وفك التشفير قد تؤدي إلى زيادة زمن التأخير، تفاوت توقيت الحزم، واحتمالية فقدان الحزم، خاصة في البيئات ذات الموارد المحدودة أو عند استخدام خوارزميات ترميز صوتي مضغوطة.

5. خوارزميات ترميز الصوت:

الكلمة codec هي اختصار لـ compressor-decompressor أو كما هو شائع أكثر coder-decoder (ترميز (ضغط) وفك الترميز (فك الضغط)) الإشارة الصوتية إلى بتات رقمية لكي تستخدم من قبل شبكات الحاسب. تُعرف تراميز الصوت (Audio Codecs) بأنها خوارزميات أو برامج تُستخدم لتحويل الإشارة الصوتية التناظرية إلى صيغة رقمية قابلة للنقل عبر شبكات البيانات، ومن ثم إعادة تحويلها إلى شكلها الأصلي عند الطرف المستقبل. وتُعد هذه العملية أساسية في تقنيات الاتصال الحديثة، خاصة في تطبيقات نقل الصوت عبر الإنترنت، حيث تُستخدم التراميز لضغط البيانات الصوتية وتقليل حجمها دون التأثير الكبير على الجودة، مما يساهم في تحسين كفاءة النقل وتقليل استهلاك عرض الحزمة [8]. تكمن أهمية تراميز الصوت في قدرتها على تحقيق التوازن بين جودة الصوت وكفاءة استخدام الموارد الشبكية، خاصة في البيئات التي تعاني من محدودية النطاق الترددي أو تقلبات في الأداء الشبكي. كما أن اختيار الترميز المناسب يؤثر بشكل مباشر على مؤشرات جودة الخدمة، مما يجعلها عنصراً حاسماً في تصميم أنظمة VoIP فعالة وموثوقة. الهدف من استخدام تراميز الصوت لا يقتصر على ضغط البيانات، بل يشمل أيضاً تحسين تجربة المستخدم، ضمان التوافق بين الأجهزة والبروتوكولات، وتوفير أداء مستقر في بيئات متنوعة مثل الشبكات اللاسلكية، شبكات VPN، أو الأنظمة المشفرة. تتنوع تراميز الصوت من حيث آلية الضغط، معدل البت، وجودة الصوت الناتجة، التراميز التي تغطيها هذه الدراسة:

ITU-T G.711:

يُعد هذا المعيار من أقدم وأهم خوارزميات ترميز الصوت المستخدمة في شبكات الاتصالات الرقمية، وقد تم اعتماده من قبل الاتحاد الدولي للاتصالات عام 1972. يعتمد هذا المعيار على تقنية الترميز النبضي المعدل (Pulse Code Modulation - PCM) لتحويل الإشارة الصوتية التناظرية إلى صيغة رقمية بمعدل نقل ثابت يبلغ 64 كيلوبت/ثانية، دون تطبيق ضغط

فعلي على البيانات. ويُستخدم نوعان من الضغط غير الخطي ضمن هذا المعيار μ-law : في أمريكا الشمالية و A-law في أوروبا، بهدف تحسين نسبة الإشارة إلى الضوضاء في الإشارات منخفضة السعة. رغم أن G.711 لا يُعد فعالاً من حيث تقليل حجم البيانات مقارنةً بتراميز حديثة مثل G.729 أوOpus ، إلا أنه يتميز بـ زمن تأخير منخفض جداً، وبساطة في التنفيذ، وتوافق واسع مع بروتوكولات VoIP مثل SIP وH.323، مما يجعله خياراً مثالياً في البيئات التي تتطلب جودة صوت عالية واستجابة زمنية فورية [9].

ITU-T G.729:

يُعد هذا المعيار من أكثر خوارزميات ترميز الصوت استخداماً في تطبيقات نقل الصوت عبر الإنترنت(VoIP) ، خاصة في البيئات التي تعاني من محدودية عرض الحزمة. تم اعتماد هذا المعيار من قبل الاتحاد الدولي للاتصالات عام 1996، ويعتمد على تقنية الترميز الخطي المثير بالرمز الجبري (CS-ACELP) لضغط الإشارة الصوتية إلى معدل منخفض يبلغ 8كيلوبت/ثانية [10]، مع الحفاظ على جودة صوت مقبولة للاستخدام العملي. يتكون G.729 من إطارات صوتية بطول 10 ميلي ثانية، ويُنفذ باستخدام خوارزميات ذات تعقيد متوسط إلى مرتفع، مما يجعله مناسباً للأنظمة التي تتطلب كفاءة في استخدام الموارد الشبكية دون التضحية الكبيرة بجودة الصوت. وقد تم تطوير عدة امتدادات لهذا المعيار، مثل G.729A الذي يتميز بتعقيد أقل مع جودة صوت أقل قليلاً، و G.729B الذي يضيف ميزة كتم الصوت (Silence Suppression)، و G.729.1 الذي يوسّع النطاق إلى الصوت العريض باستخدام طبقات ترميز قابلة للتدرج [11].

ITU-T G.723.1:

يُعد هذا المعيار من أبرز خوارزميات ترميز الصوت التي تم تطويرها لدعم خدمات الوسائط المتعددة عبر الشبكات ذات النطاق المحدود، خاصة ضمن إطار عائلة H.324 للاتصالات متعددة الوسائط. تم اعتماده من قبل الاتحاد الدولي للاتصالات (ITU–T) عام 1996، ويعمل بمعدلَي بت منخفضين 5.3 :كيلوبت/ثانية باستخدام خوارزمية ACELP، و 6.3 كيلوبت/ثانية باستخدام خوارزمية MP–MLQ، مما يوفر مرونة في التوازن بين جودة الصوت وكفاءة استخدام الموارد. يعتمد G.723.1 على تقنية التحليل التنبؤي الخطي مع الترميز التحفيزي (LPC–

(ABS، ويقوم بضغط الإشارة الصوتية إلى إطارات بطول 30 ميلي ثانية، مما يجعله مناسباً لتطبيقات مثل مؤتمرات الفيديو، VoIP، والاتصالات عبر الأقمار الصناعية. كما يتضمن ميزات متقدمة مثل كشف النشاط الصوتي (VAD) وضغط الصمت (Silence Compression)، مما يساهم في تقليل استهلاك عرض الحزمة أثناء فترات عدم الكلام [11].

يعرض الجدول (1) أهم خصائص التراميز الصوتية الثلاثة المدروسة.

الجدول (1): خصائص التراميز الصوتية المدروسة [9]

الخاصية	G.711	G.729	G.723.1
معدل البت	64 kbps	8 kbps	5.3 / 6.3 kbps
جودة الصوت	عالية جداً	جيدة	متوسطة
التأخير	منخفض جداً	متوسط	مرتفع
استهلاك الحزمة	مرتفع	منخفض	منخفض جداً
تعقيد الترميز	بسيط	متوسط	مرتفع
الاستخدام الأمثل	LAN	VoIP / WAN	VoIPمنخفض النطاق

6. الدراسات السابقة:

المرجع	شرح الدراسة
Hazzaa et al (2024) [12]	في دراسة حديثة تم تحليل أداء خوارزمية AES عند تطبيقها على بيانات صوتية متنوعة، بهدف تقييم كفاءتها في بيئات اتصالات متعددة. اعتمد الباحثون على مجموعة من مؤشرات الأداء، شملت زمن التشفير وفك التشفير، استهلاك المعالج، الطاقة المستهلكة، ومعدل الإنتاجية. أظهرت النتائج أن AES حافظت على أداء مستقر عبر الأنماط المختلفة، دون تأثيرات كبيرة على زمن الاستجابة أو كفاءة النظام، مما يعزز موثوقيتها في تطبيقات الصوت المشفر. كما ناقشت الدراسة تحديات إدارة المفاتيح وتكامل الخوارزمية مع المنصات البرمجية والعتادية، وأوصت بتطوير حلول أكثر تكيفاً مع متطلبات الاتصالات الحديثة.

Talha et al (2013) [13]	في هذه الدراسة تم تحليل أثر تطبيق خوارزمية التشفير المتقدمة AES على أداء نظم نقل الصوت عبر بروتوكول الإنترنت. ركزت الدراسة على قياس تأثير عمليات التشفير وفك التشفير على مؤشرات الأداء الأساسية مثل زمن الاستجابة، جودة الخدمة (QoS)، واستهلاك الموارد .أظهرت النتائج أن تطبيق AES يوفر مستوىً عالياً من السرية، لكنه يؤدي إلى زيادة طفيفة في زمن المعالجة وتأخير المكالمات، مما قد يؤثر على تجربة المستخدم في البيئات الحساسة للزمن .ومع ذلك، اعتبرت الدراسة أن هذا التأثير يقع ضمن الحدود المقبولة، وأوصت باستخدام AES في تطبيقات VoIP مع مراعاة التوازن بين الأمان والأداء.
Rahman & Chowdhury (2023) [14]	قارنت بين خوارزميتي AES و ChaCha20 في تأمينVoIP ، ووجدت أن AES أكثر كفاءة في البيئات ذات الموارد المحدودة، بينما توفر ChaCha20 أداءً أعلى في الأنظمة الحديثة. الدراسة استخدمت اختبارات زمنية وتحليل جودة الصوت.
Nugraha et al [15]	تهدف هذه الدراسة إلى تأمين نقل البيانات الصوتية عبر الشبكات باستخدام خوارزمية AES−128 ، مع التحكم في عملية التشفير عبر مفتاح سري. تم تضمين تقنيات إضافية مثل Forward Error Correction (FEC) و Interleaving لتحسين جودة الإشارة وتقليل تأثير الضوضاء أثناء الإرسال اللاسلكي. استخدمت الدراسة مؤشرات مثل زمن التنفيذ، حجم الملف، وقيمة SNR لتقييم الأداء، وأظهرت النتائج أن النظام المقترح يحقق تشفيراً فعالاً مع الحفاظ على جودة الصوت، خاصة عند استخدام مرشح بمتوسط 400.Hz.
Ghazi et al [16]	تحلل هذه الدراسة شبكة كلية الهندسة المعلوماتية في جامعة حمص لاختبار إمكانية إضافة خدمة نقل الصوت عبر الإنترنت. تم في البداية

	محاكاة الشبكة بدون خدمة VoIP، ثم أضيفت الخدمة وقيم الأداء باستخدام ثلاثة تراميزات صوتية، أظهرت النتائج أن G.711 يتفوق في جودة الصوت، التأخير، والتقطيع، بينما G.723.1 يتفوق في الإنتاجية واستهلاك عرض الحزمة، و G.729A يشغل موقعاً متوسطاً بينهما. توضح الدراسة أن اختيار الترميز يعتمد على حالة الشبكة وسرعة الوصلات، وتوصي باستخدام G.711 للاتصالات داخل الشبكة الداخلية للكلية أو الجامعة، بينما يُفضل استخدام G.729 أو G.723.1 للمكالمات الصوتية الخارجية.
Ghazi [17]	تلخص الدراسة تأثير دمج تشفير AES مع ثلاث خوارزميات ترميز صوتي G.711، G.729، G.723.1 على جودة خدمة VoIP في بيئة محاكاة لشبكة كلية الهندسة بجامعة حمص. أظهرت النتائج أن G.711 مع التشفير يوفر أعلى جودة صوت لكنه يعاني من تأخير وتقطيع مرتفعين، ما يجعله مناسباً للتطبيقات التي تحتاج إلى وضوح وسرية مع توفر سعة شبكية كافية .أما G.729 بدون تشفير، فقد تفوق في الأداء الزمني بفضل أقل تأخير وتقطيع، مما يجعله خياراً جيداً للبيئات التعليمية التي تتطلب استجابة سريعة واستقرار، رغم جودة صوت أقل . بينما قدمت G.723 أداءً متوسطاً يجعلها خياراً مرناً للبيئات ذات الموارد المحدودة .الدراسة تؤكد أهمية الموازنة بين الأمان والأداء واختيار التكوين المناسب بناءً على طبيعة الاستخدام.
Timilehin (2024) [18]	تستعرض الدراسة التحديات الأمنية التي تواجه أنظمة VoIP المدمجة، والتي تجمع بين خدمات الصوت والبيانات في بنية شبكية واحدة. تشير الدراسة إلى أن التحول من الشبكات التقليدية إلى شبكات VoIP يزيد من مخاطر مثل التنصت، وهجمات حجب الخدمة، وهجمات الرجل في المنتصف، والاحتيال الصوتي. وتوصي الدراسة بتطبيق استراتيجيات أمنية متقدمة تشمل التشفير الكامل، المصادقة القوية،

	الكشف عن التهديدات باستخدام الذكاء الاصطناعي، واعتماد نموذج "الثقة الصفرية". كما تناقش دور تقنيات مثل البلوك تشين والتشفير الكمي في تعزيز أمن الاتصالات الصوتية عبر الإنترنت
Michael (2020) [19]	تناولت الدراسة تأثير استخدام بروتوكول IPSec VPN على أداء شبكات VoIP، باستخدام محاكاة عبر المحاكي OPNET. أظهرت النتائج أن إضافة طبقة الأمان عبر IPSec تؤدي إلى زيادة طفيفة في التأخير والاهتزاز، لكنها لا تؤثر بشكل كبير على جودة الخدمة الصوتية .خلصت الدراسة إلى أن استخدام IPSec يعزز الأمان دون التأثير السلبي الملحوظ على أداء VoIP، مما يجعله خياراً مناسباً للشبكات التي تتطلب حماية عالية للاتصالات.
Hassan et al. (2021) [20]	قدمت نموذجاً هجيناً لتحليل أداء VoIP باستخدام OPNET، وركزت على دمج تقنيات QoS والتشفير في بيئات متعددة البروتوكولات. الدراسة أظهرت أن التصميم الشبكي يلعب دوراً حاسماً في تحسين الأداء.
Ali et al. (2021) [21]	اقترحت خوارزمية لاختيار البروتوكول الأمثل لشبكات WLAN في تطبيقات VoIP، بناءً على تحليل الأداء والتأخير وفقدان الحزم. الدراسة دعمت استخدام بروتوكولات مثل IEEE 802.11ac لتحقيق أفضل أداء.
Chakraborty & Telgote (2018) [22]	استخدمت OPNET لتحليل أداء VoIP عبر طوبولوجيات مختلفة LAN، MAN، WAN، WLAN، وخلصت إلى أن تصميم الشبكة يؤثر بشكل مباشر على جودة المكالمات، خاصة عند استخدام VPN والتشفير.

بالنظر الى جميع الدراسات السابقة يظهر أنه من الضرورة بمكان دراسة تأثير تطبيق كل الشبكات الخاصة الإفتراضية على جودة الخدمة لبروتوكول نقل الصوت عبر الإنترنت بعد تطبيق التشفير

بإستخدام خوارزمية AES في نموذج شبكي واقعي وبالتالي يعتبر هذا البحث إمتداد للدراسة المرجعية [16] و [17].

7. محاكي الشبكات أوبنت:

يُعد محاكي الشبكات OPNET (Optimized Network Engineering Tools) من أبرز أدوات المحاكاة المستخدمة في تحليل وتصميم الشبكات الحاسوبية، وقد طُوّر لأول مرة عام 1986 وأصبح منصة متكاملة قادرة على محاكاة شبكات الاتصال الكبيرة والمعقدة بنمذجة دقيقة للبروتوكولات، الأجهزة، التطبيقات، والأداء [23]. يتميز OPNET بواجهاته الرسومية القوية، ودعم جدولة الأحداث الديناميكية، وأدوات التحليل المتكاملة، مما يمكّن الباحثين من إنشاء نماذج شبكية واقعية تحاكي سلوك الشبكات تحت ظروف متعددة دون الحاجة إلى بنية تحتية فعلية، الأمر الذي يقلل التكاليف ويزيد من مرونة التجارب.

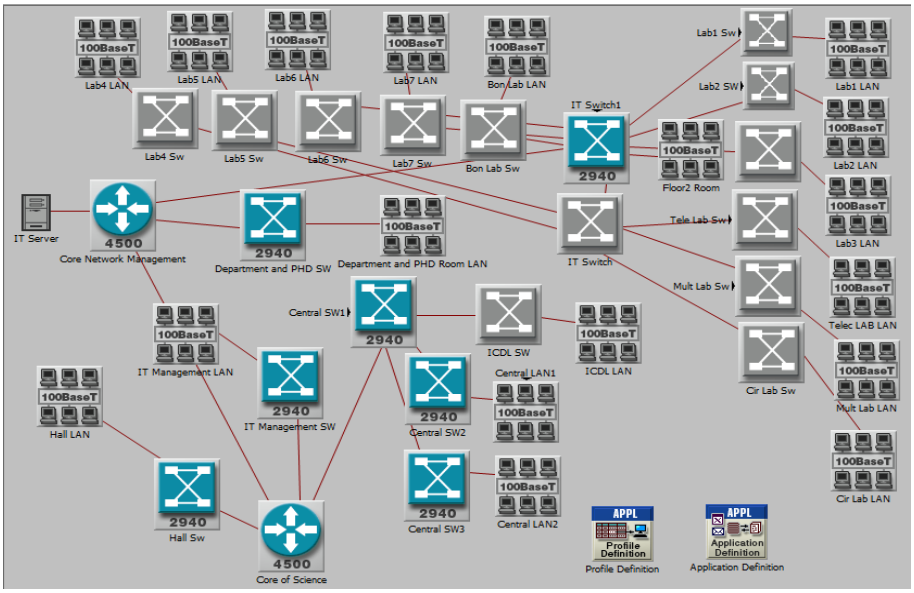
يستخدم OPNET على نطاق واسع في الدراسات الأكاديمية والتطبيقية، خاصة في تحليل أداء بروتوكولاتVoIP مع دمجه مع بوتوكولات وتقنيات أخرى وفي بيئات مختلفة، حيث يسمح بالتحكم الكامل في إعدادات الشبكة وتخصيص خصائص الأجهزة والتطبيقات[24] . كما يدعم لغات البرمجة Proto-C و C لتوسيع إمكانيات المحاكاة، ويمتلك مكتبة واسعة من النماذج الجاهزة التي يمكن تعديلها لتتناسب مع متطلبات البحث.

في هذا البحث، تم اختيار إصدار OPNET Modeler 14.5 لما له من دعم مميز لبروتوكول نقل الصوت عبر الإنترنت وخوارزميات ترميز الكلام، بالإضافة إلى سهولة استخدام واجهته الرسومية وقدرته على عرض النتائج بشكل رسومي واضح، مما يجعله ملائماً لنمذجة شبكة كلية الهندسة المعلوماتية بجامعة حمص، مع إمكانية تخصيص البنية الشبكية وتطبيق سيناريوهات متعددة تشمل بروتوكولات VoIP وخوارزميات التشفيرAES، والشبكات الخاصة الافتراضية، وهو ما يعزز موثوقية النتائج ويوفر توصيات عملية للتطبيق في بيئات أكاديمية ومؤسسية مماثلة.

8. التطبيق العملي:

في هذه الدراسة سوف يتم تحليل أداء بروتوكول نقل الصوت عبر الإنترنت بإستخدام مجموعة خوارزميات الترميز الثلاثة المدروسة مع تطبيق كل من خوارزمية التشفير AES والشبكات

الخاصة الأفتراضية ودون تفعيلهما وذلك في نموذج شبكة كلية الهندسة المعلوماتية بجامعة حمص. في البداية سوف نذكر بتوصيف نموذج شبكة كلية الهندسة المعلوماتية في جامعة حمص كما تم توصيفه سابقاً في الدراسة [25] والدراسة [17] قبل إضافة خوارزمية التشفير AES والشبكات الخاصة الإفتراضية.



الشكل (1): الطوبولوجيا الشبكية الداخلية لشبكة كلية الهندسة المعلوماتية بجامعة حمص

حيث أن شبكة كلية الهندسة المعلوماتية بجامعة حمص تتوزع على ثلاثة طوابق في الطابق الأول تتوضع المكاتب الإدارية (العميد – سكرتاريا العميد – نواب العميد – محاسب الرواتب – رئيس الدائرة – الذاتية – شؤون الطلاب العام – شؤون الطلاب الموازي – الديوان – الامتحانات – قاعة السمنار – التصوير – معتمد الرسوم) بالإضافة إلى المخبر المركزي الذي يحتوي على شبكة مكونة من 100 جهاز حاسوب ومخبر علوم الحاسب والقاعات حيث أن جميع تجهيزات هذا الطابق تتصل شبكياً بالمبدلة الرئيسية في كلية العلوم التي تتوضع في الطابق الأرضي لكلية العلوم والتي تتصل بدورها بالمبدلة الرئيسية الأخرى الموجودة في غرفة إدارة الشبكة في الطابق الثاني. أما بالنسبة للطابق الثاني فيحتوي على بعض الغرف الإدارية (المكتبة – المخبرين – مراقب الدوام – الدراسات العليا) والمخابر (1–2–3– الوسائط المتعددة – الاتصالات – الدارات)

التي تتصل جميعها بالمبدلتين IT_Switch و IT_Switch1 الموجودتين في نفس الطابق والتي تتصل احداهما بشكل مباشر مع المبدلة الرئيسية في غرفة إدارة الشبكة في نفس الطابق، وفي الطرف الأخر يوجد بعض الغرف الإدارية التي تخص أعضاء الهيئة التدريسية وغرفة أعضاء الهيئة الفنية والأقسام والسكرتارية الخاصة بهم وجميعها تتصل بالمبدلة Department and PHD SW التي تتصل بدورها بالمبدلة الرئيسية في غرفة إدارة الشبكة. أما الطابق الثالث يحتوي على المخابر (البنيان – 4 – 5 – 6 – 7) والتي تتصل جميعها بالمبدلتين IT_Switch و IT_Switch1 الموجودتين في الطابق الثاني. يبين الشكل (1) الطوبولوجيا الشبكية لكلية الهندسة المعلوماتية بجامعة حمص. كما يجمع الجدول (2) كافة التجهيزات الشبكية الخاصة بكلية الهندسة المعلوماتية. حيث تم استخدام المكون BaseT_LAN100 الموجود ضمن المحاكي أوبنت للتعبير عن الشبكات الداخلية للمكاتب الإدارية والمخابر والقاعات وغيرها بحيث تم ضبط عدد الأجهزة ضمنها باستخدام الخاصية (Number of Workstations). كما تم تعريف ستة أنواع من الحمل في هذه الشبكة كما هو مبين في الجدول (3)، وتم ضبط استخدام الأنواع الستة من الحمل في عقدة المخدم الخاصة بالكلية كما هو مبين في الشكل (2) والمتوضع في غرفة إدارة الشبكة من خلال ضبط قيمة الخاصية Supported Services. بالنسبة لسرعة الكابلات فإن جميع سرع الكابلات المستخدمة في الشبكات الداخلية الفرعية (داخل كل من المخابر والقاعات والمكاتب الإدارية والوصلات بين مبدلات المخابر (الغير قابلة للإدارة) والمبدلات الرئيسية في الطوابق والوصلات بين المبدلة الرئيسية في المخبر المركزي والمبدلات الأخرى داخله) هي 100 ميغابت في الثانية، أما بالنسبة للكابلات التي تربط بين المبدلات الرئيسية (التي من النوع سيسكو 2940) في الطوابق والمبدلتين الرئيسيتين (من النوع سيسكو 4500) في كلية العلوم وفي إدارة الشبكة هي من النوع فايبر بسرعة 1000 ميغابت في الثانية.

تم تعريف اثنان من البروفايل كما هو مبين في الشكل (3) الأول عام باسم (General Profile) يعمل بالتطبيقات الستة السابقة يتم استخدامه في أجهزة كل من المكاتب الإدارية وغرف أعضاء الهيئة التدريسية والفنية والأقسام ومخبر علوم الحاسب والمخبر المركزي، والثاني محدود باسم (Lab Profile) يعمل بثلاثة من التطبيقات فقط (نقل الملفات – تصفح الويب – الحمل الصوتي) تعمل بشكل متزامن مع بعضها ويتم استخدامه في أجهزة المخابر جميعها وفي القاعات. حيث أن

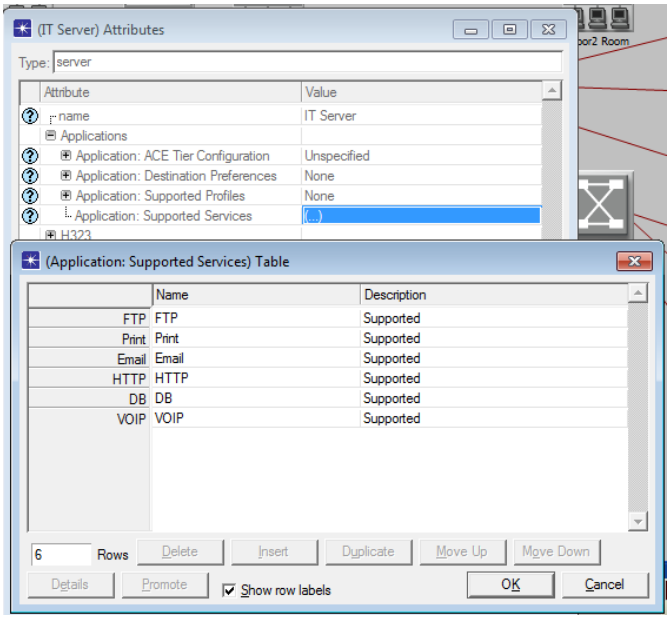
كلاهما يبدئان بالعمل عند الثانية 100 من بدء المحاكاة وينتهيان عند انتهاء زمن المحاكاة. تم ضبط استخدام كل من البروفايل الأول والثاني في العقد BaseT_LAN100 من خلال ضبط قيمة الخاصية Supported Profile.

الجدول (2): تجميع التجهيزات الشبكية الخاصة بكلية الهندسة المعلوماتية

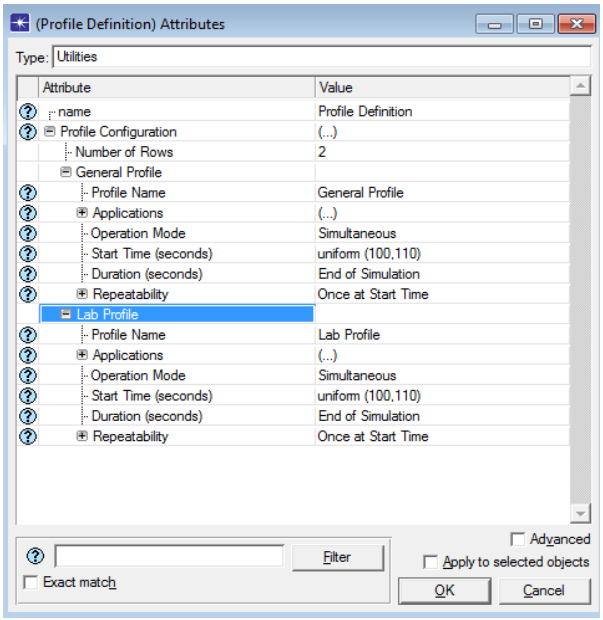
التجهيز الشبكية	العدد
النقاط الشبكية	338
مبدلة بـ 24 منفذ قابلة للإدارة	5
مبدلة بـ 48 منفذ قابلة للإدارة	2
مبدلة بـ 24 منفذ غير قابلة للإدارة	13
مبدلة شبكية مركزية من النوع سيكسو 4500	2
مخدم تطبيقات	1
أجهزة حواسيب	325
طابعة شبكية	1

الجدول (3): التطبيقات المستخدمة في الشبكة

اسم التطبيق	نوع الحمل
نقل الملفات (FTP)	عالي
طباعة (Print)	متوسط
بريد الكتروني ((Email (POP 3 , SMTP	ملفات نصية
قواعد بيانات (Database)	متوسط
تصفح مواقع الويب والتحميل (HTTPs)	عالي جداً
الحمل الصوتي (VOIP)	متوسط

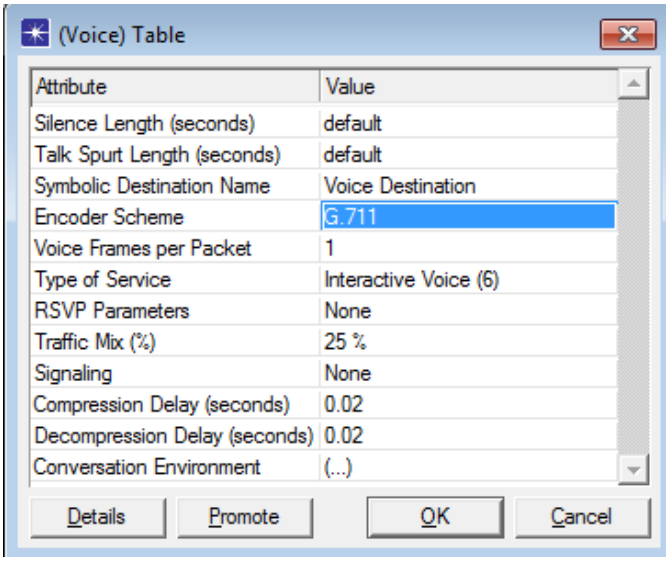


الشكل (2): ضبط الخاصية Supported Services في عقدة المخدم

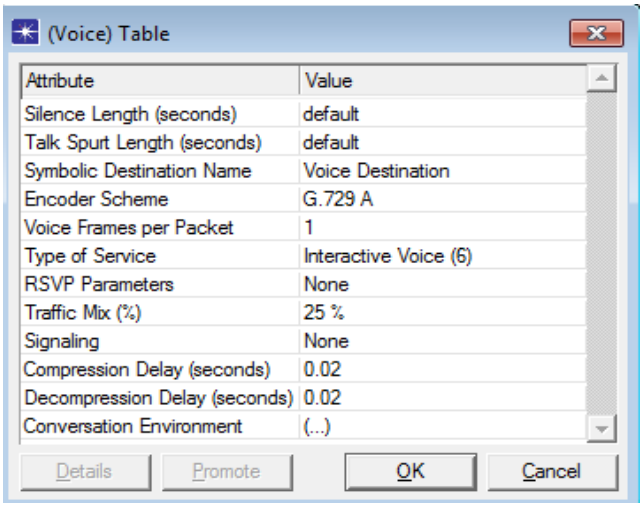


الشكل (3): اعدادات المحاكاة للمكون Profile Config

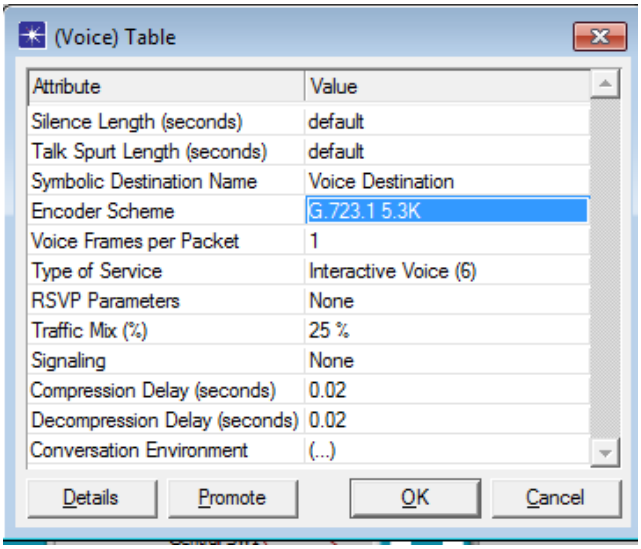
تم تطبيق كل خوارزمية من خوارزميات الترميز الثلاثة على حدا في سيناريو مستقل حيث تم ضبط اعدادات كل منها بالإعدادات التالية (عدد الإطارات الصوتية في الحزمة هو إطار واحد، تأخير الضغط وفكك الضغط هو 20 ميلي ثانية لكل منهما) كما هو مبين في الأشكال (4) (5) (6) للترامیز G.711، G.729، G.723.1 على الترتيب.



الشكل (4): اعدادات خوارزمية G.711 في المحاكي أوبنت

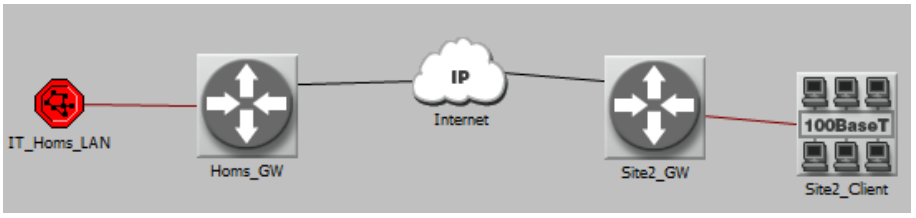


الشكل (5): اعدادات خوارزمية G.729 في المحاكي أوبنت



الشكل (6): اعدادات خوارزمية G.723.1 في المحاكي أوبنت

وقبل إضافة كل من الشبكات الخاصة الإفتراضية ومحاكاة تأثير التشفير باستخدام خوارزمية الـ AES الى الشبكة المدروسة سنقوم بتوسيع الشبكة السابقة وذلك لأن معظم استخدامات الشبكات الخاصة الإفتراضية تكون مع الاتصالات من خارج الشبكة، يبين الشكل (7) توسيع الشبكة المدروسة حيث إن الشبكة الفرعية IT_Homs_LAN تشكل الشبكة الداخلية للكلية التي تم توصيفها سابقاً، والوصلة بين موجه الجامعة والمكون IP Cloud من النوع PPP_DS3 تعمل بسرعة 44.736 ميغابت في الثانية أما الوصلة الثانية بين IP Cloud والطرف الموجه الخارجي فهي من النوع PPP_DS1 وتعمل بسرعة (1.54) ميغابت في الثانية وتم تطبيق تأخير في العقدة IP IP Cloud تم اعداده كتوزيع طبيعي (Normal distribution) خصائصه N(0.175,0.001)(بالثانية). وتم ضبط عدد الأجهزة في المكون Site2_Client بـ 20.



الشكل (7): الطوبولوجيا المدروسة بعد التوسيع

ومن ثم سوف نقوم بمحاكاة أثر اضافة الخوارزمية AES لتشفير البيانات الصوتية كما تم الإشارة اليه في دراسة سابقة [17] دون تنفيذ التشفير فعلياً من خلال الخطوات التالية:

لتحقيق ذلك، تم تعديل خصائص تطبيق VoIP داخل مكون **Application Configuration** لمحاكاة التأثير الزمني والحسابي الناتج عن استخدام خوارزمية AES، وتحديداً نمط **AES-256** الذي يُعد الأكثر تعقيداً من حيث المعالجة.

خطوات محاكاة إضافة تأثير التشفير:

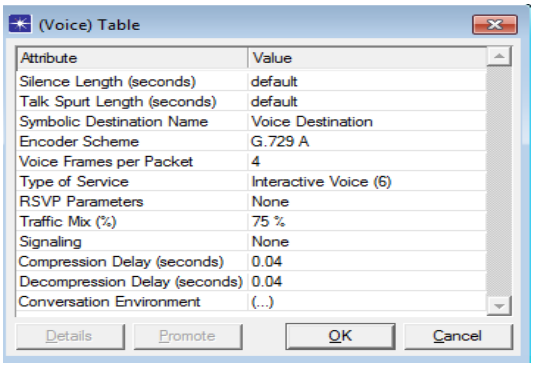
1- **تعديل الخاصية Voice Frames per Packet** تم رفع القيمة من 1 إلى 4، مما يزيد من حجم الحزمة الصوتية ويعكس تأثير التشفير على البيانات المنقولة.

2- **زيادة قيمة Compression Delay** تم ضبط التأخير إلى **4 ميلي ثانية** لمحاكاة زمن التشفير في طرف الإرسال.

3- **زيادة قيمة Decompression Delay** تم ضبط التأخير إلى **4 ميلي ثانية** لمحاكاة زمن فك التشفير في طرف الاستقبال.

4- **تعديل نمط Traffic Mix** تم اختيار نمط **75%** بدلاً من 25% لمحاكاة بيئة ذات حمل شبكي مرتفع، يعكس الضغط الناتج عن التشفير.

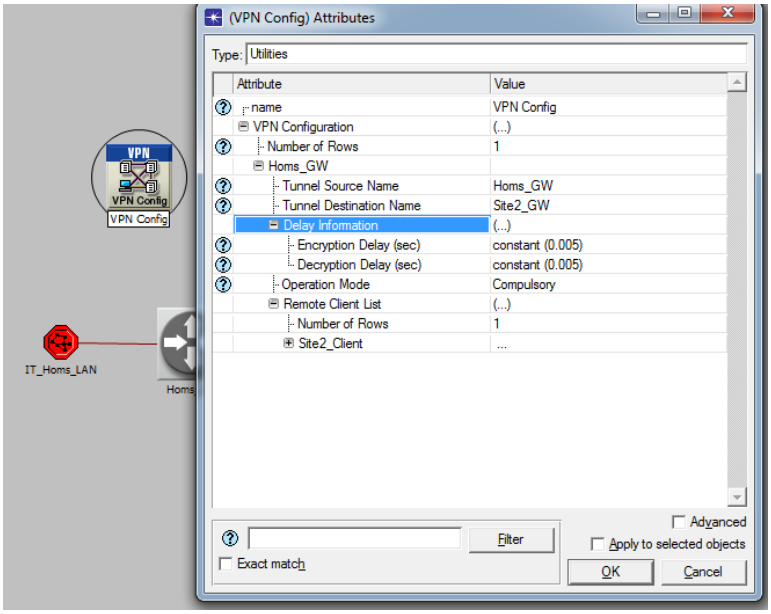
يظهر الشكل (8) التعديلات المقترحة على تطبيق الـ VOIP لمحاكاة أثر اضافة التشفير باستخدام الخوارزمية AES لأحد الترامیز الصوتية وليكن G.729 ونكرر نفس العلمية للترميز G.711 و الترميز G.723.1.



الشكل (8): تعديل الاعدادات الصوتية لمحاكاة أثر اضافة التشفير باستخدام AES على الترميز G.729

والأن سوف نقوم بإعداد الشبكات الخاصة الإفتراضية:

أولاً نقوم بإضافة المكون IP_VPN_Config الى الشبكة ونقوم بتفعيله بالإعدادات التالية والموضحة في الشكل (9) حيث تم ضبط قيمة الخاصية Encryption Delay والخاصية Decryption Delay بالقيمة 0.005 لمحاكاة تأثير استخدام الخوارزمية AES_256 في بناء النفق.

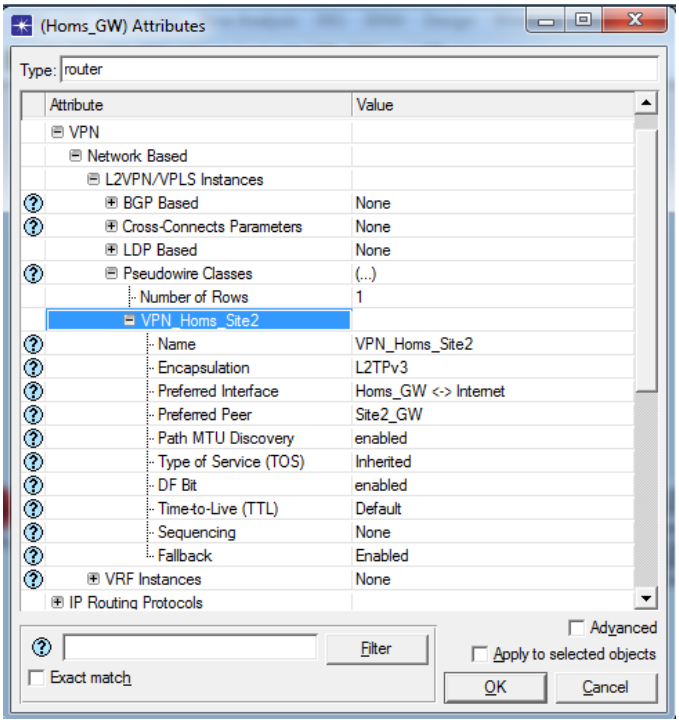


الشكل (9): اعدادات المكون VPN_Config

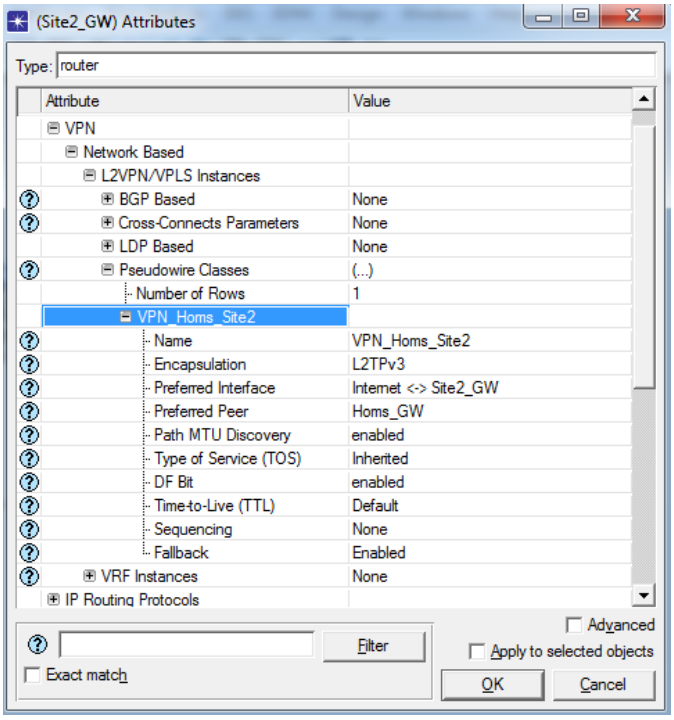
ومن ثم سوف نضبط اعدادات الـ VPN في كل من الموجه Homs_GW والموجه Site2_GW بالاعدادات المبينة في الشكل (10) و (11) على الترتيب، حيث تم ضبط جميع الخصائص في الخاصية Pseudowire Classess بشكل متناظر بين الموجهين مثل نوع التغليف، الوصلة المستخدمة، والطرف الأخر وغيرها.

في المجمل حصلنا على ستة سيناريوهات، لكل خوارزمية ترميز صوتي سيناريو مع تطبيق خوارزمية التشفير AES والشبكات الخاصة الإفتراضية وأخر دون تطبيقهما، وتم قياس كل من القيم التالية لبروتوكول نقل الصوت عبر الإنترنت (متوسط الرأي الشخصي، التقطيع، التأخير من

النهاية الى النهاية، الحمل المستلم)، بالإضافة الى الانتاجية للوصلة الخارجية بين Site2_GW والعقدة IP Cloud بواسطة المحاكي أوبنت وبزمن محاكاة مقداره 10 دقائق لكل سيناريو.



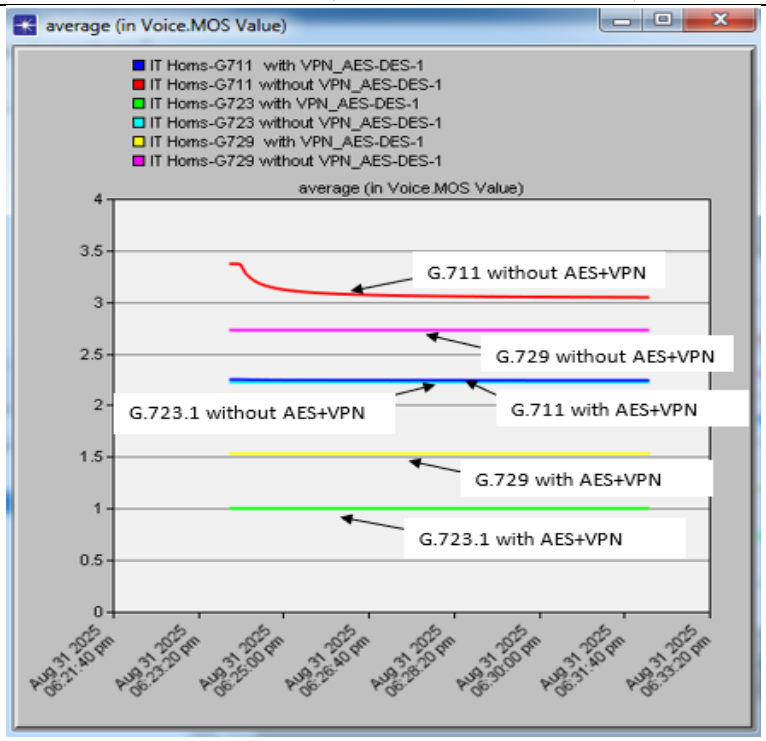
الشكل (10): اعدادات الـ VPN على الموجه Homs_GW



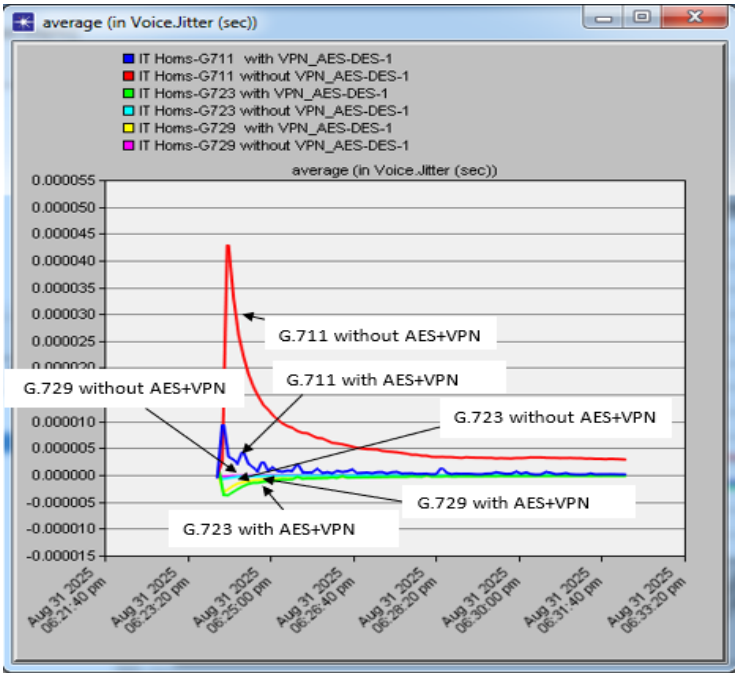
الشكل (11): اعدادات الـ VPN على الموجه Site2_GW

9. النتائج والمناقشة:

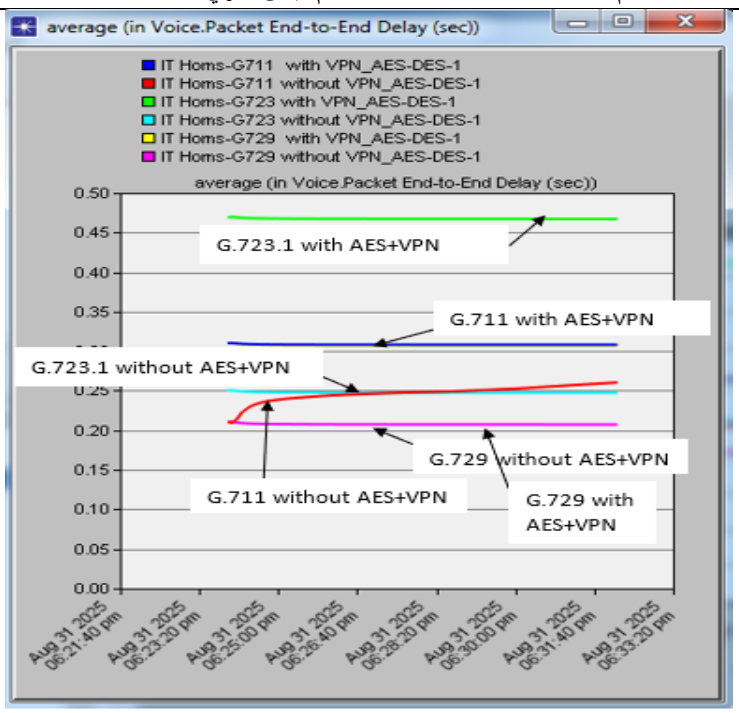
تظهر الأشكال (12) (13) (14) (15) نتائج تنفيذ المحاكاة للسيناريوهات الستة المدروسة حيث تظهر كل من متوسط كل من الرأي الشخصي، التقطيع، التأخير من النهاية الى نهاية، والحمل المستلم لبروتوكول الـ VOIP على الترتيب، كما يظهر الشكل (16) متوسط قيمة الإنتاجية للوصلة الخارجية بين Site2_GW و العقدة IP Cloud.



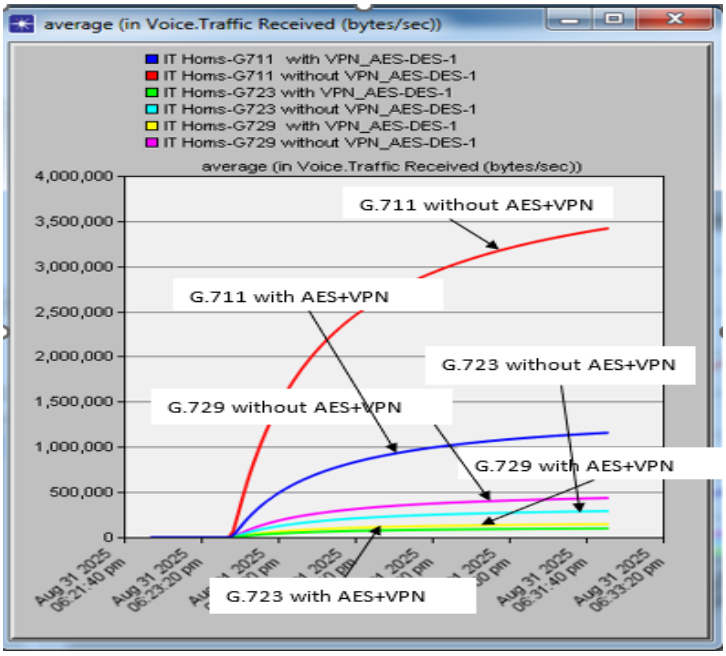
الشكل (12): متوسط الرأي الشخصي لبروتوكول VOIP في سيناريوهات المحاكاة الستة



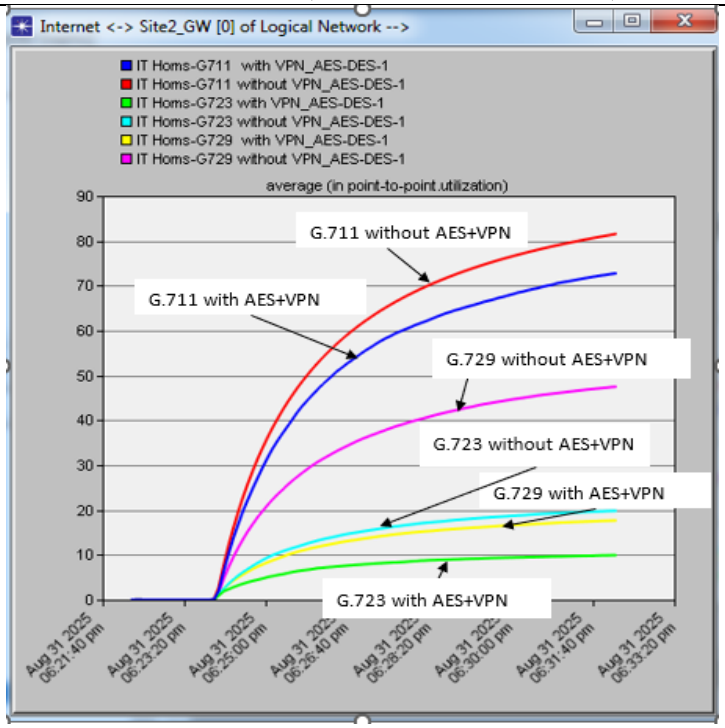
الشكل (13): متوسط التقطيع لبروتوكول VOIP في سيناريوهات المحاكاة الستة



الشكل (14): متوسط التأخير من النهاية الى نهاية لبروتوكول VOIP في سيناريوهات المحاكاة الستة



الشكل (15): متوسط الحمل المستلم لبروتوكول VOIP في سيناريوهات المحاكاة الستة



الشكل (16): متوسط الإنتاجية لكافة التطبيقات على الوصلة الخارجية بين Site2_GW و IP Cloud في سيناريوهات المحاكاة الستة

قراءة النتائج والمخططات البيانية:

متوسط التأخير من النهاية إلى النهاية (End-to-End Delay) :

- أظهرت النتائج أن خوارزمية G.723 سجلت أعلى تأخير عند تفعيل VPN وAES، حيث تجاوزت القيمة 0.45 ثانية، مقارنة بـ 0.30 ثانية بدون التشفير.
- خوارزمية G.729 أظهرت أداءً أكثر استقراراً، حيث بلغ التأخير حوالي 0.15 ثانية مع التشفير، و 0.10 ثانية بدونه.
- أما G.711 فقد سجلت أقل تأخير متوسطاً، لكنها تتأثر بشكل ملحوظ عند تفعيل التشفير، مما يشير إلى حساسية هذه الخوارزمية لحجم الحزمة المشفرة.

الاستنتاج: التشفير يزيد من التأخير، خاصة مع خوارزميات ذات معدل بيانات مرتفع.

التقطيع (Jitter) : لوحظ أن التقطيع كان أعلى في سيناريوهات G.711 بدون VPN، حيث تجاوز 5.5 ميكروثانية، ثم استقر لاحقاً. التقطيع في G.729 كان الأدنى والأكثر استقراراً، سواء مع أو بدون التشفير، مما يعكس كفاءتها في بيئات مشفرة. التشفير لم يؤثر بشكل كبير على التقطيع فيG.729 ، لكنه حسّن استقرار G.711 نسبياً بعد فترة البدء.

الاستنتاج: خوارزمية G.729 هي الأكثر ملاءمة من حيث التقطيع في بيئات مشفرة.

متوسط رأي المستخدم (MOS):

- سجلت G.729 بدون VPN أعلى قيمة MOS قاربت 4.0، تليها G.711 بدون تشفير.
- عند تفعيل VPN وAES، انخفضت قيم MOS لجميع الخوارزميات، خاصة G.723.1 التي سجلت أقل من 3.0.
- يشير ذلك إلى تأثير التشفير على جودة الصوت المدركة من قبل المستخدم النهائي.

الاستنتاج : التشفير يؤثر سلباً على تقييم المستخدم، خاصة مع خوارزميات ذات ضغط عالي مثل G.723.1.

البيانات المستلمة (Traffic Received):

- سجلت G.711 مع VPN أعلى معدل بيانات مستلمة تجاوز 3,000,000بايت/ثانية، مما يعكس حجم الحزم الكبير الناتج عن التشفير.
- G.729 و G.723.1 أظهرتا معدلات أقل، مما يجعلها أكثر كفاءة في استهلاك عرض النطاق الترددي.

الاستنتاج : التشفير يزيد من حجم البيانات المستلمة، ويؤثر على كفاءة الشبكة، خاصة مع G.711.

الإنتاجية على الوصلة الخارجية (Utilization):

- أظهرت الوصلة بين Site2_GW والإنترنت أعلى نسبة استخدام في سيناريوهات G.711 مع التشفير، حيث تجاوزت 85%.
- خوارزمية G.729 حافظت على استخدام منخفض ومستقر، مما يدل على كفاءتها في بيئات ذات ضغط شبكي.

الاستنتاج :التشفير يرفع استهلاك الوصلات الخارجية، ويجب مراعاة ذلك في تصميم الشبكات الأكاديمية.

بناءً على نتائج المحاكاة، يُوصى بما يلي:

1. اعتماد خوارزمية G.729 كخيار ترميز أساسي في بيئة الكلية، نظراً لقدرتها على تحقيق توازن أفضل بين جودة الصوت (MOS) وكفاءة استخدام الموارد، خاصة عند تفعيل تقنيات التشفير والشبكات الخاصة الافتراضية.
2. تجنب استخدام G.711 في السيناريوهات المشفرة داخل الشبكة الأكاديمية، لما أظهرته من ارتفاع ملحوظ في التأخير واستهلاك عرض النطاق الترددي، مما قد يؤثر سلباً على أداء التطبيقات التفاعلية مثل المحاضرات الصوتية أو الاجتماعات الافتراضية.
3. تفعيل تقنيات اكتشاف النشاط الصوتي(VAD) ضمن إعدادات VoIP في الشبكة، لتقليل حجم البيانات المرسلة أثناء فترات الصمت، وبالتالي تحسين الأداء العام في بيئة مشفرة.
4. مراعاة التوازن بين الأمان والأداء عند تصميم أو تحديث الشبكة الأكاديمية، بحيث يتم اختيار خوارزميات التشفير والترميز بما يتناسب مع طبيعة الاستخدام، وعدد المستخدمين، وحجم الحركة المتوقعة.
5. استخدام نتائج هذا النموذج كمرجع عملي لتطوير سياسات الشبكة في المؤسسات التعليمية المشابهة، خاصة تلك التي تعتمد على VoIP في بيئات مشفرة، لضمان جودة الخدمة دون التضحية بالأمان.

10. التطلعات المستقبلية:

في ضوء النتائج التي تم التوصل إليها من خلال تحليل أداء بروتوكول VoIP تحت تأثير الشبكات الخاصة الافتراضية وخوارزمية التشفير AES وخوارزميات الترميز الصوتي باستخدام المحاكي OPNET، تبرز مجموعة من التطلعات المستقبلية التي يمكن أن تشكّل امتداداً عملياً وتطبيقياً لهذا البحث. من أبرز هذه التطلعات تطوير نماذج محاكاة أكثر تعقيداً تشمل سيناريوهات متعددة المستخدمين، وتغيرات ديناميكية في حركة المرور، وظروف تشغيل غير مستقرة، بما يعكس واقع الشبكات في البيئات الأكاديمية والمؤسسية السورية مثل نموذج لجامعة حمص كاملاً.

كما يُمكن توسيع نطاق الدراسة ليشمل بروتوكولات VoIP أخرى مثل SIP وH.323، وتحليل أدائها تحت تأثير خوارزميات تشفير بديلة مثل ChaCha20 أوTDES ، بالإضافة إلى اختبار تراميز صوتية حديثة مثل Opus و AMR–WB التي توفر مرونة أكبر في التكيف مع ظروف الشبكة. ومن شأن ذلك أن يُسهم في بناء توصيات تقنية أكثر دقة لتصميم شبكات اتصالات آمنة وفعالة في بيئات ذات موارد محدودة.

على المستوى التطبيقي، يمكن الاستفادة من نتائج البحث في تحسين البنية الشبكية لكلية الهندسة المعلوماتية بجامعة حمص، وتطوير نماذج أولية لأنظمة اتصالات داخلية تعتمد على VoIP المؤمّن، مع مراعاة التوازن بين جودة الخدمة والأمان. كما يُمكن اقتراح سياسات تشغيلية تعتمد على اختيار الترميز المناسب حسب حالة الشبكة، وتفعيل التشفير بشكل انتقائي وفقاً لنوع البيانات وحساسيتها.

وأخيراً، يُعد هذا البحث خطوة تأسيسية نحو بناء إطار وطني لتحسين أداء شبكات VoIP في المؤسسات التعليمية والخدمية، مع إمكانية دمج نتائج المحاكاة في أنظمة اتخاذ القرار، وتطوير أدوات تقييم معيارية تعتمد على مؤشرات QoS، بما يواكب التحولات الرقمية ويعزز جاهزية البنية التحتية للاتصالات في سوريا.

11. جدول المختصرات:

MOS	Mean Opinion Score
VPN	Virtual Private Network
IPSec	Internet Protocol Security
OPNET	Optimized Network Engineering Tool
SSL/TLS	Secure Socket Layer/ Transport Layer Security
L2TP	Layer 2 Tunneling Protocol
PPTP	Point to Point Tunneling Protocol
SIP	Session Initiation Protocol
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
VAD	Voice Activity Detection
VOIP	Voice over Internet Protocol
AES	Advanced Encryption Standard
DES	Data Encryption Standard

NIST	National Institute of Standards and Technology
MOS	Mean Opinion Score
PCM	Pulse Code Modulation
QoS	Quality of Service
CS-ACELP	Conjugate-Structure Algebraic-Code-Excited Linear-Prediction

12.المراجع:

[1] manar kashmola and ahmed yassin kamil, "Implementation of a Proposal Encryption Algorithm for Voice over Internet Protocol (VoIP)," *journal of university of anbar for pure scieence,* pp. 40-47, 2021.

[2] A. Abed, "Quality of Services for VoIP," *Master thesis University of Sfax,* 2022.

[3] محمد مصطفى سوالم، هاجر الأسود، ملاك أحمد الشريف and ريان عبد الباسط قليصة، "تصميم نظام اتصالات VoIP لكلية التقنية الصناعية باستخدام منصة Asterisk," *كلية التقنية الصناعية، مصراتة، ليبيا* , 2025.

[4] Jerzy Antoniuk and Małgorzata Plechawska-Wójcik, "Comparative analysis of VPN protocols," *journal of computer sciences institute,* pp. 138-144, 2023.

[5] "SECURE PROTOCOLS AND VIRTUAL PRIVATE NETWORKS: AN EVALUATION," *Issues in Information Systems ,* vol. 20, no. 3, pp. 37-46, 2019.

[6] Subhi Aswad, "A solution to Enhance VPN effect on wireless network Performance," *Al-Nahrain Journal for Engineering Sciences,* 2017.

[7] n. a. k. m. jabali, "Extending AES with DH Key-Exchange to Enhance VoIP Encryption in Mobile Networks," *AL-Quds University,* 2017.

[8] W. C. CHU, SPEECH CODING ALGORITHMS Foundation and Evolution of Standardized Coders, San Jose, California - USA: John Wiley & Sons, Inc., 2003.

[9] رضوان دنده، محمد صبيح and شروق ميا , "Performance analysis of G.711, G.723.1, G.729 codecs over VoIP apps," *مجلة جامعة تشرين للبحوث و الدراسات العلمية : سلسلة العلوم الهندسية*, vol. 3, no. 40, 2018.

[10] I. T. Union, Coding of speech at 8 kbps using conjugate structure algebraic-codec-excited linear-prediction, ITU-T Recommendation G. 729, 1996.

[11] I.-T. R. G.723.1, "Dual Rate Speech Coder for Multimedia Communication Transmitting at 5.3 and 6.3 kbit/s," in *International Telecommunication Union*, 1996.

[12] Firas Hazzaa, Akram Qashou and Israa Ibraheem Al Barazanchi, "Performance Analysis of Advanced Encryption Standards for Voice Cryptography with Multiple Patterns," *International Information and Engineering Technology Association,* pp. 1439-1446, 2024.

[13] Sulafa Talha and Bazara Barry, "Evaluating the impact of AES encryption algorithm on Voice over Internet Protocol (VoIP) systems," *Computing, Electrical and Electronics Engineering (ICCEEE),* 2013.

[14] Rahman, A., & Chowdhury, M, "Comparative evaluation of AES and ChaCha20 in VoIP security," *Computer Networks,* 2023.

[15] Fajar Nugraha and Toni Arifin, "Voice Encryption and Decryption Using AES 128b Method With Secret Key," *SISTEMAS JURNAL,* 2022.

[16] م. يمان غازي and د. ماهر عباس، "مقارنة خوارزميات ترميز الكلام ذات معدل بتات الخرج الثابت على شبكة كلية الهندسة المعلوماتية في جامعة البعث باستخدام المحاكي أوبنت "*,مجلة جامعة البعث* .2018 ,vol. 40 ,

[17] د. ي. غازي، "تحليل أداء بروتوكول نقل الصوت عبر الإنترنت تحت تأثير خوارزمية التشفير AES وخوارزميات الترميز الصوتي باستخدام المحاكي أوبنت "*,مجلة جامعة حمص* .2025 ,

[18] O. Timilehin, "End-to-End Security in Converged VoIP Systems: Addressing Risks and Implementing Best Practices," *University of Ibadan,* 2024.

[19] M. Adelusola, "Evaluating IPSec VPN Performance in VoIP Networks: A Simulation-Based Analysis Using OPNET," *Obafemi Awolowo University,* 2024.

[20] Adamu Umaru, David Tufe Nzadon and Omega Sarjiyus, "Evaluation of a Hybrid Network Using OPNET Simulator," *IEEE Systems Journal,* 2021.

[21] Ali mohd ali, Mahmoud Dhimish, Malek Mohmmad Alsmadi and Peter J. Mather, "An algorithmic approach to identify the optimum WLAN protocol for VoIP applications," *Wireless Personal Communications,* p. 987–1003, 2021.

[22] Poonam Chakraborty and Aparna M. Telgote , "Performance Analysis of LAN, MAN, WAN, and WLAN Topologies for VoIP Services Using OPNET Modeler," *Proceedings of the International Conference on Emerging Technologies, Springer,* p. 185–196, 2018.

[23] S. Siraj, A. K. Gupta and R. Badgujar, "Network Simulation Tools Survey," *International Journal of Advanced Research in Computer and Communication Engineering,* vol. 1, no. 4, p. 10, 2012.

[24] J. Pan and R. Jain, "A Survey of Network Simulation Tools: Current Status and Future Developments," *Project,* 2008.