مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (10) العدد (10) 2026

Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (10) No. (10) 2026

تحليل تأثير الشبكات الافتراضية الخاصة وآليات جودة الخدمة على أداء الشبكات اللاسلكية

أ. د فادي غصنه *

د. ناجي محمد **

م. عبدالله سليمان ***

(تاريخ الإيداع 2026/4/19 . قُبِل للنشر في 2026/5/25)

□ ملخّص □

أصبحت الشبكات الخاصة الافتراضية (VPN) من الحلول الأساسية لتأمين الاتصالات في الشبكات الحديثة، حيث توفر سرية البيانات وحمايتها أثناء انتقالها عبر الشبكات العامة. إلا أن استخدام تقنيات التشفير والتغليف ضمن VPNيفرض حملاً إضافيًا على الشبكة، مما قد يؤدي إلى تدهور بعض مؤشرات الأداء مثل معدل النقل وزمن التأخير.

يهدف هذا البحث إلى دراسة تأثير استخدام VPN على أداء الشبكات، مع تقديم أسلوب تحسين يعتمد على تطبيق آليات جودة الخدمة (QoS)، تم تنفيذ الدراسة باستخدام بيئة المحاكاة NS2، من خلال مقارنة ثلاثة سيناريوهات: شبكة تقليدية، شبكة تستخدم VPN، وشبكة تستخدم VPN مع QoS.

أظهرت النتائج أن استخدام VPN يؤدي إلى انخفاض في معدل النقل وزيادة في زمن التأخير، في حين أن تطبيق QoS ساهم في تحسين الأداء وتقليل التأثير السلبي، خاصة من خلال إعطاء أولوية لحركة بياناتTCP تؤكد هذه النتائج أهمية دمج آليات QoS مع VPN لتحقيق توازن بين الأمان وكفاءة الأداء.

الكلمات المفتاحية: VPN، QoS، Throughput، Delay، Jitter، Packet Loss

* أستاذ دكتور، قسم هندسة تكنولوجيا الاتصالات، كلية هندسة تكنولوجيا المعلومات والاتصالات، جامعة طرطوس، طرطوس، سوريا

** أستاذ مساعد، قسم هندسة تكنولوجيا الاتصالات، كلية هندسة تكنولوجيا المعلومات والاتصالات، جامعة طرطوس، طرطوس، سوريا

*** طالب ماجستير، قسم هندسة تكنولوجيا الاتصالات، كلية هندسة تكنولوجيا المعلومات والاتصالات، جامعة طرطوس، طرطوس، سوريا

مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (10) العدد (10) 2026

Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (10) No. (10) 2026

Performance Analysis of Virtual Private Networks and Quality of Service Mechanisms on Wireless Networks

Prof.Dr. Fadi Gosnah *
Dr. Naji Mohamad**
Eng. Abdullah Suleiman***

(Received 19/4/2026. Accepted 25/5/2026)

□ ABSTRACT □

Virtual Private Networks (VPNs) have become a fundamental solution for securing communications over public networks by ensuring data confidentiality, integrity, and secure access. However, the use of encryption and encapsulation mechanisms introduces additional overhead that may negatively affect network performance, particularly in terms of throughput and delay.

This study aims to analyze the impact of VPN deployment on network performance and propose an enhancement approach based on Quality of Service (QoS) mechanisms. The evaluation is conducted using the Network Simulator (NS2) through a comparative analysis of three scenarios: a baseline network without VPN, a network with VPN, and a network with VPN integrated with QoS.

The results demonstrate that VPN usage leads to a decrease in throughput and an increase in delay and jitter. However, the integration of QoS significantly improves performance by prioritizing critical traffic, especially TCP flows. These findings highlight the importance of combining QoS techniques with VPN technologies to achieve a balance between security and performance.

Keywords: VPN, QoS, Throughput, Delay, Jitter, Packet Loss

* Professor, Department of Communications Technology Engineering, Faculty of Information and Communication Technology Engineering, Tartous University, Tartous, Syria

** Assistant Professor, Department of Communications Technology Engineeringm, Faculty of Information and Communication Technology Engineering, Tartous University, Tartous, Syria.

*** Master's student, Department of Communications Technology Engineering, Faculty of Information and Communications Technology Engineering, Tartous University, Tartous, Syria.

1- المقدمة:

شهدت شبكات الحاسوب خلال العقود الأخيرة تطورًا متسارعًا رافقه ازدياد كبير في حجم البيانات المتبادلة وعدد المستخدمين والخدمات المعتمدة على الاتصال بالشبكة (Stallings, 2017). ومع هذا التطور برزت تحديات متزايدة تتعلق بأمن المعلومات وخصوصية الاتصالات، خاصة في ظل الاعتماد المتنامي على الشبكات العامة مثل الإنترنت في إنجاز المهام المؤسسية والشخصية. وفي هذا السياق، برزت الشبكات الخاصة الافتراضية (Virtual Private Networks – VPN) كحل فعّال يتيح إنشاء قنوات اتصال آمنة فوق بنية تحتية عامة (Nawej, 2016)، بما يضمن سرية البيانات وسلامتها وإتاحة الوصول الآمن إلى الموارد البعيدة.

على الرغم من المزايا الأمنية التي توفرها تقنياتVPN ، فإن دمج آليات التشفير والتغليف ضمن مسار نقل البيانات يضيف عبئًا إضافيًا على الشبكة(Pudelko et al., 2020) و على العقد الوسيطة، الأمر الذي قد ينعكس سلبًا على الأداء العام للشبكة. ويظهر هذا الأثر بشكل خاص في التطبيقات الحساسة للزمن مثل تطبيقات نقل الملفات والتصفح الشبكي وتدفّق البيانات المستمر. من هنا تبرز إشكالية الموازنة بين مستوى الأمان المطلوب من جهة، ومستوى الأداء المقبول من جهة أخرى، وهي إشكالية تمسّ الجوانب العملية لتصميم وتشغيل الشبكات في المؤسسات المختلفة.

ولمعالجة هذه التحديات، تم تطوير آليات جودة الخدمة (Quality of Service – QoS) كوسيلة فعّالة لإدارة موارد الشبكة وتحسين أدائها (Sun et al., 2022). تتيح QoS تصنيف حركة المرور الشبكية ومنح أولوية لأنواع معينة من البيانات، مما يساعد على تقليل الازدحام وتحسين كفاءة الإرسال. ومن خلال تطبيق تقنيات جدولة وإدارة الطوابير، يمكن تقليل زمن التأخير وتحسين استقرار الشبكة بشكل ملحوظ.

2- أهمية البحث وأهدافه:

تنبع أهمية هذا البحث من الحاجة إلى تحقيق توازن فعّال بين أمان الشبكات وأدائها عند استخدام الشبكات الافتراضية الخاصة (VPN) (Zhang et al., 2024)، حيث يهدف إلى تحليل تأثير الـ VPN على مؤشرات الأداء الأساسية مثل معدل النقل وزمن التأخير والتذبذب وفقدان الحزم. كما يسعى إلى تقييم دور آليات جودة الخدمة (QoS) في تحسين الأداء دون تعديل بنية الشبكة أو الحمل المروري (Sharma and Singh, 2023).

3- طرائق البحث ومواده:

3-1 تصميم التجربة وبنية النموذج الشبكي:

اعتمدت هذه الدراسة على تصميم نموذج شبكي يحاكي بيئة شبكات المركبات ذاتية التنظيم (Vehicular Ad-Hoc Network -VANET) ضمن إطار محاكاة مضبوط، بهدف تحليل تأثير استخدام الشبكات الافتراضية الخاصة (VPN) وآليات جودة الخدمة (QoS) على أداء الشبكة (Din and Khan, 2018). يتكوّن النموذج من مجموعة من العقد المتنقلة التي تمثل المركبات، إضافةً إلى عقد وسيطة تقوم بوظائف التوجيه، مع إدراج عقدة وسيطة إلزامية تمثل نفق VPN في السيناريو الثاني والثالث.

وقد تم تمثيل آلية الـ VPN ضمن بيئة المحاكاة بشكل منطقي من خلال فرض مسار إجباري لمرور البيانات عبر عقدة وسيطة تقوم بدور النفق (Tunnel)، بحيث تتم محاكاة عملية التغليف (Encapsulation) وتأثيرها على مسار الحزم وزمن انتقالها، دون تنفيذ التشفير الفعلي، وذلك بهدف دراسة أثر أداء الـ VPN ضمن حدود بيئة المحاكاة(Rahman et al., 2024).

تصميم البنية الشبكية يتم بحيث تبقى جميع المعطيات الأساسية (عدد العقد، مساحة الانتشار، زمن المحاكاة، ونمط الحركة) ثابتة في جميع السيناريوهات، وذلك لعزل تأثير كل من VPN وQoS على مؤشرات الأداء دون إدخال متغيرات إضافية قد تؤثر على دقة المقارنة.

3-2 بيئة التنفيذ وأدوات المحاكاة:

تنفيذ التجارب يكون باستخدام برنامج Network Simulator (NS2) لما يتيحه من إمكانيات في نمذجة البروتوكولات الشبكية ومحاكاة البيئات اللاسلكية المتنقلة (Rahman et al., 2021). تم إعداد البرامج النصية للمحاكاة بحيث تعمل في جميع السيناريوهات تحت نفس ظروف التشغيل وبنفس المعلمات وذلك لضمان أن الاختلاف في النتائج يعود فقط إلى تأثير كل من VPN وآليات QoS دون وجود أي عوامل خارجية تؤثر على المقارنة كما هو موضح في الجدول (1).

الجدول (1) بارامترات المحاكاة

عدد العقد	مساحة المحاكاة	زمن المحاكاة	بروتوكول التوجيه	حجم قائمة الانتظار	حجم الحزمة	فترة الإرسال	زمن بدء الترافيك	زمن توقف الترافيك
80عقدة	2000 × 2000متر	150ثانية	AODV	50 حزمة	512 Bytes	0.3 ثانية	3 ثواني	140ثانية

3-3 توصيف حركة المرور والتطبيقات الشبكية:

اعتمدت الدراسة نوعين رئيسيين من التطبيقات الشبكية لتمثيل أنماط مختلفة من حركة البيانات داخل الشبكة:

- **تطبيق:(CBR (Constant Bit Rate**

يُستخدم لتوليد حركة بيانات بمعدل إرسال ثابت، حيث يرسل الحزم على فترات زمنية منتظمة وبحجم محدد. يساهم هذا النوع في تمثيل التطبيقات الحساسة للزمن مثل بث الفيديو أو الاتصالات اللحظية (Kumar et al., 2022).

- **تطبيق:(FTP (File Transfer Protocol**

يُستخدم لمحاكاة نقل الملفات داخل الشبكة، ويعتمد على بروتوكول (Transmission Control Protocol– TCP) الذي يوفر آليات التحكم في الازدحام وإعادة الإرسال. يتيح هذا التطبيق دراسة أداء الشبكة تحت حمل بيانات كثيف (Sakib and Singh, 2021).

يساعد هذا التنويع في حركة المرور على تقييم تأثير VPN وQoS على أنواع مختلفة من التطبيقات الشبكية.

4-3 سيناريوهات المقارنة وإجراءات الضبط:

اعتمدت الدراسة ثلاثة سيناريوهات رئيسية هي:

- **السيناريو :(A)** شبكة VANET بدون VPN (الحالة المرجعية).
- **السيناريو :(B)** شبكة VANET مع تفعيل VPN، حيث تمر البيانات عبر عقدة وسيطة تمثل نفقًا مشفّرًا .
- **السيناريو :(C)** شبكة VANET مع VPN مدعّم بآليات QoS، حيث يتم إعطاء أولوية لحركة TCPمقارنةً ب .(User Datagram Protocol– UDP) .

تم تثبيت جميع المعلمات التشغيلية في السيناريوهات الثلاثة، بما في ذلك عدد العقد، زمن المحاكاة، ونمط حركة البيانات، لضمان أن الفروقات في الأداء تعود فقط إلى تأثير VPN وQoS.

5-3 إعداد حركة البيانات في المحاكاة:

تولد حركة البيانات داخل الشبكة باستخدام التطبيقات السابقة وفق إعدادات محددة، حيث تم ضبط فترة إرسال حزم CBR بشكل ثابت، مع الحفاظ على نفس الحمل المروري في جميع السيناريوهات دون أي تعديل.

كما تم استخدام بروتوكول **TCP** في تطبيق FTP، مع ضبط حجم نافذة الإرسال بما يضمن استقرار الاتصال وتحقيق توازن بين معدل النقل والتحكم في الازدحام.

في السيناريو الثالث، تم تطبيق آلية **Priority Queue (PriQueue)**، حيث تم إعطاء أولوية أعلى لحزم TCP مقارنةً بحزم UDP، مما يساهم في تحسين جودة الخدمة للتطبيقات الحساسة (Al-Mahtab et al., 2022).

6-3 مؤشرات الأداء والعلاقات الرياضية المعتمدة:

1-6-3 معدل النقل:(Throughput)

يتم حساب معدل نقل البيانات عبر الشبكة خلال فترة المحاكاة وفق العلاقة (1).

$$Throughput = \frac{\sum_{i=1}^{N} Packet\ size\ _i}{T_{end} - T_{start}} \quad (1)$$

حيث أن:

- Packet size يمثل حجم الحزمة
- N عدد الحزم المستلمة
- T_{start} زمن بداية الإرسال
- T_{end} زمن نهاية المحاكاة

3-6-2 زمن التأخير المتوسط:(Average Delay)

يمثل زمن التأخير الفترة الزمنية التي تستغرقها الحزمة للانتقال من العقدة المرسلة إلى العقدة المستقبلة عبر الشبكة، يمكن حساب زمن التأخير للحزمة الواحدة باستخدام العلاقة (2):

$$Delay = T_{receive} - T_{send} \quad (2)$$

ولحساب **متوسط زمن التأخير** لجميع الحزم يمكن استخدام العلاقة (3):

$$Average\ Delay = \frac{\sum_{i=1}^{N}(T_{receive,i} - T_{send,i})}{N} \quad (3)$$

حيث أن:

- T_{send} زمن إرسال الحزمة
- $T_{receive}$ زمن استلام الحزمة
- N عدد الحزم المستلمة

3-6-3 التذبذب (Jitter):

يمثل التذبذب مقدار التغير في زمن التأخير بين حزمتين متتاليتين أثناء انتقالهما عبر الشبكة. يُستخدم هذا المؤشر لقياس استقرار الشبكة، حيث أن القيم المنخفضة للتذبذب تدل على انتظام وصول الحزم، بينما تشير القيم المرتفعة إلى وجود تقلبات في زمن النقل، ويتم حسابه وفق العلاقة (4):

$$Jitter = Delay_i - Delay_{i-1} \quad (4)$$

ولحساب متوسط التذبذب لجميع الحزم باستخدام العلاقة (5):

$$Average\ Jitter = \frac{\sum_{i=2}^{N}(Delay_i - Delay_{i-1})}{N-1} \quad (5)$$

حيث أن:

- $Delay_i$ زمن تأخير الحزمة الحالية
- $Delay_{i-1}$ زمن تأخير الحزمة السابقة
- N عدد الحزم المستلمة

3-6-4 فقدان الحزم (Packet Loss):

يمثل فقدان الحزم نسبة الحزم التي تم إرسالها عبر الشبكة ولكن لم يتم استلامها في الجهة المستقبِلة. يُعد هذا المؤشر من أهم مقاييس جودة الشبكة، حيث أن ارتفاع نسبة الفقدان يدل على وجود ازدحام أو مشاكل في نقل البيانات، يتم حساب نسبة فقدان الحزم كما هو موضح في العلاقة (6):

$$Packet\ Loss = \frac{Packets_{sent} - Packets_{received}}{Packets_{sent}} \quad (6)$$

حيث أن:

- $Packets_{sent}$ عدد الحزم المرسلة من المصدر
- $Packets_{received}$ عدد الحزم التي تم استلامها بنجاح
- الفرق بينهما يمثل عدد الحزم المفقودة أثناء النقل

3-7 آلية جمع البيانات ومعالجتها:

تسجيل جميع أحداث الإرسال والاستقبال ضمن ملفات تتبّع (Trace Files) الناتجة عن محاكاةNS2 و تحليل هذه الملفات باستخدام أدوات مخصصة لاستخراج القيم الزمنية وأحجام الحزم، ثم حساب مؤشرات الأداء وفق العلاقات الرياضية المعتمدة.

إن نتائج المعالجة لاستخلاص القيم المتوسطة لكل مؤشر أداء، أتاح إجراء مقارنة دقيقة بين السيناريوهات الثلاثة، وساعد هذا الأسلوب في تحليل التغيرات الزمنية في الأداء وتحديد تأثير كل من VPN و QoS على استقرار الشبكة.

4- نتائج المحاكاة والمناقشة:

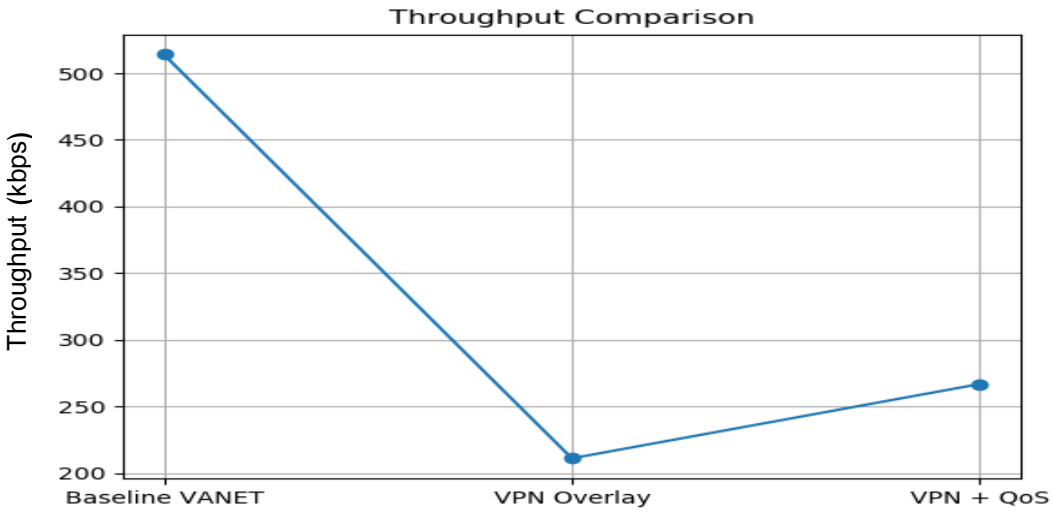
سنعرض تحليل النتائج المستخرجة من تجارب المحاكاة، وذلك لتقييم تأثير استخدام الشبكات الخاصة الافتراضية (VPN) وآليات جودة الخدمة (QoS) على أداء شبكات المركبات المتنقلة (VANET) ، واعتمد في التحليل على مجموعة مؤشرات أداء أساسية وهي: معدل النقل (Throughput) ، وزمن التأخير من طرف إلى طرف (End-to-End Delay)، والتذبذب (Jitter)، بالإضافة إلى نسبة فقدان الحزم (Packet Loss).

ولتحقيق تقييم دقيق وشامل، نفذت المحاكاة وفق ثلاث حالات تشغيل تمثل أنماطاً مختلفة من بنية الشبكة، حيث تمثل الحالة الأولى (A) الأداء المرجعي للشبكة دون أي تعديلات، بينما تعكس الحالة الثانية(B) تأثير إدخال نفق VPN كوسيط إجباري لمرور البيانات، في حين تُمثل الحالة الثالثة (C) محاولة تحسين الأداء من خلال دمج آليات QoS مع بنية ال .VPN.

ولغرض توضيح الفروقات بشكل دقيق، تم تمثيل نتائج كل مؤشر أداء باستخدام مخططات بيانية مستقلة، حيث يبيّن كل شكل التغير في قيمة المؤشر المدروس عبر الحالات المختلفة. ويسمح هذا الأسلوب بتحليل سلوك الشبكة بشكل أكثر وضوحاً، وربط النتائج العددية بالتفسير الفيزيائي لطبيعة انتقال البيانات ضمن بيئةVANET الديناميكية.

4-1 تحليل معدل النقل (Throughput):

يوضح الشكل (1) التغير في معدل النقل (Throughput) ضمن الشبكة عبر الحالات المدروسة.



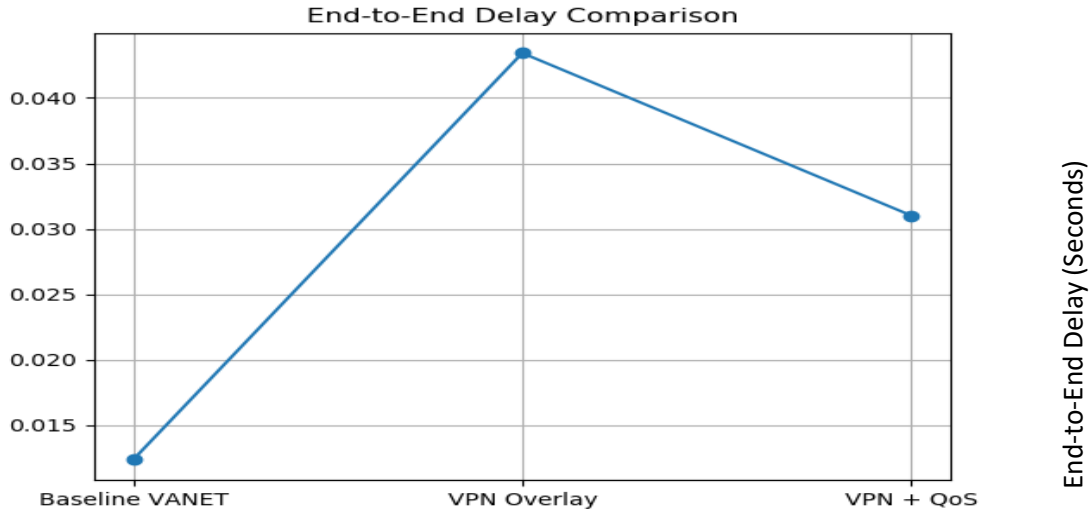
الشكل (1) يمثل التغير في معدل النقل (Throughput)

نلاحظ أن السيناريو المرجعي يحقق أعلى قيمة لمعدل النقل، ويُعزى ذلك إلى غياب أي حمل إضافي على الشبكة، مما يسمح باستغلال كامل لموارد القناة اللاسلكية. في المقابل يظهر انخفاض واضح في معدل النقل عند إدخال نفق VPN، حيث تؤدي عمليات التغليف (Encapsulation) والتشفير إلى زيادة الحمل البروتوكولي (Pudelko et al., 2020)، مما ينعكس سلباً على كفاءة نقل البيانات ويحد من معدل الإرسال الفعلي.

أما عند دمج آليات جودة الخدمة (QoS) مع ال .VPN، فيُلاحظ تحسن ملحوظ في معدل النقل مقارنةً بحالة VPN فقط، ويعود ذلك إلى قدرة QoS على إدارة حركة المرور بفعالية من خلال آليات الجدولة (Scheduling) وتحديد الأولويات (Sun et al., 2022) مما يقلل من الازدحام ويحسن استخدام عرض الحزمة المتاح. ومع ذلك، يبقى معدل النقل أقل من الحالة المرجعية، مما يدل على أن تأثير VPN لا يمكن تعويضه بشكل كامل.

4-2 تحليل زمن التأخير (End-to-End Delay):

يبين الشكل (2) زمن التأخير من أجل السيناريوهات الثلاثة.



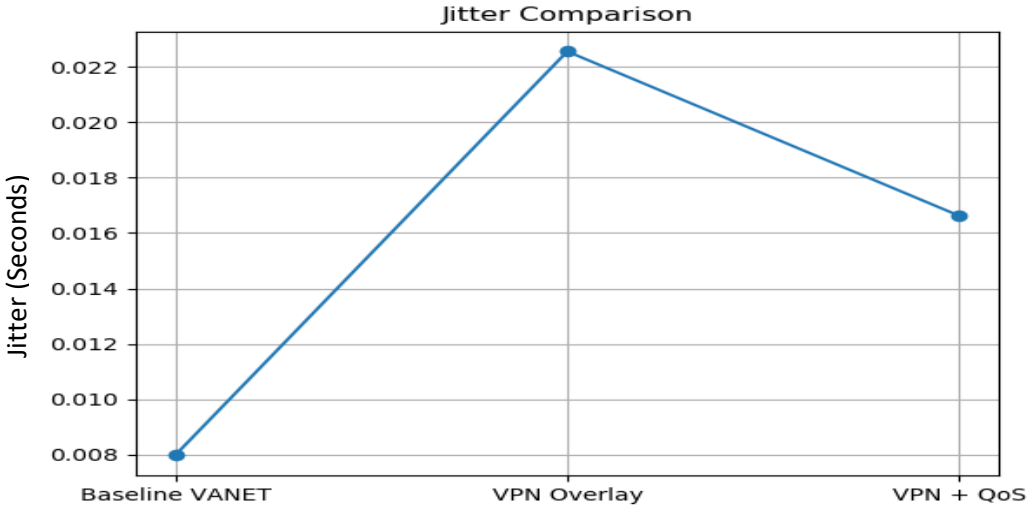
الشكل (2 زمن التأخير (End-to-End Delay)

حيث نلاحظ ازدياداً ملحوظاً في زمن التأخير عند استخدام VPN مقارنةً بالحالة المرجعية، ويُعزى ذلك إلى العمليات الإضافية التي تمر بها الحزم، مثل التشفير وفك التشفير (Sakib and Singh, 2021)، بالإضافة إلى زيادة عدد القفزات(Hops) ضمن المسار.

وعند تطبيق QoS، ينخفض زمن التأخير بشكل واضح مقارنةً بحالة VPN، نتيجة استخدام تقنيات إدارة الطوابير التي تقلل من زمن الانتظار داخل العقد الشبكية، مما يساهم في تسريع وصول الحزم. ومع ذلك يبقى زمن التأخير أعلى من السيناريو الأساسي، مما يشير إلى أن تقنيات QoS تُحسن الأداء لكنها لا تلغي تأثير البنية الإضافية التي يفرضها VPN

4-3 تحليل التذبذب (Jitter):

يوضح الشكل (3) تغير التذبذب في الشبكة.

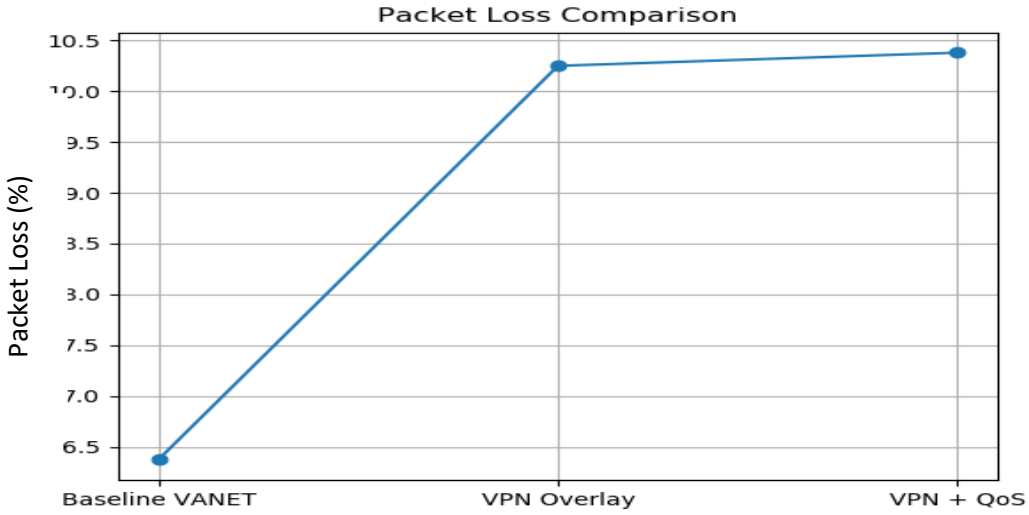


الشكل (3) يمثل تغير التذبذب (Jitter)

حيث نلاحظ أن استخدام VPN يؤدي إلى زيادة التذبذب بشكل ملحوظ، وذلك بسبب التفاوت في أزمنة معالجة الحزم داخل النفق، بالإضافة إلى تأثير الازدحام وتغير المسارات في بيئة VANET الديناميكية. عند إدخال QoS، ينخفض التذبذب بشكل ملحوظ، ويُعزى ذلك إلى قدرة هذه الآليات على تنظيم تدفق الحزم وتقليل التفاوت في أزمنة الإرسال، مما يؤدي إلى تحسين استقرار الشبكة، ويُعد هذا التحسن مهماً بشكل خاص للتطبيقات الحساسة للزمن مثل الاتصالات الفورية.

4-4 تحليل فقدان الحزم (Packet Loss):

يبين الشكل (4) نسبة فقدان الحزم في السيناريوهات المختلفة.



الشكل (4) يمثل فقدان الحزم (Packet Loss)

حيث نلاحظ زيادة في نسبة الفقد عند استخدام VPN مقارنةً بالحالة المرجعية، ويعود ذلك إلى زيادة الحمل على الشبكة، بالإضافة إلى احتمالية حدوث ازدحام أو انقطاع في المسارات نتيجة الطبيعة الديناميكية لشبكات VANET. وعلى الرغم من استخدام QoS، فإن نسبة فقدان الحزم لم تتحسن بشكل ملحوظ بل بقيت

ضمن نفس المجال تقريباً، مما يدل على أن فقدان الحزم في هذا النوع من الشبكات لا يرتبط فقط بإدارة الطوابير، بل يتأثر بشكل كبير بعوامل أخرى مثل حركة العقد (Mobility) وتغير المسارات (Route Breaks) (Rahman et al., 2024)، وهي عوامل لا يمكن التحكم بها بشكل مباشر عبر QoS.

بعد تحليل سلوك الشبكة من خلال الرسومات البيانية لكل من معدل النقل، زمن التأخير، التذبذب، ونسبة فقدان الحزم يُظهر الجدول (2) القيم التفصيلية لمؤشرات الأداء ضمن السيناريوهات الثلاثة:

الجدول (2) يوضح القيم لمؤشرات الأداء ضمن السيناريوهات الثلاثة

المؤشر	Baseline	VPN Overlay	VPN + QoS
Throughput (Kbps)	514.10	211.03	266.83
Delay (s)	0.0123	0.0434	0.0310
Jitter (s)	0.0079	0.0225	0.0166
Packet Loss (%)	6.37%	10.25%	10.38%

ولتعزيز التحليل بشكل أدق، يعرض الجدول (3) نسبة التغير المئوية بين السيناريوهات، وذلك لتوضيح حجم التأثير الحقيقي لكل من VPN و QoS على أداء الشبكة بشكل كمي نسبي.

الجدول (3) يوضح نسبة التغير المئوية بين السيناريوهات الثلاثة

المؤشر	Baseline → VPN	VPN → VPN+QoS
Throughput	-58.9%	+26.4%
Delay	+251%	-28.6%
Jitter	+183%	-26.3%
Packet Loss	+60.9%	+1.3%

حيث تتوافق هذه النتائج مع الطبيعة المعروفة لشبكات VANET من حيث الحساسية العالية للتأخير والتغير المستمر في البنية الطوبولوجية (Sharma and Singh, 2023)، وبشكل عام، تُظهر النتائج أن إدخال VPN يفرض تحديات واضحة على أداء الشبكة، إلا أن دمج آليات QoS يساهم بشكل فعّال في تحسين كفاءة الأداء واستعادة جزء مهم من جودة الخدمة، خاصة فيما يتعلق بمعدل النقل وزمن التأخير واستقرار الإرسال. ويؤكد ذلك أن استخدامQoS يشكّل خطوة أساسية نحو تحسين أداء شبكات VANET في البيئات التي تتطلب مستوى أعلى من الأمان دون التضحية الكبيرة بالأداء.

5- الاستنتاجات والتوصيات:

إن دراسة وتحليل تأثير كل من الشبكات الخاصة الافتراضية (VPN) وآليات جودة الخدمة(QoS) على أداء شبكات المركبات المتنقلة (VANET)، وذلك بالاعتماد على مجموعة من مؤشرات الأداء الأساسية وهي: معدل النقل (Throughput)، التذبذب (Jitter)، زمن التأخير (End-to-End Delay)، ونسبة فقدان الحزم (Packet Loss) توصلت إلى مجموعة من الاستنتاجات:

1. إدخال نفق VPN يؤدي إلى تأثير سلبي واضح على أداء الشبكة، حيث انخفض معدل النقل بشكل ملحوظ بنسبة 58.9%، وارتفع كل من زمن التأخير بنسبة 251% وكذلك التذبذب بنسبة 183%، ونسبة فقدان الحزم ازدادت 60.9%، ويعود ذلك إلى الحمل الإضافي الناتج عن عمليات التشفير والتغليف وزيادة التعقيد في مسار نقل البيانات.

2. دمج آليات QoS مع بيئة الـ VPN ساهم في تحسين الأداء بشكل ملحوظ حيث ارتفع معدل النقل بشكل واضح مقارنةً بحالة VPN بنسبة 26.4%، وانخفض كل من زمن التأخير بنسبة 28.6% والتذبذب بنسبة 26.3%، مما يعكس فعالية QoS في إدارة موارد الشبكة وتقليل الازدحام وتحسين استقرار الإرسال.

3. ومع ذلك، لوحظ أن تأثير QoS على تقليل فقدان الحزم كان محدوداً نسبياً، مما يشير إلى أن هذا المؤشر يتأثر بشكل أكبر بالعوامل الديناميكية الخاصة بشبكات VANET مثل تغير الطوبولوجيا وسرعة حركة العقد، أكثر من تأثره بآليات إدارة الطوابير.

4. بشكل عام، يمكن الاستنتاج أن استخدام VPN في شبكات VANET يحقق جانباً أمنياً على حساب الأداء، في حين أن دمج QoS يمثل حلاً فعالاً لاستعادة جزء مهم من الأداء وتحسين جودة الخدمة دون التأثير على البنية الأمنية.

استناداً إلى النتائج التي تم التوصل إليها في هذه الدراسة، يمكن اقتراح عدد من التوصيات المستقبلية لتعزيز أداء شبكات VANET وتحسين جودة الخدمة فيها:

- يُوصى باستخدام خوارزميات QoS أكثر تطوراً تعتمد على الذكاء الاصطناعي أو التعلم التكيفي، بهدف تحسين إدارة حركة المرور بشكل ديناميكي يتناسب مع طبيعة الشبكة المتغيرة.
- العمل على تحسين تكامل VPN مع طبقة التوجيه بحيث يتم تقليل الحمل الناتج عن التشفير والتغليف عبر تقنيات تحسين المسار (Path Optimization).

6- المراجع:

AL-MAHTAB, A.M.; ISLAM, M.S.; RAHMAN, M.A.; RAHMAN, M.S. 2022, *QoS-aware traffic management in VANET environments: A simulation study. IEEE Access*, U.S.A. Vol. 10, pp 112345–112356.

DIN, S.M.P.; KHAN, M.K. 2018, *Performance evaluation of AODV routing protocol in VANET environment using NS2 simulator. International Journal of Computer Networks and Communications Security*, Malaysia. Vol. 6, N. 7, pp 1–8.

KUMAR, A.; VERMA, R.; SHARMA, S. 2022, *A survey on QoS and routing challenges in VANETs for intelligent transportation systems. Vehicular Communications*, Netherlands. Vol. 33, p 100420.

NAWEJ, M.C. 2016, *Evaluation of Virtual Private Network Impact on Network Performance.* M.Tech. dissertation, University of South Africa, Pretoria, South Africa.

PUDELKO, M.; GALLENMÜLLER, S.; CARLE,G. 2020, *Performance analysis of VPN gateways under high load. Proc. IFIP Networking Conference*, France. pp 325–333.

RAHMAN, H.A.; M.K.HASSAN.; LEE, S. 2024, *Integrated mobility modeling and performance evaluation of VANET using NS2 and SUMO. IEEE Access*, U.S.A. Vol. 12.

RAHMAN, M.A.; ISLAM, M.S.; RAHMAN, M.S. 2021, *Performance evaluation of VANET routing protocols using NS2 under realistic mobility models. IEEE Access*, U.S.A. Vol. 9, pp 123456–123470.

SAKIB, S.K.; SINGH, J. 2021, *Performance evaluation of IPSec VPN over IPv6 networks using simulation. International Journal of Computer Networks and Communications*, India. Vol. 12, N. 2, pp 92–104.

SHARMA, R.; SINGH, P. 2023, *Impact of QoS mechanisms on MANET/VANET performance using NS2 simulation. Computer Communications*, Netherlands. Vol. 182, pp 45–56.

STALLINGS, W. 2017, *High-Speed Networks and Internets: Performance and Quality of Service.* 2nd, Pearson, U.S.A.

SUN, Y.; CHEN, X.; ZHANG, J. 2022, *QoS-aware traffic scheduling and resource allocation in next-generation wireless networks. IEEE Access*, U.S.A. Vol. 10, pp 84521–84535.

ZHANG, L.; CHEN, H.; WANG, Y.; LI, Z. 2024, *Security and performance trade-offs in VPN-enabled wireless networks. IEEE Communications Surveys & Tutorials*, U.S.A. Vol. 26, N. 1, pp 202–218.