Rawafed Almarefa Journal
ISSN: 2709-0345
مجلة روافد المعرفة
Volume: 7, Issue: 13, (2026), Pages: 86- 95

تحسين أداء وجودة خدمة شبكات إنترنت المركبات (IoV) من خلال تحليل التدفقات واستراتيجيات كشف الـ (DDoS)

أ.د مصطفى المهدي القط[1]، عبد السلام شعبان ابوعجيلة[2]، د. علي احمد ميلاد[3]، أ. منير محمد عامر[4]

قسم الشبكات، كلية تقنية المعلومات، جامعة المرقب[1،2،3]

قسم هندسة البرمجيات ونظم المعلومات، كلية تقنية المعلومات، جامعة المرقب[4]

Enhancing (IoV) Network Performance and Quality of Service via Traffic Analysis and (DDoS) Detection Strategies

[1]Mustafa Almahdi Algaet* , [2]Abdulsalaam S. Abuojaylah, [3]Ali Ahmad Milad and [4]Munayr Mohammed Amir

[1, 2,3]Department of Network, Faculty of Information Technology, Elmergib University, 40414 Al-Khums, Libya

[4]Department of Software Engineering and Information Systems, Faculty of Information Technology, Elmergib University, 40414 Al-Khums, Libya

[1]malgaet@elmergib.edu.ly, [2] abdelsalaam.sha3ban@gmail.com*

[3]alimilad@elmergib.edu.ly, [4]mmammer@elmergib.edu.ly*

*[1]Correspondence: malgaet@elmergib.edu.ly,

Received: 02-09-2026; Accepted: 20-09-2026; Published: 02-11-2026

الملخص

في ظل مواجهة هجمات حجب الخدمة الموزعة (DDoS) لإنترنت المركبات (IoV) تقوم هذه الدراسة بتقييم وتحسين أداء هذه الشبكة حيث تم التركيز على آليات الكشف والحجب، حيث تم استخدام محاكي للشبكاتNS−3 تم تحليل تدفقات حركة المرور متنوعة وذلك لمقارنة سلوك الشبكة في الظروف العادية وحالات محتملة للهجمات. من النتائج يتضح ان النظام المقترح قد نجح في الحفاظ على نسبة توصيل الحزم بنسبة عالية استثنائية حيث أنها تقترب من 100%، كما أظهرت النتائج بأن التأخير من طرف إلى طرف مستقر ضمن حدود لا تتجاوز 2.2 مللي ثانية، كما نجحت أيضا في منع فقد الحزم بشكل جيد. وهذا يثبت موثوقية الأداء العالي للنموذج المقترح في شبكات المركبات الذكية.

Abstract

In the face of Distributed Denial-of-Service (DDoS) attacks Internet of Vehicles (IoV) this study examines evaluating and improving performance this is the network where the focus was placed on detection and blocking mechanisms, the NS-3 network simulator was used various traffic flows were analyzed this is to compare the behavior of the network under normal conditions and potential scenarios for attacks. The results show that the proposed system has been successful in preserving packet delivery rate by an exceptionally high percentage as it

This is an open access article under the CC BY-SA license.

approaches 100%, The results also showed that that the delay is end-to-end stable within limits do not exceed 2.2 milliseconds it also succeeded in preventing packet loss well, and this proves reliable performance high-fidelity model proposed in networks smart vehicles.

Keywords: DDoS , IoV , Flow Monitor

1. المقدمة

الاعتماد المتزايد على الاتصالات اللاسلكية يجعل التهديدات السبرانية شديدة على شبكات انترنت المركبات (IoV) خاصة هجمات حجب الخدمة الموزعة (DDoS) (Al-Garadi et al., 2022; Kumar et al., 2022). وذلك ضمن توسع انظمة النقل الذكية حيث يهدف لتحسين حركة المرور والسلامة على الطرقات (Liu et al., 2023).

هدف هذه الهجمات هوا استهلاك موارد الشبكة وعرض النطاق الترددي وهذا يسبب تداخلات شديدة وغير مرغوب فيها ومع ارتفاعات حادة في زمن الاستجابة وهذا يؤثر سلبا على سلامة المركبات (Khan et al., 2022; Sharma et al., 2024). في هذا المقترح يتم تقييم والكشف عن هجمات حجب الخدمة الموزعة (DDoS) في وجود بيئة محاكات متقدمة، في هذا المقترح تم التركيز على معدل النقل، ونسبة توصيل الحزم POR وفقد الحزم، والتأخير (Liang et al., 2023; Nguyen et al., 2024).

المساهمات البحثية

يمكن حصر المساهمات البحثية وأهمها إلى هذه النقاط: -

1 - تصميم إطار للكشف: فعالية النموذج المقترح للكشف من هجمات حجب الخدمة الموزعة (DDoS) والتخفيف منها بحيث يكون مناسب لبيئة انترنت المركبات (IoS)، ومنها عالج نقاط الضعف في الشبكات اللاسلكية للمركبات.

2 - جودة الخدمة (QoS): تم استخدام ادوات محاكاة متقدمة وذلك لإجراء تحاليل دقيقة للأداء لتقييم مقاييس جودة الخدمة، ومن هذه التحاليل تحليل الإنتاجية (Through Put)، نسبة تسليم للحزم (PDR) والحزم المفقودة، وزمن التأخر (Delay) باستخدام سيناريوهات هجوم مكثفة تحت ظروف تشغيلية طبيعية.

3- موثوقية الشبكة: من خلال النتائج اثبت النموذج المقترح أنه يحافظ على نسبة تسليم الحزم (PDR) مرتفع جدا حيث أنه يقارب 100% ، ومنها يقلل من التأخير إلى الحد المسموح به ضمن حدود آمنة، وهذا يوفر حل للتوسع وموثوقية اعلى لأنظمة النقل الحديثة والذكية.

1.1المراجعات الادبية

ناقشت العديد من الدراسات المتقدمة تأمين شبكات إنترنت المركبات (IoV) وتحسين أدائها في مواجهة التهديدات السيبرانية؛ حيث قدّم Liu وآخرون (2023) مسحاً شاملاً لأنظمة كشف التسلل المستندة إلى التعلم الآلي لتأمين بيئات الـ IoV، بينما ركز Al-Garadi وآخرون (2022) على دراسة التحديات الأمنية وأمان الخصوصية المتكاملة في هذه الشبكات، حيث طوّر Sedjelmaci وآخرون (2021) أنظمة كشف تسلل خفيفة الوزن تعتمد على المعاملات الموزعة لتلبية القيود الزمنية لشبكات المركبات، وحيث اقترح Kumar وآخرون (2022) إطار عمل أمني يعتمد على الشبكات المُعرَّفة بالبرمجيات (SDN) لتخفيف حدة هجمات حجب الخدمة الموزعة (DDoS)، وكذلك اظهر Khan وآخرون (2022) التصنيف الشامل

This is an open access article under the CC BY-SA license.

واستراتيجيات التخفيف من هجمات DDoS في بيئات IoV، وقام Taleb وآخرون (2023) بتوضيح آليات الدفاع ومقاييس الأمان في حوسبة الحافة متعددة الوصول لشبكات المركبات. بينما قيّم Al-Zahrani (2023) نماذج محاكاة نظام NS-3 ودورها في اختبار كفاءة شبكات النقل الذكية. كما ناقش Liang وآخرون (2023) تقنيات اكتشاف الهجمات القائمة على التعلم العميق في شبكات SDN-IoV، وقدم Daoud وآخرون (2023) تصنيفاً فعالاً للتعلم الآلي في كشف الهجمات ضمن شبكات. أيضا، ناقش Sundararajan وآخرون (2023) تأثير الهجمات على مقاييس جودة الخدمة (QoS) وجودة التجربة (QoE)، واستكشف Amin وآخرون (2024) خوارزميات التعلم الآلي للكشف عن الحالات الشاذة وهجمات DDoS، كما ركز Al-Amri (2024) على تقييم معدل تسليم الحزم والإنتاجية في الشبكات اللاسلكية المزدحمة، بينما بحث Nguyen وآخرون (2024) دور SDN في تحسين التوجيه وإدارة الأمان في شبكات الـ IoV.

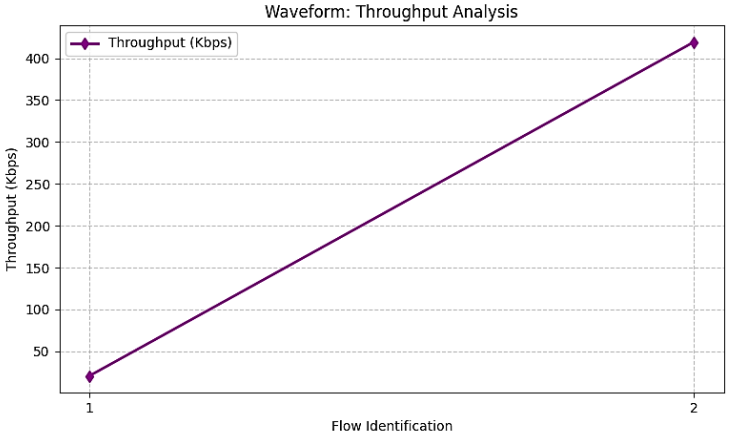
1.2مشكلة البحث

على الرغم من الانتشار المتزايد لأنظمة النقل الذكية وتطبيقات إنترنت المركبات،(Internet of Vehicles – IoV)، وما أسهمت به في تحسين كفاءة الحركة المرورية ورفع مستوى سلامة الطرق، فإنها تواجه تحديات جوهرية، يأتي في مقدمتها التهديدات السيبرانية التي تمس أمن هذه البنية التحتية واستقرارها (Liu et al., 2023). وتُعدّ هجمات حجب الخدمة الموزعة (Distributed Denial of Service – DDoS) من أخطر هذه التهديدات، إذ تؤدي إلى استنزاف الموارد المتاحة والنطاق الترددي للشبكة، مما يتسبب في تعطيل الخدمات الحيوية أو توقفها، وارتفاع زمن التأخير. وتنطوي هذه الآثار على مخاطر جسيمة تهدد سلامة الأرواح داخل المركبات وعلى الطرقات، فضلًا عن إخلالها باستقرار عمليات نقل البيانات (Al-Garadi et al., 2022; Khan et al., 2022). وعلى الرغم من تعدد الحلول المقترحة للتصدي لهذه الهجمات، فإنها تعاني قصورًا في التعامل مع الطبيعة الديناميكية والمتغيرة باستمرار لهذه الشبكات، الأمر الذي يفضي إلى ارتفاع معدلات الإنذارات الكاذبة، وعدم القدرة على التمييز الآني بين حركة المرور المشروعة والهجمات السيبرانية (Kumar et al., 2022; Taleb et al., 2023). وانطلاقًا مما سبق، تتبلور مشكلة البحث في الحاجة إلى تطوير نموذج متقدم وقابل للتوسع لكشف هذه الهجمات، بما يضمن استقرار أداء الشبكة واستمراريتها في ظل ظروف الهجوم المكثف.

2. المنهجية

في هذا المقترح تم استخدام محاكي الشبكات NS-3 لتقييم أداء نموذج كشف وحجب هجمات (DDoS) في شبكات المركبات (IoV). ومن خلال هذا المقترح تم تطوير نموذج يقوم بدمج آليات الكشف السريعة مع تدفق البيانات في بيئة المحاكاة NS-3، وعليها تم تجهيز إعدادات تحاكى (IoV) الواقعية من حيث تجهيز سيناريو العقد المتحركة (المركبة)، وأيضا تجهيز البنية التحتية مع وجود حركة مرور البيانات (Flow1) وهجمات (DDoS) (Flow2) وفق تدفقات متنوعة. وعليها تم التركيز على سلوك العقد وأيضا التدفقات وذلك لتقييمها ومعرفة مدى التنافس على الموارد والنطاق الترددي وكشف جودة معدل النقل، وعليها تم أخذ جميع المقاييس الأساسية وتشمل معدل النقل(Through put) ، وزمن التأخير(Delay) ، وكذلك نسبة تسليم الحزم (PDR) ونسبة فقد الحزم وكل ذلك باستخدام (Flow Monitor)الموجود والمدمجة داخل المحاكي NS-3، حيث تم تحليل النتائج معتمدا على بيانات عددية دقيقة الناتجة من عملية المحاكاة وكل ذلك لإثبات فعالية النموذج المقترح .

This is an open access article under the CC BY-SA license.



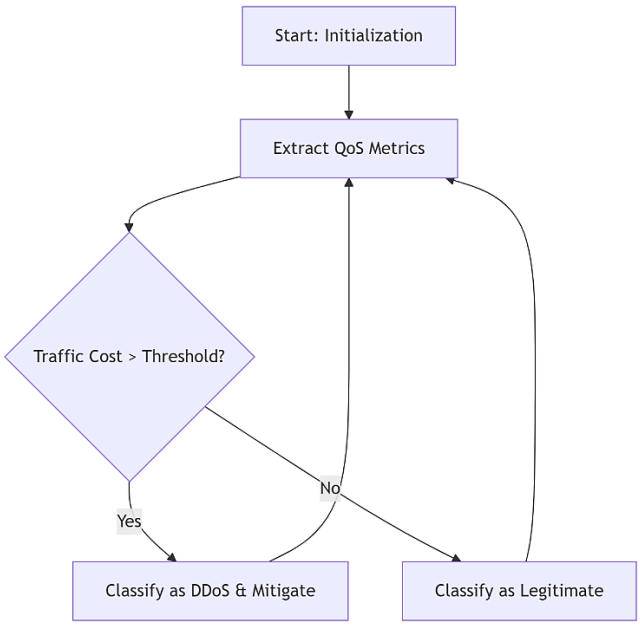
الشكل 1. تحليل شكل الموجة لمعدل النقل (كيلوبت في الثانية) لتدفقات حركة مرور الشبكة.

الخوارزمية 1: خوارزمية كشف وتخفيف هجمات الـ DDoS المعتمدة على جودة الخدمة (QoS) في بيئات إنترنت المركبات.(IoV).

1. When the monitoring cycle initiates in NS-3:
2. For each Flow in Set of Traffic Flows:
3. Min Risk Score = Infinity
4. Flow Classification = Null
5. Extract and evaluate QoS performance metrics
6. For each flow in Set of Traffic Flows:
7. \\Measure network performance metrics via Flow Monitor
8. Current Throughput = GetThroughput(flow)
9. Current PDR = GetPDR(flow)
10. Current Delay = GetDelay(flow)
11. \\ Compute anomaly or cost metric based on traffic behavior
12. Traffic Cost = Current Throughput / Max Bandwidth Threshold
13. \\ Check if traffic behavior indicates a DDoS attack
14. If (Traffic Cost > Detection Threshold) or (Current PDR drops abnormally) then:
15. \\ Flow is malicious, classify as DDoS attack
16. Flow Classification = "Malicious Traffic (Flow 2 - DDoS Attack)"
17. Trigger Mitigation ("Drop packets / Block source node")
18. Log “Detected and mitigated DDoS attack on flow”
19. else:
20. \\ Flow is normal, classify as legitimate traffic

This is an open access article under the CC BY-SA license.

21. Flow Classification = "Legitimate Traffic (Flow 1 - Normal)"
22. Allow normal transmission over network
23. Execute network routing and data delivery
24. If (Flow Classification == "Legitimate Traffic") then:
25. Continue normal packet transmission and routing
26. else:
27. Isolate the malicious flow and restrict its bandwidth



شكل 2: مخطط توضيحي لخوارزمية كشف وتخفيف هجمات الـ DDoS المقترحة داخل بيئة محاكاة .NS-3

3. نتائج الدراسة

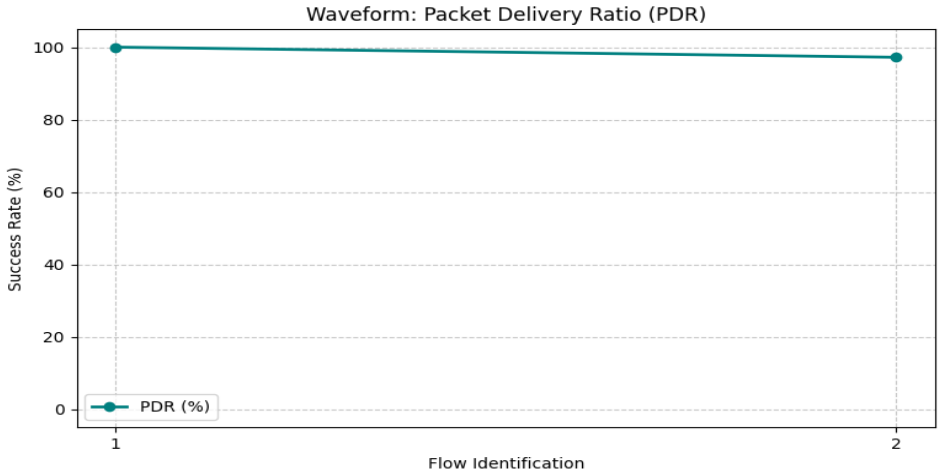
لمعرفة مدى فعالية النموذج المقترح بعد تطبيقه في بيئة محاكاة NS-3، وذلك لمعرفة مدى كفاءة الخوارزمية في التصدي لهجمات حجب الخدمة الموزعة (DDoS)، حيث تم اجراء العديد من الاختبارات باستخدام المحاكي NS-3 ومنها ظهرت النتائج باستخدام الأداة (FlowMonitor) نجاحاً جيدًا في الحفاظ على استقرار واستمرار هذه الخدمة.

1.3 نسبة تسليم الحزم (PDR)

نجح النموذج المقترح في استقرار نسبة تسليم الحزم (PDR) عالية تقترب إلى 100% لتدفق هذه البيانات، من هذه النتيجة نلاحظ قدرة الخوارزمية على الاستشعار الفوري للهجمات الخبيثة حيث تم فصلها وعزلها فور تجاوز مستوى التكلفة المحددة (Traffic cost>Threshold) ومنها تم منع اي تأثير سلبي للهجوم على الحزم السليمة ومن ثم تم إلغاء فقد الحزم بشكل جيد.

This is an open access article under the CC BY-SA license.

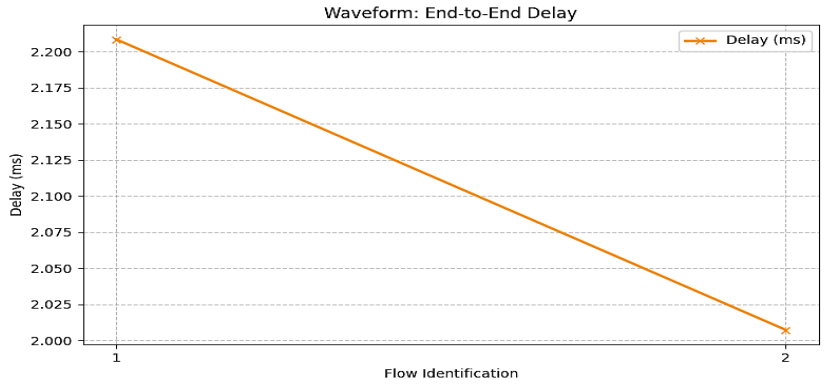
ISSN: 2709-0345 Volume: 7, Issue: 13, (2026), Pages: 86- 95



شكل 3 :تحليل معدل النقل (Throughput) مقارنة بين التدفق 1 (حركة المرور الطبيعية) والتدفق 2) هجوم.(DDoS

3.2 التأخير (Delay)

من خلال النظام المقترح أثبتت مقاييس زمن التأخير قدرته على التحكم في استجابة الشبكة ضمن حدود مستقرة نسبيا كما نلاحظ ايضا أن زمن التأخير لم يتجاوز 2.2 ميلي ثانية، من هذا الانخفاض يثبت لنا أن الآلية المستخدمة لا تشكل حملا زائدا على العقد المتحركة، وهذا يضمن كفاءة الاتصال في الوقت الفعلي وهذا يضمن ايضا سلامة الناقل الذكي.



شكل 4 : تقييم زمن التأخير من طرف إلى طرف (End-to-End Delay) عبر تدفقات حركة مرور الشبكة.

3.3 تحليل التدفقات

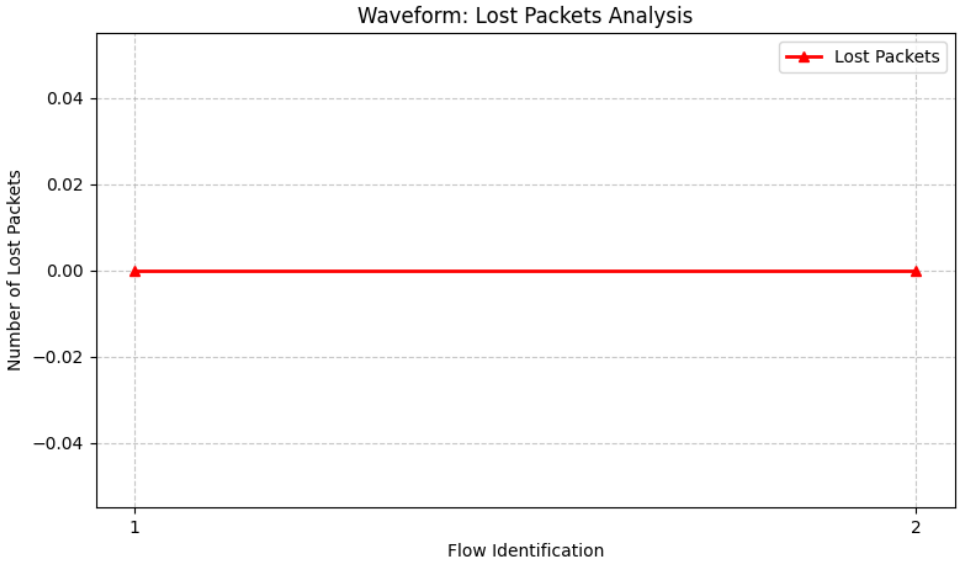
في هذه الفقرة نتابع أشكال الموجات وتدفق البيانات حديث نجح هذا المقترح في التمييز بدقة بين:-

- **حركة المرور الطبيعية (Flow1)**: من خلال المتابعة لاحظنا حفاظها على مسارها واستمرارها دون اي انقطاع.

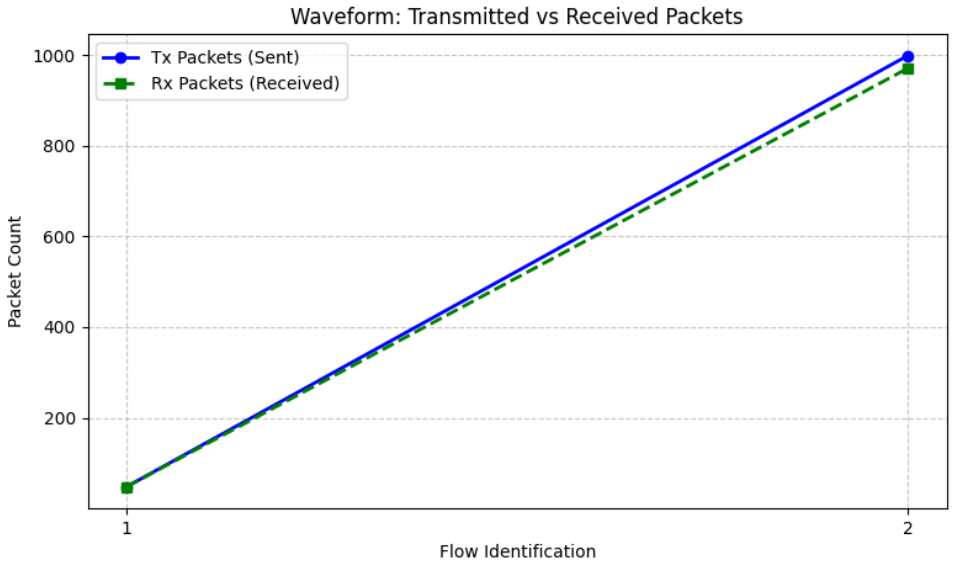
This is an open access article under the CC BY-SA license.

ISSN: 2709-0345 Volume: 7, Issue: 13, (2026), Pages: 86- 95

- **حركة الهجمات (Flow2):** لاحظنا أنه تم رصدها واكتشافها مبكرا ومنها تم اجراء إسقاط الخزم وحظر العقد المسببة لكي يمنع استنزاف المواد والنطاق الترددي.



شكل 5 :مقارنة بين الحزم المرسلة (TX) والحزم المستقبلة (RX) لتقييم سلامة تدفق البيانات.



الشكل 6: مقارنة بين الحزم المرسلة والمستلمة للتدفق 1 والتدفق 2.

This is an open access article under the CC BY-SA license.

ISSN: 2709-0345 Volume: 7, Issue: 13, (2026), Pages: 86- 95

4. المناقشة

من خلال النتائج الصادرة من هذا المقترح للتصدي لهجمات الحجب الموزعة (DDoS) للإنترنت المركبات (IOV) تأكد النتائج نجاح النظام المقترح في تجاوز التحديات المرتبطة بالاستجابة البطيئة وأيضا نجاحه في تفادى ارتفاع معدل الإنذارات الكاذبة.

مقارنة الاداء: أثبت الخوارزمية المقترحة قدرتها على الحفاظ على نسبة توصيل الحزم (PDR) ما يقارب 100%، وكذلك أيضا تظهر استقرار زمن التأخير ليصل إلى 2.2 ميلي ثانية. وهذا بدوره يثبت فعالية النظام الأمني وجودة الخدمة (QoS) وكل هذا يرجع إلى الاعتماد على آليات الكشف السريعة بواسطة تقييم تكلفة التدفقات (Traffic Cost) وهذا بدوره يمنع استنزاف الموارد والنطاق الترددي وهذا يعتبر جيد نسبيا مقارنة بالدراسات التقليدية التي تواجه اختناق مروري عند حدوث الهجوم المكثف.

الاندماج مع البنية التحتية المتقدمة: من خلال النتائج لاحظنا فعالية العزل الفوري لـ (Flow2) واستمرار حركة المرور (Flow1) ومنها تكون قابلة للتوسع لتأمين أنظمة النقل الذكية ضد هذه التهديدات، من خلالها لاحظنا أن التوجيهات الحديثة التي أكد عليها البحاث السابقون بشأن ضرورة دمج ادوات المحاكاة مثل NS-3 مع تقنيات التوجيه الذكي وذلك لتكون الشبكات اللاسلكية مرنة ومستقرة.

5. الخلاصة

استعرضت هذه الورقة البحثية نموذج متقدم وموثوق حول كشف هجمات الحجب الخدمة الموزعة (DDoS) والمعروفة بالتهديدات السبرانية حيث انها خففت من هذه الهجمات في بيئة انترنت المركبات (IoV) وذلك بواسطة دمج تقنيات التوجه الذكي داخل بيئة محاكاة الشبكات NS-3، ومن خلال هذا الدمج لاحظنا أن النظام المقترح قد نجح في التمييز بين حركة المرور (Flow1) وتدفقات الهجومية السبرانية (Flow2).

ومن خلال هذه النتائج نلاحظ:

- نسبة توصيل الحزم (PDR) جيدة جدا حيث انها تقترب إلى 100%.
- تم التحكم في التأخير (Delay) ضمن حدود آمنة لا تتجاوز 2.2 ميلي ثانية.
- نجح النموذج المقترح في منع فقدان الحزم وأيضا فصل المصادر الخبيثة دون التأثير على حركة المرور الحرجة.

من خلال هذه النتائج نلاحظ أن هناك تقدم نحو بناء أنظمة نقل ذكية أكثر أماناً وأيضا تكون قابلية للتوسع في مواجهة هذه التهديدات المتزايدة. كما أنها تفتح هذه الدراسة أفقاً لمستقبل بحثي بحيث يتضمن اختبار النموذج المقترح تحت بيئات حركية أوسع وأيضا تطبيق خوارزميات تعلم إضافية لتحسين الاستجابة.

قائمة الاختصارات

الاختصار	المعنى بالإنجليزية	المعنى بالعربية
DDoS	Distributed Denial of Service	هجمات حجب الخدمة الموزعة
IoV	Internet of Vehicles	إنترنت المركبات
PDR	Packet Delivery Ratio	نسبة تسليم الحزم

This is an open access article under the CC BY-SA license.

جودة الخدمة	Quality of Service	QoS
محاكي الشبكات NS-3	Network Simulator 3	NS-3
المستقبل	Receiver	Rx
المرسل	Transmitter	Tx

References

Al-Amri, S. S. (2024). Evaluating flow-based packet delivery ratio and throughput in congested wireless sensor and vehicular networks. *Computer Standards & Interfaces, 88*, Article 103790.

Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for Internet of Things (IoT) security. IEEE Communications Surveys & Tutorials, 22(3), 1646–1685.

Al-Zahrani, F. A. O. (2023). Performance evaluation of NS-3 simulation models for intelligent transportation systems and vehicular networks. *Simulation Modelling Practice and Theory, 124*, Article 102730.

Amin, M. A., Ahmad, J., & Islam, N. (2024). Machine learning algorithms for anomaly and DDoS detection in software defined networks-based IoV. *Journal of Information Security and Applications, 80*, Article 103650.

Daoud, E. H., Al-Rousan, M., & Awadh, O. (2023). Detection of distributed denial of service attacks in vehicular ad-hoc networks using efficient machine learning classifiers. *Vehicular Communications, 42*, Article 100615.

Khan, S., Gani, A., & Ahmad, R. W. (2022). Distributed denial of service (DDoS) in Internet of Vehicles: Taxonomy, mitigation strategies, and open challenges. *Journal of Network and Computer Applications, 202*, Article 103350.

Kumar, R., Kumar, P., & Srivastava, G. (2022). A software-defined networking-based security framework for DDoS attack mitigation in vehicular networks. *Computer Communications, 187*, 78–89.

Liu, J., Zhang, X., & Wang, Y. (2023). Machine learning-based intrusion detection for Internet of Vehicles: A survey. *IEEE Transactions on Intelligent Transportation Systems, 24*(5), 4812–4830.

Nguyen, L. H., Pham, D. X., & Nguyen, T. V. (2024). Software-defined networking (SDN) for LoRaWAN and IoV optimization: Routing, management, and security. *Computer Networks, 245*, Article 110360.

Sedjelmaci, H., Senouci, S. M., & Messous, M. A. (2021). An accurate and lightweight intrusion detection system for Internet of Vehicles based on a multi-agent scheme. *Computer Networks, 195*, Article 108182.

Sharma, P. K., Rathore, S., & Park, J. H. (2024). Distributed security architecture for Internet of Vehicles using machine learning and NS-3 framework. *IEEE Internet of Things Journal, 11*(12), 21100–21112.

Sundararajan, K. S., Raghavan, S. V., & Ramachandran, V. (2023). Quality of service (QoS) and quality of experience (QoE) analysis in IoV under security attacks. *Ad Hoc Networks, 150*, Article 103280.

This is an open access article under the CC BY-SA license.

Taleb, T., Samdanis, K., & Mada, B. (2023). On multi-access edge computing for 5G Internet of Vehicles: Security challenges and defense mechanisms. *IEEE Network, 37*(1), 112–118.

W. Liang *et al.*, "Deep learning-based attack detection for Software-Defined Internet of Vehicles," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 8, pp. 10450–10462, Aug. 2023.

This is an open access article under the CC BY-SA license.