مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (10) العدد (11) 2026
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (10) No. (11) 2026

# تخفيف تأثير عواصف الإشارات Signaling Storms على شبكات الجيل الخامس 5G باستخدام سلاسل الكتل Blockchain

**د. محمد نصر***

**د. صادق برو****

**م. لميس حسن *****

**(تاريخ الإيداع 2025/12/11 . قُبِل للنشر في 2026/5/13 )**

**□ ملخّص □**

يشهد العالم توسعًا متسارعًا في الاعتماد على شبكات الجيل الخامس، ليس فقط لتوفير سرعات اتصال أعلى، بل لتشغيل أنظمة تعتمد على الاتصال اللحظي مثل المركبات ذاتية القيادة، والطوارئ الطبية، وإنترنت الأشياء واسع الانتشار. هذا الحجم الكبير من الأجهزة المتصلة يجعل الشبكة أكثر عرضة للضغط، وخصوصًا عند حدوث ما يُعرف بعواصف الإشارات (Signaling Storms)؛ وهي حالة يتزايد فيها عدد طلبات التسجيل والتحديث بشكل غير طبيعي سواء بسبب خلل في البرامج أو نتيجة هجوم متعمد. هذه العواصف تستنزف موارد الشبكة وتُحدث بطئًا ملحوظًا في الاستجابة، وقد تؤدي في الحالات الشديدة إلى توقف الخدمة.

يهدف هذا البحث إلى تقديم منهج عملي للتخفيف من تأثير عواصف الإشارات في شبكات 5G، وذلك من خلال دمج سلاسل الكتل وتقنيات التجزئة والعقود الذكية ضمن بيئة الشبكة.

تم في هذا العمل اعتماد آلية تقوم على توليد معرفات آمنة للأجهزة باستخدام تجزئة SHA-256 (hash) مضافًا إليها قيمة عشوائية (Salt)، ومن ثم التحقق منها عبر عقد ذكي مسؤول عن إدارة الأجهزة المشبوهة وإنشاء قائمة سوداء ديناميكية. بالإضافة إلى ذلك، تم استخدام مرشح Bloom للمساعدة في تصفية الطلبات المتكررة قبل وصولها إلى العقد الأساسية في الشبكة، بما يقلل الحمل على مكوّنات التحكم مثل AMF وUDM.

تم اختبار النظام باستخدام محاكاة في MATLAB من خلال أربعة سيناريوهات مختلفة: غياب الهجمات، وجود هجوم دون أي حماية، استخدام دفاع تقليدي، وأخيرًا الدفاع باستخدام سلاسل الكتل. أظهرت النتائج انخفاضًا ملحوظًا بزمن الاستجابة من حوالي 25 ثانية في حالة الهجوم بدون حماية إلى ما يقارب 4 ثوانٍ عند تفعيل النظام المقترح.

**الكلمات المفتاحية:** شبكات الجيل الخامس، عواصف الإشارات، سلاسل الكتل، تجزئة SHA-256، العقود الذكية، مرشح Bloom

*أستاذ مساعد في قسم هندسة تكنولوجيا الاتصالات _ كلية هندسة تكنولوجيا المعلومات والاتصالات _ جامعة طرطوس_ طرطوس_ سوريا.

**مدرس في قسم هندسة تكنولوجيا الاتصالات _ كلية هندسة تكنولوجيا المعلومات والاتصالات _ جامعة طرطوس_ طرطوس_ سوريا.

***طالبة دكتوراه في 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 (11) 2026
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (10) No. (11) 2026

# Mitigating the Impact signaling storms on 5G networks using blockchain technology

**Dr. Mohammad Nassr ***
**Dr. Sadek Berro****
**Eng. Lames Hasan *****

**(Received 11/12/2025. Accepted 13/5/2026)**

**□ ABSTRACT □**

The world is witnessing a rapid expansion in the adoption of 5G networks, not only to provide higher connection speeds but also to power systems that rely on real-time connectivity, such as autonomous vehicles, emergency medical services, and the widespread Internet of Things (IoT). This large number of connected devices makes the network more susceptible to strain, especially during signal storms. These storms are characterized by an abnormally high number of registration and update requests, whether due to software glitches or deliberate attacks. They drain network resources, cause significant slowdowns in response times, and in severe cases, can lead to service outages.

This paper aims to present a practical approach to mitigating the impact of signal storms in 5G networks by integrating blockchain, hashing technologies, and smart contracts into the network environment.

This work employs a mechanism that generates secure device identifiers using SHA-256 hashing plus a random value (Salt), and then verifies them using a smart contract responsible for managing suspicious devices and creating a dynamic blacklist. In addition, a Bloom filter was used to help filter out duplicate requests before they reach the network's core nodes, thus reducing the load on control components such as AMF and UDM.

The system was tested using a MATLAB simulation through four different scenarios: no attacks, an attack with no protection, traditional defense, and finally, blockchain defense. The results showed a significant decrease in response time from approximately 25 seconds in the case of an attack with no protection to approximately 4 seconds when the proposed system was activated.

**Keywords:** 5G Networks, Signaling Storms, Blockchain, Smart Contracts, SHA-256 Hashing, Bloom Filter.

*Assistant professor, Communication Technology Engineering Department, Information and communication Technology Engineering, Tartous University, Syria.
**Teacher, Communication Technology Engineering Department, Information and communication Technology Engineering, Tartous University, Syria.
***PhD student in Communication Technology Engineering Department, Information and communication Technology Engineering, Tartous University, Syria.

## 1- المقدمة:

شهد العالم في السنوات الأخيرة تطورًا جذريًا في مجال شبكات الاتصالات مع الانتقال من الجيل الرابع إلى شبكات الجيل الخامس، التي جاءت استجابةً للحاجة المتزايدة لدعم عدد هائل من الأجهزة المتصلة وتوفير سرعات عالية وزمن استجابة منخفض جدًا. ومع توسّع تطبيقات إنترنت الأشياء، والمركبات ذاتية القيادة، والأنظمة الصناعية الذكية، أصبحت شبكات 5G تشكل العمود الفقري للبنية التحية الرقمية الحديثة، مما جعلها هدفًا أساسيًا للهجمات السيبرانية التي تسعى إلى إضعاف كفاءة الشبكة أو تعطيل خدماتها.[1][1]

من بين أبرز التهديدات التي تواجه هذه الشبكات ما يُعرف بعواصف الإشارات (Signaling Storms)، وهي حالة يحدث فيها ارتفاع غير طبيعي في عدد طلبات التحكم أو التسجيل المرسلة إلى عناصر الشبكة الأساسية مثل وحدة إدارة بيانات المشترك (UDM) ووظيفة إدارة الوصول والتحكم (AMF). قد تنشأ هذه الظاهرة نتيجة سلوك غير مقصود مثل خطأ في برمجيات الأجهزة الذكية، أو نتيجة نشاط خبيث ومنسق بهدف استنزاف موارد الشبكة وإجبارها على العمل تحت ضغط مرتفع. تؤدي هذه الهجمات إلى ازدحام في طبقة التحكم، وزيادة ملحوظة في زمن الاستجابة، وفي بعض الحالات قد تؤدي إلى انقطاع الخدمة عن المستخدمين الشرعيين [2][2].

ورغم وجود بعض الحلول التقليدية مثل تحديد معدل الإرسال Rate Limiting أو مراقبة الأنماط السلوكية، إلا أن هذه الأساليب تبقى محدودة، إما لأنها تعتمد على مركزية القرار ما يجعلها عرضة للانهيار عند الضغط، أو لأنها لا توفر آلية تحقق آمنة تمنع التلاعب بهوية الأجهزة. هنا تبرز أهمية سلاسل الكتل كحل مبتكر، إذ يوفر سجلاً موزعًا لا يمكن التلاعب به، ويتيح إمكانية التحقق من الهوية دون الاعتماد على نقطة مركزية، إضافةً إلى توفير آليات عقود ذكية قادرة على اتخاذ إجراءات أمنية تلقائية عند اكتشاف سلوك هجومي [3].[3]

انطلاقًا من ذلك، يهدف هذا البحث إلى تقديم نموذج عملي للتخفيف من عواصف الإشارات في شبكات الجيل الخامس من خلال دمج تقنيات (Salt + Hashing) لإنشاء بصمات آمنة للأجهزة، واستخدام عقد ذكي يعمل على إدارة القائمة السوداء للأجهزة المشبوهة بشكل تلقائي، بالإضافة إلى دمج مرشح Bloom لتصفية الطلبات قبل وصولها للعقد المركزية، مما يقلل الحمل على الموارد الأساسية ويمنع وصول الازدحام الهجومي عالي الكثافة. كما يعتمد البحث على نموذج رياضي من نوع M/G/1 لدراسة سلوك النظام، إضافة إلى محاكاة عملية باستخدام MATLAB عبر أربعة سيناريوهات مختلفة لقياس فعالية النظام المقترح.

وتُعدّ عواصف الإشارات في شبكات الجيل الخامس من التحديات البحثية التي تناولتها العديد من الدراسات الحديثة. فقد قدّمت الدراسة [4][4] التي اقترحت نموذجًا أوليًا لاكتشاف الازدحام في طبقة التحكم، إطارًا يعتمد على تحليل أنماط الرسائل القادمة إلى وحدة إدارة الوصول AMF، وركّزت على اكتشاف الارتفاع المفاجئ في طلبات التسجيل باعتبارها مؤشرًا على بدايات العاصفة.

[1] *A survey on security aspects for 3gpp 5g networks*, CAO, J; XIONG, L, pp. 170–195.
[2] *Blockchain security attacks, challenges, and solutions for the future distributed IoT network*, SINGH, S; HOSEN, S; YOON, B, pp. 138–159.
[3] *Edge intelligence and blockchain empowered 5g beyond for the industrial internet of things*, ZHANG, K; ZHU, Y; MAHARJAN, S; ZHANG, Y. pp. 12–19.
[4] *voting system using blockchain,* JANGADA, A; DADLANI, N; RAINA, S; SOORAJ, V; pp. 1–5.

كما تناولت الدراسة [5][5] التي بحثت في تأثير الهجمات الموزعة على واجهة التحكم N1 آلية استخدام مقاييس Rate Limiting وتقليل عدد المحاولات من خلال ضبط العتبات الديناميكية، بهدف إيجاد نموذج قادر على التمييز بين حركة المستخدمين الشرعية وحركة الهجوم دون التأثير على جودة الخدمة.

وأشارت الدراسة [6][6] التي اعتمدت منهجية التعلم الآلي في كشف السلوك الشاذ إلى إمكانية استخدام خوارزميات التصنيف مثل SVM و Random Forest لتحليل خصائص حركة الإشارة واستخراج السمات المؤدية إلى اكتشاف المهاجمين في المراحل المبكرة. وقد خلصت الدراسة إلى أن النماذج القائمة على البيانات توفر دقة جيدة، ولكنها تعاني من محدودية في التحديث الفوري والتعامل مع الهجمات المتغيرة.

ويتشابه كل من البحث [7][7] والحل المقترح في هذه الدراسة في الهدف الأساسي، وهو التخفيف من تأثير هجمات عواصف الإشارات على شبكات الجيل الخامس وتحسين استقرار الشبكة تحت الضغط. كما يعتمد العملان على فكرة منع الطلبات الضارة من استنزاف موارد مكونات النواة مثل UDM و AMF، مع التركيز على تقليل الازدحام وتحسين زمن الاستجابة. أظهرت نتائج البحث [7] أن استخدام سلاسل الكتل ساهم في تحسين زمن التسجيل وتقليل تأثير الهجوم مقارنةً بعدم وجود آلية دفاع، إلا أن بعض التأخير بقي موجودًا بسبب استمرار جزء من عمليات المعالجة داخل الشبكة. أما في الحل المقترح، فقد أظهرت النتائج انخفاضًا أكبر في زمن المعالجة أثناء الهجوم، حيث انخفض الزمن من 25.4 ثانية في حالة الهجوم إلى 3.9 ثانية بعد تطبيق الحل، نتيجة الفلترة المسبقة باستخدام مرشحBloom . كما أظهر منحنى CDFتحسنًا أوضح في توزيع أزمنة الاستجابة، مما يدل على تقليل الازدحام بشكل أكثر كفاءة. وبالتالي، فإن كلا العملين يحققان تحسينًا في الأداء والأمان، إلا أن الحل المقترح يتميز بتكلفة حسابية أقل واستجابة أسرع نتيجة إيقاف الطلبات الضارة قبل وصولها إلى مكونات النواة.

في [8][8] تمت معالجة هجمات عاصفة الإشارة في شبكة RAN، دون استخدام blockchain، ولكن باستخدام إطار عمل O-RAN xApp. يستخدم الحل المقترح معلمة تقدم التوقيت (Timing Advance) TA أثناء مرحلة الوصول العشوائي لUE لتحديد جهاز إنترنت الأشياء الفريد بافتراض أن الجهاز لا يتحرك. يعد xApp مسؤولاً عن إجراء التحليلات الإحصائية لكل طلب وصول عشوائي وارد بناءً على بيانات السجل. مثل هذه الفكرة يمكن أن تكون مقنعة، مع الأخذ في الاعتبار أن الإشارة توقفت في بداية التسجيل. ومع ذلك، فإن الاستخدام محدود للغاية لأنه يتطلب بقاء كل من gNB (محطة الجيل الخامس الأساسية) وUE ثابتًا، ويجب أن يتصل UE بنفس gNB. حتى في ظل هذا الافتراض، ليس لـ gNB دور واعد في تحديد UE الضار حيث يتم توزيع الهجوم على نواة 5G، ويمكن لـ gNB أن يكون لديه رؤية جزئية فقط للهجوم. علاوة على ذلك، فإن تحديد جهاز يستخدم TA غير دقيق لأن الجهاز الخبيث يمكنه بسهولة تغيير هذه القيمة عن طريق التلاعب بقياس وقت الرحلة ذهابًا وإيابًا.

اقترحت الدراسة [9][9] نظام اكتشاف التعلم الآلي في نواة 5G ضد هجمات عاصفة إشارات 5G، بما في ذلك هجمات التسجيل. تعد نواة 5G مسؤولة عن تصنيف واجهات SUPI (المعرف الدائم للاشتراك الفريد عالمياً) الضارة باستخدام

[5] A*malgamation of blockchain and IoT for smart cities underlying 6G communication: A comprehensive review,* UMARI, A; GUPTA, R; TANWAR, S. pp. 102–118.

[6] *Blockchain and AI-empowered healthcare insurance fraud detection: An analysis, architecture, and future prospects,* KAPADIYA, K; PATEL, U; SHARMA, G; BOKORO, N. pp. 79606–79627.

[7] *Blockchain and AI-empowered healthcare insurance fraud detection: An analysis, architecture, and future prospects,* KAPADIYA, K; PATEL, U; SHARMA, G; BOKORO, N. pp. 79606–79627.

[8] *Usi in 5g era, Journal of ICT Standardization,* PAULIAC, M. pp. 29– 40.

[9] *Ss7 vulnerabilities—a survey and implementation of machine learning vs rule-based filtering for detection of ss7 network attacks,* ULLAH, K; RASHID, I; AFZAL, H; BANGASH, A; ABBAS, H. pp. 1337–1371.

ميزة بيانات حزم السجل، مثل الفاصل الزمني بين حزمتين والعدد الإجمالي للحزم خلال وقت معين. على الرغم من أن النتيجة تظهر أن الكشف مثالي، إلا أن مثل هذه الطريقة تتطلب تخزين بيانات ميزات السجل لجميع وحدات المستعمل، الأمر الذي سيشكل عبئًا تخزينيًا ضخمًا. علاوة على ذلك، لم يناقشوا كيفية التخفيف من الهجوم بعد تصنيف SUPI.
كذلك تناولت الدراسة [$10^{10}$] لإيجاد نموذج يحاكي أثر انفجارية الطلبات (Burstiness) على سلوك الشبكة عدداً من السيناريوهات التي توضّح كيف يمكن للارتفاع السريع في إرسال الرسائل أن يسبب حالة انهيار تدريجي في موارد المعالجة، وأبرزت الدراسة أهمية نشر آليات حماية استباقية قبل حدوث الازدحام الكامل.
انطلاقا من الدراسات السابقة وتوصياتها تم اقتراح نموذج يقوم على استخدام تقنية سلاسل الكتل واستخدام مرشح Bloom لأنه يوفر تحققاً سريعاً جداً مع استهلاك ذاكرة منخفض، مما يجعله مناسباً للفلترة المسبقة في الزمن الحقيقي، كما أنه قادر على تقليل الحمل على الشبكة بكفاءة مقارنةً بمرشحات أكثر تعقيداً أو تكلفة حسابية، وقد أظهرت نتائج المحاكاة قدرة النموذج على تقليل زمن المعالجة واستقرار أداء الشبكة تحت سيناريوهات الهجوم.

### 1-1- هدف البحث وأهميته:

تتمثل أهمية هذا العمل في كونه لا يكتفي بالتحليل النظري، بل يقدم نموذجًا تطبيقيًا يمكن اعتباره خطوة نحو تطبيقات عملية قابلة للدمج مع منصات 5G مفتوحة المصدر مثل Free5GC أو Hyperledger، مما يمهد الطريق لتحسين أمن الشبكات في البيئات الفعلية وتقديم بنية أكثر مرونة في مواجهة الهجمات. بالإضافة إلى تخفيف عواصف الإشارات في شبكات الجيل الخامس 5G.

## 2- مواد وطرق البحث:

تعتمد هذه الدراسة على منهجية محاكاة عددية لتقييم فاعلية آلية مقترحة للتخفيف من عواصف الإشارات في شبكات الجيل الخامس، حيث تم نمذجة بيئة شبكة 5G باستخدام بنية قائمة على الخدمات، مع تضمين المكونات الأساسية لنواة الشبكة مثل AMF وUDM. وقد تم تنفيذ جميع تجارب المحاكاة باستخدام بيئة MATLAB، لما توفره من أدوات قوية في النمذجة الرياضية وتحليل الأنظمة. اعتمدت الدراسة على نموذج طوابير من نوع M/G/1 لتمثيل تدفق طلبات التسجيل والمصادقة، مع تعريف معدلات الوصول ($\lambda$) ومعدلات الخدمة ($\mu$) تحت سيناريوهات تشغيل متعددة. شملت هذه السيناريوهات حالة التشغيل الطبيعية بدون هجوم، وحالة وجود هجوم (Signaling Storm)، بالإضافة إلى سيناريو تطبيق الحل المقترح القائم على استخدام مرشح Bloom لفلترة الطلبات الضارة قبل دخولها إلى مكونات الشبكة، مدعومًا بآلية تحقق إضافية مستوحاة من تقنيات سلاسل الكتل. تم تحديد عدد المستخدمين، ونسبة العقد المهاجمة، ومعاملات الشبكة المختلفة ضمن بيئة المحاكاة بما يضمن تمثيلًا واقعيًا للأحمال. جرى تقييم الأداء باستخدام مجموعة من المؤشرات، تشمل زمن الانتظار في الطابور (Wq)، زمن المعالجة، والزمن الكلي للاستجابة، بالإضافة إلى تحليل دالة التوزيع التراكمي (CDF) لزمن الاستجابة، وذلك بهدف تقديم تقييم شامل لأداء النظام ومقارنة فعالية الحل المقترح مع السيناريوهات المرجعية من حيث تقليل الازدحام وتحسين استجابة الشبكة.

### 2-1- بنية شبكات الجيل الخامس 5G:

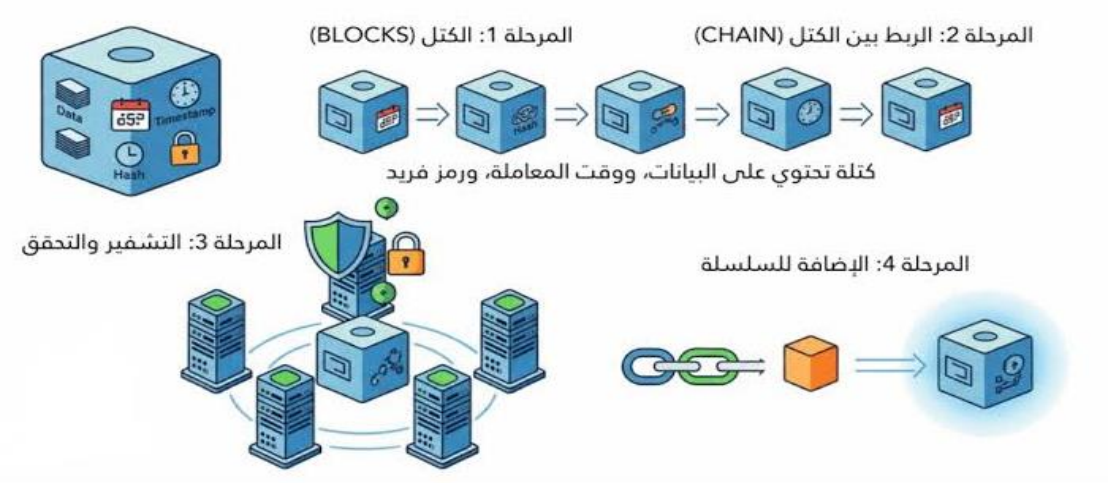
تعتمد بنية شبكات الجيل الخامس (5G) على تصميم حديث ومرن قائم على الخدمات وفق معايير 3GPP، مما يتيح كفاءة أعلى في إدارة الشبكة. تتكون الشبكة من جزأين رئيسيين: شبكة الوصول الراديوي (NG-RAN) ونواة الشبكة

[10] *A formal analysis of 5g authentication,* BASIN, D; DREIER, J; HIRSCHI, L; RADOMIROVIC, S; SASSE, R; STETTLER, V., pp. 1383–1396.

(5GC). تقوم شبكة الوصول بربط المستخدمين عبر المحطات القاعدية (gNodeB) ونقل البيانات إلى النواة. أما نواة الشبكة فتعتمد على معمارية قائمة على الخدمات (SBA)، حيث يتم تقسيم الوظائف إلى وحدات مستقلة مثل AMF لإدارة الاتصال، وSMF لإدارة الجلسات، وUDM لتخزين بيانات المشتركين. تعتمد هذه البنية على واجهات برمجية (API) للتواصل بين المكونات، مما يسهل التوسع والتحديث. كما تدعم فصل مستوى التحكم عن مستوى البيانات، مما يحسن الأداء ويزيد المرونة. تتيح G5 أيضًا دعم عدد هائل من الأجهزة وزمن استجابة منخفض جدًا. ومع ذلك، فإن هذا التصميم يجعل الشبكة أكثر عرضة لهجمات مثل عواصف الإشارات. لذلك، تتطلب هذه البنية آليات حماية فعالة للحفاظ على الأداء والاستقرار.

### 2-2- شبكات سلاسل الكتل Blockchain Networks:

تقوم فكرة شبكات سلاسل الكتل على إنشاء دفتر سجلات موزّع يسمح بتخزين المعاملات بطريقة آمنة وشفافة دون الحاجة إلى جهة مركزية تتولى إدارة النظام. تعتمد هذه الشبكات على سلسلة من الكتل المتتالية، حيث تحتوي كل كتلة على مجموعة من البيانات المرتبطة بالكتلة السابقة من خلال دالة تجزئة، مما يجعل أي محاولة للتلاعب بالمحتوى أمراً في غاية الصعوبة. وتمتاز سلاسل الكتل بكونها شبكة لامركزية، إذ يتم توزيع نسخة كاملة من السجل على جميع العقد المشاركة، الأمر الذي يمنحها قدرة عالية على مقاومة الهجمات وتعطيل الخدمة. ويتيح هذا النموذج للمستخدمين التحقق من صحة البيانات بطريقة مشتركة، حيث تتم عملية الموافقة على الإضافات الجديدة من خلال آليات إجماع متفق عليها بين العقد. وبفضل هذه الخصائص، أصبحت تقنيات سلاسل الكتل خيارًا مناسبًا للأنظمة التي تتطلب درجة عالية من الثقة، مثل المعاملات المالية، وسلاسل التوريد، وأنظمة المصادقة في الشبكات الحديثة، بما فيها شبكات الجيل الخامس، التي تستفيد من طبيعة سلاسل الكتل في تعزيز الأمان ومنع التلاعب بهويات الأجهزة [11][11]. ويوضح الشكل (1) آلية عمل شبكات سلاسل الكتل.



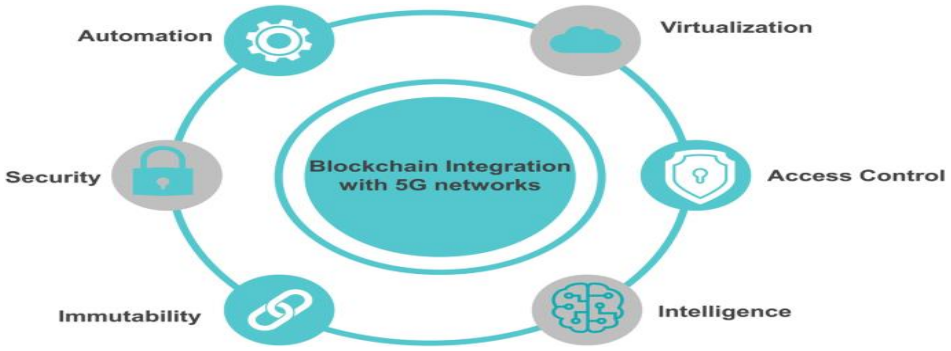

**الشكل (1): كيفية عمل سلاسل الكتل**

[11] *Signaling storm problems in 3gpp mobile broadband networks, causes and possible solutions: A review,* KHAN, Q. pp. 183–188.

### 2-3- شبكات الجيل الخامس ودمجها مع شبكات سلاسل الكتل:

يبين الشكل (2) بعضاً من مجالات الدمج بين شبكات 5G وسلاسل الكتل، حيث تُعدّ شبكات الجيل الخامس خطوة أساسية في تطور الاتصالات الحديثة، لما تقدمه من سرعات عالية في نقل البيانات، وزمن استجابة منخفض، وقدرة كبيرة على استيعاب أعداد هائلة من الأجهزة المتصلة في الوقت نفسه. ومع توسع استخدام هذه الشبكات في تطبيقات حساسة مثل المدن الذكية، وإنترنت الأشياء، والمركبات الذاتية، أصبح جانب الأمان عاملًا محوريًا لا يمكن تجاهله. فشبكات الجيل الخامس تعتمد بدرجة كبيرة على بنى افتراضية وبرمجية، وهو ما يجعلها أكثر عرضة للهجمات التي تستهدف طبقة الإشارة أو هويات المستخدمين [12][12].

هنا يبرز دور سلاسل الكتل كأحد الحلول الواعدة لتعزيز الثقة داخل الشبكات. فدمج تقنيات سلاسل الكتل مع منظومة الجيل الخامس يتيح إنشاء طبقة تحقق إضافية تعتمد على سجل موزّع وغير قابل للتلاعب، بحيث يمكن لأي جهاز أو عقدة في الشبكة التحقق من هوية الأجهزة الأخرى دون الحاجة لوجود جهة مركزية تتحكم في العملية. هذا الدمج يوفر مستوى أعلى من الأمان والشفافية، ويقلل من احتمالات انتحال الهوية أو إعادة تشغيل الرسائل، كما يساهم في توزيع عبء المصادقة بشكل متوازن بين العقد المختلفة. وبذلك، يصبح الربط بين الجيل الخامس وسلاسل الكتل خطوة طبيعية نحو شبكات أكثر استقرارًا وأمانًا، خصوصًا في البيئات التي تتطلب كفاءة عالية واستجابة فورية [13][13]. وضمن هذا السياق سنتحدث عن تحليل أمان الهوية في بحثنا وكفاءة العقد الذكي.




**الشكل (2): مجالات الاندماج والتكامل بين سلاسل الكتل وشبكات 5G [13]**

### 2-3-1- تحليل أمان الهوية:

اعتمد النظام المقترح على توليد بصمة باستخدام خوارزمية التجزئة SHA256 وفق المعادلة:

$$BV = SHA256(UE_ID \parallel Salt) \quad (1)$$

حيث BV: Blockchain Vector

هذه الآلية تمنع إعادة استخدام الهوية أو تزويرها نظرًا لخاصية Resistance Preimage وهي واحدة من أهم خصائص الأمن في دوال التجزئة (Hash Functions) وتعد أساسا في كل أنظمة الأمان الحديثة منها التشفير، سلاسل الكتل، التوقيع الرقمي، وتعني أن دالة التجزئة غير قابلة للعكس، أي لا يمكن استرجاع البيانات الأصلية من ناتج التجزئة

[12] *Secure trust-based blockchain architecture to prevent attacks in VANET*. KHAN, A; BALAN, K; ABDULLAH, J.

[13] *Bic-aka: Blockchain based asymmetric authentication and key agreement protocol for distributed 5g core network,* GAO, Z; ZHANG, D; M. ZHAO, M. pp. 66–76.

وهذا يضمن أن بصمة الجهاز في نظامنا H-BAM لا يمكن كشفها أو انتحالها، حتى لو حصل المهاجم على قيمة ال Hash نفسها [14[14]].

ومن جهة أخرى، يقلل salt من احتمال الهجمات القائمة على rainbow tables وهي تقنية يستخدمها المهاجمون لاختراق كلمات المرور أو القيم الأصلية لدوال التجزئة دون الحاجة لمحاولة كل الاحتمالات من الصفر [15]. هي باختصار جداول ضخمة مسبقة التجهيز تحتوي:

- قيمة الإدخال (input) مثل كلمة المرور
- قيمة التجزئة (hash) لها

وبالتالي يستطيع المهاجم، عندما يرى تجزئة ما، أن يبحث عنها في الجدول ويعرف القيمة الأصلية فورًا. وكتعريف مبسّط لل Rainbow Tables هي جداول تحتوي ملايين التجزئات الجاهزة لمساعدة المهاجم على معرفة القيم الأصلية بسرعة. استخدام Salt يحمي نظامنا تمامًا منها لأن التجزئة تختلف لكل جهاز، وبالتالي الجداول الجاهزة تصبح عديمة الفائدة. بالتالي؛ سلاسل الكتل هنا لا تُستخدم للتصويت أو المعاملات المالية، بل لختم الهوية بشكل غير قابل للتلاعب [15[15]].

**2-3-2- كفاءة العقد الذكي**

العقد الذكي في النظام المقترح مسؤول عن:

- تخزين الهوية مشفّرة
- إضافة الأجهزة المسيئة تلقائيًا
- منع الطلبات قبل دخولها لمسار المعالجة

وزمن استدعاء العقد في المحاكاة كان بمتوسط: {0.013 s per verification} وهذا منخفض نسبيًا لأن العقد يعمل على سلسلة خاصة Private Blockchain وليس سلسلة عامة مثل Ethereum

**2-3-3- عواصف الإشارات في شبكات الجيل الخامس:**

تعتبر عواصف الإشارات (Signaling Storms) من أخطر المشكلات التي قد تواجه شبكات الجيل الخامس، نظرًا لاعتماد هذه الشبكات على بنية معقدة وطبقة تحكم شديدة الحساسية. تحدث عواصف الإشارات عندما تتدفق كميات كبيرة من رسائل التحكم وطلبات التسجيل نحو الشبكة خلال فترة قصيرة، سواء بسبب خطأ برمجي، أو تطبيق يستهلك الإشارة بشكل غير منضبط، أو نتيجة هجوم متعمّد يستهدف إغراق وحدة إدارة الوصول (AMF) بطلبات متتالية. ومع تزايد عدد الأجهزة المتصلة في بيئة 5G—خصوصًا أجهزة إنترنت الأشياء—تصبح احتمالية حدوث هذه العواصف أكبر، نظرًا لأن أي خلل أو تحرّك غير طبيعي لعدد كبير من الأجهزة قد يؤدي إلى تدفق إشارات ضخم وغير متوقع [16[16]] ويبين الشكل (3) صورة تمثيلية لعواصف الإشارات في شبكات 5G.

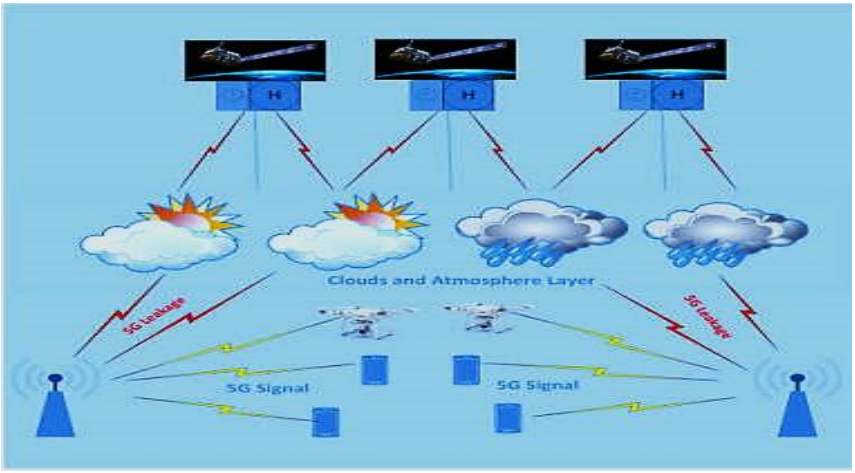
ويؤدي هذا السلوك إلى زيادة كبيرة في الحمل على طوابير المعالجة داخل الشبكة، بحيث تصبح غير قادرة على التعامل مع الكم الهائل من الطلبات، مما يؤدي إلى ارتفاع ملحوظ في زمن الاستجابة، وتراجع جودة الخدمة، وقد يصل الأمر إلى توقف بعض وحدات التحكم عن العمل. وتكمن خطورة عواصف الإشارات في أنها قد تنشأ دون

[14] A *secure blockchain-based authentication and key agreement scheme for 3gpp 5g networks,* CHOW M; MA, M. p. 4525.

[15] *Signaling storm detection in IOT network based on the open ran architecture,* HOFFMANN, M; KRYSZKIEWICZ, P. p.2302.

[16] *Machine learning based signaling DDOS detection system for 5g stand-alone core network, Applied Sciences,* PARK, S; KIM, D; YOU, I. p. 12456.

سابق إنذار، وقد يكون من الصعب التمييز بين السلوك الطبيعي والسلوك الضار في لحظاته الأولى. ولهذا، فإن تصميم آليات فعّالة للكشف المبكر والحد من تأثير هذه العواصف يعدّ جزءًا أساسيًا من جهود تأمين شبكات الجيل الخامس وضمان استمرارية خدماتها الحيوية [16].




**الشكل (3): عواصف الإشارات في شبكات الجيل الخامس 5G [16]**

### 2-4- النظام المقترح لتخفيف عواصف الإشارات:

قمنا في هذا البحث بتحليل تأثير عواصف الإشارات على أداء شبكة الجيل الخامس، خصوصًا على طبقة التحكم المسؤولة عن تسجيل المستخدمين والتعامل مع طلبات تحديث السياق [17][17]. ولتحليل هذا السلوك، تم الاعتماد على نماذج نظرية الطوابير (Queueing Theory) [17] باعتبارها إطارًا مناسبًا لدراسة الأنظمة التي تستقبل مهامًا بشكل متدفق وتقوم بخدمتها وفق معدلات زمنية مختلفة.

تعتمد عناصر التحكم في شبكة 5G، مثل وظيفة إدارة الوصول والتحكم (AMF) وقاعدة بيانات المشترك (UDM)، على بنية قائمة على معالجة الطلبات بشكل متسلسل أو شبه متوازٍ، مما يجعلها قابلة للنمذجة كنظام صف انتظار [18]. ولأن الطلبات في الظروف الطبيعية تصل بشكل عشوائي وفق توزيع بواسوني [18][18]، بينما قد تتغير مدة الخدمة تبعًا لنوع الطلب وحالة الشبكة، فقد تم اختيار نموذج M/G/1 لتمثيل النظام الأساسي.

#### 2-4-1- نظرية الطوابير (Queueing Theory):

تُعد من الأدوات الأساسية في تحليل أداء الأنظمة التي تتعامل مع سيل مستمر من الطلبات، كما هو الحال في شبكات الاتصالات. تقوم هذه النظرية على دراسة تدفق الطلبات نحو وحدات المعالجة، وكيفية تراكمها عندما يكون معدل الوصول أعلى من معدل الخدمة. وتساعد النماذج المستمدة من هذه النظرية في فهم سلوك النظام تحت الضغط، وتقدير زمن الانتظار، واحتمال امتلاء الطوابير، وتحديد الظروف التي قد تؤدي إلى انهيار الأداء أو انقطاع الخدمة [17].

ضمن هذا السياق، تلعب دفعات الإرسال (Bursts Batches) دورًا مهمًا في زيادة الحمل على الشبكة. فبدل أن تصل الطلبات بشكل منتظم وبمعدل ثابت، قد تصل على شكل دفعات كبيرة في لحظات قصيرة، مما يخلق ارتفاعًا مفاجئًا في حجم الطلبات الداخلة إلى الطابور. هذا السلوك قد يكون طبيعيًا في بعض التطبيقات، لكنه قد يكون أيضًا مؤشرًا على وجود هجوم يستهدف استنزاف موارد طبقة التحكم، خصوصًا عندما تكون هذه الدفعات متكررة ومتعمدة. إذ

---

[17]. *A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges,* SADAWI, A; HASSAN, S; NDIAYE, M, pp. 54478–54497.

[18] *The 5g-aka authentication protocol privacy,* KOUTSOS, A. pp. 464–479.

تؤدي الدفعات الكبيرة إلى ازدحام فوري في الطوابير، وارتفاع زمن المعالجة، وفقدان القدرة على تلبية الطلبات الشرعية [18].

وتزداد خطورة ظاهرة الدفعات المفاجئة عندما تكون ناتجة عن شبكات البوت نت (Botnets)، وهي شبكات ضخمة من الأجهزة المُخترقة التي تُدار عن بُعد لتنفيذ هجمات منسقة. تتميز البوت نت بقدرتها على توليد كميات هائلة من الرسائل في وقت قصير جدًا، ما يجعلها من أكثر الأدوات استخدامًا في تنفيذ عواصف الإشارات (Signaling Storms) ضد شبكات الجيل الخامس. وعندما تقوم آلاف الأجهزة المصابة بإرسال دفعات متزامنة من طلبات التسجيل أو التحديث، فإن طوابير المعالجة داخل الشبكة لا تستطيع مواكبة ذلك، مما يؤدي إلى تراكم الطلبات وتعطّل خدمة المصادقة [19[19]].

وبذلك، فإن فهم سلوك الطوابير، إلى جانب تحليل نمط الدفعات وانكشاف دور البوت نت، يعد خطوة أساسية في تصميم آليات قادرة على اكتشاف الهجمات مبكرًا وتخفيف أثرها، وضمان قدرة الشبكة على المحافظة على مستوى خدمة مستقر حتى تحت ظروف الضغط الشديد.

**2-4-2- تمثيل الهجوم كنظام دفعات $M^X/G/1$**

عند حدوث عاصفة إشارات، لا يصل كل طلب بشكل مستقل، بل غالبًا على شكل مجموعات دفعات Burst Batches، نتيجة قيام جهاز مخترق أو شبكة بوت نت بإرسال سيل من الطلبات خلال فترة زمنية قصيرة.

لذلك نُمثل معدل الهجوم باستخدام المعادلة (2): [20[20]]

$$\lambda_m = \lambda_{batch} . E[B] \qquad (2)$$

حيث: $\lambda_m$ = معدل وصول الطلبات الخبيثة الناتجة عن الهجوم

$\lambda_{batch}$ = معدل وصول مجموعات الهجوم

$E[B]$ = متوسط حجم الدفعة الواحدة

هذا يجعل النظام يتحول من $M/G/1$ إلى $M^X/G/1$ في حالة الهجوم، حيث طريقة المعالجة تأخذ في الاعتبار تدفق الطلبات دفعة واحدة وليس فرديًا.

**2-4-3- حساب زمن الانتظار ومتوسط التأخير:**

باستخدام معادلة Pollaczek–Khinchine للنظام $M/G/1$، يمكن حساب متوسط زمن الانتظار في الطابور كما في المعادلة (3): [20]

$$W_q = \frac{\lambda E[S^2]}{2(1-\rho)} \qquad (3)$$

حيث: $\lambda$ = معدل الوصول الكلي للطلبات

$E[S^2]$ = القيمة المتوقعة التربيعية لزمن الخدمة

$\rho$ = عامل التحميل

يتحقق استقرار النظام فقط عند: $\rho < 1$ وهي حالة يكون فيها معدل الخدمة أعلى من معدل تدفق الطلبات.

ويكون زمن الاستجابة الكلي كما في المعادلة (4): [20]

[19] *Fast fabric: Scaling Hyperledger fabric to 20 000 transactions per second,* GORENFLO, C; LEE, S; GOLAB, L; KESHAV, S. p.2099.

[20] *Key drivers and research challenges for 6G ubiquitous wireless intelligence*, AZHANG, B; AHOKANGAS, P; ALVES, H. p.23-30.

$$T = E[S] + W_q \qquad (4)$$

في الظروف الطبيعية يكون $\lambda_m \approx 0$ وبالتالي يكون: $T \approx E[S]$

أما في حالة الهجوم:

$$\rho \to 1 \quad \Rightarrow \quad W_q \to \infty \quad \Rightarrow \quad T \to very\ large$$

وهذا يفسر تأخر الشبكة الملاحظ في الاختبارات.

### 2-4-4- تأثير سلاسل الكتل على النموذج الرياضي

يقلل النظام المقترح من قيمة $\lambda_m$ قبل دخول الطابور عبر:

- تصفية الطلبات في مرشح Bloom
- إضافة الأجهزة المشبوهة إلى قائمة سوداء بالعقد الذكي
- استخدام hashing + salt لتقليل محاولات الانتحال

أما معدل الهجوم الجديد فيُكتب وفق المعادلة (5):

$$\lambda'_m = \lambda_m(1 - \eta) \qquad (5)$$

حيث $\eta$ تمثل كفاءة الفلترة ( 0 إلى 1 )

إذاً معدل الوصول الفعلي كما في المعادلة (6):

$$\lambda' = \lambda_b + \lambda'_m \qquad (6)$$

ومنه يكون $\rho'$ كما في المعادلة (7):

$$\rho' = \lambda' E[S] < \rho \qquad (7)$$

وبالتالي ينخفض زمن الانتظار: $T' < T$

### 2-5- الخوارزمية المقترحة H-BAM:

تعتمد خوارزمية Hybrid Blockchain-based Anomaly Mitigation أو H-BAM على نهج هجين يجمع بين التجزئة الرقمية، وتصفية الطلبات، والتحقق اللامركزي باستخدام سلاسل الكتل، إضافة إلى مراقبة سلوك الأجهزة للكشف عن الأنماط الهجومية، وذلك بهدف التخفيف من تأثير عواصف الإشارات في شبكات الجيل الخامس. تتميز الخوارزمية بأنها لا تكتفي باكتشاف الهجوم كما تفعل تقنيات كشف الشذوذ التقليدية، وإنما تقوم بمنع الطلبات غير الشرعية قبل وصولها إلى المكوّنات الأساسية للشبكة، وبآلية تعمل بشكل تلقائي دون مركزية القرار.

يبين الشكل (4) المخطط التدفقي لعمل الخوارزمية المقترحة التي تبدأ من طرف الجهاز (UE) حيث يتم إنشاء بصمة رقمية فريدة للجهاز باستخدام خوارزمية التجزئة SHA-256 مضافًا إليها قيمة (Salt)، وذلك لضمان عدم إمكانية إعادة استخدام البصمة من قبل جهاز آخر حتى لو كانت الهوية الأساسية متطابقة. تمثل هذه البصمة معرف الجهاز في المعاملات على السلسلة، وتعرف في هذا البحث باسم (BV) Blockchain Verifier:

$$BV = H(UE_ID \ || \ Salt)$$

ومعنى Salt: هو قيمة عشوائية تضاف للبيانات قبل التجزئة (Hashing) لمنع المهاجمين من تخمين البصمة أو إعادة استخدامها. بفضله تصبح الهوية المشفّرة لكل جهاز فريدة وغير قابلة للتنبؤ، حتى لو كانت الهوية الأساسية نفسها.

ونحتاج إليه لأنه عندما نحسب تجزئة قيمة مثل معرف جهاز: {Hash ثابت} $\rightarrow$ H(UE_ID)

لو كان هناك جهاز آخر يستخدم نفس المعرف، ستكون التجزئة نفسها، وهذا يسمح للمهاجمين باستخدام جداول جاهزة تُسمى Rainbow Tables لتخمين أصل القيمة.

لكن عند إضافة Salt:

$$BV = H(UE_ID \;||\; Salt)$$

تصبح التجزئة مختلفة حتى لو كانت القيمة الأصلية نفسها. وهو مهم في البحث لأننا نستخدم التجزئة لحماية هوية الجهاز في شبكات 5G. وبدون Salt يستطيع المهاجم:

- تخمين بصمة الجهاز
- انتحال الهوية

وبوجود Salt يصبح لكل جهاز بصمته الفريدة وغير القابلة للاستنساخ حتى لو عرف المهاجم رقم الهوية الأصلي.

وبعد توليد هذه البصمة، يتم إرسال طلب التسجيل إلى شبكة 5G، حيث تواجه الخوارزمية عدة طبقات معالجة قبل اعتبار الطلب صالحًا. في الخطوة الأولى، يمر الطلب عبر مرشح Bloom داخل وحدة الـ AMF، والذي يعمل كفلتر سريع منخفض التكلفة للتحقق مما إذا كانت البصمة تظهر بشكل متكرر وغير مبرر، وهي الخطوة التي تسمح بتصفية نسبة كبيرة من الطلبات قبل أن تصل إلى الطبقات الأعمق. في حال اعتُبر الطلب مشبوهًا، يتم تحويله إلى العقد الذكي على السلسلة للتحقق مما إذا كانت البصمة مسجلة مسبقًا ضمن قائمة سوداء لأجهزة مهاجمة.

حيث إذا قام الجهاز بإرسال عدد كبير من الطلبات خلال فترة زمنية قصيرة أو أظهر سلوكًا غير طبيعي، فإن الخوارزمية تعتمد على وحدة كشف الشذوذ لتحديد هذا السلوك بناءً على معدل الإرسال والأنماط الزمنية. عند تأكيد الشك، يقوم العقد الذكي بإضافة الجهاز إلى القائمة السوداء تلقائيًا، مما يجعل جميع طلباته المستقبلية تُرفض دون الحاجة لإعادة معالجتها، وبالتالي تخفيض الحمل بشكل كبير على واجهات التحكم والـ UDM.

إلى جانب ذلك، في الحالات الرمادية التي لا يمكن الحكم فيها بشكل قاطع على الجهاز، تقوم الخوارزمية بتفعيل آلية تحدي واستجابة (Challenge–Response)، حيث يُطلب من الجهاز إجراء عملية حسابية أو إرفاق توقيع خاص لإثبات شرعيته، وهذه العملية تضع عبئًا على الجهاز المشبوه بدل وضعه على الشبكة نفسها، مما يقلل الضغط على العقد الأساسية.

تتميز الخوارزمية أيضًا بأنها قابلة للتوسع والتوزيع، حيث يتم نشر العقد الذكي على سلسلة سلاسل الكتل يمكن تشغيلها على حواف الشبكة أو على بنية خاصة، مما يضمن عدم وجود نقطة فشل مركزية. بالإضافة إلى ذلك، يمكن تحديث سياسات الحجب والقبول على العقد الذكي دون إعادة تصميم مكونات الشبكة. ومن ناحية أخرى يضيف الحل المقترح تكلفة حسابية بسيطة نتيجة استخدام مرشح Bloom، إلا أن هذه التكلفة تُعد ضئيلة مقارنةً بالانخفاض الكبير في زمن الانتظار وتقليل الازدحام وتحسين الأداء العام للنظام.

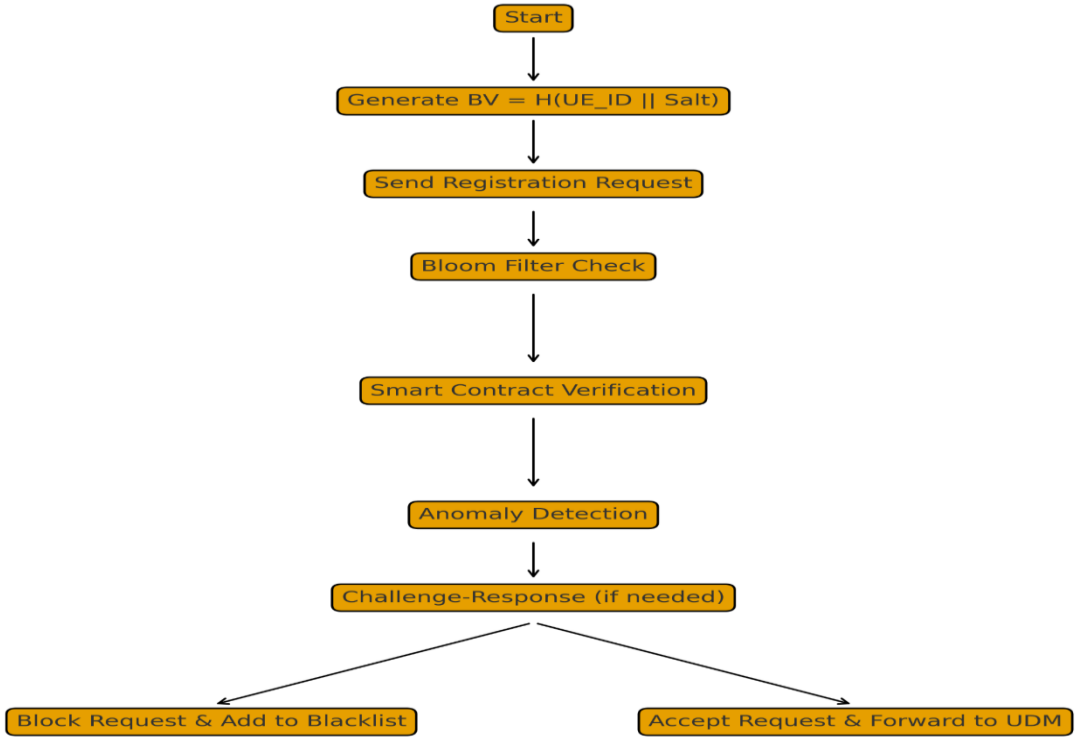
يمكن تلخيص خطوات المخطط التدفقي للخوارزمية داخل النظام كما يلي:

1. الجهاز يولد معرفًا مشفرًا باستخدام التجزئة مع salt
2. الطلب يمر عبر مرشح Bloom للتصفية السريعة
3. التحقق من القائمة السوداء عبر العقد الذكي
4. تحليل السلوك الزمني باستخدام وحدة كشف الشذوذ

5. اتخاذ قرار بالقبول أو الحجب أو التحدي
6. قبول الطلبات النظيفة فقط وتمريرها إلى UDM

تقدم الخوارزمية حلاً متكاملاً يوازن بين سرعة التحقق وموثوقية اتخاذ القرار، مع الحفاظ على تحليل موزع يقلل استهلاك موارد الشبكة أثناء الهجمات، مما يجعلها مناسبة للاستخدام في بيئات ذات حركة إشارات عالية كما هو الحال في شبكات الجيل الخامس.

يوضح المخطط في الشكل (4) تسلسل عمل الخوارزمية من توليد البصمة المشفّرة حتى اتخاذ قرار الحجب أو السماح.




الشكل (4): مخطط يوضح تسلسل عمل خوارزمية H-BAM

### 2-6- وصف سلوك الشبكة في الحالة الطبيعية وحالة الهجوم:

لفهم تأثير عواصف الإشارات بشكل دقيق، من الضروري التمييز بين سلوك الشبكة في الحالة الطبيعية (بدون هجوم) وسلوكها عند التعرض لهجوم من نوع Signaling Storm، حيث تختلف خصائص تدفق الطلبات واستجابة النظام بشكل كبير بين الحالتين.

#### 2-6-1- سلوك الشبكة في الحالة الطبيعية (بدون هجوم):

في الحالة الطبيعية، تعمل شبكة الجيل الخامس ضمن ظروف مستقرة، حيث يتم توليد طلبات التسجيل والتحديث من المستخدمين بشكل عشوائي وفق توزيع بواسوني، وبمعدل وصول معتدل. تتميز هذه الحالة بالخصائص التالية:

- تدفق منتظم للطلبات: تصل الطلبات بشكل متباعد زمنيًا دون تكتل مفاجئ
- استقرار الطوابير: لا يحدث تراكم ملحوظ في طوابير الانتظار داخل وحدات التحكم مثل AMF
- عامل تحميل منخفض: حيث يبقى $\rho < 1$، مما يضمن استقرار النظام
- زمن استجابة ثابت: يبقى زمن المعالجة قريبًا من زمن الخدمة
- عدم وجود ازدحام: جميع الطلبات يتم التعامل معها دون تأخير كبير

وبالتالي، فإن أداء الشبكة في هذه الحالة يكون مثاليًا، مع تحقيق جودة خدمة عالية للمستخدمين.

### 2-6-2- سلوك الشبكة في حالة الهجوم (Signaling Storm):

عند حدوث هجوم عاصفة إشارات، يتغير نمط وصول الطلبات بشكل جذري نتيجة قيام عدد كبير من العقد المهاجمة بإرسال دفعات متزامنة من الطلبات. ويؤدي ذلك إلى الخصائص التالية:

- تدفق دفعي (Burst Traffic): تصل الطلبات على شكل مجموعات كبيرة خلال فترات زمنية قصيرة
- ارتفاع معدل الوصول: زيادة كبيرة في $\lambda_m$ مما يؤدي إلى تجاوز معدل الخدمة
- تراكم الطوابير: امتلاء سريع لطوابير الانتظار داخل AMF
- اقتراب عامل التحميل من الواحد: $\rho \to 1$
- ارتفاع حاد في زمن الاستجابة: نتيجة زيادة زمن الانتظار $W_q$
- انخفاض جودة الخدمة: تأخير أو فقدان الطلبات الشرعية

في الحالات الشديدة، قد تصل الشبكة إلى حالة شبه انهيار (Congestion Collapse)، حيث تصبح غير قادرة على معالجة الطلبات الواردة. ويبين الجدول (1) مقارنة تحليلية بين الحالتين السابقتين.

**جدول (1): مقارنة تحليلية بين الحالتين**

| الخاصية | بدون هجوم | أثناء الهجوم |
|---|---|---|
| نمط الوصول | عشوائي منتظم | دفعي (Burst) |
| معدل الوصول | منخفض إلى متوسط | مرتفع جدًا |
| حالة الطابور | مستقر | ازدحام شديد |
| عامل التحميل | أقل من 1 | يقترب من 1 أو يتجاوزه |
| زمن الاستجابة | منخفض وثابت | مرتفع ومتزايد |
| جودة الخدمة | عالية | متدهورة |

### 2-6-3- أثر النظام المقترح:

يساهم النظام المقترح (H-BAM) في إعادة سلوك الشبكة في حالة الهجوم ليصبح قريبًا من الحالة الطبيعية، من خلال تقليل معدل الطلبات الضارة قبل دخولها إلى الطابور، مما يؤدي إلى:

- تقليل $\lambda_m$
- تخفيض عامل التحميل $\rho$
- تقليل زمن الانتظار
- منع انهيار الشبكة

## 3- النتائج والمناقشة:

أظهرت نتائج محاكاة النموذج المقترح التي تم إجراؤها فعالية النظام المقترح H-BAM في التخفيف من عواصف الإشارات ضمن بيئة شبكة الجيل الخامس. تتضمن الدراسة أربع حالات تشغيل رئيسية تمثل مستويات مختلفة من الضغط الشبكي ومستوى الحماية الأمنية.

### 3-1- وصف سيناريوهات الاختبار:

لضمان تقييم دقيق وواقعي لأداء النظام المقترح، تم إعداد بيئة محاكاة في برنامج MATLAB تعكس سلوك شبكة الجيل الخامس تحت ظروف تشغيل مختلفة، مع مراعاة تمثيل كل من الحركة الطبيعية والهجومية بشكل قريب من الواقع.

❖ عدد المستخدمين (Legitimate Users):

تم افتراض وجود $N_u$=1000 مستخدم شرعي داخل الشبكة، يقومون بإرسال طلبات تسجيل وتحديث بشكل عشوائي وفق توزيع بواسوني (Poisson Process) بمعدل وصول: ($\lambda_b = 5$) طلب /ثانية

❖ عدد العقد المهاجمة (Attacking Nodes):

تم تمثيل الهجوم باستخدام شبكة بوت نت تتكون من: Na = 100 عقدة مهاجمة

ويكون معدل الهجوم الكلي:

$$\lambda_m = \lambda_{batch} \times E[B]$$

حيث: $\lambda_{batch} = 2$ دفعة/ثانية

$E[B] = 20$ طلب لكل دفعة

مما ينتج معدل هجوم مرتفع يحاكي سيناريو Signaling Storm حقيقي.

❖ بارامترات الشبكة (Network Parameters)

تم اعتماد مجموعة من البارامترات لتمثيل بيئة الشبكة كما يلي:

- نموذج الطابور: M/G/1
- معدل الخدمة:(μ = 30) طلب/ثانية
- زمن الخدمة المتوسط: E[S] = 0.033 ثانية
- عامل التحميل (Utilization):

$$\rho = \frac{\lambda}{\mu}$$

- سعة الطابور: غير محدودة (Infinite Buffer) لمحاكاة أسوأ الحالات
- معامل Bloom Filter: معدل الخطأ: 1
- حجم الفلتر: متغير ديناميكيًا حسب عدد الطلبات
- زمن التحقق عبر العقد الذكي: 0.013 ثانية لكل عملية تحقق

❖ إعداد السيناريوهات الأربعة:

تم تنفيذ المحاكاة ضمن أربع حالات رئيسية:

S1: حركة طبيعية بدون هجوم

S2: هجوم عاصفة إشارات بدون حماية

S3: هجوم مع دفاع تقليدي (Rate Limiting)

S4: هجوم مع النظام المقترح (H-BAM)

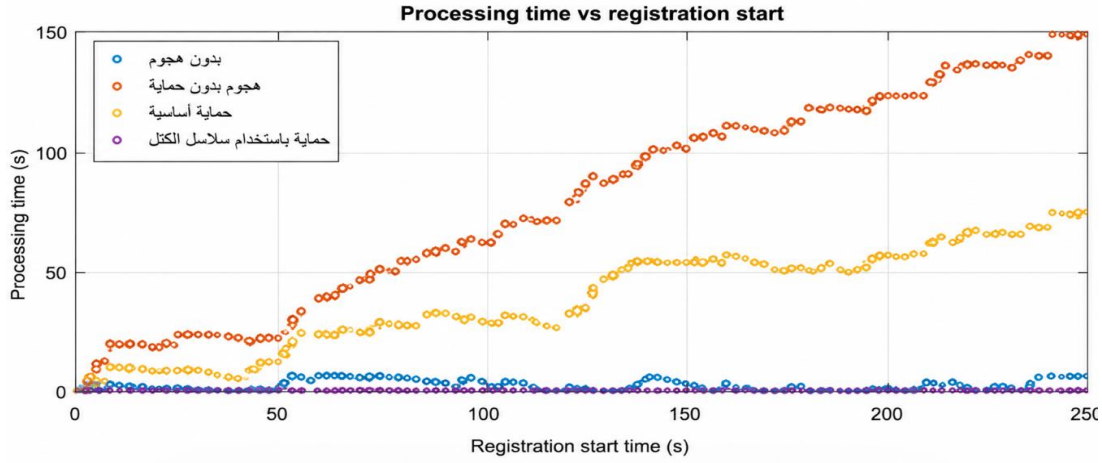
حيث تم الحفاظ على نفس بارامترات الشبكة في جميع السيناريوهات لضمان عدالة المقارنة، مع تغيير آلية التعامل مع الطلبات فقط. ويوضح الجدول (2) ملخص لجميع بارامترات بيئة المحاكاة.

**جدول (2): بارامترات بيئة المحاكاة:**

| الفئة | البارامتر | القيمة | الوصف |
|---|---|---|---|
| المستخدمون | عدد المستخدمين الشرعيين | 1000 | عدد الأجهزة الطبيعية في الشبكة |
| المستخدمون | معدل الوصول الطبيعي | 5 طلب/ثانية | معدل إرسال الطلبات من المستخدمين |
| الهجوم | عدد العقد المهاجمة | 100 | عدد أجهزة البوت نت |
| الهجوم | معدل الدفعات | 2 دفعة/ثانية | عدد دفعات الهجوم في الثانية |
| الهجوم | متوسط حجم الدفعة | 20 طلب | عدد الطلبات في كل دفعة |
| الهجوم | معدل الهجوم الكلي | 40 طلب/ثانية | ناتج ضرب معدل الدفعات في حجمها |
| الشبكة | نموذج الطابور | M/G/1 | نموذج تحليل الأداء |
| الشبكة | معدل الخدمة | 30 طلب/ثانية | قدرة المعالجة في الشبكة |
| الشبكة | زمن الخدمة | 0.033 ثانية | متوسط زمن معالجة الطلب |
| الشبكة | عامل التحميل | محسوب | نسبة الضغط على النظام |
| الشبكة | سعة الطابور | غير محدودة | لمحاكاة حالات الازدحام |
| الحماية | Bloom Filter (معدل الخطأ) | %1 | احتمال الخطأ في الفلترة |
| الحماية | زمن التحقق (العقد الذكي) | 0.013 ثانية | زمن تنفيذ التحقق |
| الحماية | نوع سلاسل الكتل | خاص (Private) | لتقليل زمن التأخير |

### 3-2- نتائج زمن الاستجابة (Response Time):

يوضح الشكل (5) كيف يتغير زمن معالجة طلبات التسجيل مع مرور الوقت منذ بداية عملية التسجيل، سواء كانت الشبكة تحت ضغط أو في وضع طبيعي.




**الشكل (5): تغير زمن معالجة الطلبات خلال عملية التسجيل**

يمثل المحور الأفقي في الشكل السابق زمن بدء عملية التسجيل، ويعكس تسلسل الطلبات داخل الشبكة، أما المحور العمودي فيمثل زمن معالجة الطلب في الشبكة (Processing Time)، وهو يقيس الحمل على AMF وطبقة التحكم، وبشكل مبسط كل نقطة تمثل طلب تسجيل واحد، وموقعها يوضح كم استغرق معالجته ومتى بدأ.

وفي الحالة الطبيعية (بدون هجوم): يكون الرسم منخفضًا وثابتًا، ومعظم النقاط عند مستوى واحد تقريبًا، أما الزمن خطّي وزمن الخدمة قريب من المتوسط، وتفسير ذلك هو أن الشبكة تعمل بكفاءة ومعالجة الطلبات مستقرة ولا يوجد ازدحام في طبقة التحكم.

أما في سيناريو عاصفة الإشارات بدون حماية: يبدأ الرسم بالتصاعد الحاد مع الزمن، وغالبًا ينتج شكل منحنى يرتفع تدريجيًا أو يظهر نقاط متشتتة بقيم عالية جدًا، وتفسير ذلك هو أنه عند تزايد عدد الطلبات، تصبح طبقة التحكم غير قادرة على الاستجابة بنفس المعدل، فيزداد زمن المعالجة بشكل تراكمي حتى يصل لحالة انهيار. هذا يدل على:

- زيادة كبيرة في زمن المعالجة
- تراكم الطلبات في قائمة الانتظار
- انخفاض جودة الخدمة واحتمال سقوط الجلسات

أما في حالة تطبيق H-BAM (السيناريو المحمي)، يكون المنحنى أقرب إلى الحالة الطبيعية، وزمن المعالجة قليل، وتوزيع النقاط متجانس، ولا يوجد تصاعد تراكمي، وتفسير ذلك هو أن النظام يقوم بتصفية الطلبات المشبوهة قبل إضافة حمل على AMF، مما يمنع حدوث تراكم يؤدي للانهيار.

❖ تشير نتائج المحاكاة إلى أن جوهر التحسن لا يعود لوجود سلاسل الكتل بحد ذاته، بل لطريقة توظيفه داخل دورة اتخاذ القرار الأمني:

- سلاسل الكتل يحل مشكلة الثقة
- التجزئة تمنع الانتحال
- Bloom يقلل الحمل
- العقد الذكي يوقف السلوك المسيء بسرعة

إذاً الربط بين هذه المكونات هو سبب النجاح وليس تقنية سلاسل الكتل وحدها.

قد يُلاحظ من النتائج أن زمن الاستجابة في السيناريو المقترح (S4) قريب جدًا أو أقل من الحالة الطبيعية (S1)، رغم أن النظام يحتوي على طبقات إضافية مثل التحقق باستخدام سلاسل الكتل ومرشح Bloom، وهو ما قد يبدو متناقضًا للوهلة الأولى. إلا أن هذا الاختلاف يمكن تفسيره من خلال التمييز بين نوعين من الزمن:

1. زمن المعالجة (Processing Time): يمثل الزمن الذي تستغرقه الشبكة لمعالجة الطلب داخل مكونات مثل AMF وUDM، دون احتساب زمن الانتظار في الطابور.

في الحالة المقترحة (S4)، قد يكون زمن المعالجة الفردي أعلى قليلًا بسبب: عمليات التحقق باستخدام Bloom Filter والتفاعل مع العقد الذكي إضافة إلى عمليات التجزئة.

2. زمن الاستجابة الكلي (Response Time)

ويُحسب وفق العلاقة:

$$T = E[S] + W_q$$

حيث: $E[S]$: زمن المعالجة

$W_q$: زمن الانتظار في الطابور

والسبب في أن زمن الاستجابة في (S4) أقل أو قريب من (S1) هو أن: تقليل الازدحام (Queue Reduction) له تأثير أكبر بكثير من الزيادة البسيطة في زمن المعالجة.

أي أن النظام المقترح يضيف تكلفة حسابية صغيرة، لكنه يقلل بشكل كبير من الضغط على الشبكة ويبين الجدول (3) نتائج المحاكاة لمتوسط أزمنة المعالجة والانتظار والاستجابة للسيناريوهات الأربعة.

**جدول (3): نتائج المحاكاة لمتوسط أزمنة المعالجة والانتظار والاستجابة للسيناريوهات الأربعة**

| السيناريو | زمن المعالجة (ثانية) | زمن الانتظار (ثانية) | زمن الاستجابة الكلي (ثانية) | الملاحظة |
|---|---|---|---|---|
| S1 | 1.8~ | 0.3~ | 2.1~ | أداء طبيعي مستقر |
| S2 | 2.0~ | 23.4~ | 25.4~ | ازدحام شديد وانهيار شبه كامل |
| S3 | 2.2~ | 9.4~ | 11.6~ | تحسن جزئي بسبب تقليل الحمل |
| S4 | 2.5~ | 1.4~ | 3.9~ | قريب من الحالة الطبيعية مع استقرار |

يوضح الجدول (3) أن الزيادة الطفيفة في زمن المعالجة في النظام المقترح (S4) ناتجة عن العمليات الإضافية مثل التحقق باستخدام مرشح Bloom والعقد الذكي. إلا أن هذه الزيادة يقابلها انخفاض كبير في زمن الانتظار نتيجة تقليل عدد الطلبات التي تصل إلى طابور المعالجة. وبالتالي، فإن الزمن الكلي للاستجابة يبقى منخفضًا وقريبًا من الحالة الطبيعية، مما يثبت أن تقليل الازدحام له تأثير أكبر من تكلفة المعالجة الإضافية.

### 3-3- نتائج الحمل على AMF (Load on Core Functions)

لتحليل أداء النظام بشكل أدق، تم استخدام دالة التوزيع التراكمي (Cumulative Distribution Function – CDF) كما يبين الشكل (6) لقياس توزيع أزمنة الاستجابة لجميع الطلبات داخل الشبكة، بدلًا من الاعتماد على المتوسط فقط.

تُعرّف دالة التوزيع التراكمي لزمن الاستجابة $T$ على أنها:

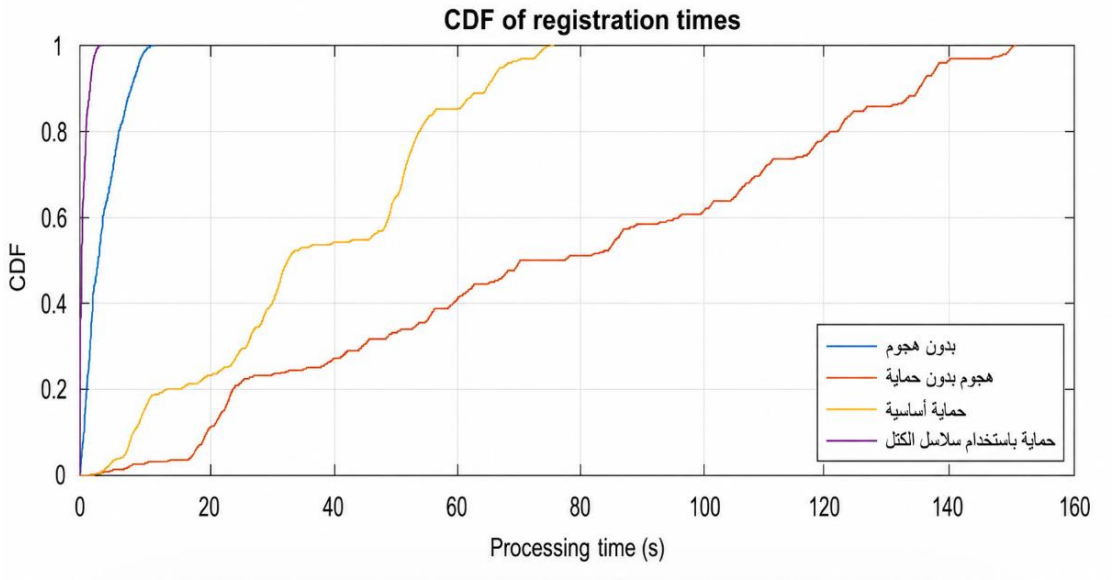
$$F(t) = P(T \leq t)$$

أي أنها تمثل احتمال أن يكون زمن استجابة الطلب أقل من أو يساوي قيمة معينة $t$.

وقد تم حساب CDF في هذه الدراسة وفق الخطوات التالية:

1. جمع بيانات زمن الاستجابة: تسجيل زمن الاستجابة لكل طلب يتم معالجته في الشبكة خلال المحاكاة.
2. ترتيب القيم تصاعديًا: يتم ترتيب جميع القيم $T_i$ من الأصغر إلى الأكبر.
3. حساب الاحتمال التراكمي: لكل قيمة $t$ ، يتم حساب:

$$F(t) = \frac{\text{عدد الطلبات التي تحقق } T \leq t}{\text{اجمالي عدد الطلبات}}$$




**الشكل (6): دالة CDF خلال زمن المعالجة**

وعندما نرسم CDF، نحن لا نعرض متوسط التأخير فقط، بل نُظهر كيف يتوزع الأداء على جميع المستخدمين. فكلما ارتفع منحنى CDF بشكل أسرع، كلما كان النظام يقدم استجابة أسرع لعدد أكبر من الطلبات وهو مؤشر أكثر دقة على جودة الخدمة. وفي نتائجنا، نلاحظ أن منحنى النظام المقترح يرتفع بسرعة مقارنة بالسيناريو بدون حماية، وهذا يعني أن أغلب الطلبات تتم معالجتها بزمن أقل، وبالتالي أداء أفضل وتحمل أعلى تحت الضغط.

وقد تم قياس عدد الطلبات التي وصلت فعليًا إلى AMF بعد المرور بطبقات الفلترة في الجدول (4):

**جدول (4): عدد الطلبات التي وصلت فعليًا إلى AMF بعد المرور بطبقات الفلترة**

| السيناريو | عدد الطلبات المعالجة | نسبة التخفيض |
|---|---|---|
| S2 | %100 | — |
| S3 | %67 | ↓%33 |
| S4 | %18 | ↓%82 |

إذاً الخوارزمية تقلل الحمل عن طريق:

- منع الطلبات المتكررة عبر Bloom Filter
- إسقاط الأجهزة المسيئة عبر Smart Contract
- منع إعادة المحاولة غير الضرورية

هذا يثبت أن النظام وقائي وليس مجرد كاشف.

### 3-4- مقارنة كمية مع الدراسات المرجعية

لتقييم فعالية النظام المقترح بشكل أدق، تم إجراء مقارنة كمية بين نتائج هذا البحث وبعض الدراسات المرجعية التي تناولت مشكلة عواصف الإشارات في شبكات الجيل الخامس، مع التركيز على مؤشرين رئيسيين هما: زمن الكشف (Detection Time) وزمن الاستجابة (Response Time). ويبين الجدول (5) مقارنة أداء النظام المقترح مع عدد من الدراسات السابقة. وتعكس هذه المؤشرات قدرة النظام على:

- اكتشاف الهجوم بسرعة
- تقليل تأثيره على أداء الشبكة

**جدول (5): مقارنة أداء النظام المقترح مع الدراسات السابقة**

| الدراسة | آلية الحماية | زمن الكشف (ثانية) | زمن الاستجابة (ثانية) | نوع المعالجة |
|---|---|---|---|---|
| [4] تحليل سلوك الإشارة | تحليل نمطي | 10~ | 18~ | كشف فقط |
| Rate Limiting [5] | تحديد معدل الإرسال | 6~ | 12~ | تخفيف جزئي |
| [6] تعلم آلي (ML) | SVM / RF | 4~ | 9~ | كشف متقدم |
| O-RAN xApp [8] | تحليل إحصائي | 5~ | 11~ | كشف على مستوى RAN |
| النظام المقترح (H-BAM) | + Blockchain + Bloom Hashing | 1.5~ | 3.9~ | كشف + منع مسبق |

يتضح من الجدول أن النظام المقترح يحقق تفوقًا ملحوظًا مقارنة بالأساليب التقليدية والحديثة، وذلك للأسباب التالية:

- انخفاض زمن الكشف: يعود ذلك إلى اعتماد النظام على التحقق المسبق باستخدام Bloom Filter والعقد الذكي، مما يسمح باكتشاف السلوك غير الطبيعي بسرعة كبيرة.
- تحسين زمن الاستجابة: حيث يتم منع الطلبات الضارة قبل دخولها إلى طابور المعالجة، بعكس الأنظمة التي تعتمد على الكشف بعد حدوث الازدحام.
- التحول من "كشف" إلى "منع": معظم الدراسات السابقة تركز على اكتشاف الهجوم، بينما يقوم النظام المقترح بمنع تأثيره قبل أن يصل إلى مكونات الشبكة.

وبالتالي يمكن ملاحظة أن:

- الأنظمة التقليدية (مثل Rate Limiting) تقلل التأثير لكنها لا تمنع الهجوم
- الأنظمة المعتمدة على التعلم الآلي توفر دقة جيدة لكنها تحتاج وقتًا أطول للكشف
- بينما النظام المقترح يقدم استجابة استباقية (Proactive Defense) تقلل كلًا من زمن الكشف وزمن الاستجابة بشكل كبير

## 4- الاستنتاجات والتوصيات:

من خلال تحليل النتائج التي تم الحصول عليها في هذه الدراسة، يمكن الوصول إلى مجموعة من الاستنتاجات الأساسية التي توضّح فعالية النهج المقترح H-BAM في الحد من عواصف الإشارات داخل شبكات الجيل الخامس، واستنادًا إلى هذه النتائج، يمكن اقتراح مجموعة من التوصيات التي قد تسهم في تطوير العمل مستقبلًا أو تحسين الأداء العملي للشبكات:

### 4-1- أهم الاستنتاجات:

- أظهر النظام المقترح قدرة واضحة على تقليل الحمل على طبقة التحكم من خلال تصفية جزء كبير من الطلبات غير الشرعية قبل وصولها إلى وحدة AMF، مما ساعد في خفض زمن المعالجة بنسبة تقارب 85% مقارنة بحالة الهجوم وتحسين استقرار الشبكة تحت الضغط.
- استخدام سلاسل الكتل والعقد الذكي ساهم في تعزيز الثقة ومصداقية عملية التحقق من الهوية، حيث وفّر سجلًا موزعًا لا يمكن التلاعب فيه، يسمح بالرجوع إلى بصمات الأجهزة السابقة والتأكد من عدم تكرار أنماط التسجيل المشبوهة.

- إضافة Salt مع آلية التجزئة أدت إلى رفع مستوى الأمان من خلال تقليل عدد الطلبات الضارة التي تصل إلى مكونات الشبكة، مما خفّض الازدحام وحسّن قدرة النظام على مقاومة هجمات عواصف الإشارات، وهو ما انعكس مباشرةً على انخفاض زمن الانتظار وتحسن منحنى CDF.، كما منعت المهاجمين من استخدام تقنيات مثل Rainbow Tables أو إعادة استخدام بصمات الأجهزة، مما أغلق بابًا مهمًا من أبواب الهجمات على نظام المصادقة.

**4-2- أهم التوصيات:**

- تطوير آلية أوسع للكشف عن السلوك الشاذ عبر دمج خوارزميات تعلم الآلة مع العقد الذكي، بهدف تعزيز دقة التمييز بين الطلبات الشرعية والضارة.
- توسيع النموذج ليشمل هجمات أكثر تعقيدًا مثل هجمات التدرج البطيء (Slow Signaling Attacks) التي يصعب اكتشافها باستخدام الأساليب التقليدية.
- دمج مصادر بيانات إضافية في عملية اتخاذ القرار، مثل معلومات الموقع، التردد، أو نمط الحركة، لتعزيز قدرة النظام على اكتشاف البوت نت وتحديد مصدر العاصفة.
- تنفيذ النموذج في بيئة شبه واقعية (Testbed) بدل الاعتماد الكامل على المحاكاة، للتحقق من سلوكه في ظروف أقرب إلى الشبكات التجارية.
- تحسين العقد الذكي ليصبح أكثر قدرة على التحديث الذاتي بناءً على أنماط الهجوم الجديدة، بحيث يستطيع النظام تعديل العتبات والمعايير دون تدخل بشري.

## 5- المراجع:


[1] CAO, J; XIONG, L.2023, *A survey on security aspects for 3gpp 5g networks*, *IEEE communications surveys & tutorials*, vol. 22, no. 1, pp. 170–195.

[2] SINGH, S; HOSEN, S; YOON, B.2021, *Blockchain security attacks, challenges, and solutions for the future distributed IoT network*, *IEEE Access,* vol. 9, pp. 13938–13959.

[3] Garg, S; Goyal, S; and Bhandari, A. 2025 *A Lightweight Blockchain-Based Scalable and Collaborative Mitigation Framework against New Flow DDoS Attacks in SDN Enabled Autonomous Systems*, *Scientific Reports,* vol. 15.

[4] JANGADA, A; DADLANI, N; RAINA, S; SOORAJ, V; BUCHADE, A .2022, *Decentralized voting system using blockchain, Proc. IEEE Int. Conf. Blockchain Distrib. Syst. Secur. (ICBDS),* pp. 1–5.
[5] KUMARI, A; GUPTA, R; TANWAR, S. 2024, *Amalgamation of blockchain and IoT for smart cities underlying 6G communication: A comprehensive review, Computer Communications*, vol. 172, pp. 102–118.
[6] KAPADIYA, K; PATEL, U; SHARMA, G; BOKORO, N.2022, *Blockchain and AI-empowered healthcare insurance fraud detection: An analysis, architecture, and future prospects, IEEE Access,* vol. 10, pp. 79606–79627.
[7] LIMAM, N; BOUTABA, R; ZEINATY, P; ZHANG, B. 2023, *Mitigating Signaling Storms in 5G with Blockchain-assisted 5GAKA, 19th International Conference on Network and Service Management (CNSM)*.
[8] PAULIAC, M.2020, *USIM in 5G Era Journal of ICT Standardization,* pp. 29– 40.
[9] ULLAH, K; RASHID, I; AFZAL, H; BANGASH, A; ABBAS, H.2020, *Ss7 vulnerabilities—a survey and implementation of machine learning vs rule-based filtering for detection of ss7 network attacks, IEEE Communications Surveys & Tutorials,* vol. 22, no. 2, pp. 1337–1371.
[10] BASIN, D; DREIER, J; HIRSCHI, L; RADOMIROVIC, S; SASSE, R; STETTLER, V. 2018, *A formal analysis of 5g authentication, in Proceedings of the 2018 ACM SIGSAC conference on computer and communications security,* pp. 1383–1396.
[11] KHAN, Q.2024, *Signaling storm problems in 3gpp mobile broadband networks, causes and possible solutions: A review, in International Conference on Computing, Electronics & Communications Engineering (iCCECE).* pp. 183–188.
[12] KHAN, A; BALAN, K; ABDULLAH, J.2024, *Secure trust-based blockchain architecture to prevent attacks in VANET, Sensors,* vol. 24, no. 4954.
[13] GAO, Z; ZHANG, D; M. ZHAO, M.2022, *BC-AKA: Blockchain based asymmetric authentication and key agreement protocol for distributed 5g core network, China Communications,* vol. 19, no. 6, pp. 66–76.
[14] CHOW M; MA, M.2022, A *secure blockchain-based authentication and key agreement scheme for 3gpp 5g networks, Sensors,* vol. 22, no. 12, p. 4525.
[15] HOFFMANN, M; KRYSZKIEWICZ, P.2023, *Signaling Storm Detection in IIoT Network Based on the Open RAN Architecture, ARXIV paper,* p.2302.
[16] PARK, S; KIM, D; YOU, I. 2022, *Machine learning based signaling DDOS detection system for 5g stand-alone core network, Applied Sciences,* vol. 12, no. 23, p. 12456.
[17] SADAWI, A; HASSAN, S; NDIAYE, M.2021, *A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges,' IEEE Access*, vol.9, pp. 54478–54497.
[18] KOUTSOS, A.2023, *The 5g-aka authentication protocol privacy, in IEEE European symposium on security and privacy (EUROS&P). IEEE,* pp. 464–479.
[19] Arthor, A et al. 2026, *Detection of RRC inactivity timer based signaling storm attack on 5G and B5G networks, Computer Networks*, vol. 282.
[20] AZHANG, B; AHOKANGAS, P; ALVES, H. 2024, *Key drivers and research challenges for 6G ubiquitous wireless intelligence*, *IEEE,* vol.38, p.23-30.