International Science and Technology Journal
المجلة الدولية للعلوم والتقنية
Volume 37 العدد
Part 1 المجلد
المجلة الدولية للعلوم والتقنية
International Science and Technology Journal
ISTJ

http://www.doi.org/10.62341/fagf0820

Received	2025/07/25	تم استلام الورقة العلمية في
Accepted	2025/08/23	تم قبول الورقة العلمية في
Published	2025/08/24	تم نشر الورقة العلمية في

تحديات الأمن في تقطيع شبكات الجيل الخامس (5G)

فدوى فريد الشيخ، أسماء عبد الله المنقوش، جبريل احمد جنات

كلية التقنية الصناعية – مصراتة، ليبيا.
Fadwa.farid90@cit.edu.ly, asma_elmangoush@cit.edu.ly,
ggannat@cit.edu.ly

الملخص

تعد شبكات الجيل الخامس Fifth generation networks (G5) نقلةً نوعيةً في عالم الاتصالات، فهي لا تهدف فقط لزيادة سرعة نقل البيانات، بل لخلق بنية تحتية مرنة وقادرة على استيعاب تنوع هائل في متطلبات التطبيقات والخدمات الحديثة. وفي صميم تحقيق هذه الرؤية، تبرز تقنية تقطيع الشرائح (Network Slicing) كأحد أهم الابتكارات المعمارية التي تعيد تعريف طريقة تشغيل الشبكات.

ومع ذلك هناك مخاوف أمنية لهذه التقنية، هذه المخاوف تفرض تحديات تحتاج إلى بحث وتحليل معمق، لهذا من الضروري تطوير حلول أمنية جديدة تتناسب مع الطبيعة الديناميكية لشبكات الجيل الخامس (5G)، فيجب مراعاة عدة قضايا أمنية مثل العزل بين الشرائح (Isolation)، المصادقة (Authentication)، التفويض أو التحقق من الصلاحيات (Authorization).

تقدم هذه الدراسة مراجعة منهجية للأبحاث العلمية الحديثة التي تناولت كيفية استخدام تقنيات مختلفة لتأمين شرائح شبكات الجيل الخامس (5G)، مستندة في ذلك إلى المقالات العلمية التي جُمعت من قواعد بيانات معتمدة، كما تقدم أيضاً توصيات عملية قابلة للتطبيق لتعزيز الأمن في بيئات (5G).

وقد تم التركيز على أهمية حماية تقنية تقطيع الشبكة إلى شرائح من التهديدات المحتملة ضمن ثلاثة مستويات مهمة وهي أمن دورة حياة الشريحة (Life-cycle Security)، أمن داخل الشريحة الواحدة (Intra-slice Security)، أمن بين الشرائح المختلفة (Inter-slice Security). تُظهر مراجعة الدراسات والأبحاث تقطيع الشبكات (Network Slicing) في شبكات الجيل الخامس (5G) اهتمام بحثي واسع بتقنية تقطيع

http://www.doi.org/10.62341/fagf0820

الشبكات في (5G) حيث يُركز الباحثون على الإدارة الذكية للموارد باستخدام التعلم العميق (Deep Learning) مثل نموذج(DeepSlice) لتحسين سرعة ومرونة الشبكة، نظرية استقرار ليابونوف (Lyapunov Stability Theory) وهي: أداء رياضية قوية لضمان استقرار النظام حتى في ظل نقص البيانات، التعلم المعزز متعدد الوكلاء (Multi-Agent RL) لإدارة الموارد من طرف إلى طرف (End-to-End)، التقنيات التمكينية مثل الافتراضية لوظائف الشبكة (NFV) Network Function Virtualization والشبكات المعرفة بالبرمجيات (SDN) Software Defined Networking تُعد أساسًا لتقطيع الشبكات، تم تطوير حلول أمنية تعتمد على الذكاء الاصطناعي لكشف هجمات (Denial of Service/ Distributed Denial of Service) (DoS/DDoS) بدقة عالية، بعض الأبحاث تحاكي الهجمات لتحليل الثغرات وتعزيز الدفاعات حيث تُستخدم تقنيات مثل التعلم الفيدرالي (Federated Learning) وتوجيه البصل (Onion Routing) مع التشفير الكامل لضمان إخفاء الهوية وسرية البيانات داخل الشريحة.

تعد هذه الورقة الأولى التي أعدت باللغة العربية في هذا المجال، تقدم مراجعة علمية للجوانب الأمنية في موضوع تقسيم الشبكات. تم إختيار الورقات العلمية التي نشرت خلال الخمس سنوات الماضية وتركز على الجانب الأمني لتقنية تقطيع الشبكات، مما يسهم في إثراء المحتوى العربي العلمي في هذا التخصص.

الكلمات المفتاحية: تقطيع الشبكة، شبكات الجيل الخامس (5G)، العزل بين الشرائح، المصادقة، التفويض، التهديدات الأمنية، الشبكات الافتراضية، أمن دورة حياة الشريحة، أمن داخل الشريحة، أمن بين الشرائح.

International Science and Technology Journal
المجلة الدولية للعلوم والتقنية
Volume 37 العدد
Part 1 المجلد
المجلة الدولية للعلوم والتقنية
International Science and Technology Journal
ISTJ

http://www.doi.org/10.62341/fagf0820

Security Challenges in 5G Network Slicing

Fadwa F. Alshaik , Asma Elmangoush, Gebriel A. Gananat

The College of Industrial Technology- Misrata, Libya
Fadwa.farid90@cit.edu.ly, asma_elmangoush@cit.edu.ly, ggannat@cit.edu.ly

Abstract

Fifth Generation (5G) networks represent a transformative leap in the world of telecommunications, as they aim not only to increase data transfer speeds but also to establish a flexible infrastructure capable of accommodating the vast diversity of modern application and service requirements. At the heart of realizing this vision, network slicing technology emerges as one of the most significant architectural innovations that redefine how networks operate. However, this technology raises security concerns, which pose challenges that necessitate in-depth research and analysis. Therefore, it is essential to develop new security solutions that align with the dynamic nature of 5G networks, taking into account several security issues such as isolation between slices, authentication, and authorization.

This study presents a systematic review of recent scientific research focusing on securing network slices in 5G environments. The review is based on peer-reviewed articles collected from trusted academic databases and offers practical and applicable recommendations to enhance 5G network security.

The paper emphasizes the protection of network slicing technology from potential threats across three critical levels: Life-cycle Security, Intra-slice Security, and Inter-slice Security.

The literature review highlights the extensive research interest in 5G network slicing, with particular attention to intelligent resource management using Deep Learning techniques such as the DeepSlice model to enhance network speed and flexibility. It also discusses the application of Lyapunov Stability Theory, a robust mathematical method to ensure system stability under data scarcity, and Multi-Agent Reinforcement Learning (MARL) for End-to-End resource management.

Enabling technologies such as Network Function Virtualization (NFV) and Software Defined Networking (SDN) are identified as foundational pillars of network slicing. AI-based security solutions have been developed to accurately detect Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. Some studies

http://www.doi.org/10.62341/fagf0820

simulate attacks to analyze vulnerabilities and strengthen defenses using techniques like Federated Learning and Onion Routing combined with end-to-end encryption to ensure data confidentiality and anonymity within slices.
This paper is the first prepared in Arabic in this field, providing a scientific review of the security aspects of network slicing. It selects scientific papers published over the past five years that focus on the security aspect of network slicing technology, contributing to enriching the Arabic scientific content in this specialization.
Keywords: Network Slicing, 5G Networks, Slice Isolation, Authentication, Authorization, Security Threats, Virtual Networks, Life-cycle Security, Intra-slice Security, Inter-slice Security.

1. مقدمة

مقارنة بالأجيال السابقة في مجال الاتصالات تقدم شبكات الجيل الخامس (5G) سرعة فائقة لنقل البيانات وزمن التأخير صغير جداً (Ultra-low latency)، مع القدرة على ربط عدد ضخم من الأجهزة، مما يجعل شبكات الجيل الخامس البنية التحتية الأساسية للكثير من الصناعات التي تحتاج إلى نقل البيانات بسرعة كبيرة وتطبيقات الزمن الحقيقي مثل: السيارات ذاتية القيادة والمدن الذكية والصناعة الذكية [1]. وتظهر معظم الدراسات التي تقارن بين أداء شبكات الجيل الرابع Fourth generation networks (4G) والجيل الخامس Fifth generation networks (5G) من حيث معدل الإرسال ونطاق التردد وعرض النطاق الترددي للقناة تفوق كبير لأداء شبكات الجيل الخامس [2].

شبكات (5G) تدعم عدد كبير جدًا من الأجهزة المتصلة التي تحتاج إلى اتصال موثوق يدعم كثافة عالية من الأجهزة في مناطق محدودة، يهدف هذا الاستخدام إلى تلبية احتياجات إنترنت الأشياء Internet of Things (IoT) بما يضمن الحصول على جودة الخدمة Quality of Service (QoS) لمجموعة متنوعة من الخدمات. وفقًا لمعيار 3rd Generation Partnership Project (3GPP) وإن المفاهيم الأساسية التي تشكل أساس شبكات الجيل الخامس هي [3]:

- **النطاق العريض المحمول المحسن Enhanced Mobile Broadband (eMBB)**: يهدف إلى توفير اتصال مستقر ومعدلات بيانات عالية، أي مخصص لنقل كميات كبيرة من البيانات مثل: بث فيديو عالي الدقة والواقع الافتراضي والوصول إلى الإنترنت بسرعات عالية.

http://www.doi.org/10.62341/fagf0820

- **الاتصالات فائقة الموثوقية ومنخفضة التأخير Ultra-Reliable (URLLC) Low Latency Communications:** تهدف إلى توفير زمن استجابة منخفض للغاية والموثوقية العالية جدًا، يُستخدم بشكل أساسي في التطبيقات التي تتطلب استجابات في الوقت الحقيقي، يستخدم في مجالات المصانع أو المركبات ذاتية القيادة والروبوتات والرعاية الصحية وخدمات الطوارئ التي تعتمد على تقنيات مثل إرسال نسخ متعددة من البيانات وتقنيات النقل المتقدم لضمان موثوقية الاتصال وتقليل التأخير.
- **الاتصالات من نوع الألة الضخم Massive Machine-Type (mMTC) Communications:** شبكات (5G) تهدف إلى دعم عدد كبير جدًا من الأجهزة المتصلة، هذه الأجهزة تحتاج إلى اتصال موثوق يدعم كثافة عالية من الأجهزة في مناطق محدودة ويهدف هذا الاستخدام إلى تلبية احتياجات إنترنت الأشياء (IoT) مع ضمان استهلاك منخفض للطاقة ودعم التوصيلات المستمرة للأجهزة المنتشرة في بيئة صناعية وتجارية متنوعة.

أحد الابتكارات الرئيسية لشبكات الجيل الخامس هي تقنية تقطيع الشبكة (Network Slicing)، التي تتيح إنشاء عدة شبكات افتراضية متعددة على بنية تحتية فيزيائية واحدة. مع هذه التكنولوجيا الجديدة تظهر مجموعة من التحديات المعقدة حيث يعد الأمان من أبرز القضايا في تقطيع الشبكة، فتقديم خدمات آمنة ومستمرة والحفاظ على نزاهة الشبكة أمرا بالغ الأهمية.

الهدف الأساسي من هذه الدراسة هو فهم شرائح الشبكة وإمكاناتها الأمنية، تحديد نقاط الضعف فيها وتحليل المتطلبات الأمنية الأساسية، واقتراح استراتيجيات للحماية. إذ توفر شرائح الشبكة مزايا كبيرة ولكنها تظل عرضة للثغرات سواء أثناء إنشائها لتقديم الخدمات من خلالها أو عند إنهائها. على حد علم المؤلفين، شهدت السنوات الأخيرة العديد من الأبحاث التي تناولت موضوع تقسيم الشبكات (Network Slicing) لكن عددًا محدودًا منها ركّز بشكل شامل على الجوانب الأمنية لهذه التقنية بداية من إعداد الشريحة وحتى إنهائها بعد انتهاء استخدامها. تعد هذه الورقة الأولى التي أعدت باللغة العربية في هذا المجال وتقدم مراجعة علمية للجوانب الأمنية في موضوع تقسيم الشبكات.

حيث تناولت هذه الدراسة مقدمة عن الجيل الخامس (5G) وشرح أهمية تقطيع الشبكة والتقنيات المساعدة لها، مع التركيز على التهديدات الأمنية المحتملة والطرق المتاحة لتأمينها، وتطرقنا إلى شرح خلفية تقنية تقطيع الشبكة وفحص المكونات الرئيسية والابتكارات والتقنيات المساعدة مثل: الافتراضية لوظائف الشبكة (NFV) Network

http://www.doi.org/10.62341/fagf0820

Software (SDN) والشبكات المعرفة بالبرمجيات Function Virtualization Defined Networking. التركيز على الجوانب الأمنية لتجزئة الشبكة، حيث يتم مناقشة أهمية تأمين هذه التقنية ضد التهديدات والهجمات المحتملة على شرائح الشبكة ويقترح حلولاً للتعامل معها، يقدم مراجعة منهجية للأبحاث العلمية ذات صلة التي درست كيفية استخدام تقنيات مختلفة لتأمين شرائح الشبكة، من المتوقع أن تساهم هذه الدراسة في تعزيز فهم التحديات الأمنية المرتبطة بتقطيع الشبكة وتقديم إطار عمل شامل لحماية الشبكات الافتراضية في بيئة شبكات الجيل الخامس (5G).

2. تقطيع الشبكة في الجيل الخامس (Network Slicing)

في العقود الأخيرة شهدنا زيادة كبيرة في عدد الأجهزة المتصلة بشبكات لاسلكية مثل الهواتف الذكية والتلفزيونات والأجهزة المنزلية الذكية ومع زيادة الطلب على الشبكات اللاسلكية، والتطور في تقنيات الحوسبة والاتصالات تطور الجيل الخامس من الشبكات المحمولة (5G) لدعم مختلف التطبيقات والخدمات الجديدة من خلال توفير سرعة عالية لنقل البيانات، وانخفاضاً في زمن الاستجابة، وقدرة على ربط عدد أكبر من الأجهزة مقارنة بالجيل الرابع (4G).

ولتحقيق ذلك قدمت شبكات الجيل الخامس (5G) مفهوم تقطيع الشبكة (Network Slicing) بأنه عملية تقسيم البنية التحتية الفعلية للشبكة إلى عدة شبكات افتراضية لتخصيص كل شريحة لتلبية خدمات متنوعة بشكل مرن وفعال، حيث يتم دمج العديد من الشبكات المنطقية ضمن بنية تحتية مشتركة، لكل شبكة منطقية لها طوبولوجيا منطقية خاصة بها، بذلك تقوم كل شبكة منطقية بأداء المهام المخصصة لها حيث تم تصميم كل جزء من الشبكة بناءً على خصائص الشبكة لتكون قادرة على تقديم خدمة للمستخدم النهائي، تكون الشرائح معزولة عن بعضها البعض لتوفير عزل أفضل للموارد.

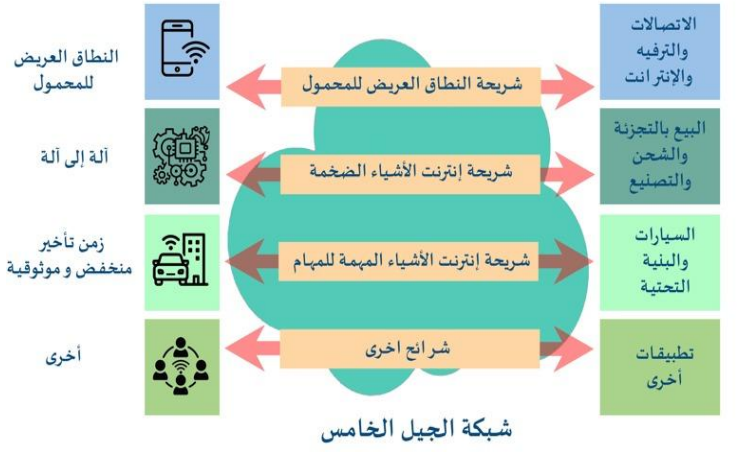
الشكل (1) يوضح مفهوم تقسيم الشبكة، حيث تعتبر كل شريحة بمثابة شبكة افتراضية شاملة صممت بشكل خاص وفقاً لاحتياجات محددة، ويمكن لمشغلي الشبكة تخصيص الموارد للمستأجرين (مقدمي الخدمات) الذين يمكنهم التحكم في كيفية استخدام هذه الموارد لتلبية متطلبات العملاء.

يعتمد تقسيم الشبكة على تقنيات الشبكات المعرفة بالبرمجيات (SDN) والافتراضية لوظائف الشبكة (NFV)، يتيح تقطيع الشبكة إنشاء شبكات منطقية متعددة فوق بنية تحتية مادية مشتركة، مما يُمكّن من تقديم الشبكة كخدمة Network-as-a-Service

http://www.doi.org/10.62341/fagf0820

(NaaS) أو كبنية تحتية قابلة للتخصيص Network-as-a-Platform (NaaP) تستخدم للشركات.

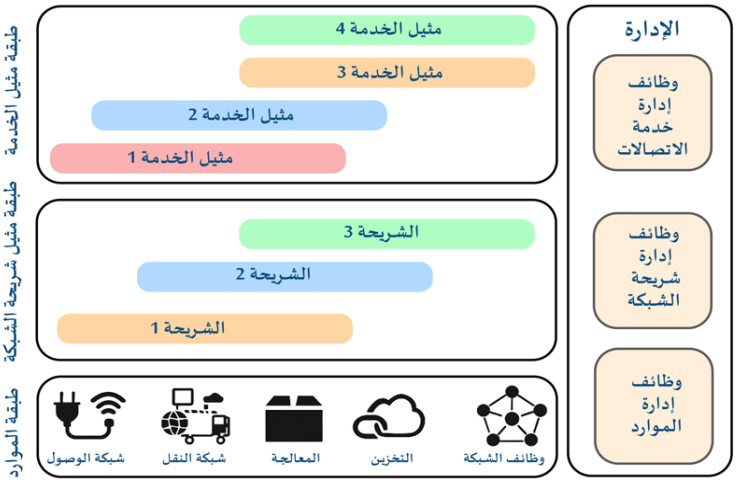
- NaaS: تقدم خدمات الشبكة للمستخدمين على أساس الاشتراك مثل باقي الخدمات السحابية.
- NaaP: تتيح تخصيص البنية التحتية للشبكة وبرمجتها حسب التطبيقات والخدمات المطلوبة دون الحاجة لإنشاء شبكة خاصة منفصلة [4].



الشكل (1): مفهوم تقطيع الشبكة

1.2. هيكل تقسيم الشبكة (Network Slicing Architecture): تقسيم الشبكة هو مفهوم رئيسي في شبكات الجيل الخامس حيث يسمح للمشغلين بتخصيص واستخدام البنية التحتية للشبكة بطريقة مرنة وفعالة لتلبية احتياجات مختلفة من الخدمات والتطبيقات، يعتمد تقسيم الشبكة على تقنيات الشبكات المعرفة بالبرمجيات (SDN) والافتراضية لشبكات الوظائف (NFV) باستخدام نفس البنية التحتية مما يتيح للمشغلين إدارة الموارد بشكل فعال، مما يمكنهم من التعامل مع زيادة حركة البيانات بشكل مناسب [5]؛ كما هو موضح في الشكل (2) تتكون بنية تقسيم الشبكة من ثلاث طبقات رئيسية:

http://www.doi.org/10.62341/fagf0820



الشكل (2): البنية العامة في تقطيع الشبكة

- **طبقة الموارد (Resource Layer):** الطبقة السفلية في هيكل تقسيم الشبكة التي تشمل وظائف الشبكة (اختيار الشريحة، التبديل وتوجيه البيانات) وتشمل الموارد التخزين والمعالجة ونقل بين العقد، تُستخدم هذه الموارد والوظائف لخدمة شريحة واحدة أو أكثر إذا لزم الأمر وتعمل هذه الطبقة على تزويد الطبقات العليا بالموارد المادية والافتراضية اللازمة لتوفير الخدمات [6].
- **طبقة مثيل الشريحة (Network Slice Instance Layer):** هذه الطبقة تم تصميمها لتلبية متطلبات الشبكة التي تم طلبها من قبل مثيل الخدمة، يمكن لكل شريحة أن تدير خدمة واحدة أو أكثر ولكن لا يمكن دمج شريحتين على نفس البنية المادية تقوم هذه الطبقة بتخصيص وتنظيم الشرائح لتلبية المتطلبات المحددة للخدمات المختلفة [6].
- **طبقة مثيل الخدمة (Service Instance Layer):** هذه الطبقة تحتوي على مثيل الخدمة التي تكون جاهزة للعملاء كل مثيل خدمة مرتبط بوظائف إدارة الموارد والشبكة الأساسية، يمكن تخصيص وظائف إدارة الموارد والشبكة إلى نطاقات إدارية مختلفة يتم إدارة دورة حياة الشريحة تتم عبر وظيفة إدارة تقسيم الشبكة التي تشرف على كل العمليات المتعلقة بإدارة الشرائح من التكوين إلى التفاعل مع العملاء [6].

2.2. دورة حياة الشريحة (Slice Life Cycle): دورة حياة الشريحة هي عملية متكاملة تتكون من أربع مراحل رئيسية تُدار عبر إدارة الشبكة لتحقق أهداف تخصيص

http://www.doi.org/10.62341/fagf0820

الموارد بفعالية كل مرحلة من هذه المراحل لها دور حاسم في ضمان الأداء الأمثل للشبكة كما هو موضح في الشكل (3)، فإن دورة حياة الشريحة تتضمن المراحل التالية:

الشكل (3): دورة حياة شريحة الشبكة

- **تخصيص الشريحة (Slice Commissioning):** في هذه المرحلة لا توجد شريحة حقيقية بعد، يتم إعداد البيئة الشبكية من خلال جمع معلومات العملاء لتحديد الخدمات التي يتوقعونها (مثل المتطلبات من حيث الأداء، النطاق الترددي، وزمن التأخير) بناءً على هذه المعلومات يتم إنشاء قالب الشريحة الذي يحتوي على تفاصيل حول مكونات الشريحة وهيكلها وتكوينها وكما يشمل أيضاً تحديد الموارد المطلوبة (مثل المعالجة، التخزين، النقل) وكيفية تخصيصها لتلبية احتياجات الخدمة المحددة. أي هي المرحلة التمهيدية التي يتم فيها تهيئة البيئة الشبكية لاستيعاب الشريحة الجديدة بشكل فعّال تشمل هذه المرحلة ما يلي [6]:

1) جمع المتطلبات الفنية (Technical Requirements).
2) تحديد حالات الاستخدام (Use Cases) بدقة.
3) تحديد الموارد اللازمة (موارد الحوسبة، التخزين، الشبكة).
4) دراسة شاملة للاعتبارات الأمنية.
5) تحديد معايير جودة الخدمة (QoS).
6) إنشاء قوالب شرائح (Slice Templates) تُستخدم في المراحل التالية.

- **تنشيط الشريحة (Slice Activation):** في هذه المرحلة تبدأ عملية تثبيت وتكوين الموارد والوظائف الشبكية بناءً على القالب الذي تم إنشاؤه في مرحلة تخصيص

http://www.doi.org/10.62341/fagf0820

الشريحة (المرحلة الأولي) فيتم إنشاء الشريحة باستخدام هذا القالب مع تخصيص الموارد الافتراضية والمادية اللازمة، بعد أن يتم إعداد الشريحة بشكل كامل تُصبح جاهزة للتنشيط في هذه المرحلة تصبح الشريحة عملية وقادرة على تقديم الخدمة للمستخدمين أو العملاء الذين طلبوا الخدمة أي:

1) نشر الشريحة الجاهزة مسبقًا بناءً على القالب الذي يحدد متطلبات الأداء (مثل السعة وجودة الخدمة)
2) تفعيل الخدمات لتكون جاهزة للاستخدام من قبل المستخدمين أو العملاء.

- **العمليات والمراقبة في وقت التشغيل (Run Time Operations and Monitoring):** في هذه المرحلة تبدأ الشريحة في العمل الفعلي وتقديم الخدمات المطلوبة للعملاء يتم مراقبة الشريحة بشكل دوري لضمان توفر الخدمة وجودتها باستمرار للتأكد من أدائها الصحيح تشمل هذه المراقبة متابعة جوانب مثل [6]:

1) تحسين استخدام الموارد (مثل المعالجة، النطاق الترددي).
2) جودة الخدمة (QoS).
3) اكتشاف الأعطال ومعالجتها فورا.
4) زمن التأخر وموثوقية الشبكة.

التعديلات قد تكون ضرورية في هذه المرحلة، مثل تغيير بعض التكوينات أو تحديث الروابط بين وظائف الشبكة والموارد لضمان أن الشريحة تظل قادرة على تلبية متطلبات العملاء بشكل فعال.

- **إلغاء تخصيص الشريحة (Slice Decommissioning):** في هذه المرحلة يتم إلغاء تخصيص الشريحة بشكل كامل أي يتم تحرير جميع الوظائف والموارد المرتبطة بالشريحة وهذا يعني أن جميع الموارد التي كانت مخصصة لهذه الشريحة تُسترجع وتصبح متاحة للاستخدام في خدمات أو شرائح أخرى ويُعد هذا بمثابة انتهاء دورة حياة الشريحة، حيث لا يتم تقديم الخدمة بعد الآن وتُعتبر الشريحة قد تم إنهاؤها [6].

3. حاجة الأمان في تقسيم الشبكات (Need for Security in Slices)

تقسيم الشبكات يُعدّ ابتكارًا مثيرًا له القدرة على تغيير كيفية استخدام الشبكات بشكل جذري، لكن كما هو الحال مع أي ابتكار تقني فإن هذا التحول الكبير في البنية التحتية للشبكة يأتي مع تحديات أمنية يجب عدم تجاهلها من أجل الاستفادة الكاملة من تقسيم الشبكات

http://www.doi.org/10.62341/fagf0820

مع الحفاظ على الاعتمادية والثقة في النظام البيئي للشبكة، يجب معالجة هذه المخاوف الأمنية بشكل فعَّال [7]، لتحقيق المتطلبات الاساسية وهي:

1.3. السرية (Confidentiality): الحفاظ على حماية البيانات والمعلومات الحساسة من الوصول غير المصرح به داخل الشريحة من المهم ضمان وصول الأجهزة المصرح بها فقط إلى البيانات. التدابير للتحقق من سرية البيانات يمكن تلخيصها فيما يلي:

- العزل (Isolation): يجب عزل الشرائح عن بعضها لتجنب تسرب البيانات بين الشرائح.
- البروتوكولات الآمنة: استخدام بروتوكولات آمنة في نقل البيانات لمنع التنصت والتلاعب بالبيانات.
- إخفاء البيانات (Data Masking): في بعض الحالات الحساسة يمكن استبدال البيانات الأصلية ببيانات وهمية أو معرّفة بشكل جزئي أثناء النقل.
- بالإضافة إلى آليات مثل التحكم بالوصول، التشفير، وفك التشفير.

2.3. سلامة البيانات (Integrity): التأكد من أن البيانات والموارد داخل بيئة الشبكة الافتراضية صحيحة ولم يتم التلاعب بها أي غير معدلة. والتدابير المستخدمة للتحقيق من سلامة البيانات هي [7]:

- التحقق من البيانات (Data Validation and Verification): تطبيق آليات للتحقق من سلامة البيانات باستخدام دوال التحقق مثل التجزئة (Hashing).
- كشف ومنع التسلل (Intrusion Detection and Prevention): تطبيق آليات لكشف ومنع الوصول غير المصرح به أو الأنشطة التي قد تضر سلامة البيانات.
- النسخ الاحتياطي والاستعادة (Backup and Recovery): تنفيذ عمليات نسخ احتياطي واستعادة منتظمة لضمان العودة إلى حالة معروفة في حال حدوث تلاعب أو فساد للبيانات.

3.3. التوافر (Availability): ضمان أن الموارد والخدمات والتطبيقات داخل الشريحة قابلة للوصول والتشغيل عند الحاجة إليها. التدابير لتحقيق التوافر[7]:

- التكرار وتوزيع الحمل (Redundancy and Load Balancing): التكرار يعني نسخ المكونات الحاسوبية الهامة مثل الخوادم والموجهات router بحيث يمكن استخدام النسخة الاحتياطية في حالة الفشل، أما توزيع الحمل فيتضمن توزيع حركة المرور عبر عدة خوادم لضمان الأداء الأمثل.

http://www.doi.org/10.62341/fagf0820

- اتفاقيات مستوى الخدمة Service Level Agreements (SLAs): الالتزام باتفاقيات مستوى الخدمة التي تحدد مستوى التوافر المتوقع للخدمات المختلفة.
- آلية الفشل (Failover Mechanism): إعداد آلية لتحويل الخدمة تلقائيًا إلى الموارد الاحتياطية في حال الفشل لضمان استمرارية التوافر.

4.3. الطبيعة المشتركة للتقسيم (Shared Nature of Slicing): يسمح تقسيم الشبكات بالعديد من الشبكات الافتراضية بالتشارك في نفس البنية التحتية المادية، مما يجعل من الصعب حماية كل شبكة من الهجمات.

المخاطر المتعلقة بالطبيعة المشتركة: استنفاد الموارد، استغلال الموارد، القنوات السرية، المخاطر متعددة الإيجار (Multi-Tenancy Risks)، التغيرات الديناميكية، وأحمال غير قابلة للتوقع.

التدابير للتعامل مع المخاطر:

- التكيف الديناميكي للأمن (Dynamic Security Adaption): تنفيذ تدابير أمنية قابلة للتكيف واستخدام أدوات تعتمد على التعلم الآلي أو الذكاء الاصطناعي للكشف والاستجابة للتهديدات المستجدة.
- التحكم في تعدد الإيجارات (Multi-Tenancy Controls): ضمان عزل بين المستأجرين وتطبيق آليات قوية للتحكم بالوصول والمصادقة لضمان وصول آمن للمستأجرين المصرح لهم فقط.

5.3. التهديدات الإلكترونية (Cyber Threats): التهديدات الإلكترونية أصبحت أكثر تطورا واستهدافا؛ مما يشكل تحديا كبيرا للحصول على شبكة أمنة من التهديدات المحتملة: انتحال هوية الشريحة (Slice Identity Spoofing)، الجيران الصاخبين (Noisy Neighbors)، التحرك الجانبي (Lateral Movement)، التداخل (Interference)، مشاكل جودة الخدمة (QoS). التدابير لمكافحة التهديدات: إجراء تدقيقات أمنية دورية ومراقبة أداء الشريحة ونمط حركة المرور لضمان عدم حدوث أي اختراقات.

http://www.doi.org/10.62341/fagf0820

4. التحديات الأمنية في تجزئة تقسيم الشبكة Security Challenges in Network Slicing

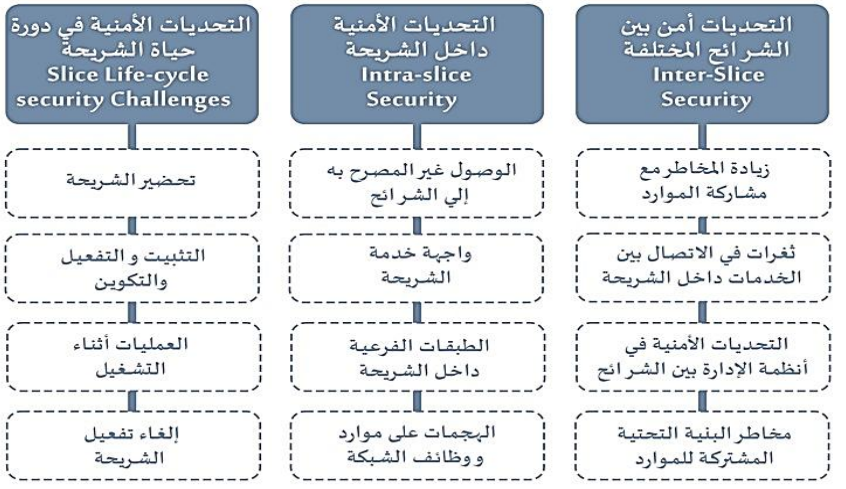
يعد تقسيم الشبكة باستخدام تقسيم للبنية التحتية والموارد منفتحًا على مجموعة متنوعة من الثغرات الأمنية في تكنولوجيا (5G)، أيضاً مشاركة الموارد بين شرائح الشبكة تنشئ ثغرات أمنية مع وجود بنية أساسية مشتركة، يتم تصميم الشرائح لتحتوي على بروتوكولات أمنية مختلفة بهدف تحسين الأداء، ومع ذلك هذا قد يخلق ثغرات إذا كانت الشرائح الأخرى على نفس الشبكة تشترك في نفس البروتوكولات الأمنية في هذه الحالة يمكن استغلال البروتوكولات القابلة للتعديل على أساس الشريحة مما يشكل تهديدًا لبقية الشرائح لذلك من الضروري أخذ بروتوكولات الأمان في الاعتبار بين الشرائح المختلفة عند التعامل مع المخاوف المتعلقة بمشاركة الموارد.

لمشاركة البنية التحتية مزايا كبيرة في تقليل التكلفة واستهلاك الموارد ومع ذلك فإن هذه المشاركة تخلق تحديات في تأمين شبكات (5G) والتخفيف من المخاطر المرتبطة ببنية تقسيم الشبكة [8].

تصنيفات الثغرات الأمنية المتعلقة بتقسيم الشبكة في تكنولوجيا (5G) في إنشاء مخاوف جديدة تتطلب معالجة دقيقة وتتمثل هذه المخاوف الأمنية في ثلاثة أنواع رئيسية من الثغرات الأمنية نستعرضها في هذا المقال مع أهم التوصيات للتغلب عليها:

- تحديات أمن دورة الحياة الشريحة (Life-cycle Security).
- تحديات أمن داخل الشريحة الواحدة (Intra-slice Security).
- تحديات أمن بين الشرائح المختلفة (Inter-slice Security).

http://www.doi.org/10.62341/fagf0820



الشكل (4): التهديدات لكل مرحلة من مراحل دورة حياة الشريحة

1.4. التحديات الأمنية في دورة حياة الشريحة (Slice Life-Cycle Security Challenges):

في الجزء السابق من المقالة، تم توضيح مراحل حياة الشريحة: تحضير الشريحة والتثبيت والتكوين والتفعيل الشريحة والعمليات والمراقبة في وقت التشغيل وإلغاء تخصيص الشريحة، هناك بعض القلق الأمني المرتبط بدورة حياة الشريحة في مراحل مختلفة من هذه الدورة. يمكن حل هذه المخاوف في التصميم خلال مراحل التحضير والتثبيت والتكوين والتفعيل وكذلك الثغرات الوظيفية خلال مرحلة التشغيل وأيضًا أثناء إلغاء التفعيل.

- **المرحلة الأولى: تحضير الشريحة (Preparation):** تُعرف هذه المرحلة أيضًا بالتحضير حيث قد تؤدي القوالب المصممة بشكل غير جيد للشريحة إلى تعرضها للثغرات التي قد يتم استغلالها في المستقبل، في هذه المرحلة من الممكن أن تصبح الشريحة هدفًا للهجمات بسبب العيوب في التصميم أي يمكن أن تؤدي العيوب التي يتم اكتشافها أثناء مرحلة تطوير النظام إلى مخاوف أمنية خطيرة في مرحلة التشغيل وأثناء إلغاء التفعيل، فإذا العيوب في مرحلة التحضير هي نقطة الانطلاق للهجمات المحتملة في المستقبل، يمكن استخدام البروتوكولات التشفير لضمان السرية (سواء أثناء النقل أو التخزين) والنزاهة والمصداقية للقوالب، يجب أيضًا التحقق من صحة القالب قبل الاستخدام، يمكن اعتبار التحليل الأمني في الوقت الفعلي عند استخدام القالب كممارسة جيدة.
- **المرحلة الثانية: التثبيت والتفعيل والتكوين (Installation, Activation, and Configuration):** هذه المرحلة تمثل بداية تنفيذ القالب التصميمي لشبكة

http://www.doi.org/10.62341/fagf0820

الشريحة إلى شريحة فعلية في الشبكة، حيث تبدأ الشريحة في أداء وظائفها، قد تظهر بعض المخاوف الأمنية في هذه المرحلة نتيجة لتطبيق القالب التصميمي على الشبكة قد يؤدي التطبيق غير الصحيح للقالب إلى أخطاء قد تفتح الشبكة لثغرات أمنية مثل إنشاء شرائح مزيفة أو تعديل تكوينات الشرائح قبل أو أثناء هذه المرحلة، أخطاء في التثبيت أو التكوين قد تجعل الشبكة عرضة لمشاكل أمنية من الممكن أن تؤثر بشكل كبير على عمل الشريحة.

- **المرحلة الثالثة: العمليات أثناء التشغيل (Run-Time Operations):** تُعد مرحلة التشغيل هي المرحلة التي تتم فيها معالجة الوظائف الفعلية للشريحة في الشبكة إذا كانت المرحلتان السابقتان تعانيان من عيوب فإن هذه المرحلة ستعرض هذه العيوب وتظهر الثغرات الأمنية بشكل أكثر وضوحًا، في هذه المرحلة يمكن أن تصبح الشريحة عرضة للهجمات مثل هجمات رفض (حجب) الخدمة الموزعة Distributed (DDoS) Denial of Service هذه الهجمات تستهدف تعطيل توفير الخدمات الشبكة عن طريق إغراق الشبكات بحزمة بيانات ضخمة مما يؤدي إلى تعطلها وجعلها غير قابلة للوصول من قبل المستخدمين الآخرين، انتهاك خصوصية البيانات أو حتى الرفض الكامل للوصول إلى الشريحة أي تغييرات في تكوين الموارد خلال هذه المرحلة قد تفتح المجال أمام المزيد من الثغرات الأمنية لذلك يجب معالجة هذه المخاوف من خلال مراقبة دقيقة وتحسين أمان الشريحة خلال فترة التشغيل.
- **المرحلة الرابعة :إلغاء تفعيل الشريحة (Decommissioning):** المرحلة الأخيرة من دورة حياة الشريحة هي مرحلة إلغاء التفعيل، حيث قد تكون هناك مخاوف أمنية تتعلق بخصوصية البيانات وإعادة تخصيص الموارد إذا كانت بروتوكولات إلغاء التفعيل غير فعالة فقد يؤدي ذلك إلى تعريض البيانات الحساسة للخطر أو استنفاد الموارد التي كانت مخصصة سابقًا بشكل غير ضروري قد يؤدي الإلغاء غير الفعّال للشريحة إلى مشاكل أمنية إضافية تتعلق بعدم تنظيف الموارد بشكل صحيح أو ترك البيانات الحساسة مكشوفة بعد إلغاء التفعيل لذا من الضروري أن يتم إلغاء التفعيل بطريقة آمنة لضمان عدم تعرض الشبكة لأي اختراقات أو تسريبات بعد إنهاء الشريحة [6].

2.4. التحديات الأمنية داخل الشريحة (Intra-slice Security): في شبكات (5G) تتعلق بالحفاظ على الأمان داخل الشريحة نفسها، حيث يمكن أن تكون هناك ثغرات أمنية تؤثر على الأداء والخدمات في الشبكة أبرز هذه التحديات:

http://www.doi.org/10.62341/fagf0820

- **الوصول غير المصرح به إلى الشرائح:** يتطلب الوصول إلى الشريحة آليات تحقق قوية لحماية الشبكة من الهجمات غير المصرح بها، مثل هجمات "رفض الخدمة(Denial of Service) (DoS)" التي قد تؤثر على وظائف الشبكة.
- **واجهة خدمة الشريحة:** تشكل الواجهة بين الشريحة والخدمات نقطة ضعف محتملة، حيث يمكن استغلالها في الهجمات لذلك من المهم تطبيق ضوابط أمنية قوية وتحقيق عزل جزئي بين الخدمات للحد من تأثير الهجمات.
- **الطبقات الفرعية داخل الشريحة:** تتكون الشريحة أحيانًا من طبقات فرعية قد تحتوي على بروتوكولات أمان ضعيفة مما يعرضها لهجمات يمكن تقليل هذا الخطر عبر العزل التام بين الطبقات الفرعية وتنفيذ تطبيق متطلبات التحقق المتبادل حيث يشارك كل من المستأجرين (Tenants) والمضيفين (Host) في عملية التحقق عند وجود مدير واحد للشريحة وفي حالة كان هناك عدة مستأجرين يديرون الشريحة يجب أن يقوموا بالتحقق من بعضهم البعض لتقليل خطر الوصول غير المصرح به.
- **الهجمات على الموارد ووظائف الشبكة:** قد تتعرض الموارد ووظائف الشبكة التي تعتمد عليها الشريحة لعدة أنواع من الهجمات، بما في ذلك التلف المادي أو الهجمات الإلكترونية أو الهجمات البرمجية التي قد تضر بوظيفة الشريحة، لضمان التحقق الموثوق، يجب إعطاء أولوية لـ:

1) الإقلاع الآمن (Secure Booting).
2) الوصول إلى البيانات المعتمدة (Credential Access).
3) التحقق من النزاهة (Integrity Verification).
4) الأمن المادي (Physical Security).

كل هذه الجوانب تتطلب الاهتمام لضمان أن الشريحة يمكنها الحفاظ على وظائفها وحمايتها من الهجمات أو الاستغلال التي قد تضر بها [6].

3.4. التحديات أمن بين الشرائح المختلفة (Inter-Slice Security):

تقسيم الشبكة يظهر من خلال الثغرات المحتملة التي قد تنتج عن مشاركة الموارد في البنية التحتية الأساسية المشتركة مع زيادة انتشار أجهزة المستهلكين في شبكات (G5)، تصبح هذه الأجهزة هدفًا مغريًا للهجمات قد يستغل جهاز مستهلك مُصرح له بالوصول إلى شريحة روابط بين الشرائح ليحصل على وصول غير مصرح به إلى شرائح أخرى مما يسهل على المهاجمين التسلل، هذه التهديدات تكون أكثر خطورة لأن المهاجم قد يكون

http://www.doi.org/10.62341/fagf0820

جهازًا موثوقًا بالفعل وليس طرفًا خارجيًا وبالتالي قد يتمكن المهاجم من استغلال سلسلة من الشرائح داخل الشبكة للوصول إلى معلومات أو خدمات أخرى، أبرز هذه التحديات:

- **زيادة المخاطر مع مشاركة الموارد:** عندما تشارك الشرائح في الموارد يكون من الأسهل تنفيذ هجمات مثل "رفض الخدمة (DoS)" ضد شريحة تشارك الموارد مقارنة بشريحة مستقلة، حيث يمكن للاختراق في شريحة أقل أمانًا أن يفتح الطريق لتهديد الشرائح الأخرى للتقليل من هذه المخاطر يجب فرض عزل صارم بين الشرائح.
- **ثغرات في الاتصال بين الخدمات داخل الشريحة:** الاتصال بين الخدمات داخل الشريحة أو بين الشرائح يمكن أن يكون نقطة ضعف محتملة، إذا كانت الشرائح في البنية التحتية تقدم خدمات مختلفة فقد يؤدي وجود ثغرة في خدمة واحدة إلى تسريب الهجوم إلى خدمات أخرى، حيث يمكن أن يستخدم المهاجم خدمة مخترقة في شريحة للوصول إلى خدمات أخرى يحمي العزل بين الشرائح هذا النوع من المخاطر.
- **التحديات الأمنية في أنظمة الإدارة بين الشرائح:** إدارة الشرائح المشتركة تزيد من خطر الهجمات التي تستهدف عدة شرائح في وقت واحد لذلك من الضروري عزل مناسب داخل البنية التحتية لإدارة الشرائح، كما يجب فرض قيود على التغييرات التي يمكن إجراؤها على الشرائح داخل ادارة الشرائح لضمان أنه لا يمكن تعديل إعدادات الشرائح إلا من قبل الأفراد المصرح لهم.
- **مخاطر البنية التحتية المشتركة للموارد:** مشاركة الموارد الحسابية بين الشرائح يمكن أن يؤدي إلى استهلاك مفرط للموارد مما يضر بأداء الشبكة لتقليل هذه المخاطر يجب تخصيص الموارد بعناية وعزل الشرائح التي تشترك في نفس الموارد [6].

5. الحلول التكنولوجية نحو أمان شبكة (5G) Technological Solutions (Towards 5G Network Security)

تم تحليل الثغرات الأمنية التي يقدمها تقسيم الشبكة بعمق في الأقسام السابقة بناءً على نوع الثغرة في هذا القسم، سيتم تقييم الحلول المختلفة التي يمكن تنفيذها لمكافحة هذه الثغرات الأمان من النهاية إلى النهاية، والعزل، والإدارة الآمنة وتنسيق شرائح الشبكة ضمن بنية مشتركة [6].

1.5. الأمان من النهاية إلى النهاية (End-to-End Security): هو استراتيجية فعّالة لحماية شبكات (5G) المبنية على تقنية تقسيم الشبكة من المخاطر الأمنية،

http://www.doi.org/10.62341/fagf0820

ويشمل حماية البيانات والاتصالات بين المكونات المختلفة داخل الشبكة، يتمثل التحدي الأمني في وجود نوعين من الاعداء:

- **المعتدون ذوي التحكم الإداري (Adversaries with administrative control)**: مثل مشغلي الشبكة أو مهاجمين تمكنوا من اختراق الشبكة.
- **المعتدون الخارجيون (External adversaries)**: مثل مستخدمي الشبكة الذين قد يحاولون الهجوم على الشبكة.

مفهوم الأمان من النهاية إلى النهاية يتضمن عزل الشبكات الافتراضية التي تشكلها الشرائح عن بعضها وعن البنية التحتية للشبكة، مما يحسن الأمان ضد المعتدين الخارجيين وأولئك الذين يمتلكون صلاحيات إدارية، التحكم في الضعف الناتج عن التواصل بين الواجهات يشمل حماية الاتصال بين الشرائح الأجزاء الفرعية والخدمات عبر تطبيق الأمان من نهاية إلى النهاية باستخدام التشفير وفك التشفير للبيانات التي تخرج وتدخل الشريحة لضمان أن البيانات محمية أثناء النقل، التشفير يُعد جزءًا أساسيًا من الأمان من النهاية إلى النهاية حيث يضمن حماية البيانات أثناء انتقالها عبر الشبكة وعدم تعرضها للسرقة أو التلاعب [8].

2.5. العزل (Isolation): في شبكات (5G) يُعتبر وسيلة أساسية لمواجهة التحديات الأمنية الناتجة عن تقسيم الشبكة ومشاركة الموارد بين العديد من المستأجرين العزل يساعد في تقليل الثغرات الأمنية ومنع انتقال التهديدات بين الشرائح المختلفة داخل الشبكة هناك نوعان رئيسيان من العزل في هذا السياق:

- **العزل بين الشرائح (Inter-slice isolation)**: يتم في هذا النوع فصل الموارد المادية (الأجهزة المضيفة) عن كل شريحة مما يحول دون مشاركة الشرائح لنفس الموارد المادية هذا يحد من التواصل بين الشرائح ويمنع التهديدات من الانتقال من شريحة إلى أخرى، مما يوفر حماية قوية ضد الهجمات المشتركة على البنية التحتية.
- **العزل داخل الشريحة (Intra-slice isolation)**: يركز هذا النوع على فصل الموارد داخل الشريحة نفسها بحيث يتم تخصيص موارد منفصلة لكل مكون من مكونات الشريحة الهدف من هذا هو زيادة الكفاءة وتقليل الحاجة إلى تدابير أمان معقدة عبر جميع الشرائح، مما يحسن الأداء ويقلل من المخاطر الأمنية داخل الشريحة [8].

فوائد العزل في تقليل الهجمات: أثبت العزل كأداة فعّالة في تقليل تأثير هجمات الحرمان من الخدمة الموزعة (DDoS)، حيث يحد من انتشار الهجوم بين الشرائح إذا تم استهداف

http://www.doi.org/10.62341/fagf0820

شريحة معينة تبقى الشرائح الأخرى محمية العزل يساهم أيضًا في تقليل الروابط بين الشرائح، مما يقلل من فرص الهجوم الواسع النطاق [9].

3.5. الإدارة المؤمنة وتنسيق شرائح الشبكة (Secure Management and Orchestration): تعتبر من الإجراءات الأساسية لتقليل المخاطر الأمنية في شبكات (5G) التي تعتمد على تقسيم الشبكة بينما يُعد الأمان من النهاية إلى النهاية مناسبًا لمواجهة التهديدات الخارجية، إلا أنه هناك مخاطر كبيرة تتعلق بالمهاجمين الذين يمتلكون التحكم الإداري في النظام لذلك يجب تعزيز الإدارة والتنظيم للحد من هذه المخاطر تشمل الأساليب المستخدمة:

- **تحسين أنظمة التحكم في الوصول:** لضمان عدم الوصول غير المصرح به إلى الشرائح.
- **الشبكات الخاصة الافتراضية:(Virtual Private Networks (VPNs))** تساعد في حماية البيانات وحركة المرور داخل الشبكة.
- **قدرات التوثيق المتقدمة:** تهدف إلى تقليل الثغرات الناتجة عن مشاركة الموارد بين الشرائح [9].

4.5. التحقق المتبادل واتفاقيات مستوى الخدمة الأمنية (Security Level Service Agreement (SLSA)): من أجل تقليل المخاطر الناتجة عن مشاركة بنية تحتية بين مستأجرين مختلفين يمكن تنفيذ التحقق المتبادل بين المستأجرين لضمان عدم الوصول غير المصرح به إلى الشرائح الأخرى، إلى جانب ذلك فإن اتفاقيات مستوى الخدمة الأمنية (SLSA) تلزم مزودي الخدمات بتطبيق بروتوكولات أمان معتمدة لإدارة الشرائح بشكل آمن. يمكن تعزيز الأمان من خلال توزيع الوظائف بين الشرائح بحيث يتم تخصيص المهام، مما يقلل من تعرض الشرائح لهجمات مثل هجمات الحرمان من الخدمة الموزعة (DDoS) ولتحقيق هذا، يتم استخدام بنية تحتية للمفاتيح العامة (Public Key Infrastructure (PKI)) لتحسين إدارة الشرائح وتعزيز الأمان فيها [9].

6. المراجعة المنهجية للأعمال السابقة.

شهدت السنوات الأخيرة العديد من الأبحاث التي تناولت موضوع تقسيم الشبكات (Network Slicing) لكن عددًا محدودًا منها ركّز بشكل شامل على الجوانب الأمنية

http://www.doi.org/10.62341/fagf0820

لهذه التقنية بداية من إعداد الشريحة وحتى إنهائها بعد انتهاء استخدامها. تعد هذه الورقة الأولى التي أعدت باللغة العربية في هذا المجال وتقدم مراجعة علمية للجوانب الأمنية في موضوع تقسيم الشبكات. تم إختيار الورقات العلمية التي نشرت خلال الخمس سنوات الماضية والتي تركز على الجانب الأمني لتقنية تقطيع الشبكات.

من خلال مراجعة البحوث والدراسات يظهر الاهتمام البحثي المكثف بتقنية تقطيع الشبكات (Network Slicing) في الجيل الخامس (5G). ركز عدد من الباحثين: على آليات الإدارة الذكية لتقطيع الشبكات، إذ يوجد اتجاهان لتحقيق الادارة الذكية من خلال التحسين الديناميكي للموارد باستخدام الذكاء الاصطناعي لرفع كفاءة تقطيع الشبكات وإدارة الموارد بذكاء.

الاتجاه الأول يقدمان البحثان [10] و [11] انموذجاً ذكياً (DeepSlice) يعتمد على التعلم العميق لاتخاذ قرارات ديناميكية بشأن اختيار الشريحة المناسبة وتخصيص الموارد بكفاءة، مما يجعل الشبكة أسرع وأكثر مرونة وقدرة على التعامل مع ملايين الطلبات بدقة عالية. يقدم الباحث [12] مستوى أعمق حيث يدمج التعلم العميق مع نظرية استقرار ليابونوف (Lyapunov Stability Theory) وهي أداة رياضية قوية لضمان استقرار النظام حتى في ظل نقص البيانات محققاً تحسناً ملحوظاً مقارنة بالخوارزميات الأخرى.

الاتجاه الثاني يعمل في سياق إدارة الموارد من طرف إلى طرف (End-to-End) يستخدم الباحث [13] التعلم المعزز متعدد الوكلاء (Multi-Agent RL) لتنسيق تخصيص الموارد بشكل تعاوني وفعال في بيئات الحوسبة الطرفية متعددة الوصول (Multi-access Edge Computing (MEC)).

يقدم الباحث [14] مسحاً شاملاً للتقنيات التمكينية الرئيسية مثل (SDN) و(NFV) التي تعتبر كأساس لتقطيع الشبكات. يقدم الباحث [15، 16] تصنيفاً للحلول الأمنية المعتمدة على تعلم الآلي ((Machine Learning (ML)، مصنفاً التهديدات والحلول وفقاً لمعايير محددة.

تواجه تقنية تقطيع الشبكات تحديات عديدة خاصةً فيما يتعلق بالعزل ومشاركة الموارد بين الخدمات، مما يخلق مشكلات أمنية، فمعالجة هذه التحديات أمر ضروري لحماية خصوصية المستخدمين وضمان جودة الخدمة (QoS) المطلوبة. في هذا البحث قدم الباحث [17] مراجعة شاملة لجميع هذه الجوانب وناقشنا كيف يمكن ضمان الأمن داخل وخارج الشرائح من خلال العزل والتعلم الآلي والتشفير مع ضمان أمن شامل من طرف

http://www.doi.org/10.62341/fagf0820

إلى طرف (End-to-End) كما قام بتقييم أداء بعض الحلول المقترحة في مواجهة الهجمات عبر تجارب باستخدام منصة (Open Air Interface).

يوضح الباحث [18] التطبيقات العملية لهذه التقنيات في قطاعات حيوية مثل الرعاية الصحية، مبرزاً كيف تساهم (5G) في تطوير خدمات مثل التطبيب عن بعد إنترنت الأشياء (IoT).

في مجال تأمين شرائح الشبكة، يقدم البحثان [19] (Secure5G) [20] و [21] (SliceSecure) نماذج تعتمد على الشبكات العصبية العميقة (DNN/LSTM) (Deep Neural Network/ Long Short-Term Memory) للكشف عن هجمات حجب الخدمة (DoS/DDoS) بدقة فائقة تصل إلى 99.99%، تؤكد هذه الأبحاث على أهمية بناء نماذج قادرة على عزل التهديدات وضمان استمرارية الخدمة. سياق أخر يركز على التحليل المسبق للهجمات يظهر من خلال البحثان [22] و [23]، حيث تستخدم التعلم المعزز ((Reinforcement Learning(RL)) لتصميم هجمات "إغراق" أو هجمات عدائية متقدمة. الهدف من هذه الأبحاث ليس التخريب بل فهم نقاط ضعف النظام بشكل مسبق لتطوير دفاعات أكثر قوة ومرونة. يبرز اتجاه متقدم نحو حماية الخصوصية بالاعتماد على دمج الخصوصية في التصميم الأمني

يقدم الباحث [24] نموذج ((Multi-Agent Deep Q-Networks (MADQN) لتحسين كفاءة اتصالات التعلم الفيدرالي (Federated Learning) على الحواف في شبكات إنترنت الأشياء المعرفة برمجياً (Software-Defined IoT)، حيث يجمع بين تقنيات (SDN) و(NFV) لتعزيز إدارة الموارد وتقليل فقدان الحزم وتحسين جودة الخدمة (QoS) عبر خوارزميات تعلم معزز متقدمة.

يقدم الباحث [25] انموذجاً مبتكراً (FLeSO) يعتمد على التعلم الفيدرالي (Federated Learning) لتمكين التعاون الأمني بين الشرائح دون الحاجة لمشاركة البيانات الحساسة. بينما يدمج الباحث [26] تقنية توجيه البصل (Onion Routing) مع التشفير الكامل (End-to-End) لضمان إخفاء الهوية وسرية البيانات داخل الشريحة.

7. الخلاصة والتوصيات

في سياق شبكات الجيل الخامس (5G) قدَّمت هذه الدراسة تحليلًا شاملاً لتقنية تقطيع الشبكة (Network Slicing)، كاشفةً عن دورها المحوري في إحداث تحوُّل جذري في إدارة الموارد الشبكية، ورفع كفاءة جودة الخدمة (QoS) وتعزيز المرونة التشغيلية. من

http://www.doi.org/10.62341/fagf0820

خلال استعراض تأثيرات التقنية واستراتيجيات تطبيقها سلَّط البحث الضوء على التحديات الرئيسية التي تواجهها، لا سيما في مجالات الأمن السيبراني والواجهات المعيارية والضوابط التنظيمية.

هذا يبرز الحاجة إلى المزيد من الأبحاث والتطوير في مجالات الذكاء الاصطناعي، والتعلم الآلي، والأمن السيبراني. وتسلط الدراسة الضوء على الإمكانيات التحويلية لتقنية تقطيع الشبكة التي تتجاوز الاتصالات المحمولة التقليدية، داعية إلى المزيد من الاستقصاء حول كيفية الاستفادة الكاملة من شبكات الجيل الخامس لتلبية متطلبات مختلف الصناعات. نؤكد على أهمية تقطيع الشبكة كعامل تمكين رئيسي للنظم الرقمية المستقبلية، ندعو إلى التعاون المشترك لتجاوز العقبات واستغلال الفرص في بيئة تكنولوجيا الاتصالات والشبكات سريعة التطور.

كما تناولت الدراسة كيف يمكن للحوسبة الطرفية (MEC) مدعومةً بتقنيات الذكاء الاصطناعي (AI) والتعلم الآلي (ML) أن تُحسِّن أداء تقطيع الشبكة عبر تحليل البيانات في الوقت الفعلي واتخاذ القرارات الذكية.

تكشف النتائج عن حاجة ماسَّة إلى مزيد من البحث في مجالات الذكاء الاصطناعي، والأمن الرقمي، وإدارة الموارد الديناميكية، خاصةً في ظل التهديدات المتطورة مثل هجمات حجب الخدمة (DoS/DDoS) واستغلال ثغرات العزل بين الشرائح. كما أبرزت الدراسة النماذج الناجحة القائمة على التعلم العميق (Deep Learning) مثل "DeepSlice" لتحسين حركة البيانات، "Secure5G" تقدم حلولاً مبتكرة للتعامل مع الهجمات السيبرانية، مما يجعلها ذات قيمة عالية لاكتشاف الهجمات الغير الأمنية. مؤكدةً على فاعلية التعلم المعزز (RL) في تخصيص الموارد، والتعلم الاتحادي (Federated Learning) في تعزيز الخصوصية، وتوجيه البصل (Onion Routing) تُشير إلى مسارات مبتكرة لتعزيز الكفاءة والأمان مما يجعلها مناسبة للتطبيقات الحساسة، وتقنيات التشفير من الطرف إلى الطرف (End-to-End Encryption) كحلولٍ واعدة.

على الرغم من الإمكانات الهائلة لتقنية التقطيع تظل التحديات قائمة خاصةً في أنظمة إنترنت الأشياء الذكية (Smart IoT)، حيث يتطلب تحقيق التكامل بين البُنى التحتية المُتنوِّعة تنسيقًا دقيقًا لتقسيم الموارد مثل الطيف الترددي، مع ضمان الأمان عبر طبقات متعددة. الحلول المقترحة كالتقطيع الديناميكي للطيف والإدارة الذكية للخدمات.

في الختام يُؤكد هذا البحث على أهمية التعاون بين الأوساط الأكاديمية والصناعية لمواكبة التعقيدات المتزايدة في شبكات المستقبل، داعيًا إلى تبني أطر عمل مرنة قادرة على دمج

http://www.doi.org/10.62341/fagf0820

الابتكارات التقنية مع الضوابط الأمنية والتنظيمية، يمكن تحقيق الرؤية الكاملة لتقنية تقطيع الشبكة كركيزة أساسية للتحول الرقمي عبر الصناعات المُختلفة.

8. المراجع

[1] X. Li et al., "Network slicing for 5G: Challenges and opportunities," IEEE Internet Comput., pp. 1–1, 2018, doi: 10.1109/MIC.2018.326150452.
[2] Y. Hao, "Investigation and technological comparison of 4G and 5G networks," J. Comput. Commun., vol. 9, pp. 36–43, Jan. 2021.
[3] N. Xia, H.-H. Chen, and C.-S. Yang, "Emerging technologies for machine-type communication networks," IEEE Netw., vol. 34, no. 1, pp. 214–222, 2020.
[4] F. Salahdine, Q. Liu, and T. Han, "Towards secure and intelligent network slicing for 5G networks," IEEE Open J. Comput. Soc., vol. 3, pp. 23–38, 2022.
[5] F. Granelli, "Network slicing," in Computing in Communication Networks. Amsterdam, Netherlands: Elsevier, 2020, pp. 63–76.
[6] R. F. Olimid and G. Nencioni, "5G network slicing: A security overview," IEEE Access, vol. 8, pp. 99999–100009, 2020.
[7] P. K. Singh, M. Brahma, P. Nath, and U. Ghosh, "A study on secure network slicing in 5G," in Proc. IEEE/ACM 23rd Int. Symp. Cluster, Cloud Internet Comput. Workshops (CCGridW), May 2023, pp. 52–61.
[8] D. Sattar and A. Matrawy, "Towards secure slicing: Using slice isolation to mitigate DDoS attacks on 5G core network slices," in Proc. IEEE Conf. Commun. Netw. Secur. (CNS), 2019, pp. 82–90.
[9] A. Mathew, "Network slicing in 5G and the security concerns," in Proc. 4th Int. Conf. Comput. Methodol. Commun. (ICCMC), 2020, pp. 75–78.
[10] W. Jiang, S. D. Anton, and H. D. Schotten, "Intelligence slicing: A unified framework to integrate artificial intelligence into 5G networks," in Proc. 12th IFIP Wireless Mobile Netw. Conf. (WMNC), 2019.
[11] A. Thantharate, R. Paropkari, V. Walunj, and C. Beard, "DeepSlice: A deep learning approach towards an efficient and reliable network slicing in 5G networks," in Proc. IEEE 10th

http://www.doi.org/10.62341/fagf0820

Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON), 2019.

[12] X. Cheng, Y. Wu, G. Min, A. Y. Zomaya, and X. Fang, "Safeguard network slicing in 5G: A learning augmented optimization approach," IEEE J. Sel. Areas Commun., vol. 38, no. 7, pp. 1600–1613, 2020.

[13] Y. Kim and H. Lim, "Multi-agent reinforcement learning-based resource management for end-to-end network slicing," IEEE Access, vol. 9, pp. 56178–56190, 2021.

[14] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges," Comput. Netw., vol. 167, Feb. 2020, Art. no. 106984.

[15] Q. Liu, T. Han, and N. Ansari, "Learning-assisted secure end-to-end network slicing for cyber-physical systems," IEEE Netw., vol. 34, no. 3, pp. 37–43, 2020.

[16] R. Dangi, A. Jadhav, G. Choudhary, N. Dragoni, M. K. Mishra, and P. Lalwani, "ML-based 5G network slicing security: A comprehensive survey," Future Internet, vol. 14, no. 4, p. 116, Apr. 2022.

[17] F. Salahdine, Q. Liu, and T. Han, "Towards secure and intelligent network slicing for 5G networks," IEEE Open J. Comput. Soc., vol. 3, pp. 23–38, 2022.

[18] S. M. A. A. Abir, M. Abuibaid, J. S. Huang, and Y. Hong, "Harnessing 5G networks for health care: Challenges and potential applications," in Proc. Int. Conf. Smart Appl., Commun. Netw. (SmartNets), Istanbul, Turkey, Jul. 2023, pp. 1–6.

[19] A. Thantharate, R. Paropkari, V. Walunj, C. Beard, and P. Kankariya, "Secure5G: A deep learning framework towards a secure network slicing in 5G and beyond," in Proc. 10th Annu. Comput. Commun. Workshop Conf. (CCWC), 2020.

[20] "Highly accurate and reliable wireless network slicing in 5th generation networks: A hybrid deep learning approach," J. Netw. Syst. Manage., Springer, 2022.

[21] S. Khan, B. Farzaneh, N. Shahriar, N. Saha, and M. Uddin, "SliceSecure: Impact and Detection of DoS/DDoS Attacks on 5G Network Slices," in Proc. Future Netw. Workshops (FNWF), Montreal, QC, Canada, Oct. 2022, pp. 287–292, doi: 10.1109/FNWF55208.2022.00117.

http://www.doi.org/10.62341/fagf0820

[22] Y. Shi and Y. E. Sagduyu, "Adversarial machine learning for flooding attacks on 5G radio access network slicing," in Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops), 2021.
[23] "How to attack and defend 5G radio access network slicing with reinforcement learning," arXiv, 2022.
[24] P. Tam, S. Math, A. Lee, and S. Kim, "Multi-agent deep Q-networks for efficient edge federated learning communications in software-defined IoT," Comput. Mater. Contin., vol. 71, no. 2, pp. 3319–3335, 2022.
[25] S. Wijethilaka and M. Liyanage, "A federated learning approach for improving security in network slicing," in Proc. IEEE Glob. Commun. Conf. (GLOBECOM), 2022.
[26] X. Li, M. He, and J. Ni, "Secure and privacy-preserving network slicing in 3GPP 5G system architecture," Dept. Electr. Comput. Eng., Queen's Univ., Kingston, Canada. [Unpublished manuscript].