Republic of Yemen
Ministry of Education and Scientific Research
University of Science and Technology
Deanship of Postgraduate Studies and Scientific Research

Secure Model for Mobile Network-Slice in Fifth Generation and Beyond

A Thesis Submitted by

Essam Ahmed Abduh Mohammed

To

The Council of Postgraduate Studies and Scientific Research, in Partial Fulfillment of the Requirements for the Degree of Master of Computing in Computer Networks

Supervisor

Dr. Belal Abdullah Rassea Al-Fuhaidi
Associate Professor of Communication Engineering
University of Science and Technology

November, 2024AD **Sana'a** **Jumada I, 1446AH**

Republic of Yemen
Ministry of Education and Scientific Research
University of Science and Technology
Deanship of Postgraduate Studies and Scientific Research

Secure Model for Mobile Network-Slice in Fifth Generation and Beyond

Abstract

5G is a key enabler in meeting the growing demands for many future services such as virtual reality, augmented reality, healthcare, smart cities, and the Internet of Things (IoT). Which differ in data rate, connection, and response time. To meet the diverse requirements of services, network slicing and edge computing have been promising solutions in the 5G environment. However, current registration and authentication mechanisms cannot support network slice services; users changing their slice leads to different preferences and requirements. This led to the emergence of a new form of handover called inter-slice handover. Which may cause difficult issues, such as quality of service, confidentiality and privacy violations, and wasted resources. This thesis presents a Fast and Secure Registration and Authentication ($FRAS^2$) model. that supports network slicing and is based on Cryptographically Secure Pseudo-Random Number Generators (CSPRNGs) and Elliptic Curve Cryptography (ECC). Blockchain and Chameleon Hashing. To address these issues, the registration process ends with the data being stored on the blockchain and the user receiving the slice/service types and an anonymous ticket. The trapdoor collision feature of chameleon hash functions is used with anonymous ticket and slice/service types in the authentication process. To maintain privacy, tickets were created by CSPRNGs. Thanks to 5G's edge controller capabilities, distributed edge nodes help store anonymous ticket information, ensuring that legitimate users can quickly finish authentication during handover. The performance of the $FRAS^2$ is evaluated through simulation experiments to demonstrate its efficiency and feasibility in a 5G network slice. Experimental results show that the $FRAS^2$ model can improve the registration, authentication, and handover processes. The total delay is reduced by 55.94% when compared with other systems of the same type. This makes the proposed model more suitable for IoT devices.

Candidate

Essam Ahmed Abduh Mohammed

Supervisor

Dr. Belal Abdullah Rassea Al-Fuhaidi

Associate prof. of Communication Engineering
University of Science and Technology

November, 2024AD **Sana'a** **Jumada I, 1446AH**

الجمهورية اليمنية
وزارة التربية والتعليم والبحث العلمي
جامعة العلوم والتكنولوجيا
عمادة الدراسات العليا والبحث العلمي

نموذج آمن لتقسيم شبكات الهاتف النقال في الجيل الخامس وما بعده

المُلخص

تعتبر شبكة(G5) عامل تمكين رئيسي في تلبية الطلبات المتزايدة للعديد من الخدمات المستقبلية كتطبيقات: الواقع الافتراضي، والوقع المعزز، والعناية الصحية، والقيادة الذاتية، والمدن الذكية، ونظم الوقت الحقيقي، وإنترنت الأشياء التي تختلف في معدل البيانات، واتصال العديد من الأجهزة، وزمن الاستجابة. ولتلبية المتطلبات المتنوعة للخدمات تم تصور تقطيع الشبكة والحوسبة السحابية كحلول واعدة في بنية (G5). ومع ذلك، لا يمكن لآليات التسجيل والمصادقة الحالية أن تدعم خدمات شرائح الشبكة، كما أن تغيير المستخدمين شرائحهم يودي إلى اختلف تفضيلاتهم ومتطلباتهم. وقد أدا هذا إلى ظهور شكلاً جديدًا من التسليم يسمى التسليم بين شرائح الشبكة؛ وبسبب ذا لك تظهر مشكلات صعبة، مثل: جودة الخدمة، وانتهاك السرية والخصوية، واهدار الموارد. تقدم هذه الرسالة، نقدم إطار تسجيل ومصادقة سريع وآمن ($FRAS^2$) يدعم تشريح الشبكة، يعتمد على مولدات الأرقام العشوائية الآمنة تشفيراً(CSPRNGs) ، وتشفير المنحنى الإهليلجين (ECC)، والبلوك شين (Blockchain)، وتجزئة الحرباء، لمعالجة هذه المشكلات، تنتهي عملية التسجيل بتخزين البيانات على البلوك شين، وحصول المستخدم على شريحة/الخدمة، وتذكرة مجهولة. تستخدم خاصية تصادم الباب الخلفي لوظائف تجزئة الحرباء مع التذكرة المجهولة، والشريحة/الخدمة في عملية المصادقة. وللحافظ على خصوصية التذكرة التي تم انشائها من خلال (CSPRNGs) بفضل إمكانات متحكمات الحافة في (G5)؛ تساعد العقد الطرفية الموزعة على تخزين معلومات التذكرة المجهولة، مما يضمن أن المستخدمين القانونيين يمكنهم إنهاء المصادقة بسرعة أثناء التسليم. يتم تقييم أداء الإطار المقترح من خلال تجارب المحاكاة لإثبات الكفاءة والجدوى في بيئة شرائح شبكة (G5) تظهر النتائج التجريبية لهذه الدراسة أن النموذج المقترح يمكنه تحسين عملية التسجيل والمصادقة والتسليم بالمقارنة مع الانظمة الأخرى من نفس النوع، كما تم تقليل إجمالي التأخير بنسبة (55.94%). وهذا يجعل النموذج المقترح أكثر ملاءمة لأجهزة إنترنت الأشياء (IoT).

الطالب

عصام أحمد عبده محمد

المشرف

أ.د/ بلال عبدالله راصع الفهيدي

أستاذ هندسة الاتصالات المشارك

جامعة العلوم والتكنولوجيا

نوفمبر، 2024م **صنعاء** **جمادى الأول، 1446هـ**

الجمهورية اليمنية
وزارة التربية والتعليم والبحث العلمي
جامعة العلوم والتكنولوجيا
عمادة الدراسات العليا والبحث العلمي

نموذج آمن لتقسيم شبكات الهاتف النقال في الجيل الخامس وما بعده

رسالة مقدمة من الطالب

عصام أحمد عبده محمد

إلى

مجلس الدراسات العليا والبحث العلمي، وهي جزء من متطلبات الحصول على درجة الماجستير في الحوسبة – شبكات الحاسوب

المشرف

أ.د/ بلال عبدالله راصع هزاع الفهيدي

أستاذ هندسة الاتصالات المشارك

جامعة العلوم والتكنولوجيا

نوفمبر، 2024م **صنعاء** **جمادى الأول، 1446هـ**