الجمهورية الجزائرية الديمقراطية الشعبية
People's Democratic Republic of Algeria
وزارة التعليم العالي والبحث العلمي
Ministry of Higher Education and Scientific Research
المدرسة العليا للإعلام الآلي - 08 ماي 1945 – بسيدي بلعباس
Higher School of Computer Science -8 Mai 1945- Sidi Bel Abbès (ESI-SBA)

FINAL YEAR PROJECT REPORT

To obtain an Enginnering degree

Field of Study: Computer Science

Speciality: Information Systems Engineering (ISI)

Quality of Service-Aware Moving Target Defense for SDN-Driven Mobile Edge Computing

---

Presented by: GUEZOURI Ziad

Presented on: 05/10/2025

In front of a committee composed of:

Dr. SERHANE Oussama	Supervisor
Dr. BABA-AHMED Manel	President
Dr. CHIKH Asmaa	Examiner

Academic year: 2024/2025

Abstract

Mobile Edge Computing environments face increasing vulnerability to sophisticated attacks that compromise both security and service quality. While Moving Target Defense techniques provide security through dynamic reconfiguration, some existing implementations employ rigid time-based shuffling that ignores real-time network conditions, leading to prolonged service degradation during attacks.

This thesis presents a Quality of Service-aware Moving Target Defense system for SDN-driven MEC environments. We develop an adaptive MTD mechanism that dynamically reconfigures client-MEC associations based on continuous QoS monitoring and intelligent health assessment. Our system introduces a dual-trigger shuffling approach combining reactive response to QoS degradation with proactive time-based reconfiguration, ensuring both immediate attack mitigation and long-term unpredictability.

The proposed solution includes an adaptive MEC selection algorithm that evaluates real-time health scores and load distribution to optimize client placement. We implement a probe-based monitoring architecture that continuously assesses MEC health through parallel measurements. The system integrates with ONOS SDN controller through REST APIs, utilizing the intent framework for dynamic path reconfiguration.

Experimental evaluation demonstrates significant improvements across all metrics compared to a time-based MTD baseline. The system successfully maintains service quality during attack scenarios with minimal response delay. Our results validate that intelligent MTD mechanisms can effectively balance security requirements with performance constraints, providing a practical solution for protecting latency-sensitive edge applications.

Keywords: Moving Target Defense, Software-Defined Networking, Mobile Edge Computing, Quality of Service, Intent-Based Networking, Network Security, Dynamic Reconfiguration

Résumé

Les environnements de Mobile Edge Computing sont de plus en plus vulnérables aux attaques sophistiquées qui compromettent à la fois la sécurité et la qualité de service. Bien que les techniques de Moving Target Defense offrent une sécurité par reconfiguration dynamique, certaines implémentations existantes emploient un brassage rigide basé sur le temps qui ignore les conditions réseau en temps réel, entraînant une dégradation prolongée du service pendant les attaques.

Cette thèse présente un système Moving Target Defense sensible à la qualité de service pour les environnements MEC pilotés par SDN. Nous développons un mécanisme MTD adaptatif qui reconfigure dynamiquement les associations client-MEC basées sur une surveillance continue de la QoS et une évaluation intelligente de la santé. Notre système introduit une approche de brassage à double déclencheur combinant une réponse réactive à la dégradation de la QoS avec une reconfiguration proactive basée sur le temps, assurant à la fois une atténuation immédiate des attaques et une imprévisibilité à long terme.

La solution proposée inclut un algorithme de sélection MEC adaptatif qui évalue les scores de santé en temps réel et la distribution de charge pour optimiser le placement des clients. Nous implémentons une architecture de surveillance basée sur des sondes qui évalue continuellement la santé MEC par des mesures parallèles. Le système s'intègre avec le contrôleur SDN ONOS via des API REST, utilisant le framework d'intention pour la reconfiguration dynamique des chemins.

L'évaluation expérimentale démontre des améliorations significatives sur toutes les métriques par rapport à une référence MTD basée sur le temps. Le système maintient avec succès la qualité de service pendant les scénarios d'attaque avec un délai de réponse minimal. Nos résultats valident que les mécanismes MTD intelligents peuvent effectivement équilibrer les exigences de sécurité avec les contraintes de performance, fournissant une solution pratique pour protéger les applications sensibles à la latence.

Mots-clés : Défense par cible mouvante, Réseau défini par logiciel, Mobile Edge Computing, Qualité de service, Réseau basé sur l'intention, Sécurité réseau, Reconfiguration dynamique

ملخص

تواجه بيئات حوسبة الحافة المتنقلة تزايداً في الضعف أمام الهجمات المتطورة التي تهدد كلاً من الأمان وجودة الخدمة. بينما توفر تقنيات الدفاع بالهدف المتحرك الأمان من خلال إعادة التكوين الديناميكية، فإن بعض التطبيقات الحالية تستخدم خلطاً صارماً قائماً على الوقت يتجاهل ظروف الشبكة في الوقت الفعلي، مما يؤدي إلى تدهور طويل للخدمة أثناء الهجمات.

تقدم هذه الأطروحة نظام دفاع بالهدف المتحرك واعٍ بجودة الخدمة لبيئات الحوسبة الطرفية المتنقلة المدارة بواسطة الشبكات المعرفة برمجياً. نطور آلية دفاع بالهدف المتحرك تكيفية تعيد تكوين ارتباطات العميل-الحوسبة الطرفية ديناميكياً بناءً على المراقبة المستمرة لجودة الخدمة والتقييم الذكي للصحة. يقدم نظامنا نهج خلط ثنائي المحفز يجمع بين الاستجابة التفاعلية لتدهور جودة الخدمة وإعادة التكوين الاستباقية القائمة على الوقت، مما يضمن كلاً من التخفيف الفوري للهجمات وعدم القابلية للتنبؤ على المدى الطويل.

يتضمن الحل المقترح خوارزمية اختيار تكيفية للحوسبة الطرفية المتنقلة تقيّم درجات الصحة في الوقت الفعلي وتوزيع الحمل لتحسين وضع العملاء. نطبق بنية مراقبة قائمة على المسبار تقيّم باستمرار صحة الحوسبة الطرفية من خلال قياسات متوازية. يتكامل النظام مع متحكم الشبكات المعرفة برمجياً ONOS من خلال واجهات برمجة التطبيقات REST، مستخدماً إطار النية لإعادة تكوين المسار الديناميكي.

يُظهر التقييم التجريبي تحسينات كبيرة في جميع المقاييس مقارنة بخط أساس للدفاع بالهدف المتحرك القائم على الوقت. يحافظ النظام بنجاح على جودة الخدمة أثناء سيناريوهات الهجوم مع تأخير استجابة ضئيل. تؤكد نتائجنا أن آليات الدفاع بالهدف المتحرك الذكية يمكنها بفعالية موازنة متطلبات الأمان مع قيود الأداء، مما يوفر حلاً عملياً لحماية تطبيقات الحافة الحساسة للتأخير.

الكلمات المفتاحية: الدفاع بالهدف المتحرك، الشبكات المعرفة بالبرمجيات، حوسبة الحافة المتنقلة، جودة الخدمة، الشبكات القائمة على النية، أمن الشبكات، إعادة التكوين الديناميكية