Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, ΕΛ.ΜΕ.ΠΑ. Κρήτης

Ελληνικό Μεσογειακό Πανεπιστήμιο

Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Πρόγραμμα Σπουδών Μηχανικών Πληροφορικής ΤΕ

Τίτλος:

ΑΝΙΧΝΕΥΣΗ ΠΑΡΕΙΣΦΡΗΣΗΣ ΜΕ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΜΕΣΩ ΒΑΘΕΩΝ ΑΥΤΟΚΩΔΙΚΟΠΟΙΗΤΩΝ ΣΕ ΔΙΚΤΥΑ ΕΠΟΜΕΝΗΣ ΓΕΝΙΑΣ

Title:

AI-POWERED INTRUSION DETECTION WITH DEEP AUTOENCODERS IN NEXT-GENERATION NETWORKS

ΔΗΜΗΤΡΙΟΣ ΞΟΛΙΑΣ

Επιβλέπων εκπαιδευτικός :

ΕΥΑΓΓΕΛΟΣ ΜΑΡΚΑΚΗΣ
Επιτροπή Αξιολόγησης :

- **ΕΥΑΓΓΕΛΟΣ ΜΑΡΚΑΚΗΣ**
- **ΔΗΜΗΤΡΙΟΣ ΣΤΡΑΤΑΚΗΣ**
- **ΗΛΙΑΣ ΠΟΛΙΤΗΣ**

Ημερομηνία παρουσίασης: 03/20/2026

Summary:

This thesis addresses the critical security challenges in next-generation networks (5G, IoT, SDN) by designing and implementing a novel AI-powered Intrusion Detection System (IDS). The research proposes a hybrid two-stage deep learning architecture combining a Deep Autoencoder (DAE) for dimensionality reduction with a 1D Convolutional Neural Network (1D-CNN) for classification.

The system was implemented as a lightweight, containerized Virtual Network Function (VNF) compliant with ETSI-NFV standards, enabling scalable deployment in modern network infrastructures. Validated using the RT-IoT2022 dataset within an emulated SDN testbed, the proposed model achieved 97.8% accuracy and 92.0% macro F1-score, outperforming classical machine learning baselines (Random Forest, SVM). Critically, the system demonstrated real-time operational capability with a mean inference latency of 79 milliseconds on standard CPU hardware, making it suitable for edge deployment without specialized accelerators.

Key Contributions:

- Novel hybrid DAE+1D-CNN architecture balancing accuracy and efficiency
- Strict EXPECTED_84 feature schema with robust preprocessing pipeline
- Containerized Flask-based inference service for portable VNF deployment
- Comprehensive validation demonstrating state-of-the-art performance in real-time threat detection

---

Περίληψη:

Η παρούσα πτυχιακή εργασία αντιμετωπίζει τις κρίσιμες προκλήσεις ασφάλειας στα δίκτυα επόμενης γενιάς (5G, IoT, SDN) μέσω του σχεδιασμού και υλοποίησης ενός καινοτόμου Συστήματος Ανίχνευσης Εισβολών (IDS) βασισμένου σε Τεχνητή Νοημοσύνη. Η έρευνα προτείνει μια υβριδική αρχιτεκτονική βαθιάς μάθησης δύο σταδίων που συνδυάζει έναν Βαθύ Αυτοκωδικοποιητή (DAE) για μείωση διαστάσεων με ένα Μονοδιάστατο Συνελικτικό Νευρωνικό Δίκτυο (1D-CNN) για ταξινόμηση.

Το σύστημα υλοποιήθηκε ως ελαφριά, εικονικοποιημένη Δικτυακή Λειτουργία (VNF) σύμφωνα με τα πρότυπα ETSI-NFV, επιτρέποντας την επεκτάσιμη ανάπτυξη σε σύγχρονες δικτυακές υποδομές. Αξιολογημένο με το σύνολο δεδομένων RT-IoT2022 σε εξομοιωμένο περιβάλλον SDN, το προτεινόμενο μοντέλο επέτυχε 97,8% ακρίβεια και 92,0% macro F1-score, ξεπερνώντας κλασικές μεθόδους μηχανικής μάθησης (Random Forest, SVM). Κρίσιμα, το σύστημα επέδειξε λειτουργία σε πραγματικό χρόνο με μέση καθυστέρηση 79 χιλιοστών του δευτερολέπτου σε τυπικό υλικό CPU, καθιστώντας το κατάλληλο για ανάπτυξη σε edge περιβάλλοντα χωρίς εξειδικευμένους επιταχυντές.

Βασικές Συνεισφορές:

- Καινοτόμος υβριδική αρχιτεκτονική DAE+1D-CNN που εξισορροπεί ακρίβεια και αποδοτικότητα
- Αυστηρό σχήμα χαρακτηριστικών EXPECTED_84 με ισχυρό pipeline προεπεξεργασίας
- Εικονικοποιημένη υπηρεσία εξαγωγής συμπερασμάτων βασισμένη σε Flask για φορητή ανάπτυξη VNF
- Ολοκληρωμένη επικύρωση που αποδεικνύει κορυφαία απόδοση στην ανίχνευση απειλών σε πραγματικό χρόνο