# Σύνοψη

Η εργασία αυτή αποσκοπεί κυρίως στη μελέτη και κατανόηση της λειτουργίας των συστημάτων Hierarchical Temporal Memory (HTM) –ένα καινοτόμο μοντέλο Μηχανικής Μάθησης άμεσα εμπνευσμένο από τον κλάδο της βιολογίας, και συγκεκριμένα από τον ανθρώπινο εγκέφαλο– καθώς και στην αναζήτηση μεθόδων βάσει των οποίων τα συστήματα αυτά είναι εφικτό να εφαρμοστούν ως προς την επίλυση προβλημάτων πραγματικού κόσμου υπό την μορφή κλασικών προβλημάτων Μηχανικής Μάθησης, τόσο στα πλαίσια της Επιβλεπόμενης όσο και της Μη-Επιβλεπόμενης Μάθησης. Η περίπτωση του προβλήματος που εξετάζουμε αφορά την ανίχνευση επιθέσεων «Άρνησης Εξυπηρέτησης», ένα από τα πιο διαδεδομένα είδη διαδικτυακών επιθέσεων, σκοπός των οποίων αποτελεί η διατάραξη της ομαλής λειτουργίας των διακομιστών του θύματος της επίθεσης, είτε αυτό αποτελεί μία μικρομεσαία επιχείρηση είτε ένας παγκόσμιος οργανισμός.

Στο εισαγωγικό κεφαλαίο της εργασίας αναφερόμαστε συνοπτικά στον κλάδο της Μηχανικής Μάθησης, εστιάζοντας την προσοχή μας στην διαφορά μεταξύ Επιβλεπόμενης και Μη-Επιβλεπόμενης Μάθησης, καθώς επίσης και στην γενικότερη δομή των προβλημάτων της Ταξινόμησης, βάσει της οποίας ορίζουμε το πρόβλημα που επιλύουμε. Η βασική ιδέα συνίσταται στο ότι παρακολουθώντας την δικτυακή κίνηση ενός διακομιστή και συλλέγοντας χρήσιμες πληροφορίες για αυτήν, μπορούμε ανά πάσα χρονική στιγμή να κατασκευάσουμε μεμονωμένα στιγμιότυπα ως προς την αναπαράστασή της, τα οποία στην συνέχεια τροφοδοτούμε σε ένα πλήρως εκπαιδευμένο μοντέλο Μηχανικής Μάθησης, ικανό να τα ταυτοποιήσει είτε ως μέρος της κανονικής «καλόβουλης» κίνησης, είτε ως τμήμα της «κακόβουλης» κίνησης, η οποία στην περίπτωσή μας σχετίζεται με την διεξαγωγή επιθέσεων άρνησης εξυπηρέτησης. Κλείνοντας το εισαγωγικό αυτό κεφάλαιο, αναφερόμαστε περαιτέρω στις επιθέσεις άρνησης εξυπηρέτησης καθώς και στους κινδύνους που αυτές εγκυμονούν, παρέχοντας ως παράδειγμα τις επιθέσεις «DNS Amplification», οι οποίες μας απασχολούν στα πλαίσια αυτής της εργασίας.

Στο δεύτερο κεφάλαιο της εργασίας πραγματοποιείται μία αναλυτική περιγραφή των μοντέλων Μηχανικής Μάθησης που αξιοποιούμε, δηλαδή των συστημάτων Hierarchical Temporal Memory αλλά και των Τεχνητών Νευρωνικών Δικτύων, τα οποία χρησιμοποιούμε ως ένα μέτρο σύγκρισης των επιδόσεων που κατορθώνουν τα συστήματα HTM. Το κεφάλαιο αυτό ξεκινάει κάνοντας μία ιστορική αναδρομή της εξέλιξης των νευρωνικών δικτύων, από τον απλό αλγόριθμο ταξινόμησης «Perceptron» μέχρι και τα πολυσύνθετα «Πλήρως Συνδεδεμένα» δίκτυα που χρησιμοποιούμε έως και σήμερα. Στο σημείο αυτό εμβαθύνουμε στην κατανόηση της βασικής αρχιτεκτονικής των νευρωνικών δικτύων και πώς αυτή εξυπηρετεί την επίλυση των προβλημάτων Ταξινόμησης, καθώς επίσης και στην διαδικασία της εκπαίδευσής των δικτύων στα πλαίσια της Επιβλεπόμενης Μάθησης. Αμέσως μετά η προσοχή μας στρέφεται προς τα «Αναδρομικά Νευρωνικά Δίκτυα», μία κατηγορία δικτύων κατάλληλα διαμορφωμένα ως προς την διαχείριση ακολουθιακών δεδομένων –όπως θα δούμε, η διάταξη αλλά και η γενικότερη οργάνωση των δεδομένων σε ξεχωριστές ακολουθίες εμπεριέχει μία διαφορετικού είδους «χρονική»

πληροφορία, η οποία στα πλαίσια του προβλήματος που επιλύουμε κατέχει έναν σημαντικό ρόλο. Σε αυτό το μέρος εξετάζουμε τόσο τα μοντέλα των κλασικών αναδρομικών δικτύων, όσο και τον «διάδοχό» τους, τα δίκτυα «Long Short-Term Memory». Το τρίτο και τελευταίο είδος των δικτύων τα οποία μας απασχολούν αφορά τα μοντέλα των «Αυτοκωδικοποιητών», η βασική χρήση των οποίων αν και αφορά το πρόβλημα της επιλογής χαρακτηριστικών, εμείς επικεντρωνόμαστε στην δυνατότητα της εφαρμογής τους πάνω σε προβλήματα Ανίχνευσης Ανωμαλιών στα πλαίσια της Μη-Επιβλεπόμενης Μάθησης. Τέλος πραγματοποιείται μία σύντομη αναφορά στο πρόβλημα της «Υπερεκπαίδευσης» των δικτύων, η οποία ακολουθείται από μία εξίσου σύντομη παρουσίαση ορισμένων τεχνικών αντιμετώπισής αυτού του φαινομένου.

Το υπόλοιπο μισό του δεύτερου κεφαλαίου είναι αφιερωμένο αποκλειστικά και μόνο στα συστήματα Hierarchical Temporal Memory. Λόγω του ότι τα μοντέλα αυτά δεν απολαμβάνουν της ίδιας φήμης με τα νευρωνικά δίκτυα, στην περίπτωσή τους ακολουθούμε μία αναλυτικότερη προσέγγιση ως προς την κατανόηση της λειτουργίας τους. Αφότου πραγματοποιήσουμε μία αρχική αναφορά στην γενικότερη αρχιτεκτονική και στα επιμέρους δομικά μέρη των συστημάτων HTM, καθώς και στην μορφή αναπαράστασης των δεδομένων τα οποία τα συστήματα αυτά διαχειρίζονται, τις λεγόμενες συμβολοσειρές «Sparse Distributed Representation», στην συνέχεια προβαίνουμε σε μία διεξοδική περιγραφή των δύο βασικών αλγορίθμων που διέπουν την λειτουργία των συστημάτων HTM, των «Spatial Pooler» και «Temporal Pooler», τόσο αναφορικά με τα βήματα που εκτελούνται με σκοπό την παραγωγή της τελικής εξόδου, όσο και με τις διάφορες διαδικασίες εκπαίδευσης των συστημάτων. Το κεφάλαιο αυτό κλείνει με μία λεπτομερή περιγραφή των κλάσεων της βιβλιοθήκης «NuPIC» –πρόκειται για μία βιβλιοθήκη ανοιχτού κώδικα η οποία μας παρέχεται από την εταιρεία «Numenta»– που χρησιμοποιούμε ως προς την κατασκευή πλήρους λειτουργικών συστημάτων HTM.

Κατά το ξεκίνημα του αμέσως επόμενου κεφαλαίου πραγματοποιούμε μία σύντομη ανασκόπηση του προβλήματος που αντιμετωπίζουμε, εξετάζοντας παράλληλα ορισμένες μεθόδους συναφών δουλειών οι οποίες αποσκοπούν στην επίλυση του ίδιου προβλήματος. Έχοντας στο δεύτερο κεφάλαιο αναφερθεί μονάχα στον τρόπο λειτουργίας των συστημάτων HTM, υπό την έννοια της διαδικασίας παραγωγής της εξόδου δεδομένου ενός στοιχείου στην είσοδο του συστήματος, στην συνέχεια εισάγουμε δύο διαφορετικές μεθόδους χρήσης των συστημάτων ως προς την επίλυση του προβλήματος. Η πρώτη από αυτές βασίζεται στον «Αλγόριθμο Μάθησης Φλιού» (Cortical Learning Algorithm), και αφορά την εφαρμογή των συστημάτων HTM με σκοπό την επίλυση προβλημάτων Ταξινόμησης στα πλαίσια της Επιβλεπόμενης Μάθησης. Η δεύτερη μέθοδος, η οποία στηρίζεται σε έναν από τους εσωτερικούς μηχανισμούς των συστημάτων, εντάσσεται στα πλαίσια της Μη-Επιβλεπόμενης Μάθησης, και αποβλέπει στην επίλυση του προβλήματος της Ανίχνευσης Ανωμαλιών. Τέλος, παρουσιάζουμε μία δική μας μέθοδο μέσω της οποίας το πρόβλημα της Ανίχνευσης Ανωμαλιών μετατρέπεται σε ένα κλασικό πρόβλημα Δυαδικής Ταξινόμησης, παραμένοντας ωστόσο στα πλαίσια της Μη-Επιβλεπόμενης Μάθησης. Τονίζουμε ότι η μέθοδος αυτή μετατροπής του προβλήματος Ανίχνευσης Ανωμαλιών σε πρόβλημα Δυαδικής Ταξινόμησης είναι

αρκετά γενική, γεγονός που σημαίνει ότι δεν αφορά αποκλειστικά τα συστήματα HTM, αλλά αντιθέτως μπορεί να εφαρμοστεί συνδυαστικά με κάμποσα μοντέλα Μηχανικής Μάθησης.

Το τέταρτο κεφάλαιο ασχολείται εξ ολοκλήρου με τα πειράματα που εκτελούμε στα πλαίσια αυτής της εργασίας, συγκεκριμένα με την παρουσίαση των αποτελεσμάτων που εξάγουμε μέσω αυτών, αλλά και με την περιγραφή των όποιων διαδικασιών σχετίζονται μαζί τους, είτε με άμεσο είτε με έμμεσο τρόπο. Μέρος των παραπάνω αποτελεί πρώτα και κύρια η αναφορά που γίνεται στα σύνολα δεδομένων τα οποία έχουμε στην διάθεσή μας, δίνοντας έμφαση στα χαρακτηριστικά των δεδομένων που αξιοποιούνται –όπως θα δούμε χρησιμοποιούμε δύο διαφορετικά είδη χαρακτηριστικών ως προς την αναπαράσταση της δικτυακής κίνησης, τα χαρακτηριστικά των πακέτων και τα χαρακτηριστικά των ροών πακέτων– ενώ εξίσου σημαντική είναι και η παρουσίαση της αρχιτεκτονικής, αλλά και των επιμέρους τιμών των υπερπαραμέτρων κάθε μοντέλου που χρησιμοποιούμε ως προς την εκτέλεση των πειραμάτων, είτε αυτό αποτελεί ένα νευρωνικό δίκτυο είτε ένα σύστημα HTM. Στην συνέχεια, αφότου πρώτα έχουμε περιγράψει εκτενώς την διαδικασία προετοιμασίας των πειραμάτων –μέρος της προετοιμασίας των πειραμάτων αποτελεί η κατασκευή των συνόλων δεδομένων εκπαίδευσης και αξιολόγησης, καθώς και οποιαδήποτε άλλη διαδικασία προεπεξεργασίας αυτών, όπως για παράδειγμα είναι η οργάνωση των δεδομένων σε ακολουθείες, η κανονικοποίηση των τιμών τους, κ.λπ.– προχωράμε σε μία συνοπτική περιγραφή τους, κάνοντας ταυτόχρονα μία μικρή αναφορά στην μετρική που χρησιμοποιούμε ως προς την αξιολόγηση της επίδοσης των μοντέλων στα πλαίσια της εκτέλεσής τους. Τέλος, μέσω της χρήσης πινάκων αλλά και γραφημάτων παρουσιάζουμε τα αποτελέσματα που λάβαμε μέσω της διεξαγωγής κάθε πειράματος, σχολιάζοντας παράλληλα την σημασία τους.

Το πέμπτο και τελευταίο κεφάλαιο της εργασίας εμπεριέχει μία σύντομη ανασκόπηση των αποτελεσμάτων του αμέσως προηγούμενου κεφαλαίου, ενώ στην συνέχεια προβαίνουμε σε συζήτηση αναφορικά με δύο μειονεκτήματα των συστημάτων HTM που παρατηρήθηκαν καθόλη την διάρκεια της εκπόνησης αυτής της εργασίας, τα οποία ενδέχεται σε ορισμένες περιπτώσεις να μας αποθαρρύνουν από την χρήση των εν λόγω μοντέλων. Η εργασία κλείνει παρουσιάζοντας πέντε διαφορετικές προτάσεις επέκτασης της δουλειάς μας, τόσο σε πρακτικό-προγραμματιστικό όσο και σε ερευνητικό επίπεδο, με τις οποίες ο αναγνώστης μπορεί να ενασχοληθεί ούτω ώστε να διευρύνει την γνώση του ως προς τα συστήματα HTM, συμβάλλοντας παράλληλα στην περαιτέρω βελτίωσή τους.