Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Τομέας Επικοινωνιών, Ηλεκτρονικής και Συστημάτων Πληροφορικής

Σχεδίαση και Μελέτη Αλγορίθμων Αντιστοίχισης για την Βελτιστοποίηση της Επίδοσης Ομοσπονδιακής Μάθησης Πολλαπλών Μοντέλων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΓΕΩΡΓΙΟΥ ΜΥΣΤΡΙΩΤΗ

Επιβλέπων: Συμεών Παπαβασιλείου
Καθηγητής Ε.Μ.Π.

Αθήνα, Φεβρουάριος 2025

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
Τομέας Επικοινωνιών, Ηλεκτρονικής και Συστημάτων Πληροφορικής

Σχεδίαση και Μελέτη Αλγορίθμων Αντιστοίχισης για την Βελτιστοποίηση της Επίδοσης Ομοσπονδιακής Μάθησης Πολλαπλών Μοντέλων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΓΕΩΡΓΙΟΥ ΜΥΣΤΡΙΩΤΗ

Επιβλέπων: Συμεών Παπαβασιλείου
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 11η Νοεμβρίου 2023.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Συμεών Παπαβασιλείου	Ιωάννα Ρουσσάκη	Ειρήνη Ελένη Τσιροπούλου
Καθηγητής Ε.Μ.Π.	Αναπληρώτρια Καθηγήτρια Ε.Μ.Π.	Αναπληρώτρια Καθηγήτρια A.S.U.

Αθήνα, Φεβρουάριος 2025

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
Τομέας Επικοινωνιών, Ηλεκτρονικής και Συστημάτων Πληροφορικής

(Υπογραφή)

.....

ΓΕΩΡΓΙΟΣ ΜΥΣΤΡΙΩΤΗΣ
Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Με την ανάπτυξη και ευρύτερη εφαρμογή της Ομοσπονδιακής Μάθησης (Federated Learning) τίθεται το πρόβλημα επιλογής κόμβων από τον αντίστοιχο εξυπηρετητή. Ειδικότερα σε περιβάλλοντα όπου συνυπάρχουν πάνω από ένας εξυπηρετητές μία τέτοια διαδικασία είναι καθοριστική. Μέχρι τώρα μελέτες επικεντρώνονται στην επιλογή κόμβων από την πλευρά ενός εξυπηρετητή, για την εκπαίδευση του παγκόσμιου μοντέλου του. Σε αυτή τη διατριβή προεκτείνουμε την λογική αυτή και αντιμετωπίζουμε το πρόβλημα της αντιστοίχισης κόμβων - εξυπηρετητών σε ένα περιβάλλον Ομοσπονδιακής Μάθησης πολλαπλών εξυπηρετητών - μοντέλων, με στόχο την μεγιστοποίηση των χρησιμοτήτων κόμβων και εξυπηρετητών και ως προέκταση την επίδοση των συγκεντρωτικών/παγκόσμιων μοντέλων. Κάθε ένας από τους εξυπηρετητές εκπαιδεύει ένα ξεχωριστό μοντέλο, ενώ οι κόμβοι διαθέτουν διαφορετική πληροφορία, συνεπώς για κάθε έναν από τους εξυπηρετητές έχουν διαφορετική σημασία. Σε αυτό το πλαίσιο μελετάμε και κατασκευάζουμε αλγορίθμους αντιστοίχισης σε διάφορα σενάρια ώστε να γίνουν εμφανή τα πλεονεκτήματα και μειονεκτήματα καθενός από αυτούς. Προκειμένου να προσδοθεί μια ρεαλιστική εφαρμογή ενός τέτοιου προβλήματος μελετάμε σενάρια εντοπισμού φυσικών κινδύνων (πυρκαγιών, πλημμυρών, σεισμών), μέσω φωτογραφιών, σε ένα περιβάλλον Έξυπνης Πόλης - Δημόσιας Ασφάλειας.

Για τους αλγορίθμους αντιστοίχισης καταφεύγουμε στη Θεωρία Παιγνίων (Game Theory), Ενισχυτική Μάθηση (Reinforcement Learning) και στη Μετανοητική Μάθηση (Regret Learning), και στη συνέχεια εκτελούμε τη διαδικασία της Ομοσπονδιακής Μάθησης για να λάβουμε και να συγκρίνουμε τα αποτελέσματά μας. Για τους αλγορίθμους Μετανοητικής Μάθησης που προτείνουμε, δίνουμε επιπλέον ελευθερία στους κόμβους μας να διαμορφώσουν την συμμετοχή τους / τους πόρους που θα διαθέσουν στην διαδικασία της Ομοσπονδιακής Μάθησης ανάλογα με το συμφέρον (χρησιμότητα) τους. Μέσω πειραμάτων και συγκρίσεων των διαφόρων αλγορίθμων καταλήγουμε πως ο αλγόριθμος αντιστοίχισης Θεωρίας Παιγνίων υπερέχει των αλγορίθμων Ενισχυτικής Μάθησης και της Τυχαίας Αντιστοίχισης, επιτυγχάνοντας υψηλότερες χρησιμότητες για τους κόμβους και εξυπηρετητές και καλύτερες επιδόσεις για τα παγκόσμια μοντέλα. Αντίστοιχα, οι αλγόριθμοι Μετανοητικής Μάθησης, με την επιπλέον ιδιότητά τους να διαμορφώνουν την συμμετοχή των κόμβων στην Ομοσπονδιακή Μάθηση, παρουσιάζουν ακόμη καλύτερες χρησιμότητες, πλησιάζοντας την απόδοση των παγκόσμιων μοντέλων του αλγορίθμου Θεωρίας Παιγνίων

χρησιμοποιώντας πολύ λιγότερα δεδομένα (και άρα λιγότερη ενέργεια).

Λέξεις Κλειδιά

Ομοσπονδιακή Μάθηση, Ομοσπονδιακή Μάθηση Πολλαπλών Μοντέλων, Αλγόριθμοι Αντιστοίχισης, Θεωρία Παιγνίων, Ενισχυτική Μάθηση, Μετανοητική Μάθηση, Νευρωνικά Δίκτυα, Συνασπισμοί, Διαμόρφωση Συμμετοχής Κόμβων.

Abstract

With the development and broader application of Federated Learning, the problem of node selection by the corresponding server becomes more prominent. Specifically, in environments where more than one server coexists, such a process is critical. So far, studies have focused on node selection from the perspective of a single server to train its global model. In this thesis, we extend this logic and address the problem of node - server assignment in a Federated Learning environment with multiple servers and models. The goal is to maximize the utilities of both nodes and servers and, consequently, the performance of the global models. Each server trains a distinct model, while the nodes hold different data, and therefore have varying significance/importance for each server. Within this framework, we study and design matching algorithms across various scenarios to highlight the advantages and disadvantages of each. To provide a realistic application of such a problem, we examine scenarios involving the detection of natural hazards (fires, floods, earthquakes) through images in a Smart City – Public Safety environment.

For the matching algorithms, we construct algorithms based on Game Theory, Reinforcement Learning, and Regret Learning. We then execute the Federated Learning process to obtain and compare our results. For the proposed Regret Learning algorithms, we offer additional flexibility to the nodes, allowing them to adjust their participation and the resources they allocate to the Federated Learning process based on their interests (utility). Through experiments and comparisons of the various algorithms, we conclude that the Game Theory matching algorithm outperforms the Reinforcement Learning algorithms and Random Matching, achieving higher utilities for both nodes and servers as well as better performance for the global models. Similarly, the Regret Learning algorithms, with their additional ability to shape node participation in Federated Learning, demonstrate even better utilities, approaching the performance of the global models produced by the Game Theory algorithm while using significantly less data (and thus less energy).

Keywords

Federated Learning, Multi-Model Federated Learning, Matching Algorithms, Game Theory, Reinforcement Learning, Regret Learning, Neural Networks, Coalitions, Configuration of Nodes'

Participation

Ευχαριστίες

Θα ήθελα σε αυτό το κομμάτι να ευχαριστήσω κάποια άτομα που με βοήθησαν ιδιαίτερα κατά τη διάρκεια εκτέλεσης της διπλωματικής μου εργασίας, αλλά και καθ' όλη την πορεία μου στο πανεπιστήμιο.

Ευχαριστώ τον Δρ. Συμεών Παπαβασιλείου, καθηγητή στο Εθνικό Μετσόβειο Πολυτεχνείο στον Τομέα Επικοινωνιών, Ηλεκτρονικής και Συστημάτων Πληροφορικής αρχικά για την διδασκαλία του που μου κέντρισε το ενδιαφέρον και στη συνέχεια για την καθοδήγηση και συνεργασία στη διπλωματική μου και τις συμβουλές του για τις μεταπτυχιακές μου σπουδές.

Ευχαριστώ την Δρ. Ειρήνη Ελένη Τσιροπούλου, καθηγήτρια στο Πολιτειακό Πανεπιστήμιο της Αριζόνα για την συνεργασία που είχαμε κατά τη διάρκεια της διπλωματικής μου. Η καθοδήγηση, οργάνωση και υποστήριξη από πλευράς της ήταν ανεκτίμητη και είμαι ευγνώμων που είχα την ευκαιρία να συνεργαστώ μαζί της και με ένα πανεπιστήμιο του εξωτερικού.

Ευχαριστώ την Δρ. Μαρία Διαμαντή, μεταδιδακτορική στο Εθνικό Μετσόβειο Πολυτεχνείο στον Τομέα Επικοινωνιών, Ηλεκτρονικής και Συστημάτων Πληροφορικής για την βοήθειά της στην επίλυση απορίων και προβλημάτων αλλά και στην ομαλή και γρήγορη εξοικείωσή μου με το αντικείμενο και στόχους της διπλωματικής μου εργασίας.

Ευχαριστώ τον Δρ. Γεώργιο Γκούμα, καθηγητή στο Εθνικό Μετσόβειο Πολυτεχνείο στον Τομέα Τεχνολογίας Πληροφορικής και Υπολογιστών για τις συμβουλές του κατά τη διάρκεια των σπουδών μου αλλά και για την μεταδοτική διδασκαλία του.

Ευχαριστώ τον Δρ. Δημήτριο Δελλή για την διαθεσιμότητά του και την άμεση υποστήριξή του για οποιαδήποτε τεχνικά ζητήματα στο υπολογιστικό σύστημα HPC ARIS του GRNET (HPC ARIS).

Ευχαριστώ τον Δρ. Μίνωα Αξενίδη και Δρ Δάκη Παυλίδη για την υποστήριξή τους στην εκτέλεση των πειραμάτων της διπλωματικής μου εργασίας στο υπολογιστικό σύστημα (cluster) Gauss στο Ινστιτούτο Πυρηνικής & Σωματιδιακής Φυσικής του Εθνικού Κέντρου Έρευνας Φυσικών Επιστημών Δημόκριτος (INP Demokritos).

Ευχαριστώ την οικογένειά μου που με υποστήριξε καθ' όλη τη διάρκεια των σπουδών μου, διότι χωρίς αυτούς δεν θα είχα καταφερει να φτάσω έως εδώ.

Ευχαριστώ τους φίλους μου για την υποστήριξή τους, για τις όμορφες στιγμές και αναμνήσεις

που θα κρατήσω για πάντα.

Περιεχόμενα

Κατάλογος Σχημάτων

1

Εισαγωγή

Τα τελευταία χρόνια όπου αναπτύσσεται με ραγδαίους ρυθμούς ο κλάδος της Τεχνητής Νοημοσύνης και των Νευρωνικών Δικτύων έχει μεγαλώσει αντίστοιχα η ανάγκη για μεγάλους όγκους δεδομένων, για την εκπαίδευση των εκάστοτε μοντέλων, αφού σύμφωνα με τον Goodfelow et al. ([GBC16]), η αποτελεσματική εκπαίδευση μοντέλων Τεχνητής Νοημοσύνης βασίζεται στον πλούτο και την ποικιλομορφία των δεδομένων. Ο καθένας μας, μέσω των ηλεκτρονικών συσκευών, που πλέον είναι εκτενώς διαθέσιμες (κινητά τηλέφωνα, υπολογιστές, IoT συσκευές), αλλά και με τη βοήθεια του διαδικτύου, έρχεται σε επαφή καθημερινά έναν τεράστιο όγκο δεδομένων, όπως εικόνες, βίντεο, μουσική, ηχητικά μηνύματα και απλό κείμενο. Το σημαντικό για όλα αυτά τα δεδομένα είναι πως είναι φτιαγμένα από ανθρώπους για ανθρώπους και συνεπώς αποτελούν πολύ καλή πληροφορία για την εκπαίδευση μοντέλων για πληθώρα εφαρμογών. Επιπλέον, η ιδιομορφία του κάθε ανθρώπου και η διαφορά στον χαρακτήρα του, αντικατοπτρίζεται στην καθημερινότητά του και άρα και στην αλληλεπίδρασή του στο διαδίκτυο ή στις συσκευές του. Συνεπώς, τα δεδομένα αυτά αποκτούν μια επιπλέον αξία, επιτρέποντας σε μοντέλα εκπαιδευμένα σε αυτά να αναλύσουν τις ιδιομορφίες και διαφορές στη συμπεριφορά των ανθρώπων, δημιουργώντας ένα ακόμα πιο αληθοφανές και γενικευμένο αποτέλεσμα.

Από την άλλη πλευρά, όπως υπογραμμίζεται από τους Acquisti et al. ([ABL15]), η χρήση δεδομένων σε σύγχρονες εφαρμογές δημιουργεί προκλήσεις για την ιδιωτικότητα και απαιτεί αυστηρά νομοθετικά πλαίσια. Είναι προφανές πως δεν θα θέλαμε κάποιος που μας προσφέρει μια υπηρεσία στο κινητό μας να έχει πρόσβαση στα προσωπικά δεδομένα μας (φωτογραφίες, μηνύματα κ.α.). Το πρόβλημα της ιδιωτικότητας στο διαδίκτυο δεν θεωρούταν τόσο σημαντικό πριν ακόμα και από μία δεκαετία, αλλά με την πρόσφατη εκθετική αύξηση χρησιμοποίησης του διαδικτύου και των υπηρεσιών που αυτό προσφέρει, έχει έρθει στο προσκήνιο ως μια απαραίτητη προϋπόθεση για όλες τις υπηρεσίες που απαιτούν ανάλυση προσωπικών δεδομένων. Αντίστοιχα, έπειτα από σκάνδαλα για πώληση προσωπικών δεδομένων από μικρές και μεγάλες εταιρείες, έχουν τεθεί αυστηροί κανόνες και νόμοι (είτε ανά χώρα, είτε στην Ευρώπη από την Ε.Ε.) για την προστασία των προσωπικών δεδομένων.

Η προστασία των προσωπικών δεδομένων, λοιπόν τίθεται ως ηθικό εμπόδιο στην αξιοποίηση του τεράστιου αυτού όγκου πληροφορίας. Έτσι ήταν πολύ σημαντικό να βρεθεί ένας τρόπος ο οποίος θα επιτρέπει να επωφεληθούμε από τα δεδομένα του κάθε κόμβου, χωρίς όμως να πα-

ραβιάζεται η ιδιωτικότητά του. Η Ομοσπονδιακή Μάθηση προτείνεται ως λύση στα προβλήματα της ιδιωτικότητας, αφού συνδυάζει την αποκεντρωμένη επεξεργασία δεδομένων για την ανάπτυξη μοντέλων ([McM+17]), με την ιδιωτικότητα και τη χρήση των δεδομένων με κομψό τρόπο.

1.1 Θεωρητικό Υπόβαθρο

Κατά τη διάρκεια της παρούσας διπλωματικής εργασίας, θα αναφερθούμε σε μια σειρά από βασικούς όρους και έννοιες που αποτελούν βάση για τις αναλύσεις και τις εφαρμογές που θα παρουσιαστούν. Οι έννοιες αυτές είναι κρίσιμες για την κατανόηση των θεμάτων που θα εξεταστούν και γι' αυτόν τον λόγο είναι απαραίτητο να αναφερθούν από την αρχή. Οι βασικοί αυτοί όροι παρουσιάζονται παρακάτω:

1. Συνάρτηση Χρησιμότητας (Utility Function): Στα οικονομικά και στη θεωρία παιγνίων, η συνάρτηση χρησιμότητας είναι μια μαθηματική αναπαράσταση των προτιμήσεων ενός παίκτη. Αποδίδει μια αριθμητική τιμή σε κάθε πιθανό αποτέλεσμα, υποδεικνύοντας το σχετικό επίπεδο ικανοποίησης ή οφέλους που ο παίκτης αποκομίζει από αυτό το αποτέλεσμα. Όσο υψηλότερη είναι η τιμή, τόσο μεγαλύτερη είναι η ικανοποίηση. [Wik24]

2. Θεωρία Παιγνίων (Game Theory): Η θεωρία παιγνίων είναι η μελέτη των στρατηγικών αλληλεπιδράσεων μεταξύ ατόμων. Παρέχει εργαλεία για την ανάλυση καταστάσεων όπου οι επιλογές κάθε ατόμου επηρεάζουν τα αποτελέσματα των άλλων. Με βάση την αλληλεπίδραση στο κοινό περιβάλλον, καθώς και τις προσωπικές προτιμήσεις κάθε παίκτη, στόχος είναι να πάρει ο καθένας την καλύτερη δυνατή απόφαση. [OR94]

3. Παιχνίδι Αντιστοίχισης (Matching Game): Το παιχνίδι αντιστοίχισης είναι ένας κλάδος της θεωρίας παιγνίων όπου οι παίκτες έχουν ως στόχο να αντιστοιχηθούν σε κάποιον άλλο παίκτη ή ομάδα, με σκοπό να βελτιστοποιήσουν το κέρδος τους. Τέτοια παιχνίδια συχνά χρησιμοποιούνται για την ανάλυση προβλημάτων κατανομής πόρων. [RS92]

4. Παιχνίδι Συμμαχίας (Coalition Game): Ένα παιχνίδι συμμαχίας, ή συνεργατικό παιχνίδι, είναι ένας κλάδος της θεωρίας παιγνίων όπου οι παίκτες μπορούν να σχηματίσουν συμμαχίες (συνασπισμούς) για να επιτύχουν καλύτερα αποτελέσματα συλλογικά. Η εστίαση είναι στο πώς να επιτευχθεί καλύτερο συλλογικό, αλλά και μεμονωμένο για κάθε παίκτη, αποτέλεσμα. [CEW11]

5. Ενισχυτική Μάθηση (Reinforcement Learning): Η Ενισχυτική Μάθηση (RL) είναι ένας τύπος μηχανικής μάθησης όπου ένας πράκτορας μαθαίνει να παίρνει αποφάσεις εκτελώντας ενέργειες σε ένα περιβάλλον για να μεγιστοποιήσει τη αμοιβή του. Ο πράκτορας δοκιμάζει τις δυνατές ενέργειές του σε κάθε επανάληψη, προσπαθώντας να αποφανθεί ποιες από αυτές του προσφέρουν τις καλύτερες ανταμοιβές. Έτσι προσπαθεί να πάρει απόφαση για την βέλτιστη ή τις βέλτιστες ενέργειες που μπορεί να εκτελέσει. [SB18a]

6. Εκτός Πολιτικής Αλγόριθμος (Off-policy Learning / Algorithm): Στην ενισχυτική μάθηση, ο όρος "εκτός πολιτικής" αναφέρεται σε ένα τύπο μάθησης όπου ο πράκτορας μπορεί να

μάθει για μια βέλτιστη ή επιθυμητή πολιτική ενώ ακολουθεί μια διαφορετική πολιτική συμπεριφοράς. Αυτό σημαίνει ότι ο πράκτορας μπορεί να μάθει από ενέργειες που δεν λαμβάνει απαραίτητα υπό την τρέχουσα πολιτική. Οι αλγόριθμοι εκτός πολιτικής χρησιμοποιούν εμπειρίες που δημιουργούνται από οποιαδήποτε πολιτική, όχι μόνο από αυτή που βελτιστοποιείται. Τα κύρια χαρακτηριστικά περιλαμβάνουν τη διάκριση μεταξύ της πολιτικής συμπεριφοράς, την οποία ακολουθεί ο πράκτορας για να δημιουργεί ενέργειες και να συλλέγει εμπειρίες, και της πολιτικής στόχου, την οποία ο πράκτορας επιδιώκει να βελτιστοποιήσει. Αυτή η προσέγγιση επιτρέπει στον πράκτορα να εξερευνά το περιβάλλον χρησιμοποιώντας μια πολιτική συμπεριφοράς που ενθαρρύνει την εξερεύνηση, ενώ μαθαίνει μια βέλτιστη πολιτική που εκμεταλλεύεται τις γνωστές ανταμοιβές. [SB18a]

7. Μάθηση με Μείωση της Μεταμέλειας (Μετανοητική Μάθηση - Regret Learning): Η μάθηση με μείωση της μεταμέλειας είναι μια στρατηγική στη θεωρία παιγνίων και την μηχανική μάθηση όπου οι παίκτες προσαρμόζουν τις ενέργειές τους βάσει της προηγούμενης απόδοσης για να ελαχιστοποιήσουν τη μεταμέλεια. Η μεταμέλεια μετρά τη διαφορά μεταξύ της πραγματικής αμοιβής που έλαβε ο παίκτης και της αμοιβής της κάθε δυνατής ενέργειας. Ο στόχος είναι να μάθει ο παίκτης τις καλύτερες για αυτόν ενέργειες με βάση το πόσο μετανιώνει όταν τις εκτέλεσε ή δεν τις εκτέλεσε. [Blu03]

8. Ενεργή Μάθηση (Online Learning): Η ενεργή μάθηση, στη μηχανική μάθηση, είναι ένα μοντέλο μάθησης όπου ο αλγόριθμος ενημερώνει τη γνώση του διαδοχικά καθώς φτάνουν νέα δεδομένα, επιτρέποντάς του να προσαρμόζεται σε πραγματικό χρόνο σε αλλαγές. Σε αντίθεση με την παραδοσιακή μάθηση κατά παρτίδες, η οποία επεξεργάζεται ολόκληρο το σύνολο δεδομένων ταυτόχρονα, η ενεργή μάθηση μαθαίνει συνεχώς από μεμονωμένα δεδομένα ή μικρές παρτίδες, καθιστώντας την πιο αποδοτική από άποψη μνήμης και επεκτάσιμη. Αυτή η προσέγγιση είναι ιδιαίτερα χρήσιμη σε δυναμικά περιβάλλοντα, όπως τα συστήματα συστάσεων, οι χρηματοπιστωτικές αγορές και η ανάλυση σε πραγματικό χρόνο, όπου τα δεδομένα εξελίσσονται γρήγορα. Ένα κοινό παράδειγμα είναι η Κάθοδος Στοχαστικής Κλίσης (SGD), η οποία ενημερώνει τις παραμέτρους του μοντέλου σταδιακά με κάθε νέο δεδομένο. [Set12]

9. Ταξινόμηση Εικόνας (Image Classification): Η ταξινόμηση εικόνας είναι ένα πρόβλημα όρασης υπολογιστών όπου ένας αλγόριθμος αποδίδει μια ετικέτα ή κατηγορία σε μια εικόνα βάσει του οπτικού της περιεχομένου. Περιλαμβάνει την εκπαίδευση μοντέλων, συχνά νευρωνικών δικτύων, για την αναγνώριση και κατηγοριοποίηση αντικειμένων, σκηνών ή άλλων μοτίβων στις εικόνες. [GBC16]

10. Νευρωνικά Δίκτυα / Αποδοτικά Νευρωνικά Δίκτυα (Neural Networks / Efficient Neural Networks): Τα νευρωνικά δίκτυα είναι μια κατηγορία μοντέλων μηχανικής μάθησης εμπνευσμένη από τη δομή και τη λειτουργία του ανθρώπινου εγκεφάλου. Αποτελούνται από διασυνδεδεμένα στρώματα κόμβων (νευρώνες) που επεξεργάζονται δεδομένα με ιεραρχικό τρόπο για την εκτέλεση καθηκόντων όπως ταξινόμηση, παλινδρόμηση και αναγνώριση μοτίβων. Τα αποδοτικά νευρωνικά δίκτυα είναι βελτιστοποιημένες εκδόσεις σχεδιασμένες να επιτυγ-

χάνουν υψηλή απόδοση με μειωμένους υπολογιστικούς πόρους, καθιστώντας τα κατάλληλα για εκπαίδευση και αξιοποίηση σε συσκευές με περιορισμένη ισχύ επεξεργασίας, όπως κινητά τηλέφωνα. [LBH15]

11. Μοντέλο και Στρώματα Μοντέλου (Machine Learning Model & Model Layers): Ένα μοντέλο στη μηχανική μάθηση είναι μια μαθηματική αναπαράσταση ενός συστήματος που χρησιμοποιείται για την πρόβλεψη ή τη λήψη αποφάσεων βάσει εισαγόμενων δεδομένων. Τα μοντέλα μπορεί να κυμαίνονται από απλές γραμμικές παλινδρομήσεις έως πολύπλοκα νευρωνικά δίκτυα. Τα στρώματα μοντέλου αναφέρονται στα ατομικά δομικά στοιχεία ενός νευρωνικού δικτύου. Κάθε στρώμα αποτελείται από νευρώνες που εφαρμόζουν συγκεκριμένους μετασχηματισμούς στα εισαγόμενα δεδομένα. Κοινά είδη στρώσεων περιλαμβάνουν τα συνελικτικά στρώματα (για την ανίχνευση χωρικών χαρακτηριστικών), τα στρώματα υποδειγμάτων (για τη μείωση του μεγέθους) και τα πλήρως συνδεδεμένα στρώματα (για την ενσωμάτωση χαρακτηριστικών). [Cho18]

12. Προ-εκπαιδευμένο Μοντέλο Μηχανικής Μάθησης (Pre-trained Model): Ένα προ-εκπαιδευμένο μοντέλο στη μηχανική μάθηση είναι ένα μοντέλο που έχει ήδη εκπαιδευτεί σε ένα μεγάλο σύνολο δεδομένων και στη συνέχεια προσαρμόζεται ή βελτιστοποιείται για να εκτελεί συγκεκριμένα καθήκοντα. Αυτή η προσέγγιση αξιοποιεί τη γνώση που έχει αποκτήσει το μοντέλο κατά την αρχική φάση της εκπαίδευσης για να βελτιώσει την απόδοση και να μειώσει το χρόνο και τους πόρους που απαιτούνται για την εκπαίδευση σε νέες εργασίες. [HR18]

    Αρχική Εκπαίδευση: Το μοντέλο εκπαιδεύεται πρώτα σε ένα μεγάλο, γενικό σύνολο δεδομένων. Για παράδειγμα, στην επεξεργασία φυσικής γλώσσας (NLP), μοντέλα όπως το BERT ή το GPT εκπαιδεύονται σε τεράστιες ποσότητες κειμένων από το διαδίκτυο.

    Μεταφορά Γνώσης: Το προ-εκπαιδευμένο μοντέλο έχει ήδη μάθει χρήσιμα χαρακτηριστικά και μοτίβα από την αρχική του εκπαίδευση. Αυτά τα χαρακτηριστικά μπορούν να μεταφερθούν σε νέες εργασίες, συχνά με αποτέλεσμα καλύτερη απόδοση.

    Αποδοτικότητα: Η χρήση ενός προ-εκπαιδευμένου μοντέλου μπορεί να μειώσει σημαντικά τους υπολογιστικούς πόρους και το χρόνο που απαιτείται για την εκπαίδευση, καθώς το μοντέλο δεν χρειάζεται να μάθει από την αρχή.

    Απόδοση: Τα προ-εκπαιδευμένα μοντέλα συχνά επιτυγχάνουν υψηλότερη απόδοση σε συγκεκριμένες εργασίες, καθώς αξιοποιούν τις πλούσιες αναπαραστάσεις χαρακτηριστικών που έχουν μάθει κατά την αρχική τους εκπαίδευση.

13. Ακρίβεια (Accuracy): Η ακρίβεια είναι ένα μέτρο απόδοσης σε προβλήματα ταξινόμησης, που ορίζεται ως το ποσοστό των σωστών προβλέψεων σε σχέση με το συνολικό αριθμό των παραδειγμάτων. Η ακρίβεια χρησιμοποιείται συχνά για την αξιολόγηση της απόδοσης των αλγορίθμων μηχανικής μάθησης. [GBC16]

14. Απώλεια (Loss): Η απώλεια είναι μια συνάρτηση που μετράει το πόσο καλά ή κακά αποδίδει ένα μοντέλο μηχανικής μάθησης. Αντιπροσωπεύει τη διαφορά μεταξύ των προβλέψεων του

μοντέλου και των πραγματικών τιμών. Στόχος είναι η ελαχιστοποίηση της απώλειας κατά την εκπαίδευση του μοντέλου για να βελτιωθεί η ακρίβεια των προβλέψεων. [GBC16]

15. Εξαγωγή Χαρακτηριστικών (Feature Extraction): Η εξαγωγή χαρακτηριστικών είναι μια κρίσιμη διαδικασία στη μηχανική μάθηση και την ανάλυση δεδομένων, όπου τα ακατέργαστα δεδομένα μετατρέπονται σε ένα σύνολο σχετικών γνωρισμάτων ή χαρακτηριστικών που μπορούν να χρησιμοποιηθούν για την εκπαίδευση ενός μοντέλου. Αυτή η διαδικασία αποσκοπεί στη μείωση της πολυπλοκότητας των δεδομένων διατηρώντας ταυτόχρονα τα βασικά τους μοτίβα και δομές. Η αποτελεσματική εξαγωγή χαρακτηριστικών βοηθά στη βελτίωση της απόδοσης των αλγορίθμων μηχανικής μάθησης εστιάζοντας στις πιο ενημερωτικές πτυχές των δεδομένων, επιτρέποντας έτσι στο μοντέλο να κάνει πιο ακριβείς προβλέψεις. Οι τεχνικές για την εξαγωγή χαρακτηριστικών μπορούν να διαφέρουν ανάλογα με τον τύπο των δεδομένων και το συγκεκριμένο πρόβλημα που αντιμετωπίζεται. Για παράδειγμα, στην επεξεργασία εικόνας, η εξαγωγή χαρακτηριστικών μπορεί να περιλαμβάνει την αναγνώριση ακμών, υφών ή σχημάτων μέσα σε μια εικόνα. Στην επεξεργασία φυσικής γλώσσας, μπορεί να περιλαμβάνει την εξαγωγή λέξεων-κλειδιών, n-γραμμάτων ή συντακτικών δομών από το κείμενο. Ο στόχος είναι να δημιουργηθεί μια απλοποιημένη αναπαράσταση των δεδομένων που διατηρεί τα σημαντικά τους χαρακτηριστικά, κάνοντάς τα πιο εύκολα για τα μοντέλα μηχανικής μάθησης να μάθουν και να γενικεύσουν καλά σε νέα, άγνωστα δεδομένα.

16. Υπερπροσαρμογή (Overfitting): Η υπερπροσαρμογή είναι ένα συνηθισμένο πρόβλημα στη μηχανική μάθηση, όπου ένα μοντέλο μαθαίνει τα δεδομένα εκπαίδευσης πολύ καλά, καταγράφοντας θόρυβο και ανωμαλίες μαζί με τα υποκείμενα μοτίβα. Αυτό έχει ως αποτέλεσμα ένα μοντέλο που αποδίδει εξαιρετικά καλά στα δεδομένα εκπαίδευσης, αλλά άσχημα σε νέα, άγνωστα δεδομένα. Η υπερπροσαρμογή εμφανίζεται όταν το μοντέλο είναι πολύπλοκο σε σχέση με την ποσότητα των δεδομένων εκπαίδευσης, συχνά χαρακτηριζόμενο από την ύπαρξη υπερβολικά πολλών παραμέτρων. Αυτή η υπερβολική πολυπλοκότητα επιτρέπει στο μοντέλο να προσαρμόζεται ακόμα και στις μικρές διακυμάνσεις των δεδομένων εκπαίδευσης, οδηγώντας σε έλλειψη γενίκευσης. Τεχνικές για την αποτροπή της υπερπροσαρμογής περιλαμβάνουν την απλοποίηση του μοντέλου μειώνοντας τον αριθμό των παραμέτρων, τη χρήση μεθόδων κανονικοποίησης όπως η L1 ή L2 κανονικοποίηση, και την εφαρμογή διασταυρούμενης επικύρωσης για να διασφαλιστεί ότι η απόδοση του μοντέλου αξιολογείται σε πολλαπλά υποσύνολα των δεδομένων. Μια άλλη αποτελεσματική προσέγγιση είναι η συγκέντρωση περισσότερων δεδομένων εκπαίδευσης, τα οποία μπορούν να βοηθήσουν το μοντέλο να μάθει πιο γενικευμένα μοτίβα. [Ama24]

17. Κανονικοποίηση και L2 Κανονικοποίηση (Regularization & L2 Regularization): Η κανονικοποίηση είναι μια θεμελιώδης τεχνική στη μηχανική μάθηση και τη στατιστική μοντελοποίηση που έχει σχεδιαστεί για να αποτρέπει την υπερεκπαίδευση, η οποία συμβαίνει όταν ένα μοντέλο γίνεται πολύ περίπλοκο και συλλαμβάνει θόρυβο ή τυχαίες διακυμάνσεις στα δεδομένα εκπαίδευσης αντί να γενικεύει καλά σε άγνωστα δεδομένα. Εισάγοντας πρόσθετους περιορισμούς ή ποινές, η κανονικοποίηση βοηθά στη δημιουργία ενός πιο ανθεκτικού μοντέλου που επιτυγχάνει καλύτερα σε νέα δεδομένα. [GBC16]

Η κανονικοποίηση L2, γνωστή και ως κανονικοποίηση Ridge, είναι μία από τις πιο συχνά χρησιμοποιούμενες μορφές κανονικοποίησης. Λειτουργεί προσθέτοντας μια ποινή αναλογική με το τετράγωνο του μεγέθους των βαρών στη συνάρτηση απώλειας που χρησιμοποιείται κατά την εκπαίδευση. Συγκεκριμένα, αν συμβολίσουμε τα βάρη του μοντέλου ως w, η κανονικοποίηση L2 προσθέτει έναν όρο $\lambda \sum_i w_i^2$ στη συνάρτηση απώλειας, όπου λ είναι μια υπερπαράμετρος που ελέγχει τη δύναμη της κανονικοποίησης. Αυτός ο όρος αποθαρρύνει το μοντέλο από το να δίνει υπερβολική σημασία σε οποιοδήποτε μεμονωμένο χαρακτηριστικό, επιβάλλοντας ποινές σε μεγάλους συντελεστές και ενθαρρύνοντας το μοντέλο να κατανεμηθεί πιο ομοιόμορφα σε όλα τα χαρακτηριστικά.

Το κύριο πλεονέκτημα της κανονικοποίησης L2 είναι ότι βοηθά στην εξομάλυνση της διαδικασίας εκμάθησης και στη μείωση της διακύμανσης του μοντέλου με τη μείωση των βαρών προς το μηδέν, αλλά ποτέ στο μηδέν. Αυτή η επίδραση της μείωσης συχνά οδηγεί σε απλούστερα μοντέλα που είναι λιγότερο ευαίσθητα στις διακυμάνσεις των δεδομένων εκπαίδευσης, γεγονός που ενισχύει τις ικανότητές τους για γενίκευση. Σε αντίθεση με την κανονικοποίηση L1, η οποία μπορεί να οδηγήσει σε σπάνια μοντέλα με κάποιους συντελεστές ακριβώς μηδέν, η κανονικοποίηση L2 έχει την τάση να παράγει μοντέλα όπου όλα τα χαρακτηριστικά συνεισφέρουν σε κάποιο βαθμό, αν και με μικρότερα βάρη. Αυτό το χαρακτηριστικό καθιστά την κανονικοποίηση L2 ιδιαίτερα χρήσιμη σε σενάρια όπου πιστεύουμε ότι όλα τα χαρακτηριστικά έχουν κάποια επίπεδα σημασίας και πρέπει να διατηρηθούν στο μοντέλο.

18. Ομοσπονδιακή Μάθηση (Federated Learning): Η ομοσπονδιακή μάθηση είναι μια τεχνική μηχανικής μάθησης όπου πολλές αποκεντρωμένες συσκευές συνεργάζονται για να εκπαιδεύσουν ένα μοντέλο χωρίς να μοιράζονται τα τοπικά δεδομένα τους. Αντίθετα, κάθε συσκευή εκπαιδεύει το μοντέλο τοπικά και μόνο μοιράζεται τα βάρη του μοντέλου που εκπαίδευσε με έναν κεντρικό διακομιστή. Αυτή η προσέγγιση ενισχύει την ιδιωτικότητα και την ασφάλεια των δεδομένων, ενώ επιπλέον το κεντρικό μοντέλο μπορεί να εκπαιδευτεί από πολλαπλές πηγές. Αντίστοιχα, είναι σημαντικό να σημειωθεί πως μειώνεται πολύ η κίνηση στο δίκτυο, αφού δεν απαιτείται η μεταφορά μεγάλων δεδομένων (π.χ. εικόνων) στον κεντρικό υπολογιστή στον οποίο εκπαιδεύεται το μοντέλο, αλλά γίνεται μόνο μεταφορά βαρών των επιπέδων του νευρωνικού μοντέλου. [McM+17]

1.2 Σύγχρονη Έρευνα

Όπως αναφέρεται από τον Liu et al. ([Liu+24]), η Ομοσπονδιακή Μάθηση (Federated Learning - FL) έχει αναδειχθεί ως μία πρωτοπόρος μέθοδος που επιτρέπει τη συνεργατική εκπαίδευση μοντέλων μηχανικής μάθησης, διατηρώντας παράλληλα την ιδιωτικότητα των δεδομένων. Σε αντίθεση με τις παραδοσιακές μεθόδους κεντρικής εκμάθησης που συγκεντρώνουν ακατέργαστα δεδομένα από διανεμημένες πηγές, η Ομοσπονδιακή Μάθηση επιτρέπει σε πολλαπλούς συμμετέχοντες να εκπαιδεύουν κοινά μοντέλα ανταλλάσσοντας παραμέτρους, διασφαλίζοντας έτσι ότι τα ευαίσθητα δεδομένα παραμένουν τοπικά. Αυτή η καινοτόμος προσέγγιση αντιμετωπίζει ζητήματα ιδιωτικότη-

τας, συμμόρφωσης με κανονισμούς όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) και περιορισμούς στη διαμοίραση δεδομένων σε τομείς όπως η υγεία και τα χρηματοοικονομικά.

Πρόσφατες εξελίξεις στην Ομοσπονδιακή Μάθηση επικεντρώνονται στην αντιμετώπιση βασικών προκλήσεων: ετερογένεια, ασφάλεια και δικαιοσύνη. Για να αντιμετωπιστεί η ετερογένεια που χαρακτηρίζει τα περιβάλλοντα Ομοσπονδιακής Μάθησης —η οποία προκύπτει από διαφορετικές κατανομές δεδομένων, ποικίλες αρχιτεκτονικές μοντέλων και άνισες συστημικές δυνατότητες— οι ερευνητές έχουν αναπτύξει νέες τεχνικές, όπως η πολυ-εργασιακή εκμάθηση (multi-task learning), η μεταφορά μάθησης (transfer learning) και η τοπικά συγκεντρωτική μάθηση (clustering-based approaches). Αυτές οι μέθοδοι ενισχύουν τη δυνατότητα της Ομοσπονδιακής Μάθησης να διαχειρίζεται μη-ανεξάρτητα και μη-ισοκατανεμημένα δεδομένα (non-IID) και να προσαρμόζει μοντέλα σε ποικίλα περιβάλλοντα κόμβων. Για παράδειγμα, η μετα-εκμάθηση (meta-learning) έχει προσαρμοστεί στις διαδικασίες της Ομοσπονδιακής Μάθησης, επιτρέποντας την εξατομίκευση μέσω βελτιστοποίησης για συγκεκριμένους στόχους κόμβων.

Η ασφάλεια και η ιδιωτικότητα παραμένουν κεντρικές ανησυχίες στην Ομοσπονδιακή Μάθηση, με προσπάθειες που στοχεύουν σε επιθέσεις όπως η αναστροφή βαθμίδων (gradient inversion attacks), οι κακόβουλες παρεμβάσεις (backdoor attacks) και η δηλητηρίαση μοντέλων (model poisoning). Προηγμένες τεχνικές κρυπτογράφησης, όπως η διαφορική ιδιωτικότητα (differential privacy) και η ομομορφική κρυπτογράφηση (homomorphic encryption), ενσωματώνονται όλο και περισσότερο στα πλαίσια της Ομοσπονδιακής Μάθησης για την προστασία ευαίσθητων πληροφοριών κατά τη διαδικασία συγκέντρωσης μοντέλων. Επιπλέον, τα Περιβάλλοντα Αξιόπιστης Εκτέλεσης (Trusted Execution Environments - TEEs) χρησιμοποιούνται για την παροχή ασφάλειας σε επίπεδο υλικού, διασφαλίζοντας ισχυρή άμυνα έναντι πιθανών διαρροών δεδομένων.

Η δικαιοσύνη στην Ομοσπονδιακή Μάθηση έχει επίσης αποκτήσει σημαντική προσοχή, με στόχο την αντιμετώπιση προκαταλήψεων που προκύπτουν από άνισες συνεισφορές πελατών ή άνιση απόδοση μοντέλων μεταξύ συμμετεχόντων. Προσεγγίσεις όπως η ομοσπονδιακή δίκαιη εξομάλυνση (federated fair averaging) και οι επανασταθμισμένες αντικειμενικές συναρτήσεις (reweighted objective functions) στοχεύουν στη διασφάλιση δίκαιων αποτελεσμάτων για όλα τα μέρη, βελτιώνοντας τόσο τη μεμονωμένη όσο και τη συνολική δικαιοσύνη. Αυτές οι μέθοδοι είναι κρίσιμες για την ενίσχυση της εμπιστοσύνης και της συμμετοχής στα συστήματα FL, ιδιαίτερα σε εφαρμογές με ποικίλες βάσεις κόμβων.

Ο τομέας της Ομοσπονδιακής Μάθησης γνωρίζει επίσης την ανάπτυξη κλιμακούμενων και ευέλικτων πλαισίων, όπως το FedLab και το Flower, που απλοποιούν την εφαρμογή της Ομοσπονδιακής Μάθησης σε ετερογενείς συσκευές και περιβάλλοντα. Αυτές οι πλατφόρμες διευκολύνουν πειράματα μεγάλης κλίμακας και γεφυρώνουν το χάσμα μεταξύ έρευνας και πραγματικής εφαρμογής, επιτρέποντας στην Ομοσπονδιακή Μάθηση να εξελιχθεί ως θεμέλιος λίθος της τεχνητής νοημοσύνης με διαφύλαξη ιδιωτικότητας. Στο μέλλον, οι ερευνητές εξετάζουν δυναμικά μοντέλα Ομοσπονδιακής Μάθησης που μπορούν να προσαρμόζονται σε συνεχώς μεταβαλλόμενα περιβάλλοντα δεδομένων, αποκεντρωμένα συστήματα Ομοσπονδιακής Μάθησης για την εξάλειψη της εξάρτησης από κεντρικούς διακομιστές και ενιαία σημεία αναφοράς για την τυποποίηση των αξιολογήσεων απόδοσης μεταξύ των μελετών.

Η Ομοσπονδιακή Μάθηση έχει φέρει επανάσταση σε πολλούς τομείς, επιτρέποντας τη συνερ-

γατική εκπαίδευση μοντέλων ενώ διασφαλίζει την προστασία των ευαίσθητων δεδομένων.

Σαν πρώτο παράδειγμα αναφέρουμε την υγειονομική περίθαλψη, όπου τα ευαίσθητα δεδομένα ασθενών πρέπει να παραμένουν εμπιστευτικά. Νοσοκομεία και ερευνητικά ιδρύματα χρησιμοποιούν την Ομοσπονδιακή Μάθηση για τη συνεργατική εκπαίδευση μοντέλων για ιατρική απεικόνιση, διάγνωση ασθενειών και ανακάλυψη φαρμάκων. Για παράδειγμα, επιτρέπει την ανάπτυξη προγνωστικών μοντέλων για την ανίχνευση ασθενειών όπως ο καρκίνος ή οι καρδιαγγειακές παθήσεις, συνδυάζοντας γνώσεις από διανεμημένα σύνολα δεδομένων χωρίς την κοινή χρήση ακατέργαστων ιατρικών αρχείων. Αυτή η συνεργατική προσέγγιση επιταχύνει την καινοτομία διατηρώντας αυστηρά πρότυπα ιδιωτικότητας.

Στον χρηματοοικονομικό τομέα, η Ομοσπονδιακή Μάθηση βελτιώνει την ανίχνευση απάτης, την αξιολόγηση πιστωτικού κινδύνου και τη διαχείριση κινδύνου, αξιοποιώντας κατανεμημένα σύνολα δεδομένων από τράπεζες και χρηματοοικονομικούς οργανισμούς. Ευαίσθητα χρηματοοικονομικά δεδομένα, που συχνά περιορίζονται από κανονισμούς και ανησυχίες για την ιδιοκτησία, μπορούν να χρησιμοποιηθούν για την εκπαίδευση ισχυρών προγνωστικών μοντέλων. Για παράδειγμα, τα συστήματα αξιολόγησης πιστοληπτικής ικανότητας που βασίζονται στην Ομοσπονδιακή Μάθηση συγκεντρώνουν πληροφορίες από πολλές τράπεζες, επιτρέποντας δικαιότερες και ακριβέστερες αξιολογήσεις χωρίς να εκθέτουν μεμονωμένα δεδομένα πελατών.

Η Ομοσπονδιακή Μάθηση διαδραματίζει κρίσιμο ρόλο στη βελτίωση εξατομικευμένων υπηρεσιών σε κινητές συσκευές. Εφαρμογές περιλαμβάνουν εξατομικευμένες συστάσεις, προγνωστική πληκτρολόγηση και αναγνώριση φωνής, όπως η χρήση της Ομοσπονδιακής Μάθησης από την Google στο πληκτρολόγιο Gboard για τη βελτίωση της προγνωστικής πληκτρολόγησης χωρίς τη συλλογή δεδομένων κόμβων. Η Ομοσπονδιακή Μάθηση επίσης ενισχύει συσκευές αιχμής σε οικοσυστήματα IoT, επιτρέποντας τη μάθηση σε πραγματικό χρόνο για έξυπνα σπίτια, αυτόνομα οχήματα και φορετές συσκευές, μειώνοντας την κατανάλωση εύρους ζώνης και διασφαλίζοντας την ιδιωτικότητα.

Σε βιομηχανικές ρυθμίσεις, η Ομοσπονδιακή Μάθηση χρησιμοποιείται για τη βελτιστοποίηση των διαδικασιών παραγωγής, την προγνωστική συντήρηση και τη διαχείριση της εφοδιαστικής αλυσίδας. Για παράδειγμα, αισθητήρες σε εργοστάσια μπορούν να εκπαιδεύουν συνεργατικά μοντέλα για την πρόβλεψη βλαβών εξοπλισμού χωρίς να μοιράζονται ευαίσθητα δεδομένα ή δεδομένα ιδιοκτησίας, μειώνοντας τον χρόνο διακοπής λειτουργίας της βιομηχανικής μονάδας και βελτιώνοντας την αποδοτικότητα.

Η Ομοσπονδιακή Μάθηση υποστηρίζει την ανάπτυξη εφαρμογών για έξυπνες πόλεις, όπως η διαχείριση κυκλοφορίας, η δημόσια ασφάλεια και η βελτιστοποίηση της ενέργειας. Συστήματα παρακολούθησης της κυκλοφορίας, για παράδειγμα, μπορούν να χρησιμοποιήσουν την Ομοσπονδιακή Μάθηση για την εκπαίδευση προγνωστικών μοντέλων από κατανεμημένες κάμερες κυκλοφορίας, ώστε να βελτιστοποιήσουν τη ροή της κυκλοφορίας χωρίς την συλλογή ευαίσθητων δεδομένων βίντεο.

Η Ομοσπονδιακή Μάθηση εφαρμόζεται ολοένα και περισσότερο στην εκπαίδευση για προσαρμοστικά συστήματα μάθησης που εξατομικεύουν το περιεχόμενο με βάση την απόδοση των μαθητών. Εκπαιδεύοντας μοντέλα μεταξύ ιδρυμάτων, η Ομοσπονδιακή Μάθηση διευκολύνει τη συνεργατική καινοτομία σε πλατφόρμες ηλεκτρονικής μάθησης, διατηρώντας παράλληλα την ε-

μπιστευτικότητα των δεδομένων των μαθητών.

Το πρόβλημα της επιλογής κόμβων στην Ομοσπονδιακή Μάθηση (Federated Learning - FL) έχει προσελκύσει το ενδιαφέρον της ερευνητικής κοινότητας, δεδομένου ότι μια τυχαία προσέγγιση επιλογής εισάγει σημαντικές προκλήσεις λόγω της ποικιλίας στην ποιότητα δεδομένων και των διαφορών στους διαθέσιμους πόρους των κόμβων [Weh+22]. Ένας νέος αλγόριθμος για την επιλογή κόμβων σε περιβάλλον Ομοσπονδιακής Μάθησης με πολλαπλά μοντέλα παρουσιάζεται στο [WLW22], ο οποίος βελτιστοποιεί την κατανομή πόρων και τους ρυθμούς σύγκλισης. Μια προσέγγιση αμοιβαίας εμπιστοσύνης για την επιλογή κόμβων και διακομιστών στην Ομοσπονδιακή Μάθηση αναλύεται στο [Weh+23], αξιοποιώντας θεωρία παιγνίων και μηχανισμούς bootstrap για τη βελτίωση των επιπέδων εμπιστοσύνης και της ακρίβειας του παγκόσμιου μοντέλου.

Ένα μοντέλο Ομοσπονδιακής Μάθησης που χρησιμοποιεί ενισχυτική μάθηση βάσει της κατανομής δεδομένων προτείνεται στο [TZD23] για την αντιμετώπιση της μη ανεξάρτητης και ομοιόμορφης κατανομής δεδομένων (non-IID), επιτυγχάνοντας βελτιωμένη ακρίβεια ελέγχου και μειωμένο αριθμό επικοινωνιακών γύρων σε σύγκριση με υπάρχουσες μεθόδους. Ένα ιεραρχικό μοντέλο Ομοσπονδιακής Μάθησης αναπτύσσεται στο [CDP23a] για τη βελτίωση της επικοινωνίας σε συμβατικά περιβάλλοντα Ομοσπονδιακής Μάθησης μέσω ασύρματων δικτύων, εστιάζοντας στο πρόβλημα της σύνδεσης κόμβων με διακομιστές άκρων και στην κατανομή ασύρματων πόρων για την εξισορρόπηση της ακρίβειας εκπαίδευσης και της ενεργειακής κατανάλωσης μέσω ενός κατανεμημένου πλαισίου βασισμένου στη θεωρία παιγνίων.

Πρόσφατες προσεγγίσεις εστιάζουν στη συστάδα (clustering) μεταξύ των κόμβων για την υποστήριξη εργασιών Ομοσπονδιακής Μάθησης. Ένα περιβάλλον Ομοσπονδιακής Μάθησης προτείνεται στο [Gau+22], όπου οι διακομιστές συνεργάζονται για εξατομικευμένη μάθηση μέσω συστάδων κόμβων, αντιμετωπίζοντας τις προκλήσεις ανισομερούς κατανομής κόμβων και έλλειψης δεδομένων. Ένας αλγόριθμος επιλογής κόμβων σε ιεραρχική Ομοσπονδιακή Μάθηση παρουσιάζεται στο [XZX22], βελτιώνοντας την ποιότητα εκπαίδευσης του παγκόσμιου μοντέλου με βάση την πρόβλεψη φήμης των κόμβων και την αξιοποίηση επικοινωνίας συσκευών-με-συσκευές. Ένας μηχανισμός επιλογής κόμβων σε πραγματικό χρόνο και κατ' απαίτηση για την Ομοσπονδιακή Μάθηση προτείνεται στο [Ari+23], χρησιμοποιώντας συστάδες για την ομαδοποίηση κόμβων με βάση τα κριτήρια συγκεκριμένων εργασιών, με αποτέλεσμα τη βελτίωση της συνολικής απόδοσης της Ομοσπονδιακής Μάθησης σε σύγκριση με τυχαίες μεθόδους επιλογής.

1.3 Σκοπός της Διπλωματικής Εργασίας

Παρά τις προηγούμενες ερευνητικές προσπάθειες για την αντιμετώπιση του προβλήματος επιλογής κόμβων για τη βελτίωση της απόδοσης της Ομοσπονδιακής Μάθησης, οι υπάρχουσες προσεγγίσεις επικεντρώνονται κυρίως στην κεντρική επιλογή από τους εξυπηρετητές. Μέχρι τώρα, καμία προηγούμενη εργασία δεν επιτρέπει στους κόμβους να επιλέγουν αυτόνομα τους βέλτιστους εξυπηρετητές τους, ώστε να μεγιστοποιούν τα οφέλη τους, βελτιώνοντας συλλογικά την επίδοση του παγκόσμιου μοντέλου.

Η πολυπλοκότητα αυτή αυξάνεται σε περιβάλλοντα Ομοσπονδιακής Μάθησης πολλαπλών μοντέλων, όπου διαφορετικοί εξυπηρετητές εκπαιδεύουν διαφορετικά παγκόσμια μοντέλα, ενώ η

ποιότητα, η ποικιλία δεδομένων και οι δυνατότητες εκπαίδευσης των κόμβων αποτελούν κρίσιμους παράγοντες στην επιλογή κόμβων. Το πρόβλημα επιλογής κόμβων γίνεται πιο περίπλοκο όταν τόσο οι κόμβοι όσο και οι διακομιστές στοχεύουν να βελτιστοποιήσουν από κοινού τα οφέλη τους από τη διαδικασία Ομοσπονδιακής Μάθησης.

Ως κύριες προτάσεις αυτής της διπλωματικής εργασίας έχουμε τον μηχανισμό FedLearner, ο οποίος επιτρέπει την αμφίδρομη επιλογή μεταξύ κόμβων και εξυπηρετητών για τη βελτίωση της ακρίβειας των παγκόσμιων μοντέλων και τους μηχανισμούς RegretMatching (Πλήρους και Ελλιπούς Πληροφορίας), οι οποίοι επιπλέον επιτρέπουν στους κόμβους να εξετάσουν και να διαμορφώσουν την συμμετοχή τους στην Ομοσπονδιακή Μάθηση. Τα κύρια σημεία συνοψίζονται ως εξής:

1. Παρουσιάζεται ένα ασύρματο δίκτυο Ομοσπονδιακής Μάθησης πολλαπλών μοντέλων, αποτελούμενο από πολλαπλούς εξυπηρετητές που εκπαιδεύουν παράλληλα διαφορετικά παγκόσμια μοντέλα για την υποστήριξη λειτουργιών σε έξυπνες πόλεις, όπως η ανίχνευση γεγονότων δημόσιας ασφάλειας. Διαφορετικοί κρίσιμοι τομείς ενδιαφέροντος στις έξυπνες πόλεις προσδιορίζονται, ζητώντας από τους κόμβους να συλλέξουν δεδομένα και να εκπαιδεύσουν τα παγκόσμια μοντέλα για διαφορετικά γεγονότα, π.χ., ανίχνευση φωτιάς, σεισμών και πλημμυρών.

2. Εισάγεται ο μηχανισμός FedLearner ως ένα αρθρωτό πλαίσιο που αποτελείται από τα υποσυστήματα Προσεγγιστικού FedLearner και Ακριβή FedLearner. Ο Προσεγγιστικός FedLearner αγνοεί τις εξωτερικότητες των κόμβων, δηλαδή τις αποφάσεις επιλογής εξυπηρετητών από άλλους κόμβους, για να καθορίσει γρήγορα έναν αρχικό αντιστοίχιση μεταξύ κόμβων και διακομιστών.

3. Ο Ακριβής FedLearner εξετάζει τις εξωτερικότητες των κόμβων, ενσωματώνει την έξοδο του Προσεγγιστικού FedLearner, και βελτιώνει την αντιστοίχιση, λαμβάνοντας υπόψη τα χαρακτηριστικά επικοινωνίας και υπολογισμού των κόμβων, με στόχο τη βελτιστοποίηση των οφελών τόσο για τους κόμβους όσο και για τους εξυπηρετητές.

4. Εισάγονται οι μηχανισμοί αντιστοίχισης RegretMatching (Πλήρους και Ελλιπούς Πληροφορίας). Και οι δύο μηχανισμοί επιτρέπουν στους κόμβους να επιλέξουν πόσους πόρους θα διαθέσουν στην διαδικασία της Ομοσπονδιακής Μάθησης, για παράδειγμα πόσα δεδομένα θα χρησιμοποιήσουν για την τοπική εκπαίδευση ή πόση ισχύ θα διαθέσουν για την μετάδοση των τοπικών τους παραμέτρων. Ο Αλγόριθμος Πλήρους Πληροφορίας γνωρίζει τις ενέργειες των υπολοίπων κόμβων του συστήματος ενώ αντίθετα ο Ελλιπούς Πληροφορίας τις αγνοεί και παίρνει ανατροφοδότηση από τις δικές του ενέργειες.

1.4 Διάρθρωση Διπλωματικής Εργασίας

Στο πλαίσιο της διπλωματικής εργασίας έχουμε ως στόχο την αντιστοίχιση κόμβων με εξυπηρετητές, οι οποίοι ενδιαφέρονται να εκπαιδεύσουν κεντρικά μοντέλα αναγνώρισης και ταξινόμησης

εικόνας, ώστε να πετύχουμε το καλύτερο δυνατό στην εκπαίδευση μέσω Ομοσπονδιακής Μάθησης. Στο πρώτο μέρος της διπλωματικής (Κεφ. 2) θα μελετήσουμε έναν αλγόριθμο αντιστοίχισης που βασίζεται στη Θεωρία Παιγνίων, ο οποίος αποτελείται από δύο επιμέρους αλγορίθμους που εκτελούν με σειρά Προσεγγιστική και Ακριβή αντιστοίχιση. Στη συνέχεια, θα μελετήσουμε το μοντέλο και την επίδοση της Ομοσπονδιακής Μάθησης για την παραπάνω αντιστοίχιση (Κεφ. 2.3, 2.4). Ως δεύτερο μέρος (Κεφ. 3), ακολουθεί η σύγκριση του Αλγορίθμου με Θεωρία Παιγνίων με άλλους αλγορίθμους Μηχανικής Μάθησης και συγκεκριμένα μέσω Ενισχυτικής Μάθησης, όσον αφορά την επίδοση της αντιστοίχισης αλλά και της Ομοσπονδιακής Μάθησης. Στο τρίτο μέρος (Κεφ. 4) της διπλωματικής εργασίας θα μελετήσουμε μια διαφορετική προσέγγιση στη λειτουργία των κόμβων κατά την οποία οι κόμβοι θα μπορούν να ελέγξουν τους πόρους τους οποίους διαθέτουν στην Ομοσπονδιακή Μάθηση με στόχο να μεγιστοποιήσουν το κέρδος τους. Στο πλαίσιο αυτό θα δούμε κάποιους αλγορίθμους Μετανοητικής Μάθησης, τους οποίους θα συγκρίνουμε και με τον αρχικό αλγόριθμο Θεωρίας Παιγνίων. Τέλος θα ολοκληρώσουμε την εργασία μελετώντας την σημασία των αποτελεσμάτων μας, αλλά και πιθανές άλλες εφαρμογές του συστήματός που περιγράψαμε.

Στα αποτελέσματα που θα περιγράψουμε, θα μελετήσουμε και θα αναλύσουμε την συμπεριφορά διαφόρων διαμορφώσεων του προβλήματός μας (διαφορετικός αριθμός κόμβων, διαφορετική τεχνική αντιστοίχισης κ.ο.κ.). Για την ορθή εκπόνηση των πειραμάτων, εκτελούμε κάθε ένα από αυτά 5 ή 10 φορές, ανάλογα με την απαιτητικότητά του σε πόρους. Έτσι, πειράματα που αφορούν απλώς αντιστοίχιση των κόμβων με τους εξυπηρετητές τρέχουν 10 φορές για κάθε διαφορετική διαμόρφωση, ενώ πειράματα που αφορούν το χρονοβόρο κομμάτι της Ομοσπονδιακής Μάθησης για την ταξινόμηση των εικόνων, εκτελούνται 5 φορές για κάθε διαφορετική διαμόρφωση.

2

Αντιστοίχιση με Αλγορίθμους Θεωρίας Παιγνίων - Ομοσπονδιακή Μάθηση

Στόχος της παρούσας διπλωματικής εργασίας είναι να δημιουργήσουμε από το οικοσύστημα μας (εξυπηρετητές, κρίσιμα σημεία, κόμβους, που θα περιγραφούν και στη συνέχεια), ένα συνασπισμό για κάθε εξυπηρετητή. Σε κάθε τέτοιο συνασπισμό επιχειρούμε να πετύχουμε την καλύτερη δυνατή επίδοση για το μοντέλο αναγνώρισης και ταξινόμησης εικόνας του εξυπηρετητή, μέσω Ομοσπονδιακής Μάθησης, εκπαιδεύοντας έτσι στο δίκτυό μας πολλαπλά μοντέλα. Ως πρώτο κομμάτι, θα αναφερθούμε στην χρήση Θεωρίας Παιγνίων για την αντιστοίχιση κόμβων - εξυπηρετητών, με στόχο την βελτιστοποίηση των αποτελεσμάτων της Ομοσπονδιακής Μάθησης. Συνεπώς, όπως θα περιγράψουμε και στη συνέχεια, η εκτέλεση της προσομοίωσης θα ακολουθήσει δύο φάσεις: η πρώτη αφορά την αντιστοίχιση των κόμβων με τους εξυπηρετητές, και αφού αυτή ολοκληρωθεί περνάμε στην δεύτερη φάση, αυτή της Ομοσπονδιακής Μάθησης, όπου κάθε εξυπηρετητής θα επιχειρήσει να εκπαιδεύσει το μοντέλο του με την βοήθεια των κόμβων που του ανατέθηκαν.

2.1 Προσομοίωση

Η προσομοίωση αφορά κομμάτι ενός ευρύτερου δικτύου που προσπαθεί να εξασφαλίσει την δημόσια ασφάλεια σε περιπτώσεις φυσικών καταστροφών. Οι εξυπηρετητές, θέλοντας να μάθουν να αναγνωρίζουν έγκαιρα κινδύνους για τους πολίτες, προσπαθούν να εκμαιεύσουν πληροφορία από κόμβους που έχουν βρεθεί κοντά σε τέτοιες καταστροφές. Ο όρος ”κόμβος” είναι ένας ευρύτερος όρος που αναθέτουμε είτε σε κινητά τηλέφωνα πολιτών, είτε κάμερες ασφαλείας καταστημάτων, είτε στιγμιότυπα από ειδησεογραφική κάλυψη κ.α., που διαθέτουν φωτογραφίες από την εκάστοτε φυσική καταστροφή. Στην δική μας περίπτωση, μας αφορούν φυσικές καταστροφές φωτιών, πλημμυρών και σεισμών. Συνεπώς στόχος του δικτύου μας είναι για παράδειγμα, να εντοπίζει έγκαιρα κάποια φωτιά ή πλημμύρα και να ειδοποιεί τις πυροσβεστικές δυνάμεις, αλλά και τους κοντινούς σε αυτή πολίτες για να τους προειδοποιήσει και να τους καθοδηγήσει σε ασφαλή περιοχή. Αντίστοιχα σε περιπτώσεις σεισμών, να εντοπίζει κτίρια που έχουν υποστεί σοβαρές ζημιές και να ειδοποιεί για την άμεση εκκένωσή τους και την απομάκρυνση των πολιτών από αυτά.

Η προσομοίωση μας ακολουθεί το εξής σενάριο. Έχουμε 3 εξυπηρετητές όπου ο καθένας ε-

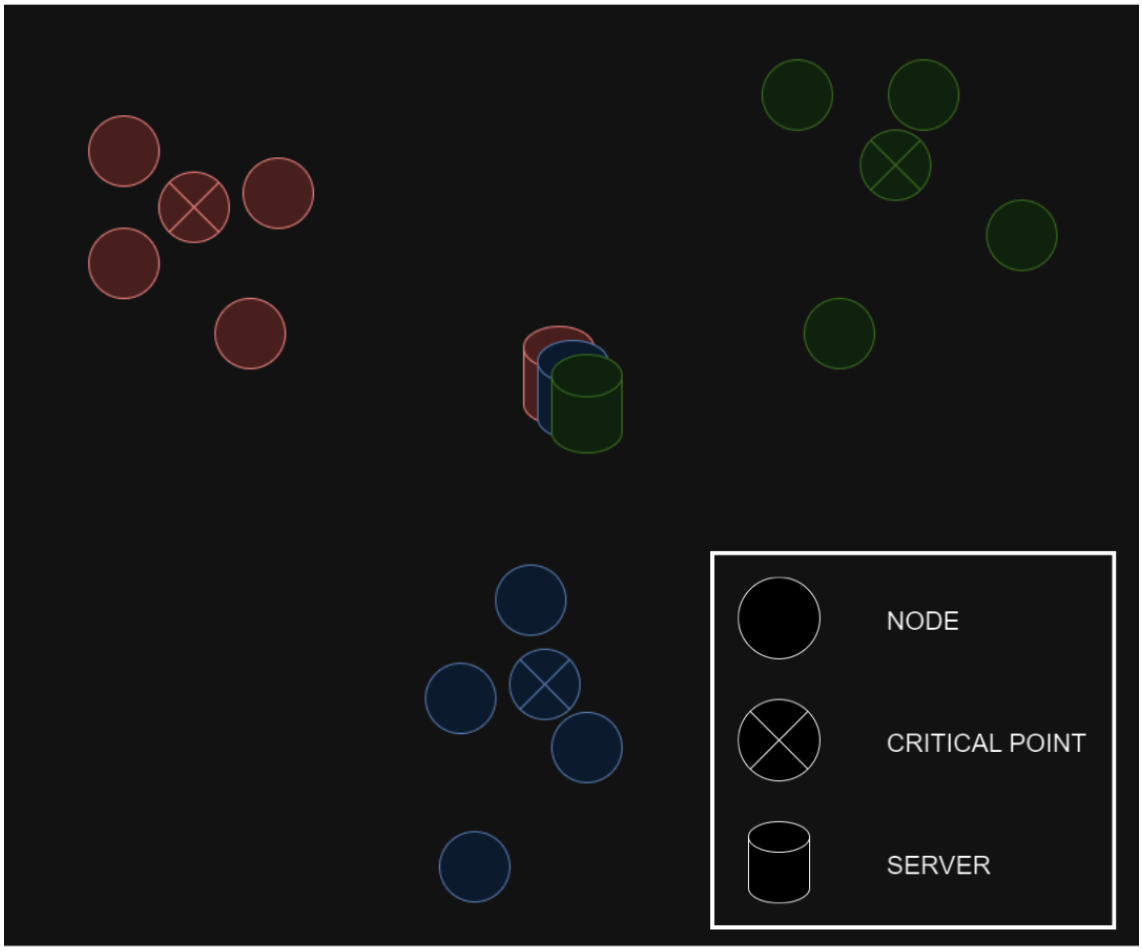
πιθυμεί να εκπαιδεύσει ένα μοντέλο αναγνώρισης - ταξινόμησης εικόνας. Ο πρώτος προσπαθεί να αναγνωρίσει εικόνες φωτιάς, ο δεύτερος πλημμυρών και ο τρίτος σεισμών. Στο οικοσύστημα μας έχουμε και K κρίσιμα σημεία, τα οποία το καθένα αφορά μια από τις προαναφερθείσες φυσικές καταστροφές. Στο πλαίσιο της εργασίας αυτής χρησιμοποιήθηκε $K = 3$, δηλαδή ένα σημείο για κάθε φυσική καταστροφή. Επιπλέον, γύρω από αυτά τα σημεία, έχουμε N κόμβους, οι οποίοι διαθέτουν φωτογραφίες από φυσικές καταστροφές, αλλά και από την καθημερινή τους χρήση, τις οποίες θα χρησιμοποιήσουν για να συμμετέχουν στην Ομοσπονδιακή Μάθηση που θα ακολουθήσει.

2.1.1 Περιγραφή

Στο πλαίσιο που περιγράψαμε παραπάνω θα διακρίνουμε 3 ξεχωριστές περιπτώσεις, όσον αφορά την περιοχή στην οποία τοποθετείται το δίκτυό μας. Έτσι διακρίνουμε σε Αστικές Περιοχές, Μικροαστικές Περιοχές και Αγροτικές Περιοχές και στη συνέχεια θα περιγράψουμε και αναλυτικά την διαφορά τους στην υλοποίηση.

Ξεκινώντας από την τοπολογία του συστήματός μας, τοποθετούμε αρχικά τους εξυπηρετητές μας στο σημείο (0,0,0), στο κέντρο του οικοσυστήματός μας. Κάθε εξυπηρετητής διαθέτει $\lceil \frac{N}{3} \rceil$ χρηματικά αποθέματα, με τα οποία μπορεί να προσελκύσει σε αυτόν κόμβους. Επιπλέον, θέτουμε ένα ανώτατο όριο κόμβων για κάθε εξυπηρετητή. Έτσι, κάθε εξυπηρετητής μπορεί να χτίσει ένα συνασπισμό το πολύ $\lceil \frac{N}{3} \rceil$ κόμβων. Μπορεί, λοιπόν, να χρηματοδοτήσει το πολύ το $\frac{1}{3}$ των κόμβων, χαρακτηριστικό που μας βοηθά στην διατήρηση της ισορροπίας μεταξύ των εξυπηρετητών. Έπειτα, σε έναν κύβο ακμής μήκους 2, γύρω από το (0,0,0) επιλέγουμε 3 σημεία, ένα για κάθε φυσική καταστροφή. Σε αυτά θεωρούμε πως έχει συμβεί η εκάστοτε φυσική καταστροφή και άρα κόμβοι γύρω από αυτά θα έχουν χρήσιμη πληροφορία για τους εξυπηρετητές μας. Εξασφαλίζουμε επίσης πως τα σημεία δεν είναι πολύ κοντά στους εξυπηρετητές. Σε μια τέτοια περίπτωση, όπως θα δούμε και στην διαδικασία της αντιστοίχισης, οι κόμβοι γύρω από αυτό θα παρουσίαζαν πολύ μεγαλύτερη χρησιμότητα στο σύστημα, απλώς επειδή βρίσκονται κοντά στους εξυπηρετητές και είναι "φθηνή" η επικοινωνία με αυτούς. Έτσι, για να διασφαλίσουμε μια ισορροπία ορίζουμε ως ελάχιστη απόσταση από τους εξυπηρετητές $d_{min} = 0.3$. Επιπλέον, για ρεαλιστικούς κυρίως λόγους, ορίζουμε ως ελάχιστη απόσταση μεταξύ δύο κρίσιμων σημείων ίση με $d_{min} = 0.8$.

Στη συνέχεια, μας απομένει να τοποθετήσουμε τους κόμβους μας γύρω από τα κρίσιμα σημεία. Η λογική που ακολουθούμε εδώ είναι η εξής: ανάλογα με την περιοχή που βρισκόμαστε (Αστική, Προαστιακή, Αγροτική) οι κόμβοι είναι λιγότερο ή περισσότερο αραιοί γύρω από το κάθε κρίσιμο σημείο. Συνεπώς, θέτουμε 3 όρια: $rural\_limit = 12, suburban\_limit = 21$ και $urban\_limit = 30$. Έτσι, για τις αγροτικές περιοχές όταν έχουμε πάνω από 12 κόμβους, αρχίζουμε να τοποθετούμε τους υπόλοιπους κόμβους πιο αραιά. Αντίστοιχα, το όριο για τις μικροαστικές περιοχές είναι 21 και για τις αστικές 30. Στις προσομοιώσεις μας, το μεγαλύτερο N που θα χρησιμοποιήσουμε είναι το $N = 30$. Επιπλέον, για δική μας διευκόλυνση ο κόμβος με διακριτικό id ανατίθεται γύρω από το κρίσιμο σημείο $id \mod 3$, και όσο μεγαλύτερο το id τόσο πιο μακριά είναι από το κρίσιμο σημείο. Άρα οι τρεις πρώτοι κόμβους είναι πολύ κοντά στα κρίσιμα σημεία τους, οι τρεις επόμενοι λίγο πιο μακριά κ.ο.κ. Όπως αναφέραμε, όταν για κάθε μία από τις διαφορετι-

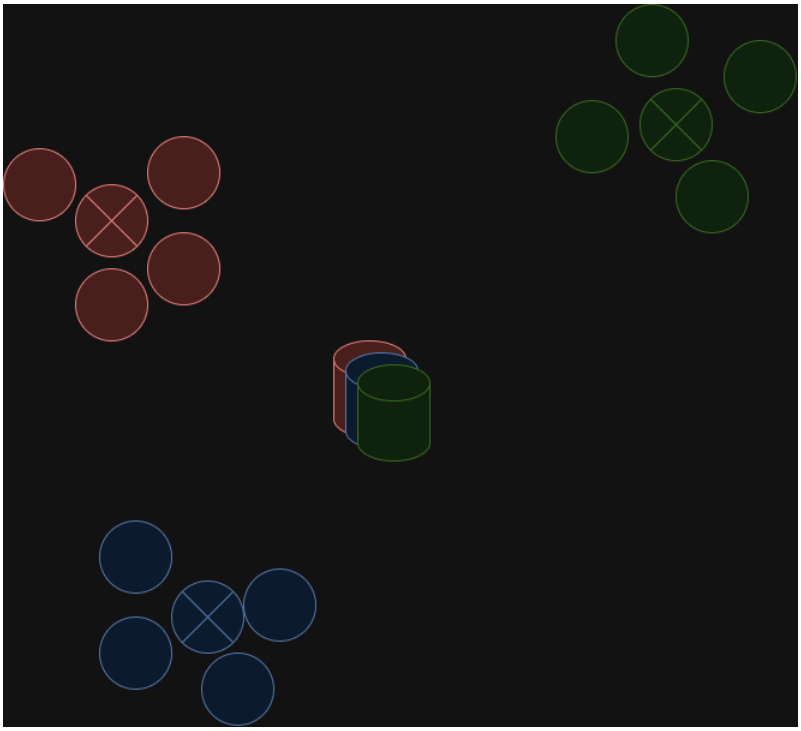


Σχήμα 2.1: Παράδειγμα Τοπολογίας Κόμβων και Εξυπηρετητών (Κόκκινο - Φωτιά, Μπλε - Πλημμύρα, Πράσινο - Σεισμός)

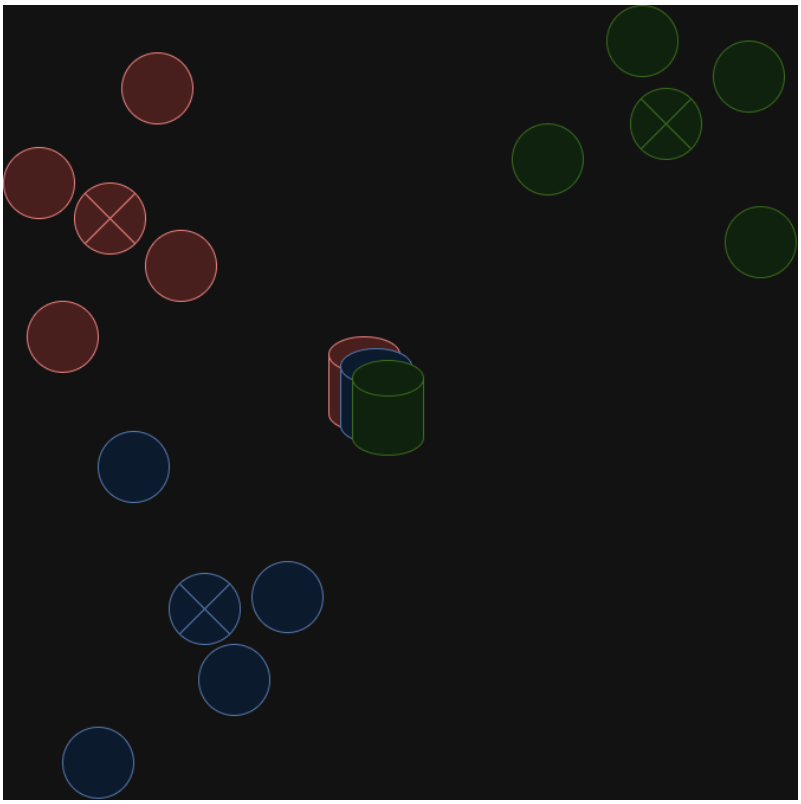
κές περιοχές ξεπεράσουμε το αντίστοιχο όριο, αρχίζουμε να προσθέτουμε πιο αραιούς-μακρινούς κόμβους. Με τον τρόπο αυτό μοντελοποιούμε το γεγονός πως σε περιοχές που βρίσκονται σε προάστια ή στην εξοχή, οι γειτονικοί στο κρίσιμο σημείο κόμβοι είναι λιγότεροι, αλλά είναι πιθανό να υπάρχουν και άλλοι, όμως πιο απομακρυσμένοι, κόμβοι. Σε κάθε περίπτωση, ολοκληρώνοντας την τοπολογία μας καταλήγουμε σε 3 κρίσιμα σημεία γύρω από τους εξυπηρετητές μας, όπου το κάθε ένα έχει γύρω του κόμβους. Ανάλογα την περιοχή όπου διατίθεται το δίκτυό μας, οι κόμβοι αυτοί είναι λιγότερο ή περισσότερο αραιοί. Είναι σημαντικό να επισημάνουμε προφανώς, πως όσο πιο κοντά είναι ένας κόμβος σε ένα κρίσιμο σημείο, τόσο πιο αξιόπιστος είναι για την πληροφορία που διαθέτει για αυτό, σημαντικό χαρακτηριστικό όπως θα δούμε και στη συνέχεια για την αντιστοίχιση κόμβων-εξυπηρετητών. Τέλος, σημειώνουμε πως ο κάθε κόμβος διαθέτει δύο παραμέτρους a_n και q_n, οι οποίες εκφράζουν τον συντελεστή αποτελεσματικής χωρητικότητας του επεξεργαστή του κόμβου και τον αριθμό κύκλων Κεντρικής Μονάδας Επεξεργασίας (ΚΜΕ)

που απαιτούνται για την εκτέλεση ενός δείγματος δεδομένων αντίστοιχα.

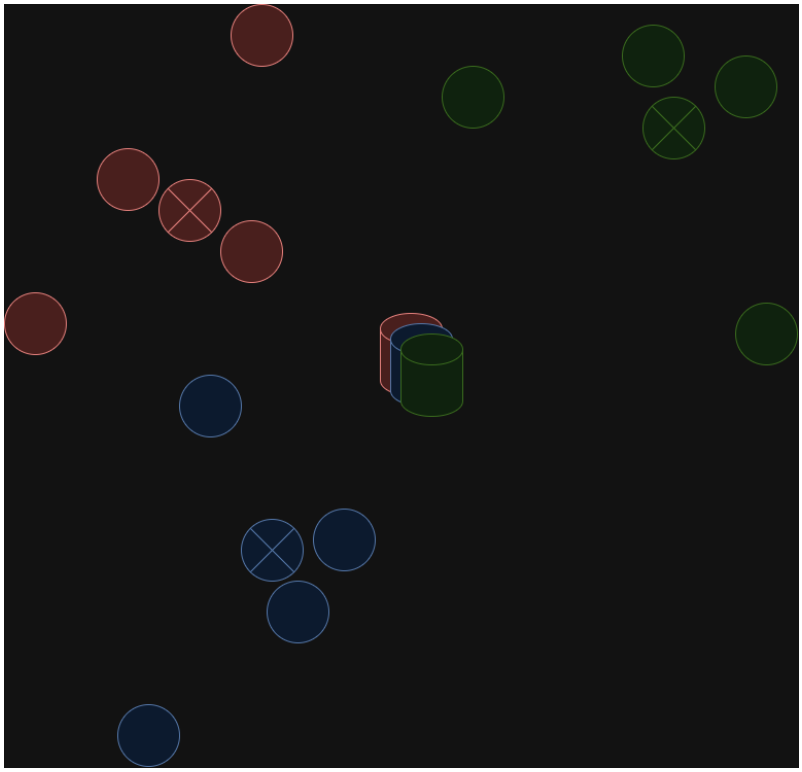
Παρακάτω παρουσιάζονται παραδείγματα των διαφορετικών τοπολογιών - σεναρίων:



Σχήμα 2.2: Αστική Περιοχή με 12 κόμβους



Σχήμα 2.3: Προαστιακή Περιοχή με 12 κόμβους



Σχήμα 2.4: Αγροτική Περιοχή με 12 κόμβους

2.1.2 Υλοποίηση

Για να συγκρίνουμε την επίδοση του αλγορίθμου μας σε διαφορετικές περιοχές (αστικό, προαστιακό ή υπαίθριο περιβάλλον) θα πρέπει να εξασφαλίσουμε μια δίκαιη και ορθή σύγκριση. Όπως αναφέραμε παραπάνω, έχουμε δύο είδη κόμβων για κάθε περιοχή, γειτονικοί - ”καλοί” και απομακρυσμένοι - ”κακοί”. Στην αστική περιοχή και οι 30 κόμβοι, που μπορούν να μπουν ως μέγιστο όριο, θεωρούνται ”καλοί” και άρα είναι σχετικά κοντά στο κρίσιμο σημείο τους. Αντίστοιχα, στην προαστιακή περιοχή μέχρι και τον 21ο κόμβο, οι κόμβοι θεωρούνται ”καλοί”, ενώ, σε περίπτωση που το N ξεπεράσει το 21, αρχίζουν να εισέρχονται στο σύστημά μας ”κακοί” κόμβοι, οι οποίοι τοποθετούνται τουλάχιστον 0.2 μακριά από το κρίσιμο σημείο τους. Τέλος, στην αγροτική περιοχή, μέχρι και τον 12ο κόμβο, οι κόμβοι θεωρούνται ”καλοί”, ενώ, σε περίπτωση που το N ξεπεράσει το 12, αρχίζουν να εισέρχονται στο σύστημά μας ”κακοί” κόμβοι, οι οποίοι τοποθετούνται τουλάχιστον 0.3 μακριά από το κρίσιμο σημείο τους. Συνεπώς, έστω πως έχουμε τον κόμβο i, τον οποίο θα πρέπει να δημιουργήσουμε. Αν το i είναι μικρότερο ή ίσο του 12 θα πρέπει όλες οι περιοχές να έχουν ίδιο κόμβο i και να μην ξαναδημιουργηθούν τυχαίοι κόμβοι i σε κάθε περιοχή. Με την ίδια λογική όταν το i είναι μικρότερο ή ίσο του 21 (αλλά μεγαλύτερο του 12), θα πρέπει οι κόμβοι i να είναι ίδιοι για την αστική και προαστιακή περιοχή, αλλά για την αγροτική περιοχή θα πρέπει να δημιουργηθεί ένας ”κακός” κόμβος i. Τέλος, για διευκόλυνση μας, υπολογίζουμε και αποθηκεύουμε τις αποστάσεις κάθε κόμβου από τους εξυπηρετητές μας και την σημασία κάθε κόμβου για τον κάθε εξυπηρετητή. Τέλος, όσον αφορά τις παραμέτρους a_n και q_n θέτουμε:

- $a_n = 2 \times 10^{(-28)} \times$ random.uniform(0.95, 1.05)

- $q_n = 20 \times$ random.uniform(0.95,1.05)

όπως αναφέρεται και σε αντίστοιχη προσομοίωση ([CDP23b]).

2.2 Αντιστοίχιση με Θεωρία Παιγνίων

Ως πρώτος μηχανισμός για την αντιστοίχιση κόμβων-εξυπηρετητών χρησιμοποιήθηκε η Θεωρία Παιγνίων. Στόχος ήταν να κατασκευαστεί ένα περιβάλλον με κανόνες, μέσα στο οποίο οι παίκτες-κόμβοι θα ανταγωνίζονται και θα ενεργούν για να επιτύχουν την καλύτερη δυνατή αμοιβή για εκείνους. Αντίστοιχα, οι εξυπηρετητές διαθέτοντας τους χρηματικούς πόρους τους στους κόμβους, προσπαθούν και αυτοί με τη σειρά τους να βελτιστοποιήσουν την δική τους απολαβή. Πιο αναλυτικά την διαδικασία θα περιγράψουμε παρακάτω.

2.2.1 Συνάρτηση Χρησιμότητας

Αρχικά θα πρέπει να εξηγήσουμε τον τρόπο με τον οποίο κάθε κόμβος, αλλά και εξυπηρετητής αντιλαμβάνεται το συμφέρον του στο δίκτυό μας. Έτσι χτίζουμε μία Συνάρτηση Χρησιμότητας. Κάθε κόμβος n έχει μια ποσότητα συλλεγμένων δεδομένων D_n [bits], και η σημασία των δεδομένων τους ορίζεται ως:

$$c_{n,k} = \frac{\min\limits_{\forall n} ||L_n - L_k||}{||L_n - L_k||} \tag{2.1}$$

όπου $L_n = (x_n, y_n, z_n)$ [απόσταση σε m] και $L_k = (x_k, y_k, z_k)$ [απόσταση σε m], με k το εκάστοτε κρίσιμο σημείο, αποτυπώνοντας πόσο κοντά στα κρίσιμα σημεία έχουν συλλεχθεί τα δεδομένα. Για κάθε έναν από τους τρεις εξυπηρετητές s υπολογίζουμε την σημασία των δεδομένων του κάθε κόμβου ως:

$$c_{n,s} = \max_{\forall k \in s} c_{n,k} \tag{2.2}$$

Όπως αναφέραμε, στην Ομοσπονδιακή Μάθηση, κάθε κόμβος n εκπαιδεύει ένα τοπικό μοντέλο βασισμένο στον εξυπηρετητή s που έχει επιλεγεί και αναφέρει το αποτέλεσμα της εκπαίδευσης σε αυτόν. Ο ρυθμός δεδομένων κάθε κόμβου n όταν εκφορτώνει το τοπικό μοντέλο στον εξυπηρετητή s δίνεται ως εξής:

$$R_{n,s} = B \log_2(1 + \frac{g_{n,s} P_{n,s}}{\sum\limits_{n' \in s} g_{n',s} P_{n',s} + I_0}) \quad [bps] \tag{2.3}$$

όπου $g_{n,s}$ δηλώνει το κέρδος καναλιού στη ζεύξη επικοινωνίας μεταξύ n και s, $P_{n,s}$ [W] είναι η ισχύς εκπομπής του κόμβου, B [Hz] είναι το εύρος ζώνης επικοινωνίας, και I_0 είναι ο λευκός προσθετικός θόρυβος (AWGN) μηδενικής μέσης τιμής. [CDP23b]

Η κατανάλωση ενέργειας ενός κόμβου n για να εκπαιδεύσει τοπικά το επιλεγμένο παγκόσμιο μοντέλο υπολογίζεται ως εξής:

$$E_n = \frac{a_n}{2} q_n D_n f_n^2 [J] \tag{2.4}$$

όπου a_n είναι ο συντελεστής χωρητικότητας του επεξεργαστή του κόμβου n, q_n είναι οι κύκλοι της Κεντρικής Μονάδα Επεξεργασίας (ΚΜΕ) που απαιτούνται για την εκτέλεση ενός δείγματος δεδομένων, και f_n [κύκλοι ΚΜΕ/δευτερόλεπτο] είναι η συχνότητα της ΚΜΕ της συσκευής του κόμβου n. [CDP23b]

Η κατανάλωση ενέργειας λόγω της μετάδοσης της ενημέρωσης του τοπικού μοντέλου υπολογίζεται ως εξής:

$$E_{n,s} = \frac{Z(\mathbf{w}n)Pn,s}{R_{n,s}}[J] \tag{2.5}$$

όπου $Z(\mathbf{w}_n)$ [bits] είναι τα δεδομένα των παραμέτρων του τοπικού μοντέλου $\mathbf{w}_n$ που μεταδίδονται για την ενημέρωση του κεντρικού μοντέλου του εξυπηρετητή s. [CDP23b]

Τέλος, ο κάθε κόμβος απολαμβάνει μια χρηματική απολαβή με βάση την σημασία των δεδομένων του, αλλά και με βάση τους υπόλοιπους κόμβους που ανήκουν στην ομοσπονδία του εξυπηρετητή:

$$Pnt_{n,s} = \frac{c_{n,s}P_s}{\sum\limits_{n' \in s} c_{n',s}} \tag{2.6}$$

Κάθε κόμβος βιώνει μια χρησιμότητα από τη συμμετοχή του στη διαδικασία αντιστοίχισης κόμβων-εξυπηρετητών που εξαρτάται από: (i) τα χαρακτηριστικά επικοινωνίας, δηλαδή τον επιτευχθέντα ρυθμό δεδομένων για την αναφορά του ενημερωμένου τοπικού μοντέλου $\mathbf{w}n^i$ στον εξυπηρετητή ($\hat{R}n,s$), (ii) το χρηματικό εισόδημα που λαμβάνεται από τον εξυπηρετητή για την παροχή κινήτρων στον κόμβο για την εκπαίδευση του τοπικού μοντέλου ($\hat{Pnt}_{n,s}$) και το σταθερό κίνητρο πρόσληψης που παρέχεται από τον εξυπηρετητή (γ), (iii) το όφελος της εκμετάλλευσης κρίσιμων δεδομένων για την εκπαίδευση του τοπικού μοντέλου ($\hat{d_n}$), και (iv) το ενεργειακό κόστος για την εκπαίδευση του τοπικού μοντέλου και την αποστολή του στον εξυπηρετητή ($\hat{E}n + \hat{E}n, s$). Έτσι, η χρησιμότητα του κόμβου ορίζεται ως εξής:

$$U_{n,s}(D_n) = \alpha\hat{R}_{n,s} + \beta\hat{Pnt}_{n,s} + \gamma + \delta\hat{d}_n - \epsilon(\hat{E}n + \hat{E}n, s) \tag{2.7}$$

όπου ο εξυπηρετητής s προσφέρει $Pnt_{n,s}$ [\$] ως χρηματικό κίνητρο στον κόμβο n για την εκπαίδευση του τοπικού μοντέλου, και $\alpha, \beta, \gamma, \delta, \epsilon \in \mathbb{R}^+$. Για να διασφαλιστεί ότι όλοι οι παράγοντες είναι της ίδιας τάξης μεγέθους, αποτυπώνοντας έτσι δίκαια την επίδρασή τους στη χρησιμότητα του κόμβου, στη χρησιμότητα του κόμβου (Εξίσωση 2.7) οι $\hat{R}n, s, \hat{Pnt}_{n,s}, \hat{E}n$, $\hat{E}n, s$ και $\hat{d_n}$ δίνονται από τις εξής κανονικοποιημένες εκφράσεις:

$$\hat{R}n, s = \frac{R_{n,s}}{\max\limits_{\forall n, \forall s} R_{n,s}}, \hat{Pnt}_{n,s} = \frac{c_{n,s}P_s}{(\sum\limits_{n' \in s} c_{n',s}) \max\limits_{\forall s} P_s}, \hat{d}n = \frac{\sum \forall k \in K c_{n,k}D_n}{\max\limits_{\forall n} \sum\limits_{\forall k \in K} c_{n,k}D_n}$$

$$\hat{E}n = \frac{E_n}{\max\limits_{\forall n} E_n}, \hat{E}n, s = \frac{En, s}{\max\limits_{\forall n, \forall s} E_{n,s}}$$

Από την άλλη πλευρά, κάθε εξυπηρετητής στοχεύει στη μεγιστοποίηση της χρησιμότητας που βιώνουν οι συνδεδεμένοι κόμβοι του, λαμβάνοντας όμως υπόψη το κόστος παροχής κινήτρων

πρόσληψης και τον ανταγωνισμό για την πρόσληψη από άλλους εξυπηρετητές εντός του δικτύου πολλαπλών μοντέλων Ομοσπονδιακής Μάθησης. Έτσι, η χρησιμότητα του ομοσπονδιακού εξυπηρετητή είναι:

$$U_s(P_s, \mathbf{P}_{-\mathbf{s}}) = \frac{\sum\limits_{\forall n \in \mathcal{N}s} Un, s - \zeta \hat{P}s^2}{\sum\limits_{\forall s' \neq s} \hat{P}_{s'}} \tag{2.8}$$

όπου $\zeta \in \mathbb{R}^+$, $\mathcal{N}s$ είναι το σύνολο των κόμβων που επιλέγουν τον εξυπηρετητή s, και $\mathbf{P}-\mathbf{s}$ είναι το διάνυσμα χρηματικών κινήτρων όλων των εξυπηρετητών εκτός από τον s. Σημειώνεται ότι ο κάθε εξυπηρετητής s έχει διαθέσει P_s χρηματικά κίνητρα τα οποία χρησιμοποιεί εξ' ολοκλήρου είτε για έναν είτε για N_s κόμβους. Προφανώς, οι κόμβοι μας βλέποντας έναν σχετικά άδειο εξυπηρετητή γνωρίζουν πως συμμετέχοντας στην ομοσπονδία του θα έχουν καλύτερες απολαβές. Βάσει του διαθέσιμου προϋπολογισμού πρόσληψης P_s, όπως αναφέραμε, κάθε εξυπηρετητής μπορεί να προσλάβει έναν μέγιστο αριθμό κόμβων N_s^{Max}, που στην περίπτωσή μας είναι το $\frac{1}{3}$ του πληθυσμού N.

2.2.2 Προσεγγιστική Αντιστοίχιση

Οι κόμβοι επιλέγουν στρατηγικά εξυπηρετητές για να προσφέρουν τις υπολογιστικές τους υπηρεσίες, με στόχο να μεγιστοποιήσουν τη χρησιμότητά τους. Οι ομοσπονδιακοί εξυπηρετητές επιδιώκουν να προσλάβουν κόμβους για να βοηθήσουν στην εκπαίδευση του παγκόσμιου μοντέλου, στρατηγικά βελτιστοποιώντας την ακρίβειά τους μέσω της πρόσληψης κόμβων. Αυτό παρουσιάζει ένα σενάριο αντιστοίχισης πολλών προς έναν, όπου πολλαπλοί κόμβοι αντιστοιχίζονται με έναν εξυπηρετητή και μπορεί να μελετηθεί βάσει της θεωρίας αντιστοίχισης.

Ορισμός 2.1. ***(Παιχνίδι Αντιστοίχισης)*** *Τα σύνολα των κόμβων $\mathcal{N}$ και των εξυπηρετητών $\mathcal{S}$ δεν έχουν καμία τομή. Μια αντιστοίχιση M είναι μία αντιστοιχία των στοιχείων του $\mathcal{N}$ στα στοιχεία του $\mathcal{S}$, που ικανοποιεί τις συνθήκες: $|M(n)| \leq 1, \forall n \in \mathcal{N}$, $|M(s)| \leq N_s^{Max}, \forall s \in \mathcal{S}$, $M(n) \in \mathcal{S}$ εάν και μόνο εάν $M(s) \in \mathcal{N}$, $n \in M(s) \Leftrightarrow M(n) = s$. Εάν $M(n) = \emptyset$, ο κόμβος n δεν αντιστοιχίζεται σε κανέναν εξυπηρετητή, ενώ εάν $M(s) = \emptyset$, τότε ο εξυπηρετητής s δεν επιλέγεται από κανέναν κόμβο.*

Η Εξίσωση 2.7 παρουσιάζει εξωτερικότητα (επιρροή μεγέθους και από άλλους κόμβους - $U_{n,s}$ εξαρτάται και από τις ενέργειες κάθε $n' \in N$) που προκύπτει από την επιλογή του εξυπηρετητή και από άλλους κόμβους, η οποία αποτυπώνεται στα μεγέθη του ρυθμού αποστολής δεδομένων και στις χρηματικές απολαβές, όπου οι κόμβοι ανταγωνίζονται για πόρους (εύρος ζώνης και χρηματικά κίνητρα). Επίσης, η Εξίσωση 2.8 περιλαμβάνει την εξωτερικότητα του διαθέσιμου προϋπολογισμού πρόσληψης άλλων εξυπηρετητών. Η Προσεγγιστική Αντιστοίχιση αγνοεί αυτές τις εξωτερικότητες για να εδραιώσει γρήγορα μια αρχική αντιστοίχιση μεταξύ κόμβων και εξυπηρετητών. Οι Εξισώσεις 2.7 και 2.8 αναδιαμορφώνονται αποκλείοντας τις εξωτερικότητες που προέρχονται από την επιλογή εξυπηρετητή από τους κόμβους, ως εξής:

$$\widetilde{U}_n(D_n) = \alpha \widetilde{\hat{R}}n, s + \beta \widetilde{\hat{P}nt}_{n,s} + \gamma + \delta \hat{d}_n - \epsilon(\hat{E}n + \hat{E}n, s) \tag{2.9}$$

$$\widetilde{R}n,s = B\log_2(1+\frac{g_{n,s}P_{n,s}}{g_{n,s}P_{n,s}+I_0})\,[bps],\quad \widetilde{\hat{R}}n,s = \frac{\widetilde{R}n,s}{\max\limits_{\forall n,\forall s}\widetilde{R}_{n,s}}$$

$$\widetilde{\hat{E}}n,s = \frac{Z(\mathbf{w}n)Pn,s}{\widetilde{\hat{R}}_{n,s}}\,[J],\quad \widetilde{\hat{Pn}t_{n,s}} = \frac{c_{n,s}P_s}{\max\limits_{\forall s}P_s}$$

$$\widetilde{U}s(P_s,\mathbf{P}{-}\mathbf{s}) = \sum_{\forall n\in N_s}\widetilde{U}_n - \zeta\hat{P}_s^2 \tag{2.10}$$

Ορισμός 2.2. ***(Σχέση Προτίμησης* $<$*)*** *Μια σχέση προτίμησης $<$ είναι μια πλήρης, αυτοπροτιμητική και μεταβατική δυαδική σχέση μεταξύ στοιχείων των συνόλων $\mathcal{N}$ και $\mathcal{S}$. Οι σχέσεις προτίμησης για έναν κόμβο (Εξίσωση 2.11) και έναν εξυπηρετητή (Εξίσωση 2.12) ορίζονται ως εξής:*

$$s >_n s' \iff \widetilde{U}_n(D_n) > \widetilde{U}n(D_n) \tag{2.11}$$

$$n >_s n' \iff \widetilde{U}s|N_s\cup n > \widetilde{U}s|N_s\cup n' \tag{2.12}$$

Algorithm 1 Αλγόριθμος Προσεγγιστικής Αντιστοίχισης

1: **Είσοδος:** $L_n, a_n, q_n, D_n, f_n, \mathbf{w}n\forall n\in\mathcal{N}, L_{k\forall k\in\mathcal{K}}, \alpha,\beta,\gamma,$
2: **Έξοδος:** Αποτελέσματα Αντιστοίχισης M
3: **Αρχικοποίηση:** $\mathcal{N}^* \leftarrow \mathcal{N}$: μη αντιστοιχισμένοι κόμβους, $\mathcal{S}_n \leftarrow \{s|\forall s\in\mathcal{S}\}, \forall n\in\mathcal{N}$: διαθέσιμοι εξυπηρετητές για κάθε κόμβου
4: **while** $\mathcal{N}^*\neq\emptyset$ και $\mathcal{S}_n\neq\emptyset, \exists n\in\mathcal{N}^*$ **do**
5: **for** $n\in\mathcal{N}^*$ **do**
6: Ο κόμβος n επιλέγει τον πιο ευνοϊκό εξυπηρετητή μεταξύ των εναλλακτικών και στέλνει πρόσκληση αντιστοίχισης βάσει της Εξίσωσης 2.11.
7: **end for**
8: **for** $s\in\mathcal{S}$ **do**
9: **if** $(N_s\leq N_s^{\max})\wedge(s$ έλαβε πρόσκληση αντιστοίχισης$)$ **then**
10: Ο εξυπηρετητής s επιλέγει τους πιο ευνοϊκούς κόμβους για αντιστοίχιση από αυτούς που έστειλαν πρόσκληση αντιστοίχισης βάσει της Εξίσωσης 2.12.
11: Διαγράφει τον s από τους εναλλακτικούς εξυπηρετητές των κόμβων που έστειλαν πρόσκληση αντιστοίχισης αλλά δεν έγιναν δεκτοί.
12: **end if**
13: **end for**
14: **end while**

Βάσει των Ορισμών 2.1 και 2.2, ο Αλγόριθμος 1 περιγράφει τον Αλγόριθμο Προσεγγιστικής Αντιστοίχισης. Αυτός ο αλγόριθμος στοχεύει να φτάσει σε μια εκτιμώμενη αντιστοίχιση μεταξύ των κόμβων και των ομοσπονδιακών εξυπηρετητών γρήγορα, δίνοντας προτεραιότητα στη μεγιστοποίηση της χρησιμότητας και για τα δύο μέρη χωρίς να λαμβάνει υπόψη τις εξωτερικότητες του συστήματος στις διαδικασίες λήψης αποφάσεων τους. Η βελτίωση του αποτελέσματος του Αλγορίθμου Προσεγγιστικής Αντιστοίχισης παρουσιάζεται στη συνέχεια μέσω της ανάπτυξης της

Ακριβούς Αντιστοίχισης, η οποία αντιμετωπίζει τις εξωτερικότητες που σχετίζονται με τους κόμβους και τους εξυπηρετητές.

2.2.3 Ακριβής Αντιστοίχιση

Λόγω της ύπαρξης εξωτερικοτήτων στη διαδικασία αντιστοίχισης των κόμβων και εξυπηρετητών, ο αλγόριθμος Προσεγγιστικής Αντιστοίχισης διασφαλίζει ένα γρήγορο, αλλά όχι βέλτιστο, αποτέλεσμα αντιστοίχισης εντός του παιχνιδιού αντιστοίχισης. Έτσι, εισάγουμε ένα παιχνίδι συμμαχιών για να βελτιώσουμε το αποτέλεσμα της αντιστοίχισης, εκμεταλλευόμενοι την έξοδο του αλγορίθμου Προσεγγιστικής Αντιστοίχισης και αντιμετωπίζοντας κατάλληλα τον αντίκτυπο των εξωτερικοτήτων.

Ορισμός 2.3. ***(Παιχνίδι Συμμαχίας)*** *Θεωρούμε ένα παιχνίδι συμμαχίας $(\mathcal{N}, \mathcal{S}, U_s)$, όπου $\mathcal{N}$ και $\mathcal{S}$ είναι τα σύνολα των κόμβων και των ομοσπονδιακών εξυπηρετητών, αντίστοιχα. Για κάθε εξυπηρετητή s, υπάρχει μια συμμαχία που επιλέγεται από μια ξεχωριστή ομάδα κόμβων $\mathcal{N}_s = 1, \ldots, n, \ldots, N_s$. Κάθε μεμονωμένος κόμβος επιλέγει μόνο έναν εξυπηρετητή. Η χρησιμότητα U_s του εξυπηρετητή s ορίζεται στην Εξίσωση 2.10.*

Μέσα στο πλαίσιο ενός παιχνιδιού συμμαχίας, ο στόχος μας είναι να βελτιστοποιήσουμε συλλογικά τις χρησιμότητες τόσο των ομοσπονδιακών εξυπηρετητών όσο και των κόμβων. Αυτό επιτυγχάνεται μέσω της διαμόρφωσης λεπτομερών *συνθηκών μετάβασης* που καθοδηγούν στρατηγικά τους κόμβους είτε να εξέλθουν είτε να ενταχθούν σε μια συμμαχία.

Ορισμός 2.4. ***(Συνθήκες Μετάβασης)*** *Το παιχνίδι συμμαχίας περιλαμβάνει διάφορους τύπους Συνθηκών Μετάβασης (TC).*
TC 1: *Για έναν κόμβου n που δεν έχει επιλέξει κάποια συμμαχία ακόμα, ο n εισέρχεται στην συμμαχία του s αν $\exists s^* = \underset{s^* \in \mathcal{S}}{\text{argmax}}\{U_{s^*}(\mathcal{N}_{s^*} \cup \{n\}) - U_{s^*}(\mathcal{N}_{s^*}) \mid U_{s^*}(\mathcal{N}_{s^*} \cup \{n\}) - U_{s^*}(\mathcal{N}_{s^*}) > 0\}$.*
TC 2: *Ο κόμβος $n \in \mathcal{N}_s, n$ φεύγει από τον εξυπηρετητή s αν $U_s(\mathcal{N}_s \setminus \{n\}) > U_s(\mathcal{N}_s)$, και άρα, $M = \{M \setminus \{\mathcal{N}_s\}\} \cup \{\mathcal{N}_s \setminus \{n\}\}$.*
TC 3: *Ο κόμβος $n \in \mathcal{N}_s$, αποχωρεί από την συμμαχία του εξυπηρετητή του s και επιλέγει την συμμαχία του εξυπηρετητή $s' \neq s$ αν $U_s(\mathcal{N}_s \setminus \{n\}) + U_{s'}(\mathcal{N}_{s'} \cup \{n\}) > U_s(\mathcal{N}_s) + U_{s'}(\mathcal{N}_{s'})$, και άρα, $M = \{M \setminus \{\mathcal{N}_s, \mathcal{N}_{s'}\}\} \cup \{\mathcal{N}_s \setminus \{n\}\} \cup \{\mathcal{N}_{s'} \cup \{n\}\}$.*
TC 4: *Ο κόμβος $n \in \mathcal{N}_s$ και ο κόμβος $n' \in \mathcal{N}_{s'}, n \neq n'$, n and n' αλλάζουν συμμαχίες μεταξύ τους αν $U_s((\mathcal{N}_s \setminus \{n\}) \cup \{n'\}) + U_{s'}((\mathcal{N}_{s'} \setminus \{n'\}) \cup \{n\}) > U_s(\mathcal{N}_s) + U_{s'}(\mathcal{N}_{s'})$, και άρα, $M = \{M \setminus \{\mathcal{N}_s, \mathcal{N}_{s'}\}\} \cup \{(\mathcal{N}_s \setminus \{n\}) \cup \{n'\}\} \cup \{(\mathcal{N}_{s'} \setminus \{n'\}) \cup \{n\}\}$.*

Βάσει των συνθηκών μετάβασης που περιγράφονται στον Ορισμό 2.4, έχουμε αναπτύξει τον Αλγόριθμο Ακριβούς Αντιστοίχισης 2. Ο Αλγόριθμος Ακριβούς Αντιστοίχισης έχει σχεδιαστεί για να διευκολύνει την καθιέρωση σταθερών συμμαχιών μεταξύ κόμβων και εξυπηρετητών και θα αποδείξουμε την ιδιότητά του αυτή αφού παρουσιάσουμε τον αλγόριθμο.

Nash-Ατομικά Σταθερός Χωρισμός κόμβων: Ένας χωρισμός των κόμβων σε συμμαχίες με ομοσπονδιακούς εξυπηρετητές, που σημειώνεται ως M^*, θεωρείται Nash-Ατομικά σταθερός αν

Algorithm 2 Αλγόριθμος Ακριβούς Αντιστοίχισης

Είσοδος: M_{initial} από τον Αλγόριθμο Προσεγγιστικής Αντιστοίχισης, και ίδιες εισόδους με τον Αλγόριθμο Προσεγγιστικής Αντιστοίχισης
Έξοδος: Βέλτιστος Διαμοιρασμός Συνασπισμών M^*
repeat
  Τυχαία επιλογή κόμβου n και συνασπισμού εξυπηρετητή s
  if n δεν ανήκει σε κανένα συνασπισμό **then**
    $s^* = \underset{s^* \in M}{\text{argmax}}\{(U_{s^*}(\mathcal{N}_{s^*} \cup \{n\}) - U_{s^*}(\mathcal{N}_{s^*}) | U_{s^*}(\mathcal{N}_{s^*} \cup \{n\}) - U_{s^*}(\mathcal{N}_{s^*}) > 0) \wedge (N_s \leq N_s^{\max})\}$
    $M = \{M \setminus \{n\}\} \cup \{\mathcal{N}_s \cup \{n\}\}$
  else
    Διαλέγουμε τυχαία $s', s' \neq s$
    if $N_s \leq N_s^{\max}$ **then**
      if $U_s(\mathcal{N}_s \setminus \{n\}) + U_{s'}(\mathcal{N}_{s'} \cup \{n\}) > U_s(\mathcal{N}_s) + U_{s'}(\mathcal{N}_{s'})$ **then**
        $M = \{M \setminus \{\mathcal{N}_s, \mathcal{N}_{s'}\}\} \cup \{\mathcal{N}_s \setminus \{n\}\} \cup \{\mathcal{N}_{s'} \cup \{n\}\}$
      end if
    else
      Διαλέγουμε τυχαία κόμβου n' από τον συνασπισμό του εξυπηρετητή s'
      if $U_s((\mathcal{N}_s \setminus \{n\}) \cup \{n'\}) + U_{s'}((\mathcal{N}_{s'} \setminus \{n'\}) \cup \{n\}) > U_s(\mathcal{N}_s) + U_{s'}(\mathcal{N}_{s'})$ **then**
        $M = \{M \setminus \{\mathcal{N}_s, \mathcal{N}_{s'}\}\} \cup \{(\mathcal{N}_s \setminus \{n\}) \cup \{n'\}\} \cup \{(\mathcal{N}_{s'} \setminus \{n'\}) \cup \{n\}\}$
      end if
    end if
  end if
  Ενημερώνουμε τους s και n πως πλέον ο n ανήκει στον συνασπισμό του s
  if $U_s(\mathcal{N}_s \setminus \{n\}) > U_s(\mathcal{N}_s)$ **then**
    $M = \{M \setminus \{\mathcal{N}_s\}\} \cup \{\mathcal{N}_s \setminus \{n\}\}$
  end if
until να μην έχουμε αλλαγές στην κατάσταση των κόμβων

κανένας μεμονωμένος κόμβος δεν μπορεί να αυξήσει τη χρησιμότητά του αλλάζοντας εξυπηρετητές ([OR94]). Ο Αλγόριθμος Ακριβούς Αντιστοίχισης είναι σχεδιασμένος να εγγυάται τουλάχιστον έναν Νας-Ατομικά σταθερό χωρισμό M^*.

Αρχικά, υποθέτουμε ότι το M^* όπως καθορίζεται από τον Αλγόριθμο Ακριβούς Αντιστοίχισης δεν είναι Νας-Ατομικά σταθερό. Τότε, τουλάχιστον μία από τις ακόλουθες συνθήκες πρέπει να ισχύει:

1. $\exists n \notin \mathcal{N}_s, \forall s \in \mathcal{S}, \exists s^* = \underset{s^* \in \mathcal{S}}{\text{argmax}}\{U_{s^*}(\mathcal{N}_{s^*} \cup \{n\}) - U_{s^*}(\mathcal{N}_{s^*}) | U_{s^*}(\mathcal{N}_{s^*} \cup \{n\}) - U_{s^*}(\mathcal{N}_{s^*}) > 0\}$
2. $\exists n \in \mathcal{N}_s$, που ικανοποιεί $U_s(\mathcal{N}_s \setminus \{n\}) > U_s(\mathcal{N}_s)$
3. $\exists n \in \mathcal{N}_s, \exists s', s \neq s'$, που ικανοποιεί $U_s(\mathcal{N}_s \setminus \{n\}) + U_{s'}(\mathcal{N}_{s'} \cup \{n\}) > U_s(\mathcal{N}_s) + U_{s'}(\mathcal{N}_{s'})$

4. $\exists n \in \mathcal{N}_s$, $\exists n' \in \mathcal{N}_{s'}$, and $s \neq s'$, που ικανοποιεί $U_s((\mathcal{N}_s \setminus \{n\}) \cup \{n'\}) + U_{s'}((\mathcal{N}_{s'} \setminus \{n'\}) \cup \{n\}) > U_s(\mathcal{N}_s) + U_{s'}(\mathcal{N}_{s'})$

Ωστόσο, στον Αλγόριθμο Ακριβούς Αντιστοίχισης, αν ισχύει οποιαδήποτε από τις παραπάνω συνθήκες, οι κόμβοι θα ακολουθήσουν τις αντίστοιχες συνθήκες μετάβασης που περιγράφονται στον Ορισμό 2.4. Έτσι, ο χωρισμός των κόμβων δεν μπορεί να είναι τελικός, καθώς θα συνεχίσουν να τροποποιούν τους εξυπηρετητές με τους οποίους συνδέονται ακολουθώντας αυτές τις συνθήκες μετάβασης. Αυτή η αντίφαση αμφισβητεί την αρχική μας υπόθεση, οδηγώντας στο συμπέρασμα ότι ο Αλγόριθμος Ακριβούς Αντιστοίχισης συγκλίνει σε μια Nash-Ατομικά σταθερή διαμόρφωση συμμαχιών.

2.2.4 Υλοποίηση

Στο πλαίσιο της υλοποίησης των παραπάνω αλγορίθμων, για την μελέτη της βέλτιστης αντιστοίχισης, τρέχουμε τον παραπάνω αλγόριθμο για ορισμένο πλήθος επαναλήψεων συλλέγοντας πληροφορία για τις προτιμήσεις και τη συμπεριφορά του κάθε κόμβου. Έτσι ανάλογα με την επιλογή και ενέργεια του τυχαίου κόμβου που επιλέγεται σε κάθε επανάληψη , αυτός παίρνοντας ανατροφοδότηση, συλλέγει μια αμοιβή από το περιβάλλον του. Συνεπώς, με την ολοκλήρωση της διαδικασίας, κάθε κόμβος έχει συλλέξει συνολική πληροφορία για τις επιλογές που διαθέτει και άρα πλέον γνωρίζει τις προτιμότερες επιλογές του. Έτσι, οι κόμβοι, σεβόμενοι το μέγιστο πλήθος κόμβων που μπορεί να υποστηρίξει κάθε εξυπηρετητής, επιλέγουν τον καλύτερο για αυτούς εξυπηρετητή.

2.3 Ομοσπονδιακή Μάθηση

Με την ολοκλήρωση της αντιστοίχισης των κόμβων με τους εξυπηρετητές, σειρά έχει η διαδικασία της Ομοσπονδιακής Μάθησης για την επίτευξη της εκπαίδευσης των μοντέλων. Εξάλλου, μας αφορά η καλή λειτουργία της αντιστοίχισης ώστε να μπορέσουμε να επιτύχουμε καλύτερα αποτελέσματα στις αποδόσεις των μοντέλων των εξυπηρετητών, εκμεταλλευόμενοι τα δεδομένα των κόμβων με βάση τα χαρακτηριστικά του καθενός. Ας περιγράψουμε σύντομα την γενική διαδικασία της Ομοσπονδιακής Μάθησης μεταξύ κόμβων και ενός εξυπηρετητή.

Η διαδικασία ξεκινά με έναν κεντρικό εξυπηρετητή να αρχικοποιεί ένα παγκόσμιο μοντέλο, το οποίο διανέμεται σε όλους τους συμμετέχοντες κόμβους. Κάθε κόμβος εκπαιδεύει στη συνέχεια το μοντέλο τοπικά χρησιμοποιώντας το δικό του σύνολο δεδομένων, ενημερώνοντας τις παραμέτρους του μοντέλου μέσω αρκετών επαναλήψεων. Μετά την τοπική εκπαίδευση, οι κόμβοι στέλνουν τα ενημερωμένα βάρη των μοντέλων τους πίσω στον εξυπηρετητή, ο οποίος συγκεντρώνει αυτές τις ενημερώσεις για να σχηματίσει ένα νέο κεντρικό μοντέλο. Αφού ο εξυπηρετητής ενημερώσει το κεντρικό μοντέλο με βάση τα βάρη που έλαβε από τους κόμβους, το αναδιανέμει στη συνέχεια πίσω σε αυτούς, και η διαδικασία επαναλαμβάνεται για πολλούς γύρους μέχρι να επιτευχθεί η επιθυμητή ακρίβεια του μοντέλου. Αυτή η μέθοδος διασφαλίζει ότι τα ευαίσθητα δεδομένα δεν φεύγουν ποτέ από τις τοπικές συσκευές, μειώνοντας τον κίνδυνο παραβιάσεων δεδομένων και αξιοποιώντας τους τοπικούς υπολογιστικούς πόρους των κόμβων για κατανεμημένη εκπαίδευση

του μοντέλου. Ωστόσο, η Ομοσπονδιακή Μάθηση αντιμετωπίζει προκλήσεις όπως ετερογενείς κατανομές δεδομένων και μεταβλητότητα συστήματος μεταξύ των κόμβων.

2.3.1 Περιγραφή

Κάθε ένας από τους εξυπηρετητές με τον συνασπισμό του, λοιπόν, ακολουθεί πιο αναλυτικά τις παρακάτω δύο φάσεις:

Τοπική Εκπαίδευση και Ενημέρωση Μοντέλου: Με την έναρξη της διαδικασίας της Ομοσπονδιακής Μάθησης, κάθε κόμβος n ανακτά το συγκεντρωτικό μοντέλο από τον επιλεγμένο εξυπηρετητή. Στη συνέχεια, το τοπικό μοντέλο υποβάλλεται σε επαναληπτική εκπαίδευση χρησιμοποιώντας το αντίστοιχο τοπικό σύνολο δεδομένων D_n. Η ενημέρωση του τοπικού μοντέλου σε κάθε κόμβο διαρκεί για έναν προκαθορισμένο αριθμό I επαναλήψεων πριν προχωρήσει στη επόμενη φάση. Ορίζοντας i ως την επανάληψη της ενημέρωσης του τοπικού μοντέλου στη συσκευή του κόμβου, ο κύριος στόχος για κάθε κόμβο n στην i-οστή τοπική επανάληψη είναι να ελαχιστοποιήσει τη συνάρτηση εμπειρικής απώλειας $F_n(\mathbf{w}_n^i)$:

$$\mathbf{w}_n^i = \arg\min_{\mathbf{w}_n^i}\{F_n(\mathbf{w}_n^i) = \frac{1}{D_n}\sum_{\forall j \in D_n} f_j(\mathbf{w}_n^i)\} \tag{2.13}$$

όπου $\mathbf{w}_n^i$ τα τοπικά βάρη του κόμβου n στην i-οστή τοπική επανάληψη και $f_j(\mathbf{w}_n^i)$ η συνάρτηση απώλειας του δείγματος j.

Η διαδικασία επαναληπτικής ενημέρωσης εντός κάθε κόμβου μπορεί να εκτελεστεί μέσω της εφαρμογής καθόδου στοχαστικής κλίσης σε mini-batches που δειγματοληπτούνται τυχαία από το τοπικό σύνολο δεδομένων:

$$\mathbf{w}_n^i = \mathbf{w}_n^{i-1} - \lambda \nabla F_n(D_n \mathbf{w}_n^{i-1}) \tag{2.14}$$

όπου $\lambda \in (0, 1)$ είναι ο ρυθμός εκμάθησης της εκπαίδευσης.

Συγκέντρωση Παγκόσμιου Μοντέλου: Μετά από I επαναλήψεις, κάθε εξυπηρετητής συγκεντρώνει τις τοπικές ενημερώσεις από τους επιλεγμένους κόμβους και αντικαθιστά το κεντρικό μοντέλο με το μέσο μοντέλο, ως ο κατά βάρος μέσος όρος των παραμέτρων του μοντέλου κάθε κόμβου. Τα βάρη προκύπτουν ως την κανονικοποιημένη σημασία του κάθε κόμβου για τον εξυπηρετητή στον οποίο ανήκει. Έτσι προκύπτει:

$$\mathbf{w}_s = \hat{g}_n \mathbf{w}_n^i, \quad \hat{g}_n = \frac{g_n}{\sum_{\forall n \in \mathcal{N}_s} g_n}, \quad g_n = \frac{c_{n,s}}{\sum_{\forall n \in N_s} c_{n,s}} \tag{2.15}$$

Στη συνέχεια, το τοπικό μοντέλο κάθε κόμβου $\mathbf{w}_n^i$ ενημερώνεται με το κεντρικό μοντέλο $\mathbf{w}_s$ από τον εξυπηρετητή με τον οποίο είναι συνδεδεμένος ο κόμβος. Η συγκέντρωση των βαρών των κόμβων στο κεντρικό μοντέλο επαναλαμβάνεται για κ επαναλήψεις μέχρι να επιτευχθεί η επιθυμητή ακρίβεια.

2.3.2 Σύνολο δεδομένων

Όσον αφορά τα δεδομένα των κόμβων, αναφέραμε πως κάθε ένας διαθέτει στο σύνολο δεδομένων του εικόνες σχετικές με τις κοντινές του φυσικές καταστροφές, αλλά και εικόνες από την

καθημερινή ζωή. Άρα έχουμε 4 ειδών ετικέτες: φωτιά, πλημμύρα, σεισμός και ουδέτερο. Προφανώς κάθε εξυπηρετητής ενδιαφέρεται για μία μόνο φυσική καταστροφή και άρα οι τελικές ετικέτες για κάθε εξυπηρετητή και τον συνασπισμό του είναι "my_disaster" ή "other". Οπότε έχουμε για κάθε εξυπηρετητή ένα πρόβλημα δυαδικής ταξινόμησης.

Οι εικόνες των φυσικών καταστροφών που χρησιμοποιήθηκαν, αποτελούν συνένωση συνόλων δεδομένων που βρέθηκαν στην πλατφόρμα του kaggle, ενώ το τροποποιημένο και συνενωμένο σύνολο μπορείτε να δείτε εδώ. Οι εικόνες αποτελούν φωτογραφίες από κοντινά πλάνα σε καταστροφές, όπως φωτογραφίες από κινητά τηλέφωνα περαστικών ή πλάνα από ειδησεογραφική κάλυψη (Δεν χρησιμοποιήθηκαν αεροφωτογραφίες, για να υπάρχει ομοιογένεια στα δεδομένα).

Σε κάθε κόμβο ανατίθενται 250 ουδέτερες εικόνες, ενώ ανάλογα με το πόσο κοντά βρίσκεται στα κρίσιμα σημεία του ανατίθενται εικόνες από τις φυσικές καταστροφές. Εάν ένας κόμβος βρίσκεται περισσότερο από 0.4 μακριά από ένα κρίσιμο σημείο, υποθέτουμε πως δεν διαθέτει πληροφορίες για αυτό. Επιπλέον, κάθε εξυπηρετητής διαθέτει ένα δικό του μικρό σύνολο δεδομένων με 250 ουδέτερες φωτογραφίες και 250 φωτογραφίες της καταστροφής που το αφορά, έτσι ώστε να συμμετέχει και αυτός στην εκπαίδευση του κεντρικού του μοντέλου.

Τέλος, για να μελετήσουμε διαφοροποιήσεις μεταξύ των διάφορων εξυπηρετητών, εφαρμόζουμε τον διαμοιρασμό των εικόνων στους κόμβους εξασφαλίζοντας ότι συνολικά: $D_{fire} > D_{flood} > D_{earthquake}$. Ο διαμοιρασμός αυτός, θα μας επιτρέψει να δούμε τις διαφορές μεταξύ των αποτελεσμάτων των διαφορετικών προβλημάτων και να καταλάβουμε την επίδραση των επιπλέον κόμβων ή επιπλέον δεδομένων σε κάθε περίπτωση.

2.3.3 Μοντέλο - Εκπαίδευση

Το μοντέλο που χρησιμοποιήθηκε για κάθε εξυπηρετητή αποτελείται από ένα προ-εκπαιδευμένο μοντέλο με δύο επίπεδα απόφασης στα κορυφαία στρώματα. Το μοντέλο αυτό θα πρέπει να μπορεί να εκπαιδευτεί και να λειτουργήσει αποδοτικά σε συσκευές που δεν είναι απαραίτητα ισχυρές υπολογιστικά (ασθενής Κεντρική Μονάδα Επεξεργασίας - ΚΜΕ και έλλειψη επιταχυντών). Συνεπώς ως προ-εκπαιδευμένο μοντέλο επιλέχθηκε το MobileNetV3 το οποίο έχει μικρό μέγεθος και εκπαιδεύεται με ικανοποιητικές ταχύτητες σε ΚΜΕ (χωρίς επιταχυντές), αλλά και σε κινητά τηλέφωνα.

Πιο αναλυτικά, το MobileNetV3 είναι ένα προηγμένο συνελικτικό νευρωνικό δίκτυο σχεδιασμένο ειδικά για εφαρμογές σε κινητές συσκευές, όπου οι υπολογιστικοί πόροι και η κατανάλωση ενέργειας είναι περιορισμένοι. Χτίζει πάνω στις αρχές των προκατόχων του, MobileNetV1 και MobileNetV2, και εισάγει πολλές σημαντικές καινοτομίες για την ενίσχυση της απόδοσης ([How+19]). Χτίζει πάνω στις αρχές των προκατόχων του, MobileNetV1 και MobileNetV2, και εισάγει πολλές σημαντικές καινοτομίες για την ενίσχυση της απόδοσης. Ένα βασικό χαρακτηριστικό που κληρονομήθηκε από το MobileNetV1 είναι οι κατά βάθος διαχωριζόμενες συνελίξεις, μια μέθοδος που διαχωρίζει τη συμβατική επιχείρηση σύγκλισης σε δύο διακριτά στάδια: κατά βάθος σύγκλιση και κατά σημείο σύγκλιση. Αυτός ο διαχωρισμός μειώνει σημαντικά τον αριθμό των παραμέτρων και το υπολογιστικό κόστος, καθιστώντας το δίκτυο πιο αποδοτικό. Η κατά βάθος σύγκλιση επεξεργάζεται κάθε κανάλι εισόδου ανεξάρτητα, ενώ η κατά σημείο σύγκλιση συνδυάζει

αυτά τα κανάλια εξόδου, επιτρέποντας στο δίκτυο να συλλαμβάνει σύνθετα χαρακτηριστικά χωρίς το υπολογιστικό βάρος των παραδοσιακών συγκλίσεων. Επιπλέον, το MobileNetV3 ενσωματώνει την έννοια των ανεστραμμένων υπολειμμάτων από το MobileNetV2. Τα ανεστραμμένα υπολείμματα χρησιμοποιούν έναν συνδυασμό ελαφρών κατά βάθος διαχωριζομένων συνελίξεων ακολουθούμενων από μια γραμμική συμφόρηση, η οποίο βοηθά στη διατήρηση των βασικών πληροφοριών χαρακτηριστικών, ενώ διατηρεί την πολυπλοκότητα του μοντέλου υπό έλεγχο ([How+19]). Αυτός ο σχεδιασμός διατηρεί μια ισορροπία μεταξύ υπολογιστικής αποδοτικότητας και αποτελεσματικής αναπαράστασης χαρακτηριστικών, εξασφαλίζοντας ότι το MobileNetV3 παραμένει τόσο ισχυρό όσο και αποδοτικό σε πόρους.

Το MobileNetV3 χρησιμοποιεί αποδοτικές αρχιτεκτονικές τεχνικές, όπως οι διαχωρίσιμες συνελίξεις σε βάθος (depthwise separable convolutions), ενώ ενσωματώνει προηγμένες τεχνικές, όπως τα μπλοκ Squeeze-and-Excitation (SE), για την ενίσχυση της δυνατότητας αναπαράστασης των συνελικτικών νευρωνικών δικτύων. Οι διαχωρίσιμες συνελίξεις σε βάθος έχουν σχεδιαστεί για να μειώνουν το υπολογιστικό κόστος και τον αριθμό των παραμέτρων σε ένα νευρωνικό δίκτυο χωρίς να θυσιάζουν σημαντικά την ακρίβεια. Αυτό είναι ιδιαίτερα χρήσιμο για ελαφριά μοντέλα όπως το MobileNet, τα οποία προορίζονται για κινητές και ενσωματωμένες συσκευές. Τα SE μπλοκς (Squeeze-and-Excitation) αποτελούν ένα εξελιγμένο αρχιτεκτονικό στοιχείο σχεδιασμένο για να ενισχύσει τη δυνατότητα αναπαράστασης των συνελικτικών νευρωνικών δικτύων ([HSS18]). Το SE μπλοκ λειτουργεί δυναμικά ανακατανέμοντας τις αντιδράσεις χαρακτηριστικών κατά κανάλια, επιτρέποντας στο δίκτυο να επικεντρωθεί σε πιο σημαντικά χαρακτηριστικά. Αυτό επιτυγχάνεται μέσω μιας διαδικασίας δύο βημάτων: πρώτα, εκτελεί παγκόσμια μέση προσαρμογή (global average pooling) για να δημιουργήσει στατιστικά στοιχεία κατά κανάλια, ”στριμώχνοντας” αποτελεσματικά τις χωρικές πληροφορίες σε μια συμπαγή αναπαράσταση. Στη συνέχεια, εφαρμόζει μια σειρά πλήρως συνδεδεμένων στρωμάτων με συνάρτηση ενεργοποίησης την σιγμοειδή, για να ”ενεργοποιήσει” ή να ανακατανείμει αυτά τα στατιστικά στοιχεία κατά κανάλια, τονίζοντας πιο σχετιζόμενα χαρακτηριστικά ενώ καταστέλλει τα λιγότερο σημαντικά. Αυτή η ανακατανομή βοηθά το δίκτυο να μάθει πιο αποτελεσματικά, ενισχύοντας την ευαισθησία του σε σημαντικά χαρακτηριστικά και βελτιώνοντας τη συνολική απόδοση. Ενσωματώνοντας μπλοκ SE, τα μοντέλα μπορούν να επιτύχουν υψηλότερη ακρίβεια και καλύτερη γενίκευση, καθιστώντας τα ιδιαίτερα πολύτιμα σε σύνθετα καθήκοντα όπου η διάκριση χαρακτηριστικών είναι κρίσιμη.

Το μοντέλο χρησιμοποιεί επίσης μια νέα συνάρτηση ενεργοποίησης, τη hard-swish, η οποία παρέχει μια υπολογιστικά αποδοτική εναλλακτική λύση στη συνάρτηση swish, συμβάλλοντας τόσο στη βελτίωση της απόδοσης όσο και στη γρηγορότερη εκτέλεση ([RZL17]). Η συνάρτηση ενεργοποίησης Swish ορίζεται ως

$$\text{swish}(x) = x \cdot \sigma(x),$$

όπου $\sigma(x)$ είναι η σιγμοειδής συνάρτηση

$$\sigma(x) = \frac{1}{1 + e^{-x}}.$$

Η συνάρτηση Swish χαρακτηρίζεται από τη λειότητα και τη μη μονοτονία της, γεγονός που της επιτρέπει να κλιμακώνει και να μετατοπίζει προσαρμοστικά την είσοδο, βελτιώνοντας έτσι την

απόδοση σε ορισμένα καθήκοντα βαθιάς μάθησης σε σύγκριση με παραδοσιακές συναρτήσεις ενεργοποίησης όπως η ReLU. Αυτή η συνάρτηση επιτρέπει στα νευρωνικά δίκτυα να μάθουν πιο σύνθετες και πλούσιες αναπαραστάσεις, ενισχύοντας την απόδοσή τους.

Αντίθετα, η συνάρτηση Hard-Swish είναι μια υπολογιστικά αποδοτική προσεγγιστική συνάρτηση της Swish, οριζόμενη ως

$$\text{hard-swish}(x) = x \cdot \text{ReLU6}(x+3)/6,$$

όπου $\text{ReLU6}(x)$ είναι η συνάρτηση ReLU6

$$\text{ReLU6}(x) = \min(\max(0, x), 6).$$

Η Hard-Swish είναι μια τμηματικά γραμμική συνάρτηση που προσεγγίζει τη Swish, ενώ είναι λιγότερο υπολογιστικά απαιτητική. Χρησιμοποιώντας τη Hard-Swish, το MobileNetV3 επωφελείται από ταχύτερους χρόνους επαγωγής και μειωμένα υπολογιστικά κόστη χωρίς σημαντική απώλεια ακρίβειας σε σύγκριση με τη χρήση της Swish άμεσα.

Η αρχιτεκτονική επωφελείται από μια αυτοματοποιημένη Αναζήτηση Νευρωνικής Αρχιτεκτονικής (NAS) που βελτιστοποιεί τόσο για καθυστέρηση όσο και για ακρίβεια, με αποτέλεσμα ένα δίκτυο που ισορροπεί υψηλή ακρίβεια με χαμηλό υπολογιστικό κόστος ([ZL16]). Η Αναζήτηση Αρχιτεκτονικής Νευρωνικών Δικτύων είναι μια προηγμένη τεχνική μηχανικής μάθησης σχεδιασμένη για την αυτόματη ανακάλυψη βέλτιστων αρχιτεκτονικών νευρωνικών δικτύων. Αντί για χειροκίνητη σχεδίαση των δομών των δικτύων, η μέθοδος Αναζήτησης Αρχιτεκτονικής Νευρωνικών Δικτύων χρησιμοποιεί αλγόριθμους για να εξερευνήσει και να αξιολογήσει διάφορες αρχιτεκτονικές διαμορφώσεις προκειμένου να εντοπίσει το πιο αποτελεσματικό σχέδιο για μια συγκεκριμένη εργασία. Η διαδικασία Αναζήτησης Αρχιτεκτονικής Νευρωνικών Δικτύων περιλαμβάνει τον καθορισμό ενός χώρου αναζήτησης, ο οποίος περιέχει δυνητικά επίπεδα δικτύου, συνδέσεις και υπερπαραμέτρους, και την εφαρμογή μιας στρατηγικής αναζήτησης που χρησιμοποιεί αλγόριθμους όπως η ενισχυτική μάθηση, οι εξελικτικές μέθοδοι ή τεχνικές βασισμένες σε βαθμούς για να εξερευνήσει συστηματικά αυτόν τον χώρο. Στη συνέχεια, γίνεται εκτίμηση απόδοσης και αξιολόγησης των υποψήφιων αρχιτεκτονικών με βάση μετρικές όπως η ακρίβεια και η υπολογιστική αποδοτικότητα. Τα οφέλη της NAS περιλαμβάνουν τη βελτιστοποιημένη απόδοση, καθώς μπορεί να ισορροπήσει την ακρίβεια και την υπολογιστική αποδοτικότητα και να δώσει εξατομικευμένες λύσεις προσαρμοσμένες σε συγκεκριμένες εργασίες και περιορισμούς.

Στην περίπτωση του MobileNetV3, η NAS χρησιμοποιήθηκε για να τελειοποιήσει την αρχιτεκτονική προκειμένου να επιτευχθεί μια βέλτιστη ισορροπία μεταξύ καθυστέρησης και ακρίβειας, με αποτέλεσμα ένα μοντέλο που διατηρεί υψηλή απόδοση ενώ ελαχιστοποιεί το υπολογιστικό κόστος. Αυτό καθιστά το MobileNetV3 ιδιαίτερα αποτελεσματικό για εφαρμογές σε περιβάλλοντα με περιορισμένους πόρους, όπως οι κινητές συσκευές.

Διαθέσιμο σε δύο παραλλαγές, MobileNetV3-Large και MobileNetV3-Small, είναι κατάλληλο για διάφορες εφαρμογές, συμπεριλαμβανομένων της επεξεργασίας εικόνας και βίντεο σε πραγματικό χρόνο, επαυξημένης πραγματικότητας (AR), εικονικής πραγματικότητας (VR), ενσωματωμένων συστημάτων και αυτόνομων οχημάτων. Συνολικά, το MobileNetV3 προσφέρει μια ελαφριά

αλλά ισχυρή λύση για την ανάπτυξη μοντέλων βαθιάς μάθησης σε συσκευές με περιορισμένους πόρους.

Στην περίπτωσή μας χρησιμοποιήθηκε το μοντέλο MobileNetV3-Large για την Εξαγωγή των Χαρακτηριστικών των εικόνων που χρησιμοποιούνται κάθε φορά στην εκπαίδευση. Σε κάθε επανάληψη της εκπαίδευσης τα χαρακτηριστικά περνούν από ένα ισοπεδωτικό επίπεδο και οδηγούνται σε ένα πλήρως συνδεδεμένο (συμπαγές) επίπεδο που αποτελείται από 128 νευρώνες, που εφαρμόζουν συνάρτηση ενεργοποίησης ReLU. Στο επίπεδο αυτό εφαρμόζουμε εγκατάλειψη 50% για να αποφύγουμε την υπερπροσαρμογή. Ως ανώτατο επίπεδο, έχουμε ένα επίπεδο απόφασης, αποτελούμενο από έναν νευρώνα στον οποίο εφαρμόζεται σιγμοειδής συνάρτηση ενεργοποίησης. Τέλος, και στα δύο επιπρόσθετα επίπεδα, εφαρμόζουμε κανονικοποίηση L2, ώστε να βοηθήσουμε την κανονικοποίηση των βαρών του μοντέλου μας και περεταίρω να βελτιώσουμε την ικανότητά του για γενίκευση. Για εξοικονόμηση χρόνου και πόρων, στην προσομοίωσή μας, στην αρχή της εκπαίδευσης του μοντέλου κάθε εξυπηρετητή εκπονούμε την διαδικασία Εξαγωγής Χαρακτηριστικών για όλες τις συμμετέχουσες εικόνες και με βάση αυτά εκπαιδεύουμε για τις απαραίτητες επαναλήψεις τα ανώτερα επίπεδα του μοντέλου. Συνεπώς, ακόμα και σε εκπαίδευση σε ΚΜΕ, έχουμε γρήγορη διάσχιση του μοντέλου και εκπαίδευσή του.

2.3.4 Υλοποίηση

Για την υλοποίηση της διαδικασίας της Ομοσπονδιακής Μάθησης αρχικά πρέπει να μοιράσουμε τα δεδομένα που έχουμε στους κόμβους μας με βάση την σημασία του καθενός για το κάθε κρίσιμο σημείο. Αυτό το πετυχαίνουμε με τον παρακάτω τρόπο:

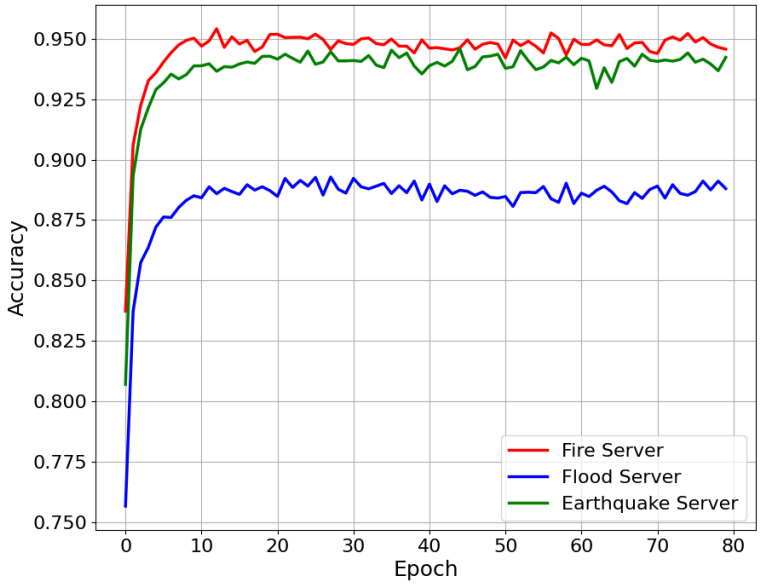
Algorithm 3 Υπολογισμός Σημασίας κόμβων

Είσοδος: Κόμβοι και Κρίσιμα Σημεία
Έξοδος: Σημασία κόμβων
for κάθε $(area, users)$ στους all_users **do**
  Αρχικοποίηση min_dist$[i] \leftarrow$ None for $i = 1, 2, \ldots, K$
  for $i = 1$ ως K **do**
    for $j = 1$ ως N **do**
      Ορίζουμε $user \leftarrow users[j]$
      $(user_x, user_y, user_z) \leftarrow (user.x, user.y, user.z)$
      $cp \leftarrow critical\_points[i]$
      $(cp_x, cp_y, cp_z) \leftarrow (cp.x, cp.y, cp.z)$
      Υπολογίζουμε $distance \leftarrow \sqrt{(cp_x - user_x)^2 + (cp_y - user_y)^2 + (cp_z - user_z)^2}$
      if min_dist$[i]$ = None ή $distance <$ min_dist$[i]$ **then**
        min_dist$[i] \leftarrow distance$
      end if
    end for
    for $j = 1$ ως N **do**
      Ορίζουμε $user \leftarrow users[j]$
      $(user_x, user_y, user_z) \leftarrow (user.x, user.y, user.z)$
      $cp \leftarrow critical\_points[i]$
      $(cp_x, cp_y, cp_z) \leftarrow (cp.x, cp.y, cp.z)$
      Υπολογίζουμε $distance \leftarrow \sqrt{(cp_x - user_x)^2 + (cp_y - user_y)^2 + (cp_z - user_z)^2}$
      Υπολογίζουμε $importance \leftarrow \frac{\text{min\_dist}[i]}{distance}$
      $user.add\_importance(importance)$
    end for
  end for
end for

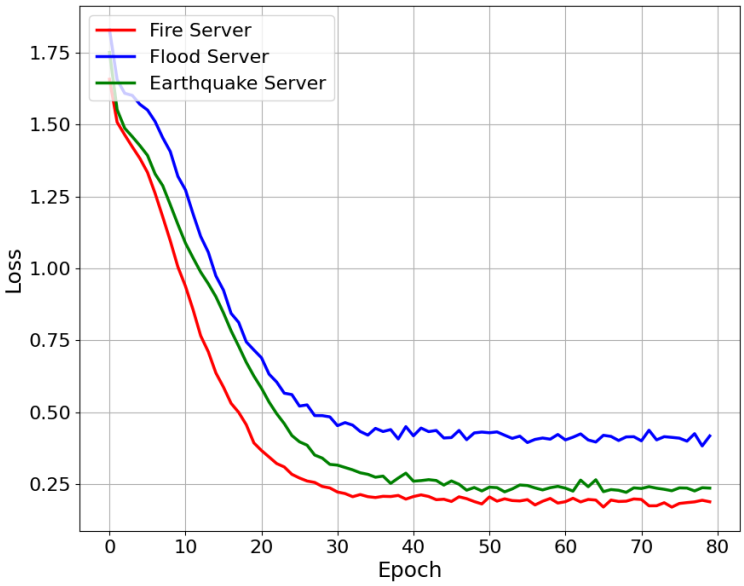
Γνωρίζοντας πλέον το μέγεθος του συνόλου δεδομένων του κάθε κόμβου για κάθε καταστροφή, μπορούμε να αντιστοιχίσουμε στον καθένα το σύνολο των φωτογραφιών που του αντιστοιχούν. Ο διαμοιρασμός θα πρέπει να γίνει με ντετερμινιστικό τρόπο, ώστε κάθε i κόμβος να διαθέτει το ίδιο σύνολο φωτογραφιών, από το οποίο, ανάλογα αν είναι ”καλός” ή ”κακός”, να επιλέγει περισσότερες ή λιγότερες. Ένας τρόπος να επιτευχθεί αυτό είναι να χωρίσουμε αρχικά τις φωτογραφίες κάθε καταστροφής σε σύνολα των 250 φωτογραφιών, όπου το σύνολο i θα ανήκει στον κόμβο i. Συνεπώς, για κάθε μία από τις τρεις καταστροφές, ο κόμβος επιλέγει, από το σύνολο που του αντιστοιχεί, φωτογραφίες ίσες με το μέγεθος συνόλου που υπολογίσαμε παραπάνω. Άρα και πάλι εξασφαλίζουμε πως παρότι ως αντικείμενα οι κόμβοι μας είναι διαφορετικοί σε κάθε περιοχή, θα αντλήσουν πληροφορία από τις ίδιες εικόνες και η μόνη διαφοροποίηση που μπορεί να έχουν θα είναι το πλήθος των φωτογραφιών τους.

Για την υλοποίηση της Ομοσπονδιακής Μάθησης χρησιμοποιήθηκε ως βάση ο κώδικας [L23], ο οποίος υλοποιεί την διαδικασία της παραδοσιακής Ομοσπονδιακής Μάθησης.

2.4 Αποτελέσματα



Σχήμα 2.5: Ακρίβεια κόμβων ανά εποχή

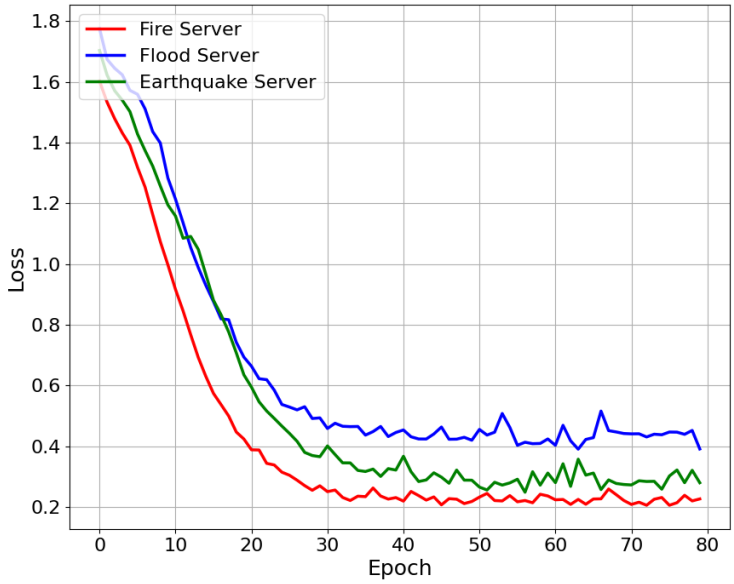


Σχήμα 2.6: Απώλεια κόμβων ανά εποχή

Όπως φαίνεται στα διαγράμματα 2.5 και 2.6 οι κόμβοι μας ξεκινούν την εκμάθηση και σταδιακά αφομοιώνουν την πληροφορία του παγκόσμιου μοντέλου, μαθαίνοντας και από τους υπόλοιπους κόμβους. Έτσι, η μέση ακρίβεια των κόμβων αυξάνεται σταδιακά, ενόσω κάθε κόμβος επεξεργάζεται ξανά τα δικά του δεδομένα σε συνδυασμό με την πληροφορία που δέχεται από τον εξυπηρετητή του, ενώ η απώλεια αντίστοιχα μειώνεται. Βλέπουμε πως μετά από περίπου 20 εποχές - επαναλήψεις αρχίζουν και οι δύο ποσότητες να σταθεροποιούνται καταλήγοντας σε σύγκλιση.

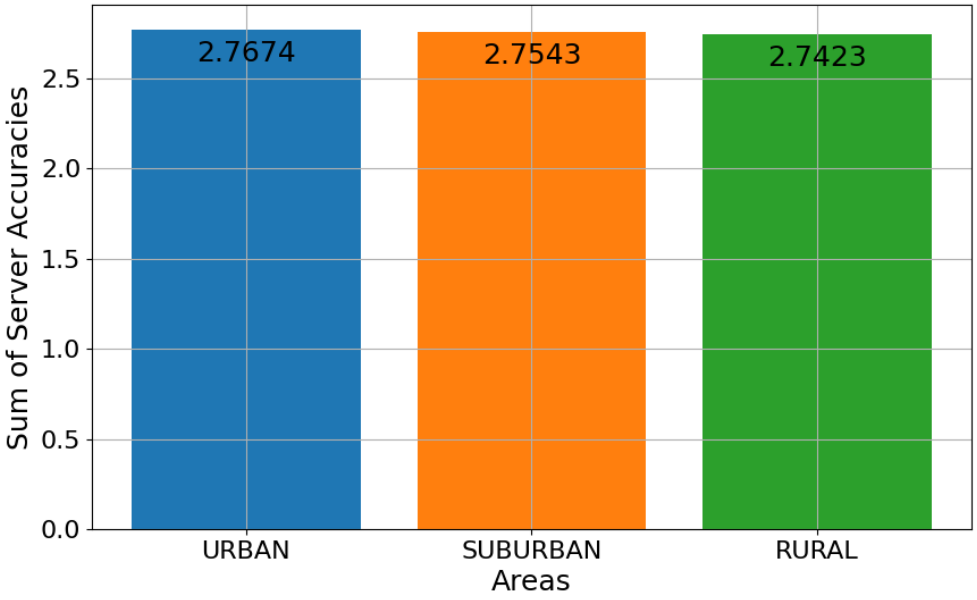
Αντίστοιχη συμπεριφορά παρατηρούμε στα διαγράμματα για τους Εξυπηρετητές. Η εξέταση της απόδοσης των εξυπηρετητών κατά τις εποχές παρουσιάζει μια συνεπή τάση, με τον Εξυπηρετητή Πυρκαγιάς να επιτυγχάνει σταθερά τη μεγαλύτερη ακρίβεια, ακολουθούμενος από τους Εξυπηρετητές Σεισμών και Πλημμυρών (2.7), δεδομένου ότι ο Εξυπηρετητής Πυρκαγιάς διαθέτει μεγαλύτερο σύνολο δεδομένων και, κατά συνέπεια, επιδεικνύει ανώτερη απόδοση. Ωστόσο, μια ενδιαφέρουσα απόκλιση παρατηρείται στον Εξυπηρετητή Πλημμυρών, ο οποίος, παρά το γεγονός ότι διαθέτει μεγαλύτερο σύνολο δεδομένων σε σύγκριση με τον Εξυπηρετητή Σεισμών, παρουσιάζει χαμηλότερη απόδοση (2.7 – 2.8). Αυτή η ανωμαλία προκύπτει από τη συμπερίληψη εικόνων με περιεχόμενο νερού στα ουδέτερα σύνολα δεδομένων που μοιράζονται οι Εξυπηρετητές. Αυτές οι εικόνες εισάγουν σύγχυση στη διαδικασία εκπαίδευσης του Εξυπηρετητή Πλημμυρών, επηρεάζοντας τελικά αρνητικά την απόδοσή του. Όπως αναφέρουν και οι Barry et al. ([BHD23]) η ποιότητα των δεδομένων και ο θόρυβος μπορούν να επηρεάσουν σημαντικά την απόδοση του μοντέλου. Ειδικότερα αν οι καλοί κόμβοι του Εξυπηρετητή Πλημμυρών διαθέτουν παρεμφερείς εικόνες με αυτές του Ουδέτερου Συνόλου Δεδομένων η εκμάθηση γίνεται πολύ δύσκολη αφού αυτοί οι κόμβοι έχουν τη μεγαλύτερη συμμετοχή στη διαδικασία.

Σχήμα 2.7: Ακρίβεια Εξυπηρετητών ανά εποχή

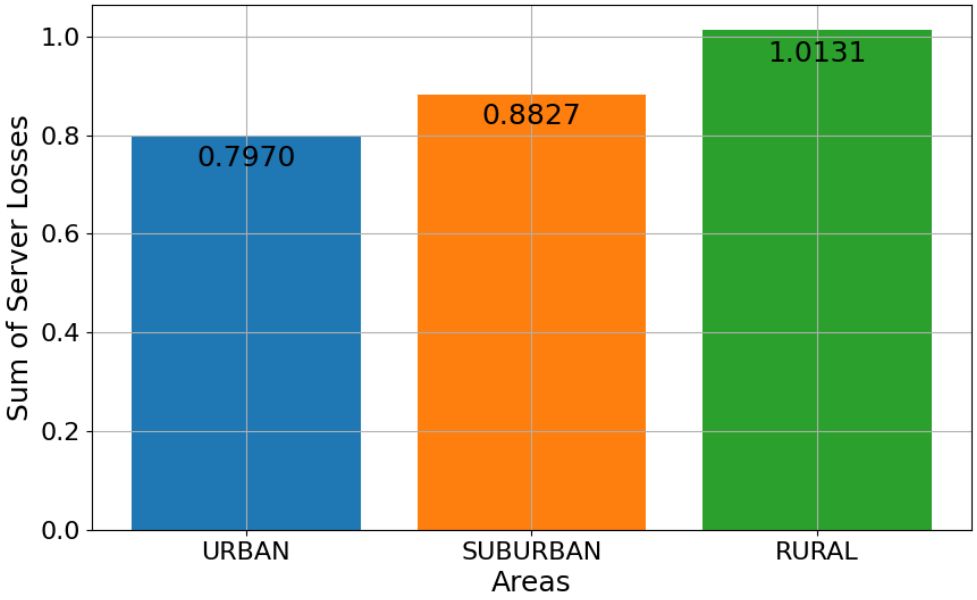


Σχήμα 2.8: Απώλεια Εξυπηρετητών ανά εποχή

Έτσι, ο Εξυπηρετητής Σεισμών, παρά το μικρότερο σύνολο δεδομένων, αποδίδει σχετικά καλύτερα από το αναμενόμενο, καταδεικνύοντας την πολύπλοκη σχέση μεταξύ μεγέθους συνόλου δεδομένων και απόδοσης. Επίσης, οι κόμβοι που σχετίζονται με τον Εξυπηρετητή Σεισμών επιτυγχάνουν σταθερά υψηλότερη τοπική ακρίβεια σε σύγκριση με τους κόμβους των Εξυπηρετητών Πυρκαγιάς και Πλημμυρών (2.5), αποδεικνύοντας την αποτελεσματικότητα των αντίστοιχων συνόλων δεδομένων. Ωστόσο, η διαφορά στην απόδοση των κόμβων δεν αντικατοπτρίζει άμεσα την ιεραρχία που παρατηρείται στην απόδοση των Εξυπηρετητών. Αυτή η απόκλιση προκύπτει από τη δυσκολία της πραγματικής σύνθεσης των συνόλων των παραμέτρων στο παγκόσμιο μοντέλο, αλλά και από υπερπροσαρμογή των κόμβων του Εξυπηρετητή Σεισμών (διαφορά μεταξύ ακρίβειας εκπαίδευσης και ακρίβειας δοκιμών).



Σχήμα 2.9: Σενάριο Δημόσιας ασφάλειας σε διαφορετικές περιοχές (αστική, προαστιακή, αγροτική) - Ακρίβεια



Σχήμα 2.10: Σενάριο Δημόσιας ασφάλειας σε διαφορετικές περιοχές (αστική, προαστιακή, αγροτική) - Απώλεια

Ο μηχανισμός αντιστοίχισης δοκιμάζεται σε ένα ρεαλιστικό σενάριο δημόσιας ασφάλειας σε αστικά, προαστιακά και αγροτικά περιβάλλοντα. Η 2.9 παρουσιάζει το άθροισμα της ακρίβειας των εξυπηρετητών για τρία διακριτά σενάρια: Αστικό, Προαστιακό και Αγροτικό, καθένα από τα οποία χαρακτηρίζεται από διαφορετική σύνθεση κόμβων. Αντίστοιχα στο 2.10 παρουσιάζει το άθροισμα της απώλειας των εξυπηρετητών στις τρεις αυτές περιοχές.

Σε κάθε σενάριο, οι κόμβοι κατηγοριοποιούνται είτε ως καλοί (κοντά στα Σημεία Ενδιαφέροντος) είτε ως κακοί (μακριά από τα Σημεία Ενδιαφέροντος, γεγονός που οδηγεί σε σύγχυση του αλγορίθμου και μειωμένη χρησιμότητα δεδομένων). Το όριο που διαχωρίζει τους καλούς από τους κακούς κόμβους διαφέρει μεταξύ των σεναρίων: Αστικό (30), Προαστιακό (21) και Αγροτικό (12), υποδεικνύοντας το σημείο πέρα από το οποίο οι κόμβοι θεωρούνται κακοί.

Τα αποτελέσματα αποκαλύπτουν ένα συνεπές πρότυπο για τα τρία σενάρια. Όσο οι κόμβοι μας είναι πιο απομακρυσμένοι από τα σημεία ενδιαφέροντος και άρα διαθέτουν λιγότερη πληροφορία, καθιστούν πιο δύσκολη την εκπαίδευση του κεντρικού μοντέλου. Για αυτό το λόγο, όπως φαίνεται, πετυχαίνουμε καλύτερη αθροιστική Ακρίβεια και μικρότερη σε μία Αστική Περιοχή απ' ότι σε μία Προαστιακή Περιοχή και μία Αγροτική Περιοχή.

Από τη συμπεριφορά αυτή φαίνεται πώς η διαφοροποίηση ανά περιοχή με καλούς και κακούς κόμβους επηρεάζει την εκμάθηση των μοντέλων. Έχοντας κόμβους με λιγότερα δεδομένα - εικόνες να συμμετέχουν στην Ομοσπονδιακή Μάθηση, δυσκολεύει σε κάποιο βαθμό τη γενίκευση στο παγκόσμιο μοντέλο. Η αρνητική επίδραση αυτή καταπολεμάται από τον αλγόριθμό μας με τη χρήση βαρών συμμετοχής στην εκμάθηση, όπου ένας κακός κόμβος, με λιγότερα, άρα και πιο μη γενικευμένα δεδομένα, συμμετέχει λιγότερο σε σχέση με έναν κόμβο που διαθέτει περισσότερη πληροφορία, με αποτέλεσμα εν τέλει σε όλες τις περιοχές να πετυχαίνουμε πολύ καλά αποτελέσματα για τα παγκόσμια μοντέλα.

3

Αντιστοίχιση με Αλγορίθμους Ενισχυτικής Μάθησης

Στο δεύτερο, αυτό κομμάτι της διπλωματικής εργασίας, θα συγκρίνουμε τον Αλγόριθμο Θεωρίας Παιγνίων, που παρουσιάσαμε στο προηγούμενο κεφάλαιο, με άλλους αλγορίθμους που χρησιμοποιούνται σε παρόμοιες περιπτώσεις. Συγκεκριμένα θα μελετήσουμε την συμπεριφορά αλγορίθμων Μηχανικής Μάθησης - Ενισχυτικής Μάθησης, αλλά θα χρησιμοποιήσουμε και ως σημείο αναφοράς τον αλγόριθμο τυχαίας αντιστοίχισης, ώστε να αποφανθούμε για τα οφέλη που μας προσφέρουν οι υπόλοιποι αλγόριθμοι.

Η Ενισχυτική Μάθηση (Reinforcement Learning, RL) περιλαμβάνει μια ποικιλία αλγορίθμων που έχουν σχεδιαστεί για να μαθαίνουν τις βέλτιστες πολιτικές επιλογής ενεργειών μέσω αλληλεπιδράσεων με ένα περιβάλλον. Οι βασικές μέθοδοι βασισμένες σε τιμές περιλαμβάνουν τους αλγόριθμους Q-Learning και SARSA (State-Action-Reward-State-Action). Το Q-Learning είναι ένας εκτός πολιτικής αλγόριθμος που ενημερώνει επαναληπτικά τις τιμές Q για να εκτιμήσει την αναμενόμενη χρησιμότητα των ενεργειών σε δεδομένες καταστάσεις, ανεξάρτητα από τις ενέργειες του πράκτορα (ατόμου - κόμβου). Στοχεύει να μάθει την βέλτιστη πολιτική μεγιστοποιώντας τη συνολική ανταμοιβή με την πάροδο του χρόνου. Αντίθετα, το SARSA είναι ένας εντός πολιτικής αλγόριθμος που ενημερώνει τις τιμές Q βάσει των πραγματικών ενεργειών που λαμβάνονται από την πολιτική, αντί της μέγιστης δυνατής ενέργειας. Αυτό επιτρέπει στο SARSA να ενσωματώνει άμεσα τα αποτελέσματα της τρέχουσας πολιτικής του πράκτορα στη διαδικασία μάθησης. [FK22]

Τα Βαθειά Q-Δίκτυα (Deep Q-Networks - DQN) επεκτείνουν το Q-Learning ενσωματώνοντας βαθιά νευρωνικά δίκτυα, επιτρέποντας τη διαχείριση χώρων καταστάσεων υψηλής διάστασης. Τα Βαθειά Q-Δίκτυα χρησιμοποιούν αναπαραγωγή εμπειριών για να αποθηκεύουν και να επαναχρησιμοποιούν παλαιότερες εμπειρίες, βοηθώντας στη διακοπή της συσχέτισης μεταξύ διαδοχικών βημάτων μάθησης και βελτιώνοντας την αποδοτικότητα της εκπαίδευσης. Επιπλέον, τα Βαθειά Q-Δίκτυα χρησιμοποιούν ένα δίκτυο στόχου για να παρέχουν σταθερούς στόχους τιμών Q, μειώνοντας έτσι τα προβλήματα αστάθειας που προκύπτουν κατά την εκπαίδευση νευρωνικών δικτύων. [FK22]

Στην δική μας περίπτωση, οι τεχνικές Ενισχυτικής Μάθησης χρησιμοποιούνται όλο και περισσότερο στις λειτουργίες αντιστοίχισης σε διάφορους τομείς, όπως συστήματα συστάσεων, διαδικτυακή διαφήμιση και κατανομή πόρων. Σε αυτές τις εφαρμογές, οι αλγόριθμοι Ενισχυτικής Μάθησης, βελτιστοποιούν τη διαδικασία αντιστοίχισης μαθαίνοντας από τις αλληλεπιδράσεις με

το περιβάλλον. Για παράδειγμα, στα συστήματα συστάσεων, οι πράκτορες Ενισχυτικής Μάθησης βελτιώνουν διαδοχικά τις προτάσεις τους λαμβάνοντας υπόψη την ανατροφοδότηση των κόμβων και ενημερώνοντας τις πολιτικές τους για τη μεγιστοποίηση της μακροπρόθεσμης εμπλοκής και ικανοποίησης των κόμβων. [ACF22]

Σε αντίστοιχη περίπτωση, μπορούμε να χρησιμοποιήσουμε τέτοιους αλγορίθμους για την αντιστοίχιση των κόμβων μας με τους εξυπηρετητές. Μέσω της Ενισχυτικής Μάθησης, οι κόμβοι λαμβάνουν αμοιβές ανάλογα με την ενέργεια που επιλέγουν κάθε φορά και έπειτα από συγκεκριμένο αριθμό επαναλήψεων, ο κάθε κόμβος επιλέγει την βέλτιστη ενέργεια με βάση τις αμοιβές που έχει συλλέξει.

3.1 Περιγραφή Αλγορίθμων Ενισχυτικής Μάθησης

Για την εξερεύνηση και επιλογή ενεργειών από τους κόμβους θα χρησιμοποιήσουμε την αλγοριθμική τεχνική Ανώτατου Ορίου Εμπιστοσύνης (Upper Confidence Bound - UCB). Ο αλγόριθμος Ανώτατου Ορίου Αυτοπεποίθησης είναι μια στρατηγική που χρησιμοποιείται στη ενισχυτική μάθηση και στα προβλήματα πολλαπλών ένοπλων ληστών (multi-armed bandit) για να εξισορροπήσει αποτελεσματικά την εξερεύνηση και την εκμετάλλευση. Σε αντίθεση με απλές μεθόδους όπως ο αλγόριθμος ε-άπληστος (ε-greedy), ο Ανώτατου Ορίου Αυτοπεποίθησης επιλέγει ενέργειες με βάση τόσο τις εκτιμώμενες ανταμοιβές όσο και την αβεβαιότητα σε αυτές τις εκτιμήσεις. Δίνοντας προτεραιότητα σε ενέργειες με μεγαλύτερη αβεβαιότητα, ο Ανώτατου Ορίου Αυτοπεποίθησης εξερευνά συστηματικά λιγότερο δοκιμασμένες επιλογές, διασφαλίζοντας ότι ο αλγόριθμος συγκεντρώνει επαρκείς πληροφορίες για όλες τις πιθανές ενέργειες. Αυτή η προσέγγιση βοηθά στην πιο αξιόπιστη αναγνώριση της βέλτιστης ενέργειας με την πάροδο του χρόνου. Η μεθοδική μέθοδος του Ανώτατου Ορίου Αυτοπεποίθησης για την εξισορρόπηση της εξερεύνησης και της εκμετάλλευσης τον καθιστά ιδιαίτερα χρήσιμο σε σενάρια όπου η κατανόηση των υποκείμενων κατανομών ανταμοιβής είναι κρίσιμη για την μακροπρόθεσμη επιτυχία. [SB18b]

Στην περίπτωσή μας, ακολουθούμε την εξής διαδικασία: Αρχικά, κάθε κόμβος δεν ανήκει σε κανέναν εξυπηρετητή. Σε κάθε επανάληψη, κάθε κόμβος συλλέγει τις ενέργειες που μπορεί να επιλέξει να εκτελέσει. Στην συνέχεια εφαρμόζει τον κανόνα επιλογής ενέργειας του Αλγορίθμου Ανώτατου Ορίου Αυτοπεποίθησης για να επιλέξει την βέλτιστη ενέργεια σύμφωνα με τα μέχρι τώρα δεδομένα του (προφανώς αρχικά δεν έχει λάβει κάποια ανατροφοδότηση από το περιβάλλον του). Ο κανόνας επιλογής ενέργειας του αλγορίθμου επιλέγει την ενέργεια που μεγιστοποιεί το ανώτερο όριο εμπιστοσύνης της εκτιμώμενης ανταμοιβής. Το ανώτερο όριο εμπιστοσύνης υπολογίζεται ως:

$$a_t = \arg\max_a \left(\hat{Q}(a) + c\sqrt{\frac{\ln t}{N(a)}} \right) \tag{3.1}$$

όπου:

- $\hat{Q}(a)$ είναι η εκτιμώμενη ανταμοιβή για την ενέργεια a.
- t είναι ο συνολικός αριθμός φορών που έχει επιλεχθεί μια ενέργεια.

- $N(a)$ είναι ο αριθμός φορών που έχει επιλεχθεί η ενέργεια a.
- c είναι μια σταθερά που εξισορροπεί την εξερεύνηση και την εκμετάλλευση.

Ο όρος $\sqrt{\frac{\ln t}{N(a)}}$ αντιπροσωπεύει την αβεβαιότητα ή το διάστημα εμπιστοσύνης για την εκτιμώμενη ανταμοιβή. Οι ενέργειες με λιγότερες επιλογές ($N(a)$) θα έχουν μεγαλύτερη αβεβαιότητα, ενθαρρύνοντας την εξερεύνηση.

Αφού επιλεγεί η βέλτιστη ενέργεια, ο κόμβος την εκτελεί και λαμβάνει την αντίστοιχη ανταμοιβή - ανατροφοδότηση, από το δίκτυο. Επιπλέον, ανανεώνει την εκτιμώμενη ανταμοιβή του για την ενέργεια **α** ως:

$$\hat{Q}(a) = \hat{Q}(a) + \gamma(r - \hat{Q}(a)) \tag{3.2}$$

όπου **r** είναι η ανταμοιβή-ανατροφοδότηση που λαμβάνει από το δίκτυο και **γ** ο όρος που καθορίζει πόσο σημαντικές είναι για την εκτιμώμενη ανταμοιβή οι μελλοντικές ανταμοιβές που λαμβάνει.

Οι υπόλοιποι κόμβους ακολουθούν την ίδια διαδικασία, αφού όμως έχει εκτελεστεί η ενέργεια του πρώτου κόμβου, με αποτέλεσμα να έχει αλλάξει το οικοσύστημα. Η διαδικασία αυτή επαναλαμβάνεται μέχρι να πετύχουμε σύγκλιση του αλγορίθμου. Η σύγκλιση εξασφαλίζεται όταν η διαφορά των πινάκων Q(a) σε δύο διαδοχικές επαναλήψεις είναι για κάθε ενέργεια κάτω από μια συγκεκριμένη τιμή ανοχής (tolerance). Όταν επιτευχθεί η σύγκλιση, κάθε κόμβος, με βάση τις αμοιβές που έχει συλλέξει, αποφασίζει για την ενέργεια την οποία θα λάβει τελικά.

Στην εργασία αυτή θα μελετήσουμε δύο εκδοχές του αλγορίθμου, οι οποίες χρησιμοποιούν διαφορετικές εκδοχές συνάρτησης ανταμοιβής για κάθε ενέργεια. Η πρώτη βασίζεται στην εστίαση στον κόμβου, δηλαδή ως ανταμοιβή για μια ενέργεια δίνεται η χρησιμότητα του κόμβου (Εξίσωση 2.7) έπειτα από την επιλογή της ενέργειας:

$$reward(a) = U_{n,s} \tag{3.3}$$

όπου s είναι ο εξυπηρετητής που επιλέγεται από την ενέργεια του κόμβου n που θεωρήθηκε βέλτιστη.

Η δεύτερη εκδοχή, εστιάζει στην προτίμηση των εξυπηρετητών και άρα αυτή τη φορά ορίζουμε ως ανταμοιβή την μέση χρησιμότητα ανά κόμβου που βιώνει ο εξυπηρετητής (Εξίσωση 2.8):

$$reward(a) = \frac{U_s(P_s, P_{-s})}{N_s} \tag{3.4}$$

όπου s είναι ο εξυπηρετητής που επιλέγεται από την ενέργεια του κόμβου n που θεωρήθηκε βέλτιστη και N_s το πλήθος του συνασπισμού του s.

Algorithm 4 Αλγόριθμος Αντιστοίχισης με Ενισχυτική Μάθηση

Είσοδος: $L_n, a_n, q_n, D_n, f_n, \mathbf{w}_n \forall n \in \mathcal{N}, L_k \forall k \in \mathcal{K}, \alpha, \beta, \gamma,$
Έξοδος: Αποτελέσματα Αντιστοίχισης M
Αρχικοποίηση: $cumulative\_reward = 0$, $N_t = 0$, $Q_n = 0$ $\forall$ πιθανή ενέργεια και $\forall n \in N$
while not convergence **do**
  for $n \in \mathcal{N}$ **do**
    Ο κόμβος n επιλέγει την βέλτιστη ενέργεια με βάση την Εξίσωση 3.1.
    Εκτελεί την ενέργεια και λαμβάνει την αντίστοιχη ανταμοιβή με βάσει τις εξισώσεις 3.3 και 3.4.
    Τέλος ανανεώνει τα: $cumulative\_reward(n, a) += reward$, $Nt(n, a) += 1$ και Qn με βάση την εξίσωση 3.2
  end for
end while
for $n \in \mathcal{N}$ **do**
  Ο κόμβος n επιλέγει την βέλτιστη ενέργεια με βάση το μεγαλύτερο cumulative reward που έχει συλλέξει για κάθε ενέργεια.
end for

Τέλος, όπως αναφέραμε, ως σημείο αναφοράς θα χρησιμοποιηθεί ο Αλγόριθμος Τυχαίας Αντιστοίχισης, σύμφωνα με τον οποίο κάθε κόμβος αντιστοιχίζεται τυχαία σε κάποιον εξυπηρετητής, τηρώντας προφανώς το όριο Ns_{max} του κάθε εξυπηρετητή.

Algorithm 5 Αλγόριθμος Τυχαίας Αντιστοίχισης

Είσοδος: $L_n, a_n, q_n, D_n, f_n, \mathbf{w}_n \forall n \in \mathcal{N}, L_k \forall k \in \mathcal{K}, \alpha, \beta, \gamma,$
Έξοδος: Αποτελέσματα Αντιστοίχισης M
for $n \in \mathcal{N}$ **do**
  Ο κόμβος n επιλέγει τυχαία έναν εξυπηρετητή εφ'όσον αυτός διαθέτει χώρο στον συνασπισμό του.
end for

3.2 Υλοποίηση

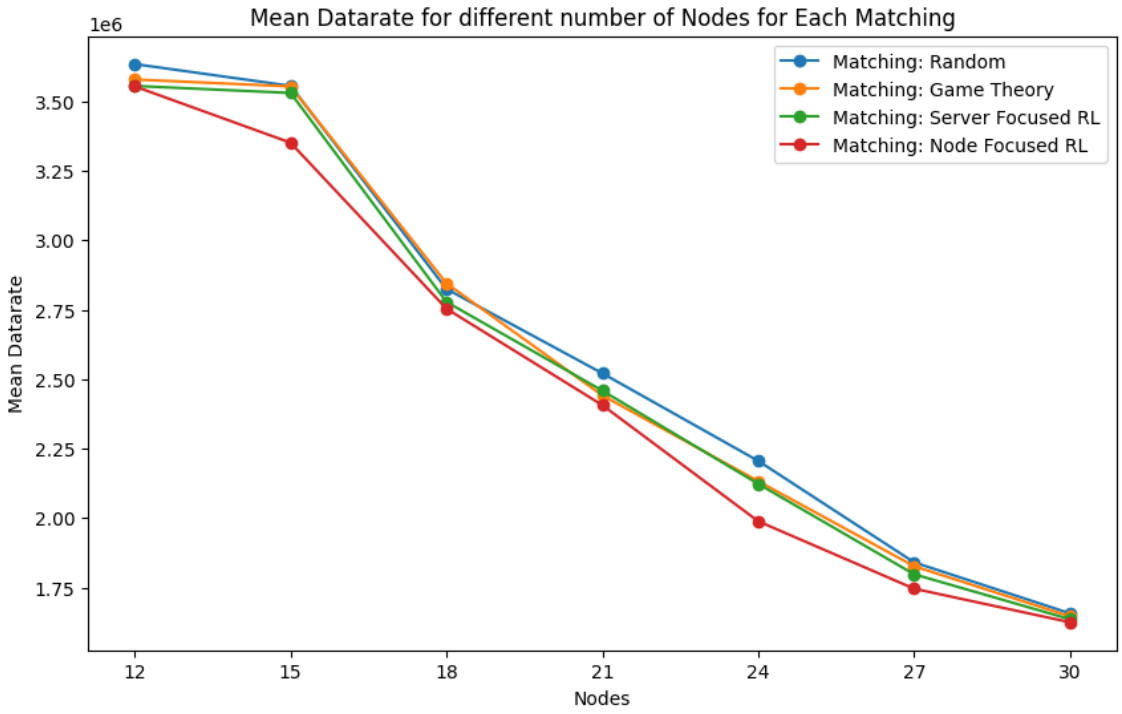
Αλλαγή Οικοσυστήματος κόμβων - Εξυπηρετητών: Στο συγκεκριμένο κεφάλαιο, για να εξεταστούν σε μεγαλύτερο βάθος οι επιδόσεις των διαφορετικών αλγορίθμων για την σύγκρισή τους, αλλάζουμε λίγο τον τρόπο με τον οποίο τοποθετούμε πάνω στον "χάρτη" τους κόμβους μας και τα κρίσιμα σημεία. Πιο συγκεκριμένα, ορίζουμε την ελάχιστη απόσταση μεταξύ δύο σημείων σε 0.4 και άρα πλέον, για μεγαλύτερα N είναι πιο πιθανό οι πιο απομακρυσμένοι κόμβοι να προσφέρουν καλύτερη χρησιμότητα για άλλους εξυπηρετητές, απ' ότι για αυτόν του κρίσιμου σημείου γύρω από το οποίο τοποθετήθηκαν αρχικά. Οι απομακρυσμένοι λοιπόν κόμβοι, θα μας δώσουν μια πιο ξεκάθαρη εικόνα για το ποιος αλγόριθμος λειτουργεί καλύτερα και σε πιο δύσκολες και όχι απαραίτητα προφανείς καταστάσεις. Επιπλέον, για να δώσουμε επιπλέον διαφοροποίηση και ισχύ στους εξυπηρετητές, κάθε εξυπηρετητής τώρα διαθέτει χρηματικούς πόρους μεταξύ $\lceil \frac{N}{3} \rceil$ και

$\lceil \frac{N}{2} \rceil$. Συνεπώς, όντας κάποιοι εξυπηρετητές πιο ισχυροί, θα έχουν την δυνατότητα να προσελκύσουν πιο εύκολα κόμβους σε αυτούς και άρα θα είναι πιο πιθανό κάποιοι απομακρυσμένοι κόμβοι να τους προτιμήσουν. Επιπλέον, δεν ασχολούμαστε πλέον με διαφορετικές περιοχές κόμβων (Αστική, Προαστιακή, Αγροτική), απλά τοποθετούμε κόμβους γύρω από τα κρίσιμα σημεία μας, με στόχο να μελετήσουμε την συμπεριφορά των διαφορετικών αλγορίθμων αντιστοίχισης.

Για την ορθή σύγκριση των αλγορίθμων, φροντίζουμε και οι τρεις να δέχονται ως είσοδο τους ίδιους κόμβους, δηλαδή να μην δημιουργούμε ξανά νέα αντικείμενα κόμβων. Αυτό μας εξασφαλίζει αντίστοιχα ότι οι σημασίες των κόμβων μας για κάθε εξυπηρετητή παραμένουν οι ίδιες και άρα οι αλγόριθμοί μας ανταγωνίζονται στο ίδιο περιβάλλον. Αντίστοιχα, όπως και στο προηγούμενο κεφάλαιο, φροντίζουμε, με ντετερμινιστικά τυχαίο τρόπο, οι κόμβοι μας να λάβουν τα ίδια δεδομένα-φωτογραφίες σε κάθε περίπτωση, ώστε κατά την εκπαίδευση του συστήματος που παράγει κάθε αλγόριθμος, να πάρουμε αντιπροσωπευτικά αποτελέσματα για την σύγκρισή τους.

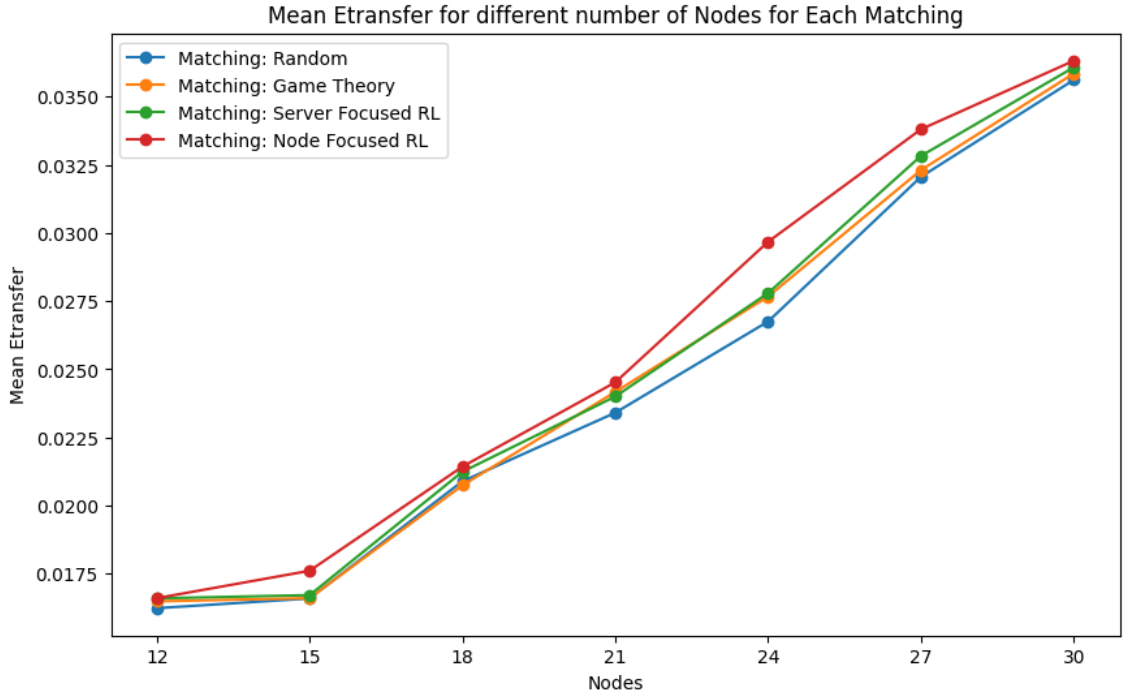
3.3 Σύγκριση - Αποτελέσματα

Σύμφωνα με τα αποτελέσματά μας, ο αλγόριθμος Θεωρίας Παιγνίων αποδίδει καλύτερα στις περισσότερες περιπτώσεις. Πετυχαίνει βέλτιστη αντιστοίχιση στα περισσότερες διαμορφώσεις του περιβάλλοντος μας (διαφορετικά πλήθη κόμβων), ενώ οι αλγόριθμοι Μηχανικής Μάθησης φαίνεται να κάνουν υποβέλτιστες αντιστοιχίσεις, κάνοντας λάθη, ειδικά όταν ο αριθμός των κόμβων μεγαλώνει και έχουμε και πιο απομακρυσμένους κόμβους. Ως βασικό σημείο αναφοράς έχουμε την επίδοση του τυχαίου αλγορίθμου αντιστοίχισης, ο οποίος εκτελείται ταχύτατα. Πιο συγκεκριμένα παίρνουμε τα εξής διαγράμματα:



Σχήμα 3.1: Μέση ροή δεδομένων ανά αριθμό κόμβων ανά αλγόριθμο αντιστοίχισης

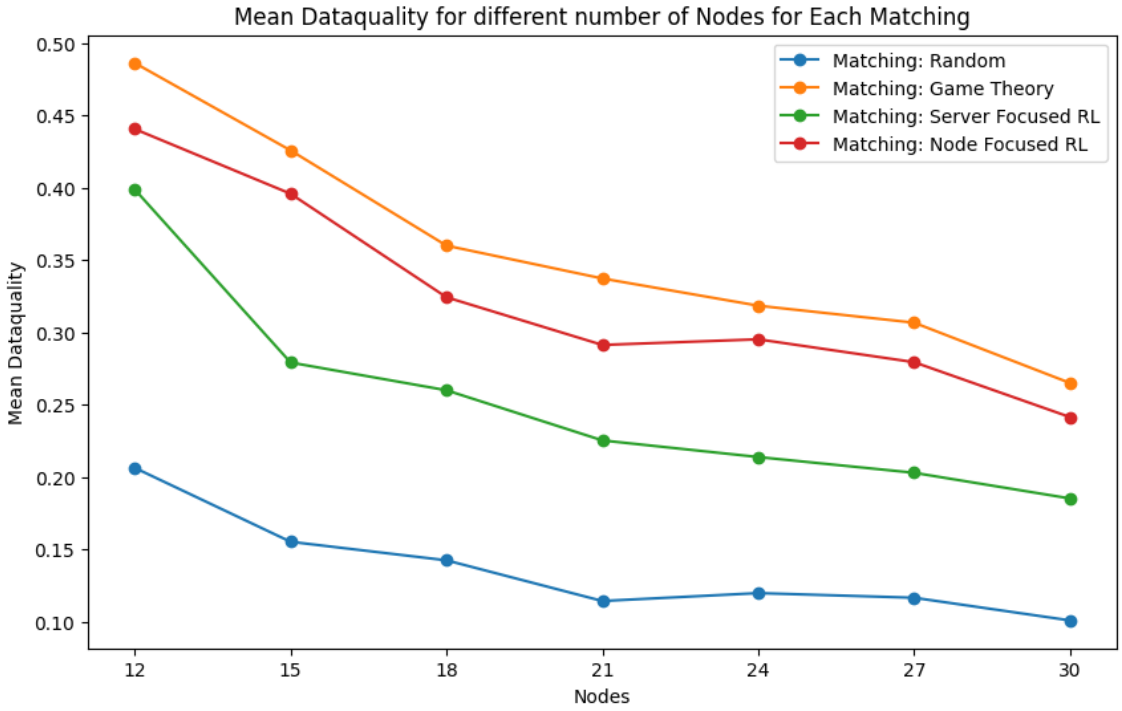
Όπως φαίνεται στο 3.1 οι αλγόριθμοί μας παρουσιάζουν αντίστοιχες μέσες ροές δεδομένων για τους κόμβους τους. Παραδόξως ο αλγόριθμος Τυχαίας Αντιστοίχισης φαίνεται να έχει την καλύτερη απόδοση κατά μέσο όρο. Αυτό συμβαίνει επειδή δεν λαμβάνει υπόψη του τις άλλες παραμέτρους και άρα είναι πιθανό να κάνει μια ”πιο δίκαιη” κατανομή των κόμβων στους εξυπηρετητές, όσον αφορά την ροή δεδομένων. Αντίθετα οι άλλοι αλγόριθμοι κοιτούν να αυξήσουν την χρησιμότητα του συστήματος η οποία διαθέτει και άλλες παραμέτρους. Παρατηρούμε πως όσο αυξάνεται ο αριθμός των κόμβων, η ροή δεδομένων μειώνεται, αφού περισσότεροι κόμβοι ανταγωνίζονται για τους διαθέσιμους πόρους κάθε εξυπηρετητή (εύρος ζώνης). Συνεπώς, όσο περισσότερους κόμβους έχουμε στο σύστημά μας τόσο λιγότερα δεδομένα μπορούν να στείλουν ταυτόχρονα στον κοινό εξυπηρετητή τους.



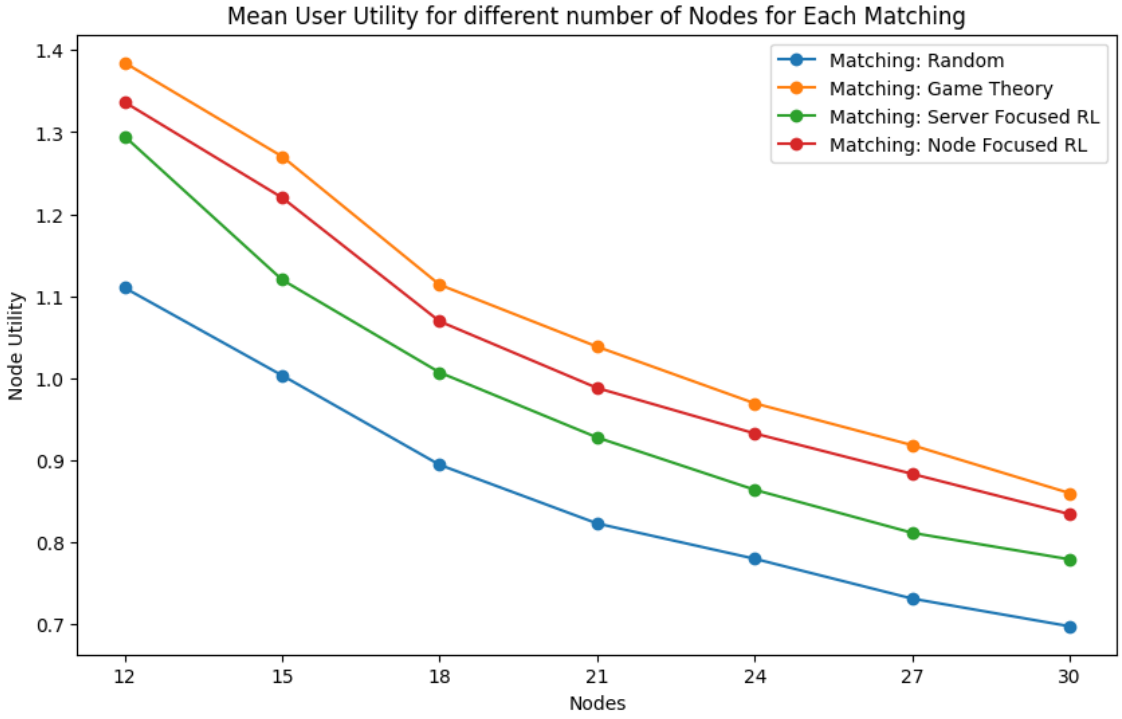
Σχήμα 3.2: Μέση ενέργεια μετάδοσης ανά αριθμό κόμβων ανά αλγόριθμο αντιστοίχισης

Όπως είναι εμφανές στο διάγραμμα 3.2 και αναφέραμε και για την ροή δεδομένων, όσο περισσότερους κόμβους έχουμε, αυτοί ανταγωνίζονται για περισσότερους πόρους και άρα η μέση ενέργεια μετάδοσης αυξάνεται. Όπως, βλέπουμε αντίστοιχα, ο αλγόριθμος Τυχαίας Αντιστοίχισης κρατά την ενέργεια μετάδοσης χαμηλότερα απ’ όλους, αφού δεν παίρνει υπόψη του την συνάρτηση χρησιμότητας, η οποία εξετάζει και άλλες παραμέτρους. Την δεύτερη καλύτερη επίδοση έχει ο αλγόριθμος Θεωρίας Παιγνίων, ο οποίος υπερέχει των δύο αλγορίθμων Ενισχυτικής Μάθησης.

Όσον αφορά την ποιότητα δεδομένων, βλέπουμε στο 3.3 πως και πάλι ο αλγόριθμος Θεωρίας Παιγνίων πετυχαίνει το καλύτερο αποτέλεσμα, με σταθερά καλύτερη ποιότητα δεδομένων. Όσο εισέρχονται κόμβοι στο σύστημά μας η μέση ποιότητα μειώνεται, αφού οι νέοι κόμβοι τοποθετούνται όλο και πιο μακριά, με αποτέλεσμα να έχουν και λιγότερα δεδομένα. Η ποιότητα δεδομένων είναι ένα πολύ σημαντικό μέγεθος, αφού επηρεάζει άμεσα την εκπαίδευση του μοντέλου Ομοσπονδιακής Μάθησης.

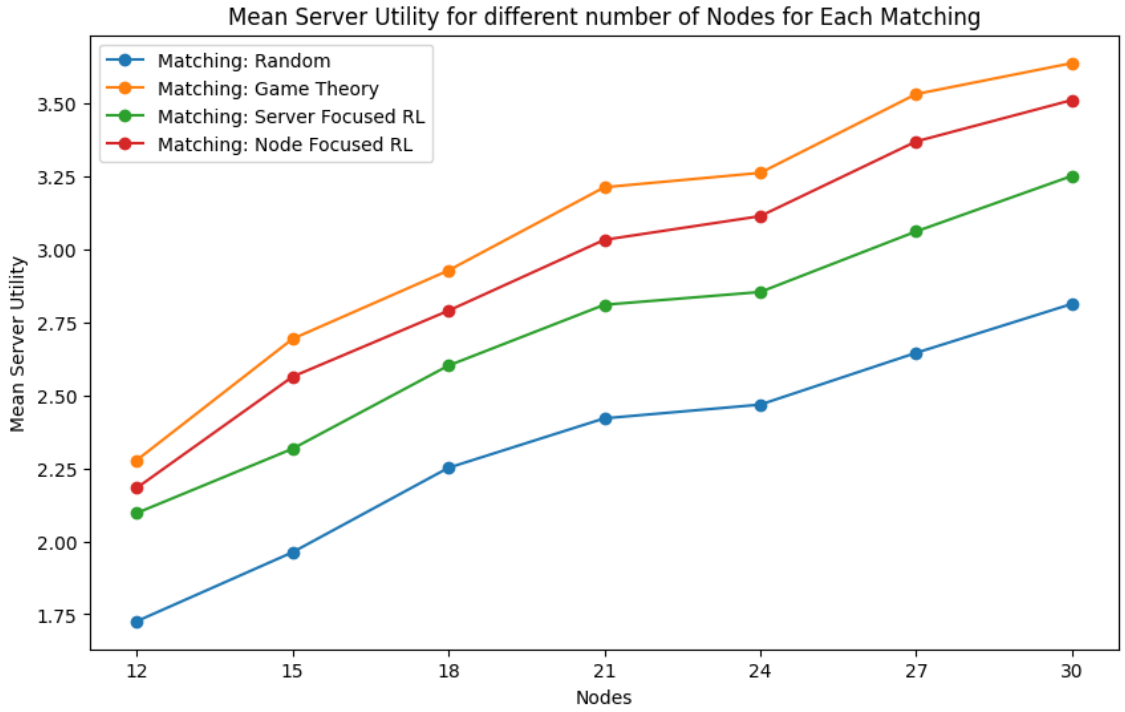


Σχήμα 3.3: Μέση ποιότητα δεδομένων ανά αριθμό κόμβων ανά αλγόριθμο αντιστοίχισης



Σχήμα 3.4: Μέση χρησιμότητα κόμβων ανά αριθμό κόμβων ανά αλγόριθμο αντιστοίχισης

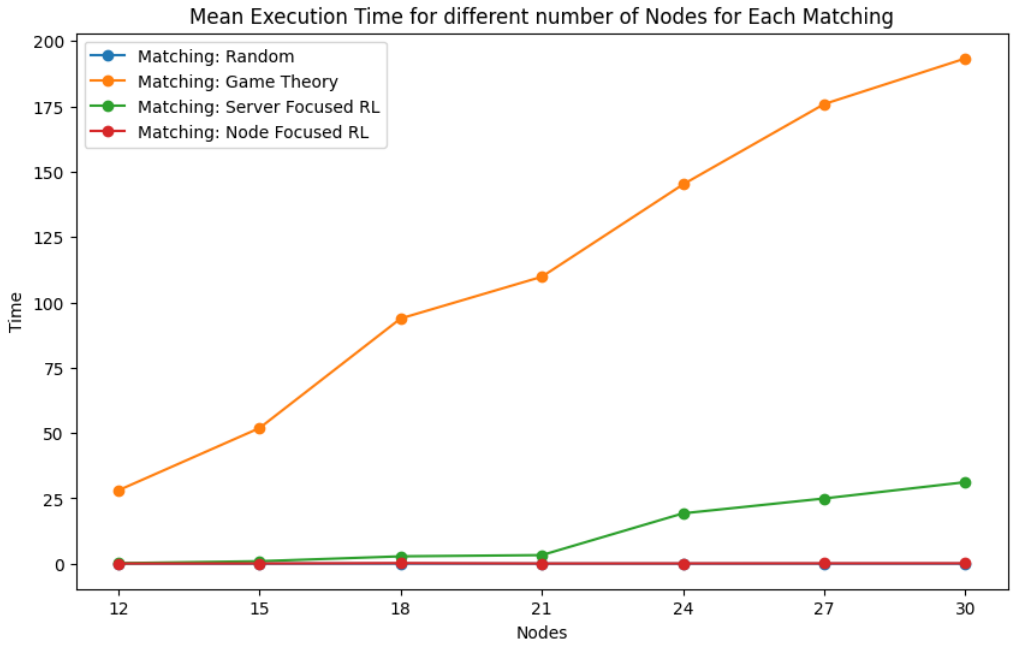
Αντίστοιχα στο διάγραμμα 3.4, παίρνοντας μετρήσεις για την μέση χρησιμότητα των κόμβων, αυτή σταδιακά μειώνεται όσο ο αριθμός των κόμβων αυξάνεται, επειδή και πάλι έχουμε ανταγωνισμό μεταξύ τους. Σε αυτή τη μέτρηση, ο αλγόριθμος Θεωρίας Παιγνίων πετυχαίνει το καλύτερο αποτέλεσμα, ακολουθούμενος από τους αλγορίθμους Ενισχυτικής Μάθησης και τέλος από την Τυχαία Αντιστοίχιση.



Σχήμα 3.5: Μέση χρησιμότητα εξυπηρετητών ανά αριθμό κόμβων ανά αλγόριθμο αντιστοίχισης

Αντίθετα στο διάγραμμα 3.5, η μέση χρησιμότητα των εξυπηρετητών αυξάνεται όσο περισσότεροι κόμβοι εισέρχονται στο σύστημά μας, αφού κάθε συμμαχία διαθέτει περισσότερους κόμβους και άρα περισσότερη πληροφορία. Ο αλγόριθμος Θεωρίας Παιγνίων και εδώ φαίνεται να κάνει τις καλύτερες αντιστοιχίσεις.

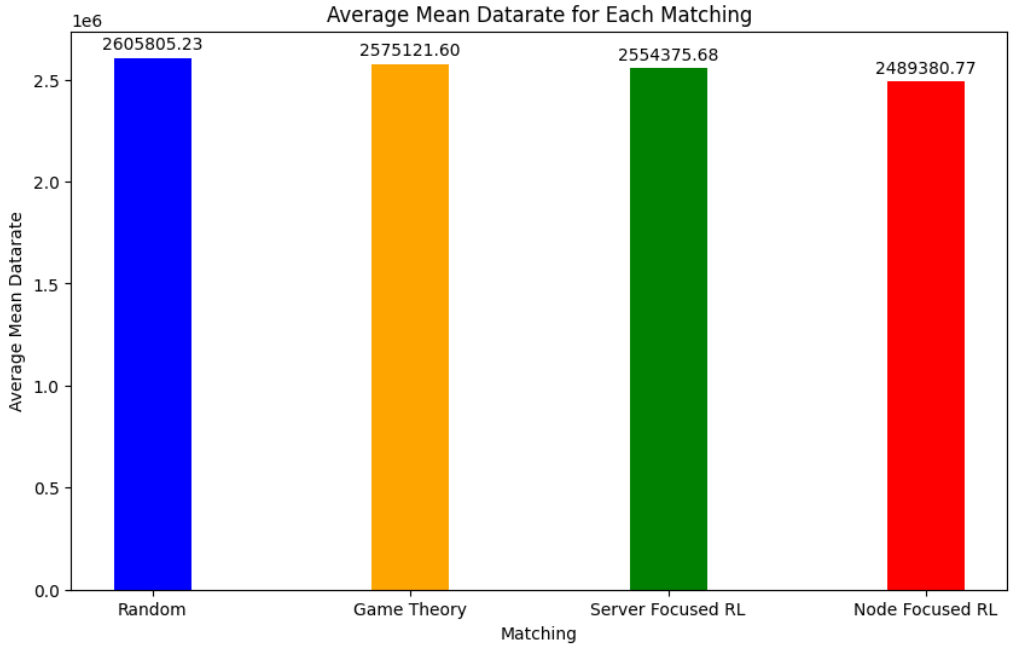
Προφανώς όσο περισσότερους κόμβους έχουμε στο σύστημά μας τόσο πιο δύσκολο θα είναι για τους αλγορίθμους μας να κάνουν την αντιστοίχισή τους στους εξυπηρετητές. Βλέποντας τα δεδομένα στο διάγραμμα 3.6, ο πιο γρήγορος αλγόριθμος είναι ο αλγόριθμος Τυχαίας Αντιστοίχισης, αφού είναι και ο πιο απλός. Από τους υπόλοιπους, ο αλγόριθμος Θεωρίας Παιγνίων επιτυγχάνει την πιο αργή αντιστοίχιση, ακολουθούμενος από τους Αλγορίθμους Ενισχυτικής Μάθησης. Είναι αξιοσημείωτο πως ο αλγόριθμος Ενισχυτικής Μάθησης με βάση την χρησιμότητα κόμβων, πετυχαίνει ταχύτατες αντιστοιχίσεις, σε χρόνο πολύ κοντά σε αυτόν της Τυχαίας Αντιστοίχισης.



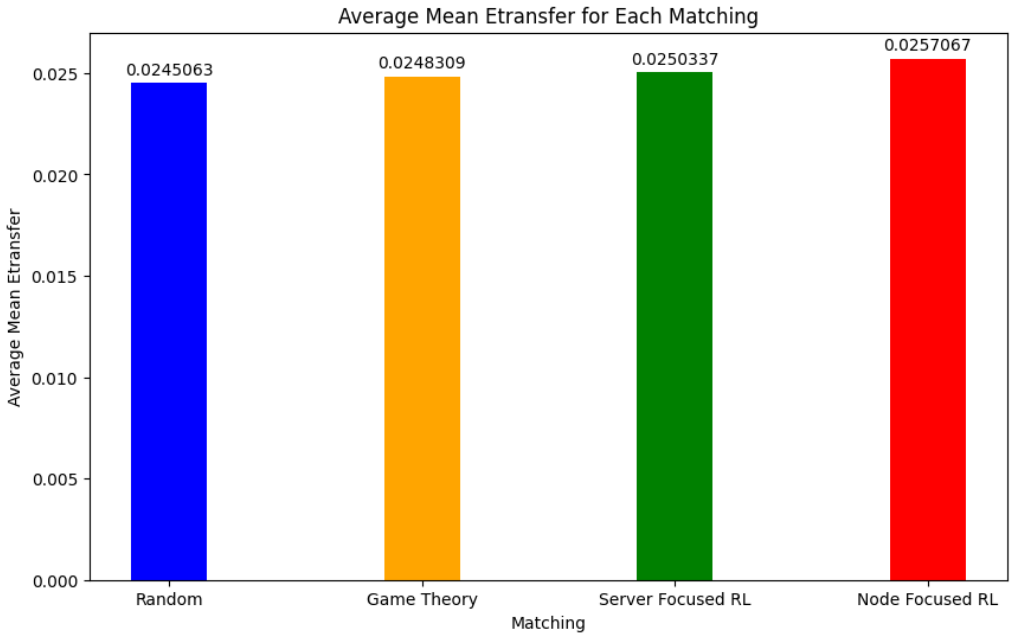
Σχήμα 3.6: Μέσος χρόνος εκτέλεσης ανά αριθμό κόμβων ανά αλγόριθμο αντιστοίχισης

Παρακάτω παρουσιάζουμε τις συνολικές διαφορές σε όλα τα πειράματα που έγιναν μεταξύ των διάφορων αλγορίθμων.

Όπως φαίνεται στο διάγραμμα 3.7 η Τυχαία Αντιστοίχιση πετυχαίνει κατά μέσο όρο το καλύτερο αποτέλεσμα όσον αφορά τη ροή δεδομένων από τους κόμβους στους εξυπηρετητές. Ελάχιστα χειρότερα αποτελέσματα πετυχαίνουν οι υπόλοιποι αλγόριθμοι με τον αλγόριθμο Θεωρίας Παιγνίων να ξεχωρίζει από αυτούς.

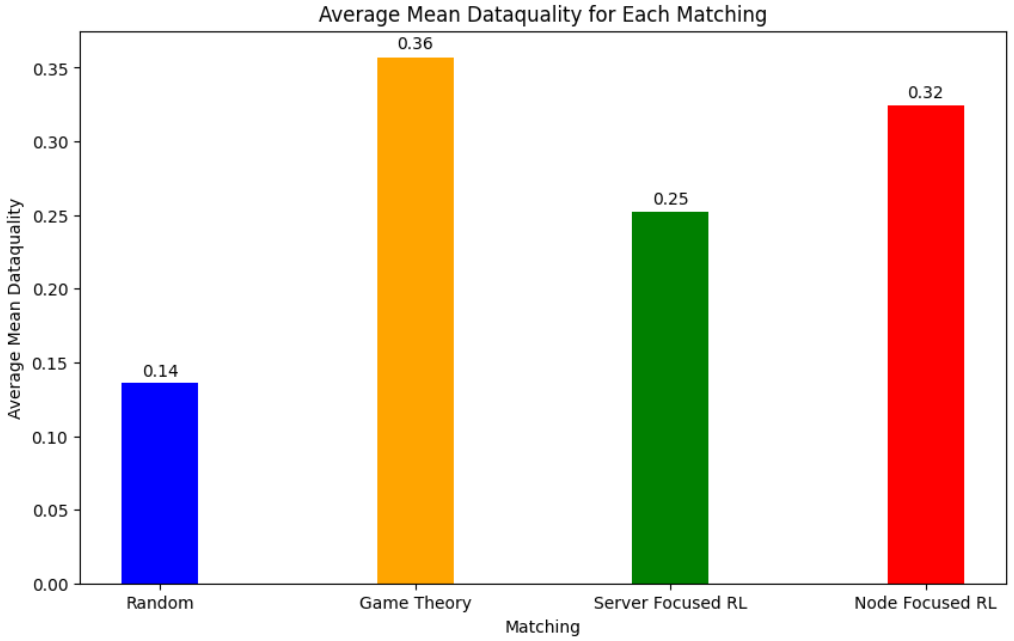


Σχήμα 3.7: Μέση ροή δεδομένων ανά αλγόριθμο αντιστοίχισης



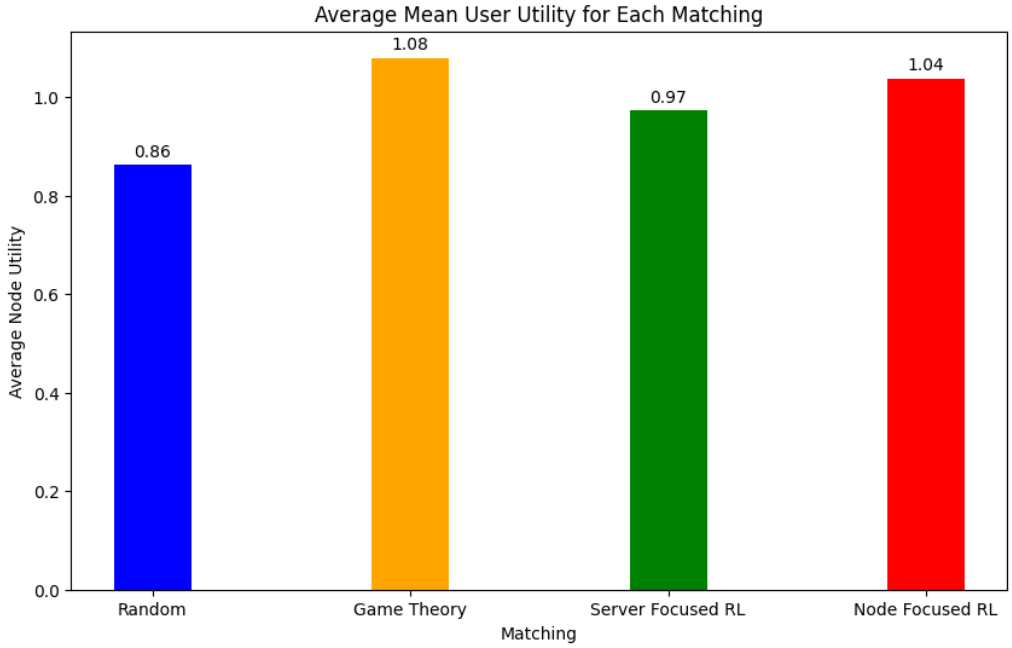
Σχήμα 3.8: Μέση ενέργεια μετάδοσης ανά αλγόριθμο αντιστοίχισης

Στο διάγραμμα 3.8 βλέπουμε τις επιδόσεις των αλγορίθμων αναφορικά με τη μέση ενέργεια μετάδοσης που απαιτείται για την αποστολή των παραμέτρων των τοπικών μοντέλων στους εξυπηρετητές. Η Τυχαία Αντιστοίχιση, έχοντας εξασφαλίσει την ταχύτερη κατά μέσο όρο ροή δεδομένων, πετυχαίνει την μικρότερη ενέργεια μετάδοσης, με τον αλγόριθμο Θεωρίας Παιγνίων να ακολουθεί και τέλος τους αλγορίθμους Ενισχυτικής Μάθησης. Παρ' όλα ταύτα, όλοι οι αλγόριθμοι είναι πολύ κοντά σε τιμές.

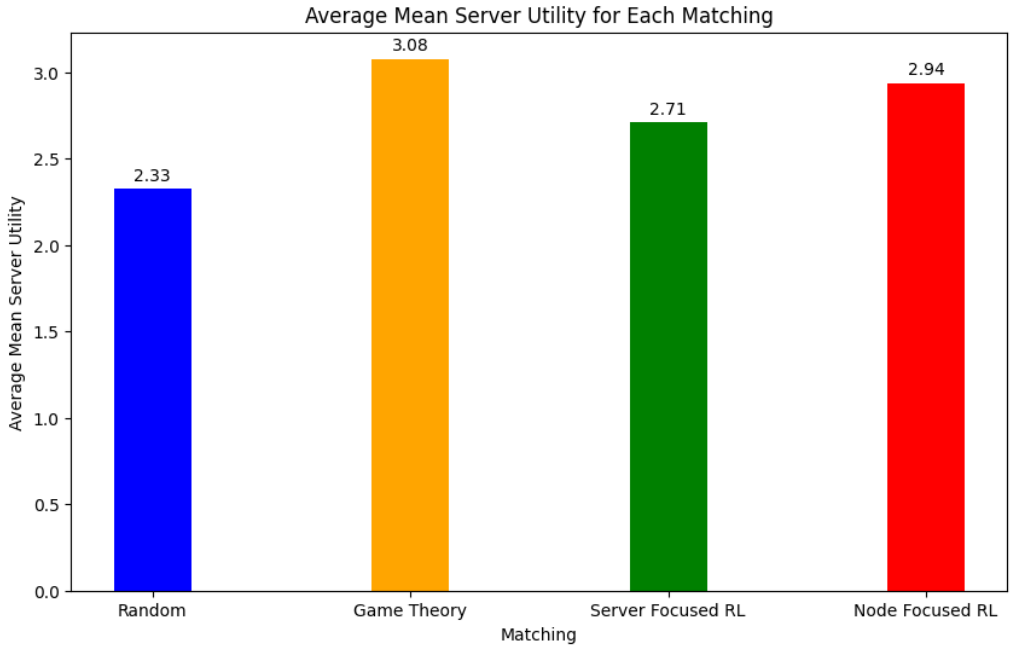


Σχήμα 3.9: Μέση ποιότητα δεδομένων ανά αλγόριθμο αντιστοίχισης

Όσον αφορά την ποιότητα δεδομένων, μπορούμε να δούμε το καθαρό μειονέκτημα της Τυχαίας Αντιστοίχισης, η οποία πετυχαίνει πολύ χειρότερα αποτελέσματα από τους υπόλοιπους αλγορίθμους. Ο αλγόριθμος Θεωρίας Παιγνίων υπερέχει των υπολοίπων, ακολουθούμενος από τον αλγόριθμο Ενισχυτικής Μάθησης ως προς τη χρησιμότητα κόμβων.



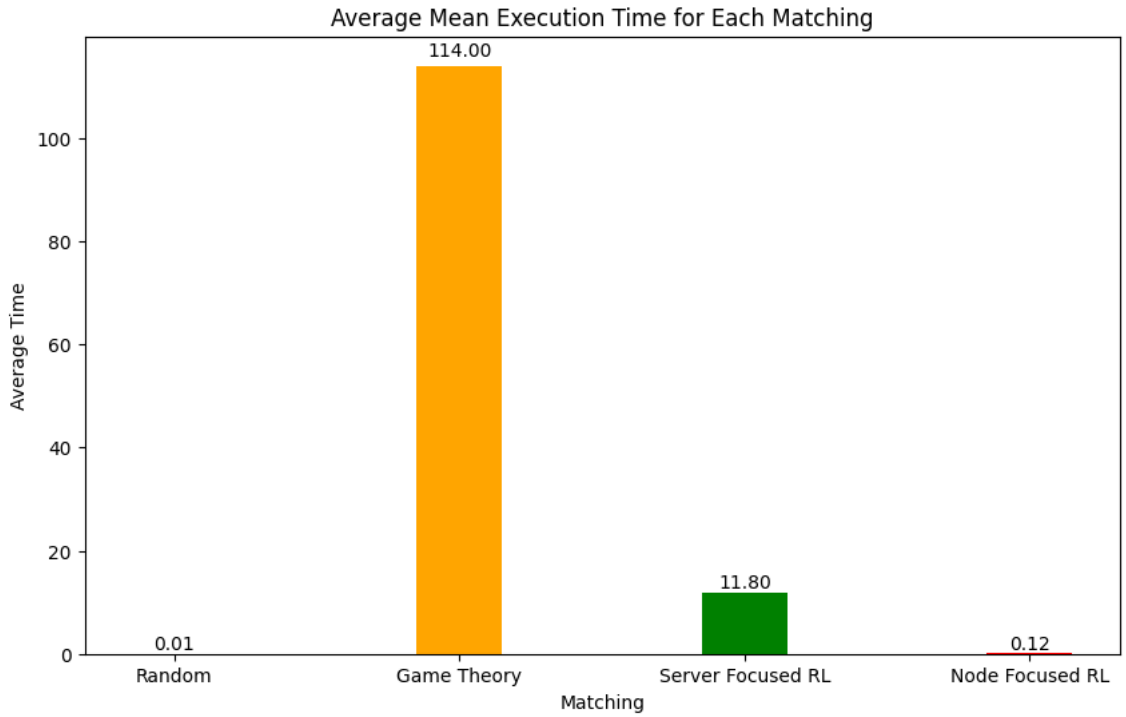
Σχήμα 3.10: Μέση χρησιμότητα κόμβων ανά αλγόριθμο αντιστοίχισης



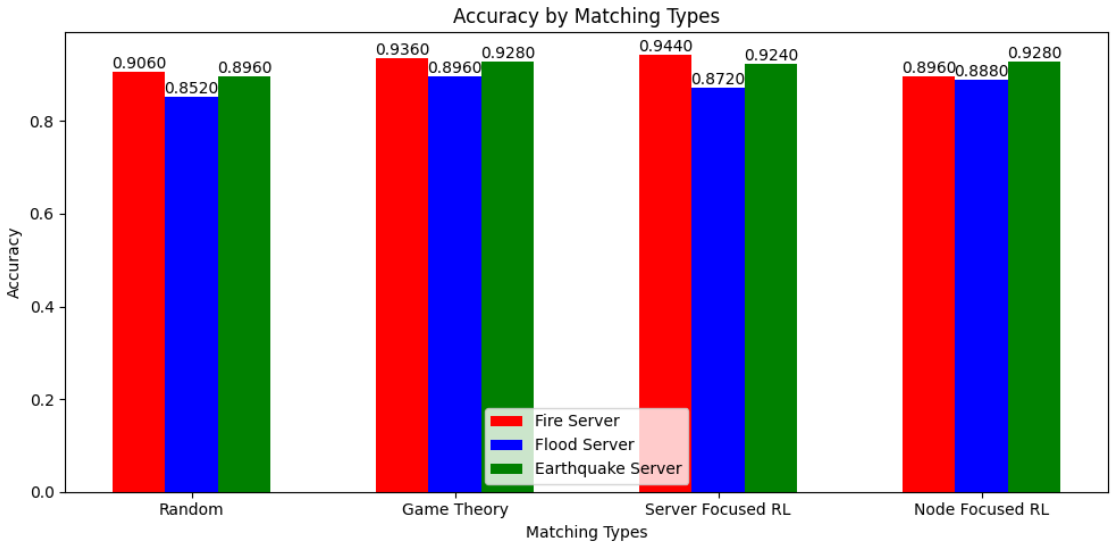
Σχήμα 3.11: Μέση χρησιμότητα εξυπηρετητών ανά αλγόριθμο αντιστοίχισης

Αντίστοιχα στα διαγράμματα 3.10 και 3.11, μπορούμε να δούμε πώς ο αλγόριθμος Θεωρίας Παιγνίων έχει την καλύτερη επίδοση όσον αφορά τις χρησιμότητες κόμβων και εξυπηρετητών. Με σειρά ακολουθούν ο αλγόριθμος Ενισχυτικής Μάθησης ως προς χρησιμότητα κόμβων, ο αλγόριθμος Ενισχυτικής Μάθησης ως προς χρησιμότητα εξυπηρετητών και τέλος η Τυχαία Αντιστοίχιση. Η σύγκριση στα δύο αυτά διαγράμματα αποτελεί ίσως την πιο σημαντική σύγκριση, αφού όλες οι αποφάσεις για την αντιστοίχιση παίρνονται ώστε να μεγιστοποιηθούν οι χρησιμότητες. Έτσι εδώ φαίνεται ξεκάθαρα η υπεροχή του αλγορίθμου Θεωρίας Παιγνίων έναντι των υπολοίπων.

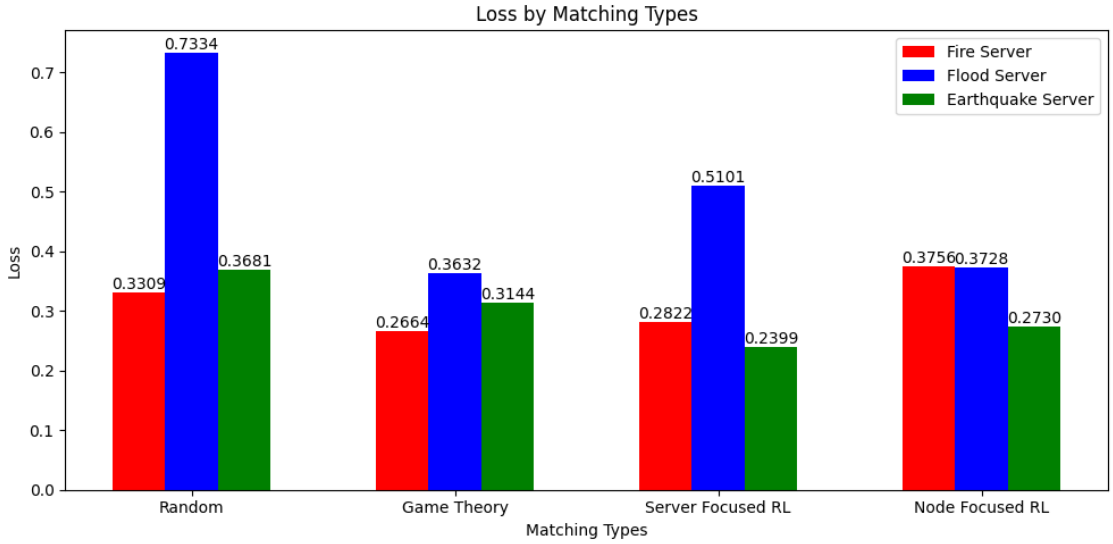
Όσον αφορά τον χρόνο εκτέλεσης της αντιστοίχισης για τους αλγορίθμους μας,στο διάγραμμα 3.12 βλέπουμε πως η Τυχαία Αντιστοίχιση προφανώς διαθέτει τον πιο γρήγορο μηχανισμό, ακολουθούμενη από τον αλγόριθμο Ενισχυτικής Μάθησης ως προς χρησιμότητα κόμβων.



Σχήμα 3.12: Μέσος χρόνος εκτέλεσης ανά αλγόριθμο αντιστοίχισης



Σχήμα 3.13: Μέση ακρίβεια εξυπηρετητών (ανά καταστροφή) για κάθε αλγόριθμο αντιστοίχισης



Σχήμα 3.14: Μέση απώλεια εξυπηρετητών (ανά καταστροφή) για κάθε αλγόριθμο αντιστοίχισης

Για την επίδοση των αλγορίθμων αντιστοίχισης ως προς την Ομοσπονδιακή Μάθηση, θα πρέπει να εξετάσουμε την ακρίβεια και την απώλεια που πετυχαίνουν, όπως αυτές φαίνονται στα διαγράμματα 3.13 και 3.14. Ο αλγόριθμος Θεωρίας Παιγνίων καταφέρνει κατά μέσο όρο να έχει την μικρότερη απώλεια στους τρεις εξυπηρετητές του, ακολουθούμενος από τους αλγορίθμους Ενισχυτικής Μάθησης. Είναι αξιοσημείωτο πως η Τυχαία Αντιστοίχιση παραμένει σχετικά κοντά στους αλγορίθμους μας, παρότι είναι το σημείο αναφοράς μας. Αυτό συμβαίνει επειδή στη διαδικασία της Ομοσπονδιακής Μάθησης συμπεριλαμβάνουμε έναν μηχανισμό ανάθεσης βαρών στους κόμβους μας, ανάλογα με την πληροφορία που διαθέτουν για τον εξυπηρετητή που έχουν συνδεθεί. Έτσι, κόμβοι με λίγη (ή και καθόλου χρήσιμη) πληροφορία θα επηρεάσουν πολύ λίγο την εκμάθηση του μοντέλου. Σε συνδυασμό με την πληροφορία που διαθέτει ο κάθε εξυπηρετητής, η Τυχαία Αντιστοίχιση επιτυγχάνει σεβαστές επιδόσεις παρά την απλότητα της.

4

Αντιστοίχιση με Αλγορίθμους Μετανοητικής Μάθησης

Σε αυτό το κεφάλαιο της διπλωματικής εργασίας θα μελετήσουμε έναν αλγόριθμο Μετανοητικής Μάθησης και θα τον συγκρίνουμε με τον αλγόριθμο Θεωρίας Παιγνίων που αναπτύξαμε στο κεφάλαιο 2. Η Μετανοητική Μάθηση (Regret Learning) είναι μια έννοια που βασίζεται στη θεωρία παιγνίων και τη μηχανική μάθηση, ιδιαίτερα σημαντική στο πλαίσιο των επαναλαμβανόμενων παιγνίων και της ενεργής μάθησης. Εστιάζει στην ελαχιστοποίηση της ενοχής (μετάνοια), ορισμένης ως η διαφορά μεταξύ της απόδοσης μιας στρατηγικής λήψης αποφάσεων και της βέλτιστης στρατηγικής με βάση την αναδρομική θεώρηση, σε επαναλαμβανόμενες αλληλεπιδράσεις ή επαναλήψεις. [Blu03]

Υπάρχουν δύο κύριοι τύποι ενοχής: η εξωτερική ενοχή, η οποία μετράει πόσο χειρότερα απέδωσε μια στρατηγική σε σύγκριση με την καλύτερη σταθερή δράση με βάση την αναδρομική θεώρηση, και η εσωτερική ενοχή, η οποία συγκρίνει την απόδοση με την καλύτερη προσαρμοστική πολιτική, όπου ο παίκτης θα μπορούσε να αλλάξει δράσεις με βάση τα προηγούμενα αποτελέσματα. Αλγόριθμοι ελαχιστοποίησης της ενοχής σχεδιάζονται για να ενημερώνουν τις πιθανότητες των δράσεων με βάση τις προηγούμενες αποδόσεις, ώστε να ελαχιστοποιήσουν την ενοχή. Αυτοί οι αλγόριθμοι έχουν εφαρμογές σε διάφορους τομείς. Για παράδειγμα στην ενεργή μάθηση, όπου βοηθούν τους αλγορίθμους να μαθαίνουν από διαδοχικά δεδομένα σε αντίπαλα περιβάλλοντα. Επιπλέον στη θεωρία παιγνίων, ιδιαίτερα σε επαναλαμβανόμενα παίγνια όπου οι παίκτες προσαρμόζουν τις στρατηγικές τους με βάση τα προηγούμενα αποτελέσματα, και στη μάθηση με ενίσχυση, όπου οι παίκτες μαθαίνουν πολιτικές για τη μεγιστοποίηση των ανταμοιβών με την πάροδο του χρόνου. [Blu03]

Τα οφέλη της Μετανοητικής Μάθησης περιλαμβάνουν την προσαρμοστικότητα, καθώς οι αλγόριθμοι μπορούν να προσαρμοστούν σε μεταβαλλόμενα περιβάλλοντα και να αποδώσουν καλά υπό διάφορες συνθήκες, και τη στιβαρότητα, που τους επιτρέπει να αντιμετωπίζουν ανταγωνιστικές καταστάσεις όπου οι αντίπαλοι μπορεί να προσπαθήσουν να εκμεταλλευτούν αδυναμίες ([Xu+24], [Abr15]). Τα θεωρητικά θεμέλια της ελαχιστοποίησης της ενοχής περιλαμβάνουν τη θεωρία πιθανοτήτων, την κυρτή ανάλυση και τη βελτιστοποίηση, με βασικά αποτελέσματα που συχνά παρέχουν όρια στην ενοχή που μπορεί να επιτευχθεί από συγκεκριμένους αλγόριθμους. Συνολικά, η μάθηση με βάση την ενοχή προσφέρει ένα στιβαρό πλαίσιο για τη λήψη αποφάσεων σε αβέβαια και ανταγωνιστικά περιβάλλοντα, διασφαλίζοντας ότι οι στρατηγικές αποδίδουν βέλτιστα

με την πάροδο του χρόνου, ελαχιστοποιώντας το χάσμα μεταξύ της πραγματικής και της ιδανικής απόδοσης.

Μέχρι τώρα μελετούσαμε το πως θα πρέπει να κατανεμηθούν οι κόμβοι στους εξυπηρετητές για να επιτύχουμε το καλύτερο δυνατό αποτέλεσμα στην Ομοσπονδιακή Μάθηση. Στο κομμάτι που ακολουθεί, αυξάνουμε το χώρο ενεργειών του κάθε κόμβου, δηλαδή του επιτρέπουμε να αλλάξει τιμές στα βασικά του μεγέθη επιλέγοντας πόσους πόρους θα θέλει ο ίδιος να διαθέσει για την Ομοσπονδιακή Μάθηση. Παρακάτω θα δούμε και πιο αναλυτικά τις παραμέτρους τις οποίες ο κάθε κόμβος μπορεί να μεταβάλλει για το συμφέρον του. Πολυδιάστατα, σαν αυτό, προβλήματα αυξάνουν πολύ σε πολυπλοκότητα όσο αυξάνεται και ο χώρος καταστάσεων που μπορούμε να έχουμε. Όμως, μπορούν να μας δώσουν και μεγάλα κέρδη σε χρησιμότητα, αφού εκ' φύσεως ο κάθε κόμβος έχει διαφορετικές βλέψεις και συμφέροντα σε ένα περιβάλλον Ομοσπονδιακής Μάθησης.

4.1 Περιγραφή Αλγορίθμου Μετανοητικής Μάθησης

Όπως αναφέραμε, πλέον κάθε κόμβος μπορεί να ελέγχει σε μεγαλύτερο βαθμό την συμπεριφορά του εντός του οικοσυστήματος. Συγκεκριμένα, μπορεί να προσαρμόζει τους διαθέσιμους πόρους του για να μεγιστοποιήσει το όφελος του, δηλαδή να αλλάξει την ισχύ μετάδοσης $P_{n,s}$, την συχνότητα του ρολογιού της ΚΜΕ του f_n και το μέγεθος του συνόλου δεδομένων που θα διαθέσει στην μάθηση D_n.

Για να μοντελοποιήσουμε πιο ρεαλιστικά το οικοσύστημά μας, αλλάζουμε λίγο τα εμπλεκόμενα μεγέθη που είδαμε στο κεφάλαιο 2. Έτσι, αντί για ποιότητα δεδομένων d_n, ενσωματώνουμε την παράμετρο D_n στην πληρωμή που λαμβάνει ένας κόμβος από τον εξυπηρετητή. Δηλαδή όσο περισσότερα δεδομένα προσφέρει ένας κόμβος στον εξυπηρετητή του, τόσο καλύτερες απολαβές θα έχει. Αντίστοιχα, ενσωματώνουμε και την παράμετρο f_n στην πληρωμή από τον εξυπηρετητή. Επιπλέον, κάθε κόμβος λαμβάνει απολαβές από τον εξυπηρετητή ανάλογα με τη σημασία του, αφού ένας εξυπηρετητής δεν θα ήθελε να πληρώνει το ίδιο έναν σημαντικό και έναν όχι τόσο σημαντικό κόμβο. Οπότε, με βάση τις παραπάνω παρατηρήσεις, διαμορφώνουμε την κανονικοποιημένη πληρωμή του κόμβου από τον εξυπηρετητή ως:

$$\hat{Pnt}_{n,s} = \frac{c_{n,s} \times current\_fn * ud_n}{max\_f_n \times max\_d_n} \tag{4.1}$$

όπου $c_{n,s}$ η σημασία δεδομένων του κόμβου, $current\_fn$ η τιμή της συχνότητας της ΚΜΕ που επιλέγει ο κόμβος να χρησιμοποιήσει, ud_n το μέγεθος του συνόλου δεδομένου που επιλέγει ο κόμβος να διαθέσει, max_f_n η μέγιστη συχνότητα της ΚΜΕ του κόμβου και max_d_n το μέγιστο σύνολο δεδομένων που διαθέτει ο κόμβος.

Αντίστοιχα για τα υπόλοιπα μεγέθη που μελετήσαμε, τα κανονικοποιούμε με τον ίδιο τρόπο και έχουμε τις παρακάτω εξισώσεις:

$$\hat{R}_{n,s} = \frac{R_{n,s}}{Rmax_{n,s}} \tag{4.2}$$

$$R_{n,s} = B \log_2(1 + \frac{g_{n,s} \times current\_P_{n,s}}{\sum\limits_{n' \in s, n' \neq n} g_{n',s} P_{n',s} + g_{n,s} \times current\_P_{n,s} + I_0}) \quad [bps]$$

$$Rmax_{n,s} = B\log_2(1 + \frac{g_{n,s} \times max\_P_{n,s}}{\sum\limits_{n' \in s, n' \neq n} g_{n',s}P_{n',s} + g_{n,s} \times max\_P_{n,s} + I_0}) \quad [bps]$$

όπου $current\_P_{n,s}$ δηλώνει την ισχύ μετάδοσης που επιλέγει ο κόμβος, $max\_P_{n,s}$ είναι η μέγιστη ισχύ μετάδοσης που μπορεί να διαθέσει ο κόμβος και άρα $R_{n,s}$ είναι ο ρυθμός μετάδοσης που πετυχαίνει ο κόμβος και $Rmax_{n,s}$ είναι ο μέγιστος ρυθμός μετάδοσης που μπορεί να πετύχει ο κόμβος με βάση την τωρινή κατάσταση του συστήματος.

$$\hat{E}_n = \frac{\frac{a_n}{2} q_n \times ud_n \times current\_f_n^2}{\frac{a_n}{2} q_n \times max\_d_n \times max\_f_n^2} = \frac{ud_n \times current\_f_n^2}{max\_d_n \times max\_f_n^2} \tag{4.3}$$

όπου $current\_f_n$ η τιμή της συχνότητας της ΚΜΕ που επιλέγει ο κόμβος να χρησιμοποιήσει, ud_n το μέγεθος του συνόλου δεδομένου που επιλέγει ο κόμβος να διαθέσει, max_f_n η μέγιστη συχνότητα της ΚΜΕ του κόμβου και max_d_n το μέγιστο σύνολο δεδομένων που διαθέτει ο κόμβος.

$$\hat{E}_{n,s} = \frac{\frac{Z(\mathbf{w}n) \times current\_Pn,s}{R_{n,s}}}{\frac{Z(\mathbf{w}n) \times max\_P_{n,s}}{Rmax_{n,s}}} = \frac{current\_P_{n,s} \times Rmax_{n,s}}{max\_P_{n,s} \times R_{n,s}} \tag{4.4}$$

όπου $current\_P_{n,s}$ δηλώνει την ισχύ μετάδοσης που επιλέγει ο κόμβος, $max\_P_{n,s}$ είναι η μέγιστη ισχύ μετάδοσης που μπορεί να διαθέσει ο κόμβος και άρα $R_{n,s}$ είναι ο ρυθμός μετάδοσης που πετυχαίνει ο κόμβος και $Rmax_{n,s}$ είναι ο μέγιστος ρυθμός μετάδοσης που μπορεί να πετύχει ο κόμβος με βάση την τωρινή κατάσταση του συστήματος.

Όπως γίνεται εμφανές από τις παραπάνω εξισώσεις, κάθε μία από τις παραμέτρους $P_{n,s}$, f_n, ud_n, όσο αυξάνονται, αυξάνουν με τη σειρά τους δύο μεγέθη, ένα θετικό και ένα αρνητικό. Επιπλέον, για την παράμετρο $P_{n,s}$ βλέπουμε πως η ισχύς της επηρεάζεται και από εξωτερικές παραμέτρους, δηλαδή από τις επιλογές των υπολοίπων κόμβων.

Συνεπώς θα πρέπει να δημιουργήσουμε μία νέα συνάρτηση χρησιμότητας η οποία θα αντικατοπτρίζει την συμπεριφορά αυτή των μεγεθών, αλλά θα μας επιτρέπει και να μοντελοποιήσουμε την συμπεριφορά των κόμβων μας. Δηλαδή για παράδειγμα, κάποιος κόμβος, γνωρίζοντας την χρησιμότητά του, αν αυτή είναι χαμηλή, μπορεί να τον συμφέρει να αφιερώσει λιγότερους πόρους στην Ομοσπονδιακή Μάθηση, απ' ότι κάποιος κόμβος ο οποίος γνωρίζει πως μπορεί να επωφεληθεί από την διαδικασία. Έτσι ορίζουμε ως νέα συνάρτηση χρησιμότητας για μια παράμετρο την:

$$Uparameter_{n,s}(pos, neg) = positive(pos, c_{n,s}, a) - negative(neg, a) \tag{4.5}$$

$$positive(pos, c_{n,s}, a) = 2c_{n,s} + 1 - e^{(\frac{-pos}{a})}$$

$$negative(neg, a) = \frac{1}{1 + e^{(\frac{-neg}{a} + 3)}}$$

όπου pos είναι το κανονικοποιημένο θετικό μέγεθος της παραμέτρου και neg το κανονικοποιημένο αρνητικό μέγεθος της παραμέτρου. Επιπλέον, θέτοντας ως άνω όριο το $2c_{n,s} + 1$ εξασφαλίζουμε καλύτερες τιμές χρησιμότητας για τους πιο σημαντικούς κόμβους, δίνοντας έτσι προτεραιότητα σε

αυτούς. Η παράμετρος a, όπως θα εξηγήσουμε και παρακάτω, μας επιτρέπει να ορίσουμε συγκεκριμένες συμπεριφορές για τους κόμβους μας, προσομοιώνοντας έτσι τις διαφορετικές επιθυμίες και συμφέροντα τους.

Συνεπώς η συνολική συνάρτηση χρησιμότητας είναι:

$$U_{n,s} = U\{P_{n,s}\}_{n,s}(\hat{R_{n,s}}, \hat{E_{n,s}}) + U\{f_n\}_{n,s}(\hat{Pnt}_{n,s}, \hat{E}_n) + U\{ud_n\}_{n,s}(\hat{Pnt}_{n,s}, \hat{E}_n) \quad (4.6)$$

Όπως βλέπουμε τα μεγέθη $\hat{Pnt}_{n,s}$ και $\hat{E}_n$ συμμετέχουν και στην χρησιμότητα της παραμέτρου f_n και στην χρησιμότητα της παραμέτρου ud_n. Για να λύσουμε το πρόβλημα αυτό θα πρέπει να δημιουργήσουμε τέσσερα νέα μεγέθη από τα δύο υπάρχοντα, όπου τα δύο θα αφορούν την παράμετρο f_n και τα άλλα δύο την παράμετρο ud_n. Έτσι έχουμε:

$$\hat{Pnt}\{f_n\}_{n,s} = \frac{c_{n,s} \times current\_f_n}{max\_f_n}$$

$$\hat{Pnt}\{ud_n\}_{n,s} = \frac{c_{n,s} \times ud_n}{max\_d_n}$$

$$\hat{E}\{f_n\}_n = \frac{current\_f_n^2}{max\_f_n^2}$$

$$\hat{E}\{ud_n\}_n = \frac{ud_n}{max\_d_n}$$

Και άρα πλέον η εξίσωση 4.6 μπορεί να γραφεί ως:

$$\begin{aligned} U_{n,s} =& U\{P_{n,s}\}_{n,s}(\hat{R_{n,s}}, \hat{E_{n,s}}) + U\{f_n\}_{n,s}(\hat{Pnt}\{f_n\}_{n,s}, \hat{E}\{f_n\}_n) + \\ & U\{ud_n\}_{n,s}(\hat{Pnt}\{ud_n\}_{n,s}, \hat{E}\{ud_n\}_n) \end{aligned} \quad (4.7)$$

Επιπροσθέτως, θα πρέπει να αναλύσουμε την λογική της παραμέτρου συμπεριφοράς a για τις συναρτήσεις χρησιμότητας των κόμβων. Κάθε συνάρτηση της μορφής 4.5 αποτελεί μία συνάρτηση με μορφή καμπάνας, δηλαδή εμφανίζει ένα ολικό μέγιστο (όχι στο άπειρο). Συγκεκριμένα αν το $a < 0.57$, το μέγιστο αυτό βρίσκεται εντός του $[0, 1]$ που είναι και το διάστημα που μας ενδιαφέρει, αφού οι τιμές των μεγεθών μας είναι κανονικοποιημένες. Όσο μεγαλύτερη είναι η τιμή του a, τόσο πιο δεξιά θα βρίσκεται το μέγιστο και άρα θα ενθαρρύνεται ο κόμβος να αφιερώσει περισσότερους πόρους στην Ομοσπονδιακή Μάθηση για την συγκεκριμένη παράμετρο. Συνεπώς, θα πρέπει για κάθε κόμβου n να δώσουμε για κάθε μία από τις παραμέτρους του μία κατάλληλη παράμετρο συμπεριφοράς a με βάση την νοοτροπία του κόμβου, δηλαδή αν πιστεύει πως μπορεί να επωφεληθεί πολύ ή λίγο από την Ομοσπονδιακή Μάθηση και τον κάθε εξυπηρετητή. Άρα αναθέτουμε τις παραμέτρους συμπεριφοράς με τον εξής τρόπο:

$$a\{P_{n,s}\} = \text{random.uniform}\left(\max\left(a_1 \times c_{n,s} - a_3, a_3\right), a_1 \times c_{n,s}\right)$$

$$a\{f_n\} = \text{random.uniform}\left(\max\left(a_2 \times \sqrt{c_{n,s}} - a_3, a_3\right), a_2 \times \sqrt{c_{n,s}}\right)$$

$$a\{ud_n\} = \text{random.uniform}\left(\max\left(a_2 \times \sqrt{c_{n,s}} - a_3, a_3\right), a_2 \times \sqrt{c_{n,s}}\right)$$

Με την κατανομή αυτή εξασφαλίζουμε πως οι κόμβους που έχουν να κερδίζουν περισσότερα από τους εξυπηρετητές (μεγαλύτερη σημασία δεδομένων) θα προτιμούν να αφιερώσουν μεγαλύτερο μέρος των διαθέσιμων πόρων τους, σε αντίθεση με τους λιγότερο σημαντικούς κόμβους, οι οποίοι γνωρίζουν πως δεν μπορούν να επωφεληθούν πολύ από την όλη διαδικασία και άρα είναι πιο διστακτικοί.

Αφού, λοιπόν, ορίσαμε την νέα συνάρτηση χρησιμότητας και τις παραμέτρους της μπορούμε να προχωρήσουμε στην ανάλυση και περιγραφή των αλγορίθμων που θα χρησιμοποιήσουμε. Θα μελετήσουμε τους εξής δύο αλγορίθμους: i) Μετανοητική Μάθηση Πλήρους Πληροφορίας ii) Μετανοητική Μάθηση Ελλιπούς Πληροφορίας. Ο πρώτος αλγόριθμος, έχοντας πλήρη γνώση των ενεργειών των υπολοίπων κόμβων εκμεταλλεύεται την γνώση αυτή για να εντοπίσει τις βέλτιστες σε κάθε περίπτωση ενέργειες. Ο δεύτερος αλγόριθμος αντιπροσωπεύει ένα πιο ρεαλιστικό σενάριο, όπου ο κάθε κόμβος λαμβάνει την δική του ανατροφοδότηση, αλλά δεν γνωρίζει για τις ενέργειες των υπολοίπων κόμβων.

Οι αλγόριθμοι που ακολουθούν είναι βασισμένοι στο άρθρο των Samarakoon et al. ([Sam+13]), με προσαρμογές στο δικό μας περιβάλλον και αλλαγές στις παραμέτρους των αλγορίθμων.

Πλήρους Πληροφορίας (Complete Information - CI): Αρχικά, κατασκευάζουμε όλες τις πιθανές καταστάσεις που μπορεί να βρίσκεται ένας κόμβος, δηλαδή για κάθε εξυπηρετητή, για κάθε τιμή κάθε παραμέτρου. Αυτός είναι ο χώρος ενεργειών μας. Στην συνέχεια, αρχικοποιούμε το διάνυσμα πιθανοτήτων έχοντας όλες τις ενέργειες ισοπίθανες και το διάνυσμα μετάνοιας σε μηδενικές τιμές. Έτσι ξεκινάμε επαναληπτικά να ακολουθούμε την εξής διαδικασία: Σε κάθε επανάληψη, οι N κόμβοι μας διαλέγουν ο καθένας, με βάση το διάνυσμα πιθανοτήτων τους, μια ενέργεια. Εκτελούν τη συγκεκριμένη ενέργεια και έπειτα ενημερώνουν το διάνυσμα μετάνοιας τους για κάθε πιθανή ενέργεια με τον παρακάτω τρόπο:

$$\begin{aligned}\text{regret\_vector}(user, action) = (1 - l(t))\,&\text{regret\_vector}(user, action) \\ &+ \text{utility\_difference}(action, taken\_action)\end{aligned} \tag{4.8}$$

$$l(t) = \frac{1}{t}$$

όπου $l(t)$ είναι ο ρυθμός εκμάθησης, δηλαδή δηλώνει πόσο σημαντική είναι η πληροφορία που έχουμε μέχρι τώρα και πόσο οι νέες πληροφορίες που μαθαίνουμε. Επίσης η utility_difference$(action, taken_action)$ μας δίνει την διαφορά σε χρησιμότητα του κόμβου μεταξύ της ενέργειας που μελετάμε και της ενέργειας που εκτελέσαμε στην τελευταία επανάληψη.

Αφού ενημερώσουμε έτσι το διάνυσμα μετάνοιας του κάθε κόμβου, ενημερώνουμε και το διάνυσμα πιθανοτήτων ως εξής:

$$P(u, action) = \begin{cases} 0 & \text{if } S_u = 0 \\ \frac{\max(0, regret\_vector(user, action))}{S_u} & \text{if } S_u > 0 \end{cases} \tag{4.9}$$

$$S_u = \sum_{action \in actions} \max(0, regret\_vector(user, action))$$

Η διαδικασία επαναλαμβάνεται μέχρι να πετύχουμε σύγκλιση, η οποία εξασφαλίζεται εφ' όσον για κάθε κόμβο υπάρχει μία ενέργεια η οποία επιλέγεται με πιθανότητα άνω του 50%. Σε τέτοια

περίπτωση σταματάμε την διαδικασία και επιλέγουμε για κάθε κόμβο την πιθανότερη ενέργειά του καταλήγοντας στο τελικό μας αποτέλεσμα.

Algorithm 6 Αλγόριθμος Μετανοητική Μάθησης Πλήρους Πληροφορίας

1: **Είσοδος:** $L_n, a_n, q_n, D_n, f_n, \mathbf{w}_n \forall n \in \mathcal{N}, L_k \forall k \in \mathcal{K}$, παράμετροι συμπεριφοράς
2: **Έξοδος:** Αποτελέσματα Αντιστοίχισης και Ενεργειών M
3: **Αρχικοποίηση:** $\forall n$ δημιουργούμε όλες τις πιθανές ενέργειες του, $\forall n, \forall actions$ αρχικοποιούμε τα διανύσματα μετάνοιας σε μηδενικές τιμές και τα διανύσματα πιθανότητας σε ίσες τιμές
4: **while** no convergence **do**
5: **for** $n \in \mathcal{N}$ **do**
6: Ο κόμβος n επιλέγει με βαρύτητα το διάνυσμα πιθανοτήτων του μια ενέργεια και την εκτελεί.
7: **end for**
8: **for** $n \in \mathcal{N}$ **do**
9: Ο κόμβος n ανανεώνει με βάση την Εξίσωση 4.8 το διάνυσμα μετανοιών του.
10: Ο κόμβος n ανανεώνει με βάση την Εξίσωση 4.9 το διάνυσμα πιθανοτήτων του.
11: **end for**
12: **end while**
13: **for** $n \in \mathcal{N}$ **do**
14: Ο κόμβος n επιλέγει και εκτελεί την πιο πιθανή ενέργειά του.
15: **end for**

Ελλιπούς Πληροφορίας (Incomplete Information - II): Αρχικά κατασκευάζουμε και πάλι τον χώρο ενεργειών. Στην συνέχεια, αρχικοποιούμε το διάνυσμα πιθανοτήτων έχοντας όλες τις ενέργειες ισοπίθανες, το διάνυσμα μετάνοιας σε μηδενικές τιμές και το διάνυσμα χρησιμότητας στις αντίστοιχες τιμές χρησιμότητας χωρίς εξωτερικότητα. Έτσι ξεκινάμε επαναληπτικά να ακολουθούμε την εξής διαδικασία: Σε κάθε επανάληψη, οι N κόμβοι μας διαλέγουν ο καθένας, με βάση το διάνυσμα πιθανοτήτων τους, μια ενέργεια. Εκτελούν τη συγκεκριμένη ενέργεια και έπειτα ενημερώνουν το διάνυσμα χρησιμότητάς τους για τη συγκεκριμένη ενέργεια με τον παρακάτω τρόπο:

$$\text{utilities\_vector}(u, action\_taken) = 0.5 \times (\text{current\_utility} + \text{utilities\_vector}(u, action\_taken)) \tag{4.10}$$

όπου το current_utility αναφέρεται στην χρησιμότητα που έλαβε ο κόμβος n εκτελώντας την τελευταία ενέργεια που επέλεξε. Στη συνέχεια ενημερώνουμε το διάνυσμα μετάνοιας του κόμβου για κάθε πιθανή ενέργεια ως:

$$\begin{aligned} \text{regret\_vector}(user, action) = (1 - l(t))\, &\text{regret\_vector}(user, action) \\ &+ \text{current\_utility} - \text{utilities\_vector}(u, action) \end{aligned} \tag{4.11}$$

$$l(t) = \frac{1}{t}$$

όπου το current_utility αναφέρεται στην χρησιμότητα που έλαβε ο κόμβος n εκτελώντας την τελευταία ενέργεια που επέλεξε. Τέλος ενημερώνουμε το διάνυσμα πιθανοτήτων ως:

$$\text{probabilities}(u, action) = \text{boltzmann\_gibbs\_vector}_u(action) \tag{4.12}$$

$$\text{boltzmann\_gibbs\_vector}_u(action) = \frac{e^{\max(0, regret\_vector(user, action))/k_m}}{S_u}$$

$$S_u = \sum_{action \in actions} \max(0, e^{\max(0, regret\_vector(user, action))/k_m})$$

Όπως και προηγουμένως, διαδικασία επαναλαμβάνεται μέχρι να πετύχουμε σύγκλιση, η οποία εξασφαλίζεται εφ' όσον για κάθε κόμβο υπάρχει μία ενέργεια η οποία επιλέγεται με πιθανότητα άνω του 50%. Σε τέτοια περίπτωση σταματάμε την διαδικασία και επιλέγουμε για κάθε κόμβο την πιθανότερη ενέργειά του καταλήγοντας στο τελικό μας αποτέλεσμα.

Algorithm 7 Αλγόριθμος Μετανοητική Μάθησης Ελλιπούς Πληροφορίας

1: **Είσοδος:** $L_n, a_n, q_n, D_n, f_n, \mathbf{w}_n \forall n \in \mathcal{N}, L_k \forall k \in \mathcal{K}$, παράμετροι συμπεριφοράς
2: **Έξοδος:** Αποτελέσματα Αντιστοίχισης και Ενεργειών M
3: **Αρχικοποίηση:** $\forall n$ δημιουργούμε όλες τις πιθανές ενέργειες του, $\forall n, \forall actions$ αρχικοποιούμε τα διανύσματα χρησιμότητας σε αντίστοιχες τιμές χρησιμότητας χωρίς εξωτερικότητα, τα διανύσματα μετάνοιας σε μηδενικές τιμές και τα διανύσματα πιθανότητας σε ίσες τιμές
4: **while** no convergence **do**
5: **for** $n \in \mathcal{N}$ **do**
6: Ο κόμβος n επιλέγει με βαρύτητα το διάνυσμα πιθανοτήτων του μια ενέργεια και την εκτελεί.
7: **end for**
8: **for** $n \in \mathcal{N}$ **do**
9: Ο κόμβος n ανανεώνει με βάση την Εξίσωση 4.10 την τιμή τους διανύσματος χρησιμότητας για την συγκεκριμένη ενέργεια.
10: Ο κόμβος n ανανεώνει με βάση την Εξίσωση 4.11 το διάνυσμα μετανοιών του.
11: Ο κόμβος n ανανεώνει με βάση την Εξίσωση 4.12 το διάνυσμα πιθανοτήτων του.
12: **end for**
13: **end while**
14: **for** $n \in \mathcal{N}$ **do**
15: Ο κόμβος n επιλέγει και εκτελεί την πιο πιθανή ενέργειά του.
16: **end for**

Σύγκλιση: Οι συγγραφείς του [Sam+13] δηλώνουν πως για τον αλγόριθμο Πλήρους Πληροφορίας, θα επιτευχθεί η σύγκλιση εφόσον ακολουθηθεί η διαδικασία της Μετανοητικής Μάθησης. Για τον αλγόριθμο Ελλιπούς Πληροφορίας, αναφέρουν πως για να επιτευχθεί η σύγκλιση όπως στον αλγόριθμο Πλήρους Πληροφορίας, θα πρέπει η συνάρτηση χρησιμότητας U να αποτελεί συνάρτηση Lipschitz. Συγκεκριμένα, στην περίπτωσή μας, μας αφορούν οι συναρτήσεις:

$$f(x) = 2 \cdot c_{n,s} + 1 - e^{-\frac{x}{a}}, \quad g(x) = \frac{1}{1 + e^{-\frac{x}{a}+3}}$$

Μια συνάρτηση είναι Lipschitz, αν και μόνο εάν αυτή έχει φραγμένη παράγωγο. Και οι δύο αυτές συναρτήσεις (και συγκεκριμένα στο $[0, \text{inf})$) έχουν φραγμένη παράγωγο και άρα είναι συναρτήσεις Lipschitz. Επιπλέον, αν έχουμε δύο συναρτήσεις Lipschitz και τις προσθέσουμε (ή αφαιρέσουμε) η νέα συνάρτηση προφανώς θα είναι και αυτή Lipschitz. Συνεπώς, οι συναρτήσεις μας της μορφής 4.5 είναι Lipschitz. Αντίστοιχα, εφαρμόζοντας τον ίδιο κανόνα προκύπτει ότι και η 4.7 θα είναι Lipschitz, εξασφαλίζοντας την ορθή λειτουργία του αλγορίθμου Ελλιπούς Πληροφορίας και την σύγκλισή του.

4.2 Υλοποίηση

Τόσο για τον αλγόριθμο Πλήρους Πληροφορίας όσο και για τον αλγόριθμο Ελλιπούς Πληροφορίας, θα πρέπει όπως και πριν να εξασφαλίσουμε τον ορθό διαμοιρασμό των δεδομένων, με συνεπή τρόπο για να μπορούμε να πάρουμε συγκρίσιμα αποτελέσματα. Αντίστοιχα, και πάλι θα πρέπει να φροντίσουμε οι κόμβοι μας να αποτελούν όμοια αντικείμενα σε κάθε περίπτωση ώστε οι αλγόριθμοι να συγκρίνονται πάνω στο ίδιο περιβάλλον.

Κάθε αντικείμενο κόμβου, θα έχει τρία βασικά χαρακτηριστικά:

- $Ptransmit$: Η ισχύς μετάδοσης που χρησιμοποιείται (W)
- f_n: Οι κύκλοι/δευτερόλεπτο που διαθέτει ο επεξεργαστής
- $used\_datasize$: Το ποσοστό του συνολικού συνόλου δεδομένων που χρησιμοποιεί ο κόμβος για την εκπαίδευση του μοντέλου του

Αυτά προφανώς μεταβάλλονται στους αλγορίθμους Μετανοητικής Μάθησης. Αντίθετα, στον αλγόριθμο Θεωρίας Παιγνίων θέτουμε τις τιμές:

- $Ptransmit = P_{max} = 2Watt$
- $f_n = fn_{max} = 2GHz$
- $used\_datasize = 1$

οι οποίες μένουν οριστικά και δεν αλλάζουν στον συγκεκριμένο αλγόριθμο.

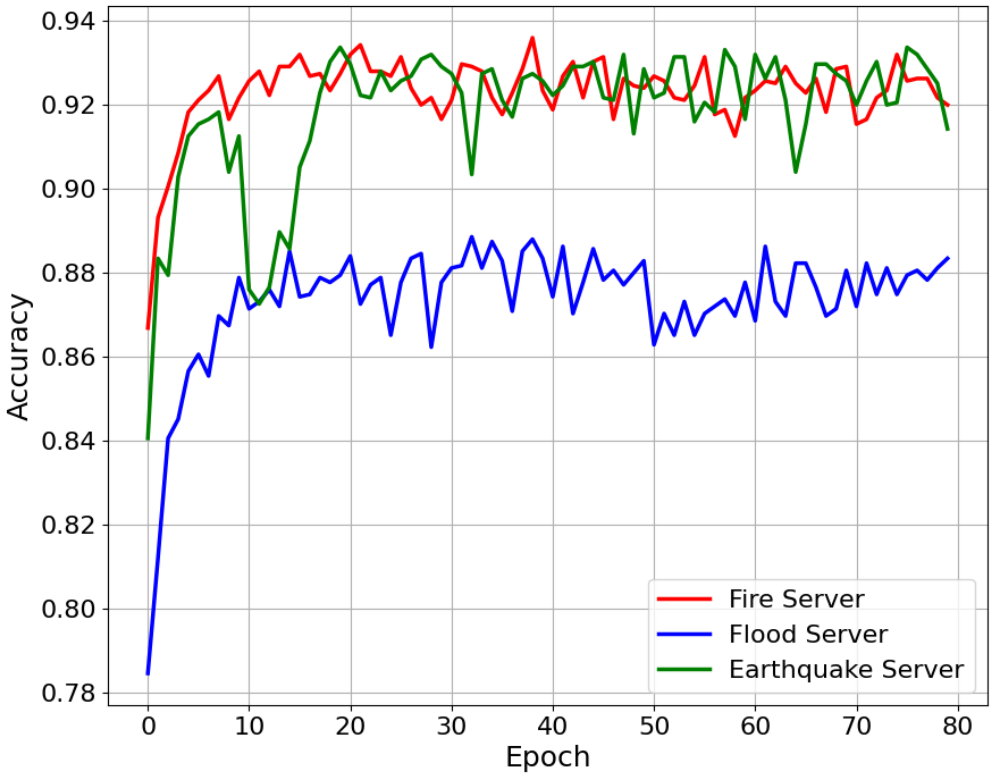
Τέλος, όπως είδαμε παραπάνω (Εξίσωση 4.5), κάθε ένα ζευγάρι κόμβου-εξυπηρετητή, δημιουργεί τρεις συναρτήσεις χρησιμότητας με βάση την χρησιμότητά του και μια παράμετρο α, η οποία επίσης εξαρτάται επίσης από τη χρησιμότητά του. Όπως είδαμε, για την παραγωγή των παραμέτρων a σε κάθε περίπτωση χρειαζόμαστε τις σταθερές a_1, a_2 και a_3. Στην περίπτωσή μας, για να έχουμε την επιθυμητή συμπεριφορά των συναρτήσεων χρησιμότητας στο διάστημα [0,1] θέτουμε:

- $a_1 = 0.4$
- $a_2 = 0.57$
- $a_3 = 0.05$

4.3 Αποτελέσματα

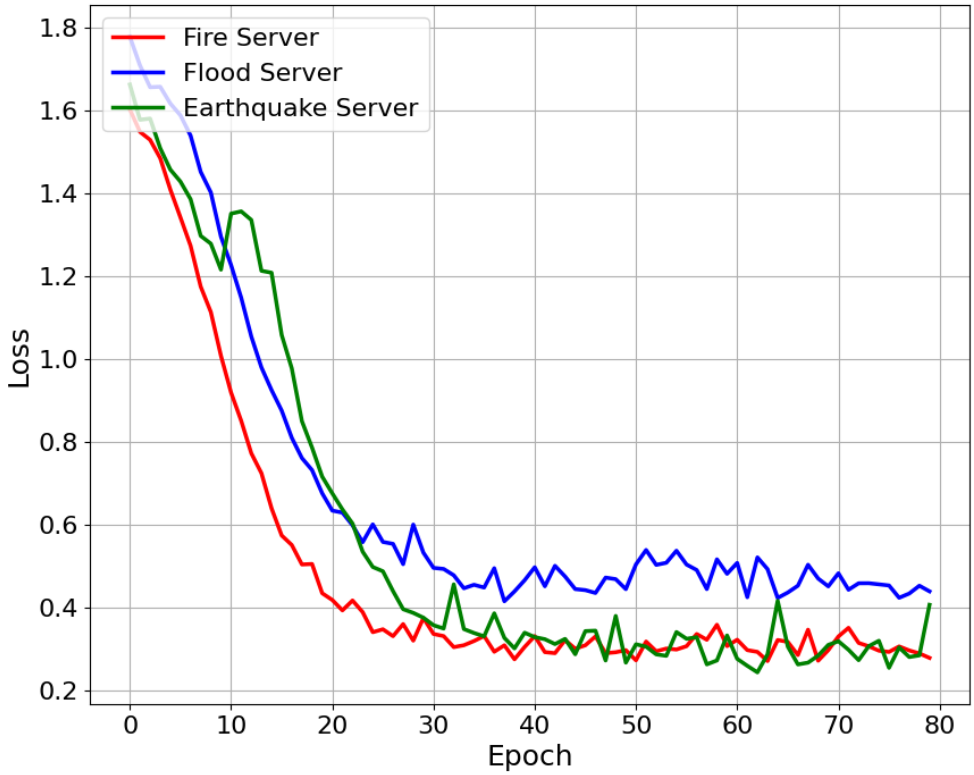
Για να μελετήσουμε την συμπεριφορά του συστήματός μας σε διάφορες καταστάσεις, εκτελούμε την διαδικασία της αντιστοίχισης και της Ομοσπονδιακής Μάθησης πολλαπλές φορές για διαφορετικό πλήθος κόμβων. Κατά την διάρκεια της εκτέλεσης, κρατάμε πληροφορία για την ποιότητα της αντιστοίχισης αλλά και την εξέλιξη της Ομοσπονδιακής Μάθησης, ώστε έπειτα από τα αρχεία αυτά να μπορούμε να κατασκευάσουμε τα απαραίτητα διαγράμματα για να κάνουμε πιο κατανοητή την συμπεριφορά του οικοσυστήματος μας.

Συνεπώς, όσον αφορά την επίδοση της Ομοσπονδιακής Μάθησης για τον κάθε εξυπηρετητή βλέπουμε το εξής:



Σχήμα 4.1: Ακρίβεια Εξυπηρετητών στην Μετανοητική Μάθηση

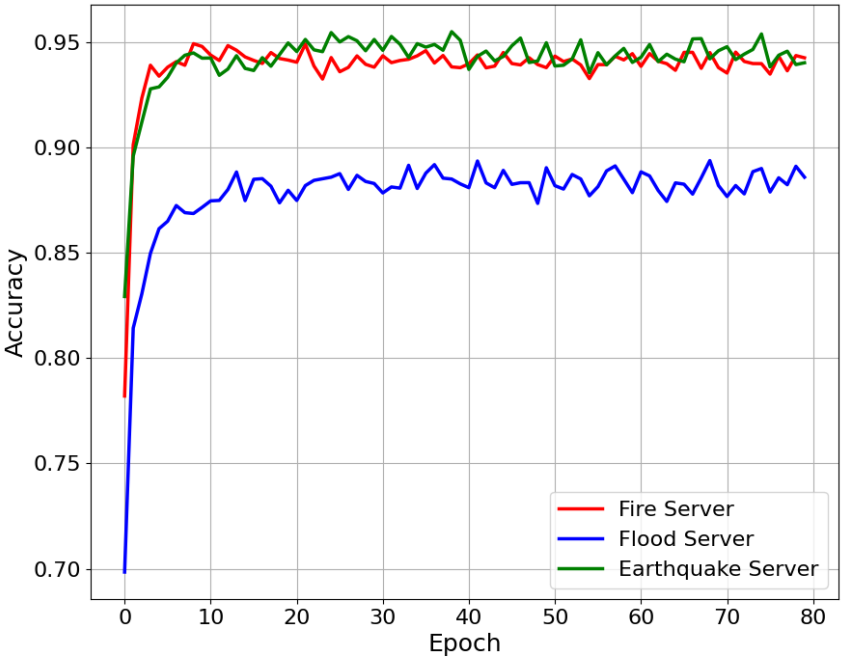
Όπως βλέπουμε στα σχήματα 4.1, 4.2, παρατηρούμε παρόμοια συμπεριφορά με τις προηγούμενες τεχνικές αντιστοίχισης. Όπως και σε προηγούμενες περιπτώσεις, έχουμε $Datasize_{fire} > Datasize_{flood} > Datasize_{earthquake}$, και επιπλέον ο εντοπισμός της φωτιάς είναι ένα πιο εύκολο πρόβλημα από ότι μιας πλημμύρας, αφού σε πλημμύρες έχουμε πιο ουδέτερα χρώματα, ενώ σε φωτιές πιο έντονα χρώματα και μεγάλες αλλαγές φωτεινότητας και σε σεισμούς πιο γήινα και ξηρά χρώματα. Επιπλέον, πολλές από τις ουδέτερες φωτογραφίες είναι πιο κοντά σε φωτογραφίες από πλημμύρες από ότι σε σεισμούς ή φωτιές, με αποτέλεσμα η διάκριση των δύο άλλων



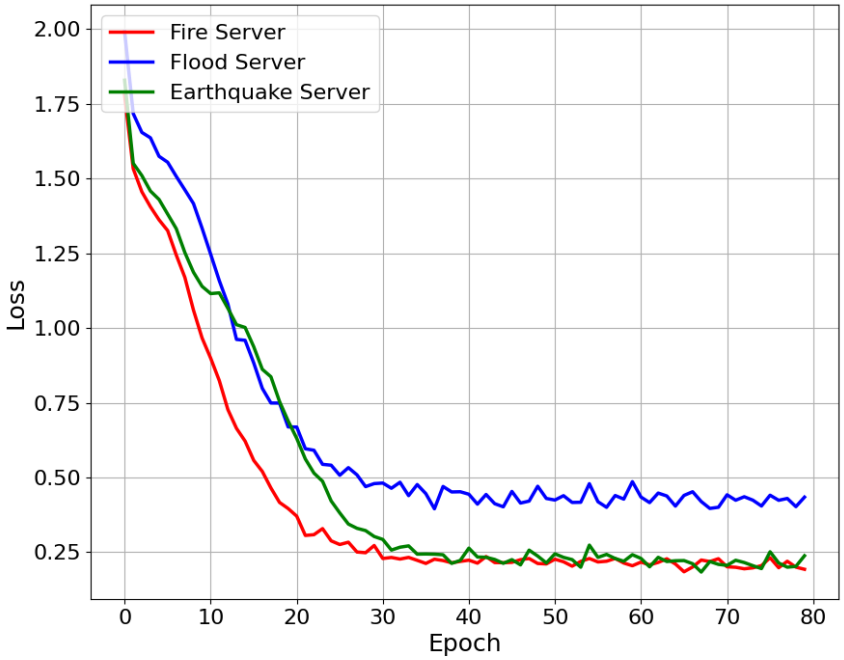
Σχήμα 4.2: Απώλεια Εξυπηρετητών στην Μετανοητική Μάθηση

καταστροφών να είναι πιο απλή. Συνεπώς, για αυτούς τους λόγους, όπως και σε προηγούμενες περιπτώσεις έχουμε την καλύτερη απόδοση στον εξυπηρετητή που ανιχνεύει φωτιές, έπειτα στον εξυπηρετητή που ανιχνεύει σεισμούς και τέλος στον εξυπηρετητή που ανιχνεύει πλημμύρες παρότι $Datasize_{flood} > Datasize_{earthquake}$.

Αντίστοιχα, για τις επιδόσεις των κόμβων, είναι εμφανές στα διαγράμματα 4.3 και 4.4, πως έχουμε παρόμοια συμπεριφορά, μόνο που η ακρίβεια των κόμβων του εξυπηρετητή που ανιχνεύει για σεισμούς είναι μεγαλύτερη. Αυτό μας δείχνει πως παρότι οι κόμβοι τοπικά πετυχαίνουν καλύτερα αποτελέσματα, ο εξυπηρετητής δυσκολεύεται να γενικεύσει από τα βάρη που λαμβάνει από τους κόμβους του. Παρ' όλα ταύτα, είναι σημαντικό όμως να αναφέρουμε πως οι κόμβοι και οι εξυπηρετητές φαίνεται να μαθαίνουν αποτελεσματικά τις ιδιότητες των εικόνων, με αποτέλεσμα να πετυχαίνουν αρκετά υψηλές τελικές ακρίβειες.

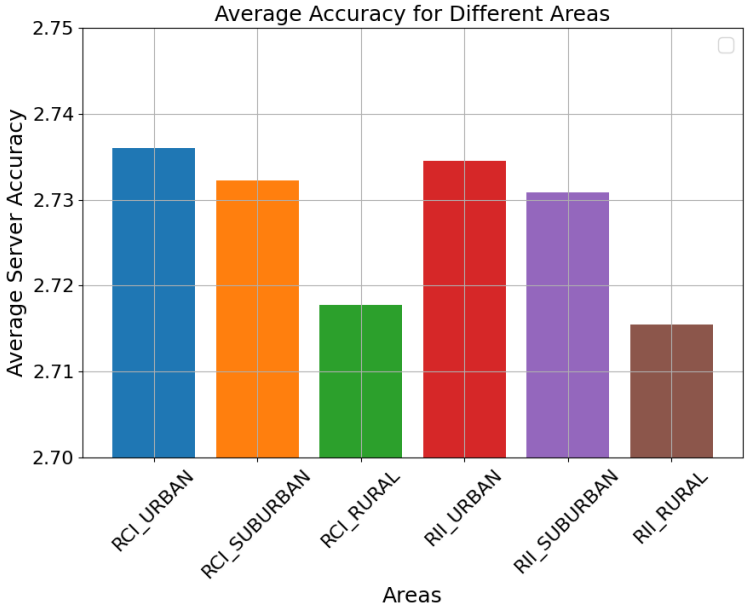


Σχήμα 4.3: Ακρίβεια κόμβων στην Μετανοητική Μάθηση

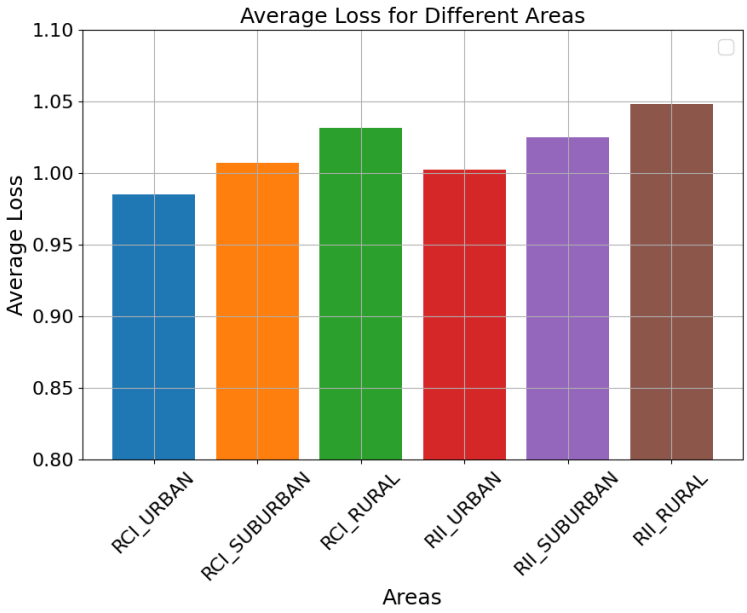


Σχήμα 4.4: Απώλεια κόμβων στην Μετανοητική Μάθηση

Όσον αφορά τις διαφορές μεταξύ των δύο αλγορίθμων Μετανοητικής Μάθησης, αλλά και όσον αφορά τις διαφορετικές περιοχές (Αστική Περιοχή, Προαστιακή Περιοχή, Αγροτική Περιοχή) παρατηρούμε τις εξής διαφορές:



Σχήμα 4.5: Ακρίβεια Εξυπηρετητών Μετανοητικής Μάθησης σε διαφορετικές περιοχές

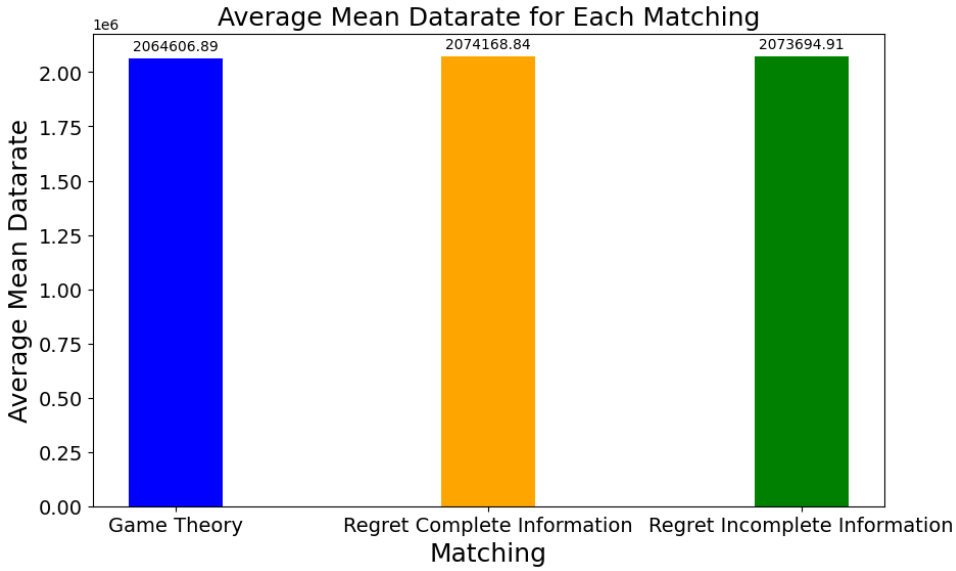


Σχήμα 4.6: Απώλεια Εξυπηρετητών Μετανοητικής Μάθησης σε διαφορετικές περιοχές

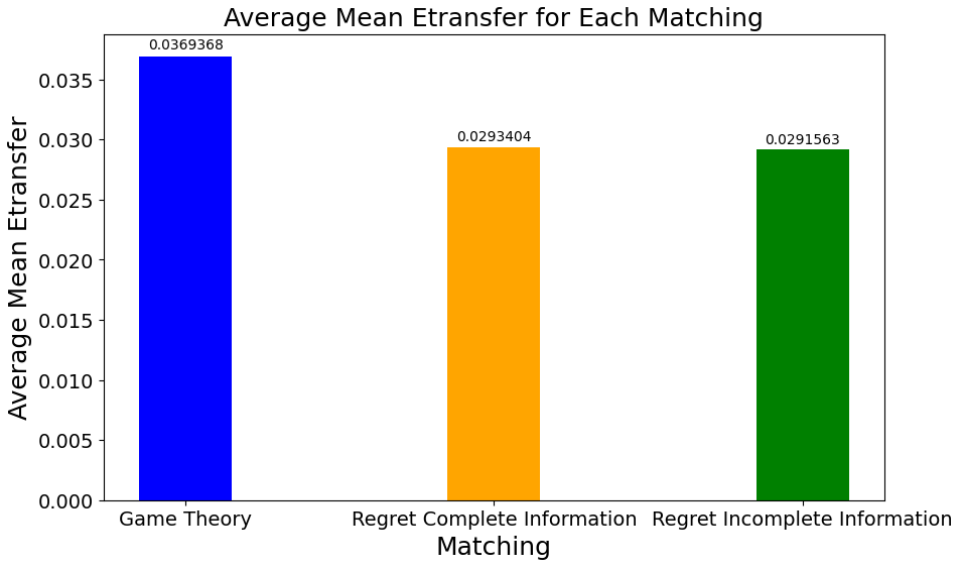
Όπως βλέπουμε στα παραπάνω σχήματα 4.5 και 4.6 υπάρχουν διαφοροποιήσεις στις επιδόσεις της Ομοσπονδιακής Μάθησης ανάλογα με τον αλγόριθμο που χρησιμοποιείται για την αντιστοίχιση και διαμόρφωση των κόμβων, αλλά και ανάλογα με την περιοχή στην οποία βρισκόμαστε. Έτσι, για τον αλγόριθμο Πλήρους Πληροφορίας, όπου βρίσκονται κατά βάση οι βέλτιστες λύσεις, παρατηρούμε πως πετυχαίνουμε την μικρότερη απώλεια στην Αστική Περιοχή, έπειτα στα Προάστια και τέλος στην Αγροτική Περιοχή, όπως είναι και το αναμενόμενο. Από την άλλη πλευρά, στον αλγόριθμο Ελλιπούς Πληροφορίας βλέπουμε μια απόκλιση στην Αστική Περιοχή που δεν συμβαδίζει με το προηγούμενο συμπέρασμα. Στον αλγόριθμο αυτό όμως δεν βρίσκουμε πάντα τις βέλτιστες λύσεις, λόγω απώλειας πλήρους πληροφορίας, και άρα οι τελικές αποφάσεις των κόμβων μπορεί να διαθέτουν λιγότερα δεδομένα στην Ομοσπονδιακή Μάθηση από ότι στην βέλτιστη λύση της Πλήρους Πληροφορίας. Όμως μένει πολύ κοντά στις επιδόσεις του αλγορίθμου Πλήρους Πληροφορίας.

4.4 Σύγκριση Μετανοητικής Μάθησης με Θεωρία Παιγνίων

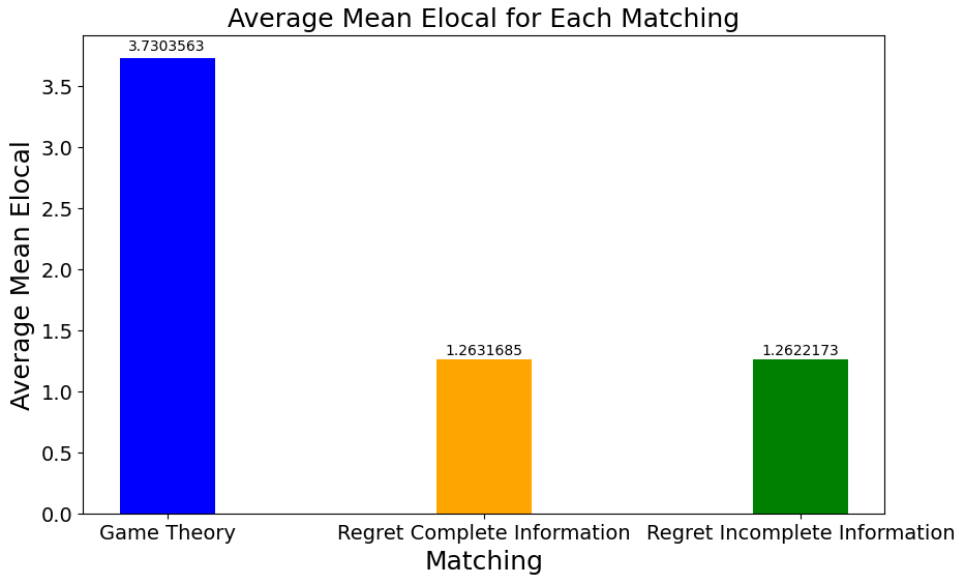
Επίσης, σημαντική πληροφορία παίρνουμε συγκρίνοντας τους δύο αλγορίθμους Μετανοητικής Μάθησης μεταξύ τους, αλλά και με τον αλγόριθμο του κεφαλαίου 2. Στο σημείο αυτό θα δούμε τα πλεονεκτήματα και μειονεκτήματα του κάθε αλγορίθμου και την επίδοσή του σε διαφορετικές περιπτώσεις. Όσον αφορά τα φυσικά μεγέθη τα οποία μελετάμε για τους κόμβους μας παρατηρούμε τα εξής:



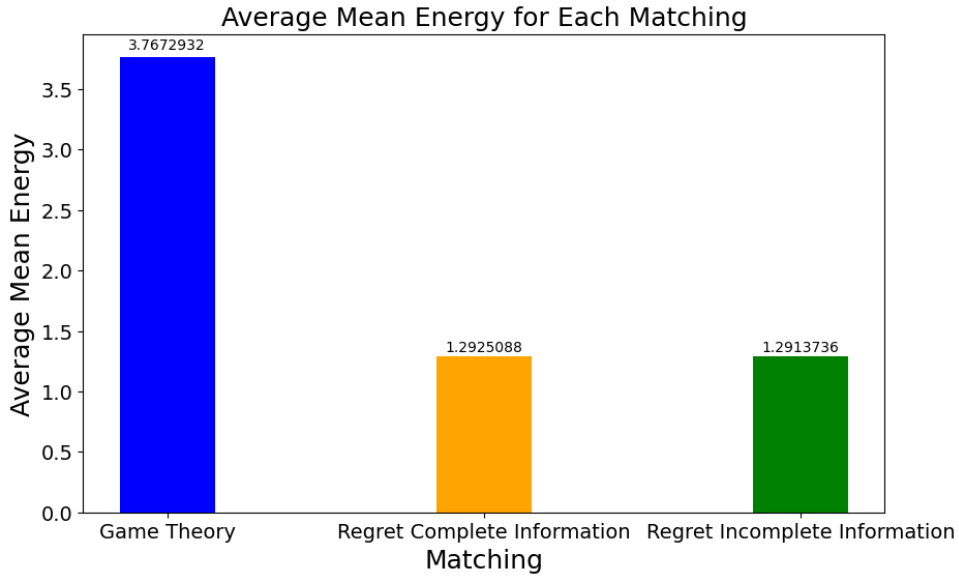
Σχήμα 4.7: Μέση ροή δεδομένων για τους κόμβους ανά αλγόριθμο αντιστοίχισης



Σχήμα 4.8: Μέση ενέργεια μετάδοσης για τους κόμβους ανά αλγόριθμο αντιστοίχισης



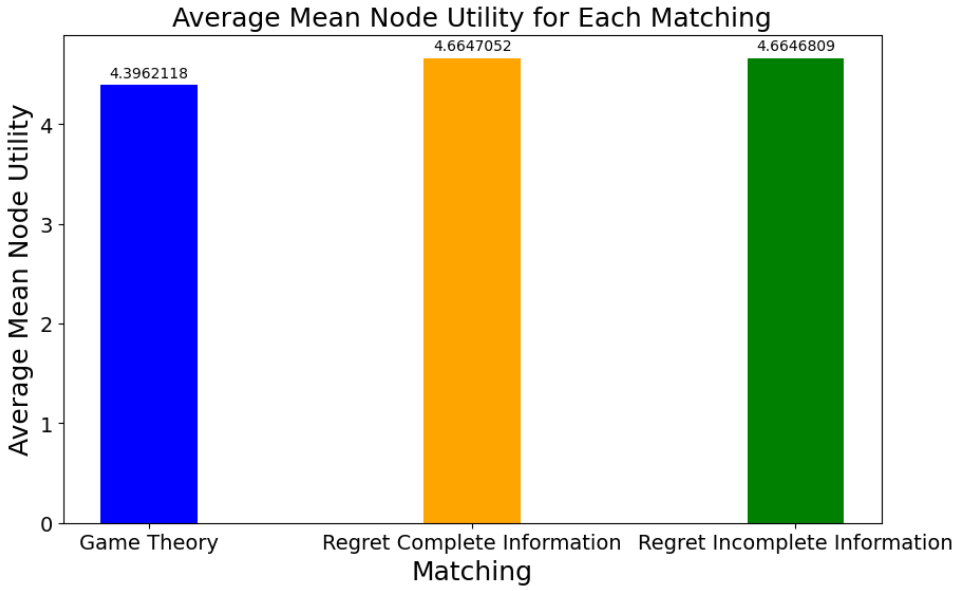
Σχήμα 4.9: Μέση ενέργεια εκπαίδευσης για τους κόμβους ανά αλγόριθμο αντιστοίχισης



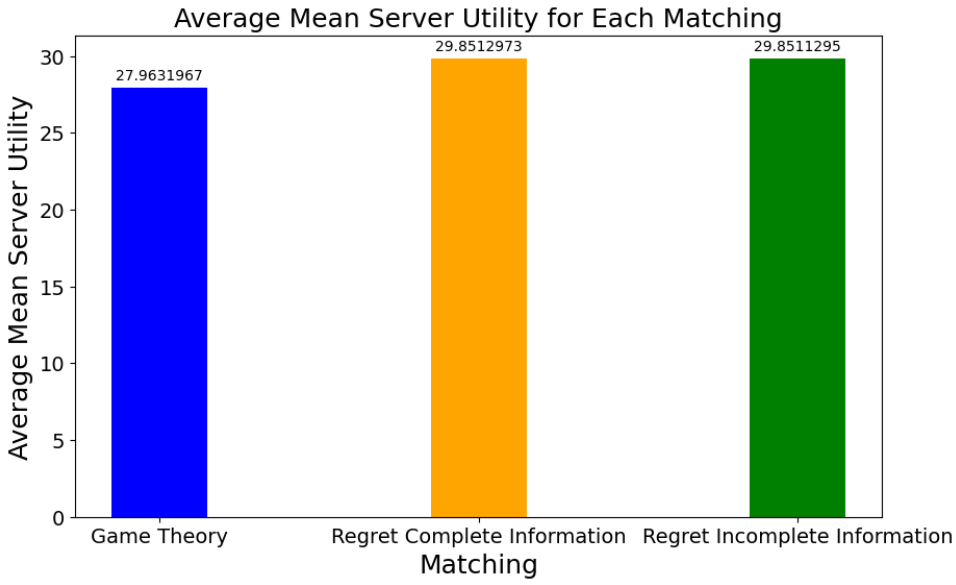
Σχήμα 4.10: Μέση συνολική ενέργεια για τους κόμβους ανά αλγόριθμο αντιστοίχισης

Αρχικά, όπως βλέπουμε στα παραπάνω διαγράμματα (4.7, 4.8, 4.9, 4.10) οι αλγόριθμοι Μετανοητικής Μάθησης μας δίνουν πολύ καλύτερα αποτελέσματα, ειδικά σε εξοικονόμηση ενέργειας (είτε μετάδοσης, είτε εκπαίδευσης), πετυχαίνοντας παράλληλα καλύτερη μέση ροή μετάδοσης δεδομένων. Αυτό είναι λογικό, αφού οι δύο αλγόριθμοι δίνουν την δυνατότητα στους κόμβους να μεταβάλλουν τους πόρους που διαθέτουν στο σύστημά μας. Έτσι κάποιος πιο απομακρυσμένος κόμβος δεν ”αναγκάζεται” να χρησιμοποιήσει όλους τους πόρους του καταναλώνοντας παραπάνω ενέργεια για μικρό κέρδος, ενώ αντίστοιχα σε ανταγωνιστικά μεγέθη όπως η Ροή Δεδομένων, ελευθερώνονται πόροι του συστήματος για τους πιο ενεργούς - σημαντικούς κόμβους. Από τους

δύο αλγορίθμους Μετανοητικής Μάθησης, καλύτερα αποτελέσματα μας δίνει προφανώς ο αλγόριθμος Πλήρους Πληροφορίας, ο οποίος εξετάζει αναλυτικά την συμπεριφορά όλων των πιθανών ενεργειών του κάθε κόμβου παίρνοντας υπόψη και τις ενέργειες των υπολοίπων. Αυτό μπορεί να μην είναι προφανές για την ώρα, αφού όπως βλέπουμε στα διαγράμματα 4.3 και 4.4, ο αλγόριθμος Ελλιπούς Πληροφορίας πετυχαίνει χαμηλότερη κατανάλωση ενέργειας από ότι ο Πλήρους Πληροφορίας.



Σχήμα 4.11: Μέση χρησιμότητα κόμβων ανά αλγόριθμο αντιστοίχισης

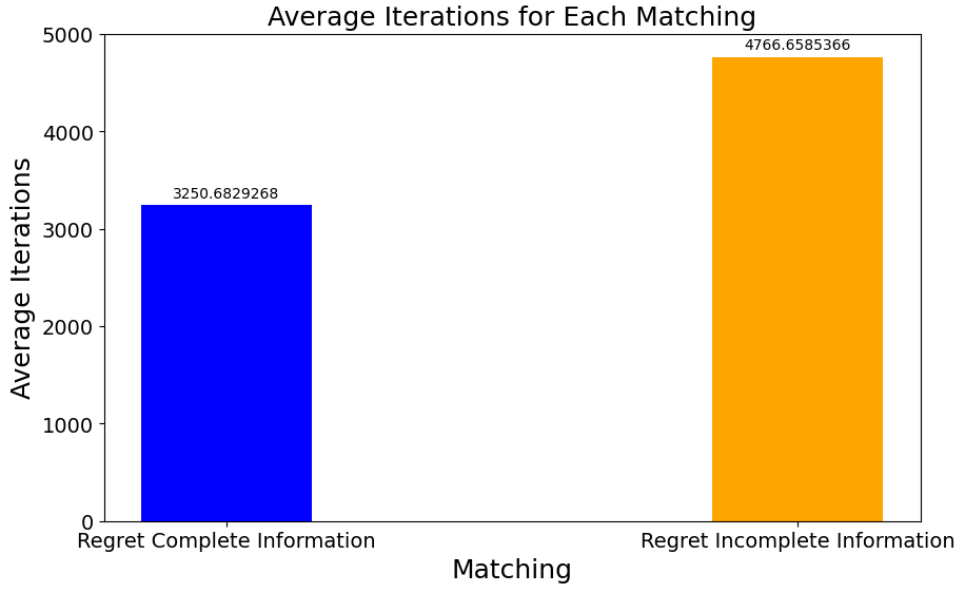


Σχήμα 4.12: Μέση χρησιμότητα εξυπηρετητών ανά αλγόριθμο αντιστοίχισης

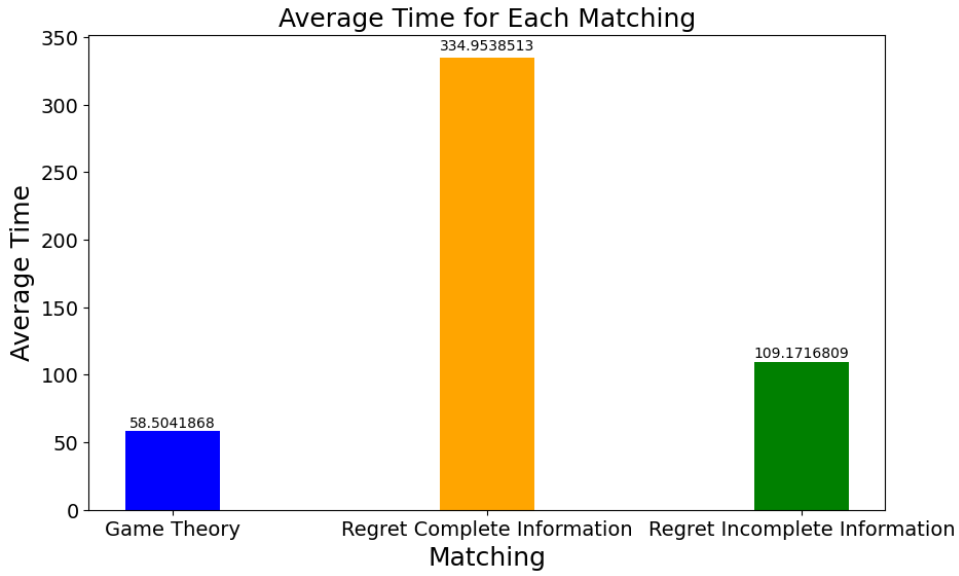
Έτσι, στα διαγράμματα 4.11 και 4.12, όπου απεικονίζεται η μέση χρησιμότητα που επιτυγχά-

νουν οι κόμβους και οι εξυπηρετητές, γίνεται εμφανές πως ο αλγόριθμος Πλήρους Πληροφορίας πετυχαίνει καλύτερα αποτελέσματα από τον αλγόριθμο Ελλιπούς Πληροφορίας, αφού εν τέλει η μετρική με την οποία παίρνονται οι αποφάσεις στον εκάστοτε αλγόριθμο είναι η χρησιμότητα. Όμως και πάλι η διαφορά τους είναι πολύ μικρή. Αντίστοιχα και οι δύο αλγόριθμοι Μετανοητικής Μάθησης έχουν καλύτερες επιδόσεις από τον αλγόριθμο Θεωρίας Παιγνίων.

Παρ' όλα ταύτα, ο αλγόριθμος Πλήρους Πληροφορίας έχει και κάποια μειονεκτήματα, συγκεκριμένα στον χρόνο που απαιτεί για να επιτύχει σύγκλιση. Πιο αναλυτικά βλέπουμε:



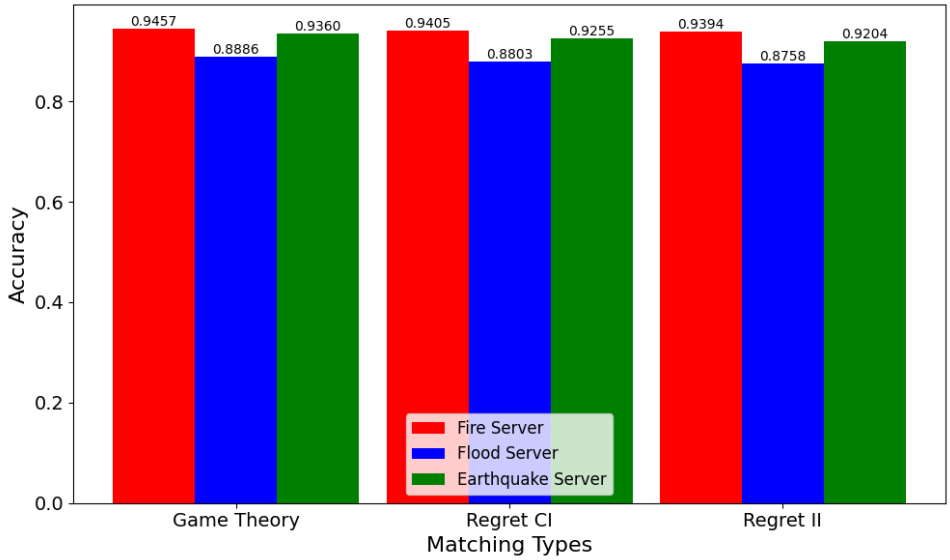
Σχήμα 4.13: Μέσος αριθμός επαναλήψεων ανά αλγόριθμο αντιστοίχισης



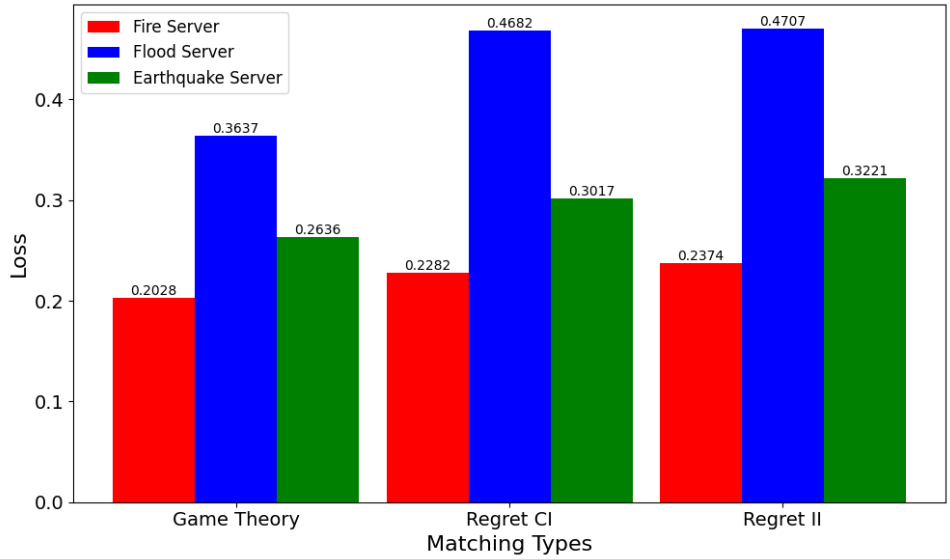
Σχήμα 4.14: Μέσος χρόνος εκτέλεσης ανά αλγόριθμο αντιστοίχισης

Άρα παρότι εν γένει παίρνουμε καλύτερα αποτελέσματα με τον αλγόριθμο Πλήρους Πληρο-

φορίας, έχει ένα μεγάλο μειονέκτημα όσον αφορά τον μεγάλο χρόνο που απαιτεί για την εκτέλεσή του (4.14). Αυτό θα μπορούσε να είναι ένα κρίσιμο σημείο για συχνά μεταβαλλόμενα συστήματα, στα οποία απαιτείται συχνή επαναπροσαρμογή των παικτών. Παρότι, έχουμε μεγαλύτερο αριθμό επαναλήψεων στον αλγόριθμο Ελλιπούς Πληροφορίας (4.13), κάθε επανάληψη του αλγορίθμου Πλήρους Πληροφορίας είναι πολύ πιο ακριβή υπολογιστικά, αφού πρέπει να εξετάσει τις πιθανές ενέργειες κάθε κόμβου στο σύστημα. Ειδικά για μεγαλύτερα σύνολα κόμβων η αντιστοίχιση γίνεται πάρα πολύ αργή.



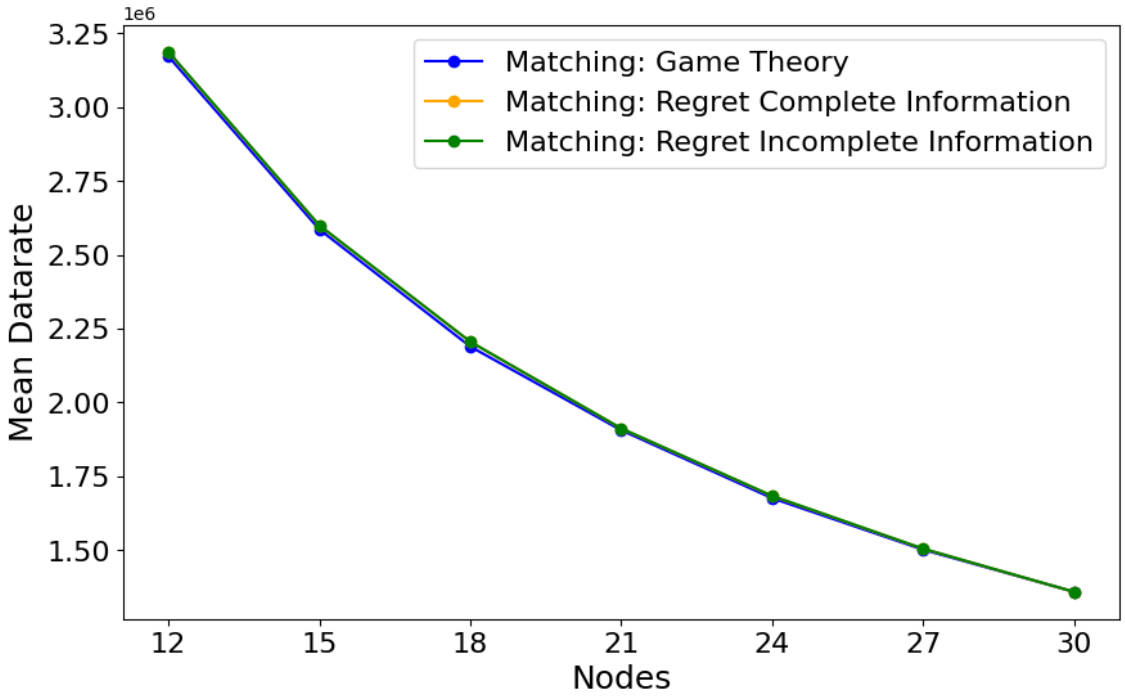
Σχήμα 4.15: Ακρίβεια Εξυπηρετητών ανά αλγόριθμο αντιστοίχισης



Σχήμα 4.16: Απώλεια Εξυπηρετητών ανά αλγόριθμο αντιστοίχισης

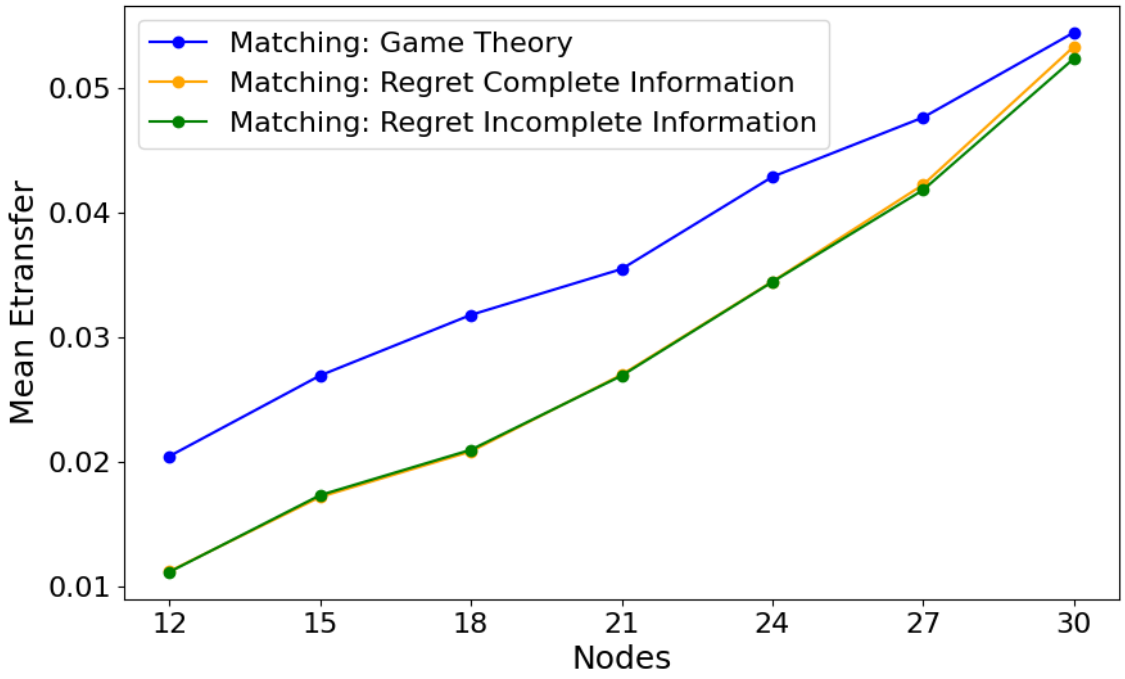
Στο κομμάτι της Ομοσπονδιακής Μάθησης παρατηρούμε πως ανάλογα με την σημασία κάθε κόμβου και τις απολαβές που μπορεί να συλλέξει, στους αλγορίθμους Μετανοητικής Μάθησης, ο κόμβος μπορεί να επιλέξει να διαθέσει λιγότερα δεδομένα στην διαδικασία της εκμάθησης. Αυτό έχει ως αποτέλεσμα, όπως φαίνεται στα 4.15 και 4.16, να πετυχαίνουμε χειρότερα αποτελέσματα στην εκπαίδευση των μοντέλων με τους δύο αυτούς αλγορίθμους. Από την άλλη πλευρά, βλέπουμε πως και οι δύο αλγόριθμοι Μετανοητικής Μάθησης φτάνουν αρκετά κοντά σε επιδόσεις συγκριτικά με τον αλγόριθμο Θεωρίας Παιγνίων. Δεδομένου ότι πετυχαίνουμε αυτό το αποτέλεσμα, με τα μικρότερα σύνολα δεδομένων που χρησιμοποιούν οι αλγόριθμοι Μετανοητικής Μάθησης, είναι εμφανές πως το μοντέλο μας σε συνδυασμό με μια ορθή αντιστοίχιση και διαμόρφωση των κόμβων πετυχαίνει πολύ καλές επιδόσεις.

Αντίστοιχα, είναι σημαντικό να μελετήσουμε και την συμπεριφορά των αλγορίθμων μας ανάλογα με το πλήθος των κόμβων που καλούνται να διαχειριστούν.



Σχήμα 4.17: Μέση ροή δεδομένων ανά αριθμό κόμβων ανά αλγόριθμο αντιστοίχισης

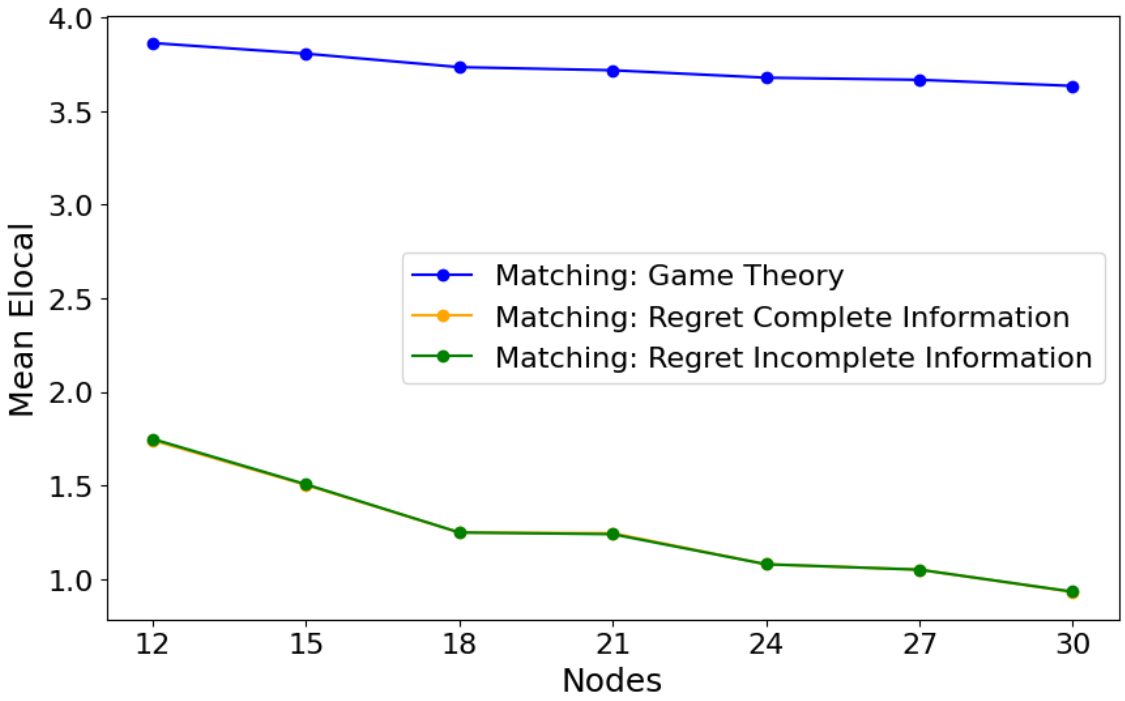
Αρχικά, όπως είδαμε και παραπάνω, επαναλαμβάνεται η επικράτηση των αλγορίθμων Μετανοητικής Μάθησης σε σχέση με τον αλγόριθμο Θεωρίας Παιγνίων, λόγω της δυνατότητάς που τους έχουμε δώσει να διαμορφώνουν τη συμπεριφορά του κάθε κόμβου (4.17, 4.18, 4.19, 4.20). Βλέπουμε πως η μέση ροή δεδομένων μειώνεται όσο ο αριθμός των κόμβων αυξάνεται (4.17), το οποίο είναι λογικό, αφού οι κόμβοι μας μοιράζονται το κοινό εύρος ζώνης που διαθέτει ο εξυπηρετητής για την επικοινωνία με αυτούς. Όλοι οι αλγόριθμοι διατηρούν περίπου όμοια κλιμάκωση ανάλογα με τον αριθμό των κόμβων, με τον αλγόριθμο Πλήρους Πληροφορίας να πετυχαίνει το καλύτερο αποτέλεσμα, ακολουθούμενο από τον αλγόριθμο Ελλιπούς Πληροφορίας και τέλος από τον αλγόριθμο Θεωρίας Παιγνίων, όμως με ελάχιστες διαφορές (βλ 4.7).



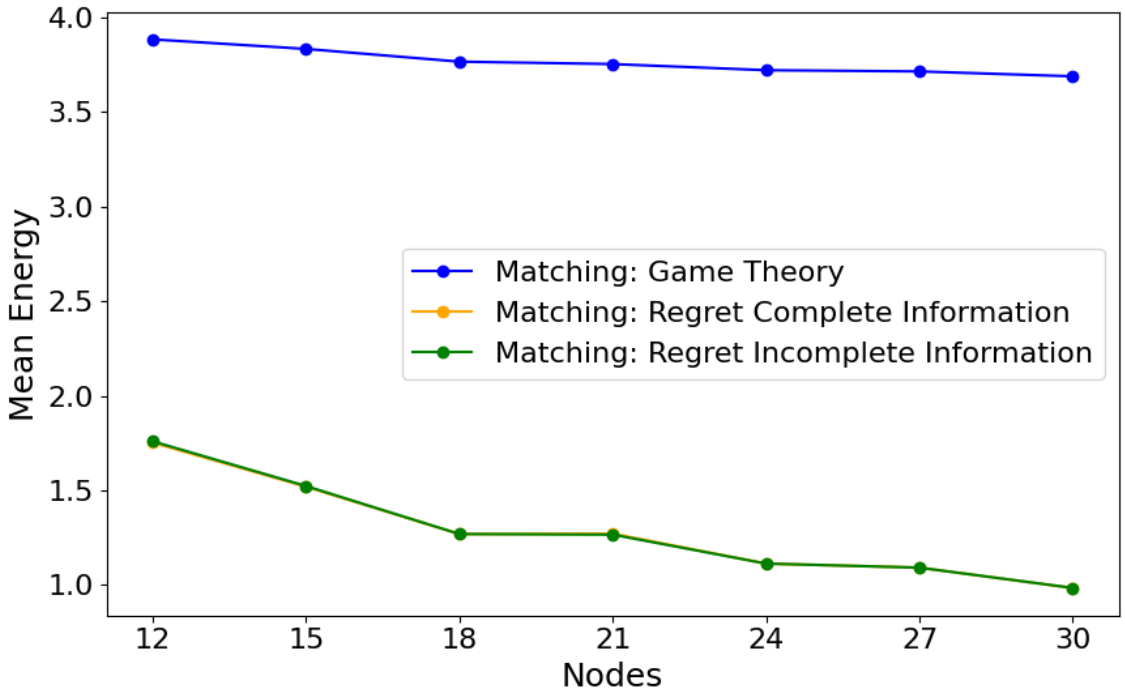
Σχήμα 4.18: Μέση ενέργεια μετάδοσης ανά αριθμό κόμβων ανά αλγόριθμο αντιστοίχισης

Και για τους τρεις αλγορίθμους η μέση ενέργεια μετάδοσης αυξάνεται όσο αυξάνεται και ο αριθμός των κόμβων (4.18). Η συμπεριφορά αυτή είναι προϊόν του ανταγωνισμού, όπως είδαμε και στη ροή δεδομένων. Οι κόμβοι ανταγωνίζονται για πόρους και άρα προσπαθούν να διαθέσουν παραπάνω ισχύ, και άρα και ενέργεια, με σκοπό να διεκδικήσουν τους πόρους αυτούς. Συγκεκριμένα, όπως βλέπουμε και στο 4.18 η ενέργεια μετάδοσης για τους αλγορίθμους Μετανοητικής Μάθησης αυξάνεται με μεγαλύτερο ρυθμό. Αυτό συμβαίνει επειδή όλοι οι κόμβους μεταδίδουν τον ίδιο αριθμό δεδομένων στον κεντρικό εξυπηρετητή, οι πιο απομακρυσμένοι, διεκδικώντας μικρότερο εύρος ζώνης θα απαιτούν περισσότερη ώρα για να μεταδώσουν την πληροφορία και άρα θα έχουν μεγαλύτερη κατανάλωση ενέργειας. Αξίζει να σημειώσουμε πως για 30 κόμβους ο αλγόριθμος Πλήρους Πληροφορίας φαίνεται να ωθεί τους κόμβους να διαθέσουν παραπάνω ισχύ και άρα μεγαλύτερη κατανάλωση ενέργειας για μετάδοση, απ' ότι ο αλγόριθμος Ελλιπούς Πληροφορίας.

Όπως βλέπουμε στο σχ.4.19, καθώς ο αριθμός των κόμβων αυξάνεται, ο μέσος όρος της ενέργειας εκπαίδευσης σε κάθε περίπτωση μειώνεται. Αυτό συμβαίνει, διότι οι πιο απομακρυσμένοι κόμβοι έχουν στη διάθεσή τους μικρότερα σύνολα δεδομένων, αφού βρίσκονται πιο μακριά από τα κρίσιμα σημεία. Αντίστοιχα, επειδή οι αλγόριθμοι Μετανοητικής Μάθησης έχουν την δυνατότητα προσαρμογής του συνόλου δεδομένου που προσφέρει ο κάθε κόμβος στην Ομοσπονδιακή Μάθηση, επιτυγχάνουν πολύ μικρότερη μέση κατανάλωση ενέργειας εκπαίδευσης.

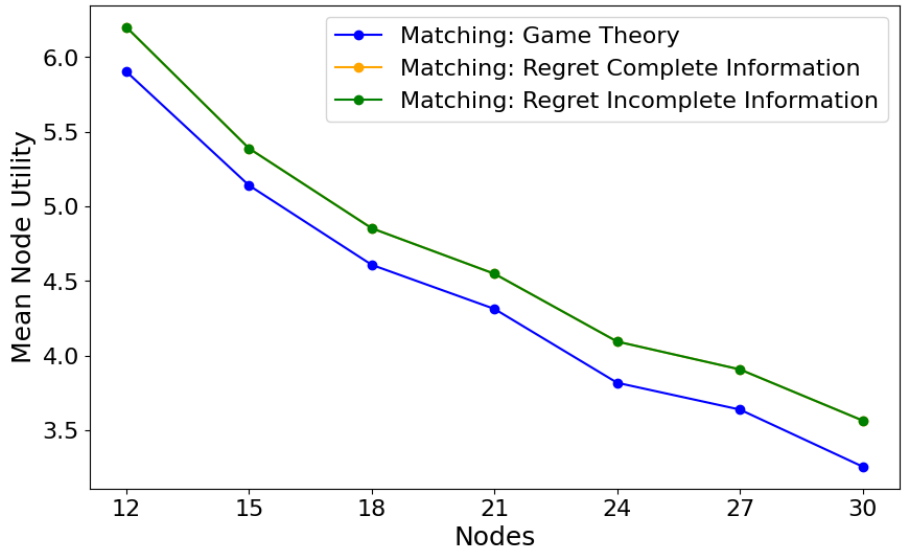


Σχήμα 4.19: Μέση ενέργεια εκπαίδευσης ανά αριθμό κόμβων ανά αλγόριθμο αντιστοίχισης

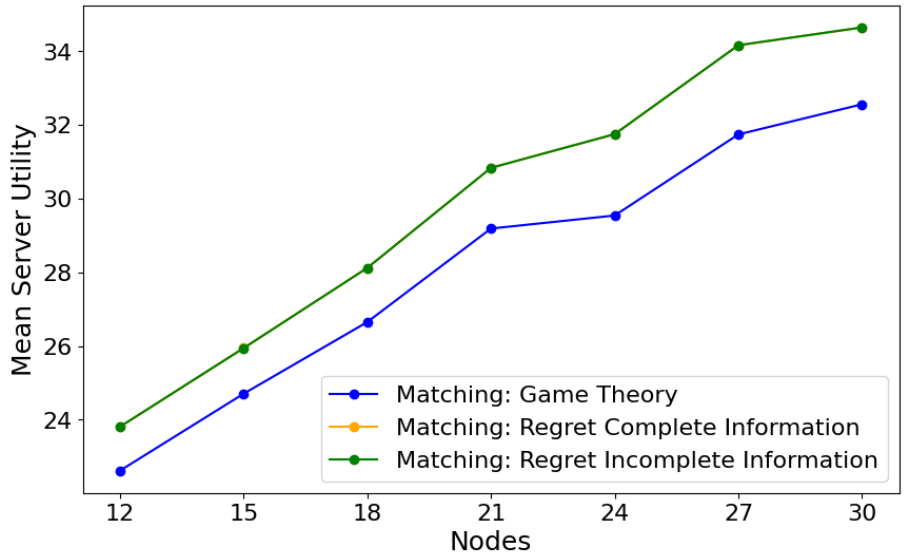


Σχήμα 4.20: Μέση συνολική ενέργεια ανά αριθμό κόμβων ανά αλγόριθμο αντιστοίχισης

Για τον ίδιο λόγο επίσης η μέση κατανάλωση ενέργειας εκπαίδευσης μειώνεται με μεγαλύτερο ρυθμό στους αλγορίθμους Μετανοητικής Μάθησης. Στον αλγόριθμο Πλήρους Πληροφορίας βλέπουμε πως γενικά έχουμε μια μεγαλύτερη κατανάλωση ενέργειας, όπου όπως είδαμε και προηγουμένως οφείλεται στην καλύτερη αξιοποίηση των συνόλων δεδομένων των κόμβων. Αντίστοιχα, στο σχ.4.20 βλέπουμε πως η μέση συνολική ενέργεια παρουσιάζει αντίστοιχη μορφή με την μέση ενέργεια εκπαίδευσης, αφού το μεγαλύτερο μέρος της ενέργειας που καταναλώνεται αφορά την τοπική εκπαίδευση για κάθε κόμβο.



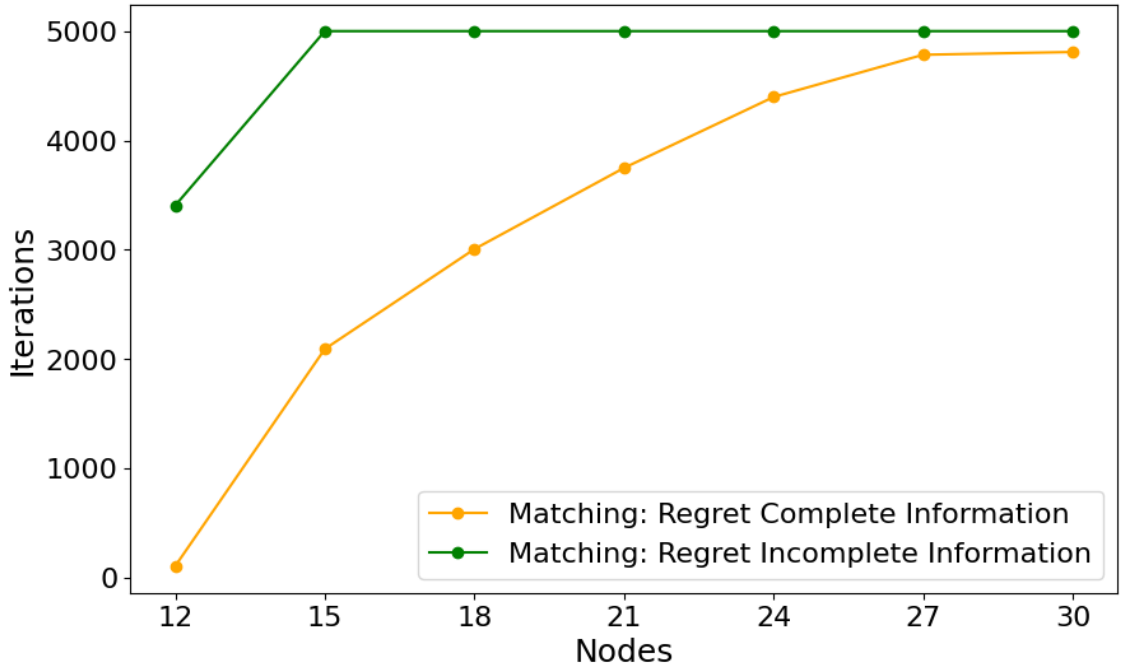
Σχήμα 4.21: Μέση χρησιμότητα κόμβων ανά αριθμό κόμβων ανά αλγόριθμο αντιστοίχισης



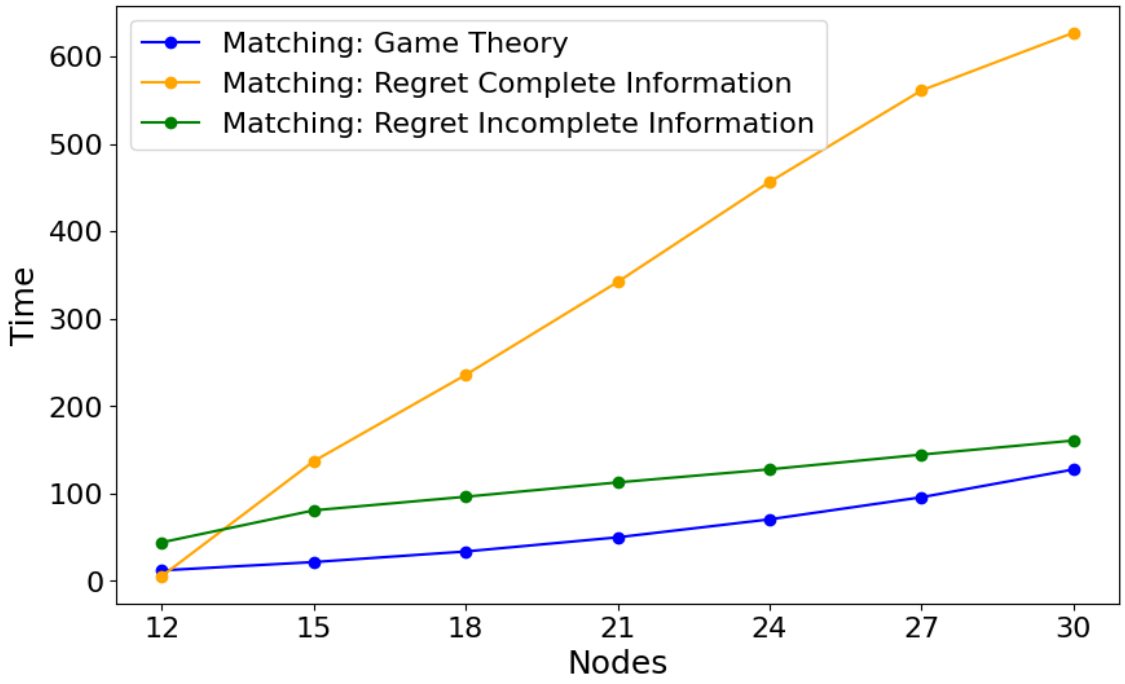
Σχήμα 4.22: Μέση χρησιμότητα εξυπηρετητών ανά αριθμό κόμβων ανά αλγόριθμο αντιστοίχισης

Όπως βλέπουμε στο σχ.4.21 η μέση χρησιμότητα των κόμβων πέφτει όσο περισσότεροι κόμβοι ζουν στο σύστημά μας. Αυτό είναι λογικό, αφού με περισσότερους κόμβους έχουμε και μεγαλύτερο ανταγωνισμό για τους μοιραζόμενους πόρους, ενώ παράλληλα οι νέοι κόμβοι, όντας πιο μακρινοί από τα κρίσιμα σημεία, είναι μικρότερης σημασίας και άρα έχουν μικρότερες μέγιστες τιμές χρησιμότητας, ρίχνοντας το μέσο όρο. Αυτό φαίνεται αντίστοιχα στο σχ.4.22, όπου όσο περισσότεροι κόμβοι είναι διαθέσιμοι, τόσο λιγότερο κλιμακώνει η χρησιμότητα των εξυπηρετητών. Επιπλέον, η χρησιμότητα των εξυπηρετητών αυξάνεται με την αύξηση των κόμβων, αφού περισσότεροι κόμβους είναι διαθέσιμοι σε κάθε εξυπηρετητή.

Όσον αφορά τον χρόνο εκτέλεσης και τον αριθμό επαναλήψεων που απαιτεί κάθε αλγόριθμος (σχ.4.23 και σχ.4.24) μπορούμε να δούμε πως ο αλγόριθμος Πλήρους Πληροφορίας αυξάνει σε υπολογιστικό κόστος πολύ γρήγορα σε σχέση με τον αριθμό των κόμβων. Αντίθετα, ο Ελλιπούς Πληροφορίας παρουσιάζει ίδιο κόστος και σε επαναλήψεις και σε χρόνο, ανεξαιρέτως του πλήθους των κόμβων καθιστώντας τον μη ιδανικό για μικρά N, αλλά δίνοντάς του πολύ καλή κλιμάκωση. Τέλος ο αλγόριθμος Θεωρίας Παιγνίων αυξάνει αργά σε υπολογιστικό κόστος, με γραμμικό τρόπο. Για τους δύο αλγορίθμους Μετανοητικής Μάθησης μπορούμε να παρατηρήσουμε επίσης το εξής. Ο αλγόριθμος Ελλιπούς Πληροφορίας φαίνεται να δυσκολεύεται στη σύγκλιση, πιθανότατα λόγω της ελλιπούς του πληροφορίας, αλλά το φθηνό υπολογιστικό του κόστος τον καθιστά πολύ γρήγορο στην εκτέλεση και άρα ιδανικό για οποιουδήποτε τύπου συστήματα. Αντίθετα φαίνεται ο αλγόριθμος Πλήρους Πληροφορίας να επηρεάζεται στην σύγκλιση και άρα και στον χρόνο εκτέλεσης από την θέση των εκάστοτε κόμβων. Όσο περισσότερους κόμβους διαθέτουμε και όσο αυτοί είναι πιο απομακρυσμένοι τόσο πιο πολλές επαναλήψεις φαίνεται να απαιτούνται για την σύγκλιση του αλγορίθμου και άρα μεγαλώνει ο χρόνος εκτέλεσης.

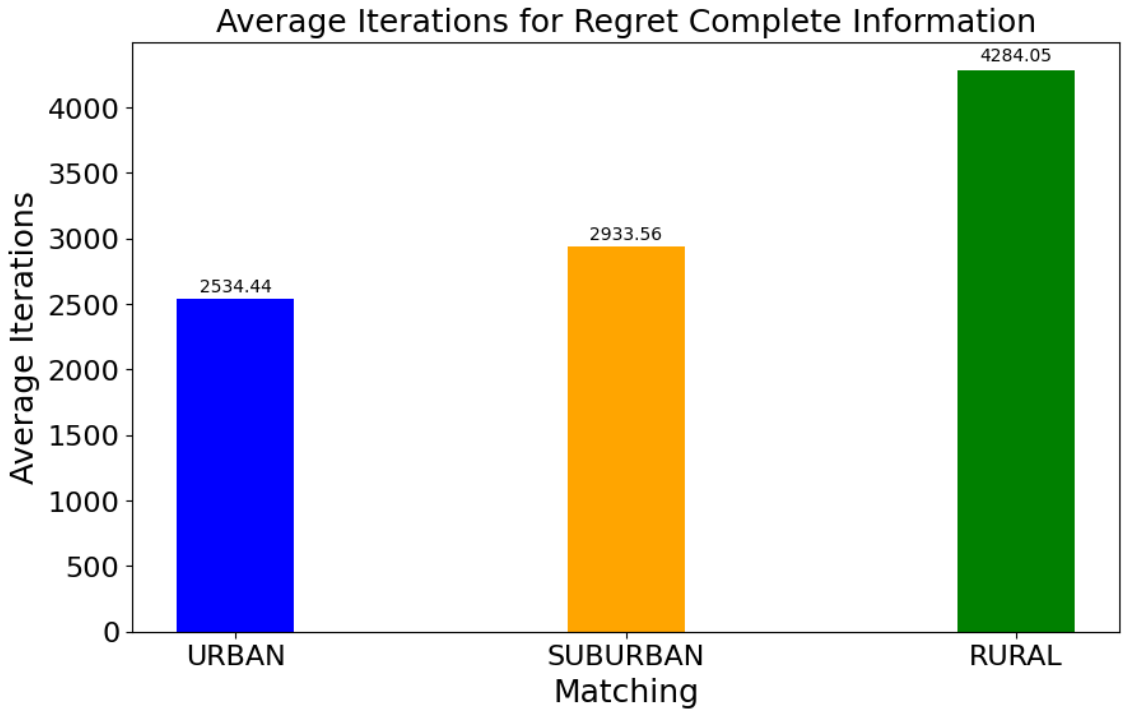


Σχήμα 4.23: Μέσος αριθμός επαναλήψεων ανά αριθμό κόμβων ανά αλγόριθμο αντιστοίχισης

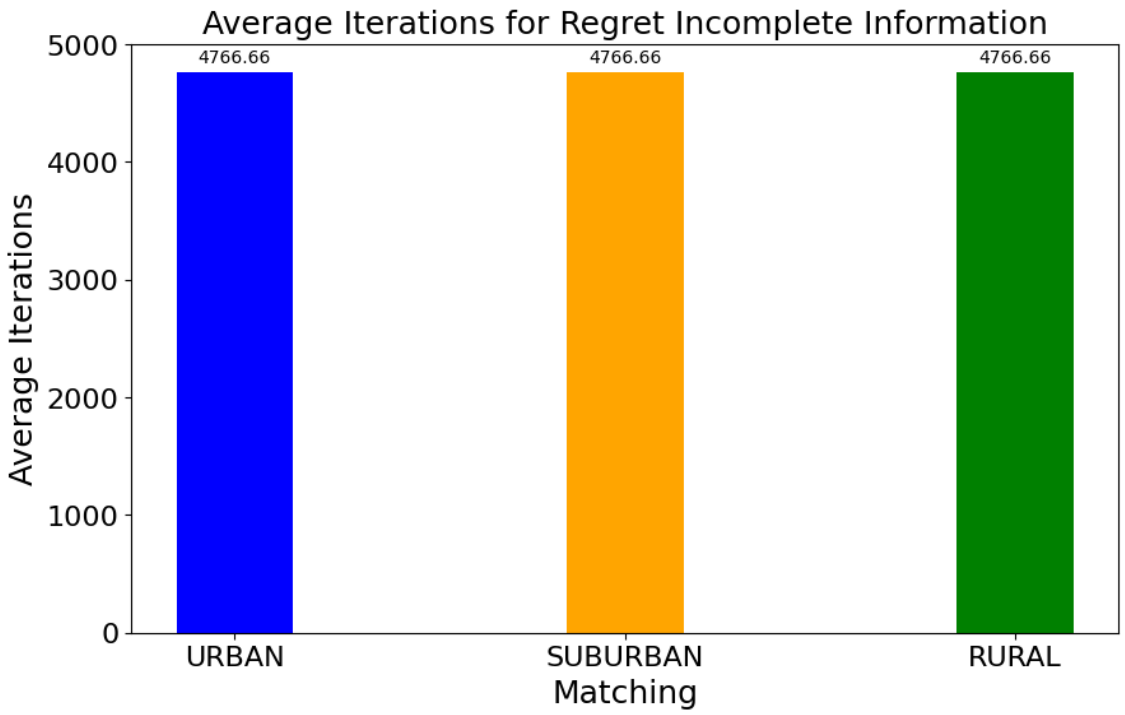


Σχήμα 4.24: Μέσος χρόνος εκτέλεσης ανά αριθμό κόμβων ανά αλγόριθμο αντιστοίχισης

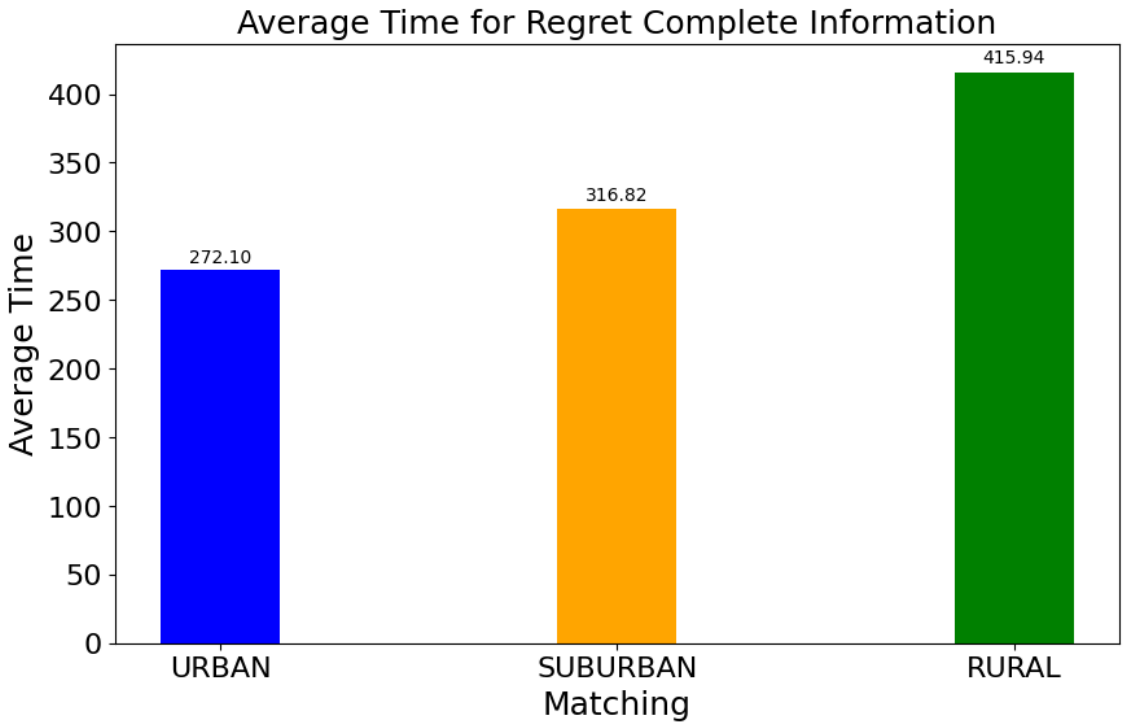
Μελετώντας παραπάνω αυτή τη συμπεριφορά βλέπουμε:



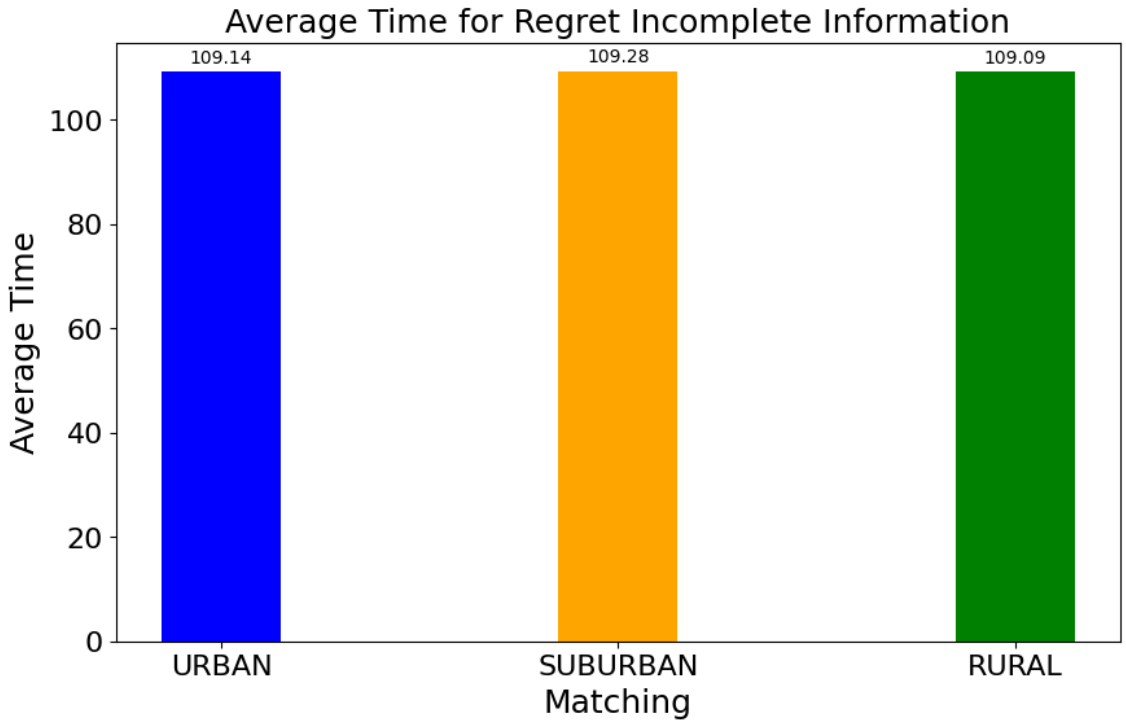
Σχήμα 4.25: Επαναλήψεις Αλγορίθμου Πλήρους Πληροφορίας ανά Περιοχή



Σχήμα 4.26: Επαναλήψεις Αλγορίθμου Ελλιπούς Πληροφορίας ανά Περιοχή

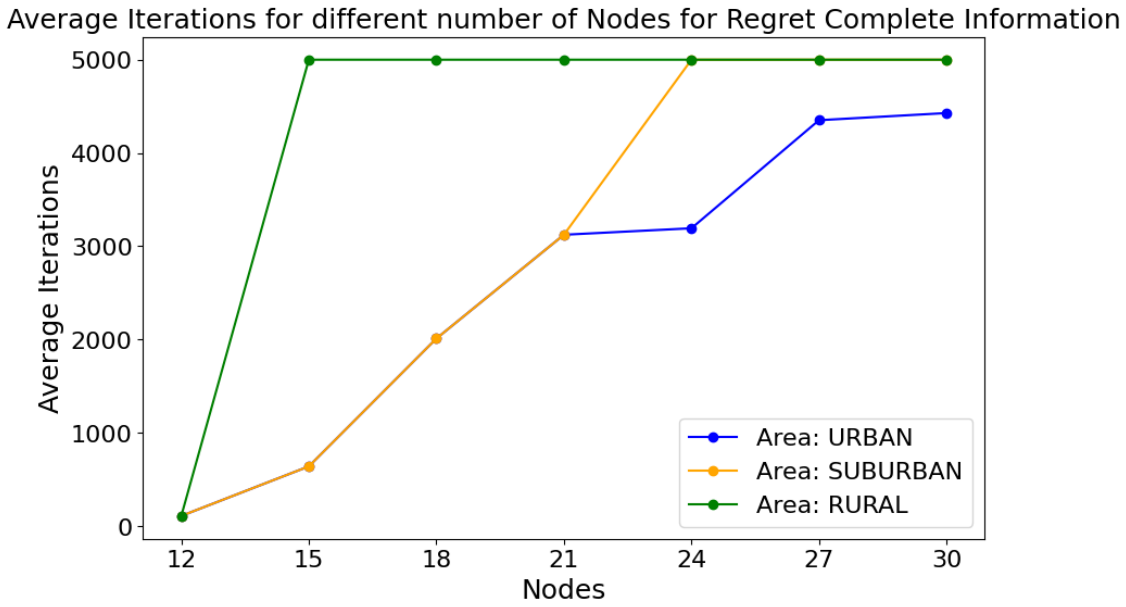


Σχήμα 4.27: Χρόνος Εκτέλεσης Αλγορίθμου Πλήρους Πληροφορίας ανά Περιοχή



Σχήμα 4.28: Χρόνος Εκτέλεσης Αλγορίθμου Ελλιπούς Πληροφορίας ανά Περιοχή

Στα σχήματα 4.25 και 4.26 γίνεται εμφανής η παρατήρηση που κάναμε παραπάνω. Όσο πιο πολλοί απομακρυσμένοι κόμβοι ζουν στο σύστημά μας τόσο περισσότερο δυσκολεύεται να φτάσει σε σύγκλιση ο αλγόριθμος Πλήρους Πληροφορίας σε αντίθεση με τον Ελλιπούς Πληροφορίας. Αντίστοιχα αυτό μας οδηγεί στα διαγράμματα 4.27 και 4.28, όπου αντίστοιχα με τον αριθμό των επαναλήψεων του αλγορίθμου έχουμε και διαμόρφωση των χρόνων εκτέλεσης. Η διαφοροποίηση αυτή στους δύο αλγορίθμους συμβαίνει, διότι όσο πιο μακρινούς κόμβους έχουμε, τόσο πιο δύσκολη είναι η σύγκλιση στον αλγόριθμο Πλήρους Πληροφορίας στην βέλτιστη διαμόρφωση του κόμβου, διότι αυτή κατά πάσα πιθανότητα διαφέρει από άλλες κατά πολύ λίγο και συνεπώς, οι τιμές μετάνοιας για τις κοντινές αυτές πράξεις μειώνονται με πολύ αργό ρυθμό. Αντίθετα, στον αλγόριθμο Ελλιπούς Πληροφορίας η αρχικοποίηση των χρησιμοτήτων, σε συνδυασμό με το γεγονός πως σε κάθε επανάληψη δεν ενημερώνονται όλες οι χρησιμότητες, αλλά και λόγω του λευκού θορύβου που δημιουργεί μεγαλύτερες διαφορές στις χρησιμότητες, επιτυγχάνουμε παρόμοια σύγκλιση σε όλες τις περιπτώσεις.



Σχήμα 4.29: Μέσος αριθμός επαναλήψεων ανά αριθμό κόμβων ανά περιοχή για τον αλγόριθμο Πλήρους Πληροφορίας

Στο διάγραμμα 4.29 βλέπουμε πιο αναλυτικά την διακύμανση των απαιτούμενων επαναλήψεων για τον αλγόριθμο Πλήρους Πληροφορίας, ανά περιοχή, όσο αυξάνεται ο αριθμός των κόμβων. Είναι εμφανές, πως όταν αρχίσουν σε κάθε περιοχή να εισέρχονται πιο απομακρυσμένοι κόμβοι, η σύγκλιση δυσχεραίνει. Αντίστοιχα, όσο περισσότεροι κόμβοι υπάρχουν στο σύστημά μας, τόσο πιο δύσκολη γίνεται η σύγκλιση, αφού κατ' αρχήν θέλουμε όλοι μας οι κόμβοι να συγκλίνουν, ενώ επιπλέον, αφού το περιβάλλον μας είναι ανταγωνιστικό, οι αλλαγές συμπεριφοράς ενός κόμβου είναι πιθανό να επηρεάσουν και τους υπολοίπους στη βέλτιστη επιλογή τους.

5

Συμπεράσματα

Έπειτα από μελέτη των διαφόρων σεναρίων, αλγορίθμων και αποτελεσμάτων μπορούμε να καταλήξουμε σε κάποια γενικά συμπεράσματα από την διαδικασία αυτής της διπλωματικής εργασίας.

Η Ομοσπονδιακή Μάθηση είναι ένας μηχανισμός που μας επιτρέπει να εξάγουμε πληροφορία από δεδομένα, χωρίς να αποκτούμε συνολική πρόσβαση σε αυτά. Έτσι διασφαλίζουμε την ιδιωτικότητα, που είναι απαραίτητη ιδιαίτερα σε συγκεκριμένους τομείς, πετυχαίνοντας παράλληλα την εκπαίδευση των μοντέλων που χρειαζόμαστε. Στην περίπτωσή μας, είχαμε τρία μοντέλα, τα οποία εκπαιδεύονταν από τους κόμβους του περιβάλλοντός μας. Ο κάθε ένας κόμβος διέθετε μια συγκεκριμένη ποσότητα και τύπο δεδομένων και άρα θα είχε διαφορετική σημασία για κάθε μοντέλο - εξυπηρετητή. Αυτό αποδίδεται στους αλγορίθμους μας με τις συναρτήσεις χρησιμότητας. Τις συναρτήσεις αυτές φαίνεται να διαχειρίζεται καλύτερα ο αλγόριθμος Θεωρίας Παιγνίων, ο οποίος καταφέρνει να κάνει τις καλύτερες αντιστοιχίσεις, κρατώντας τις χρησιμότητες υψηλότερα από τους υπόλοιπους αλγορίθμους. Συνεπώς, είναι ευθύνη μας να χτίσουμε μία αντιπροσωπευτική συνάρτηση χρησιμότητας που να αντικατοπτρίζει ορθά το πρόβλημα και τις παραμέτρους του.

Όπως είδαμε ακόμη και με μία σχετικά απλή συνάρτηση χρησιμότητας, ο αλγόριθμος Θεωρίας Παιγνίων προσπαθώντας να την μεγιστοποιήσει καταφέρνει να πετύχει υψηλή ροή δεδομένων, χαμηλή ενέργεια μετάδοσης και καλύτερη επίδοση στην Ομοσπονδιακή Μάθηση έναντι των υπόλοιπων αλγορίθμων αντιστοίχισης. Παρ' όλα ταύτα, και οι άλλοι αλγόριθμοι πετυχαίνουν πολύ καλά αποτελέσματα, με τον αλγόριθμο Ενισχυτικής Μάθησης να είναι κοντά ως προς τη χρησιμότητα κόμβων. Είναι επίσης σημαντικό να επαναλάβουμε πως και να γίνει κάποια μη βέλτιστη αντιστοίχιση και να υπάρχει κάποιος μη χρήσιμος κόμβος στον συνασπισμό ενός εξυπηρετητή, ο μηχανισμός της ανάθεσης βαρών για την διαδικασία της Ομοσπονδιακής Μάθησης επιτρέπει να μην επηρεαστεί ιδιαίτερα η επίδοση του συγκεντρωτικού μοντέλου. Μία επιπλέον βελτίωση θα ήταν ένας εξυπηρετητής να μην λαμβάνει υπόψη του κάποιον κόμβο ο οποίος έχει πολύ μικρό βάρος έτσι ώστε να μην καταναλώνονται πόροι για την τοπική εκπαίδευση και μετάδοση των παραμέτρων του μοντέλου. Από την άλλη πλευρά με μη βέλτιστη αντιστοίχιση δεν αξιοποιείται πληροφορία που για κάποιον άλλο εξυπηρετητή θα ήταν χρήσιμη. Έτσι, ξεχωρίζουμε την ικανότητα του αλγορίθμου Θεωρίας Παιγνίων να κάνει βέλτιστη αντιστοίχιση σχεδόν σε κάθε ένα από τα σενάρια που του ανατέθηκαν. Προφανώς ο αλγόριθμος αυτός μπορεί να εφαρμοστεί και σε

περιπλοκότερα συστήματα, με περισσότερους κόμβους, εξυπηρετητές και κρίσιμα σημεία, αλλά και με πιο σύνθετες συναρτήσεις χρησιμότητας (όπως είδαμε και στο κεφάλαιο 4).

Στο κεφάλαιο 4, εξετάσαμε μία άλλη προσέγγιση στο υπάρχον πρόβλημα. Οι κόμβοι πέρα από την συσχέτισή τους με τους εξυπηρετητές, μπορούν να διαμορφώσουν την συμμετοχή τους στην διαδικασία της Ομοσπονδιακής Μάθησης. Αυτό δίνει την ευελιξία στο σύστημά μας να μεγιστοποιήσει τις συναρτήσεις χρησιμότητας περαιτέρω, επιτρέποντας σε κόμβους που είναι πιο απομακρυσμένοι ή με λιγότερη πληροφορία να συμμετέχουν λιγότερο. Το μεγάλο πλεονέκτημα των αλγορίθμων Μετανοητικής Μάθησης που εφάρμοσαν την παραπάνω στρατηγική ήταν στην μεγάλη μείωση στην ενέργεια εκπαίδευσης των τοπικών μοντέλων, το οποίο αντίστοιχα μεταφράζεται και σε μείωση του χρόνου που απαιτείται για την εκπαίδευση, αφού οι πιο απομακρυσμένοι κόμβοι τείνουν να συμμετέχουν με λιγότερα δεδομένα, εφ' όσον οι κοντινοί στα κρίσιμα σημεία κόμβοι διαθέτουν την περισσότερη και κύρια πληροφορία. Όπως είδαμε φτάνουμε αρκετά κοντά σε απόδοση στην Ομοσπονδιακή Μάθηση σε σχέση με την απόλυτη προσέγγιση του αλγορίθμου Θεωρίας Παιγνίων. Όμως πετυχαίνουμε καλύτερη χρησιμότητα, με μικρότερες ενέργειες εκπαίδευσης και μετάδοσης και μεγαλύτερη ροή δεδομένων.

Αντίστοιχα, οι δυο διαφορετικές προσεγγίσεις στην Μετανοητική Μάθηση μας δείχνουν πως δεν χρειάζεται να γνωρίζουμε τις ακριβείς συμπεριφορές όλων των κόμβων στο σύστημά μας για να πάρουμε ένα εξίσου καλό, αλλά και πολύ πιο γρήγορο αποτέλεσμα. Ο αλγόριθμος Πλήρους Πληροφορίας τείνει να κάνει καλύτερες επιλογές απ' ότι ο Ελλιπούς Πληροφορίας, αλλά εν' τέλει η διαφορά είναι αρκετά μικρή ώστε να δίνει πλεονέκτημα στον μικρό χρόνο εκτέλεσης του αλγορίθμου Ελλιπούς Πληροφορίας και στην πιο γρήγορη σύγκλισή του. Συνεπώς ο αλγόριθμος αυτός κάνει μια πολύ γρήγορη αντιστοίχιση (παίρνοντας υπόψη το πόσες διαφορετικές επιλογές υπάρχουν για τον κάθε κόμβο) και πετυχαίνει υψηλές χρησιμότητες κατά μέσο όρο μένοντας λίγο πίσω από τον Πλήρους Πληροφορίας. Όσον αφορά την Ομοσπονδιακή Μάθηση έχει την μικρότερη επίδοση, όμως μένει αξιοπρεπώς κοντά στους άλλους δύο.

Τα σενάρια που μελετήσαμε μπορούν να εφαρμοστούν αντίστοιχα και σε άλλες περιπτώσεις. Η Αστική, Προαστιακή και Αγροτική Περιοχή μπορούν να δώσουν πληροφορίες για την συμπεριφορά των μοντέλων στον πραγματικό κόσμο αλλά επιτρέπει και να μελετηθούν περιπτώσεις χρήσιμων και λιγότερο χρήσιμων κόμβων. Με την πληθώρα εφαρμογών της Ομοσπονδιακής Μάθησης ένα τέτοιο οικοσύστημα μπορεί να χρησιμοποιηθεί και με άλλα δεδομένα ή για άλλα μοντέλα. Για παράδειγμα σε σενάριο μίας Έξυπνης Πόλης, μπορεί αντί για Δημόσια Ασφάλεια (πυρκαγιές, πλημμύρες, σεισμοί) να εξετασθεί μια περίπτωση αυτόματης ρύθμισης της κυκλοφορίας στους δρόμους. Το μοντέλο που χρησιμοποιήθηκε (MobileNetV3) είναι ένα πολύ μικρό σε μέγεθος και υπολογιστική πολυπλοκότητα και άρα ιδανικό για εγκατάσταση σε οποιαδήποτε συσκευή. Επιπλέον, με την τεχνική εξαγωγής δεδομένων, το ακριβό υπολογιστικά κομμάτι ανάλυσης των εικόνων γίνεται μία μόνο φορά, επιτρέποντας φθηνές επαναλήψεις στην διαδικασία της Ομοσπονδιακής Μάθησης. Αντίστοιχα, με άλλα μοντέλα (όχι εικόνων) μπορούν να μελετηθούν άλλα φαινόμενα. Για παράδειγμα, η μελέτη του κινδύνου πυρκαγιών μέσω μετρήσεων θερμοκρασίας ή η πρόγνωση σεισμών μέσω δεδομένων από δίκτυα σεισμικής παρακολούθησης, αποτελούν δύο διαφορετικές προσεγγίσεις στο πρόβλημα το οποίο εμείς εξετάσαμε με εικόνες. Στο πλαίσιο των εικόνων - δεδομένων, προφανώς με ελάχιστες αλλαγές μπορούν να δοκιμασθούν και άλλα μοντέλα, όπως τα

μοντέλα EfficientNet. Ανάλογα την εφαρμογή μπορεί να κάνουν καλύτερη εξαγωγή χαρακτηριστικών από τις εικόνες και αξίζει να γίνει μελέτη για την κατάλληλη επιλογή.

Βιβλιογραφία

[ABL15] Alessandro Acquisti, Laura Brandimarte και George Loewenstein. «Privacy and human behavior in the age of information». Στο: *Science* 347.6221 (2015), σσ. 509–514.

[Abr15] Myriam Abramson. «Toward Adversarial Online Learning and the Science of Deceptive Machines». Στο: *Papers from the AAAI 2015 Fall Symposium: Deceptive and Counter-Deceptive Machines*. Washington, DC, 2015.

[ACF22] M. Mehdi Afsar, Trafford Crump και Behrouz Far. «Reinforcement Learning Based Recommender Systems: A Survey». Στο: *ACM Computing Surveys* 55.6 (2022), σσ. 1–38. DOI: 10.1145/3543846. URL: https://dl.acm.org/doi/10.1145/3543846.

[Ama24] Amazon Web Services. *Overfitting*. 2024. URL: https://aws.amazon.com/what-is/overfitting/#:~:text=Overfitting%20occurs%20when%20the%20model,all%20possible%20input%20data%20values..

[Ari+23] S. Arisdakessian κ.ά. «Towards instant clustering approach for federated learning client selection». Στο: *2023 Int. Conf. on Comp., Networking and Comm.* 2023, σσ. 409–413.

[BHD23] Aki Barry, Lei Han και Gianluca Demartini. «On the Impact of Data Quality on Image Classification Fairness». Στο: *Proceedings of the [Insert Conference Name]*. The University of Queensland. Australia, 2023.

[Blu03] Avrim Blum. *Regret Minimization in Game Theory and Machine Learning*. 2003. URL: https://www.cs.cmu.edu/~avrim/Papers/regret-chapter.pdf.

[CDP23a] P. Charatsaris, M. Diamanti και S. Papavassiliou. «On the accuracy-energy tradeoff for hierarchical federated learning via satisfaction equilibrium». Στο: *2023 19th Int. Conf. on Distributed Computing in Smart Systems and the Internet of Things*. 2023, σσ. 422–428.

[CDP23b] Panagiotis Charatsaris, Maria Diamanti και Symeon Papavassiliou. «On the Accuracy-Energy Tradeoff for Hierarchical Federated Learning via Satisfaction Equilibrium». Στο: *Proceedings of the 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSSIoT)*. Institute of Communication, Computer Systems, School of Electrical και Computer Engineering, 2023.

[CEW11] Georgios Chalkiadakis, Edith Elkind και Michael Wooldridge. *Computational Aspects of Cooperative Game Theory*. Morgan & Claypool Publishers, 2011.

[Cho18] François Chollet. *Deep Learning with Python*. Manning Publications, 2018.

[FK22] AlMahamid Fadi και Grolinger Katarina. «Reinforcement Learning Algorithms: An Overview and Classification». Στο: *arXiv preprint arXiv:2209.14940* (2022). URL: https://arxiv.org/abs/2209.14940.

[Gau+22] F. Gauthier κ.ά. «Clustered graph federated personalized learning». Στο: *2022 56th Asilomar Conference on Signals, Systems, and Computers*. 2022, σσ. 744–748.

[GBC16] Ian Goodfellow, Yoshua Bengio και Aaron Courville. *Deep Learning*. Available online at https://www.deeplearningbook.org. MIT Press, 2016.

[How+19] Andrew Howard, Mark Sandler, Grace Chu, Liang-Chieh Chen, Bo Chen, Mingxing Tan, Weijun Wang, Yukun Zhu, Ruoming Pang, Vijay Vasudevan κ.ά. «Searching for MobileNetV3». Στο: *Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV)*. 2019, σσ. 1314–1324.

[HR18] Jeremy Howard και Sebastian Ruder. «Universal Language Model Fine-tuning for Text Classification». Στο: *Proceedings of the 56th Annual Meeting of the Association for Computational Linguistics (ACL)*. 2018.

[HSS18] Jie Hu, Li Shen και Gang Sun. «Squeeze-and-Excitation Networks». Στο: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*. 2018, σσ. 7132–7141.

[L23] Jerry W. Z. L. *Hierarchical Federated Learning*. 2023. URL: https://github.com/wzljerry/Hierarchical-Federated-Learning/blob/main/FL.ipynb.

[LBH15] Yann LeCun, Yoshua Bengio και Geoffrey Hinton. «Deep Learning». Στο: *Nature* 521.7553 (2015), σσ. 436–444.

[Liu+24] Bingyan Liu, Nuoyan Lv, Yuanchun Guo και Yawen Li. «Recent advances on federated learning: A systematic survey». Στο: *Artificial Intelligence* (2024). Beijing University of Posts and Telecommunications, HaiDian, Beijing, 100871, China. URL: https://www.sciencedirect.com/science/article/abs/pii/S0004370224000181.

[McM+17] Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson και Blaise Aguera y Arcas. «Communication-Efficient Learning of Deep Networks from Decentralized Data». Στο: *arXiv preprint arXiv:1602.05629* (2017).

[OR94] Martin J. Osborne και Ariel Rubinstein. *A Course in Game Theory*. MIT Press, 1994.

[RS92] Alvin E. Roth και Marilda Sotomayor. *Two-Sided Matching: A Study in Game-Theoretic Modeling and Analysis*. Cambridge University Press, 1992.

[RZL17] Prajit Ramachandran, Barret Zoph και Quoc V Le. «Searching for activation functions». Στο: *arXiv preprint arXiv:1710.05941* (2017).

[Sam+13] Sumudu Samarakoon, Mehdi Bennis, Walid Saad και Matti Latva-aho. «Backhaul-Aware Interference Management in the Uplink of Wireless Small Cell Networks». Στο: *IEEE Transactions on Wireless Communications* (2013).

[SB18a] Richard S. Sutton και Andrew G. Barto. *Reinforcement Learning: An Introduction*. 2nd. MIT Press, 2018.

[SB18b] Richard S. Sutton και Andrew G. Barto. «Upper-Confidence-Bound Action Selection». Στο: *Reinforcement Learning: An Introduction*. 2nd. MIT Press, 2018. Κεφ. 2.7, σσ. 35–36. URL: `https://web.mit.edu/reinforcement_learning/RLbook2020.pdf`.

[Set12] Burr Settles. *Active Learning*. Morgan & Claypool Publishers, 2012.

[TZD23] C. Tu, S. Zhao και H. Deng. «Fedwns: Data distribution-wise node selection in federated learning via reinforcement learning». Στο: *26th Int. Conf. on Comput. Supported Coop. Work in Design*. 2023, σσ. 600–605.

[Weh+22] O. Wehbi κ.ά. «Towards bilateral client selection in federated learning using matching game theory». Στο: *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*. 2022, σσ. 01–06.

[Weh+23] O. Wehbi κ.ά. «Towards mutual trust-based matching for federated learning client selection». Στο: *2023 International Wireless Communications and Mobile Computing (IWCMC)*. 2023, σσ. 1112–1117.

[Wik24] Wikipedia contributors. *Utility*. 2024. URL: `https://en.wikipedia.org/wiki/Utility`.

[WLW22] X. Wei, J. Liu και Y. Wang. «Joint participant selection and learning scheduling for multi-model federated edge learning». Στο: *2022 IEEE 19th Int. Conf. on Mobile Ad Hoc and Smart Systems*. 2022, σσ. 537–545.

[Xu+24] Yanran Xu, Kangxin He, Shu Hu και Hui Li. «A reinforcement learning framework based on regret minimization for approximating best response in fictitious self-play». Στο: *IEEE* (2024). URL: `https://ieeexplore.ieee.org/document/10074743`.

[XZX22] S. Xin, L. Zhuo και C. Xin. «Node selection strategy design based on reputation mechanism for hierarchical federated learning». Στο: *2022 18th Int. Conf. on Mobility, Sensing and Networking*. 2022, σσ. 718–722.

[ZL16] Barret Zoph και Quoc V Le. «Neural architecture search with reinforcement learning». Στο: *arXiv preprint arXiv:1611.01578*. 2016.

Γλωσσάριο

Απόδοση	Ξενόγλωσσος όρος
Ομοσπονδιακή Μάθηση	Federated Learning (FL)
Θεωρία Παιγνίων	Game Theory
Ενισχυτική Μάθηση	Reinforcement Learning (RL)
Μετανοητική Μάθηση	Regret Learning
Παιχνίδι Αντιστοίχισης	Matching Game
Παιχνίδι Συμμαχίας/Συνασπισμών	Coalition Game
Συνάρτηση Χρησιμότητας	Utility Function
Νευρωνικά Δίκτυα	Neural Networks
Ταξινόμηση Εικόνας	Image Classification
Ακρίβεια	Accuracy
Απώλεια	Loss
Κανονικοποίηση	Normalization
Υπερπροσαρμογή	Overfitting
Εξαγωγή Χαρακτηριστικών	Feature Extraction
Προ-εκπαιδευμένο Μοντέλο	Pre-trained Model
Αρχιτεκτονική Μοντέλων	Model Architecture
Ενεργή Μάθηση	Active Learning
Σενάρια Δημόσιας Ασφάλειας	Public Safety Scenarios
Φυσικές Καταστροφές	Natural Hazards
Κόμβοι	Nodes
Εξυπηρετητές	Servers
Συνασπισμοί	Coalitions
Κεντρική Μονάδα Επεξεργασίας (ΚΜΕ)	Central Processing Unit (CPU)
Ροή Δεδομένων	Datarate
Εύρος Ζώνης	Bandwidth
Λευκός Προσθετικός Θόρυβος Γκάους	Additive White Gaussian Noise (AWGN)
Συγκεντρωτικό/Παγκόσμιο Μοντέλο	Global Model

Συνάρτηση Ενεργοποίησης	Activation Function
Επίπεδο Απόφασης	Decision Layer
Κρίσιμο Σημείο/Σημείο Ενδιαφέροντος	Point of Interest (POI)
Αλγόριθμος Ανώτατου Ορίου Αυτοπεποίθησης	Upper Confidence Bound Algorithm (UCB)
Ρυθμός Εκμάθησης	Learning Rate
Εκμάθηση Πλήρους Πληροφορίας	Complete Information Learning
Εκμάθηση Ελλιπούς Πληροφορίας	Incomplete Information Learning