ΠΑΝΕΠΙΣΤΗΜΙΟ
ΙΩΑΝΝΙΝΩΝ

ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΧΑΡΤΟΓΡΑΦΗΣΗ ΤΗΣ ΕΞΕΛΙΞΗΣ ΤΟΥ DNS ΜΕΣΩ ΒΙΒΛΙΟΜΕΤΡΙΚΗΣ ΑΝΑΛΥΣΗΣ

Πετσέρη Μαρία

Επιβλέπουσα: Σπυριδούλα Μαργαρίτη

ΕΔΙΠ, Α

Άρτα, Ιούνιος, 2026

MAPPING THE EVOLUTION OF DNS THROUGH BIBLIOMETRIC ANALYSIS

Εγκρίθηκε από τριμελή εξεταστική επιτροπή

Άρτα, Ιούνιος 2026α

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Επιβλέπουσα καθηγήτρια

   Μαργαρίτη Σπυριδούλα

2. Μέλος επιτροπής

   Λιαροκάπης Δημήτριος

3. Μέλος επιτροπής

   Στεργίου Ελευθέριος

Δήλωση μη λογοκλοπής

Δηλώνω υπεύθυνα και γνωρίζοντας τις κυρώσεις του Ν. 2121/1993 περί Πνευματικής Ιδιοκτησίας, ότι η παρούσα μεταπτυχιακή εργασία είναι εξ ολοκλήρου αποτέλεσμα δικής μου ερευνητικής εργασίας, δεν αποτελεί προϊόν αντιγραφής ούτε προέρχεται από ανάθεση σε τρίτους. Όλες οι πηγές που χρησιμοποιήθηκαν (κάθε είδους, μορφής και προέλευσης) για τη συγγραφή της περιλαμβάνονται στη βιβλιογραφία.

Πετσέρη, Μαρία

Υπογραφή

ΕΥΧΑΡΙΣΤΙΕΣ

Με την ολοκλήρωση της παρούσας πτυχιακής εργασίας, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες σε όλους όσοι συνέβαλαν, άμεσα ή έμμεσα, στην εκπόνησή της.

Θα ήθελα να ευχαριστήσω θερμά την επιβλέπουσα καθηγήτριά μου για την καθοδήγηση, την υποστήριξη και τις πολύτιμες συμβουλές της καθ' όλη τη διάρκεια της εκπόνησης της εργασίας. Η συμβολή της υπήρξε καθοριστική για την ολοκλήρωση της παρούσας προσπάθειας. Επιπλέον, θα ήθελα να ευχαριστήσω την οικογένειά μου για τη συνεχή στήριξη, την κατανόηση και την ενθάρρυνση που μου προσέφερε σε όλη τη διάρκεια των σπουδών μου.

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία μελετά τη διαχρονική εξέλιξη και την επιστημονική χαρτογράφηση του Συστήματος Ονοματοδοσίας Διαδικτύου (DNS), ενός θεμελιώδους μηχανισμού για τη λειτουργία του σύγχρονου Διαδικτύου. Στόχος της μελέτης είναι η ανάδειξη των κυρίαρχων ερευνητικών τάσεων και η ανάλυση της μετάβασης από τις πρώιμες μεθόδους ονοματοδοσίας στις σύγχρονες τεχνολογικές βελτιώσεις ασφάλειας και ιδιωτικότητας. Για την επίτευξη αυτού του στόχου, εφαρμόστηκε βιβλιομετρική ανάλυση σε ένα δείγμα 1.770 δημοσιεύσεων από τη διεθνή βάση δεδομένων Scopus για την περίοδο 1990-2025. Η επεξεργασία και η οπτικοποίηση των βιβλιογραφικών δεδομένων πραγματοποιήθηκε με τη χρήση της γλώσσας προγραμματισμού R και του εξειδικευμένου εργαλείου Biblioshiny. Τα αποτελέσματα δείχνουν μια σταθερά ανοδική τάση στην επιστημονική παραγωγή, με ιδιαίτερη ένταση μετά το 2017. Η έρευνα χαρακτηρίζεται από έντονη γεωγραφική συγκέντρωση, με τα κινεζικά ακαδημαϊκά ιδρύματα να πρωτοστατούν σε όγκο δημοσιεύσεων, ενώ οι ΗΠΑ διατηρούν την πρωτιά σε ερευνητικό αντίκτυπο μέσω των αναφορών. Αξιοσημείωτη είναι η θέση της Ελλάδας, η οποία καταλαμβάνει την 5η θέση στην παγκόσμια κατάταξη αναφορών, υπογραμμίζοντας την ποιότητα και την επίδραση της εγχώριας επιστημονικής συνεισφοράς στο πεδίο. Τέλος, η ανάλυση περιεχομένου δείχνει την τεχνολογική μετατόπιση από το αρχικό συγκεντρωτικό αρχείο hosts.txt στην ιεραρχική δομή και, πλέον, στην υιοθέτηση κρυπτογραφημένων πρωτοκόλλων όπως το DNS-over-TLS (DoT), το DNS-over-HTTPS (DoH) και το DNS-over-QUIC (DoQ). Οι εξελίξεις αυτές ανταποκρίνονται στις σύγχρονες προκλήσεις ασφάλειας και τη διασφάλιση της ιδιωτικότητας, διαμορφώνοντας το μέλλον της διαχείρισης της κίνησης στο Διαδίκτυο.

Λέξεις-κλειδιά:**Λέξεις-κλειδιά:** Σύστημα Ονοματοδοσίας Διαδικτύου (DNS), Βιβλιομετρική Ανάλυση, Ασφάλεια Δικτύων, Κρυπτογραφημένα Πρωτόκολλα, Biblioshiny.

ABSTRACT

This thesis explores the evolution and scientific mapping of the Domain Name System (DNS), a fundamental mechanism for the operation of the modern Internet. The study aims to highlight dominant research trends and analyze the transition from early naming methods to contemporary technological improvements in security and privacy. To achieve this objective, a bibliometric analysis was conducted on a sample of 1,770 publications retrieved from the international Scopus database for the period 1990-2025. The processing and visualization of bibliographic data were performed using the R programming language and the specialized package Biblioshiny. The results demonstrate a consistently upward trend in scientific production, with particular intensity after 2017. The research is characterized by strong geographical concentration, with Chinese academic institutions leading in publication volume, while the USA maintains the lead in research impact through citations. Notably, Greece occupies the 5th position in the global citation ranking, underscoring the quality and impact of domestic scientific contribution to the field. Finally, the content analysis reveals a technological shift from the original centralized hosts.txt file to the hierarchical structure and, currently, to the adoption of encrypted protocols such as DNS-over-TLS (DoT), DNS-over-HTTPS (DoH), and DNS-over-QUIC (DoQ). These developments address modern security challenges and ensure privacy, shaping the future of traffic management on the Internet.

Keywords: Domain Name System (DNS), Bibliometric Analysis, Network Security, Encrypted Protocols, Biblioshiny.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΔΙΑΓΡΑΜΜΑΤΩΝ/ΕΙΚΟΝΩΝ

1.ΕΙΣΑΓΩΓΗ

1.1 Γενικά

Το Σύστημα Ονοματοδοσίας Διαδικτύου (DNS) αποτελεί έναν από τους πλέον θεμελιώδεις μηχανισμούς για τη λειτουργία του σύγχρονου διαδικτύου, έχοντας ως κύριο ρόλο την αντιστοίχιση ονομάτων τομέων (domain names) σε αριθμητικές διευθύνσεις IP. Στις απαρχές του διαδικτύου (εποχή ARPANET), η διαδικασία αυτή γινόταν χειροκίνητα μέσω ενός κεντρικού αρχείου, του hosts.txt, το οποίο όμως κατέστη μη λειτουργικό καθώς ο αριθμός των συνδεδεμένων συσκευών αυξανόταν ραγδαία. Η ανάγκη για ένα σύστημα που θα μπορούσε να κλιμακωθεί οδήγησε στη δημιουργία του DNS από τον Paul Mockapetris το 1983. Το DNS σχεδιάστηκε ως μια ιεραρχική και κατανεμημένη βάση δεδομένων, επιτρέποντας τη διανομή της πληροφορίας σε εκατομμύρια διακομιστές παγκοσμίως. Παρά την επιτυχία του, ο αρχικός σχεδιασμός στερούνταν μηχανισμών ασφαλείας, καθιστώντας το πρωτόκολλο ευάλωτο σε επιθέσεις όπως η δηλητηρίαση προσωρινής μνήμης (cache poisoning). Σήμερα, η έρευνα επικεντρώνεται σε σύγχρονες βελτιώσεις και κρυπτογραφημένα πρωτόκολλα (όπως τα DoT, DoH και DoQ) που στοχεύουν στην ενίσχυση της ιδιωτικότητας και της ασφάλειας των χρηστών.

1.2 Σκοπός και Στόχοι

Ο κύριος σκοπός της παρούσας εργασίας είναι η μελέτη και η χαρτογράφηση της εξέλιξης του επιστημονικού πεδίου του DNS μέσω της μεθοδολογίας της βιβλιομετρικής ανάλυσης. Η εργασία θέλει να αναδείξει πώς έχει μεταβληθεί το ερευνητικό ενδιαφέρον διαχρονικά και ποιες είναι οι κυρίαρχες τάσεις στην παγκόσμια βιβλιογραφία.
Οι επιμέρους στόχοι της μελέτης περιλαμβάνουν:

- Τη διερεύνηση της διαχρονικής εξέλιξης της επιστημονικής έρευνας γύρω από το DNS από το 1990 έως σήμερα.
- Την αναγνώριση των σημαντικότερων συγγραφέων, οργανισμών και χωρών που συνεισφέρουν στο πεδίο.
- Την ανάλυση των κυρίαρχων ερευνητικών θεμάτων και των δικτύων συνεργασίας μεταξύ των ερευνητών.

- Την εξέταση των σύγχρονων τεχνολογικών εξελίξεων και πρωτοκόλλων ασφαλείας που διαμορφώνουν το μέλλον του συστήματος.

1.3 Δομή της Εργασίας

Η εργασία είναι οργανωμένη σε πέντε κύρια κεφάλαια.

- Κεφάλαιο 1 (Εισαγωγή): Παρουσιάζεται το γενικό πλαίσιο, ο σκοπός και η δομή της πτυχιακής εργασίας.
- Κεφάλαιο 2 (Σύστημα Ονοματοδοσίας Διαδικτύου): Αναλύεται η λειτουργία του DNS, η ιεραρχική του δομή, οι τύποι εγγραφών πόρων (Resource Records) και οι μηχανισμοί κλιμάκωσης και επίλυσης ερωτημάτων.
- Κεφάλαιο 3 (Μεθοδολογία και Εργαλεία): Περιγράφεται η διαδικασία συλλογής δεδομένων από τη βάση Scopus και η χρήση του πακέτου Bibliometrix (Biblioshiny) στη γλώσσα προγραμματισμού R για τη διεξαγωγή της ανάλυσης.
- Κεφάλαιο 4 (Βιβλιομετρική Ανάλυση): Παρουσιάζονται τα ευρήματα της έρευνας, συμπεριλαμβανομένης της ετήσιας επιστημονικής παραγωγής, των πιο συχνών πηγών δημοσίευσης και της γεωγραφικής κατανομής της έρευνας.
- Κεφάλαιο 5 (Ανάλυση Περιεχομένου: Η εξέλιξη του DNS): Εξετάζεται η ιστορική μετάβαση από το hosts.txt στο σύγχρονο DNS και αναλύονται οι πρόσφατες βελτιώσεις ασφάλειας και τα κρυπτογραφημένα πρωτόκολλα όπως το DNS-over-TLS και το DNS-over-HTTPS.

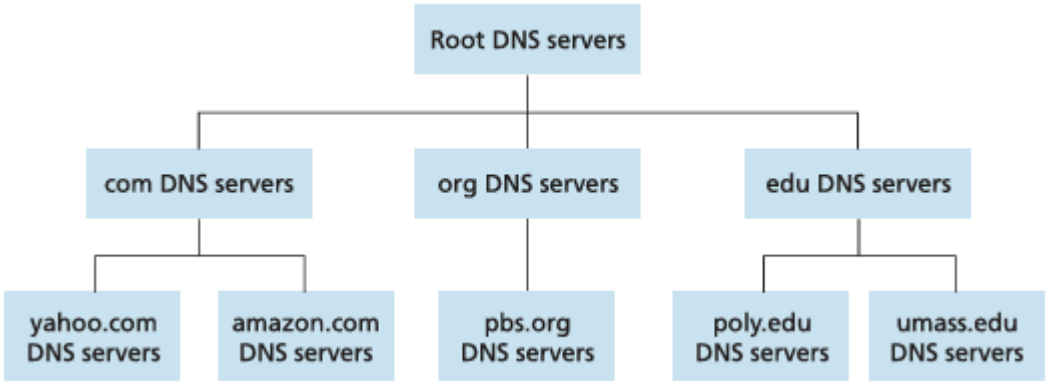
Η εργασία ολοκληρώνεται με την παράθεση των τελικών συμπερασμάτων και της βιβλιογραφίας που χρησιμοποιήθηκε.

2. Σύστημα Ονοματοδοσίας Διαδικτύου (DNS)

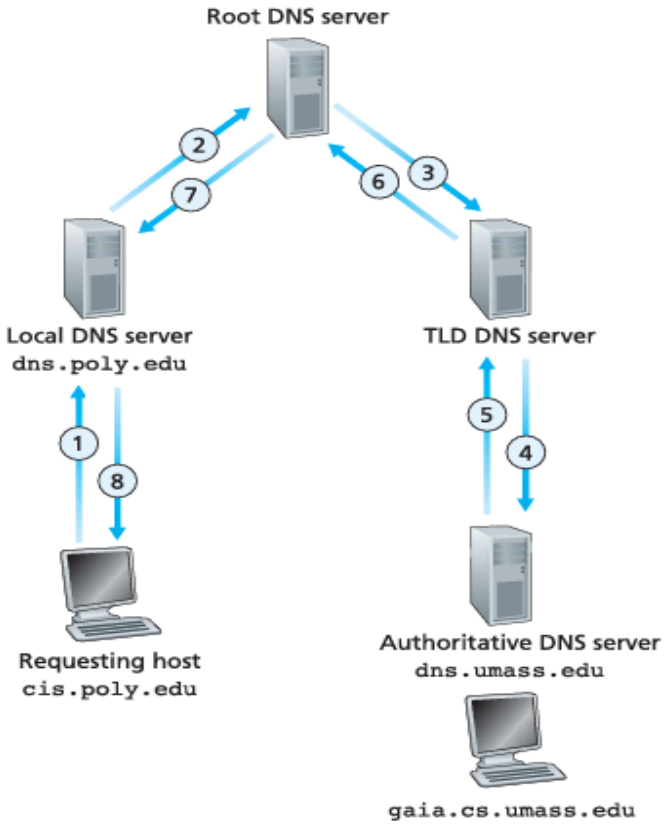
Το Σύστημα Ονοματοδοσίας Διαδικτύου (DNS) αποτελεί έναν από τους βασικότερους μηχανισμούς λειτουργίας του διαδικτύου. Ο κύριος ρόλος του είναι η αντιστοίχιση φιλικών προς τον άνθρωπο ονομάτων τομέων (domain names), όπως *www.example.com*, σε διευθύνσεις IP, οι οποίες χρησιμοποιούνται από τα δίκτυα για την επικοινωνία μεταξύ υπολογιστών. Χωρίς το Σύστημα Ονοματοδοσίας Διαδικτύου οι χρήστες θα έπρεπε να θυμούνται πολύπλοκες αριθμητικές διευθύνσεις, κάτι που θα καθιστούσε τη χρήση του διαδικτύου ιδιαίτερα δύσκολη. Στις πρώτες μέρες του διαδικτύου (ARPANET), ένα αρχείο, το hosts.txt το οποίο ανανεώνονταν κάθε βράδυ, κρατούσε όλους τους συσχετισμούς ονόματος–IP. Αυτό λειτουργούσε ικανοποιητικά για μερικές-εκατοντάδες συσκευές. Όμως καθώς οι συσκευές αυξάνονταν γρήγορα διαπιστώθηκε ότι αυτό δεν θα δούλευε στο μέλλον όχι μόνο γιατί το αρχείο θα γινόταν πολύ μεγάλο αλλά επειδή θα υπήρχαν συγκρούσεις λόγω ύπαρξης ίδιων ονομάτων διευθύνσεων. Κάπως έτσι δημιουργήθηκε το Σύστημα Ονοματοδοσίας Διαδικτύου ,από τον Paul Mockapetris, το 1983 για να λύσει αυτά τα προβλήματα. Το Σύστημα Ονοματοδοσίας Διαδικτύου δεν είναι απλώς μία υπηρεσία καταλόγου αλλά ένα σύνθετο κατανεμημένο συστημα (Kurose and Ross, 2017).

2.1 Πως λειτουργεί το Σύστημα Ονοματοδοσίας Διαδικτύου (DNS)

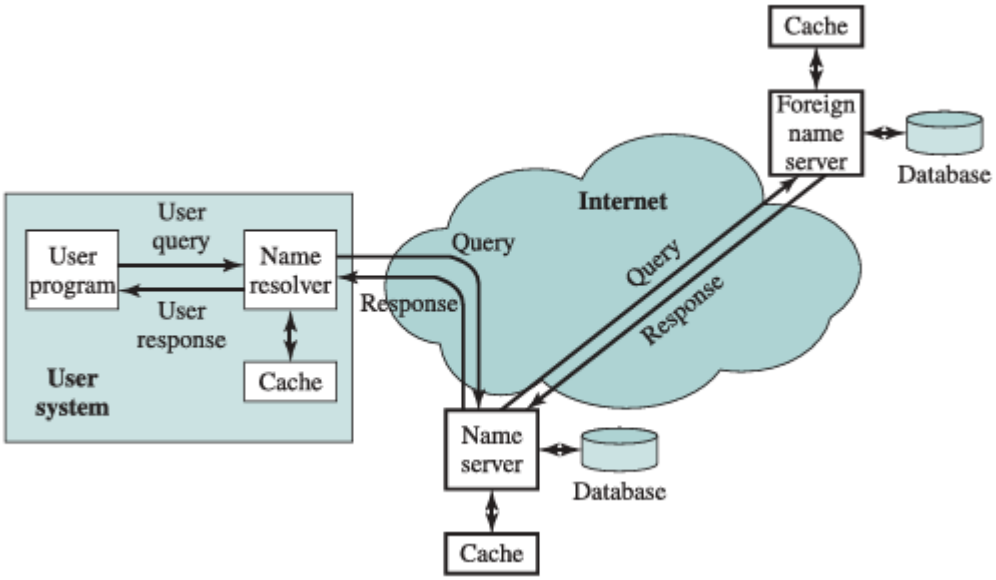
Η λειτουργία του βασίζεται σε μια ιεραρχική δομή τριών επιπέδων. Στην κορυφή των διακομιστών βρίσκονται οι 13 κεντρικοί διακομιστές ριζών (root name servers), οι οποίοι κατευθύνουν τα ερωτήματα προς τους κατάλληλους Ανωτάτου Επιπέδου διακομιστές (Top Level Domain servers), για καταλήξεις όπως .org, .edu, καθώς και για εθνικούς κωδικούς όπως .gr ή .uk. και τελικά στους εξουσιοδοτημένους διακομιστές (authoritative servers) που ανήκουν σε οργανισμούς και κατέχουν τις τελικές εγγραφές για τον συγκεκριμένο τομέα. Κάθε οργανισμός που διαθέτει δημόσια προσβάσιμους υπολογιστές πρέπει να παρέχει εγγραφές DNS που αντιστοιχίζουν τα ονόματα αυτών των υπολογιστών σε διευθύνσεις IP. Σημαντικό ρόλο παίζει επίσης ο τοπικός διακομιστής DNS (local DNS server), ο οποίος λειτουργεί ως μεσάζων και χρησιμοποιεί το DNS caching για να αποθηκεύει προσωρινά τις πληροφορίες, μειώνοντας έτσι τον αριθμό των μηνυμάτων που απαιτούνται και την καθυστέρηση του συστήματος (Stallings, 2014).



Εικόνα 1 Ιεραρχία διακομιστών (Kurose and Ross, 2017).



Εικόνα 2 Παράδειγμα αναζήτησης διεύθυνσης σελίδας (Kurose and Ross, 2017).



Εικόνα 3 Αρχιτεκτονική DNS (Stallings, 2014).

2.2 Εγγραφές Πόρων (Resource Records - RRs)

Στη βάση δεδομένων του DNS υπάρχουν εγγραφές πόρων (Resource Records), οι οποίες έχουν μια συγκεκριμένη δομή που περιλαμβάνει το όνομα τομέα (domain name), τον τύπο της εγγραφής (type), την κλάση πρωτοκόλλου (class), τον χρόνο ζωής (Time to Live - TTL) και τα δεδομένα του πόρου (Rdata). Υπάρχουν διάφοροι τύποι εγγραφών, όπως η εγγραφή 'A' για διευθύνσεις IPv4, η 'AAAA' για διευθύνσεις IPv6, η 'MX' για διακομιστές αλληλογραφίας και η 'NS' που υποδεικνύει τον εξουσιοδοτημένο διακομιστή ονομάτων για έναν τομέα. Ο χρόνος ζωής (TTL) είναι σημαντικός καθώς καθορίζει για πόσο διάστημα μια εγγραφή μπορεί να παραμείνει στην μνήμη (cache) ενός διακομιστή πριν θεωρηθεί παρωχημένη και χρειαστεί εκ νέου αναζήτηση (Tanenbaum & Wetherall, 2011).

Οι εγγραφές πόρων (Resource Records – RRs) αποτελούν τη βασική μονάδα πληροφορίας στο Σύστημα Ονοματοδοσίας Διαδικτύου (DNS). Κάθε εγγραφή αντιστοιχεί ένα όνομα τομέα (domain name) με συγκεκριμένα δεδομένα και αποθηκεύεται στους DNS servers. Το Σύστημα Ονοματοδοσίας Διαδικτύου λειτουργεί κυρίως πάνω από το UDP στη θύρα 53, καθώς απαιτεί ταχύτητα και χαμηλή επιβάρυνση. Ωστόσο, μπορεί να χρησιμοποιηθεί και

το TCP για μεγαλύτερες μεταφορές δεδομένων (π.χ. μεταφορές ζωνών) ή όταν η ασφάλεια απαιτεί DoT (DNS over TLS) ή DoH (DNS over HTTPS).

Κάθε Εγγραφή Πόρων αποτελείται από τα εξής βασικά πεδία:

- ***Name***: Το όνομα τομέα στο οποίο αναφέρεται η εγγραφή
- ***Type***: Ο τύπος της εγγραφής (π.χ. A, MX, CNAME)
- ***Class***: Συνήθως IN (Internet)
- ***TTL (Time to Live)***: Χρόνος αποθήκευσης στην cache
- ***RDATA:*** Τα πραγματικά δεδομένα της εγγραφής

Οι σημαντικότεροι τύποι εγγραφών είναι οι εξής:

- ***A (Address Record)***: Αντιστοιχίζει ένα domain name σε διεύθυνση IPv4.
- ***AAAA***: Αντιστοιχίζει ένα domain name σε διεύθυνση IPv6.
- ***CNAME (Canonical Name)***: Δηλώνει ότι ένα domain είναι ψευδώνυμο (alias) ενός άλλου.
- ***MX (Mail Exchange)***: Καθορίζει τους mail servers που διαχειρίζονται την ηλεκτρονική αλληλογραφία για ένα domain.
- ***NS (Name Server)***: Δηλώνει τους εξουσιοδοτημένους DNS servers για ένα domain.
- ***TXT***: Χρησιμοποιείται για αποθήκευση αυθαίρετων πληροφοριών (π.χ. SPF, verification).

Οι εγγραφές αυτές επιτρέπουν στο DNS να λειτουργεί ως μια κατανεμημένη βάση δεδομένων, η οποία μεταφράζει τα ονόματα τομέων σε πληροφορίες χρήσιμες για τη λειτουργία του διαδικτύου.

2.2.1 DNS Queries

Κατά τη διαδικασία των ερωτημάτων χρησιμοποιούνται δύο βασικές τεχνικές: η αναδρομική (recursive) και η επαναληπτική (iterative). Στην αναδρομική τεχνική, ο διακομιστής ονομάτων αναλαμβάνει την πλήρη ευθύνη να βρει την απάντηση ρωτώντας άλλους διακομιστές για λογαριασμό του πελάτη. Αντίθετα, στην επαναληπτική τεχνική, ο διακομιστής επιστρέφει στον πελάτη τη διεύθυνση του επόμενου διακομιστή που πρέπει να ρωτήσει, μεταφέροντας το βάρος της αναζήτησης στον επιλυτή του πελάτη.

2.2.2 Κλιμάκωση (scaling)

Η κλιμάκωση (scaling) του Συστήματος Ονοματοδοσίας Διαδικτύου είναι η ικανότητα του συστήματος να ανταπεξέρχεται αποτελεσματικά στη συνεχή και γρήγορη ανάπτυξη του διαδικτύου, διαχειριζόμενο έναν ολοένα και αυξανόμενο όγκο ονομάτων και ερωτημάτων χωρίς να υποβαθμίζεται η απόδοσή του. Η κλιμάκωση επιτυγχάνεται πρωτίστως μέσω της ιεραρχικής δομής του συστήματος, η οποία εφαρμόζεται στα ονόματα, στην αυθεντία (authority) και στην υποδομή. Ένας κεντρικός σχεδιασμός θα αντιμετώπιζε ανυπέρβλητα προβλήματα, όπως το μοναδικό σημείο αποτυχίας, τον υπερβολικό όγκο κίνησης και τις μεγάλες καθυστερήσεις στην απόκριση για απομακρυσμένους πελάτες. Για την επίλυση αυτών των ζητημάτων, το Σύστημα Ονοματοδοσίας Διαδικτύου διανέμει τις πληροφορίες του σε εκατομμύρια εξυπηρετητές παγκοσμίως, οι οποίοι είναι οργανωμένοι σε επίπεδα (root, TLD και authoritative servers). Επιπλέον, ο διαχωρισμός του χώρου ονομάτων σε μη επικαλυπτόμενες ζώνες, καθεμία από τις οποίες διοικείται από μια συγκεκριμένη αρχή, επιτρέπει την αποκεντρωμένη διαχείριση και ενημέρωση των δεδομένων, αποτρέποντας τη δημιουργία συμφόρησης και διασφαλίζοντας την ευρωστία του συστήματος. Αυτή η αποκεντρωμένη διαχείριση διασφαλίζει ότι κανένας μεμονωμένος διακομιστής δεν επιβαρύνεται με το σύνολο των παγκόσμιων δεδομένων, επιτρέποντας στο σύστημα να αναπτύσσεται, καθώς προστίθενται νέοι κόμβοι (Kurose and Ross, 2017).

Κεντρικό ρόλο στην αποδοτική κλιμάκωση παίζει ο μηχανισμός της προσωρινής αποθήκευσης (caching), ο οποίος μειώνει δραστικά τον φόρτο στους εξουσιοδοτημένους διακομιστές. Οι αναδρομικοί επιλυτές αποθηκεύουν τις απαντήσεις για ένα ορισμένο χρονικό διάστημα (TTL), εξυπηρετώντας πολλαπλούς χρήστες χωρίς να επαναλαμβάνουν την πλήρη διαδικασία αναζήτησης στην ιεραρχία. Επιπλέον, για τη διασφάλιση της διαθεσιμότητας, κάθε ζώνη υποστηρίζεται από πρωτεύοντες και δευτερεύοντες διακομιστές, ενώ οι ριζικοί διακομιστές (root servers) χρησιμοποιούν την τεχνική Anycast. Με το Anycast, χιλιάδες φυσικοί διακομιστές παγκοσμίως μοιράζονται την ίδια διεύθυνση IP, κατευθύνοντας αυτόματα το αίτημα του χρήστη στον πλησιέστερο διαθέσιμο κόμβο, ενισχύοντας έτσι την ανθεκτικότητα και την ταχύτητα του συστήματος.

Πέρα από την απλή αντιστοίχιση ονομάτων σε διευθύνσεις IP (εγγραφές A και AAAA), το Σύστημα Ονοματοδοσίας Διαδικτύου λειτουργεί ως ένας γενικός μηχανισμός επίλυσης υπηρεσιών (service resolution). Μια από τις σημαντικότερες πρόσθετες χρήσεις του είναι η διαχείριση του ηλεκτρονικού ταχυδρομείου (Email) μέσω των εγγραφών MX (Mail

Exchange). Οι εγγραφές αυτές ορίζουν τους διακομιστές αλληλογραφίας ενός τομέα και περιλαμβάνουν τιμές προτεραιότητας, επιτρέποντας την ιεράρχηση των διακομιστών λήψης. Επίσης, μέσω των εγγραφών CNAME, το Σύστημα παρέχει τη δυνατότητα δημιουργίας ψευδωνύμων (aliases), επιτρέποντας σε πολλά ονόματα να αντιστοιχούν σε ένα κύριο (canonical) όνομα, γεγονός που απλοποιεί τη διαχείριση της υποδομής.

Το Σύστημα Ονοματοδοσίας Διαδικτύου αποτελεί επίσης ένα ισχυρό εργαλείο για την εξισορρόπηση φορτίου (load-balancing) και τη βελτιστοποίηση της απόδοσης των εφαρμογών. Οι name servers μπορούν να επιστρέφουν πολλαπλές διευθύνσεις IP για ένα μόνο όνομα τομέα, ανακατεύοντας τη σειρά τους σε κάθε απάντηση ώστε οι πελάτες να κατανέμονται σε διαφορετικούς διακομιστές. Σε πιο σύνθετες υλοποιήσεις, χρησιμοποιείται γεωγραφική εξισορρόπηση φορτίου, όπου ο διακομιστής παρέχει διαφορετική απάντηση ανάλογα με την τοποθεσία του χρήστη. Αυτή η τεχνική επιτρέπει την κατεύθυνση των χρηστών στον "πλησιέστερο" ή καλύτερα αποδίδοντα διακομιστή, βελτιώνοντας την απόκριση και μειώνοντας την καθυστέρηση (latency) στο δίκτυο. Τέλος, το σύστημα υποστηρίζει την αντίστροφη αναζήτηση (reverse DNS), επιτρέποντας την εύρεση του ονόματος τομέα που αντιστοιχεί σε μια συγκεκριμένη διεύθυνση.

3. Μεθοδολογία και εργαλεία

Η εργασία βασίζεται στη μεθοδολογία της βιβλιομετρικής ανάλυσης, η οποία αποτελεί μία ευρέως χρησιμοποιούμενη μέθοδο αξιολόγησης της επιστημονικής παραγωγής. Μέσω της βιβλιομετρικής ανάλυσης είναι δυνατή η συστηματική μελέτη της εξέλιξης ενός επιστημονικού πεδίου, η αναγνώριση των σημαντικότερων συγγραφέων, οργανισμών και χωρών, καθώς και η χαρτογράφηση των ερευνητικών τάσεων και των σχέσεων μεταξύ των δημοσιεύσεων.

Στόχος της μελέτης αυτής είναι η διερεύνηση της επιστημονικής βιβλιογραφίας που σχετίζεται με το Domain Name System (DNS), η καταγραφή της διαχρονικής εξέλιξης της έρευνας και η ανάδειξη των βασικών χαρακτηριστικών του συγκεκριμένου ερευνητικού πεδίου.

3.1 Επιστημονικα ερωτήματα

1. Πώς η μετάβαση σε εξελιγμένα DNS πρωτόκολλα επηρεάζει την ικανότητα λήψης αποφάσεων δρομολόγησης;
2. Πώς έχει εξελιχθεί η επιστημονική έρευνα γύρω από το DNS (Domain Name System) διαχρονικά, όπως αποτυπώνεται μέσω βιβλιομετρικής ανάλυσης;
3. Ποια είναι τα κυρίαρχα ερευνητικά θέματα που σχετίζονται με το DNS;

3.2 Συλλογή Δεδομένων

Η συλλογή των βιβλιογραφικών δεδομένων πραγματοποιήθηκε μέσω της βάσης δεδομένων Scopus, η οποία αποτελεί μία από τις μεγαλύτερες και πλέον αξιόπιστες διεθνείς βιβλιογραφικές βάσεις επιστημονικών δημοσιεύσεων. Η επιλογή της Scopus βασίστηκε στην εκτεταμένη κάλυψη επιστημονικών περιοδικών και συνεδρίων και στη δυνατότητα εξαγωγής δεδομένων κατάλληλων για βιβλιομετρική επεξεργασία.Η αναζήτηση πραγματοποιήθηκε τον Απρίλιο του 2026 και βασίστηκε στο συγκεκριμένο ερώτημα αναζήτησης που αφορούσε το Domain Name System (DNS). Η αναζήτηση εφαρμόστηκε στα πεδία τίτλου, περίληψης και λέξεων-κλειδιών των δημοσιεύσεων, προκειμένου να εξασφαλιστεί ότι οι εργασίες που θα συμπεριληφθούν σχετίζονται άμεσα με το αντικείμενο της έρευνας. Επιπλέον εφαρμόστηκαν περιορισμοί ως προς τη γλώσσα των δημοσιεύσεων, τις θεματικές κατηγορίες και το χρονικό διάστημα δημοσίευσης. Συγκεκριμένα, επιλέχθηκαν μόνο δημοσιεύσεις στην αγγλική γλώσσα

που ανήκαν στις θεματικές περιοχές Computer Science, Engineering and Energy και είχαν δημοσιευθεί κατά την περίοδο 1990–2025.
Μετά την εφαρμογή των παραπάνω κριτηρίων προέκυψε τελικό σύνολο 1.770 δημοσιεύσεων, το οποίο αποτέλεσε το δείγμα της βιβλιομετρικής ανάλυσης.

Ερώτημα αναζήτησης που χρησιμοποιήθηκε στη βάση Scopus

```
TITLE-ABS-KEY ( dns , Domain Name System )
AND PUBYEAR > 1989
AND PUBYEAR < 2026
AND (
   LIMIT-TO ( SUBJAREA , "COMP" )
   OR LIMIT-TO ( SUBJAREA , "ENGI" )
   OR LIMIT-TO ( SUBJAREA , "ENER" )
)
AND ( LIMIT-TO ( LANGUAGE , "English" ) )
AND (
   LIMIT-TO ( EXACTKEYWORD , "Internet Protocols" )
   OR LIMIT-TO ( EXACTKEYWORD , "Domain Name System" )
   OR LIMIT-TO ( EXACTKEYWORD , "Network Security" )
   OR LIMIT-TO ( EXACTKEYWORD , "Dns" )
   OR LIMIT-TO ( EXACTKEYWORD , "Domain Names" )
   OR LIMIT-TO ( EXACTKEYWORD , "Internet" )
   OR LIMIT-TO ( EXACTKEYWORD , "Servers" )
   OR LIMIT-TO ( EXACTKEYWORD , "Domain Name System (dns)" )
)
```

3.3 Εξαγωγή και Προετοιμασία των Δεδομένων

Τα αποτελέσματα της αναζήτησης εξήχθησαν από τη βάση δεδομένων Scopus σε μορφή αρχείου CSV. Το αρχείο περιλάμβανε πλήθος βιβλιογραφικών δεδομένων, όπως ονόματα συγγραφέων, τίτλους εργασιών, έτος δημοσίευσης, περιοδικά ή πρακτικά συνεδρίων, περιλήψεις, λέξεις-κλειδιά, οργανισμούς προέλευσης, χώρες και βιβλιογραφικές αναφορές. Πριν από την έναρξη της βιβλιομετρικής ανάλυσης πραγματοποιήθηκε διαδικασία προετοιμασίας των δεδομένων με στόχο τη βελτίωση της ποιότητας των αποτελεσμάτων. Ιδιαίτερη έμφαση δόθηκε στην αντιμετώπιση συνωνύμων που εμφανίζονταν στις λέξεις-κλειδιά. Δημιουργήθηκε ένα αρχείο .txt με τα εξής δεδομένα (3.1). Κατά την ανάλυση στο Biblioshiny εισήχθει το αρχείο αυτό για να γίνει φιλτράρισμα παρόμοιων λέξεων, η

διαδικασία αυτή έγινε, καθώς η ίδια έννοια μπορεί να εμφανίζεται στη βιβλιογραφία με διαφορετικές ονομασίες.

domain name system;dns domain name system;domain name system (dns)
3.1 Πίνακας συνωνύμων

3.4 Εργαλεία Βιβλιομετρικής Ανάλυσης

Η ανάλυση πραγματοποιήθηκε στο περιβάλλον ανάπτυξης RStudio με τη χρήση της γλώσσας προγραμματισμού R και του πακέτου Bibliometrix. Χρησιμοποιήθηκε το Biblioshiny, το οποίο αποτελεί τη διαδικτυακή γραφική διεπαφή του Bibliometrix και επιτρέπει την πραγματοποίηση βιβλιομετρικών αναλύσεων μέσω ενός φιλικού περιβάλλοντος χρήστη.

Η ενεργοποίηση του Biblioshiny πραγματοποιήθηκε με τις ακόλουθες εντολές:

- library(bibliometrix)
- biblioshiny()

Στη συνέχεια το αρχείο CSV που είχε εξαχθεί από τη Scopus έγινε μία προεπεξεργασία των δεδομένων και καθαρισμός των διπλότυπων εγγραφών και έπειτα εισήχθη το αρχείο CSV στο Biblioshiny και χρησιμοποιήθηκε για την παραγωγή των βιβλιομετρικών δεικτών, των πινάκων και των διαγραμμάτων που παρουσιάζονται στο επόμενο κεφάλαιο.

4. Βιβλιομετρική Ανάλυση

4.1 Γενική ανάλυση

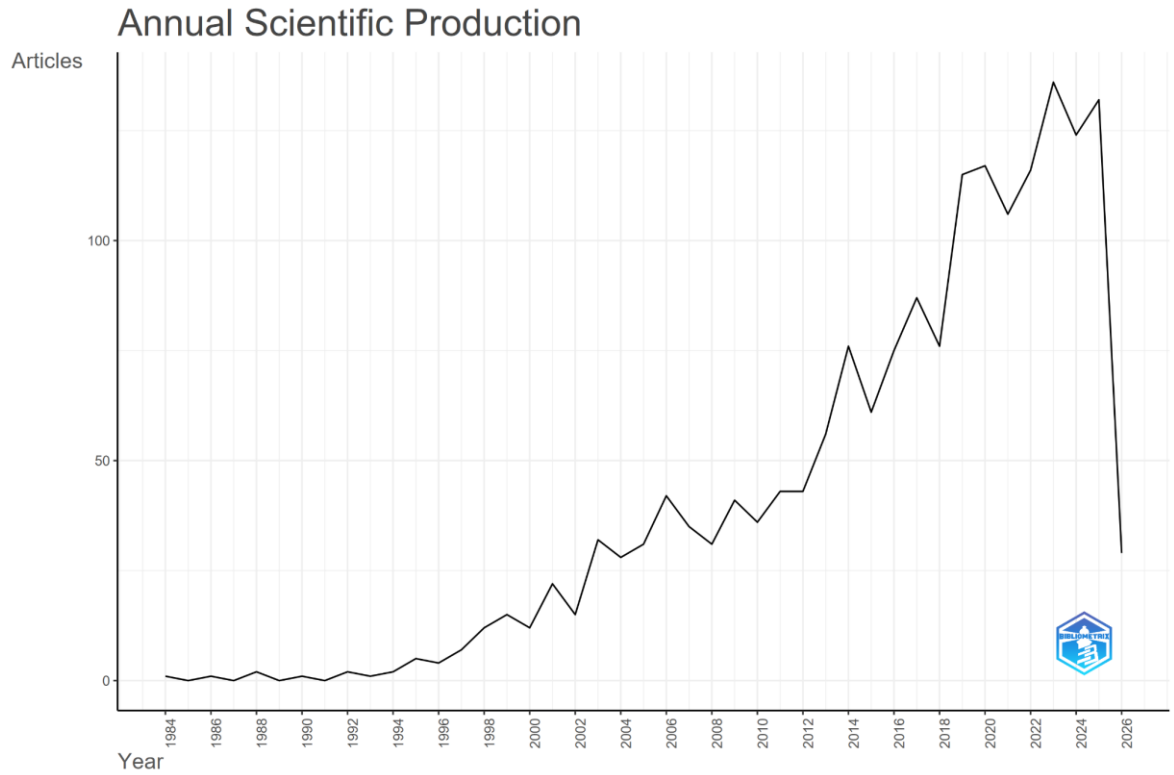
Στο κεφάλαιο αυτο παρουσιάζονται τα αποτελέσματα της βιβλιομετρικής ανάλυσης της επιστημονικής βιβλιογραφίας που σχετίζεται με το Domain Name System (DNS). Η ανάλυση πραγματοποιήθηκε με τη χρήση του εργαλείου Biblioshiny και βασίστηκε στα δεδομένα που εξήχθησαν από τη βάση δεδομένων Scopus. Αρχικά παρουσιάζονται τα βασικά χαρακτηριστικά του συνόλου των δεδομένων και στη συνέχεια αναλύονται η εξέλιξη της επιστημονικής παραγωγής, η επιρροή των δημοσιεύσεων μέσω των αναφορών, οι σημαντικότεροι συγγραφείς, πηγές δημοσίευσης, οργανισμοί και χώρες, καθώς και τα κυριότερα ερευνητικά θέματα που προκύπτουν από την ανάλυση των λέξεων-κλειδιών. Τέλος, παρουσιάζονται τα δίκτυα αναφορών και συν-αναφορών, τα οποία συμβάλλουν στην κατανόηση της δομής και της εξέλιξης του ερευνητικού πεδίου.

Το τελικό σύνολο δεδομένων που χρησιμοποιήθηκε στην παρούσα μελέτη αποτελείται από 1.770 επιστημονικές δημοσιεύσεις σχετικές με το Domain Name System (DNS). Οι δημοσιεύσεις προέρχονται από 971 διαφορετικές πηγές δημοσίευσης, συμπεριλαμβανομένων επιστημονικών περιοδικών και πρακτικών συνεδρίων. Στο σύνολο των εργασιών συμμετέχουν 4.317 διαφορετικοί συγγραφείς, γεγονός που υποδεικνύει την ύπαρξη μιας ιδιαίτερα εκτεταμένης ερευνητικής κοινότητας γύρω από το DNS. Παράλληλα, οι συγγραφείς συνδέονται με 2.922 διαφορετικούς οργανισμούς και ερευνητικά ιδρύματα.

Δείκτης	**Τιμή**
Συνολικές δημοσιεύσεις	1.770
Συγγραφείς	4.317
Πηγές δημοσίευσης	971
Οργανισμοί	2.922
Μεταβλητές dataset	45
Βάση δεδομένων	Scopus
Εργαλείο ανάλυσης	Biblioshiny

4.1.1 Ετήσια επιστημονική παραγωγή

Η Εικόνα 4 (ετήσια επιστημονική παραγωγή (Annual Scientific Production)) απεικονίζει την εξέλιξη του αριθμού δημοσιεύσεων στον τομέα του Συστήματος Ονοματοδοσίας Διαδικτύου διαχρονικά.



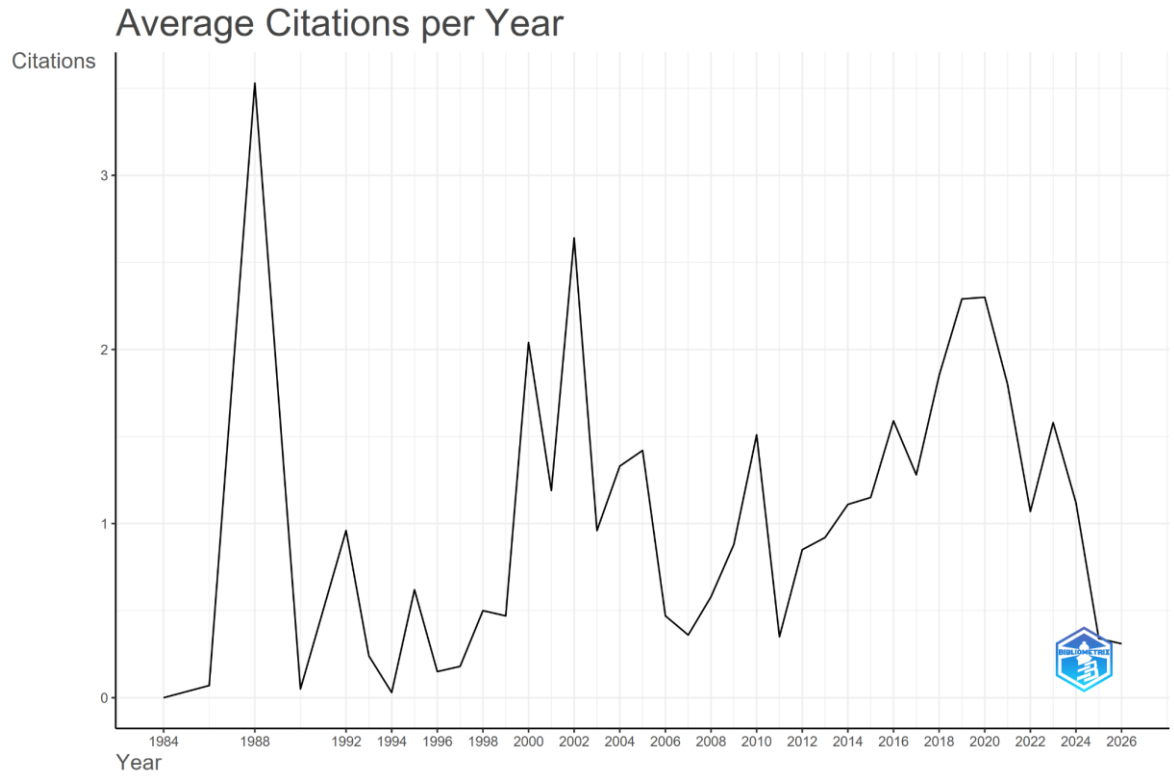
Εικόνα 4 Ετήσια επιστημονική παραγωγή

Η ανάλυση της ετήσιας επιστημονικής παραγωγής μας δείχνει ξεκάθαρα μία ανοδική τάση στην έρευνα γύρω από το Σύστημα Ονοματοδοσίας Διαδικτύου (Εικόνα 4). Η πρόσφατη πτώση πιθανότατα οφείλεται σε καθυστερήσεις στην καταγραφή των δεδομένων και όχι σε πραγματική μείωση του ερευνητικού ενδιαφέροντος. Συνολικά, τα αποτελέσματα δείχνουν

ότι το Σύστημα Ονοματοδοσίας Διαδικτύου αποτελεί ένα ιδιαίτερα ενεργό και επίκαιρο ερευνητικό αντικείμενο.

4.1.2 Μέσος όρος αναφορών ανά χρόνο

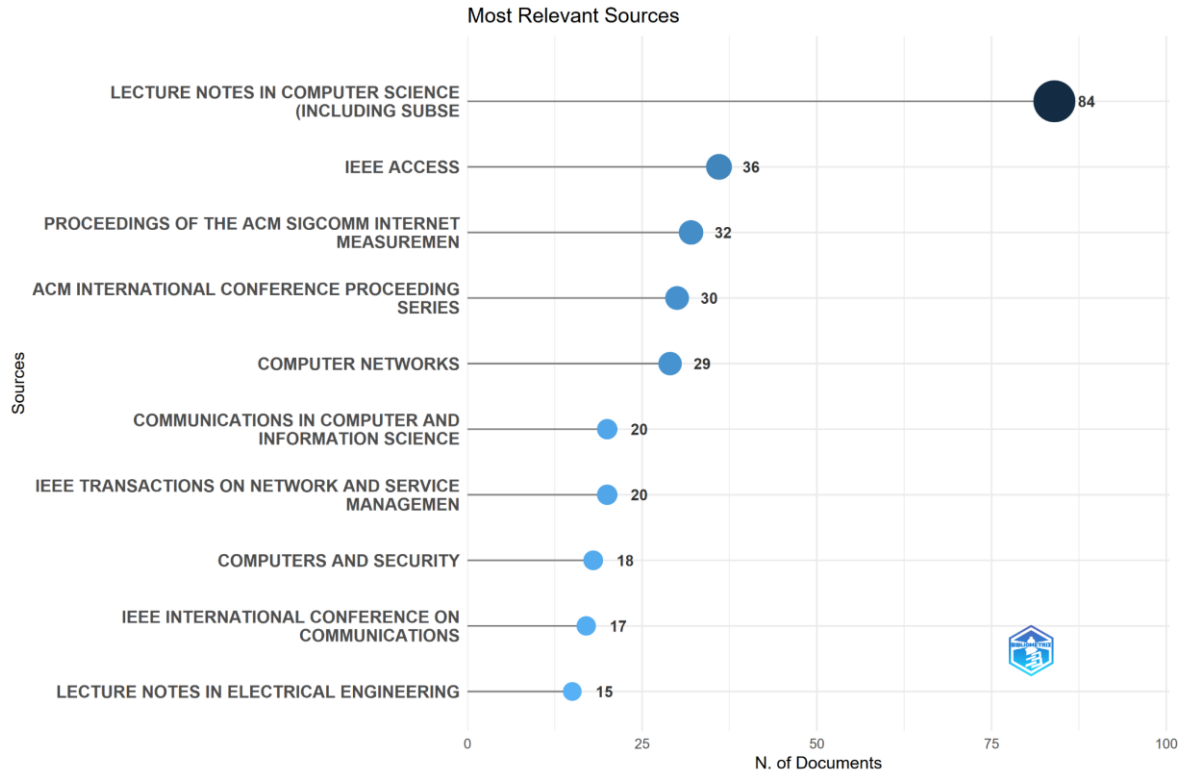
Ο Μέσος όρος αναφορών ανά χρόνο είναι ένας δείκτης που χρησιμοποιείται για τη μέτρηση του αντίκτυπου ενός επιστημονικού έργου, υπολογίζοντας τον μέσο αριθμό των φορών που έχει αναφερθεί ανά έτος από τη δημοσίευσή του. Παρέχει μια ένδειξη της συνεχιζόμενης επιρροής και συνάφειας του έργου στην ακαδημαϊκή κοινότητα.



Εικόνα 5 Μέσος όρος αναφορών ανά χρόνο

Η ανάλυση των μέσων ετήσιων αναφορών αποκαλύπτει ότι η επιρροή της έρευνας στο Σύστημα Ονοματοδοσίας Διαδικτύου παρουσιάζει αρχικά έντονες διακυμάνσεις, με χαρακτηριστική αιχμή στα τέλη της δεκαετίας του 1980 (Εικόνα 5). Κατά την περίοδο 1990–2005, η απήχηση παραμένει ασταθής, ενώ από το 2005 και έπειτα παρατηρείται σταδιακή σταθεροποίηση.

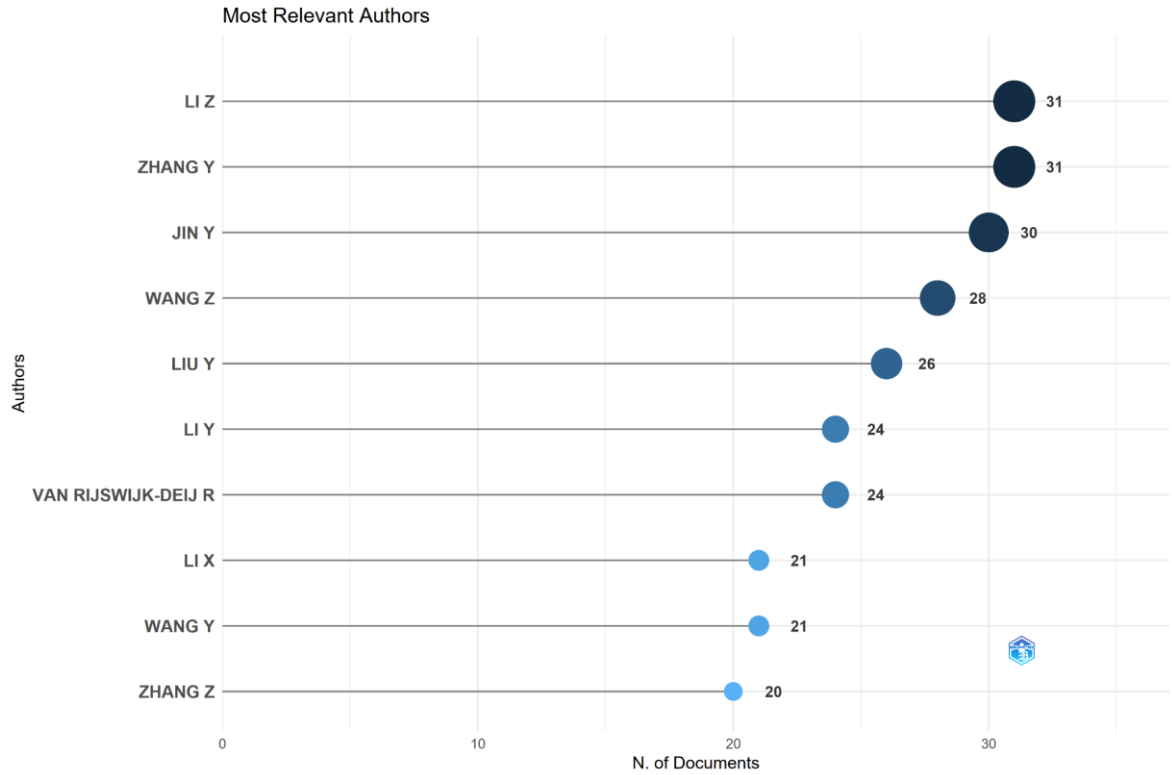
4.1.3 Συχνές πηγές



Εικόνα 6 Πιο συχνές πηγές

Η Εικόνα 6 παρουσιάζει τις πιο σημαντικές πηγές δημοσίευσης στο πεδίο του DNS, με βάση τον αριθμό των σχετικών δημοσιεύσεων. Ξεχωρίζει με μεγάλη διαφορά το Lecture Notes in Computer Science, το οποία συγκεντρώνει τον υψηλότερο αριθμό εργασιών (84). Ακολουθούν πηγές όπως το IEEE Access, το Proceedings ACM SIGCOMM Internet Measurement και το ACM International Conference Proceedings Series, με σημαντικά αλλά αισθητά χαμηλότερα μεγέθη δημοσιεύσεων. Επίσης εμφανίζονται και εξειδικευμένα επιστημονικά περιοδικά, όπως το IEEE Transactions on Network and Service Management, τα οποία συμβάλλουν σταθερά στη βιβλιογραφία, αν και με μικρότερο όγκο δημοσιεύσεων.

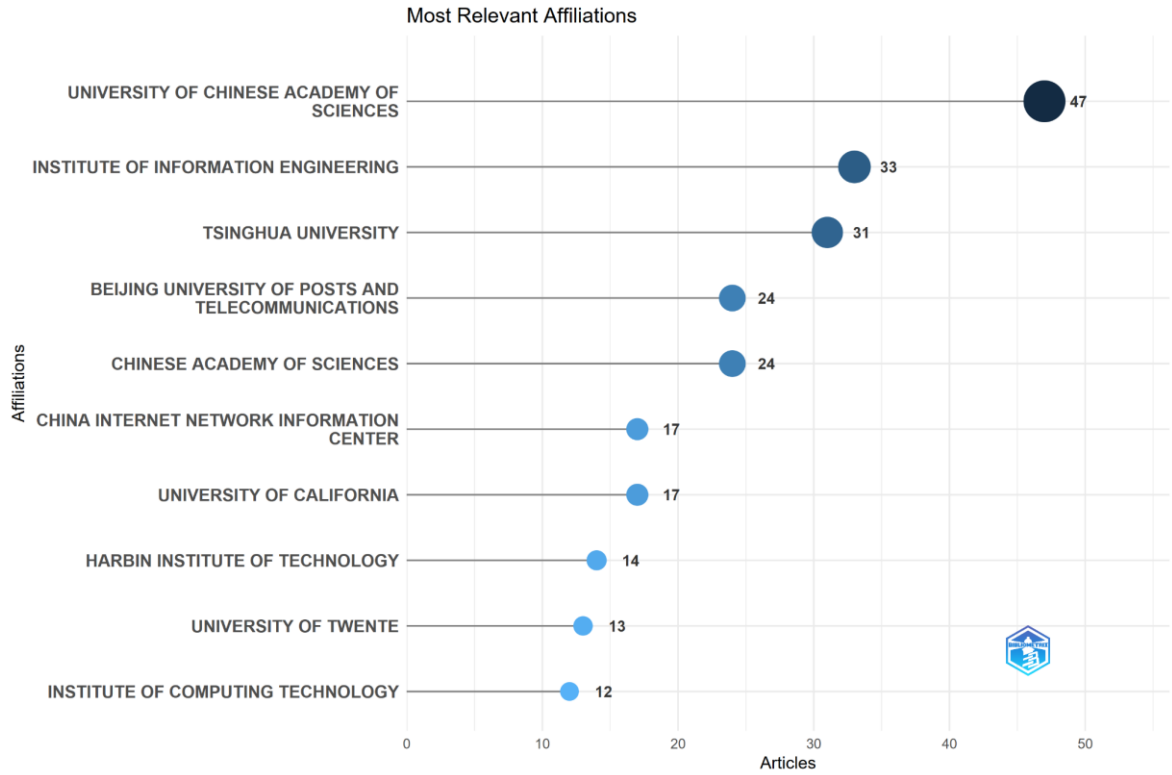
4.2 Ανάλυση σχετικά με τους συγγραφείς



Εικόνα 7 Ανάλυση σχετικά με τους συγγραφείς

Η Εικόνα 7 παρουσιάζει τους πιο σημαντικούς συγγραφείς στο πεδίο του DNS με βάση τον αριθμό των δημοσιεύσεών τους, αναδεικνύοντας την κατανομή της επιστημονικής παραγωγής μεταξύ των ερευνητών. Παρατηρείται ότι οι συγγραφείς Li Z και Zhang Y κατέχουν την πρώτη θέση με 31 δημοσιεύσεις ο καθένας, ακολουθούν πολύ κοντά ο Jin Y με 30, γεγονός που δείχνει υψηλό επίπεδο παραγωγικότητας αλλά και έντονο ανταγωνισμό στην κορυφή. Στη συνέχεια, εμφανίζονται οι Wang Z και Liu Y με ελαφρώς μικρότερο αριθμό εργασιών, ενώ οι υπόλοιποι συγγραφείς κινούνται σε παρόμοια επίπεδα (20–24 δημοσιεύσεις), υποδηλώνοντας μια σχετικά ισορροπημένη κατανομή μετά τους πρώτους. Συνολικά το γράφημα δείχνει ότι, αν και υπάρχουν ορισμένοι κορυφαίοι ερευνητές, η επιστημονική παραγωγή κατανέμεται σε μια ευρύτερη ομάδα συγγραφέων, γεγονός που υποδηλώνει ενεργή και πολυπρόσωπη ερευνητική κοινότητα.

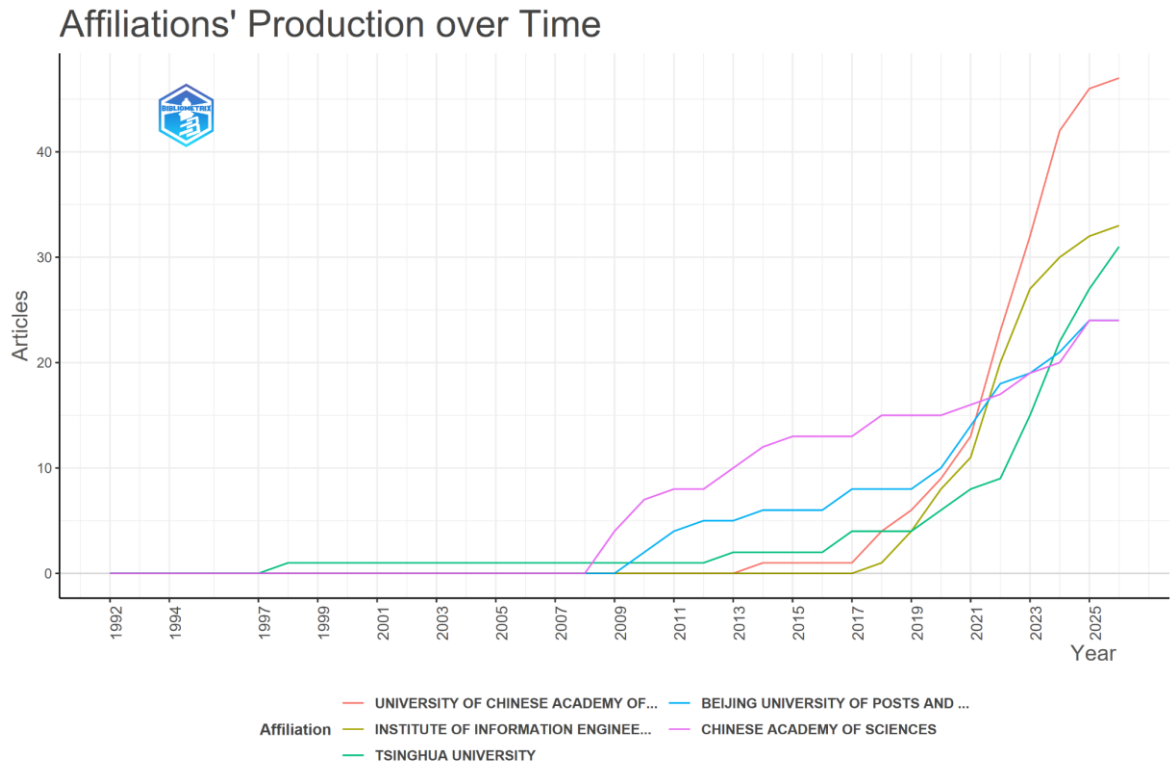
4.3 Ανάλυση σχετικά με φορείς (ερευνητικά ιδρύματα-ινστιτούτα)



Εικόνα 8 Ανάλυση σχετικά με ερευνητικά ιδρύματα-ινστιτούτα

Η Εικόνα 8 παρουσιάζει τους σημαντικότερους ερευνητικούς οργανισμούς (affiliations) στο πεδίο του DNS, με βάση τον αριθμό των δημοσιευμένων άρθρων, αναδεικνύοντας τη γεωγραφική κατανομή της επιστημονικής δραστηριότητας. Την πρώτη θέση καταλαμβάνει το University of Chinese Academy of Sciences με 47 δημοσιεύσεις, ακολουθεί το Institute of Information Engineering και το Tsinghua University, γεγονός που δείχνει έντονη συγκέντρωση ερευνητικής παραγωγής σε κορυφαία Κινέζικα ιδρύματα. Παράλληλα, εμφανίζονται και άλλοι σημαντικοί οργανισμοί όπως το Beijing University of Posts and Telecommunications και η Chinese Academy of Sciences. Αν και υπάρχουν συμμετοχές και από διεθνή ιδρύματα, όπως το University of California και το University of Twente, η

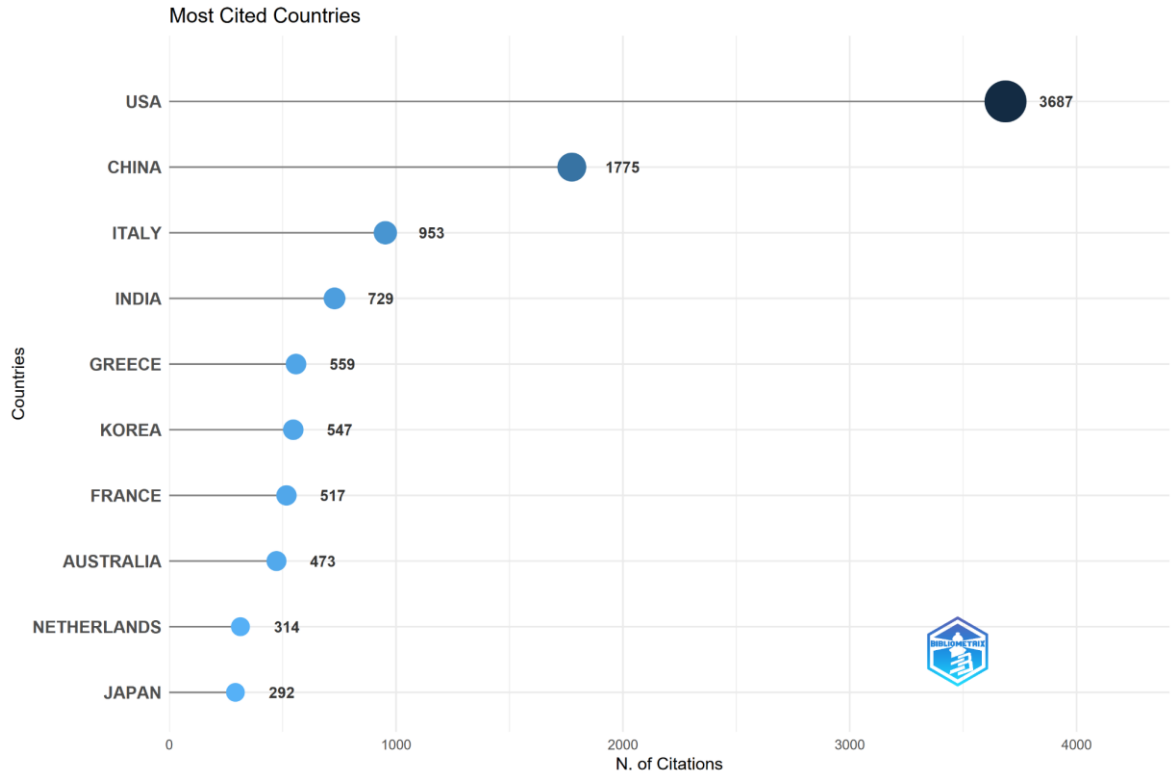
συνεισφορά τους είναι συγκριτικά μικρότερη. Συνολικά, το γράφημα μας δείχνει ότι η έρευνα στο DNS χαρακτηρίζεται από έντονη γεωγραφική συγκέντρωση, με κυρίαρχο ρόλο να έχει η Κίνα.



Εικόνα 9 Παραγωγή ιδρυμάτων-ινστιτούτων ανά χρόνο

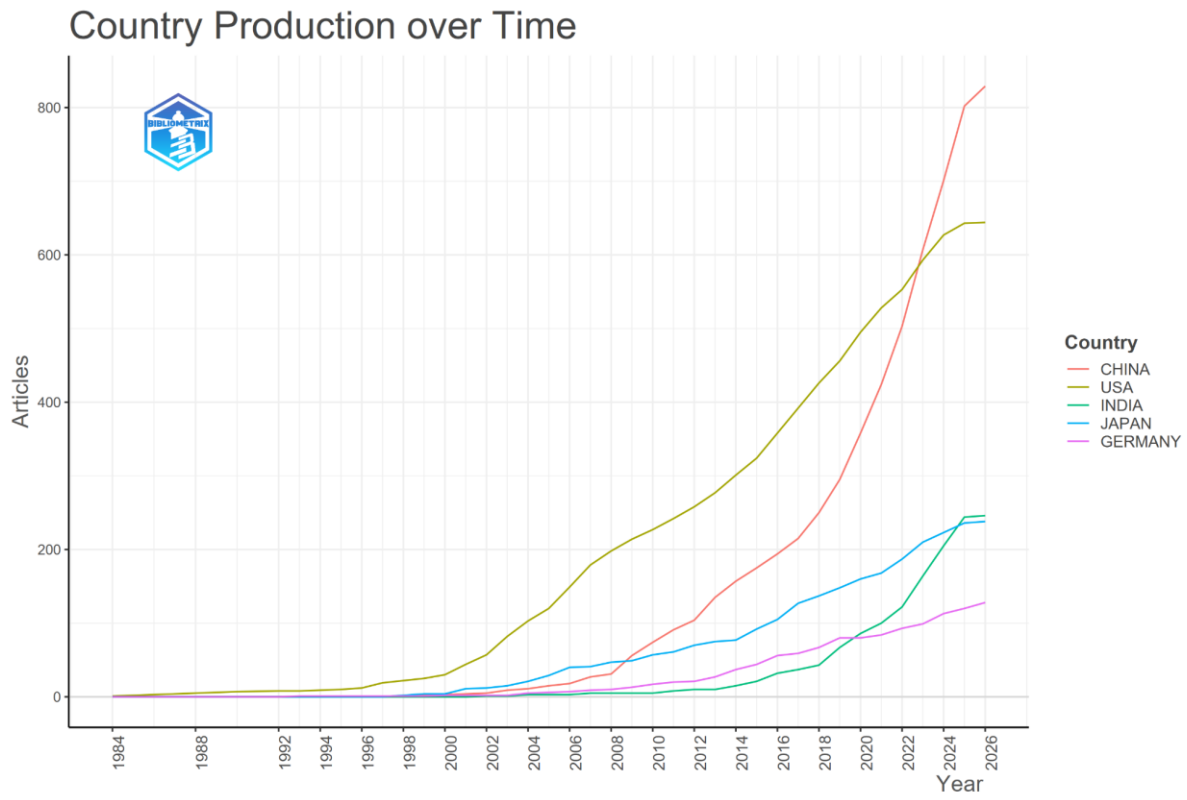
Η Εικόνα 9 απεικονίζει τον αριθμό των επιστημονικών άρθρων που δημοσιεύτηκαν από συγκεκριμένα πανεπιστήμια και ερευνητικά ιδρύματα σε βάθος χρόνου. Βλέπουμε μέχρι το 2008-2010, η ερευνητική παραγωγή ήταν σχεδόν μηδενική για τους περισσότερους φορείς στο συγκεκριμένο αντικείμενο. Μετά το 2017, παρατηρείται μια εκθετική αύξηση σε όλα τα ιδρύματα με την πιο εντυπωσιακή άνοδο να έχει το University of Chinese Academy of Sciences παρόλο που ξεκίνησε αργότερα από τους άλλους (γύρω στο 2013), "προσπέρασε" τους πάντες μετά το 2021, φτάνοντας σχεδόν τα 45-50 άρθρα το 2025.

4.4 Γεωγραφική κατανομή έρευνας



Εικόνα 10 Κατάταξη χωρών βάσει αριθμού αναφορών

Η Εικόνα 10 παρουσιάζει την επιστημονική επίδραση των χωρών που δραστηριοποιούνται ερευνητικά στο πεδίο του DNS. Η κατάταξη βασίζεται στο συνολικό αριθμό των αναφορών (citations). Οι Ηνωμένες Πολιτείες κατέχουν την πρώτη θέση με 3.687 αναφορές. Η Κίνα και η Ινδία κατέχουν τις επόμενες θέσεις αλλά βλέπουμε και την Ελλάδα στην 5η θέση της παγκόσμιας κατάταξης, η οποία δείχνει ότι ολοένα και περισσότεροι Έλληνες ερευνητές καταφέρνουν να έχουν μεγαλύτερη επίδραση στη διεθνή βιβλιογραφία σε σχέση με χώρες με πολύ μεγαλύτερους πληθυσμούς και οικονομίες που βρίσκονται σε χαμηλότερες θέσεις.



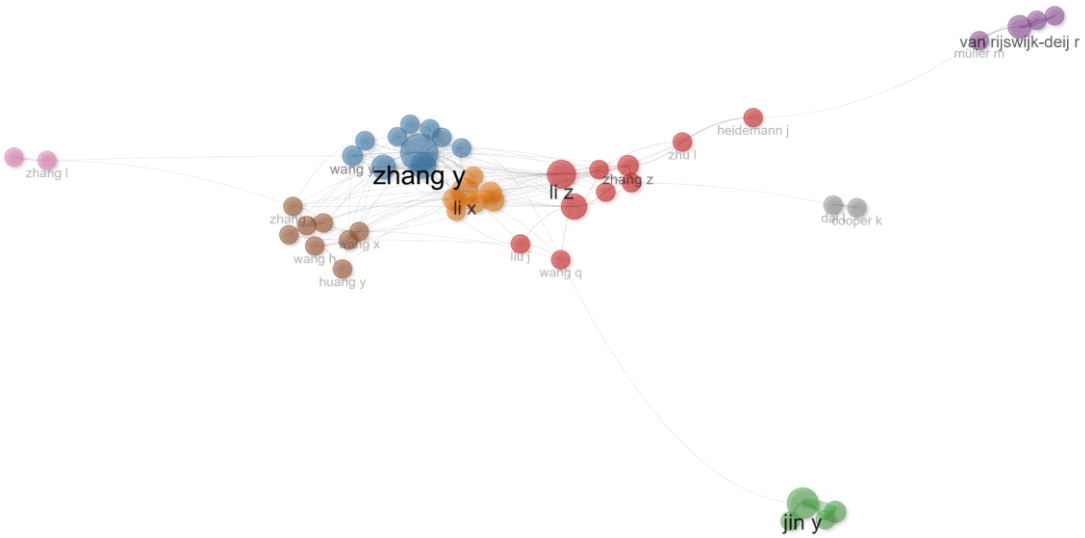
Εικόνα 11 Κατάταξη χωρών βάσει αριθμού αναφορών

Η Εικόνα 11 απεικονίζει τη διαχρονική εξέλιξη της επιστημονικής παραγωγής σε πέντε χώρες από το 1984 έως το 2026 και δείχνει μια επιτάχυνση της έρευνας κυρίως μετά το 2000. Οι ΗΠΑ διατηρούν για μεγάλο διάστημα την πρώτη θέση με σταθερή αύξηση των δημοσιεύσεων, ωστόσο η Κίνα εμφανίζει σημαντική άνοδο ιδιαίτερα μετά το 2010 και τελικά τις ξεπερνά προς το τέλος της περιόδου, καταγράφοντας την υψηλότερη παραγωγή. Η Ιαπωνία παρουσιάζει πιο ήπια αλλά συνεχή ανάπτυξη, ενώ η Ινδία ξεκινά με χαμηλά επίπεδα και επιταχύνει σημαντικά μετά το 2016. Η Γερμανία ακολουθεί επίσης ανοδική πορεία, αλλά παραμένει σε χαμηλότερα επίπεδα συγκριτικά.

4.5 Δίκτυα συνεργασία/συνύπαρξης

Το δίκτυο συνεργασιών (Εικόνα 12) δείχνει ότι υπάρχει μια κεντρική ομάδα ερευνητών που συνεργάζονται συχνά μεταξύ τους. Οι μεγαλύτεροι κόμβοι αντιστοιχούν σε συγγραφείς με

περισσότερες συνεργασίες και μεγαλύτερη συμμετοχή στις δημοσιεύσεις όπως είναι οι Zhang Y, Li X. Επίσης υπάρχουν κάποιοι ερευνητές που συνδέουν διαφορετικές ομάδες μεταξύ τους, ενώ άλλες μικρότερες ομάδες εμφανίζονται πιο απομονωμένες. Συνολικά, το δίκτυο δείχνει ότι στο συγκεκριμένο πεδίο υπάρχει αρκετή συνεργασία και διασύνδεση μεταξύ των ερευνητών.

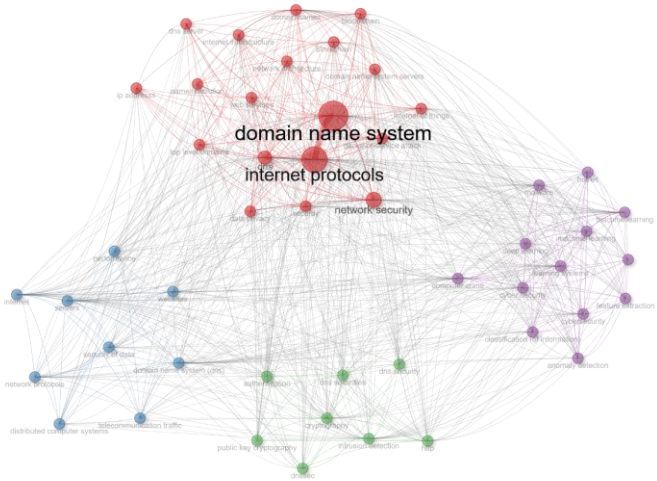


Εικόνα 12 Δίκτυα συνεργασίας

4.5.1 Λέξεις κλειδιά

Η συν-εμφάνιση λέξεων-κλειδιών στη βιβλιομετρική ανάλυση αναφέρεται στη συχνότητα με την οποία συγκεκριμένοι όροι ή φράσεις εμφανίζονται μαζί σε επιστημονικές δημοσιεύσεις. Εντοπίζοντας μοτίβα συν-εμφάνισης, οι ερευνητές μπορούν να ανακαλύψουν σχέσεις μεταξύ εννοιών, θεμάτων σε μία βιβλιογραφία. Αυτή η ανάλυση βοηθά στη χαρτογράφηση της πνευματικής δομής ενός ερευνητικού πεδίου, αναδεικνύοντας τα επικρατούντα θέματα και τους συσχετισμούς μεταξύ διαφορετικών ιδεών. Πρόκειται για μια σημαντική τεχνική για την απόκτηση γνώσεων σχετικά με τα

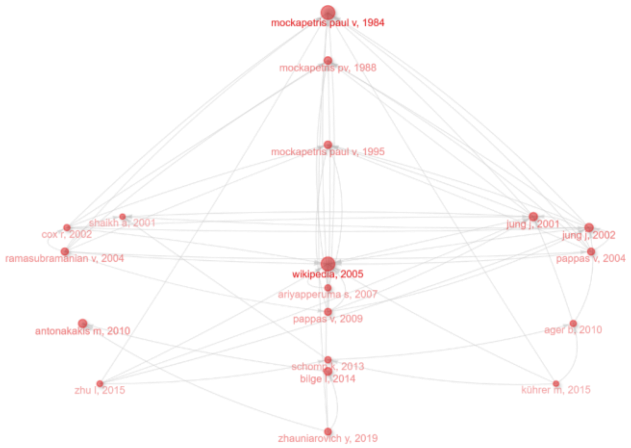
βασικά θέματα και τις τάσεις εντός ενός συγκεκριμένου ακαδημαϊκού κλάδου ή ερευνητικού τομέα. Όπως βλέπουμε στην Εικόνα 13, οι πιο συχνές χρησιμοποιούμενες λέξεις-κλειδιά, είναι οι “domain name system” και “internet protocols”.



Εικόνα 13 Λέξεις κλειδιά

4.5.2 Δίκτυο αναφορών

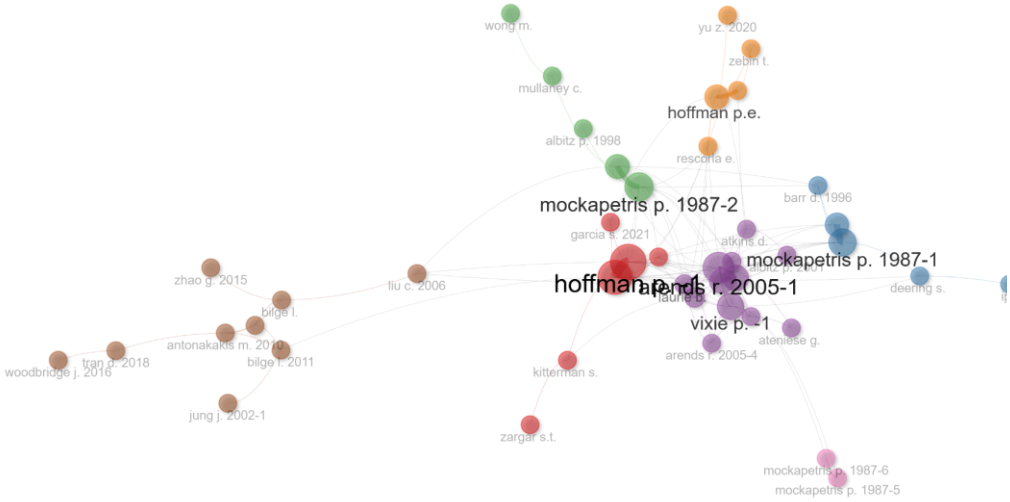
Ένα δίκτυο αναφορών στη βιβλιομετρική ανάλυση καταγράφει τις σχέσεις μεταξύ των ακαδημαϊκών εργασιών με βάση τις βιβλιογραφικές παραπομπές που χρησιμοποιούν (ποιες πηγές αναφέρουν) και τις αναφορές που δέχονται από άλλες εργασίες (από ποιους αναφέρονται).(Εικόνα 14)



Εικόνα 14 Δίκτυο αναφορών

4.5.3 Δίκτυο συν-αναφορών

Ένα δίκτυο συν-αναφορών στη βιβλιομετρική ανάλυση οπτικοποιεί τις συνδέσεις μεταξύ άρθρων με υψηλό αριθμό αναφορών εντός ενός συγκεκριμένου πεδίου. Κάθε κόμβος αντιπροσωπεύει ένα από τα κορυφαία άρθρα και οι σύνδεσμοι υποδεικνύουν περιπτώσεις όπου δύο άρθρα παρατίθενται συχνά μαζί από άλλες εργασίες (Εικόνα 15). Αυτή η ανάλυση δικτύου βοηθά στον εντοπισμό επιδραστικών άρθρων και στην ανάδειξη βασικών θεμάτων ή τάσεων στο πεδίο, βάσει των προτύπων συν-αναφορών.



Εικόνα 15 Δίκτυο συν-αναφορών

5. Ανάλυση περιεχομένου: Η εξέλιξη του DNS

Η μετάβαση σε εξελιγμένα πρωτόκολλα και επεκτάσεις του DNS επηρεάζει καθοριστικά την ικανότητα λήψης αποφάσεων δρομολόγησης, επιτρέποντας μια πολύ πιο ακριβή και έξυπνη κατεύθυνση της κυκλοφορίας στο Διαδίκτυο. Οι κυριότεροι τρόποι με τους οποίους επιτυγχάνεται αυτό είναι οι εξής:

- ***EDNS0 Client Subnet (CS)***: Πρόκειται για μία από τις σημαντικότερες επεκτάσεις, η οποία επιτρέπει στον εξουσιοδοτημένο DNS server να γνωρίζει το υποδίκτυο IP του πελάτη που αρχικά έκανε το ερώτημα, και όχι μόνο την IP του αναδρομικού επιλυτή (recursive resolver). Αυτό είναι κρίσιμο όταν χρησιμοποιούνται δημόσιοι επιλυτές (όπως της Google ή της Cloudflare), καθώς χωρίς το EDNS0 CS, ο εξουσιοδοτημένος server θα μπορούσε να δρομολογήσει τον χρήστη σε έναν διακομιστή κοντά στον επιλυτή αλλά γεωγραφικά μακριά από τον ίδιο τον χρήστη. Η πληροφορία αυτή επιτρέπει μια αποτελεσματικότερη αντιστοίχιση σε κοντινές υπηρεσίες (Tanenbaum & Wetherall, 2011).
- ***Βελτιστοποίηση Δικτύων Διανομής Περιεχομένου (CDNs)***: Εξελιγμένες εφαρμογές του DNS επιτρέπουν σε εταιρείες όπως η Akamai να λαμβάνουν πιο εξελιγμένες αποφάσεις για τη διανομή περιεχομένου στον Παγκόσμιο Ιστό. Κατευθύνοντας τους χρήστες σε συγκεκριμένες διευθύνσεις IP βάσει της τοποθεσίας τους, το DNS λειτουργεί ως ένας μηχανισμός δρομολόγησης επιπέδου εφαρμογής που μειώνει την καθυστέρηση και βελτιώνει την εμπειρία του χρήστη (Kurose and Ross, 2017).
- ***Κατανομή Φορτίου (Load Distribution)***: Το DNS χρησιμοποιείται για την κατανομή φορτίου μεταξύ πολλών αντιγράφων ενός διακομιστή (replicated servers). Με την τεχνική του DNS rotation, ο εξυπηρετητής απαντά με ένα σύνολο διευθύνσεων IP αλλάζοντας τη σειρά τους σε κάθε απάντηση, γεγονός που δρομολογεί τους πελάτες σε διαφορετικούς φυσικούς διακομιστές και αποτρέπει τη συμφόρηση (Kurose and Ross, 2017).
- ***Επιρροή Κρυπτογραφημένων Πρωτοκόλλων (DoT/DoH)***: Η μετάβαση προς το DNS-over-TLS και το DNS-over-HTTPS αλλάζει το ποιος έχει την ορατότητα για τη λήψη αποφάσεων. Ενώ προστατεύουν την ιδιωτικότητα, οι τοπικοί πάροχοι χάνουν τη δυνατότητα να παρατηρούν τα ερωτήματα DNS και να επεμβαίνουν στη δρομολόγηση (π.χ. για διαχείριση κίνησης), ενώ η ευθύνη αυτή μεταφέρεται στους παρόχους των επιλυτών cloud.

- ***Anycast Routing στους Root Servers***: Η χρήση της τεχνικής anycast επιτρέπει στο πρωτόκολλο δρομολόγησης IP να κατευθύνει αυτόματα ένα ερώτημα DNS προς τον πλησιέστερο φυσικά εξυπηρετητή από μια ομάδα εξυπηρετητών που μοιράζονται την ίδια IP διεύθυνση, βελτιώνοντας την αξιοπιστία και την ταχύτητα απόκρισης της ιεραρχίας (Stallings, 2014).

5.1 Κεντρικοποιημένη προσέγγιση (HOSTS.TXT)

5.1.1 pre-DNS

Στις απαρχές του Διαδικτύου, κατά την εποχή του ARPANET, η αντιστοίχιση των ονομάτων των υπολογιστών στις αριθμητικές διευθύνσεις IP τους γινόταν μέσω ενός μοναδικού αρχείου με το όνομα **hosts.txt**. Αυτό το αρχείο περιελάμβανε μια πλήρη λίστα με όλα τα ονόματα των υπολογιστών και τις αντίστοιχες διευθύνσεις τους, και κάθε υπολογιστής στο δίκτυο έπρεπε να το "κατεβάζει" περιοδικά από μια κεντρική τοποθεσία στην οποία διατηρούνταν. Για ένα δίκτυο μερικών εκατοντάδων μεγάλων υπολογιστών χρονομερισμού, η προσέγγιση αυτή ήταν επαρκής και λειτουργούσε ικανοποιητικά. Ωστόσο, η ραγδαία αύξηση του αριθμού των συστημάτων που συνδέονταν στο δίκτυο κατέστησε σαφές ότι αυτή η κεντρικοποιημένη μέθοδος δεν μπορούσε να κλιμακωθεί επ' αόριστον (Tanenbaum & Wetherall, 2011).

Τα κύρια προβλήματα μιας κεντρικοποιημένης βάσης δεδομένων περιελάμβαναν το μοναδικό σημείο αποτυχίας (single point of failure), όπου μια βλάβη στον κεντρικό διακομιστή θα παρέλυε ολόκληρη τη διαδικασία αντιστοίχισης ονομάτων παγκοσμίως, και τον τεράστιο όγκο κίνησης (traffic volume) που θα έπρεπε να διαχειριστεί ένας μόνο διακομιστής για εκατομμύρια αιτήματα. Επιπλέον, μια απομακρυσμένη κεντρική βάση δεδομένων θα προκαλούσε σημαντικές καθυστερήσεις στους χρήστες λόγω απόστασης, ενώ η συντήρηση και η διαρκής ενημέρωση ενός τόσο ογκώδους αρχείου για κάθε νέο υπολογιστή θα ήταν πρακτικά αδύνατη (Kurose and Ross, 2017).

5.1.2 Δημιουργία DNS

Προκειμένου να αντιμετωπιστούν αυτά τα ζητήματα κλιμάκωσης και διαχείρισης, το Σύστημα Ονοματοδοσίας Διαδικτύου (DNS) εφευρέθηκε το 1983. Αντί για ένα κεντρικό αρχείο, το Σύστημα Ονοματοδοσίας Διαδικτύου σχεδιάστηκε ως μια ιεραρχική και

κατανεμημένη βάση δεδομένων. Η νέα αυτή προσέγγιση επέτρεπε τη διανομή των πληροφοριών σε εκατομμύρια διακομιστές σε όλο τον κόσμο, διασφαλίζοντας την ευρωστία και την ταχύτητα του συστήματος. Το DNS ορίζεται επίσημα στα έγγραφα RFC 1034 και RFC 1035, τα οποία περιγράφουν τη δομή και τη λειτουργία του ως μια θεμελιώδη υπηρεσία καταλόγου για το σύγχρονο διαδίκτυο (Tanenbaum & Wetherall, 2011).

5.2 Κατανεμημένη προσέγγιση -ιεραρχική δομή

5.2.1 Resolvers

Οι **resolvers** (επιλυτές) είναι προγράμματα που αναλαμβάνουν να εξάγουν πληροφορίες από τους διακομιστές ονομάτων ανταποκρινόμενοι σε αιτήματα πελατών. Συνήθως, μια εφαρμογή (όπως ένας Web browser) καλεί μια βιβλιοθήκη διαδικασιών του λειτουργικού συστήματος, γνωστή ως stub resolver, περνώντας το όνομα του υπολογιστή ως παράμετρο. Ο stub resolver στέλνει ένα ερώτημα που περιέχει το όνομα σε έναν τοπικό DNS εξυπηρετητή (local DNS server), ο οποίος συχνά λειτουργεί ως local recursive resolver (τοπικός αναδρομικός επιλυτής). Ο τοπικός αναδρομικός επιλυτής αναλαμβάνει στη συνέχεια τη διαδικασία επικοινωνίας με την ιεραρχία των διακομιστών DNS για να βρει την τελική διεύθυνση IP και να την επιστρέψει στον υπολογιστή του χρήστη (Tanenbaum & Wetherall, 2011).

5.2.2 Authoritative name servers

Οι **authoritative name servers** (εξουσιοδοτημένοι διακομιστές ονομάτων) είναι οι διακομιστές που κατέχουν τις επίσημες εγγραφές για έναν συγκεκριμένο τομέα (domain). Κάθε οργανισμός που διαθέτει δημόσια προσβάσιμους υπολογιστές στο διαδίκτυο είναι υποχρεωμένος να παρέχει δημόσια προσβάσιμες εγγραφές DNS που αντιστοιχίζουν τα ονόματα αυτών των υπολογιστών σε διευθύνσεις IP. Αυτές οι εγγραφές φιλοξενούνται στον εξουσιοδοτημένο διακομιστή του οργανισμού, ο οποίος μπορεί να συντηρείται από τον ίδιο τον οργανισμό ή από έναν εξωτερικό πάροχο υπηρεσιών.(#Kurose) Μια εγγραφή θεωρείται εξουσιοδοτημένη όταν προέρχεται απευθείας από τη διαχειριστική αρχή που ελέγχει τον συγκεκριμένο τομέα, διασφαλίζοντας ότι η πληροφορία είναι πάντα έγκυρη και ορθή (Tanenbaum & Wetherall, 2011).

5.3 Βελτίωση ασφάλειας

Ο αρχικός σχεδιασμός του DNS δεν προέβλεπε μηχανισμούς ασφαλείας, με αποτέλεσμα το πρωτόκολλο να είναι ευάλωτο σε μια σειρά από επιθέσεις. Οι κυριότερες απειλές περιλαμβάνουν τη δηλητηρίαση προσωρινής μνήμης (cache poisoning), όπου ο επιτιθέμενος εισάγει πλαστές εγγραφές σε έναν DNS server, και τις επιθέσεις Man-in-the-Middle, κατά τις οποίες παρακολουθούνται ή τροποποιούνται τα ερωτήματα των χρηστών. Επιπλέον, το DNS αποτελεί συχνό στόχο επιθέσεων DDoS, είτε μέσω κατακλυσμού των root servers με πακέτα είτε μέσω της αποστολής τεράστιου όγκου ερωτημάτων σε Ανωτάτου επιπέδου διακομιστές (TLD servers). Η έλλειψη κρυπτογράφησης στα παραδοσιακά ερωτήματα DNS επιτρέπει επίσης σε τρίτους, όπως παρόχους υπηρεσιών Διαδικτύου (ISPs) ή κακόβουλους χρήστες σε κοινόχρηστα δίκτυα, να παρακολουθούν το ιστορικό περιήγησης των χρηστών (Tanenbaum & Wetherall, 2011).

5.3.1 DNSCrypt

Το **DNSCrypt** αποτελεί ένα από τα πρώτα πρωτόκολλα που σχεδιάστηκαν για την ασφάλεια της επικοινωνίας μεταξύ του επιλυτή (stub resolver) και του αναδρομικού επιλυτή (recursive resolver). Λειτουργεί κρυπτογραφώντας την κίνηση DNS, διασφαλίζοντας έτσι ότι τα δεδομένα δεν μπορούν να υποκλαπούν ή να τροποποιηθούν από τρίτους κατά τη μεταφορά τους. Παρόλο που δεν αποτελεί επίσημο πρότυπο του IETF όπως το DoT ή το DoH, υιοθετήθηκε από διάφορους παρόχους (όπως το OpenDNS) για την προστασία από τη δηλητηρίαση μνήμης και την ενίσχυση της ιδιωτικότητας του τελικού χρήστη (Tanenbaum & Wetherall, 2011).

5.3.2 DNS-over-TLS

Το **DNS-over-TLS (DoT)** είναι ένα σύγχρονο πρότυπο που αξιοποιεί το πρωτόκολλο TLS για την κρυπτογράφηση των ερωτημάτων και των απαντήσεων DNS. Σε αντίθεση με το παραδοσιακό DNS που βασίζεται κυρίως στο UDP, το DoT χρησιμοποιεί το πρωτόκολλο TCP ως μέσο μεταφοράς για να εξασφαλίσει αξιόπιστη και ασφαλή σύνδεση. Με την εφαρμογή του DoT, η επικοινωνία μεταξύ του υπολογιστή του χρήστη και του τοπικού επιλυτή γίνεται αόρατη για οποιονδήποτε ενδιάμεσο παρατηρητή στο δίκτυο. Πολλές μεγάλες εταιρείες, όπως η Google και η Cloudflare, προσφέρουν πλέον δημόσιους επιλυτές

που υποστηρίζουν DoT, επιτρέποντας στους χρήστες να προστατεύουν την ιδιωτικότητά τους από την παρακολούθηση της κίνησης DNS (Tanenbaum & Wetherall, 2011).

5.3.3 DNS-over-HTTPS

Το **DNS-over-HTTPS (DoH)** ακολουθεί μια διαφορετική προσέγγιση, ενσωματώνει τα ερωτήματα DNS μέσα σε κανονικά αιτήματα **HTTPS**. Αυτό καθιστά την κίνηση DNS πανομοιότυπη με τη συνήθη κίνηση στον Παγκόσμιο Ιστό, καθιστώντας εξαιρετικά δύσκολο για τους διαχειριστές δικτύων ή τους ISPs να φιλτράρουν ή να παρακολουθήσουν τα ερωτήματα. Μια σημαντική εξέλιξη είναι ότι η διαχείριση του DoH μπορεί να μεταφερθεί από το λειτουργικό σύστημα απευθείας στον **π**εριηγητή (Web browser). Αν και αυτό ενισχύει την ιδιωτικότητα, εγείρει ανησυχίες καθώς οι κατασκευαστές περιηγητών (όπως η Mozilla ή η Google) αποκτούν τον έλεγχο της κίνησης DNS, αφαιρώντας τη δυνατότητα από τους ISPs να παρατηρούν μολύνσεις από κακόβουλο λογισμικό ή να εφαρμόζουν γονικούς ελέγχους (Lyu, 2021). Τέλος, εξελιγμένες μορφές όπως το **Oblivious DoH** στοχεύουν στον πλήρη διαχωρισμό της γνώσης της διεύθυνσης IP του χρήστη από το περιεχόμενο του ερωτήματος DNS (Tanenbaum & Wetherall, 2011) .

5.4 Σύγχρονες προσεγγίσεις/ Private DNS (DoH/DoT)

Οι σύγχρονες προσεγγίσεις για την προστασία της ιδιωτικότητας στο DNS (DNS-over-Encryption - DoE) αποσκοπούν στην εξάλειψη της μετάδοσης ερωτημάτων σε απλή μορφή κειμένου (plaintext), η οποία επέτρεπε τη δημιουργία προφίλ χρηστών και την παρακολούθηση της περιήγησής τους. Οι πρώτες προσπάθειες τυποποίησης περιελάμβαναν το **DNS-over-TLS (DoT)** το 2016 και το **DNS-over-HTTPS (DoH)** το 2018, τα οποία χρησιμοποιούν το πρωτόκολλο TLS για την κρυπτογράφηση των δεδομένων. Παρά τη βελτίωση της ασφάλειας, τα πρωτόκολλα αυτά περιορίζονται από τους πολλαπλούς κύκλους διαδρομής (round-trips) που απαιτούνται για την καθιέρωση σύνδεσης μέσω TCP και TLS, καθώς και από το πρόβλημα της παρεμπόδισης κεφαλής γραμμής (**head-of-line blocking**). Η εξέλιξη των σύγχρονων μεθόδων επικεντρώνεται πλέον στη χρήση του πρωτοκόλλου **QUIC**, το οποίο ενσωματώνει την κρυπτογράφηση στο επίπεδο μεταφοράς για βελτιστοποιημένη ταχύτητα (Kosek et al., 2022).

5.4.1 DNS-over-HTTPS

Το πρωτόκολλο **DNS-over-HTTPS (DoH)** επιτυγχάνει την ιδιωτικότητα ενσωματώνοντας τα ερωτήματα DNS μέσα στην κίνηση HTTPS στη θύρα 443. Αυτή η αρχιτεκτονική επιτρέπει στο DNS να επωφελείται από σύνθετες δυνατότητες του HTTP, όπως η ανακατεύθυνση, η χρήση διαμεσολαβητών (proxies) και η συμπίεση, ενώ καθιστά την κίνηση DNS δυσδιάκριτη από την υπόλοιπη κίνηση ιστού. Μια κρίσιμη πτυχή του DoH είναι ότι η υλοποίησή του μπορεί να γίνει απευθείας από τον περιηγητή (browser), παρακάμπτοντας τις ρυθμίσεις DNS του λειτουργικού συστήματος και του τοπικού παρόχου. Μια σημαντική εξέλιξή του είναι το **Oblivious DoH (oDoH)**, το οποίο χρησιμοποιεί έναν ενδιάμεσο διαμεσολαβητή για να διαχωρίσει την IP διεύθυνση του χρήστη από το περιεχόμενο της αναζήτησής του, προσφέροντας ένα επιπλέον επίπεδο ανωνυμίας (Tanenbaum & Wetherall, 2011).

5.4.2 DNS-over-QUIC

Το πρωτόκολλο **DNS-over-QUIC** αποτελεί την πιο πρόσφατη εξέλιξη, σχεδιασμένο να παρέχει ιδιωτικότητα με την ελάχιστη δυνατή καθυστέρηση. Συνδυάζει τα πλεονεκτήματα της κρυπτογράφησης TLS 1.3 με χαμηλότερη καθυστέρηση και καλύτερη απόδοση σε σύγκριση με τα πρωτόκολλα που βασίζονται στο TCP. Η χρήση ανεξάρτητων ροών δεδομένων (streams) επιτρέπει την ταχύτερη επεξεργασία πολλαπλών DNS ερωτημάτων, ενώ παράλληλα αποφεύγονται προβλήματα όπως το Head-of-Line Blocking που εμφανίζεται στις TCP συνδέσεις. Παρά την ταχύτητά του, το DoQ παραμένει ευάλωτο σε επιθέσεις **Website Fingerprinting (WFP)**, όπου εξελιγμένα μοντέλα Τεχνητής Νοημοσύνης (Transformers) μπορούν να αναγνωρίσουν τις σελίδες που επισκέπτεται ένας χρήστης αναλύοντας τα μοτίβα της κίνησης των πακέτων (Ferlin-Reiter *et al.*, 2026).

5.4.3 DNS-over-HTTPS3

Το πρωτόκολλο **DNS-over-HTTPS/3 (DoH/3** αποτελεί την εξέλιξη του DoH πάνω από το HTTP/3, το οποίο με τη σειρά του λειτουργεί πάνω από το QUIC. Αν και προσφέρει παρόμοια πλεονεκτήματα με το DoQ όσον αφορά την εξάλειψη του head-of-line blocking, οι μελέτες δείχνουν ότι το DoQ υπερέχει ελαφρώς στις επιδόσεις λόγω της ευρύτερης υποστήριξης λειτουργιών όπως το 0-RTT (66% των επιλυτών DoQ έναντι χαμηλότερων ποσοστών στο DoH/3). Παρόλα αυτά, το DoH/3 είναι το **προτιμώμενο πρωτόκολλο** από τους περισσότερους

σύγχρονους browsers. Σε συνθήκες δικτύου χαμηλής καθυστέρησης, οι διαφορές στην απόδοση μεταξύ DoQ, DoH/3 και DoUDP είναι πρακτικά ανεπαίσθητες για τον χρήστη, με αποκλίσεις μικρότερες του **1%** στο συνολικό χρόνο φόρτωσης. Η τεχνολογία αυτή θεωρείται μία από τις πιο σύγχρονες προσεγγίσεις για ασφαλή και ιδιωτική επίλυση ονομάτων στο διαδίκτυο, καθώς συνδυάζει την ευελιξία του DoH με τα πλεονεκτήματα των νέων πρωτοκόλλων μεταφοράς δεδομένων (Ferlin-Reiter *et al.*, 2026).

Συμπεράσματα

Με βάση τα ευρήματα της βιβλιομετρικής ανάλυσης και τη μελέτη της εξέλιξης των πρωτοκόλλων που παρουσιάζονται στις πηγές, τα κύρια συμπεράσματα της πτυχιακής εργασίας συνοψίζονται στα εξής:

- **Συνεχής Αύξηση του Ερευνητικού Ενδιαφέροντος:** Η ανάλυση των 1.770 δημοσιεύσεων δείχνει μια ξεκάθαρη **ανοδική τάση** στην επιστημονική παραγωγή γύρω από το DNS, επιβεβαιώνοντας ότι παραμένει ένα εξαιρετικά ενεργό και επίκαιρο πεδίο έρευνας.
- **Μετάβαση από την Κλιμάκωση στην Ασφάλεια:** Η ιστορική εξέλιξη του συστήματος ξεκίνησε από την ανάγκη για κλιμάκωση αλλά πλέον η έρευνα επικεντρώνεται στην ασφάλεια και την ιδιωτικότητα. Ο αρχικός σχεδιασμός κρίθηκε ευάλωτος σε επιθέσεις, οδηγώντας στην ανάπτυξη κρυπτογραφημένων λύσεων.
- **Κυριαρχία των Κρυπτογραφημένων Πρωτοκόλλων (DoT/DoH):** Η υιοθέτηση πρωτοκόλλων όπως το DNS-over-TLS (DoT) και το DNS-over-HTTPS (DoH) ενισχύει την προστασία από την παρακολούθηση, αλλά μεταφέρει τον έλεγχο της κίνησης από τους τοπικούς παρόχους (ISPs) στους κατασκευαστές περιηγητών και τους παρόχους cloud.
- **Τεχνολογική Υπεροχή των Νέων Πρωτοκόλλων:** Τα σύγχρονα πρωτόκολλα που βασίζονται στο QUIC, όπως το DNS-over-QUIC (DoQ) και το DoH/3, στοχεύουν στη μείωση της καθυστέρησης (latency) και την εξάλειψη τεχνικών προβλημάτων όπως το *head-of-line blocking*. Το DoQ φαίνεται να υπερέχει ελαφρώς σε επιδόσεις, αν και το DoH/3 είναι το προτιμώμενο πρωτόκολλο από τους περισσότερους σύγχρονους browsers.
- **Βελτιστοποίηση Δικτύων:** Το εξελιγμένο DNS λειτουργεί πλέον ως ένας έξυπνος μηχανισμός δρομολόγησης επιπέδου εφαρμογής, επιτρέποντας την καλύτερη διανομή περιεχομένου (CDNs) και την αποτελεσματικότερη εξισορρόπηση φορτίου (load-balancing)

Συμπερασματικά, το Σύστημα Ονοματοδοσίας Διαδικτύου μετασχηματίζεται από μια απλή υποδομή σε ένα **κρυπτογραφημένο σύστημα προσανατολισμένο στην ιδιωτικότητα**, διασφαλίζοντας τη συνέχεια και την ασφάλεια του παγκόσμιου ιστού στον 21ο αιώνα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. A Survey on DNS Encryption: Current Development, Malware Misuse, and Inference Techniques MINZHAO LYU, University of New South Wales, Australia
2. Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., & Hoffman, P. (2016). *Specification for DNS over Transport Layer Security (TLS)* (RFC 7858). RFC Editor.
3. Ferlin-Reiter, S. et al. (eds) (2026) *Passive and Active Measurement: 27th International Conference, PAM 2026, Proceedings*. Cham: Springer Nature Switzerland.
4. Kosek, M., Doan, T.V., Granderath, M. and Bajpai, V. (2022) 'One to Rule them All? A First Look at DNS over QUIC', *Proceedings of the 2022 ACM SIGCOMM Internet Measurement Conference*, pp. 432–440.
5. Kurose, J.F. and Ross, K.W. (2017) *Computer Networking: A Top-Down Approach*. 7th edn. Boston: Pearson.
6. Lyu, M. (2021) 'A Survey on DNS Encryption: Current Development, Malware Misuse, and Inference Techniques', *ACM Computing Surveys*, pp. 1–28.
7. Stallings, W. (2014) *Data and Computer Communications*. 10th edn. Boston: Pearson.
8. Tanenbaum, A.S. and Wetherall, D. (2011) *Computer Networks*. 5th edn. Boston: Pearson Prentice Hall.