ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)

στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

“Ανάθεση Ελέγχου Πρόσβασης για αρχιτεκτονικές NDN/CCN ICN”

Γεράσιμος Μεντζελόπουλος

ΑΘΗΝΑ, ΣΕΠΤΕΜΒΡΙΟΣ 2017

Περιεχόμενα

Σχήματα και Πίνακες

Περίληψη

1 Εισαγωγή

Η σημερινή αρχιτεκτονική του Διαδικτύου βασίζεται σε διευθύνσεις από αριθμούς της μορφής xxx.xxx.xxx.xxx όπου το x = 0 – 254. Κάθε υπολογιστής που είναι συνδεδεμένος σε αυτό έχει υποχρεωτικά μια τέτοια διεύθυνση. Κάθε φορά όμως που ένα χρήστης ζητά στοιχεία από έναν κόμβο πληκτρολογεί το αντίστοιχο μνημονικό του όνομα και όχι τη διεύθυνση και ο λόγος είναι προφανής: μνημονικά είναι ευκολότερο ένα περιγραφικό όνομα παρά μια σειρά αριθμών διαχωρισμένων με τελεία. Κατά συνέπεια στο υποκείμενο περιβάλλον του διαδικτύου υπάρχει ένας μηχανισμός (Domain Name Service, DNS) που αντιστοιχεί κάθε μνημονικό όνομα που πληκτρολογείται με την αντίστοιχη διεύθυνση πρωτοκόλλου (Internet Protocol, IP) του υπολογιστή που την έχει. Η προσέγγιση αυτή δημιουργεί αρκετά θέματα με κυριότερα την ασφάλεια, την αποδοτικότητα, την ευκολία κ.α.

Προσφάτως έχει αναπτυχθεί μια νέα, πολλά υποσχόμενη, αρχιτεκτονική η οποία προωθεί τη λογική ενός δικτύου προσανατολισμένου στην πληροφορία (Information Centric Network, ICN) και όχι στις διευθύνσεις IP. Σε αυτό το περιβάλλον οποιαδήποτε πληροφορία έχει ένα περιγραφικό όνομα και οποιοσδήποτε ενδιαφέρεται για αυτή την αναζητά βάσει αυτού.

Στην αρχιτεκτονική ICN το δίκτυο μπορεί να αποθηκεύει το περιεχόμενο κατανεμημένα, διευκολύνοντας έτσι την αποδοτική μεταφορά του, την απόδοση μιας κλιμακούμενης πολιτική ελέγχου πρόσβασης σε περίπτωση που χρειάζεται η προστασία του περιεχομένου κ.α.

Η Ανάθεση Ελέγχου Πρόσβασης (ΑΕΠ) είναι ένας μηχανισμός που επιτρέπει σε μια έμπιστη $3^{η}$ οντότητα, αναφερόμενη ως Πάροχος Ελέγχου Πρόσβασης (ΠΕΠ), να πάρει μια απόφαση ανάθεσης ελέγχου πρόσβασης, για έναν χρήστη που αιτείται πρόσβαση σε δεδομένα, εκ μέρους οποιασδήποτε οντότητας. Στο περιβάλλον του ICN μια τυπική συναλλαγή περιλαμβάνει τα ακόλουθα βήματα:

(i) Ο δημιουργός ενός περιεχομένου δεδομένων (Εκδότης) δημιουργεί μια Πολιτική Ελέγχου Πρόσβασης, την αποθηκεύει σε έναν ΠΕΠ και ανακτά ένα URI για αυτή την πολιτική.

(ii) Ο Εκδότης στη συνέχεια αποθηκεύει κάποιο περιεχόμενο σε έναν αποθηκευτικό κόμβο μαζί με το URI της πολιτικής που το προστατεύει.

(iii) Ένας χρήστης ζητά το περιεχόμενο από τον κόμβο αποθήκευσης και μαθαίνει το URI της πολιτικής ελέγχου πρόσβασης

(iv) Ο χρήστης αυθεντικοποιείται μέσω του ΠΕΠ και ανακτά μια σήμανση «αυθεντικοποίηση»

(v) Ο χρήστης παρουσιάζει την «αυθεντικοποίηση» στον κόμβο αποθήκευσης και ανακτά το περιεχόμενο.

Η ανάθεση ελέγχου πρόσβασης έχει πολλά πλεονεκτήματα όταν χρησιμοποιείται με μία ICN αρχιτεκτονική. Σε αυτές τις αρχιτεκτονικές, όλες οι δικτυακές λειτουργίες γίνονται με βάση ονόματα περιεχομένου αντί δικτυακών τοποθεσιών, με αποτέλεσμα οι χρήστες να ζητούν απευθείας από το δίκτυο ένα αντικείμενο περιεχομένου με βάση το όνομά του και το δίκτυο να είναι υπεύθυνο στο να το βρει και να το ανακτήσει. Στις ICN αρχιτεκτονικές το περιεχόμενο είναι διασκορπισμένο σε πολλές δικτυακές τοποθεσίες, συχνά εκτός του κόσμου που διαχειρίζεται ο ιδιοκτήτης του περιεχομένου.

Στόχος αυτής της Διπλωματικής Εργασίας είναι η υιοθέτηση του μηχανισμού ΑΕΠ για τα δίκτυα με αρχιτεκτονική NDN/CCN ICN.

2 Αρχιτεκτονική ICN

Γενική περιγραφή του ICN (Information-Centric Networking) [1]

Η τεράστια ανάπτυξη του διαδικτύου που συντελέστηκε τα προηγούμενα χρόνια με την εμφάνιση νέων εφαρμογών δημιούργησε νέες απαιτήσεις και ανάγκες όπως υποστήριξη για επεκτάσιμη διανομή περιεχομένου, κινητικότητα, ασφάλεια, εμπιστοσύνη κλπ. Όμως το διαδίκτυο δεν σχεδιάστηκε εξαρχής ώστε να υποστηρίζει τέτοιες απαιτήσεις, με αποτέλεσμα αυτές να «εκπληρώνονται» με τη χρήση «λογισμικού επιδιόρθωσης» κάτι το οποίο αύξησε την πολυπλοκότητα χωρίς οι παρεμβάσεις αυτές να αποτελούν μόνιμες και εγγενείς. Επιπρόσθετα αρκετές από τις νέες ανάγκες δεν μπορούν να εκπληρωθούν επαρκώς από την τρέχουσα αρχιτεκτονική. Συνεπώς είναι φανερό ότι ένας τρόπος αντιμετώπισης των νέων αυτών προκλήσεων είναι ο σχεδιασμός νέων αρχιτεκτονικών στη βάση τωρινών και μελλοντικών απαιτήσεων.

Ο όρος «Δικτύωση με βάση την Πληροφορία» (ICN) εμφανίστηκε περίπου το 2010, εμπνευσμένος πιθανόν από την ομιλία «Ένας νέος τρόπος αναζήτησης στη δικτύωση» του Van Jacobson το 2006. Στην ομιλία αυτή επισημάνθηκε μια αναδυόμενη τάση στο διαδίκτυο, σχετική με την αρχιτεκτονική διανομής περιεχομένου. Η τάση αυτή, εμπνευσμένη από το γεγονός ότι υπάρχει αύξηση της διάχυσης της πληροφορίας που διακινείται στο διαδίκτυο, στοχεύει στο να αντιμετωπίσει τα προβλήματα και τις δυσχέρειες της τρέχουσας αρχιτεκτονικής. Χρησιμοποιώντας ονοματολογία στην πληροφορία, στο επίπεδο του δικτύου, το ICN ευνοεί την ανάπτυξη αποθήκευσης εντός του δικτύου και μηχανισμών πολλαπλής διανομής διευκολύνοντας έτσι την αποτελεσματική και έγκαιρη παράδοση πληροφορίας στους χρήστες του διαδικτύου. Επιπρόσθετα στοχεύει στο να διευθετήσει θέματα όπως τη διαχείριση κινητικότητας και την επιβολή πολιτικών ασφάλειας.

2.1 Σημαντικές έννοιες, ορολογία και αρχές του ICN

A. Προσανατολισμός στην ονομασία της Πληροφορίας

Η πληροφορία αποκτά όνομα, διεύθυνση και ταίριασμα ανεξάρτητα από την τοποθεσία που βρίσκεται, αποκτώντας έτσι τη δυνατότητα να βρίσκεται οπουδήποτε στο δίκτυο. Αυτό έχει σαν αποτέλεσμα η ανάκτηση της διατιθέμενης πληροφορίας να καθοδηγείται αποκλειστικά από τον ενδιαφερόμενο λήπτη, σε αντίθεση με το σημερινό διαδίκτυο όπου οι αποστολείς έχουν τον απόλυτο έλεγχο στα δεδομένα που ανταλλάσσονται. Από τη στιγμή που γίνει μια αίτηση για συγκεκριμένη πληροφορία το δίκτυο ICN είναι υπεύθυνο για την εύρεση της καλύτερης πηγής που την παρέχει μέσω της δρομολόγησης των αιτήσεων για την εύρεση της καταλληλότερης πηγής.

Β. Προσανατολισμός στην παράδοση της Πληροφορίας

Το δίκτυο ICN, από τη στιγμή που ζητηθεί μια συγκεκριμένη πληροφορία, εκτός του ότι εντοπίζει την αρχική πηγή της, εκμεταλλεύεται ταυτόχρονα δικτυακές θέσεις προσωρινής αποθήκευσης οι οποίες κρατούν αντίγραφα, είτε ολόκληρης είτε τμήματος, της αιτηθείσας πληροφορίας. Η διαδικασία αυτή είναι ενσωματωμένη στο επίπεδο του δικτύου αποφεύγοντας έτσι την ανάγκη για επιπρόσθετες, πολυδάπανες και συχνά μη δημόσιες, υλοποιήσεις όπως συμβαίνει με τα δίκτυα CDN (Δίκτυα Διανομής Περιεχομένου).

Γ. Προσανατολισμός στην Κινητικότητα

Η κινητικότητα ενός κόμβου υποστηρίζεται στο δίκτυο ICN από το μοντέλο επικοινωνίας εκδότη/συνδρομητή. Σε αυτό το μοντέλο οι χρήστες που ενδιαφέρονται για μια πληροφορία δηλώνουν το ενδιαφέρον τους, κάνοντας μια συνδρομή για αυτή και αντίστοιχα οι χρήστες που προσφέρουν πληροφορίες τις κοινοποιούν χρησιμοποιώντας τη διαδικασία της έκδοσής τους στο δίκτυο. Μεσίτες που υπάρχουν μέσα στο δίκτυο είναι υπεύθυνοι στο να ταιριάξουν τις συνδρομές με τις εκδόσεις παρέχοντας π.χ. μια λειτουργία ραντεβού. Η ευελιξία του ICN έγκειται στο ότι δεν μεταφέρονται αυτό καθεαυτό τα δεδομένα στην έκδοση, ενώ η συνδρομή αναφέρεται σε μια πληροφορία που είναι ήδη διαθέσιμη αφήνοντας έτσι ως προαιρετική τη δυνατότητα για μόνιμες συνδρομές (πχ. όταν η λήψη πολλαπλών εκδόσεων ταιριάζει με μια συνδρομή). Επιπλέον το μοντέλο είναι ανεξάρτητο χώρου και χρόνου. Η επικοινωνία μεταξύ εκδότη και συνδρομητή δεν είναι απαραίτητα συγχρονισμένη, όπως επίσης δεν έχει καμία αναφορά ο ένας για τον άλλο. Τα στοιχεία αυτά διευκολύνουν πολύ την υποστήριξη κινητικότητας χωρίς περιορισμούς.

Δ. Έμφαση στην Ασφάλεια

Ο αρχικός σχεδιασμός του διαδικτύου ήταν να λειτουργεί σε ένα περιβάλλον αμοιβαίας εμπιστοσύνης, ευελιξίας, μακριά από αυθεντικοποίηση χρηστών και δεδομένων δίνοντας ελεύθερα τη δυνατότητα σε νέους κόμβους να συνδεθούν στο δίκτυο. Όμως αυτά τα χαρακτηριστικά έδωσαν αργότερα τη δυνατότητα σε κακόβουλους χρήστες να τα χρησιμοποιήσουν ώστε να επιτύχουν σκοπούς ξένους προς τον σκοπό του διαδικτύου. Η χρήση επιθέσεων Άρνησης Υπηρεσιών (DoS) εξελίχθηκε σε μια τεχνική που βάλει υπολογιστές και υπηρεσίες καλύπτοντας ταυτόχρονα τα ίχνη του επιτιθέμενου. Για να αντιμετωπισθούν τέτοιες περιπτώσεις αναπτύχθηκαν διορθώσεις ασφάλειας καθώς και νέα πρωτόκολλα επικοινωνίας με έμφαση την ασφάλεια. Σε κάθε περίπτωση όμως οι λύσεις αυτές δεν ενσωματώθηκαν εγγενώς στον πυρήνα λειτουργιών του διαδικτύου αλλά αποτέλεσαν επεκτάσεις της υπάρχουσας υποδομής ζητώντας ταυτόχρονα περισσότερους υπολογιστικούς πόρους ώστε να λειτουργήσουν. Τα περισσότερα από τα προβλήματα ασφάλειας βασίζονται στο γεγονός ότι δεν υπάρχει σύνδεση μεταξύ της σημασιολογίας της πληροφορίας στο επίπεδο εφαρμογής και των δεδομένων που υπάρχουν στα μεμονωμένα IP πακέτα. Η έλλειψη αυτή

επιφέρει αξιοσημείωτη επιβάρυνση στην προσπάθεια ενσωμάτωσης μηχανισμών ανάληψης ευθύνης στην τρέχουσα αρχιτεκτονική με αποτέλεσμα οι μηχανισμοί αυτοί να ενεργοποιούνται μόνο σε κρίσιμες περιπτώσεις όπως πχ. η επιβολή του νόμου.

Σε αντίθεση με το προαναφερθέν πλαίσιο, οι αρχιτεκτονικές του δικτύου ICN καθοδηγούνται από το κίνητρο και την αναζήτηση της πληροφορίας, δηλαδή δεν υπάρχει ροή δεδομένων παρά μόνο όταν κάποιος χρήστης ζητήσει αποκλειστικά μια συγκεκριμένη πληροφορία. Αναμένεται ότι η φιλοσοφία αυτή θα μειώσει σημαντικά την ποσότητα μετακίνησης «κακών» δεδομένων, όπως πχ. η ανεπιθύμητη αλληλογραφία, ενώ ταυτόχρονα θα διευκολύνει την ανάπτυξη της ανάληψης ευθύνης και μηχανισμούς εύρεσης εγκληματολογικής δραστηριότητας. Επιπρόσθετα, για τις αρχιτεκτονικές που χρησιμοποιούν αυτο-πιστοποιημένα ονόματα για την πληροφορία δίνουν τη δυνατότητα εγγενούς φιλτραρίσματος κακόβουλων δεδομένων. Επίσης το γεγονός της έμμεσης και όχι άμεσης σχέσης του χρήστη που ζητά πληροφορίες με τον χρήστη που τις παρέχει, δίνει τη δυνατότητα ενός παραπάνω βήματος στην προσπάθεια καταπολέμησης των τακτικών Άρνησης Υπηρεσιών διότι τα αιτήματα των ενδιαφερόμενων χρηστών μπορούν να αξιολογηθούν προτού φτάσουν στον τελικό τους προορισμό προσδίδοντας μάλιστα στον αιτούμενο ιδιωτικότητα καθώς ο πάροχος (εκδότης) της πληροφορίας δεν γνωρίζει την ταυτότητά του.

2.2. Λειτουργίες κλειδιά στο ICN

Ονομασία: Η δομή του ονόματος που ανατίθεται σε ένα τμήμα πληροφορίας ή υπηρεσίας η οποία μπορεί να κυκλοφορήσει στο δίκτυο. Σε όλες τις υπάρχουσες αρχιτεκτονικές ICN τα ονόματα πληροφορίας είναι ανεξάρτητα της τοποθεσίας που βρίσκεται η πληροφορία, μπορούν να κυμαίνονται από μη ιεραρχικά σε ιεραρχικά και μπορούν να είναι ή να μην είναι σε αναγνώσιμη μορφή από τον άνθρωπο.

Εύρεση ονόματος και δρομολόγηση δεδομένων: Αφορά το ταίριασμα του ονόματος μιας πληροφορίας με τον πάροχο ή την πηγή που μπορεί να την παρέχει ενώ η δρομολόγηση αφορά την κατασκευή μιας διαδρομής που θα ακολουθηθεί για τη μεταφορά των σχετικών δεδομένων. Οι δύο διαδικασίες μπορεί να είναι ενοποιημένες ή ανεξάρτητες. Στην πρώτη περίπτωση το αίτημα της πληροφορίας δρομολογείται σε έναν πάροχο πληροφοριών ο οποίος στη συνέχεια στέλνει τα δεδομένα στον αιτούντα (συνδρομητή) ακολουθώντας την αντίστροφη διαδρομή από αυτή που ακολουθήθηκε κατά την αίτηση. Αντίθετα, στην δεύτερη περίπτωση, η λειτουργία της εύρεσης τους ονόματος δεν προσδιορίζει το μονοπάτι που θα ακολουθήσουν τα δεδομένα από τον πάροχο προς τον συνδρομητή, οπότε θα χρησιμοποιηθεί μια ανεξάρτητη λειτουργία δρομολόγησης των δεδομένων.

Προσωρινή Αποθήκευση: Ξεχωρίζει σε προσωρινή αποθήκευση δεδομένων κατά μήκος της διαδρομής που προκύπτει από κάποιο αίτημα εύρεσης πληροφορίας και σε αποθήκευση εκτός διαδρομής. Σε

αρχιτεκτονικές με ανεξάρτητες την εύρεση πληροφορίας και τη δρομολόγησή της, η αποθήκευση εκτός διαδρομής πρέπει να υποστηρίζεται από την λειτουργία της εύρεσης του ονόματος ενώ σε αρχιτεκτονικές με ενοποιημένες τις δύο αυτές λειτουργίες η υποστήριξη πρέπει να γίνεται από το σύστημα προώθησης των αιτήσεων για πληροφορία.

Κινητικότητα: Η υποστήριξη κινητικότητας είναι εγγενής για τους συνδρομητές αλλά πιο δύσκολα να υποστηριχθεί για τους εκδότες αφού τα συστήματα εύρεσης ονόματος και δρομολόγησης πρέπει πρώτα να ενημερωθούν.

Ασφάλεια: Σχετίζεται πολύ με τη δομή ονομασίας. Στην περίπτωση ονοματοδότησης αναγνώσιμης από ανθρώπους είναι απαραίτητος ένας έμπιστος πράκτορας ή μια σχέση εμπιστοσύνης με τη λειτουργία της εύρεσης του ονόματος ώστε να υπάρχει επαλήθευση ότι η επιστρεφόμενη πληροφορία πράγματι αντιστοιχεί με το αιτούμενο όνομα. Στην περίπτωση των μη ιεραρχικών ονομάτων αυτά μπορούν να υποστηρίξουν αυτο-πιστοποίηση αλλά δεν είναι ανθρωπίνως αναγνώσιμα, απαιτώντας έτσι ένα άλλο έμπιστο σύστημα που να ταιριάζει αναγνώσιμα ονόματα σε μη ιεραρχικά.

Υπό αυτή την κατεύθυνση, μερικές διαφορετικές αρχιτεκτονικές ICN εμφανίστηκαν τα επόμενα χρόνια, όπως:

- το έργο DONA [2] στο Berkeley,
- το έργο Publish-Subscribe Internet Technology (PURSUIT) [3] και ο προκάτοχός του Publish-Subscribe Internet Routing Paradigm (PSIRP) [4] που χρηματοδοτήθηκαν από την Ε.Ε.,
- το Scalable & Adaptive Internet soLutions (SAIL) [5] και ο προκάτοχός του 4WARD [6],
- το COntent Mediator architecture for contentaware nETworks (COMET) [7],
- το έργο CONVERGENCE [8],
- το Named Data Networking (NDN) [9] και ο προκάτοχός του Content Centric Networking (CCN) [10] καθώς και το MobilityFirst [11], έργα που χρηματοδοτήθηκαν από τις ΗΠΑ,
- όπως επίσης το έργο ANR Connect [12] που υιοθετεί την αρχιτεκτονική NDN και χρηματοδοτήθηκε από τη Γαλλία.

3 Λεπτομέρειες Δικτύου NDN

3.1 Γενικά Χαρακτηριστικά

Το Named Data Networking (NDN) είναι ένα από τα πέντε ερευνητικά έργα που χρηματοδοτούνται από το Εθνικό Ίδρυμα Επιστήμης των Η.Π.Α. στο πλαίσιο του Προγράμματος Μελλοντικής Αρχιτεκτονικής του Διαδικτύου. Το NDN έχει τις ρίζες του σε ένα προηγούμενο έργο, το Content-Centric Networking (CCN), το οποίο ο Van Jacobson ξεκίνησε στο Xerox PARC, την ίδια χρονική περίοδο με την ομιλία του το 2006 στη Google «A New Way to look at Networking» [13], ώστε να μετατρέψει το όραμα που είχε, να προωθήσει την τρέχουσα αρχιτεκτονική του διαδικτύου στην αρχιτεκτονική διανομής περιεχομένου, σε ένα ενεργό και συνεχώς εξελισσόμενο πρωτότυπο. [14]

Το κίνητρο του έργου NDN [15]

Το κίνητρο πίσω από το έργο NDN είναι η θεμελιώδης διαφορά μεταξύ της σημερινής αρχιτεκτονικής του Διαδικτύου και της χρήσης του. Σήμερα χτίζονται, υποστηρίζονται και χρησιμοποιούνται εφαρμογές και υπηρεσίες στο Internet πάνω από μια εξαιρετικά ικανή αρχιτεκτονική που όμως δεν έχει σχεδιαστεί για να τις υποστηρίξει.

Ειδικότερα, τα σημερινά πακέτα IP μπορούν να ονομάσουν μόνο τα τελικά σημεία των επικοινωνιών (διευθύνσεις IP) στο επίπεδο δικτύου. Τι γίνεται αν γενικευτεί αυτό το επίπεδο για να ονομαστεί οποιαδήποτε πληροφορία (ή περιεχόμενο), σε κάθε σημείο και όχι μόνο στα τελικά; Μπορεί να διευκολυνθεί η ανάπτυξη, η διαχείριση, η ασφάλεια και η χρήση των δικτύων;

Πως διαφέρει το NDN από το CCN (Content-Centric Networking)

Το CCN αναφέρεται στο έργο που ξεκίνησε στο PARC, το οποίο περιελάμβανε την καθοδήγηση για την ανάπτυξη ενός κώδικα βάσης λογισμικού που αντιπροσωπεύει μια βασική υλοποίηση αυτής της αρχιτεκτονικής. Το Networked Data Networking (NDN) αναφέρεται στο χρηματοδοτούμενο από την NSF Project Future Internet Architecture, μια συνεργασία 12 πανεπιστημίων που ξεκίνησε το 2010 και περιελάμβανε το PARC. Το έργο NDN αρχικά χρησιμοποίησε το CCNx ως κωδικό βάσης του, αλλά από το 2013 έχει αναπτύξει μια έκδοση για να υποστηρίξει τις ανάγκες που σχετίζονται ειδικά με την έρευνα και ανάπτυξη της αρχιτεκτονικής που χρηματοδοτείται από το NSF (και όχι απαραίτητα του PARC).

Η διαφορά στην έννοια μεταξύ NDN και ICN

Το ICN ερευνά ευρύτερα την διαδικτυακή αρχιτεκτονική που σχετίζεται με το τρίπτυχο περιεχόμενο/πληροφορία/δεδομένο, ενώ το NDN στοχεύει μια συγκεκριμένη αρχιτεκτονική κάτω από την ομπρέλα του ICN .

Ο μελλοντικός ρόλος του ICN σε 20 χρόνια. Θα είναι το κυρίαρχο παράδειγμα των επικοινωνιών;

Το ICN έχει κυριαρχήσει πλέον στον χώρο των δικτύων παροχής περιεχομένου. Οι δικτυακοί τόποι YouTube, Netflix, Amazon, iTunes κλπ. είναι αμιγώς δίκτυα ICN και καταναλώνουν περισσότερο από το 50% της διαδικτυακής κίνησης παγκοσμίως. Όμως, το σημερινό ICN-over-IP είναι αναποτελεσματικό και ανασφαλές, επειδή το επίπεδο που είναι προσανατολισμένο στην πληροφορία έχει μια φτωχή αντιστοίχιση με το επίπεδο του διαδικτυακού περιβάλλοντος. Το Διαδίκτυο επίσης χρησιμοποιείται ευρέως από κινητές συσκευές (οι χρήστες των οποίων είναι επίσης προσανατολισμένοι στο περιεχόμενο), τις οποίες η αρχιτεκτονική IP δεν υποστηρίζει καλά. Τέλος, η αρχιτεκτονική IP δεν σχεδιάστηκε για να υποστηρίζει φυσικά ασφαλή επικοινωνία ή ασφαλή διανομή δεδομένων. Το ICN αντί να αγνοεί την αυξανόμενη ασυμφωνία μεταξύ της αρχιτεκτονικής και της παγκόσμιας χρήσης του Διαδικτύου, εμπνέεται από το σχεδιασμό, την ανάπτυξη και τη σταδιακή εξάπλωση μιας αρχιτεκτονικής που καλύπτει τη διαφορά με το τωρινό κυρίαρχο πρότυπο επικοινωνιών.

Αυτή η αρχιτεκτονική ασυμφωνία είναι ανάλογη με αυτήν που επικρατεί μεταξύ των πακέτων προσανατολισμένων στο IP και του υποστρώματος της κυκλωματικής τηλεφωνίας κατά τη διάρκεια των πρώτων 20 ετών του Διαδικτύου. Φανταστείτε το ερώτημα του 1990: "Ποιος θα είναι ο ρόλος του Διαδικτύου στο παγκόσμιο σύστημα τηλεφωνίας 20 χρόνια από τώρα;" Γνωρίζουμε τώρα ότι η απάντηση ήταν ότι "το παγκόσμιο τηλεφωνικό σύστημα έγινε μόνο μία από πολλές εφαρμογές που τρέχουν μέσω IP διαδικτύου". Η επικάλυψη έγινε το υπόστρωμα επειδή μπορούσε να κάνει καλύτερα περισσότερα πράγματα. Προβλέπεται ότι θα μπορούσε να υποκατασταθεί το "Internet" για το "τηλεφωνικό σύστημα" και το "NDN / ICN" για το "internet IP" για να μετακινηθεί το ρολόι 20 χρόνια μπροστά.

Σχεδίαση από την αρχή

Το NDN είναι σχεδιασμένο από την αρχή, καθώς είναι μια εντελώς νέα αρχιτεκτονική και δεν έχει εξάρτηση από το IP. Όπως αναφέρεται στην πρώτη πρόταση προς την NSF, "Το NDN είναι μια εντελώς νέα αρχιτεκτονική, αλλά η λειτουργία της μπορεί να βασιστεί στην τρέχουσα πρακτική. Ο σχεδιασμός του

αντικατοπτρίζει την κατανόηση των δυνατοτήτων και των περιορισμών της τρέχουσας αρχιτεκτονικής του Διαδικτύου".

Σύνοψη των θεμελιωδών αρχών του NDN

Πρώτον, αξιοποιούνται οι επιτυχημένες αρχές TCP / IP, συμπεριλαμβανομένου του "κομβικού σημείου" στο επίπεδο του δικτύου, για την προώθηση ανεξάρτητης καινοτομίας και ελέγχου από άκρο σε άκρο, όπου ενδείκνυται.

Δεύτερον, λαμβάνεται υπόψη η εξέλιξη στη χρήση του δικτύου τα τελευταία τριάντα χρόνια, και συγκεκριμένα η κυρίαρχη και η αδιάκοπα αυξανόμενη έμφαση στο περιεχόμενο. Γενικεύοντας το "κομβικό σημείο" για να ικανοποιηθεί αυτή η εξέλιξη, επιτρέπεται στα πακέτα να ονομάζουν (και να ζητούν) περιεχόμενο.

Τέλος, ενσωματώνονται θεμελιώδεις αρχιτεκτονικές βασισμένες στα μαθήματα από τις αδυναμίες του TCP / IP: κρυπτογραφικός έλεγχος ταυτότητας κάθε πακέτου. εγγενής έλεγχος ροής κυκλοφορίας (ισορροπία ροής) και προσαρμοστικές δυνατότητες δρομολόγησης και προώθησης.

Πως το NDN διαφέρει από τα CDNs

Ένα δίκτυο διανομής περιεχομένου (CDN) είναι ένα καλό παράδειγμα υπηρεσίας που υλοποιείται ως επικάλυψη στην σημερινή αρχιτεκτονική TCP / IP για να καλύψει τη ζήτηση για διανομή κλιμακούμενου περιεχομένου, όταν το ίδιο περιεχόμενο ζητείται από πολλούς χρήστες. Οι πελάτες CDN τείνουν να είναι σχετικά μεγάλοι ιδιοκτήτες περιεχομένου που είναι διατεθειμένοι να πληρώσουν για υψηλότερη απόδοση του περιεχομένου τους. Οι παραγωγοί περιεχομένου χωρίς υπηρεσίες CDN θα αντιμετώπιζαν προβλήματα φορτίου και επιδόσεων εάν κάποτε το περιεχόμενό τους γίνει δημοφιλές.

Τα δίκτυα CDN λειτουργούν στο επίπεδο εφαρμογής, γεγονός που εγείρει δύο ζητήματα: πώς να αποκτηθούν αιτήματα περιεχομένου πελατών στο σύστημα CDN (μια κοινή λύση είναι για τον πάροχο του CDN να φιλοξενήσει την υπηρεσία DNS για το όνομα τομέα του περιεχομένου που εξυπηρετεί). και χαρτογράφηση κάθε αιτήματος στον πλησιέστερο κόμβο CDN που εξυπηρετεί το περιεχόμενο. Το NDN λειτουργεί απευθείας στο επίπεδο του δικτύου και φυσικά προωθεί τα πακέτα ενδιαφέροντος κατά μήκος των καλύτερων διαδρομών στα επιθυμητά δεδομένα.

Κοινά σημεία μεταξύ IP αρχιτεκτονικής και NDN

- Και οι δύο αρχιτεκτονικές μοιράζονται το ίδιο σχήμα κλεψύδρας, με το επίπεδο IP / NDN να είναι η στενή μέση.
- Στέλνουν datagrams.
- Ακολουθούν την αρχή από άκρο σε άκρο [16].
- Και οι δύο χρησιμοποιούν το δικό τους χώρο ονομάτων για την παράδοση δεδομένων (δηλ. Το IP χρησιμοποιεί διευθύνσεις IP για να παραδώσει datagrams μεταξύ κόμβων IP, το NDN χρησιμοποιεί το χώρο ονομάτων της εφαρμογής για να παραδώσει datagrams μεταξύ κόμβων NDN).

Οι βασικές διαφορές μεταξύ IP και NDN

- Χρησιμοποιούν διαφορετικό χώρο ονόματος: διεύθυνση IP και όνομα.
- Το NDN περιλαμβάνει ένα πρωτόκολλο ασφαλείας απευθείας στη στενή μέση (υπογράφεται κάθε πακέτο δεδομένων).
- Το IP στέλνει πακέτα στις διευθύνσεις προορισμού. Το NDN χρησιμοποιεί πακέτα ενδιαφέροντος για να ανακτήσει τα πακέτα δεδομένων.
- Το IP (εξ ορισμού) έχει ένα επίπεδο που δεν κρατά την κατάσταση των εισερχόμενων δεδομένων στους δρομολογητές. Αντίθετα το NDN διατηρεί σε κάποιο επίπεδο την κατάσταση των δεδομένων. Μαζί με τη στρατηγική προώθησης, αυτό το επίπεδο προσφέρει στα δίκτυα NDN μια ποικιλία επιθυμητών λειτουργιών.

Προώθηση Πακέτων με Κατάσταση

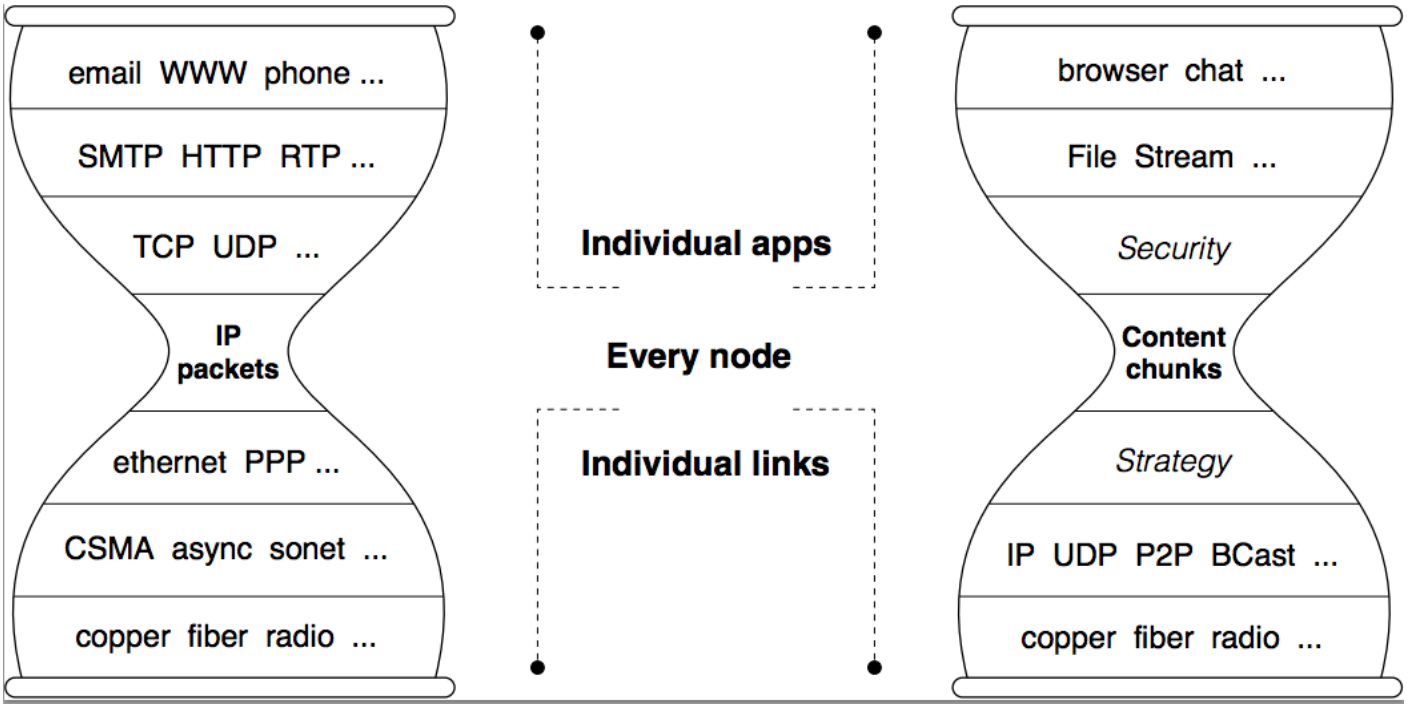
Στο NDN τα πακέτα μεταφέρουν ονόματα δεδομένων αντί για διευθύνσεις προέλευσης και προορισμού. Αυτή η πρακτική οδηγεί σε ένα νέο τύπο προώθησης δικτύου: οι καταναλωτές στέλνουν πακέτα ενδιαφέροντος για να ζητήσουν τα επιθυμητά δεδομένα, οι δρομολογητές τα προωθούν και διατηρούν την κατάσταση όλων των εκκρεμών Ενδιαφερόντων, τα οποία στη συνέχεια χρησιμοποιούνται για να καθοδηγήσουν τα πακέτα Δεδομένων πίσω στους καταναλωτές.

Η διατήρηση της εκκρεμούς κατάστασης ενδιαφέροντος, σε συνδυασμό με την αμφίδρομη ανταλλαγή ενδιαφέροντος και δεδομένων, επιτρέπει τη διαδικασία προώθησης δρομολογητών NDN για τη μέτρηση της απόδοσης διαφόρων διαδρομών, την ταχεία ανίχνευση αποτυχιών και την χρήση εναλλακτικών διαδρομών.

Σύμφωνα με σχετική μελέτη [17] που περιγράφει ένα αρχικό σχέδιο του επιπέδου διαβίβασης του NDN και αξιολογεί την απόδοση παροχής δεδομένων του υπό δυσμενείς συνθήκες, τα αποτελέσματα δείχνουν ότι αυτό το μοντέλο προώθησης μπορεί να παρακάμψει επιτυχώς τους hackers που επιτίθενται στο πρόθεμα ενός πακέτου, να αποφύγει τους αποτυχημένους συνδέσμους και να χρησιμοποιήσει πολλαπλές διαδρομές για να μετριάσει τη συμφόρηση.

NDN: Τα κυριότερα σημεία [18]

Η αρχιτεκτονική κλεψύδρας του Internet έκανε τον σχεδιασμό του κομψό και ισχυρό. Η καρδιά αυτής της αρχιτεκτονικής είναι ένα απλό, καθολικό στρώμα δικτύου (IP) που υλοποίησε όλες τις λειτουργίες που απαιτούνται για την παγκόσμια διασύνδεση. Αυτό το κομβικό σημείο ήταν ο βασικός παράγοντας της εκρηκτικής ανάπτυξης του Διαδικτύου, αλλά μία από τις σχεδιαστικές της είναι η αιτία των σημερινών προβλημάτων στο Διαδίκτυο. Το Διαδίκτυο σχεδιάστηκε ως δίκτυο επικοινωνίας έτσι ώστε οι μοναδικές οντότητες που θα μπορούσαν να ονομαστούν στα πακέτα του ήταν τα τελικά σημεία της κάθε επικοινωνίας. Η πρόσφατη ανάπτυξη του ηλεκτρονικού εμπορίου, των ψηφιακών μέσων, της κοινωνικής δικτύωσης και των εφαρμογών smartphone έχει ως αποτέλεσμα το Διαδίκτυο να χρησιμοποιείται κυρίως ως δίκτυο διανομής. Τα δίκτυα διανομής είναι από τη βάση τους πιο γενικά από τα δίκτυα επικοινωνιών και η επίλυση προβλημάτων διανομής με ένα δίκτυο επικοινωνιών είναι πολύπλοκη και επιρρεπής σε σφάλματα.



Σχήμα 1 - Αρχιτεκτονικές Κλεψύδρας του Διαδικτύου και του NDN

Η ονοματολογία στα δίκτυα NDN

Το πεδίο ονοματολογίας του σημερινού διαδικτύου εξυπηρετείται μέσω της υπηρεσίας DNS μαζί με μια πολύ καλά καταξιωμένη διαδικασία κατανομής και φορέων διοίκησης. Το NDN μπορεί να χρησιμοποιήσει την υπάρχουσα υποδομή για την παράδοση των δεδομένων. Τα δεδομένα ονοματίζονται βάσει της σχεδίασης κάθε εφαρμογής και η ονομασία αυτή είναι «διαφανής» στο δίκτυο.

Τα ονόματα που χρησιμοποιούνται για ανάκτηση δεδομένων παγκόσμια χρειάζονται παγκόσμια μοναδικότητα. Μεμονωμένα ονόματα δεδομένων μπορούν να έχουν νόημα σε συγκεκριμένα πεδία ενδιαφέροντος π.χ. από «το φως σε αυτό το δωμάτιο» μέχρι το «όλα τα ονόματα χωρών». Η εύρεση αποδοτικών στρατηγικών για ανάκτηση δεδομένων εντός των πεδίων ενδιαφέροντος αποτελεί μια νέα περιοχή έρευνας. [19] Τα δίκτυα NDN δεν χρειάζονται την υπηρεσία αναζήτησης «όνομα DNS σε διεύθυνση IP». Όμως επειδή το DNS είναι μια παγκόσμια κατανεμημένη βάση δεδομένων και σήμερα χρησιμοποιείται και για σκοπούς εκτός της αντιστοίχισης ονομάτων τομέα, υπάρχει δυνητικά η πιθανότητα χρήσης ενός συστήματος παρόμοιου με το DNS ώστε να αντιμετωπισθούν θέματα κλιμάκωσης δρομολόγησης διευθύνσεων καθώς και άλλα θέματα.

Διαδίκτυο και NDN. Οι αρχιτεκτονικές Κλεψύδρας

Το NDN διατηρεί την αρχιτεκτονική κλεψύδρας του Internet αλλά εξελίσσει το κομβικό σημείο ώστε να επιτρέψει τη δημιουργία εντελώς γενικών δικτύων διανομής. Το βασικό στοιχείο αυτής της εξέλιξης είναι η κατάργηση του περιορισμού ότι μόνο τα πακέτα μπορούν να ονομάσουν τα τελικά σημεία μιας επικοινωνίας. Όσον αφορά το δίκτυο, το όνομα σε ένα πακέτο NDN μπορεί να είναι οτιδήποτε - ένα τελικό σημείο, ένα κομμάτι ταινίας ή βιβλίου, μια εντολή για την ενεργοποίηση ορισμένων φώτων κλπ. Αυτή η εννοιολογικά απλή αλλαγή επιτρέπει στα δίκτυα NDN να χρησιμοποιούν σχεδόν όλα τις καλά κατανοητές και καλά δοκιμασμένες μηχανικές ιδιότητες του Διαδικτύου για την αποτελεσματική επίλυση όχι μόνο προβλημάτων επικοινωνίας αλλά και προβλημάτων ψηφιακής διανομής και ελέγχου.

Η θεμελιώδης ερευνητική πρόκληση του έργου NDN είναι να εξελιχθεί σε αρχιτεκτονικό πλαίσιο ικανό να επιλύσει πραγματικά προβλήματα, ιδίως σε περιοχές εφαρμογών που εξυπηρετούνται ελάχιστα από το σημερινό Internet. Η επίλυση πραγματικών προβλημάτων αναγκάζει τη συμπλήρωση αρχιτεκτονικών λεπτομερειών και, το σημαντικότερο, επαληθεύει και διαμορφώνει την αρχιτεκτονική κατεύθυνση. Οι συντελεστές του έργου NDN έχουν την πεποίθηση ότι μια αρχιτεκτονική ερευνητική προσπάθεια πρέπει να είναι βασικά πειραματική. Οι ιδιότητες του σχεδιασμού δεν μπορούν να εξαχθούν από μια πνευματική άσκηση ούτε η επικύρωση να γίνει μέσω δοκιμών θερμοκηπίου. Η σχεδίαση του Internet ωρίμασε μέσω της πραγματικής χρήσης του μέσω της πρώιμης εγκατάστασης και το ερευνητικό πρόγραμμα NDN ακολουθεί τα επιτυχημένα βήματα του Internet.

Εφαρμογές και Ανάπτυξή τους στο NDN

Όλων των ειδών οι εφαρμογές μπορούν να επωφεληθούν όταν εκτελούνται σε δίκτυα NDN. Μερικά από τα σημαντικότερα πλεονεκτήματα είναι:

- Βασική υποστήριξη ασφάλειας, ενσωματωμένη στο επίπεδο παράδοσης δεδομένων, που υποστηρίζει εκλεπτυσμένη εμπιστοσύνη επιτρέποντας στους καταναλωτές να αιτιολογήσουν αν ο ιδιοκτήτης ενός δημοσίου κλειδιού είναι αποδεκτός ως εκδότης για συγκεκριμένο τμήμα πληροφορίας σε ορισμένο περιβάλλον.

- Τα ονοματισμένα δεδομένα αντί των ονοματισμένων τοποθεσιών αφαιρούν ένα σημαντικό εμπόδιο στην υποστήριξη κινητικότητας σε TCP/IP δίκτυα.

- Το NDN ενεργοποιεί την αποθήκευση εντός δικτύου διότι τα δεδομένα μπορούν να είναι αυτόνομα δίνοντας τη δυνατότητα κλιμακωμένης και εύρωστης διάδοσης δεδομένων.

Κάθε εφαρμογή που υποστηρίζεται από το IP μπορεί να υποστηριχτεί από το NDN το οποίο αφαιρεί τους περιορισμούς της αρχιτεκτονικής TCP/IP χωρίς να εισάγει νέους.

Το NDN δεν εγγυάται ότι τα πακέτα ενδιαφέροντος ενός καταναλωτή θα αφιχθούν στον παραγωγό με την ίδια σειρά που έχουν εκφρασθεί. Επαφίεται στους κατασκευαστές λογισμικού να το σχεδιάσουν έτσι ώστε να διαχειρίζεται το ίδιο τα πακέτα εκτός σειράς. Θα μπορούσε για παράδειγμα ο κατασκευαστής να αναπτύξει ένα μηχανισμό σταμάτα και περίμενε. Όμως αυτό θα περιορίσει το ρυθμό μεταφοράς δεδομένων οπότε σε περίπτωση π.χ. σχεδίασης εφαρμογής αναπαραγωγής ζωντανού video, ο κατασκευαστής δε χρειάζεται να κάνει κάτι.

Επιδιωκόμενο αποτέλεσμα [18]

Ο σχεδιασμός της αρχιτεκτονικής του NDN βασίζεται στα συμπεράσματα από τις επιτυχίες του σημερινού διαδικτύου. Όπως φαίνεται στο **Σχήμα 1**, η αρχιτεκτονική NDN διατηρεί το ίδιο σχήμα κλεψύδρας με την αρχιτεκτονική IP και το κομβικό σημείο να είναι το κεντρικό στοιχείο αυτής της αρχιτεκτονικής. Ωστόσο, η ελάχιστη λειτουργικότητα του κομβικού σημείου του NDN, όπως περιγράφεται στην επισκόπηση της αρχιτεκτονικής, είναι ουσιαστικά διαφορετική από την IP. Η ελάχιστη λειτουργικότητα του NDN περιλαμβάνει υποστήριξη για την παράδοση δεδομένων με γνώμονα τον καταναλωτή, ενσωματωμένη ασφάλεια δεδομένων και χρήση μνήμης εντός δικτύου. Η παροχή δεδομένων με γνώμονα τον καταναλωτή πραγματοποιείται μέσω της ρύθμισης της κατάστασης προώθησης πακέτων. Μαζί με τη μνήμη δικτύου, αυτή η κατάσταση προώθησης παρέχει υποστήριξη για την κλιμάκωση της διάδοσης των δεδομένων (παράδοση σε πολλαπλούς αποδεκτών και διανομή περιεχομένου), εξισορρόπηση ροών δεδομένων για έλεγχο συμφόρησης, ανάκτηση δεδομένων μέσω πολλαπλών διαδρομών και διευκόλυνση κινητών επικοινωνιών και επικοινωνιών με ελεγχόμενο χρόνο καθυστέρησης.

Σύμφωνα με την ομάδα ανάπτυξης αναμένονται τα ακόλουθα μεγάλα παραδοτέα μέχρι το τέλος αυτού του έργου.

- Μια προδιαγραφή των τυποποιημένων μορφών για τους δύο τύπους πακέτων, Ενδιαφέρον και Δεδομένα, στην παράδοση δεδομένων NDN. Αναμένεται ότι αυτή η προδιαγραφή θα διαδραματίσει ρόλο ισοδύναμο με εκείνον του RFC791 (προδιαγραφή πρωτοκόλλου Internet) για δίκτυα NDN. Η πρόκληση για την κάλυψη αυτής της προδιαγραφής δεν είναι η μορφή, αλλά η επαλήθευση και επικύρωση ακριβώς των λειτουργιών που πρέπει να υποστηρίζονται από το κομβικό σημείο.

- Μια λειτουργική έκδοση κάθε μιας από τις απαραίτητες μονάδες υποστήριξης σε ένα λειτουργικό δίκτυο NDN. Οι τρέχουσες προσδιορισμένες μονάδες περιλαμβάνουν βιβλιοθήκες για συμβάσεις ονομασίας που βρίσκονται πάνω από το επίπεδο NDN, πρωτόκολλα δρομολόγησης και μονάδα στρατηγικής προώθησης που βρίσκονται στο κομβικό επίπεδο του NDN, διαχείριση εμπιστοσύνης και εύχρηστη, αποτελεσματική κρυπτογραφία για την ασφάλεια των δεδομένων.

  Υπάρχει μια αναλογία μεταξύ της παραπάνω λίστας και της IP με τα υποστηριζόμενα συστατικά της. Παρόλο που το σύστημα κατανομής διεύθυνσης IP, τα πρωτόκολλα δρομολόγησης και το DNS δεν αποτελούν μέρος του IP, είναι απαραίτητα υποστηρικτικά στοιχεία για την δημιουργία ενός λειτουργικού δικτύου IP. Το γεγονός ότι το DNS προστέθηκε μετά την αρχική ανάπτυξη IP υπογραμμίζει περαιτέρω τη σημασία της αναγνώρισης στοιχείων που λείπουν από την πραγματική ανάπτυξη.

- Ένα σύνολο εφαρμογών, συμπεριλαμβανομένων αλλά όχι περιορισμένων σε αυτές που έχουν εντοπιστεί, οι οποίες λειτουργούν μέσω δικτύου NDN. Αυτές οι εφαρμογές θα περιλαμβάνουν τόσο νέες που έχουν σχεδιαστεί ειδικά για να τρέχουν πάνω από το NDN, όσο και παραδοσιακές που έχουν αναπτυχθεί στο σημερινό Internet.

Βασικές αρχές της σχεδίασης του NDN [20]

[1] Ομοιογένεια: Το NDN πρέπει να είναι ένα κοινό πρωτόκολλο δικτύου για όλες τις εφαρμογές και τα περιβάλλοντα δικτύου. Οι εφαρμογές και τα περιβάλλοντα δικτύου που υποστηρίζει το NDN, μεταξύ άλλων, περιλαμβάνουν:

- Την επικοινωνία βασισμένη σε σύγχρονες υποδομές (Web, YouTube, διασκέψεις πραγματικού χρόνου κ.λπ.).

- Εξειδικευμένες περιπτώσεις με ή χωρίς υποδομή επικοινωνίας (εφαρμογές IoT, δίκτυα ασύρματων δικτύων, δικτύωση μεταξύ οχημάτων, δικτύωση μεταξύ οχημάτων και υποδομών κ.λπ.)

- Επικοινωνία τύπου DTN, επικοινωνία μέσω διακοπτόμενων και διαταραγμένων συνδέσεων (περιβάλλοντα πρώτης απόκρισης), εφαρμογή με χρήση συνδέσμων μίας κατεύθυνσης (π.χ. δορυφόρος)

Επομένως, το πρωτόκολλο NDN και η μορφή πακέτων NDN θα πρέπει να υποστηρίζουν ευρύ φάσμα εφαρμογών, από περιορισμένα περιβάλλοντα (IoT) έως μεγάλες εφαρμογές επιστήμης δεδομένων:

- Η μορφή πακέτου NDN πρέπει να είναι ευέλικτη και επεκτάσιμη.

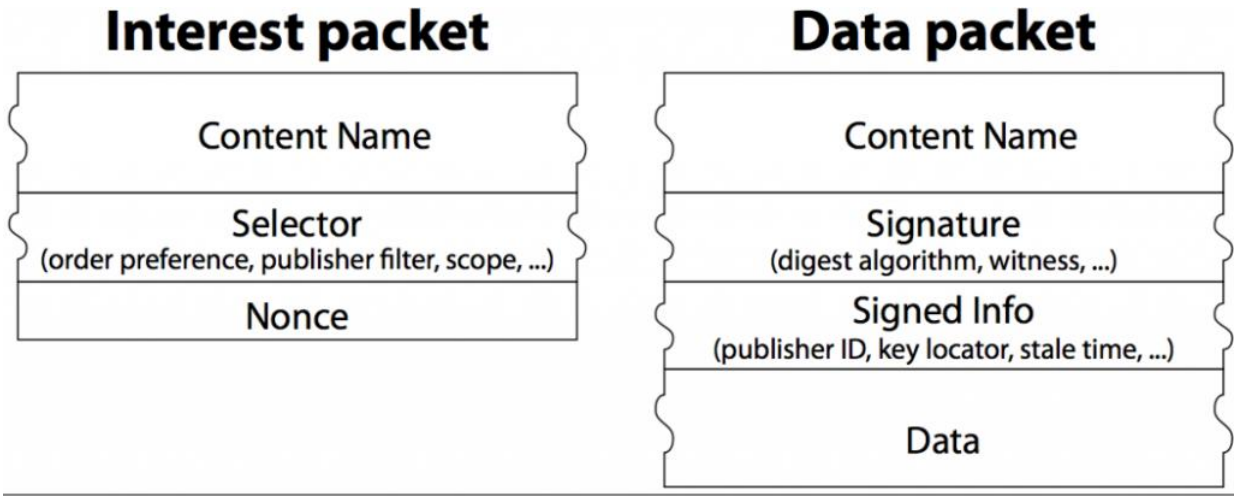
- Το πρωτόκολλο NDN και η μορφή πακέτου θα πρέπει να υποστηρίζουν την εξέλιξη του πρωτοκόλλου χωρίς ημέρες σημαίας: δεν πρέπει να υπάρχουν σταθερά μέρη ή πεδία σταθερού μήκους στην κεφαλίδα.

- Οι λειτουργίες δικτύου στον πυρήνα του πρωτοκόλλου δεν θα πρέπει να εξαρτώνται από συγχρονισμό ρολογιού.

[2] Κεντρικοποίηση και Αμεταβλητότητα Δεδομένων: Το NDN θα πρέπει να αντλεί μοναδικά ονόματα και αμετάβλητα "πακέτα δεδομένων" που ζητούνται χρησιμοποιώντας "πακέτα ενδιαφέροντος".

- Το πρωτόκολλο NDN και η μορφή πακέτου θα πρέπει να περιλαμβάνουν μόνο στοιχεία που σχετίζονται άμεσα με τα δεδομένα, δηλ. απαιτούνται γενικά, χρειάζονται και έχουν νόημα σε όλα τα περιβάλλοντα επικοινωνίας. Άλλα στοιχεία που απαιτούνται σε συγκεκριμένα περιβάλλοντα (π.χ. στην υποδομή του σημερινού διαδικτύου) θα πρέπει να βρίσκονται στα επίπεδα προσαρμογής δικτύου.

- Η αμεταβλητότητα του πακέτου δεδομένων επιτρέπει το συντονισμό σε κατανεμημένο σύστημα που μπορεί να μην είναι πάντα συνδεδεμένο. Παρόλο που τα πακέτα δεδομένων είναι αμετάβλητα, οι εφαρμογές μπορούν να κάνουν αλλαγές στο περιεχόμενο που μεταδίδεται με τη δημιουργία νέων εκδόσεων αμετάβλητων πακέτων δεδομένων. [21]



Σχήμα 2 – Πακέτα NDN

[3] Απευθείας Εξασφάλιση δεδομένων: Η ασφάλεια πρέπει να είναι βασική ιδιότητα των πακέτων δεδομένων, παραμένοντας η ίδια ανεξάρτητα από το εάν τα πακέτα είναι σε κίνηση ή σε ηρεμία.

- Τα άμεσα εξασφαλισμένα και έχοντας μοναδική ονομασία δεδομένα καταργούν την ανάγκη για απευθείας κανάλια μεταξύ των επικοινωνούντων άκρων και καθιστούν δυνατή την ασύγχρονη παραγωγή και κατανάλωση ονοματισμένων και ασφαλών δεδομένων, π.χ. χρησιμοποιώντας ενδοδικτυακές προσωρινές αποθήκες (caches) και διαχειριζόμενους αποθηκευτικούς χώρους.

- Οι καταναλωτές θα πρέπει να είναι σε θέση να επικυρώνουν μεμονωμένα πακέτα δεδομένων. Στην ιδανική περίπτωση, κάθε πακέτο πρέπει να μπορεί να εξακριβωθεί από μόνο του. Ως βελτιστοποίηση μηχανικής, τα πακέτα μπορούν να γίνουν επαληθεύσιμα στο πλαίσιο άλλων, υπό την προϋπόθεση ότι το πλαίσιο μπορεί να συναχθεί από το ίδιο το πακέτο δεδομένων (το όνομα ή η πληροφορία του στο πεδίο υπογραφής).

[4] Ιεραρχική Ονοματοδοσία: Τα πακέτα πρέπει να φέρουν ιεραρχικά ονόματα για να επιτρέπουν την αποπολυπλεξία τους.

- Η ιεραρχία των ονομάτων παρέχει το πλαίσιο για την εφαρμογή και επιβολή διαφόρων μοντέλων ασφαλείας, δηλ. να δοθούν δομημένοι περιορισμοί στα οποία τα κλειδιά μπορούν να υπογράψουν συγκεκριμένα δεδομένα.

- Τα ιεραρχικά ονόματα επιτρέπουν «επίπεδα» μοντέλα ονομασίας, εάν είναι επιθυμητά ή χρειάζονται από εφαρμογές.

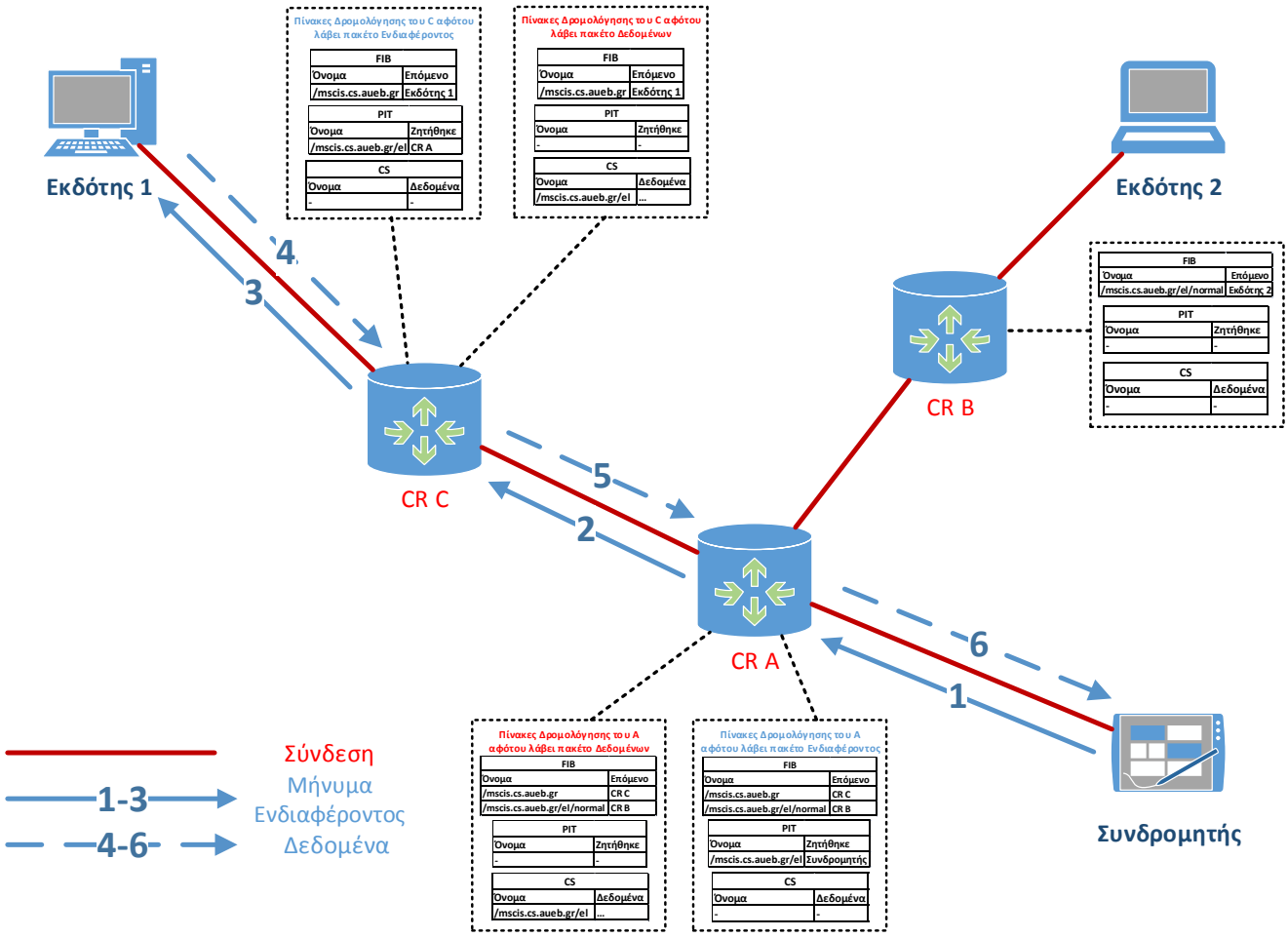
[5] Ανακάλυψη Ονόματος εντός Δικτύου: Τα «ενδιαφέροντα» θα πρέπει να μπορούν να χρησιμοποιούν ελλιπή ονόματα για την ανάκτηση πακέτων δεδομένων. Ένας καταναλωτής μπορεί να μην γνωρίζει το πλήρες όνομα της πληροφορίας που ζητά σε επίπεδο δικτύου, καθώς ορισμένα τμήματα του ονόματος δεν μπορούν να βρεθούν τυχαία, να υπολογιστούν ή να συναχθούν εκ των προτέρων.

Μόλις ληφθούν τα αρχικά δεδομένα, οι συμβάσεις ονομασίας μπορούν να βοηθήσουν στον προσδιορισμό των πλήρων ονομάτων άλλων σχετικών δεδομένων.

- Η πλειοψηφία των εκδηλώσεων «ενδιαφέροντος» θα φέρει πλήρη ονόματα
- Η ανακάλυψη ονόματος εντός του δικτύου αναμένεται να χρησιμοποιείται για την αρχικοποίηση κατά την εκκίνηση μιας επικοινωνίας

[6] Εξισορρόπηση ροής από κόμβο σε κόμβο: Σε κάθε ζεύξη, ένα πακέτο ενδιαφέροντος δεν πρέπει να επιφέρει περισσότερα από ένα πακέτα δεδομένων. Η εξισορρόπηση ροής από κόμβο σε κόμβο (hop-by-hop) επιτρέπει σε κάθε κόμβο να ελέγχει το φορτίο με τους συνδέσμους του. Με την απόφαση αποστολής ενός ενδιαφέροντος μέσω συνδέσμου, ο δρομολογητής δεσμεύει κάποιο εύρος ζώνης για τα δεδομένα που επιστρέφονται. Με τον περιορισμό του αριθμού των ενδιαφερόντων που στέλνονται, κάθε δρομολογητής και κόμβος πελάτης στο δίκτυο ελέγχει πόσα δεδομένα θα λάβει.

3.2 Αρχιτεκτονική NDN [1]



Σχήμα 3 – Η Αρχιτεκτονική του NDN

Στο δίκτυο NDN, ένα επίπεδο **στρατηγικής** μεσολαβεί ανάμεσα στο επίπεδο ονοματοδοσίας δεδομένων και τις υποκείμενες τεχνολογίες δικτύου με σκοπό τη βελτιστοποίηση της χρήσης των πόρων, π.χ. για την επιλογή μιας σύνδεσης σε έναν κόμβο με πολλαπλές συνδέσεις, ενώ ένα επίπεδο **ασφαλείας** εφαρμόζει λειτουργίες ασφαλείας απευθείας σε ονομασμένα δεδομένα. Μία κρίσιμη πτυχή του NDN είναι ότι τα ονόματα είναι ιεραρχικά, επιτρέποντας έτσι την ομαδοποίηση της ανάκτησης των ονομάτων και των πληροφοριών δρομολόγησης δεδομένων, σε παρόμοια ονόματα, κάτι που θεωρείται κρίσιμο για την κλιμάκωση της αρχιτεκτονικής.

1) **Ονομασία:** Τα ονόματα στο NDN είναι **ιεραρχικά** και μπορεί να είναι παρόμοια με τις διευθύνσεις URL, για παράδειγμα, ένα όνομα NDN μπορεί να είναι **/mscis.cs.aueb.gr/el/normal/home**. Ωστόσο, τα ονόματα NDN δεν είναι απαραίτητα διευθύνσεις URL: το πρώτο μέρος τους δεν είναι όνομα DNS

ή διεύθυνση IP και δεν χρειάζεται να είναι αναγνώσιμα από άνθρωπο. Αντίθετα, στο NDN, κάθε συστατικό όνομα μπορεί να είναι οτιδήποτε, συμπεριλαμβανομένης μιας συμβολοσειράς που διαβάζεται από τον άνθρωπο ή μιας τιμής κατακερματισμού.

Στο NDN, ένα αίτημα για ένα όνομα θεωρείται ότι ταιριάζει με κάθε πληροφορία της οποίας το όνομα έχει το επιθυμητό όνομα ως πρόθεμα, για παράδειγμα, το **/mscis.cs.aueb.gr/el/normal/home** μπορεί να αντιστοιχιστεί με ένα αντικείμενο πληροφοριών που ονομάζεται **/mscis.cs.aueb.gr/el/normal/home/_v1/_s1**, που θα μπορούσε να σημαίνει το πρώτο τμήμα της πρώτης έκδοσης των ζητούμενων δεδομένων. Μετά την παραλαβή αυτού του αντικειμένου πληροφοριών, ο συνδρομητής θα μπορούσε να ζητήσει το επόμενο τμήμα δεδομένων είτε απευθείας ζητώντας το **/mscis.cs.aueb.gr/el/normal/home/_v1/_s2**, είτε το επόμενο τμήμα αυτής της έκδοσης. Εναλλακτικά, ο συνδρομητής μπορεί να ζητήσει την επόμενη έκδοση ζητώντας το πρώτο τμήμα του **/mscis.cs.aueb.gr/el/normal/home/_v1**.

Ενώ ο τρόπος με τον οποίο τα αντικείμενα πληροφοριών είναι τεμαχισμένα αναμένεται να είναι γνωστός από την εφαρμογή του συνδρομητή, ο κανόνας αντιστοίχισης προθέματος επιτρέπει σε μια εφαρμογή να ανακαλύψει τι είναι διαθέσιμο. Επιπλέον, επιτρέπει στον συνδρομητή να ζητήσει δεδομένα που δεν έχουν παραχθεί ακόμα: ένας εκδότης μπορεί να διαφημίσει ότι μπορεί να ικανοποιήσει αιτήματα για ένα συγκεκριμένο πρόθεμα και στη συνέχεια να επιστρέψει αντικείμενα πληροφοριών με πλήρη ονόματα NDN. Αυτό μπορεί να χρησιμοποιηθεί για την υλοποίηση διαφόρων εφαρμογών όπου τα αντικείμενα πληροφοριών παράγονται δυναμικά, επομένως τα πλήρη ονόματα τους δεν μπορούν να είναι γνωστά εκ των προτέρων, όπως π.χ. η φωνητική συνδιάσκεψη [22].

2) **Επιλογή ονόματος και δεδομένων:** Οι συνδρομητές NDN εκδίδουν μηνύματα Ενδιαφέροντος για να ζητήσουν αντικείμενα πληροφοριών που φτάνουν με τη μορφή μηνυμάτων Δεδομένων, με τους δύο τύπους μηνυμάτων να φέρουν το όνομα του αντικειμένου πληροφοριών που ζητήθηκε / μεταφέρθηκε. Όπως δείχνει το **Σχήμα 3**, όλα τα μηνύματα μεταδίδονται από κόμβο σε κόμβο μέσω των Δρομολογητών Περιεχομένου (CRs).

   Κάθε CR διατηρεί τρεις δομές δεδομένων:

   - τη Βάση Προώθησης Πληροφοριών (FIB),
   - τον Πίνακα Εκκρεμών Ενδιαφερόντων (PIT) και
   - την Αποθήκη Δεδομένων (CS).

Αναλυτικά:

- Η FIB ταιριάζει ονόματα πληροφοριών στις διεπαφές εξόδου που πρέπει να χρησιμοποιηθούν για την προώθηση των μηνυμάτων Ενδιαφέροντος προς τις κατάλληλες πηγές δεδομένων.
- Ο PIT παρακολουθεί τις εισερχόμενες διεπαφές από τις οποίες έφτασαν τα εκκρεμή μηνύματα Ενδιαφέροντος, δηλαδή τα μηνύματα Ενδιαφέροντος για τα οποία αναμένονται τα αντίστοιχα μηνύματα Δεδομένων.
- Τέλος, η CS χρησιμεύει ως τοπική κρυφή μνήμη για αντικείμενα πληροφοριών που έχουν περάσει από τον CR.

Οι δρομολογητές NDN δεν χρειάζονται απαραίτητα τεράστιο αποθηκευτικό χώρο αφού η CS παρέχει ευκαιριακή κρυφή μνήμη μειώνοντας έτσι το χρόνο λήψης δεδομένων και την ανάγκη για μεγάλο εύρος ζώνης μεταφοράς. Πόσο μεγάλη αποθήκευση θα χρησιμοποιηθεί σε έναν δρομολογητή NDN είναι θέμα σχεδίασης.

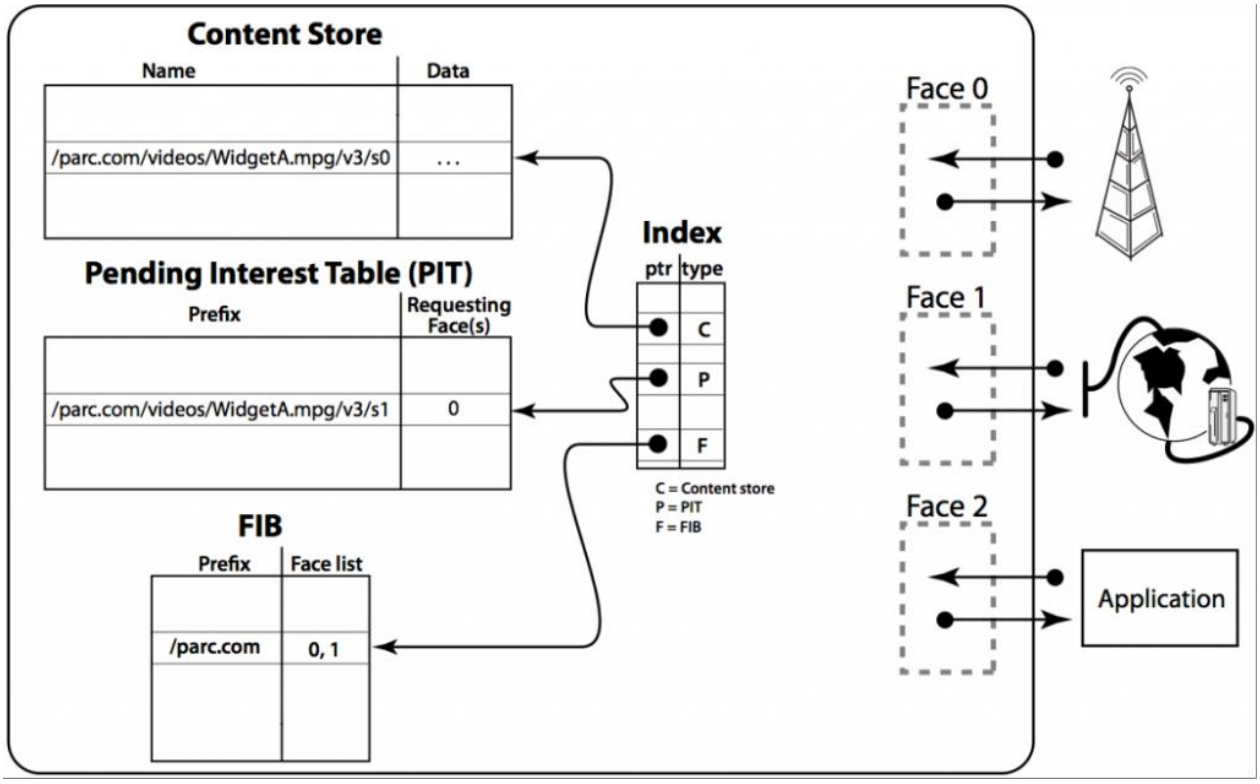
Ένα δίκτυο NDN μπορεί να χρησιμοποιήσει υπάρχοντα πρωτόκολλα δρομολόγησης διαδίδοντας προθέματα ονομάτων παρά προθέματα IP. Η ανάπτυξη των παραδοσιακών πρωτοκόλλων γίνεται μέσω της Ανταλλαγής πακέτων Ενδιαφέροντος.

Όταν το όνομα δεδομένων ενός παραγωγού είναι ανέφικτο να ανακοινωθεί παγκόσμια υπάρχει η λύση της επισύναψης στο πακέτο Ενδιαφέροντος του ονόματος του παρόχου που φιλοξενεί τα δεδομένα. Σε αυτήν την περίπτωση το όνομα του παρόχου καλείται Προωθητικό Στοιχείο. Όταν ένας δρομολογητής δεν βρίσκει ένα πρόθεμα που να ταιριάζει με το όνομα σε ένα πακέτο Ενδιαφέροντος τότε προωθεί το Ενδιαφέρον σύμφωνα με το στοιχείο προώθησης που επισυνάπτεται σε αυτό.

Όταν ένα πακέτο Ενδιαφέροντος φτάσει, ο CR εξάγει το όνομα της πληροφορίας και ψάχνει για ένα αντικείμενο πληροφοριών στην CS, του οποίου το όνομα ταιριάζει με το απαιτούμενο πρόθεμα. Εάν εντοπιστεί κάτι, αποστέλλεται αμέσως μέσω της εισερχόμενης διεπαφής σε ένα μήνυμα Δεδομένων και το Ενδιαφέρον απορρίπτεται. Διαφορετικά, ο δρομολογητής πραγματοποιεί μια μεγαλύτερη προθεματική αντιστοίχιση στη FIB του, προκειμένου να αποφασίσει προς ποια κατεύθυνση θα πρέπει να προωθηθεί αυτό το ενδιαφέρον. Εάν εντοπιστεί μια καταχώρηση στη FIB, ο δρομολογητής καταγράφει την εισερχόμενη διεπαφή στον PIT και προωθεί το μήνυμα στον CR που υποδεικνύει η FIB. Στο **Σχήμα 3**, ο συνδρομητής στέλνει ένα ενδιαφέρον για το όνομα **/mscis.cs.aueb.gr/el** (βέλη 1-3).

Αν ο PIT περιέχει ήδη μια καταχώρηση για το ακριβές όνομα, πράγμα που σημαίνει ότι αυτό το ακριβές πληροφοριακό αντικείμενο είχε ήδη ζητηθεί, ο δρομολογητής προσθέτει την εισερχόμενη διεπαφή σε αυτή την εγγραφή του PIT και απορρίπτει το Ενδιαφέρον, δημιουργώντας ένα δέντρο πολυεκπομπής (multicast) για αυτό το αντικείμενο πληροφοριών.

Όταν ένα αντικείμενο πληροφοριών, που ταιριάζει με το ζητούμενο όνομα, βρίσκεται ήδη σε έναν κόμβο εκδότη ή μία CS, τότε το μήνυμα Ενδιαφέροντος απορρίπτεται και η πληροφορία επιστρέφεται σε ένα μήνυμα Δεδομένων. Αυτό το μήνυμα μεταδίδεται πίσω στους συνδρομητές από κόμβο σε κόμβο (hop-by-hop), με βάση την κατάσταση που διατηρείται στους PITs. Συγκεκριμένα, όταν ένας CR λαμβάνει ένα μήνυμα Δεδομένων, αποθηκεύει πρώτα το αντίστοιχο αντικείμενο πληροφοριών στη δική του CS και στη συνέχεια εκτελεί μια μεγαλύτερη αντιστοίχιση προθέματος στον δικό του PIT ώστε να εντοπίσει μια εγγραφή που να ταιριάζει με το πακέτο Δεδομένων. Να σημειωθεί πως η μακρύτερη αντιστοίχιση προθέματος είναι απαραίτητη, δεδομένου ότι το ζητούμενο όνομα μπορεί να είναι ένα πρόθεμα της επιστροφής. Εάν μια εγγραφή του PIT έχει πολλές διεπαφές, τότε το μήνυμα Δεδομένων αντιγράφεται, επιτυγχάνοντας έτσι πολλαπλή παράδοση (multicast). Τέλος, ο CR προωθεί το πακέτο μηνυμάτων Δεδομένων σε αυτές τις διεπαφές και διαγράφει την εγγραφή από τον PIT (βέλη 4-6). Σε περίπτωση που δεν υπάρχουν καταχωρήσεις που να ταιριάζουν στον PIT, ο δρομολογητής απορρίπτει το πακέτο Δεδομένων ως διπλότυπο.



Σχήμα 4 – Κόμβος NDN

Στο NDN η εύρεση ονόματος και η δρομολόγηση δεδομένων είναι συζευγμένες, δεδομένου ότι τα μηνύματα Δεδομένων ακολουθούν τους δείκτες που έχουν απομείνει στους PITs με μηνύματα Ενδιαφέροντος, επομένως η δρομολόγηση είναι εξ ορισμού συμμετρική. Για να συμπληρωθούν οι FIBs, το NDN μπορεί να χρησιμοποιήσει πρωτόκολλα κατανεμημένης δρομολόγησης όπως π.χ το OSPF [14], στο οποίο οι CR διαφημίζουν προθέματα ονομάτων αντί για περιοχές διευθύνσεων IP, π.χ. ένας δρομολογητής θα μπορούσε να διαφημίσει **/mscis.cs.aueb.gr** για να ενημερώσει το δίκτυο ότι μπορεί να παρέχει αντικείμενα πληροφορίας των οποίων το πρόθεμα είναι **/mscis.cs.aueb.gr**. Ένας CR μπορεί να έχει για ένα πρόθεμα πολλαπλές διασυνδέσεις στη δική του FIB, για παράδειγμα, εάν έχει συνδέσεις σε πολλαπλά δίκτυα (multi-homed) ή αν γνωρίζει πολλούς διακομιστές CDN που φιλοξενούν τις πληροφορίες. Σε αυτή την περίπτωση το επίπεδο στρατηγικής μπορεί να επιλέξει να στείλει το Ενδιαφέρον είτε σε όλες αυτές τις διασυνδέσεις (εάν έχουν επιστραφεί πολλαπλά μηνύματα Δεδομένων, όλα εκτός από τα πρώτα απορρίπτονται αυτόματα) ή μόνο στη διεπαφή που έχει επιδείξει τις καλύτερες επιδόσεις μέχρι στιγμής.

3) **Κρυφή μνήμη (Caching):** Το NDN υποστηρίζει εγγενώς την κρυφή μνήμη, δεδομένου ότι κάθε CR συμβουλεύει αρχικά τη δική του CS κάθε φορά που λαμβάνει ένα μήνυμα Ενδιαφέροντος και αποθηκεύει στην κρυφή μνήμη όλα τα αντικείμενα πληροφοριών που μεταφέρονται με μηνύματα Δεδομένων. Η CS μπορεί να χρησιμοποιήσει τον αλγόριθμο του λιγότερο προσφάτως χρησιμοποιημένου αντικειμένου (LRU) ή οποιαδήποτε άλλη πολιτική αντικατάστασης, αλλά, ρεαλιστικά, δεν μπορεί να χρησιμοποιηθεί για μακροχρόνια αποθήκευση αν αποθηκεύσει μόνο ό, τι βλέπει [23], [24], επομένως είναι ως επί το πλείστον χρήσιμο για ανάκτηση από απώλειες πακέτων και για το χειρισμό "εκρήξεων" ζήτησης, όπου πολλοί χρήστες ζητούν διαδοχικά τα ίδια δεδομένα σε μικρό χρονικό διάστημα. Η προσωρινή αποθήκευση εκτός διαδρομής υποστηρίζεται παραδίδοντας ένα Ενδιαφέρον σε κάθε πηγή δεδομένων που μπορεί να φιλοξενεί το αντικείμενο πληροφοριών που ζητήθηκε, π.χ. το επίπεδο στρατηγικής μπορεί να κατευθύνει το Ενδιαφέρον σε ένα διακομιστή CDN και όχι στον αρχικό εκδότη του. Αυτό δεν είναι διαφανές για το NDN, ωστόσο, καθώς απαιτεί τη συγκέντρωση των FIBs με δείκτες σε τέτοια αντίγραφα, τα οποία με τη σειρά τους χρειάζονται τα προθέματα ονομάτων τους να διαφημίζονται από το διακομιστή CDN μέσω του χρησιμοποιούμενου πρωτοκόλλου δρομολόγησης.

4) **Κινητικότητα:** Όταν ένας συνδρομητής στο δίκτυο NDN κινείται, μπορεί απλά να εκδίδει νέα μηνύματα Ενδιαφέροντος από την τρέχουσα τοποθεσία για τα αντικείμενα πληροφοριών που δεν έχει λάβει ακόμη. Αυτά τα αιτήματα θα κατασταλούν από τον PIT του πρώτου CR που είναι κοινός

και στις δύο διαδρομές παράδοσης (πριν και μετά τη μεταφορά). Τελικά τα αντίστοιχα αντικείμενα πληροφοριών θα παραδοθούν στην αρχική τοποθεσία του συνδρομητή.

Από την άλλη πλευρά όταν ένας εκδότης κινείται, οι FIB που τον επισημαίνουν πρέπει να ενημερωθούν, πράγμα που απαιτεί να διαφημιστούν και πάλι τα προθέματα ονομάτων για τις πληροφορίες που φιλοξενούνται, μέσω του πρωτοκόλλου δρομολόγησης. Δεδομένου ότι αυτό σημαίνει πολύ υψηλό κόστος σε λύσεις υψηλής κινητικότητας, το NDN χρησιμοποιεί το πρωτόκολλο "Ακούστε Πρώτα Μεταδώστε Αργότερα" (LFBL) [25] για να εφαρμόσει κινητικότητα σε ευκαιριακά δίκτυα αυτού του σκοπού (ad hoc). Στο πρωτόκολλο LFBL, τα μηνύματα Ενδιαφέροντος πλημμυρίζουν το δίκτυο. Όταν μια πιθανή πηγή για τις ζητούμενες πληροφορίες λάβει ένα ενδιαφέρον, τότε ακούει το ασύρματο κανάλι για να ανακαλύψει εάν υπάρχει άλλος κόμβος στον οποίο έχει ήδη αποσταλεί ένα αντίστοιχο μήνυμα Δεδομένων. Εάν όχι, στέλνει το μήνυμα Δεδομένων προς τον συνδρομητή.

5) **Ασφάλεια:** Το NDN υποστηρίζει τη συσχέτιση ονομάτων ιεραρχικής πληροφορίας, σε μορφή αναγνώσιμη από τον άνθρωπο, με τα αντίστοιχα πληροφοριακά αντικείμενα κατά τρόπο επαληθεύσιμο [26]. Κάθε μήνυμα Δεδομένων περιέχει μια υπογραφή πάνω στο όνομα και τις πληροφορίες που περιλαμβάνονται στο μήνυμα καθώς και πληροφορίες σχετικά με το κλειδί που χρησιμοποιείται για την παραγωγή της υπογραφής, π.χ. το δημόσιο κλειδί του υπογράφοντος, ένα πιστοποιητικό για το δημόσιο κλειδί ή έναν δείκτη σε αυτά. Αυτό επιτρέπει σε οποιονδήποτε κόμβο, συμπεριλαμβανομένων των CRs, να επαληθεύσει τη σύνδεση μεταξύ του (ενδεχομένως αναγνωρίσιμου από τον άνθρωπο) ονόματος του πακέτου και των συνοδευτικών πληροφοριών. Για να επιβεβαιωθεί ότι οι πληροφορίες προέρχονται από μια εξουσιοδοτημένη πηγή, ο συνδρομητής πρέπει να εμπιστευτεί τον κάτοχο του δημόσιου κλειδιού που χρησιμοποιείται για την υπογραφή. Η ιεραρχική δομή των ονομάτων απλοποιεί τη δημιουργία σχέσεων εμπιστοσύνης, για παράδειγμα το **/mscis.cs.aueb.gr/el/normal** μπορεί να υπογραφεί από τον κάτοχο του τομέα **/mscis.cs.aueb.gr/el**, του οποίου το κλειδί μπορεί να πιστοποιηθεί από τον κάτοχο του τομέα **/mscis.cs.aueb.gr**. Το NDN υποστηρίζει επίσης ανώνυμη λειτουργία χρησιμοποιώντας μια προσέγγιση τύπου Tor όπως το ANDaNA [27].

4 Εφαρμογή Ελέγχου Πρόσβασης στο NDN

4.1 Γενικός Σχεδιασμός Συστήματος

Στη συνέχεια αναλύεται η υιοθέτηση μηχανισμού Ανάθεσης Ελέγχου Πρόσβασης για τα δίκτυα με αρχιτεκτονική NDN/CCN ICN βασιζόμενη σε ανάλογη εφαρμογή του ως υπηρεσία στο Cloud [28]

Οντότητες:

- **Εκδότης Δεδομένων** (Publisher)
- **Συνδρομητής** (Subscriber)
- **Δρομολογητής Περιεχομένου** (Content Router)
- **Πάροχος Ελέγχου Πρόσβασης** (Access Control Provider)

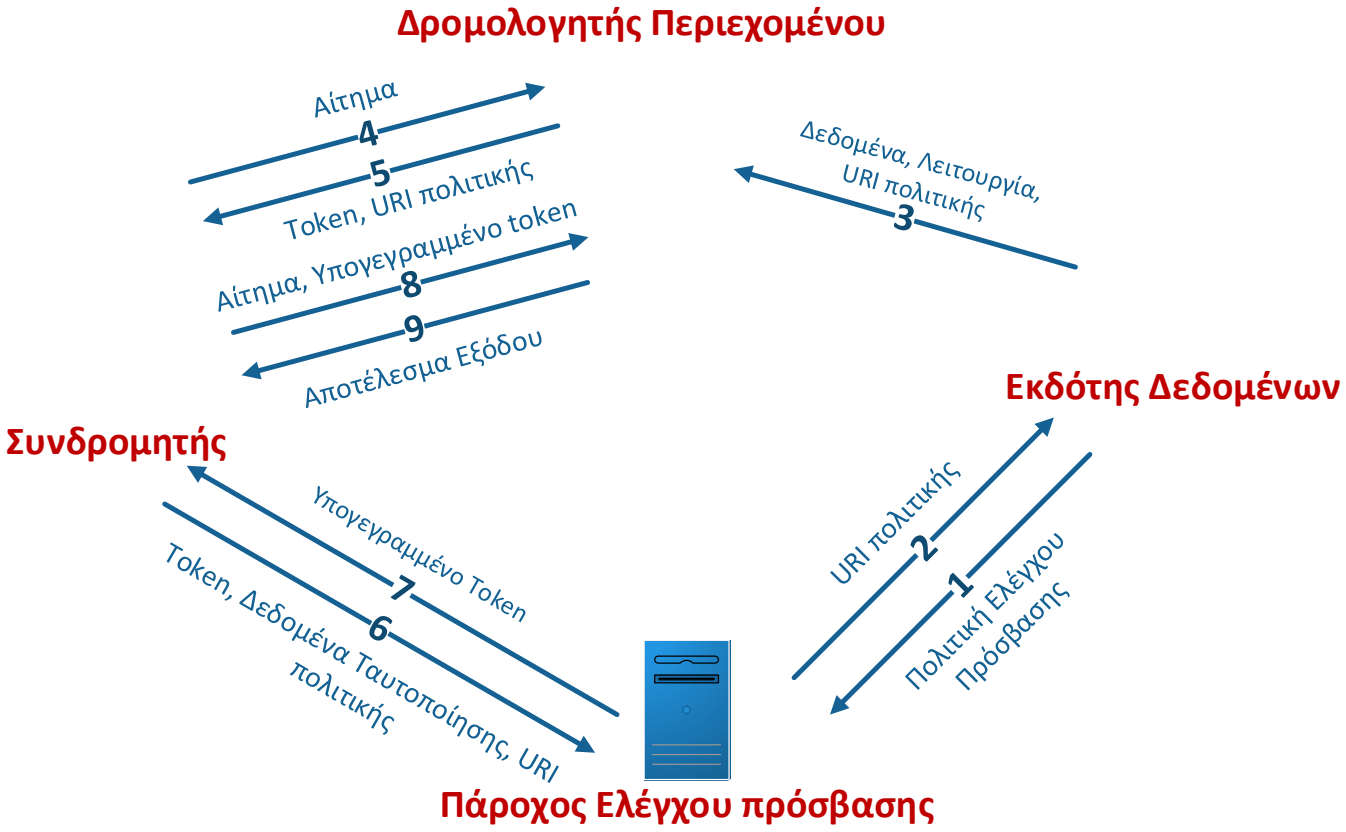
Στόχοι:

- Ο **Εκδότης Δεδομένων** να μπορεί να αποθηκεύει τα δεδομένα που θέλει στο **Δίκτυο NDN**
- Να επιτρέπεται σε **Εξουσιοδοτημένους Συνδρομητές** να εκτελούν λειτουργίες πάνω στα δεδομένα που παρέχει ο **Εκδότης Δεδομένων**.
- Κάθε λειτουργία να είναι προστατευμένη από μια **Πολιτική Ελέγχου Πρόσβασης**
- Κάθε **Πολιτική Ελέγχου Πρόσβασης** να αποθηκεύεται σε κάποιον **Πάροχο Ελέγχου Πρόσβασης** και αντιστοιχίζει την ταυτότητα ενός **Συνδρομητή** με μια τιμή αληθείας (αληθές/ψευδές).
- Ο **Συνδρομητής** που παρέχει δεδομένα ταυτότητας στα οποία η αντίστοιχη **Πολιτική Ελέγχου Πρόσβασης** επιστρέφει τιμή **αληθή** θα θεωρείται **Εξουσιοδοτημένος**.

Σχέσεις Εμπιστοσύνης:

- Οι **Εκδότες Δεδομένων** εμπιστεύονται τους **Παρόχους Ελέγχου Πρόσβασης** ώστε να εξουσιοδοτούν πρόσβαση σε **Συνδρομητές**
- Οι **Εκδότες Δεδομένων** και οι **Συνδρομητές** εμπιστεύονται ότι οι **Δρομολογητές Περιεχομένου** σέβονται τις αποφάσεις των **Παρόχων Ελέγχου Πρόσβασης**.

Σχηματική Αναπαράσταση Τυπικής Συναλλαγής:



Σχήμα 5 – Αναπαράσταση Τυπικής Συναλλαγής

- **Βήμα 1:** Ο **Εκδότης Δεδομένων** αποθηκεύει μια **Πολιτική Ελέγχου Πρόσβασης** στον **Πάροχο Ελέγχου Πρόσβασης**
- **Βήμα 2:** Ο **Εκδότης Δεδομένων** λαμβάνει από τον **Πάροχο Ελέγχου Πρόσβασης** ένα **URI** που σηματοδοτεί την αντίστοιχη **Πολιτική Ελέγχου Πρόσβασης**.
- **Βήμα 3:** Ο **Εκδότης Δεδομένων** παράγει την επιθυμητή λειτουργία που μπορεί να εφαρμοσθεί στα δεδομένα και αποθηκεύει το URI της **Πολιτική Ελέγχου Πρόσβασης** που προστατεύει τη λειτουργία.
- **Βήμα 4:** Ο **Συνδρομητής** ζητεί για πρώτη φορά να εκτελέσει μια προστατευόμενη λειτουργία σε κάποια δεδομένα,
- **Βήμα 5:** Ο **Δρομολογητής Περιεχομένου** απαντά αποστέλλοντας το URI της **Πολιτικής Ελέγχου Πρόσβασης** και μία μοναδική ένδειξη/σήμανση (token)

- **Βήμα 6:** Ο **Συνδρομητής** αυθεντικοποιείται σε κάποιον **Πάροχο Ελέγχου Πρόσβασης** παρέχοντας το URI, την ένδειξη (token) που έλαβε στο βήμα 5 καθώς και δεδομένα που προσδιορίζουν την ταυτότητά του ζητώντας εξουσιοδότηση που να ικανοποιεί την **Πολιτική Ελέγχου Πρόσβασης.**
- **Βήμα 7:** Σε περίπτωση που ικανοποιείται η **Πολιτική Ελέγχου Πρόσβασης** τότε ο **Πάροχος Ελέγχου Πρόσβασης** υπογράφει την ένδειξη (token) και την αποστέλλει στον **Συνδρομητή**
- **Βήμα 8:** Ο **Συνδρομητής** επαναλαμβάνει την προσπάθεια εκτέλεσης της προστατευόμενης λειτουργίας (βήμα 4) παρέχοντας επιπλέον στον **Δρομολογητή Περιεχομένου** την υπογεγραμμένη ένδειξη.
- **Βήμα 9:** Ο **Δρομολογητής Περιεχομένου** ελέγχει την εγκυρότητα της υπογεγραμμένης ένδειξης (token) και εάν είναι έγκυρη εκτελεί την επιθυμητή λειτουργία επιστρέφοντας το αποτέλεσμα εξόδου

Επιθυμητές Ιδιότητες:

- **Ασφαλές Σύστημα:** Δεδομένου ότι όλες οι οντότητες που συμμετέχουν σέβονται τις **Σχέσεις Εμπιστοσύνης** δεν θα είναι δυνατόν σε μη εξουσιοδοτημένους χρήστες να είναι εκτελέσουν ενέργειες που προστατεύονται.
- **Διατήρηση Ιδιωτικότητας Συνδρομητή:** Ο **Δρομολογητής Περιεχομένου** πρέπει να λαμβάνει την ελάχιστη πληροφορία σχετικά με την ταυτότητα του συνδρομητή. Ιδανικά θα πρέπει να γνωρίζει μόνο τον **Πάροχο Ελέγχου Πρόσβασης** που εξουσιοδότησε τον συνδρομητή. Επίσης ο **Πάροχος Ελέγχου Πρόσβασης** δεν πρέπει να έχει γνώση της ενέργειας που επιθυμεί να εκτελέσει ένας συνδρομητής ή των δεδομένων στα οποία τελικά έχει πρόσβαση.
- **Εύκολη Μετανάστευση Δεδομένων:** Οι μόνες οντότητες που πρέπει να είναι ενήμερες σχετικά με μια **Πολιτική Ελέγχου Πρόσβασης** και της υλοποίησής της είναι ο **Εκδότης Δεδομένων** και ο **Πάροχος Ελέγχου Πρόσβασης** ενώ **ο Δρομολογητής Περιεχομένου** πρέπει να την αγνοεί παντελώς. Με αυτόν το τρόπο τα δεδομένα μπορούν να φιλοξενούνται σε πολλούς **Εκδότες Δεδομένων και Δρομολογητές Περιεχομένου** χωρίς επιπλέον διαδικασίες παρά μόνο την ύπαρξη αντιγράφου τους.
- **Η Πολιτική δεν αποκαλύπτει πληροφορία για τα Δεδομένα και τις Προστατευμένες Λειτουργίες:** Η **Πολιτική Ελέγχου Πρόσβασης** θα πρέπει να ορίζεται έτσι ώστε να λαμβάνει υπόψη μόνο τα χαρακτηριστικά του συνδρομητή και να είναι αποσυνδεδεμένη από τα δεδομένα και τις προστατευμένες λειτουργίες προς αυτά.
- **Επαναχρησιμοποίηση Πολιτικών Ελέγχου Πρόσβασης:** Μία **Πολιτική Ελέγχου Πρόσβασης** πρέπει να μπορεί να προστατεύει πολλά και διαφορετικά δεδομένα αποθηκευμένα σε πολλαπλούς **Δρομολογητές Περιεχομένου** και επιπρόσθετα να μπορεί να εφαρμοσθεί σε διαφορετικές ενέργειες.

- **Εύκολη τροποποίηση Πολιτικών Ελέγχου Πρόσβασης:** Η μόνη οντότητα που θα εμπλέκεται στη διαδικασία τροποποίησης μιας **Πολιτική Ελέγχου Πρόσβασης** θα πρέπει να είναι ο **Πάροχος Ελέγχου Πρόσβασης** στον οποίο είναι αποθηκευμένη η εν λόγω πολιτική.

4.2 Αναλυτική Περιγραφή της Ανάθεσης Επιβολής Πρόσβασης (ΑΕΠ)

Θεωρούνται δεδομένα τα εξής:

- Ο **Πάροχος Ελέγχου Πρόσβασης** και ο **Δρομολογητής Περιεχομένου** έχουν ένα ζευγάρι δημοσίου-Ιδιωτικού κλειδιού.
- Το δημόσιο κλειδί του **Παρόχου Ελέγχου Πρόσβασης** και του **Δρομολογητής Περιεχομένου** πρέπει να είναι γνωστό στους συνδρομητές και
- Όλα τα μηνύματα ανταλλάσσονται μέσω ασφαλούς σύνδεσης

Διαδικασίες:

- **Δημιουργία Πολιτικής Ελέγχου Πρόσβασης και Αποθήκευση Δεδομένων:** Μέσω της διαδικασίας αυτής ο **Εκδότης Δεδομένων** δημιουργεί και αποθηκεύει μια **Πολιτική Ελέγχου Πρόσβασης** σε έναν **Πάροχο Ελέγχου Πρόσβασης** ο οποίος ως απάντηση παρέχει ένα **URIacp.** Για κάθε προστατευμένη λειτουργία που έχει αναπτυχθεί σε ένα **Πάροχο Δεδομένων**, ο εκδότης των δεδομένων ορίζει το **URIacp** της πολιτικής που την προστατεύει και το δημόσιο κλειδί **PUBacp** του **Παρόχου Ελέγχου Πρόσβασης** στον οποίο είναι αποθηκευμένη η πολιτική**.** Η πληροφορία αυτή διατηρείται σε έναν **Πίνακα Πρόσβασης** του **Δρομολογητή Περιεχομένου** που περιέχει πλειάδες της μορφής:

  [Λειτουργία, URIacp, PUBacp]

  Ένα **URIacp** μπορεί να είναι επαναχρησιμοποιήσιμο, για παράδειγμα μπορεί να προστατεύει πολλαπλές λειτουργίες αποθηκευμένες σε διάφορους **Δρομολογητές Περιεχομένου**. Ο μηχανισμός της δημιουργίας της **Πολιτικής Ελέγχου Πρόσβασης** αφορά τον **Πάροχο Ελέγχου Πρόσβασης** και της ενημέρωσης του **Πίνακα Πρόσβασης** στον **Δρομολογητή Περιεχομένου**.

- **Μη Εξουσιοδοτημένο Αίτημα:** Η διαδικασία λαμβάνει χώρα από έναν **Συνδρομητή** όταν επιχειρεί μια προστατευμένη λειτουργία για πρώτη φορά. Ο **Δρομολογητής Περιεχομένου** που λαμβάνει το αίτημα δημιουργεί ένα μοναδικό χαρακτηριστικό (token) π.χ. με τη χρήση γεννήτρια τυχαίων αριθμών μεγάλου μήκους και το στέλνει στον **Συνδρομητή** μαζί με το αντίστοιχο **URIacp**. Τα μηνύματα που ανταλλάσσονται στη διαδικασία αυτή έχουν τη μορφή:

(1) Συνδρομητής: αίτημα λειτουργίας προς **Δρομολογητή Περιεχομένου**

(2) Δρομολογητής Περιεχομένου: απαντά στέλνοντας το Token και το URIacp

Για να μπορεί να παρακολουθεί τα δημιουργηθέντα tokens ο **Δρομολογητής Περιεχομένου** διατηρεί έναν **Πίνακα Token** που περιέχει εγγραφές της μορφής:

[Token, Αυθεντικοποιημένος, Λήξη, URIacp]

Όταν ένα καινούριο ενδεικτικό (token) δημιουργείται, τότε μια νέα καταχώριση προστίθεται στον **Πίνακα Token.** Η αρχική τιμή του πεδίου **Αυθεντικοποιημένος** ορίζεται σε **ψευδή** και η τιμή του πεδίου **Λήξη** στο χρόνο δημιουργίας + ένα πολύ μικρό χρονικό διάστημα αρκετό όμως ώστε να ληφθεί η αναμενόμενη εξουσιοδότηση.

- **Αυθεντικοποίηση και Εξουσιοδότηση Αιτήματος Συνδρομητή:** Διαδικασία που συμβαίνει αφότου ο **Συνδρομητής** έχει κάνει ένα μη εξουσιοδοτημένο αίτημα. Αρχικά ο **Συνδρομητής** στέλνει τα δεδομένα που προσδιορίζουν την ταυτότητά του, το URIacp και το χαρακτηριστικό (token) στον **Πάροχο Ελέγχου Πρόσβασης**. Ο **Συνδρομητής** ελέγχεται αν ικανοποιεί το URIacp και αν ναι τότε ο **Πάροχος Ελέγχου Πρόσβασης** δημιουργεί ένα μήνυμα εξουσιοδότησης που περιέχει το token, το χρονικό διάστημα που θα είναι αυτό έγκυρο, το URIacp και το δημόσιο κλειδί PUBcr. Στη συνέχεια υπογράφει το μήνυμα και το στέλνει στον **Συνδρομητή**. Τα μηνύματα που ανταλλάσσονται είναι της μορφής:

  (3) Συνδρομητής: ID, PUBcr, URIacp, Token αποστολή προς τον **Πάροχο Ελέγχου Πρόσβασης**

  (4) Πάροχος Ελέγχου Πρόσβασης: Εξουσιοδότηση, Υπογραφή Εξουσιοδότησης **αποστολή προς Συνδρομητή**

  Όπου: **Εξουσιοδότηση** = Token, Διάρκεια εγκυρότητας, URIacp, PUBcr και

  Υπογεγραμμένη Εξουσιοδότηση = SignACP(auth)

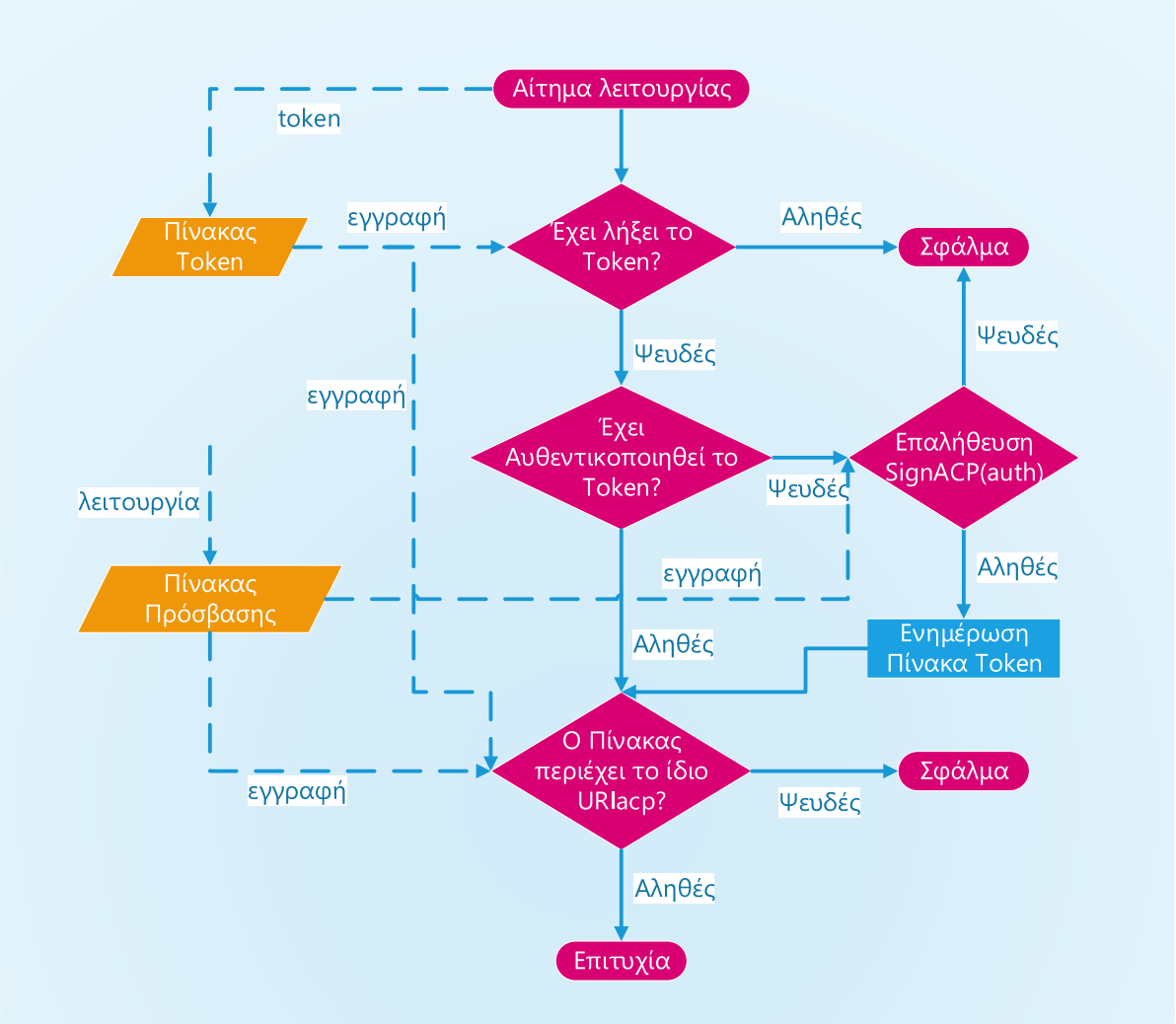
- **Εξουσιοδοτημένο Αίτημα Καταναλωτή:** Λαμβάνει χώρα από έναν **Συνδρομητή** που έχει εξουσιοδοτηθεί για την εκτέλεση μιας προστατευμένης λειτουργίας από έναν **Πάροχο Ελέγχου Πρόσβασης.** Ο **Συνδρομητής** στέλνει ένα μήνυμα που περιέχει το αίτημα λειτουργίας, το token, τη χρονική διάρκεια εγκυρότητας του token και την υπογραφή του εξουσιοδοτημένου μηνύματος. Η διαδικασία απεικονίζεται με το ακόλουθο μήνυμα:

(5) Συνδρομητής: αίτημα λειτουργίας, Token, Διάρκεια Εγκυρότητας Token, Υπογεγραμμένη Εξουσιοδότηση αποστολή προς τον **Δρομολογητή Περιεχομένου**

Από τη στιγμή που ο **Δρομολογητής Περιεχομένου** παραλάβει το μήνυμα πρέπει να αποφασίσει εάν ο **Συνδρομητής** επιτρέπεται να εκτελέσει την ενέργεια που έχει αιτηθεί. Προκειμένου αυτό να ολοκληρωθεί εκτελούνται τα ακόλουθα βήματα:

1. Αναζήτηση στον **Πίνακα Token** της εγγραφής που περιέχει το **token** της αίτησης και έλεγχος εάν είναι ακόμα έγκυρο. Εάν δεν είναι τότε επιστρέφεται μήνυμα σφάλματος
2. Εάν το πεδίο **Αυθεντικοποιημένος** της αντίστοιχης εγγραφής του **Πίνακα Token** έχει την τιμή Ψευδής τότε γίνονται τα εξής:
    a. Ανάκτηση του **PUBacp** που αντιστοιχεί με τη λειτουργία του **Πίνακα Πρόσβασης**
    b. Ανάκτηση του **URIacp** που αντιστοιχεί στη λειτουργία από τον **Πίνακα Token**
    c. Επανακατασκευή του μηνύματος εξουσιοδότησης
    d. Επαλήθευση της υπογεγραμμένης Αυθεντικοποίησης **SignACP(auth)** με τη χρήση του Δημόσιου Κλειδιού **PUBacp**
    e. Εάν η επαλήθευση είναι επιτυχής τότε ενημέρωση της εγγραφής στον Πίνακα ως εξής:
        - ορισμός του πεδίου **Λήξης** ίσο με την τιμή του πεδίου **Χρονική Διάρκεια** από το μήνυμα αυθεντικοποίησης,
        - ορισμός του πεδίου **Αυθεντικοποιημένος** σε Αληθής,
        - Συνέχεια στο βήμα 3a.
    f. Εάν η επαλήθευση αποτύχει τότε επιστροφή σφάλματος
3. Εάν το πεδίο **Αυθεντικοποιημένος** της αντίστοιχης εγγραφής του **Πίνακα Token** έχει την τιμή Αληθές τότε γίνονται τα εξής:
    a. Εντοπισμός του **URIacp** που αντιστοιχεί με το **token** από τον **Πίνακα Token**
    b. Εύρεση του **URIacp** της αιτηθείσας λειτουργίας από τον **Πίνακα Πρόσβασης**
    c. Έλεγχος εάν οι ανακτηθείσες τιμές ταιριάζουν. Εάν ναι επιστροφή, διαφορετικά επιστροφή μηνύματος σφάλματος

Εάν η διαδικασία είναι επιτυχής τότε κάθε επόμενη **Εξουσιοδοτημένη Αίτηση** μπορεί να έχει μόνο το token. Επίσης το ίδιο **token** μπορεί να χρησιμοποιηθεί πολλές φορές ακόμα και να ενεργοποιήσει διαφορετικές λειτουργίες που προστατεύονται από το ίδιο **URIacp**.



Σχήμα 6 - Διαδικασία απόφασης εξουσιοδότησης Αιτήματος

Παράδειγμα Χρήσης:

Ακολουθεί ένα παράδειγμα που σκιαγραφεί τον τρόπο εφαρμογής ΑΕΠ σε ένα δίκτυο NDN:

Ο **Εκδοτικός Οίκος Α** έχει τα δικαιώματα βιβλίων από διαφορετικούς συγγραφείς και τα έχει αποθηκεύσει στο δίκτυο NDN μαζί με τα αντίστοιχα οικονομικά στοιχεία. Επίσης θέλει να υπάρχει η δυνατότητα στους συνδρομητές του εκδοτικού οίκου να μπορούν να αναγνώσουν τα βιβλία, οι υπάλληλοι του οικονομικού τμήματος του εκδοτικού οίκου να μπορούν να έχουν πρόσβαση στα οικονομικά στοιχεία ώστε να μπορούν να εκτελούν τιμολογήσεις και τέλος οι συγγραφείς να μπορούν να κάνουν ανάγνωση αλλά και διορθώσεις στις εκδόσεις των βιβλίων τους. Οι λειτουργίες που εφαρμόζονται στον CRa είναι:

- Ανάγνωση βιβλίων,
- Τιμολόγηση βιβλίων και
- Διόρθωση έκδοσης βιβλίου.

Ο **Εκδοτικός Οίκος Α** έχει τις ακόλουθες πολιτικές ελέγχου πρόσβασης:

- Πολιτική 1: Όλοι οι συνδρομητές και οι συγγραφείς μπορούν να αναγνώσουν τα βιβλία
- Πολιτική 2: Μόνο οι υπάλληλοι του οικονομικού τμήματος μπορούν να δουν τα οικονομικά στοιχεία
- Πολιτική 3: Όλοι οι συγγραφείς μπορούν να ενημερώσουν τα βιβλία τους

Ο **Εκδοτικός Οίκος Α** εφαρμόζει τις προαναφερόμενες πολιτικές ελέγχου πρόσβασης έχοντάς τις αποθηκευμένες σε έναν ACP. Το δημόσιο κλειδί αυτού του ACP αναφέρεται από το Pub_{ACP}. Για κάθε πολιτική, ο ACP δημιουργεί τα αντίστοιχα URI, δηλαδή τα ekdOikA.gr/Policy1, ekdOikA.gr/Policy2 και ekdOikA.gr/Policy3. Ο Πίνακας Πρόσβασης του CRa ενημερώνεται με τις ακόλουθες καταχωρίσεις:

Λειτουργία	**URIacp**	**Δημόσιο κλειδί ACP**
Ανάγνωση βιβλίων	ekdOikA.gr/Policy1	Pub_{ACP}
Τιμολόγηση βιβλίων	ekdOikA.gr/Policy2	Pub_{ACP}
Διόρθωση έκδοσης βιβλίου	ekdOikA.gr/Policy3	Pub_{ACP}

Πίνακας 1 – Νέες εγγραφές του Πίνακα Πρόσβασης CRa

Ο συγγραφέας ενός βιβλίου εκδίδει μια μη εξουσιοδοτημένη αίτηση για την διόρθωση της έκδοσης ενός βιβλίου του. Ο CRa δημιουργεί ένα διακριτικό, π.χ. Token1, και αποκρίνεται στέλνοντας το ακόλουθο μήνυμα:

(ekdOikA.gr/Policy3, Token1)

Ο πίνακας Token του CRa ενημερώνεται στη συνέχεια με την ακόλουθη καταχώριση:

Token	**Αυθεντικοποίηση**	**Λήξη**	**URIacp**
Token1	Ψευδής	Timestamp1	ekdOikA.gr/Policy3

Πίνακας 2 – Νέες εγγραφές του Πίνακα Token CRa

Στο επόμενο βήμα ο συγγραφέας επικυρώνει τον εαυτό του στον ACP, ο οποίος απαντά με το ακόλουθο ψηφιακά υπογεγραμμένο μήνυμα εξουσιοδότησης:

[Token1, timestamp2, ekdOikA.gr/Policy3, PubCRa].

Στη συνέχεια, ο συγγραφέας εκδίδει το ακόλουθο εξουσιοδοτημένο αίτημα:

["Διόρθωση έκδοσης βιβλίου", Token1, timestamp2, SignACP(auth)]

Ο CRa ελέγχει αν το Token1 έχει λήξει. Στη συνέχεια, ανακατασκευάζει το μήνυμα εξουσιοδότησης ανακτώντας το URIacp που σχετίζεται με τη λειτουργία Διόρθωσης έκδοσης βιβλίου (δηλ. ekdOikA.gr/Policy3) από τον Πίνακα Πρόσβασης και επαληθεύει το SignACP(auth) χρησιμοποιώντας το PubACP, επίσης από τον Πίνακα Πρόσβασης. Τέλος, ο CRa ελέγχει εάν το URIacp που βρίσκεται στον Πίνακα Πρόσβασης αντιστοιχεί στο URIacp που περιλαμβάνεται στην καταχώρηση για το Token1 στον Πίνακα Token. Εάν όλα αυτά τα βήματα είναι επιτυχή, ο CRa εκτελεί τη λειτουργία **"Διόρθωση έκδοσης βιβλίου"** και τροποποιεί την καταχώριση για το Token1 στον πίνακα Token ως εξής:

Token	**Αυθεντικοποίηση**	**Λήξη**	**URIacp**
Token1	Αληθής	timestamp2	ekdOikA.gr/Policy3

Πίνακας 3 – Ενημερωμένες εγγραφές του Πίνακα Token CRa

Από τη στιγμή που το Token1 χαρακτηρίζεται πλέον ως αυθεντικοποιημένο / επικυρωμένο, ο συγγραφέας μπορεί να το χρησιμοποιήσει σε όλες τις επόμενες αιτήσεις μέχρι να λήξει. Επιπλέον, όσο ισχύει το Token1, το SignACP(auth) δεν χρειάζεται να συμπεριληφθεί στα επόμενα αιτήματα.

Στο παραπάνω παράδειγμα χρήσης, μπορεί να παρατηρηθεί ότι εάν συγγραφέας επιθυμεί να εκτελέσει τη λειτουργία **"Ανάγνωση βιβλίου"**, πρέπει να αυθεντικοποιηθεί εκ νέου, δεδομένου ότι η λειτουργία αυτή προστατεύεται από διαφορετικό URIacp. Το ζήτημα αυτό θα μπορούσε να μετριασθεί αν προστεθεί ένα νέο πεδίο **"Επίπεδο Συνδρομητή"** στον Πίνακα Πρόσβασης CRa. Το επίπεδο των συνδρομητών είναι ένας αριθμός που υποδηλώνει το ελάχιστο επίπεδο που πρέπει να έχει ένας συνδρομητής για να επικαλεστεί μια πράξη. Χρησιμοποιώντας αυτήν την επέκταση, ο Πίνακας Πρόσβασης του Δρομολογητή Περιεχομένου μπορεί να τροποποιηθεί ως εξής:

Λειτουργία	**URIacp**	**Δημόσιο κλειδί ACP**	**Επίπεδο Συνδρομητή**
Ανάγνωση βιβλίων	ekdOikA.gr/Policy1	Pub_{ACP}	100
Τιμολόγηση βιβλίων	ekdOikA.gr/Policy2	Pub_{ACP}	100
Διόρθωση έκδοσης βιβλίου	ekdOikA.gr/Policy1	Pub_{ACP}	200

Πίνακας 4 – Επέκταση του Πίνακα Πρόσβασης CRa

Με αυτήν την επέκταση, ένας ACP πρέπει να συμπεριλάβει το επίπεδο των συνδρομητών στα μηνύματα εξουσιοδότησης. Επιπλέον, ένας CR συμμετέχει πλέον στην απόφαση ελέγχου πρόσβασης, καθώς πρέπει να ελέγξει εάν το επίπεδο που περιλαμβάνεται στο μήνυμα εξουσιοδότησης είναι μεγαλύτερο ή ίσο με το επίπεδο που περιλαμβάνεται στον Πίνακα Πρόσβασης. Τέλος, εάν χρησιμοποιείται η επέκταση επιπέδου, οι πίνακες Token θα πρέπει επιπλέον να περιλαμβάνουν το επίπεδο που αντιστοιχεί σε ένα διακριτικό token.

Στο προηγούμενο παράδειγμα αν υπήρχε το Επίπεδο Συνδρομητή με την τιμή 200 για τον συγγραφέα τότε θα μπορούσε να εκτελέσει επιτυχώς τη λειτουργία **"Ανάγνωση βιβλίου"** χρησιμοποιώντας το Token1 χωρίς την ανάγκη εκ νέου αυθεντικοποίησης.

4.3 Διαχείριση Κρυπτογραφικών Κλειδιών και Πιστοποιητικών

NDNCERT Σύστημα Διαχείρισης Εμπιστοσύνης

Η αρχιτεκτονική δικτύωσης δεδομένων (NDN) δημιουργεί τις προϋποθέσεις ασφαλείας στο επίπεδο δικτύου: όλα τα πακέτα δεδομένων που έχουν ανακτηθεί πρέπει να υπογραφούν για να εξασφαλίσουν την ακεραιότητα, την αυθεντικότητα και την προέλευσή τους. Για να διασφαλιστεί ότι τα θεμελιώδη αυτά στοιχεία χρησιμοποιούνται χωρίς να επιβάλλονται αδικαιολόγητα βάρη στους χρήστες του NDN, η διαχείριση κρυπτογραφικών κλειδιών και πιστοποιητικών πρέπει να λειτουργεί με τρόπο απλό, ασφαλές και φιλικό προς το χρήστη.

Το πρόσφατο σύστημα NDN Trust Management (NDNCERT) [29][30] έχει σχεδιαστεί για να καλύψει την ανάγκη αυτή. Το NDNCERT παρέχει ευέλικτους μηχανισμούς για την ανάθεση εμπιστοσύνης μεταξύ των πιστοποιητικών, είτε μέσα σε μία μόνο συσκευή (διαχείριση αδειών για τοπικές εφαρμογές σε κόμβο που λειτουργεί κάτω από ένα συγκεκριμένο χώρο ονομάτων) είτε σε διάφορες συσκευές / οντότητες.

Το NDNCERT διαθέτει έναν αρθρωτό σχεδιασμό για να αντιμετωπίσει προκλήσεις ασφάλειας που δημιουργούν εμπιστοσύνη για την έκδοση πιστοποιητικών εκτός ζώνης (out of band). Μόλις ένας κόμβος ή μια εφαρμογή λάβει ένα έγκυρο πιστοποιητικό για το χώρο ονομάτων του (ή έχει ρυθμιστεί με πιστοποιητικό που έχει υπογράψει αυτόματα), γίνεται αυτόματα αρχή πιστοποίησης για το χώρο ονομάτων του και μπορεί να χρησιμοποιήσει το ίδιο πρωτόκολλο NDNCERT για την παραγωγή πιστοποιητικών για τα δευτερεύοντα διαμερίσματα ονομάτων .

Με το σύστημα αυτό η Ανάθεση Ελέγχου Πρόσβασης σε ένα δίκτυο NDN εξασφαλίζει την ακεραιότητα, αυθεντικότητα και προέλευση όλων των ενεργειών που λαμβάνουν χώρα.

4.4 Αποτίμηση Εφαρμογής Ελέγχου Πρόσβασης

Μπορεί εύκολα να παρατηρηθεί ότι το σύστημα που παρουσιάστηκε προηγουμένως ενισχύει την ιδιωτική ζωή των συνδρομητών. Η μόνη πληροφορία που μαθαίνει ένας CR σχετικά με έναν συνδρομητή είναι η σχέση εμπιστοσύνης του με ένα συγκεκριμένο ACP. Στην περίπτωση που χρησιμοποιηθεί η επέκταση επιπέδου, ο CR μαθαίνει επίσης το επίπεδό του. Φυσικά, το τελευταίο μπορεί να κωδικοποιηθεί με τρόπο που να μην αποκαλύπτει ουσιαστικές πληροφορίες. Οποιεσδήποτε άλλες ευαίσθητες πληροφορίες αποθηκεύονται σε έναν αξιόπιστο ACP.

Επιπλέον, ανεξάρτητα από τη διάρκεια ζωής ενός διακριτικού (token), ο συνδρομητής μπορεί να το εγκαταλείψει και να ζητήσει ένα νέο, προκειμένου να αποφευχθεί η δημιουργία προφίλ από τον CR.

Τέλος, ο ACP δεν αποκτά πληροφορίες σχετικά με τις πράξεις που επικαλείται ένας συνδρομητής και τα δεδομένα στα οποία έχει πρόσβαση: οι μόνες πληροφορίες που μαθαίνει ένας ACP είναι το δημόσιο κλειδί του CR με το οποίο αλληλεπιδρά ο συνδρομητής.

Ένα άλλο χαρακτηριστικό ασφάλειας του συστήματος είναι ότι οι πολιτικές ελέγχου πρόσβασης μπορούν εύκολα να τροποποιηθούν. Οι πολιτικές ελέγχου πρόσβασης αποθηκεύονται σε ένα μόνο σημείο (δηλ. στον ACP) και όλα οι CR έχουν δείκτες στις πολιτικές. Επομένως, η τροποποίηση μιας πολιτικής ελέγχου πρόσβασης δεν συνεπάγεται επικοινωνία με κανένα CR. Όταν τροποποιείται μια πολιτική ελέγχου πρόσβασης, όλοι οι νέοι συνδρομητές θα εξουσιοδοτηθούν χρησιμοποιώντας τη νέα πολιτική, ενώ όλοι οι ήδη εξουσιοδοτημένοι συνδρομητές θα λάβουν εκ νέου έγκριση με τη νέα πολιτική όταν λήξει το σήμα τους.

Η εξασφάλιση των ανωτέρω προϋποθέτει ότι όλα τα μηνύματα που ανταλλάσσονται να είναι κρυπτογραφημένα μέσα από ασφαλείς συνδέσεις. Επιπρόσθετα το σύστημα Διαχείρισης Εμπιστοσύνης παρέχει έναν ευέλικτο μηχανισμό για την έκδοση των πιστοποιητικών που είναι απαραίτητα για την εξασφάλιση της εμπιστοσύνης σημαντικών οντοτήτων του συστήματος όπως οι ACP και οι CR.

5 Συμπεράσματα

Στην παρούσα Διπλωματική Εργασία παρουσιάστηκε ένα Σύστημα Ανάθεσης και Επιβολής Πολιτικής Ελέγχου Πρόσβασης σε δίκτυα NDN. Η προτεινόμενη λύση δίνει τη δυνατότητα σε Εκδότες Πληροφοριακού Περιεχομένου να δημιουργήσουν και να εφαρμόσουν Πολιτικές Ελέγχου Πρόσβασης σε οποιονδήποτε Συνδρομητή και για οποιαδήποτε ενέργεια επιθυμεί αυτός να εκτελέσει πάνω σε δεδομένα που αποθηκεύουν και διαθέτουν σε περιβάλλον δικτύου NDN.

Οι οντότητες που έχουν κομβικό ρόλο σε αυτό το περιβάλλον είναι ο **Πάροχος Ελέγχου Πρόσβασης** (ACP) ο οποίος είναι και ο υπεύθυνος για την αποθήκευση, διατήρηση αλλά και επιβολή της εκάστοτε πολιτικής που διέπει μια ενέργεια σε δεδομένα, καθώς και ο **Δρομολογητής Περιεχομένου** (CR) που τα διανέμει. Ο ACP δίνει τη δυνατότητα κάθε διαφορετικός Εκδότης Πληροφοριακού Περιεχομένου να ορίσει ο ίδιος ξεχωριστά τους κανόνες, τις λειτουργίες και τις προϋποθέσεις που θα εφαρμοστούν, ενώ ο Δρομολογητής οφείλει να σεβαστεί τον ACP με αμοιβαία εμπιστοσύνη.

Η εμπιστοσύνη εξασφαλίζεται με την παροχή κατάλληλων πιστοποιητικών που εκδίδονται μέσω του συστήματος **NDNCert** και εμπλουτίζουν το σύστημα με τις ενδεδειγμένες διαδικασίες πιστοποίησης.

Δεδομένου ότι το σύστημα NDN υποστηρίζει εγγενώς κρυπτογράφηση των δεδομένων που μετακινούνται αλλά και της αποκεντρικοποιημένης και απλής φιλοσοφίας που το διέπει σε συνδυασμό με εξασφάλιση του τι μπορεί να γίνει από ποιόν σε τι μπορούμε να ισχυρισθούμε ότι εξελίσσεται σε ένα σύστημα διακίνησης πληροφορίας τέτοιο που να μπορεί να ανοίξει το έδαφος για νέες συναρπαστικές εφαρμογές και επιχειρηματικές ευκαιρίες σε παγκόσμια κλίμακα.

Λεξικό Όρων

ACD: Access Control Delegation

ACP: Access Control Provider

ACPol: Access Control Policy

ANDaNA: Anonymous Named Data Networking Application

CCN: Content-Centric Networking

CDN: Content Distribution Network

COMET: COntent Mediator architecture for content aware nETworks

CR: Content Router

CS: Content Store

DNS: Domain Name Service

DONA: Data-Oriented (and beyond) Network Architecture

DoS: Denial of Service

FIB: Forward Information Base

ICN: Information Centric Network

IP: Internet Protocol

IoT: Internet of Things

LFBL: Listen First Broadcast Later

LRU: Least Recent Used

NDN: Named Data Network

NSF: National Science Foundation

OSPF: Open Shortest Path First

PARC: Palo Alto Research Center

PIT: Pending Interests Table

PSIRP: Publish-Subscribe Internet Routing Paradigm

PURSUIT: Publish-Subscribe Internet Technology

RFC: Request For Comments

SAIL: Scalable & Adaptive Internet soLutions

TCP: Transport Control Protocol

URI: Universal Resource Identifier

Αναφορές

[1] G. Xylomenos, C. N. Ververidis, V. A. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K. V. Katsaros, and G. C. Polyzos, "A Survey of Information-Centric Networking Research"

[2] T. Koponen, M. Chawla, B. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica, "A data-oriented (and beyond) network architecture," in *ACM SIGCOMM*, 2007, pp. 181–192.

[3] FP7 PURSUIT project. [Online]. Available: http://www.fp7-pursuit.eu/PursuitWeb/

[4] FP7 PSIRP project. [Online]. Available: http://www.psirp.org/

[5] FP7 SAIL project. [Online]. Available: http://www.sail-project.eu/

[6] FP7 4WARD project. [Online]. Available: http://www.4ward-project.eu/

[7] FP7 COMET project. [Online]. Available: http://www.comet-project.org/

[8] FP7 CONVERGENCE project. [Online]. Available: http://www.ictconvergence.eu/

[9] NSF Named Data Networking project. [Online]. Available: http://www.named-data.net/

[10] Content Centric Networking project. [Online]. Available: http://www.ccnx.org/

[11] NSF Mobility First project. [Online]. Available: http://mobilityfirst.winlab.rutgers.edu/

[12] ANR Connect project. [Online]. Available: http://anr-connect.org/

[13] V. Jacobson, "A new way to look at networking," Google Tech Talk, August 2006

[14] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in *ACM CoNEXT*, 2009.

[15] NDN Frequently Asked Questions (FAQ). [Online]. Available: https://named-data.net/project/faq/#What_is_the_motivation_behind_the_NDN_project

[16] The End-to-end principle. [Online]. Available: https://cs.stanford.edu/people/eroberts/cs201/projects/2010-11/NetNeutrality/Articles/Proponents.html

[17] A Case for Stateful Forwarding Plane. [Online]. Available: http://named-data.net/publications/comcom-stateful-forwarding/

[18] Named Data Networking: Executive Summary. [Online]. Available: https://named-data.net/project/execsummary/

[19] Named Data Networking: Motivation & Details. [Online]. Available: http://named-data.net/project/archoverview/

[20] NDN Protocol Design Principles. . [Online]. Available: https://named-data.net/project/ndn-design-principles/

[21] P. Helland, "Immutability changes everything" in *Communications of the ACM*, vol 59 Issue 1, January 2016, pp. 64-70

[22] V. Jacobson, D. K. Smetters, N. H. Briggs, M. F. Plass, P. Stewart, J. D. Thornton, and R. L. Braynard, "VoCCN: Voice over content-centric networks," in *ACM ReArch Workshop*, 2009.

[23] W. K. Chai, D. He, I. Psaras, and G. Pavlou, "Cache "less for more" in information-centric networks," in *Proc. IFIP-TC6 Networking Conference*, 2012.

[24] I. Psaras, W. K. Chai, and G. Pavlou, "Probabilistic in-network caching for information-centric networks," in *ACM Workshop on Information-Centric Networking (ICN)*, 2012.

[25] M. Meisel, V. Pappas, and L. Zhang, "Ad hoc networking via named data," in *ACM MobiArch*, 2010

[26] D. Smetters and V. Jacobson, "Securing network content," PARC, Tech. Rep. TR-2009-01, October 2009.

[27] S. DiBenedetto, P. Gasti, G. Tsudik, and E. Uzun, "ANDaNA: Anonymous named data networking application," in *Network and Distributed System Security Symposium (NDSS)*, 2012.

[28] N. Fotiou, A. Machas, G. Xylomenos, G. C. Polyzos, "Access control as a service for the Cloud", *Journal of Internet Services and Applications*, Vol. 6, no.1, 2015

[29] Z. Zhang, Y. Yu, A. Afanasyev, L. Zhang, "NDN Certificate Management Protocol (NDNCERT)", *NDN, Technical Report NDN-0050*, Revision 1: April 29, 2017

[30] Z. Zhang, A. Afanasyev, L. Zhang, "NDNCERT: Universal Usable Trust Management for NDN", *ICN '17*, September 26–28, 2017, Berlin, Germany