ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Προστασία Πολυμεσικού Περιεχομένου σε Δίκτυα με Επίκεντρο την Πληροφορία

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Ιωάννης Π. Παπάνης

Αθήνα, Ιανουάριος 2014

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Προστασία Πολυμεσικού Περιεχομένου σε Δίκτυα με Επίκεντρο την Πληροφορία

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Ιωάννης Π. Παπάνης

Συμβουλευτική Επιτροπή : Ιάκωβος Στ. Βενιέρης
Γεώργιος Στασινόπουλος
Δήμητρα-Θεοδώρα Ι. Κακλαμάνη

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή την 20η Ιανουαρίου 2014.

.....	.....	.....
Ι. Βενιέρης	Γ. Στασινόπουλος	Δ.-Θ. Κακλαμάνη
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π	Καθηγήτρια Ε.Μ.Π
.....	.....	.....
Μ. Θεολόγου	Ν. Ουζούνογλου	Σ. Παπαβασιλείου
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Αναπλ. Καθηγητής Ε.Μ.Π.
	.....	
	Χ. Δουληγέρης	
	Καθηγητής Παν. Πειραιώς	

Αθήνα, Ιανουάριος 2014

.....

Ιωάννης Π. Παπάνης

Διδάκτωρ Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Σε αυτούς, που εξακολουθούν να κάνουν

περισσότερα όνειρα για μένα απ' ό,τι εγώ ο ίδιος.

Αντί Προλόγου

Για την αγάπη, τη στήριξη, την ανοχή, την ύπαρξη…

Σας ευχαριστώ.

Περίληψη

Η πρόοδος των Τεχνολογιών Πληροφορίας και Επικοινωνιών έχει δώσει ώθηση στη διανομή πολυμεσικού περιεχομένου μέσω Διαδικτύου. Σήμερα γινόμαστε μάρτυρες της ταχύτατης σύγκλισης στον τρόπο κατανάλωσης οπτικοακουστικού περιεχομένου —είτε μέσω κλασσικής τηλεόρασης ευρείας εκπομπής, είτε μέσω διαδικτυακών υπηρεσιών— σε μια συσκευή. Όροι όπως έξυπνη (υβριδική) τηλεόραση, βίντεο κατά παραγγελία, διαδικτυακά κανάλια εισέρχονται με γοργούς ρυθμούς στην καθημερινότητά μας.

Ωστόσο, η παροχή υπηρεσιών διανομής πολυμεσικού περιεχομένου παρουσιάζει δυσκολίες και ιδιαιτερότητες, καθώς τόσο οι παραγωγοί, όσο και οι καταναλωτές του περιεχομένου έχουν ιδιαίτερα υψηλές απαιτήσεις αναφορικά με την ποιότητα, την προσβασιμότητα και την προστασία του διανεμόμενου υλικού. Η πολυπλοκότητα του περιβάλλοντος διανομής —ετερογενή δίκτυα, μη διαλειτουργικές συσκευές, απουσία προτυποποίησης— έχει συμβάλει στην επικράτηση μη συμβατών, ιδιόκτητων λύσεων και επικαλυπτικών δικτύων.

Το παράδειγμα των Δικτύων με Επίκεντρο την Πληροφορία (ICN), που αποτελεί μία υποψήφια αρχιτεκτονική για το μελλοντικό Διαδίκτυο, έχει βασιστεί στη διαπίστωση ότι το παρόν Διαδίκτυο, που έχει δομηθεί στις αρχές της επικοινωνίας δύο απομακρυσμένων κόμβων, είναι εγγενώς ακατάλληλο για να ικανοποιήσει τις ανάγκες της διανομής περιεχομένου. Το περιεχόμενο έρχεται στο προσκήνιο, καθώς η δρομολόγηση πραγματοποιείται με χρήση του ονόματός του και όχι την τοποθεσία των πελατών και εξυπηρετητών, κάτι που επιτρέπει την εύκολη ενδοδικτυακή αποθήκευση.Ωστόσο, στα Δίκτυα ICN, θέματα όπως η ασφάλεια και η ιδιωτικότητα είναι ανοιχτά.

Η Διατριβή έχει σαν αντικείμενο την προστασία του πολυμεσικού περιεχομένου κατά τη διάρκεια της διανομής του, μέσω της σχεδίασης και ανάπτυξης μιας πρωτότυπης λύσης η οποία ενσωματώνει την τεχνολογία της Κρυπτογραφίας βάσει Χαρακτηριστικών (ABE) σε Δίκτυα ICN. Η Κρυπτογραφία ABE ενσωματώνεται σε συστήματα Διαχείρισης Ψηφιακών Δικαιωμάτων (DRM). Η διαδικασία απόκτησης άδειας χρήσης πολυμεσικού περιεχομένου παρουσιάζεται αναλυτικά, με έμφαση στην ενορχήστρωση πολλαπλών αρχών πιστοποίησης. Εν συνεχεία επιδεικνύεται η διανομή αδειών χρήσης και πολυμέσων μέσω ICN, και, τέλος, προτείνεται μια τεχνική ανάκλησης χρήστη στο πλαίσιο της συνέργειας της Κρυπτογραφίας ABE και των Δικτύων ICN.

Η προτεινόμενη λύση είναι σύμφωνη με τις αρχές της Αρχιτεκτονικής Προσανατολισμένης σε Υπηρεσίες (SOA). Αφού αιτιολογηθεί η καταλληλότητα του παραδείγματος SOA για τους παρόχους υπερκείμενων υπηρεσιών OTT, παρουσιάζεται λεπτομερώς η ενσωμάτωση της Κρυπτογραφίας ABE σε μια τέτοια αρχιτεκτονική.

Ακολούθως πραγματοποιείται αξιολόγηση των Δικτύων ICN σε αντιπαραβολή με τα Δίκτυα CDN —εξετάζοντάς τα βάσει μετρικών, που καθορίζουν την ποιότητα της παρεχόμενης υπηρεσίας και την εξοικονόμηση δικτυακής κίνησης. Τέλος, η Διατριβή ολοκληρώνεται, με την παράθεση των συμπερασμάτων και μελλοντικών επεκτάσεων.

Λέξεις κλειδιά: Διανομή πολυμεσικού περιεχομένου, προστασία πολυμεσικού περιεχομένου, δίκτυα με επίκεντρο την πληροφορία, κρυπτογραφία βάσει χαρακτηριστικών, αρχιτεκτονική προσανατολισμένη σε υπηρεσίες, σύστημα μεσισμικού.

Abstract

The advances of the Information and Communication Technologies have enabled the provision of multimedia content using Internet protocols. Today, we witness the rapid convergence of linear (broadcast) and non-linear (broadband) services and terms such as Video on Demand, Over-The-Top content, Connected TV enter our everyday life and shape the market. Video streaming dominates the Internet traffic, a trend that is expected to increase in the next years.

However, the provision of such services is very challenging, due to a number of factors. End users expect to access high quality video content, regardless of their device, connection type and location. On the other hand, Content Providers set strict security and quality requirements in order to license their content, making up an overall difficult and challenging context for Over-The-Top (OTT) Service Providers. The heterogeneity of underlying networks, the variety of user devices (hardware and software), the high volumes and other characteristics of network traffic combined with the lack of standardization compose a domain highly fragmented by proprietary solutions and overlay networks.

The paradigm of Information-Centric Networking (ICN), which has emerged as a promising Future Internet Architecture, is being driven by the realization that the current Internet architecture cannot meet the demands posed by content provision. In ICN content is treated as first-class citizen, through the introduction of name-based routing and the extensive use of in-network caching. At the same moment, issues including content protection and privacy are open.

This Thesis targets the protection of multimedia content in the context of ICN. The Thesis proposes an architecture that utilizes ICN in order to provide scalable and efficient video distribution, and Attribute-Based Encryption (ABE) to securely distribute this content in the ICN environment. ABE is incorporated into Digital Rights Management (DRM) schemes. The video license acquisition process is presented, with a focus on orchestrating multiple authorities; subsequently, the video distribution over ICN is demonstrated, and finally, user revocation techniques are investigated in the ABE and ICN context and an appropriate mechanism one is adopted.

Extensive effort is put towards the compliance of the proposed solution with the principles of Service Oriented Architectures (SOA). After providing arguments about the benefits of SOA for the OTT Service Providers, detailed implementation blueprints are provided towards the seamless introduction of ABE in the OTT architectures.

The performance of ICN is compared against the popular Content Delivery Network (CDN) solution using extensive simulations. Using standard metrics, we show that ICN composes an alternative for both users and Internet Service Providers. Finally, the Thesis is concluded, by discussing the main findings and highlighting open issues and future work.

Keywords: Content delivery, content protection, Information-Centric Networking, Attribute-Based Encryption, Digital Rights Management, User revocation, Service Oriented Architecture.

Πίνακας Περιεχομένων

Πίνακας Σχημάτων

1 Εισαγωγή

Στις απαρχές του 21ου αιώνα, και καθώς το όραμα του Mark Weiser για την πανταχού παρούσα «υπολογιστική» (ubiquitous computing) [1] σταδιακά παίρνει σάρκα και οστά, ένας ολοένα και αυξανόμενος αριθμός συσκευών δικτυώνεται και παράλληλα η υπολογιστική ισχύς διαχέεται στο περιβάλλον. Σταδιακά, η σχέση ανθρώπου-υπολογιστή εξελίχθηκε από την εποχή των κεντρικών μονάδων (mainframes), όπου ένας υπολογιστής αντιστοιχούσε σε πολλούς χρήστες (50s-70s) στην εποχή του προσωπικού υπολογιστή, ο οποίος αντιστοιχούσε σε ένα μοναδικό χρήστη (80s-90s), ενώ πλέον έχει περάσει σε αυτή της κινητής υπολογιστικής, όπου ένας χρήστης έχει στην κατοχή του περισσότερες της μίας συσκευές (2000-σήμερα). Παράλληλα η δικτύωση έχει προχωρήσει ένα βήμα παραπέρα, καθώς είναι ήδη πανταχού παρούσα και αόρατη, επιτρέποντας την αδιάλειπτη πρόσβαση των συσκευών στον παγκόσμιο ιστό και τις υπηρεσίες που προσφέρονται μέσω αυτού.

Η πλειονότητα των επιχειρήσεων και οργανισμών έχει εισέλθει στην ψηφιακή εποχή και οι διαθέσιμες υπηρεσίες προσφέρονται μέσω του Διαδικτύου, αν όχι αποκλειστικά, τουλάχιστον σε μεγάλο βαθμό, γνωρίζοντας μεγάλη αποδοχή. Η χρήση του Διαδικτύου έχει μετατοπιστεί πλέον από την επικοινωνία δύο απομακρυσμένων υπολογιστών, στη διανομή περιεχομένου προς πολλούς παραλήπτες. Ιδιαίτερα μεγάλη επιτυχία γνωρίζουν οι υπηρεσίες διανομής πολυμεσικού περιεχομένου. Οι υπηρεσίες αυτές είναι ιδιαίτερα απαιτητικές σε διαδικτυακούς πόρους, ενώ παράλληλα εγείρουν και ζητήματα προστασίας περιεχομένου, τα οποία είναι εξίσου σημαντικά για τους παρόχους.

Σε ένα τέτοιο, ραγδαίως μεταβαλλόμενο, περιβάλλον, το οποίο χαρακτηρίζεται από την ετερογένεια των συσκευών, των υποκείμενων δικτύων και των μορφοποιήσεων του διαθέσιμου πολυμεσικού περιεχομένου και υπό την πίεση των υψηλών απαιτήσεων των χρηστών, έχει προκύψει ένας μεγάλος αριθμός μη-προτυποποιημένων και μη-διαλειτουργικών λύσεων. Η απουσία προτυποποίησης, αν και αρχικά έδωσε ώθηση στη νέα αυτή αγορά, φέρνοντας στο προσκήνιο τους παρόχους υπερκείμενων υπηρεσιών, λειτουργεί σαν τροχοπέδη για την περαιτέρω ανάπτυξη και την εύρυθμη λειτουργία της, καθώς οι ιδιόκτητες, κλειστές λύσεις καθίστανται ακατάλληλες για το σύνολο του περιεχομένου.

Οι αδυναμίες στις υφιστάμενες τεχνολογίες διανομής πολυμεσικού υλικού είναι ένα από τα κίνητρα που ωθούν την έρευνα σε μία καινοτόμα μορφή δικτύωσης, τα Δίκτυα με Επίκεντρο την Πληροφορία (Information Centric Networks – ICN) [2]. Η πρόταση αυτή θέτει το περιεχόμενο στο επίκεντρο, προτείνοντας τη δρομολόγηση βάσει ονόματος και την ευρεία χρήση ενδοδικτυακών αποθηκευτικών χώρων για την αποδοτική διανομή του περιεχομένου. Το συγκεκριμένο παράδειγμα δικτύωσης έχει καταφέρει να στρέψει πάνω του τα φώτα της ερευνητικής κοινότητας, αποτελώντας αντικείμενο σημαντικών ερευνητικών προγραμμάτων, τα οποία εστιάζουν σε πτυχές της ονοματοδοσίας, της δρομολόγησης και της χρήσης των αποθηκευτικών κόμβων, ενώ θέματα όπως η ασφάλεια του περιεχομένου και η ιδιωτικότητα των χρηστών παραμένουν ανοιχτά.

Η Διατριβή έχει σαν αντικείμενο την προστασία του πολυμεσικού περιεχομένου κατά τη διάρκεια της διανομής του, μέσω της σχεδίασης και ανάπτυξης μιας πρωτότυπης λύσης η οποία ενσωματώνει την τεχνολογία της Κρυπτογραφίας βάσει Χαρακτηριστικών (Attribute-Based Encryption – ABE) [3] σε Δίκτυα ICN. Η Κρυπτογραφία ABE ενσωματώνεται σε συστήματα Διαχείρισης Ψηφιακών Δικαιωμάτων (DRM). Η διαδικασία απόκτησης άδειας χρήσης πολυμεσικού περιεχομένου έχει δομηθεί με επίκεντρο την ενορχήστρωση πολλαπλών αρχών πιστοποίησης. Η διανομή αδειών χρήσης και πολυμέσων πραγματοποιείται μέσω Δικτύων ICN και προτείνεται μια τεχνική ανάκλησης χρήστη στο πλαίσιο της συνέργειας της Κρυπτογραφίας ABE και των Δικτύων ICN.

Η προτεινόμενη λύση είναι σύμφωνη με τις αρχές της Αρχιτεκτονικής Προσανατολισμένης σε Υπηρεσίες (SOA), η οποία είναι κατάλληλη για τους παρόχους υπερκείμενων υπηρεσιών OTT. Η ενσωμάτωση της Κρυπτογραφίας ABE και η διάθεση των λειτουργικοτήτων της υπό μορφή υπηρεσιών σε μια τέτοια αρχιτεκτονική αποτελεί κεντρικό σημείο της λύσης.

Τα Δίκτυα ICN αξιολογούνται σε αντιπαραβολή με τα Δίκτυα CDN με χρήση προσομοιωτή —εξετάζοντάς τα βάσει μετρικών, που καθορίζουν την ποιότητα της παρεχόμενης υπηρεσίας και την εξοικονόμηση δικτυακής κίνησης.

1.1 Ορισμοί

Στη συνέχεια του κειμένου χρησιμοποιούνται διάφορες έννοιες, των οποίων το νόημα μπορεί να προκαλέσει σύγχυση. Για το λόγο αυτό, παρατίθενται οι παρακάτω ορισμοί:

- Πολυμεσικό περιεχόμενο (multimedia content): Σαν πολυμεσικό περιεχόμενο ορίζεται το ψηφιακό περιεχόμενο πολλαπλών μορφών. Οι μορφές αυτές περιλαμβάνουν κείμενο, εικόνα, βίντεο, ήχο, καθώς και συνδυασμούς τους. Το πολυμεσικό περιεχόμενο είναι ευρύτερο από το κλασσικό οπτικοακουστικό περιεχόμενο, ενώ περιλαμβάνει και την έννοια της αλληλεπίδρασης με το χρήστη.
- Υπερκείμενες Υπηρεσίες (Over-The-Top ή OTT Services): Υπερκείμενες ονομάζονται όλες οι διαδικτυακές υπηρεσίες, οι οποίες δεν παρέχονται στους τελικούς χρήστες από τον ίδιο τον πάροχο Διαδικτύου (ISP) τους, αλλά με χρήση των υποδομών του μέσω του Διαδικτύου. Στα πλαίσια της Διατριβής, ο όρος θα χρησιμοποιηθεί συγκεκριμένα για τις υπηρεσίες διανομής πολυμεσικού περιεχομένου.
- Πάροχος υπερκείμενων υπηρεσιών: ο οργανισμός που παρέχει υπερκείμενες υπηρεσίες, χωρίς να διαθέτει (απαραίτητα) δίκτυο μέσω του οποίου ο τελικός χρήστης έχει πρόσβαση σε αυτές
- Πάροχος υπηρεσιών Διαδικτύου: η επιχείρηση που συνιστά, λειτουργεί, ελέγχει ή διαθέτει δίκτυο για ηλεκτρονικές υπηρεσίες ή που απλώς παρέχει υπηρεσίες ηλεκτρονικών επικοινωνιών.[1]
- Πάροχος περιεχομένου: ο οργανισμός που διαθέτει υπηρεσίες και περιεχόμενο σε έναν πάροχο υπηρεσιών Διαδικτύου. Η Διατριβή επικεντρώνεται σε παρόχους πολυμεσικού περιεχομένου. Ας σημειωθεί ότι μια επιχείρηση —κατά περίπτωση— μπορεί να ιδωθεί είτε σαν πάροχος περιεχομένου, είτε σα διανομέας άλλων παρόχων περιεχομένου. Παραδείγματος χάριν η υπηρεσία Netflix είναι ταυτόχρονα διανομέας παρόχων περιεχομένου (Disney, Time

[1] Ν.3431 (ΦΕΚ 13/Α/3-2-2006) "Περί Ηλεκτρονικών Επικοινωνιών και άλλες διατάξεις"

Warner) προς τελικούς χρήστες, αλλά θεωρείται και η ίδια πάροχος περιεχομένου για την υπηρεσία Apple iTunes. Ιδιαίτερη μνεία πρέπει να δοθεί στο γεγονός ότι πλέον πάροχοι περιεχομένου δύνανται να είναι και τελικοί χρήστες (μέσω καναλιών όπως το YouTube).

1.2 Διάρθρωση της Διατριβής

Η Διατριβή αποτελείται από συνολικά οκτώ Κεφάλαια. Πέρα από το παρόν εισαγωγικό Κεφάλαιο, το περιεχόμενο των υπολοίπων Κεφαλαίων συνοψίζεται ως ακολούθως.

Στο δεύτερο Κεφάλαιο παρουσιάζονται οι τεχνολογίες διανομής πολυμεσικού υλικού, με τη σειρά εμφάνισής τους. Ξεκινώντας από το μοντέλο πελάτη-εξυπηρετή (client-server model), πάνω στο οποίο στηρίζεται και το World Wide Web, εξετάζονται τα πρωτόκολλα που αναπτύχθηκαν για τη διανομή πολυμεσικών ροών. Εν συνεχεία συνοψίζονται οι αδυναμίες του μοντέλου, οι οποίες και οδήγησαν στην ανάπτυξη και εδραίωση των Δικτύων Διανομής Περιεχομένου (Content Delivery Networks - CDNs). Τα Δίκτυα CDNs αντιμετωπίζουν ικανοποιητικά την ανάγκη για κλιμάκωση και απόδοση στην διανομή πολυμέσων, αλλά αφορούν μια υποκατηγορία δεδομένων που υπόκεινται σε συμβόλαιο. Έπειτα παρουσιάζεται η τεχνολογία δικτύων ομότιμων κόμβων (Peer2Peer ή P2P Networks), τα οποία αποτελούν ένα δραστικά διαφορετικό παράδειγμα δικτύωσης, όπου κάθε κόμβος δρα τόσο ως πελάτης όσο και ως εξυπηρετητής. Αξίζει να σημειωθεί πως οι προαναφερόμενες τεχνολογίες αυτές, δεν αντικαθιστούν η μία την άλλη, αλλά αντιθέτως συνυπάρχουν και αλληλοσυμπληρώνονται. Τέλος, παρουσιάζεται το περιβάλλον και οι τεχνολογίες αιχμής αναφορικά με τη διανομή πολυμεσικών ροών (βίντεο κατά παραγγελία), όπου παράλληλα δίδεται έμφαση και στην προστασία του περιεχομένου. Όπως γίνεται σαφές, κυριαρχούν κλειστές, ιδιόκτητες και μη διαλειτουργικές λύσεις. Στο τέλος του Κεφαλαίου επισκοπούνται οι τρέχουσες προσπάθειες προτυποποίησης.

Στο τρίτο Κεφάλαιο παρουσιάζεται η αναδυόμενη τεχνολογία των Δικτύων με Επίκεντρο την Πληροφορία (Information-Centric Networks - ICN), τα οποία αποτελούν έναν από τους πυλώνες της έρευνας για το μελλοντικό Διαδίκτυο (Future Internet). Συνοψίζονται οι κυριότερες ερευνητικές προσπάθειες στον τομέα αυτό, και εν συνεχεία παρουσιάζονται οι βασικές αρχές των Δικτύων ICN, με κυριότερες τη δρομολόγηση βάσει

ονόματος περιεχομένου και την αποθήκευση του περιεχομένου σε διαδικτυακά στοιχεία. Συνοπτικά εξετάζονται οι ομοιότητες και οι διαφορές προσεγγίσεων των ερευνητικών προγραμμάτων. Κατόπιν παρουσιάζεται η αρχιτεκτονική και το πρωτόκολλο μετάδοσης της αρχιτεκτονικής Content-Centric Networking (CCN), πάνω στο οποίο έχει στηριχθεί η δικτυακή αρχιτεκτονική της παρούσας Διατριβής. Ακολούθως επισκοπείται η μελέτη της διανομής ροών πολυμεσικού περιεχομένου στα πλαίσια των Δικτύων ICN και τέλος, παρουσιάζονται επιλεγμένα ανοιχτά θέματα, με έμφαση στην ασφάλεια και την ιδιωτικότητα στο περιβάλλον αυτό.

Το τέταρτο Κεφάλαιο αποτελεί την επισκόπηση των κυριότερων τάσεων στην Κρυπτογραφία ABE, η οποία αποτελεί μια πολλά υποσχόμενη τεχνολογία προστασίας περιεχομένου και η οποία έχει επιλεχθεί για την προστασία του πολυμεσικού περιεχομένου στα πλαίσια της προτεινόμενης αρχιτεκτονικής. Η Κρυπτογραφία ABE συγκεντρώνει ορισμένα χαρακτηριστικά που την καθιστούν κατάλληλη για την προστασία δεδομένων πάνω από Δίκτυα ICN. Εν συντομία παρουσιάζονται οι παραλλαγές της που έχουν προταθεί στη βιβλιογραφία και οι τρέχουσες ερευνητικές εργασίες που γίνονται προς την κατεύθυνση της αντιμετώπισης ανοιχτών θεμάτων. Ειδικότερα εξετάζονται τα θέματα της ανάκλησης χρηστών, των πολλαπλών αρχών πιστοποίησης και της απόκρυψης χαρακτηριστικών, τα οποία οφείλουν να απαντηθούν ικανοποιητικά, προτού γίνει δυνατή η ευρεία αποδοχή της. Τέλος, παρουσιάζονται οι κυριότερες προτάσεις εφαρμογής της Κρυπτογραφίας ABE, που καλύπτουν ένα ευρύ φάσμα περιβαλλόντων.

Το πέμπτο Κεφάλαιο παρουσιάζει αναλυτικά την προτεινόμενη αρχιτεκτονική που αποτελεί μία από τις βασικές συνεισφορές της Διατριβής. Εξετάζονται διάφορες πτυχές της αρχιτεκτονικής, με έμφαση τόσο στην ενσωμάτωση της Κρυπτογραφίας ABE σε Δίκτυα ICN, όσο και σε μία ενσωμάτωσή της σε τρέχουσες τεχνολογίες προστασίας πολυμεσικού περιεχομένου. Ειδική μνεία γίνεται σε θέματα, τα οποία άπτονται της δημιουργίας των κλειδιών των χρηστών με χρήση πολλαπλών αρχών πιστοποίησης, όσο και της ανάκλησης των χρηστών, οι οποίοι έχουν εκπέσει των χαρακτηριστικών τους.

Στο έκτο Κεφάλαιο, παρουσιάζεται η λεπτομερής αρχιτεκτονική μεσισμικού, η οποία σχεδιάστηκε και αναπτύχθηκε στο πλαίσιο της Διατριβής. Το προτεινόμενο σύστημα έχει δομηθεί βάσει των κανόνων του επιχειρησιακού δίαυλου υπηρεσιών και της αρχιτεκτονικής προσανατολισμένης στις υπηρεσίες. Περιγράφονται τα βασικά

δομικά στοιχεία της αρχιτεκτονικής, με έμφαση στη λειτουργία που αφορά την πιστοποίηση χρήστη και εν συνεχεία την απόδοση κλειδιού βάσει χαρακτηριστικών, με δυνατότητα ανάκλησης καθώς και στη λειτουργία που καλύπτει τον κύκλο κρυπτογράφησης του πολυμεσικού περιεχομένου. Αναλύεται η λειτουργία του κάθε δομικού στοιχείου, με επίκεντρο τον Ενορχηστρωτή Συνδρομητικής Υπηρεσίας και τον Ενορχηστρωτή Κρυπτογράφησης Περιεχομένου, καθώς και οι διεπαφές μεταξύ των δομικών στοιχείων και τρίτων συστημάτων, προκειμένου να επιτευχθεί ο στόχος της ομαλής ενσωμάτωσης της τεχνολογίας κρυπτογραφίας βάσει χαρακτηριστικών σε αρχιτεκτονικές παρόχων υπερκείμενων υπηρεσιών.

Στο έβδομο Κεφάλαιο αξιολογείται η προτεινόμενη λύση. Η αξιολόγηση πραγματοποιείται με κριτήρια που αντικατοπτρίζουν αφενός την προσφερόμενη ποιότητα υπηρεσίας προς το χρήστη και αφετέρου την οικονομία στη δικτυακή κίνηση που εξασφαλίζει ο πάροχος υπηρεσιών Διαδικτύου. Η κρίση πραγματοποιείται βάσει των αποτελεσμάτων που προκύπτουν από τη χρήση εξομοιωτή ο όποιος προσομοιώνει τη λειτουργία των δικτύων με επίκεντρο την πληροφορία καθώς και των δικτύων διανομής περιεχομένου, τα οποία χρησιμοποιούνται σήμερα.

Τέλος, το όγδοο Κεφάλαιο αποτελεί τον επίλογο της Διατριβής, υπογραμμίζοντας κάποια βασικά συμπεράσματα, αλλά και σκιαγραφώντας τις βασικές κατευθύνσεις που θα αποτελέσουν τους άξονες της συνέχισης της έρευνας έχοντας ως βάση τη λύση που προτείνεται από τη Διατριβή.

2 Τεχνολογίες διανομής πολυμεσικού περιεχομένου

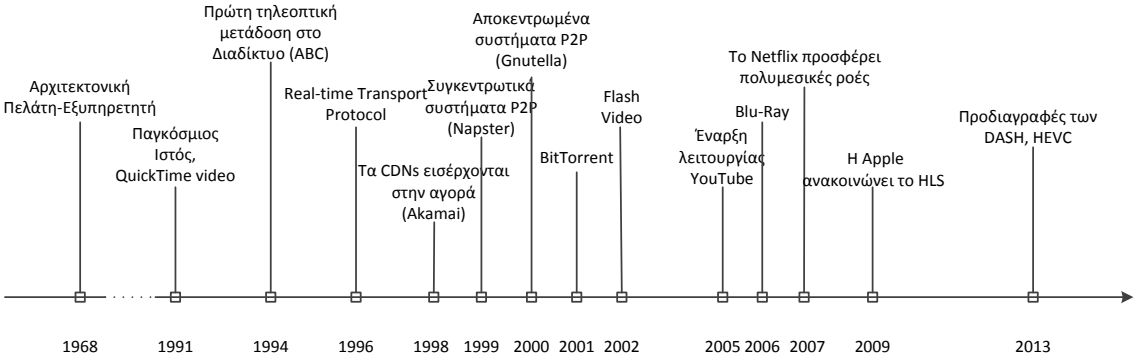
Το Κεφάλαιο αυτό παρουσιάζει συνοπτικά τις τεχνολογίες διανομής πολυμεσικού περιεχομένου από την εισαγωγή του Παγκόσμιου Ιστού και μετέπειτα.

Έπειτα από μία σύντομη εισαγωγή και μια σφαιρική επισκόπηση των ζητημάτων που διέπουν τη διανομή πολυμεσικού περιεχομένου, περιγράφονται διαδοχικά το μοντέλο πελάτη εξυπηρετητή, τα δίκτυα διανομής περιεχομένου και τα δίκτυα ομότιμων κόμβων. Θα πρέπει να τονιστεί ότι οι συγκεκριμένες τεχνολογίες δεν αντικατέστησαν η μία την άλλη, αλλά συνυπάρχουν αρμονικά και πολλές φορές λειτουργούν συμπληρωματικά με γνώμονα την αποδοτική διανομή περιεχομένου. Στη συνέχεια, εξετάζονται οι τρέχουσες τεχνολογίες διανομής και προστασίας πολυμεσικού περιεχομένου, όπου τονίζονται τα πλεονεκτήματα και τα μειονεκτήματά τους —με έμφαση στα τελευταία, τα οποία αποτέλεσαν την γενεσιουργό αιτία για την παρούσα Διατριβή.

2.1 Εισαγωγή

Η διανομή πολυμεσικού περιεχομένου είναι αναμφισβήτητα η σημαντικότερη των διαδικτυακών υπηρεσιών, αφενός γιατί σε αυτήν οφείλεται το μεγαλύτερο μέρος της κίνησης στο Διαδίκτυο σήμερα [4] και αφετέρου γιατί αποτελεί την κινητήριο δύναμη πίσω από τις ραγδαίες εξελίξεις και ανακατατάξεις στην βιομηχανία που περιστρέφεται γύρω από την εκμετάλλευση οπτικοακουστικού περιεχομένου (και η οποία πλέον εκτείνεται από εταιρίες παραγωγής και διάθεσης περιεχομένου και τηλεοπτικούς σταθμούς, μέχρι τηλεπικοινωνιακούς παρόχους και παρόχους υπηρεσιών Διαδικτύου). Ωστόσο η διαδρομή προς την παρούσα κατάσταση δε μπορεί να χαρακτηριστεί σαν μια ευθεία γραμμή – την τελευταία 15ετία έχουν δοκιμαστεί μια πληθώρα τεχνολογιών και μοντέλων υπηρεσιών (κάποιες από τις οποίες έχουν επανέρθει ανανεωμένες στο προσκήνιο με χαρακτηριστικότερο παράδειγμα αυτό των ροών (streaming) με χρήση του πρωτοκόλλου HTTP). Τα σημαντικότερα ορόσημα στην εξέλιξη της διανομής πολυμεσικού περιεχομένου απεικονίζονται στο Σχήμα 1. Οι τεχνολογικές προδιαγραφές βρίσκονται σε διαρκή ώσμωση με τις απαιτήσεις των χρηστών και ανατροφοδοτούνται

από την επιτυχία των ίδιων των υπηρεσιών πολυμέσων. Στο πλαίσιο αυτό, η ερευνητική δραστηριότητα στον τομέα αυτό έχει κάθε άλλο παρά ατονήσει, εντάσσοντας τις υπηρεσίες διανομής πολυμεσικού περιεχομένου στους κεντρικούς πυλώνες των υπό εξέταση μελλοντικών αρχιτεκτονικών Διαδικτύου.



Σχήμα 1 Ορόσημα στη διανομή πολυμεσικού περιεχομένου

Η τηλεόραση είναι η εφεύρεση με το μεγαλύτερο αντίκτυπο στην καθημερινότητα των ανθρώπων τα τελευταία 50 χρόνια. Από την αρχή της λειτουργίας των τηλεοπτικών σταθμών μέχρι πρόσφατα, το μοντέλο λειτουργίας παρέμενε —στις βασικές του αρχές— απαράλλακτο. Με την εμφάνιση του Διαδικτύου και ιδιαίτερα με την καθιέρωση των υπηρεσιών πολυμέσων, το παραδοσιακό μοντέλο της μετάδοσης τηλεοπτικού προγράμματος μετασχηματίζεται σ' ένα νέο, το οποίο διαφοροποιείται από το παλαιό σε όλους σχεδόν τους τομείς. Πιο συγκεκριμένα ο κάθε χρήστης του Διαδικτύου μπορεί πλέον —με σχετική ευκολία— να παραγάγει και να διαθέτει πολυμεσικό περιεχόμενο, ενώ αντίστοιχα ο καταναλωτής μπορεί να επιλέξει ένα προσωποποιημένο πρόγραμμα, στο οποίο έχει πρόσβαση όχι μόνο μέσω της κλασσικής συσκευής τηλεόρασης, αλλά από μία ευρύτατη γκάμα συσκευών (κινητά τηλέφωνα, ταμπλέτες, κονσόλες, υπολογιστές, έξυπνες τηλεοράσεις), που του επιτρέπουν την πρόσβαση ανεξαρτήτως τοποθεσίας, χρόνου και είδους σύνδεσης. Αυτή η δραματική αλλαγή έχει γίνει δυνατή χάρη στις συνεχώς εξελισσόμενες τεχνολογίες Διαδικτύου –για την υιοθέτηση των οποίων κόπτονται όλοι οι εμπλεκόμενοι στη διαδικασία, προκειμένου να ανταποκριθούν στις απαιτήσεις των χρηστών-καταναλωτών και να παραμείνουν ανταγωνιστικοί.

Η ανταπόκριση στις απαιτήσεις των χρηστών και η παροχή ποιοτικών διαδικτυακών υπηρεσιών πολυμέσων αποτελεί σημείο καμπής για όλους τους παίκτες στη βιομηχανία αυτή, αλλάζοντας εν τέλει άρδην το σκηνικό. Στο μεταίχμιο αυτό, έχουν αναδυθεί νέοι ηγεμονικοί παίκτες που καλούνται πάροχοι υπηρεσιών OTT. Οι υπηρεσίες OTT γνωρίζουν μεγάλη εξάπλωση, αρχικά με τη μορφή εφαρμογών ανταλλαγής μηνυμάτων (σύμφωνα με την Ευρωπαία Επίτροπο για την Ψηφιακή Ατζέντα, Neelie Kroes, το 2013 τα μηνύματα μέσω τέτοιων εφαρμογών ξεπέρασαν τα SMS παγκοσμίως [5]), αλλά ήρθαν στο προσκήνιο με τη δυνατότητα φωνητικής επικοινωνίας (VoIP π.χ. Skype). Την τελευταία πενταετία, με την ανάπτυξη κατάλληλων τεχνολογιών και ταχύτερων δικτύων, οι πάροχοι υπηρεσιών OTT έχουν εισέλθει πολύ δυναμικά στην παροχή πολυμεσικού περιεχομένου, εκτοπίζοντας τα κλασσικά μοντέλα διανομής περιεχομένου (IPTV), τα οποία εν γένει προσφέρονται στα περιορισμένα πλαίσια κάθε ISP. Οι δύο σημαντικότεροι είναι το Netflix [6], το οποίο διαμοιράζει εμπορικό πολυμεσικό περιεχόμενο και το YouTube [7], το οποίο δίνει βήμα σε περιεχόμενο που έχει δημιουργηθεί από χρήστες. Την ίδια στιγμή, οι μεγάλοι παραγωγοί περιεχομένου (κινηματογραφικά στούντιο, ειδησεογραφικά πρακτορεία), τα τηλεοπτικά κανάλια και οι πάροχοι υπηρεσιών Διαδικτύου προσπαθούν να βρουν το ρόλο τους, καθώς βλέπουν τα έσοδά τους να συρρικνώνονται, και να συμμετάσχουν στη νομή των κερδών της αναπτυσσόμενης αυτής αγοράς.

Οι προκλήσεις που πρέπει να αντιμετωπιστούν είναι πολλές και μεγάλες. Η ίδια η πολλαπλότητα τρόπων πρόσβασης στο περιεχόμενο – διαφορετικά χαρακτηριστικά δικτύων πρόσβασης και συσκευών (μέγεθος οθόνης, υπολογιστική ισχύς, αποθηκευτικός χώρος) έχει αντίκτυπο στις προσπάθειες προτυποποίησης του πολυμεσικού περιεχομένου, ενώ οι διαρκώς αυξανόμενες απαιτήσεις των χρηστών για αξιόπιστο, υψηλής ευκρίνειας περιεχόμενο, ανεξαρτήτως συνθηκών πρόσβασης, εγείρουν ερωτήματα σχετικά με τη χωρητικότητα και την επεκτασιμότητα των δικτύων πρόσβασης και αναγκάζουν τους τηλεπικοινωνιακούς παρόχους να επαγρυπνούν για την ικανοποίησή των αναγκών αυτών, χωρίς παράλληλα εγγυημένα κέρδη.

Τα ζητήματα που ενέκυψαν λόγω των διαφορετικών ποιοτήτων βίντεο, που παραδίδονται σε ένα εύρος ανομοιογενών τερματικών πάνω από ετερογενή δίκτυα πρόσβασης έχουν εξεταστεί σε διάφορες λύσεις κωδικοποίησης βίντεο. Οι λύσεις αυτές περιλαμβάνουν τις Κωδικοποιήσεις Κλιμακώσιμου Βίντεο (Scalable Video Coding - SVC)

και Πολλαπλής Θέασης (Multi-view Coding - MVC), που αποτελούν επεκτάσεις του προτύπου H.264/MPEG-4 Advanced Video Coding (AVC) [8], και οι οποίες υποστηρίζουν αντίστοιχα την κωδικοποίηση σε διάφορα ιεραρχικά επίπεδα ποιότητας και την κωδικοποίηση διαφορετικών θεάσεων. Πιο πρόσφατα οι προβληματισμοί αυτοί έχουν ληφθεί υπόψη στο πρότυπο High Efficiency Video Coding (HEVC) [9], το οποίο τη στιγμή αυτή βρίσκεται υπό διαμόρφωση[1].

Όσον αφορά την επεκτασιμότητα, η απουσία εγγενούς υποστήριξη της πολυεκπομπής (IP Multicast) στο Διαδίκτυο έχει οδηγήσει στην ευδοκίμηση εταιριών που διαθέτουν ιδιωτικά δίκτυα επικάλυψης (overlay networks). Τα δίκτυα αυτά συνήθως εφαρμόζουν δενδρικές κατανομές Application Layer Multicast (ALM) [10] που καλύπτουν ένα μεγάλο αριθμό Αυτόνομων Συστημάτων (Autonomous Systems – AS), και οι οποίες είναι σήμερα υπεύθυνες για τη διανομή του περιεχομένου ενός σημαντικού αριθμού παρόχων. Με τη χρήση αυτών των δικτύων αποφεύγεται η συμφόρηση πλησίον του διακομιστή του παρόχου και καθίσταται δυνατή η ευρύτερη γεωγραφική κάλυψη της διανομής.

Η εισαγωγή ταχύτερων δικτύων πρόσβασης, σε συνδυασμό με την ολοένα και μεγαλύτερη επεξεργαστική ισχύ και αποθηκευτική δυνατότητα των τερματικών, έδωσε τη δυνατότητα εφαρμογής σε μια άλλη λύση στο επίπεδο του στρώματος εφαρμογής, η οποία έχει αποκτήσει μεγάλη δημοτικότητα την τελευταία δεκαετία. Η λύση αυτή τροποποιεί το κλασσικό μοντέλο πελάτη-εξυπηρετητή για να επιτρέψει την ανταλλαγή δεδομένων (και γενικότερα πόρων) σε ένα δίκτυο ομότιμων κόμβων (Peer-to-Peer ή P2P). Τα συστήματα αυτά αποτελούν ένα δίκτυο επικάλυψης ομότιμων κόμβων, όπου κάθε κόμβος χαρακτηρίζεται σαν «παραγωγοκαταναλωτής» (prosumer), δηλαδή δρα και ως εξυπηρετητής (που παρέχει υπηρεσίες σε άλλους ομότιμους) και ως πελάτης (που καταναλώνει πόρους από άλλους ομότιμους).

Σε αυτή την μετάβαση από την κλασική, «μονοπωλιακή» τηλεοπτική εκπομπή προς μια μη-γραμμική, κατά παραγγελία του χρήστη, ανά πάσα στιγμή, τοποθεσία και τύπο συσκευής, κατανάλωση οπτικοακουστικού υλικού, η τεχνολογία P2P μπορεί να αποτελέσει μία από τις επιτρεπτικές υποδομές τόσο της διαδικασίας ψηφιακής σύγκλισης όσο και της βιομηχανίας του θεάματος, και όχι ο κύριος εχθρός της, όπως

[1] Μία πρώτη έκδοση του προτύπου διατέθηκε εντός του 2013

αρχικά είχε θεωρηθεί, λόγω της ευρείας χρήσης της με σκοπό την πειρατεία πολυμεσικού περιεχομένου.

Επί του παρόντος, το BitTorrent [11] αποτελεί μία από τις πιο δημοφιλείς λύσεις P2P. Έχει σχεδιαστεί με σκοπό την διάθεση αρχείων σε μεγάλη κλίμακα, δίνοντας ιδιαίτερο βάρος στην επεκτασιμότητα της διανομής. Τα δεδομένα προς διανομή αρχικά τεμαχίζονται σε μικρότερα τμήματα, τα οποία στη συνέχεια παραδίδονται στους ομότιμους με ένα μη-σειριακό τρόπο. Πρόσφατα οι κυριότερες υλοποιήσεις P2P εξελίχθηκαν, προσφέροντας υποστήριξη στην ανταλλαγή περιεχομένου σε πραγματικό χρόνο [12]. Στην πράξη, με κατάλληλες προσαρμογές, το πρωτόκολλο P2P μπορεί να αλλάξει τον τρόπο διανομής οπτικοακουστικού υλικού σε πραγματικό χρόνο μέσω του Διαδικτύου.

Η ερευνητική δραστηριότητα με αντικείμενο τη χρήση του κλασσικού πρωτόκολλου HTTP για τη μετάδοση πολυμέσων στο Διαδίκτυο, είχε σαν αποτέλεσμα την ανάπτυξη μιας τεχνικής, η οποία ονομάζεται προσαρμοσμένη μετάδοση ροών πολυμεσικού περιεχομένου πάνω από HTTP (HTTP Adaptive Streaming), και η οποία — σύμφωνα με το φόρουμ Open IPTV— καθιστά εφικτή την ανάπτυξη καινοτόμων, συναρπαστικών, συγκλινουσών υπηρεσιών ψυχαγωγίας σε συσκευές τηλεόρασης, ταμπλέτες και κινητά [13].

Ο συνδυασμός της Κωδικοποίησης Κλιμακούμενου Βίντεο (SVC), των δικτύων P2P και των διαδικτυακών τεχνολογιών για τη μετάδοση υψηλής ποιότητας, ζωντανού και ετεροχρονισμένου, πολυμεσικού περιεχομένου, αποτελεί ένα πεδίο καινοτομίας, το οποίο επιτρέπει την ανάπτυξη ενός παγκόσμιου οικοσυστήματος διανομής περιεχομένου. Το οικοσύστημα αυτό εκτείνεται από τα στοιχεία υποδομής, όπως π.χ. διαδικτυακοί αποθηκευτικοί χώροι και κόμβοι Δικτύων Διανομής Περιεχομένου (CDN), έως το επίπεδο εφαρμογών, π.χ. ευφυείς πελάτες κατανάλωσης πολυμεσικού περιεχομένου μέσω HTML5.

Υπό αυτό το πρίσμα, η ποιότητα των διανεμόμενων πολυμέσων πάει ένα βήμα παραπέρα από την απλή αξιολόγηση της Ποιότητας Υπηρεσίας (Quality of Service QoS) και της Ποιότητας Εμπειρίας (Quality of Experience - QoE), οι οποίες αποτελούν τις δύο όψεις του ίδιου νομίσματος (μία αντικειμενική από την πλευρά του παρόχου και μία υποκειμενική από την πλευρά του χρήστη). Πλέον δίνεται μεγάλος βάρος στην αντιληπτή ποιότητα υπηρεσίας (Quality of Perception - QoP) [14] του χρήστη, η οποία

αποτελεί ένδειξη της ποιότητας της υπηρεσίας, όπως την αντιλαμβάνεται ο χρήστης. Η αντιληπτή ποιότητα υπηρεσίας και η ποιότητα της εμπειρίας εξετάζουν την ποιότητα από την πλευρά του χρήστη, διαφέροντας όμως στα δεδομένα που χρησιμοποιούν. Η αντιληπτή ποιότητα υπηρεσίας επηρεάζεται τόσο από την αντικειμενική επίδοση δικτυακών στοιχείων και τερματικών συσκευών όσο και από υποκειμενικούς ψυχολογικούς παράγοντες (προσδοκίες, διάθεση) και το εξωτερικό περιβάλλον χρήσης. Συνεπώς, για να εξεταστεί η αντιληπτή ποιότητα υπηρεσίας σε υπηρεσίες πολυμέσων, θα πρέπει να πάμε ένα βήμα παραπέρα από την επίγνωση της ποιότητας της υπηρεσίας κατά τη διάρκεια της μετάδοσης και να συμπεριλάβουμε στις μετρήσεις μας τους παραπάνω παράγοντες.

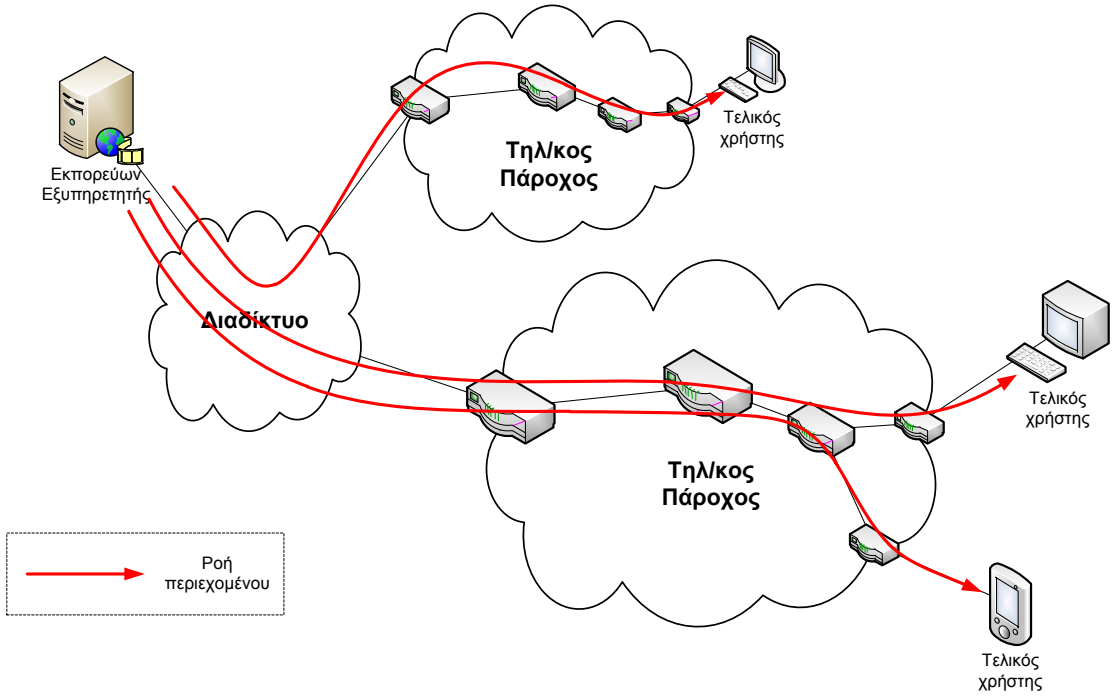
Η αξιολόγηση της αντιληπτής ποιότητας υπηρεσίας απαιτεί νέες μεθοδολογίες αξιολόγησης, οι οποίες θα θέτουν στο επίκεντρο τον χρήστη. Η συνήθης πρακτική είναι η χρήση μιας υποκειμενικής κλίμακας, όπως για παράδειγμα το Mean Opinion Score - MOS [15], στο οποίο η ποιότητα βαθμολογείται από 1 (χαμηλότερη) έως 5 (υψηλότερη). Σε τελική ανάλυση, η επιτυχία μιας υπηρεσίας καθορίζεται από την εμπειρία του χρήστη με αυτή. Σε αυτό το πλαίσιο, είναι σημαντικό οι διάφορες εξελισσόμενες τεχνολογίες να συνδυαστούν με ένα συνεπή και ενορχηστρωμένο τρόπο με απώτερο στόχο τη βελτίωση της εμπειρίας του χρήστη.

2.2 Διανομή σύμφωνα με το μοντέλο πελάτη - εξυπηρετητή

Καταρχήν πρέπει να γίνει μία διάκριση μεταξύ των λεγόμενων μη-γραμμικών υπηρεσιών, όπως το βίντεο κατά παραγγελία (Video-on-Demand - VoD) και η υπηρεσία φωνής πάνω από IP (VoIP) από τη μία, και των γραμμικών υπηρεσιών (τηλεοπτική μετάδοση) από την άλλη. Οι γραμμικές υπηρεσίες περιλαμβάνουν όλες τις μεταδόσεις, οι οποίες δεν ενεργοποιούνται από τον ίδιο τον καταναλωτή, αποτελώντας κατά λέξη εκπομπές, ανεξαρτήτως εάν η τεχνολογία που χρησιμοποιείται για την μετάδοση βασίζεται στην παράδοση μέσω του Διαδικτύου ή δικτύων κινητής τηλεφωνίας, μέσω Multicast ή Unicast, μέσω P2P ή άλλων τεχνολογιών. Οι γραμμικές υπηρεσίες διέπονται από τους ίδιους κανόνες, ανεξαρτήτως των τεχνικών μετάδοσης του σήματος (over-the-air, μέσω δορυφόρου, καλωδιακή, ευρυζωνική σύνδεση, μικροκυματική ζεύξη, τηλεφωνική γραμμή) και των ιδιαιτεροτήτων του δέκτη (μέγεθος και ανάλυση της

οθόνης κλπ). Αντιθέτως στις μη-γραμμικές υπηρεσίες η παροχή των υπηρεσιών διαφοροποιείται ανάλογα με το τερματικό και τον τρόπο μετάδοσης.

Το πλέον κλασσικό μοντέλο για την μετάδοση ροών πολυμέσων πάνω από IP δίκτυα (και το Διαδίκτυο) είναι η αρχιτεκτονική πελάτη-εξυπηρετητή (client-server model), το οποίο προδιαγράφηκε για την επικοινωνία απομακρυσμένων υπολογιστών στα τέλη της δεκαετίας του '60 [16]. Σε αυτό το μοντέλο, ο εξυπηρετητής δίνει στέγη στο περιεχόμενο, ο πελάτης αιτείται το επιθυμητό περιεχόμενο και τα πολυμέσα, που επιλέγει, μεταφορτώνονται στον πελάτη από το συγκεκριμένο εξυπηρετητή (Σχήμα 2). Το εύρος ζώνης πρόσβασης και άλλες παράμετροι που σχετίζονται με την υπολογιστική ισχύ και τη διαθέσιμή μνήμη του εξυπηρετητή αποτελούν τους πλέον περιοριστικούς παράγοντες όσον αφορά την επεκτασιμότητα του συστήματος, καθώς επηρεάζουν άμεσα τη διαθεσιμότητα και την ποιότητα της προσφερόμενης υπηρεσίας.



Σχήμα 2 Διανομή περιεχομένου στο μοντέλο Client-Server

Οι υπηρεσίες ροών πολυμέσων πάνω από IP δίκτυα χρησιμοποιούν Unicast ή Multicast τρόπους μετάδοσης· ο δεύτερος, στην περίπτωση όπου πολλοί κόμβοι-πελάτες ζητούν (και λαμβάνουν) ταυτόχρονα την ίδια ροή από έναν κόμβο εξυπηρετητή. Το Multicast είναι μια μέθοδος για τη μετάδοση IP datagrams από μία πηγή σε μια ομάδα δεκτών

αποφεύγοντας την άσκοπη επανάληψη, που επιφέρει το μοντέλο Unicast, όπου για κάθε δέκτη υπάρχει και ξεχωριστή ροή. Το Multicast είναι ένα εξειδικευμένο πρωτόκολλο που μπορεί να εγκατασταθεί σε διαφορετικά επίπεδα του OSI (με πλέον συνήθη τα επίπεδα δικτύου και εφαρμογής). Παρόλη την αξία του, η εξάπλωση του IP Multicast με τη σημερινή του μορφή και οι εφαρμογές του είναι περιορισμένες, για μια σειρά από (διαχειριστικούς κυρίως) λόγους όπως οι κατακερματισμένες λύσεις αναφορικά με την ποιότητα της υπηρεσίας, ζητήματα ασφαλείας σχετιζόμενα με επιθέσεις Άρνησης Υπηρεσίας (Denial of Service – DoS) [17], αυξημένα λειτουργικά έξοδα για την απαιτούμενη υποδομή κ.α. Αυτοί οι περιορισμοί έχουν εμποδίσει την εφαρμογή του IP Multicast σε ευρεία κλίμακα στο Διαδίκτυο, καθώς και την υποστήριξή του από τους παρόχους υπηρεσιών Διαδικτύου. Συνήθως το πρωτόκολλο χρησιμοποιείται από παρόχους υπηρεσιών IPTV, αλλά συνήθως περιορίζεται στην διαχείριση των δικτύων διανομής τους.

Η αρχική προσέγγιση για τις ροές (κατ' ευφημισμό, καθώς δεν αποτελούσαν ροές) πολυμέσων ήταν ο κατακερματισμός του πολυμεσικού αρχείου και η τμηματική αποστολή του (σαν απλό αρχείο) μέσω HTTP στον πελάτη, όπου το τεμαχισμένο αρχείο αποθηκευόταν σε έναν ενταμιευτή και αναπαραγόταν, μόλις συμπληρωνόταν επαρκής αριθμός τεμαχίων. Η μέθοδός αυτή – παραλλαγή της οποίας χρησιμοποιήθηκε στο YouTube – ονομάζεται προοδευτική μεταφόρτωση (progressive download). Η διάθεση κατάλληλων εφαρμογών αναπαραγωγής πολυμέσων και η δυνατότητα χρήσης κοινών εξυπηρετητών Διαδικτύου για την αποθήκευση των ροών συνέτειναν στη δημοφιλία της λύσης. Αν και πρακτική, αυτή η μέθοδος δεν επιτρέπει κύριες λειτουργίες αναπαραγωγής, όπως η αναζήτηση στο χρόνο, η γρήγορη προώθηση, ενώ ένα άλλο μειονέκτημα ήταν η συνέχιση της μεταφόρτωσης (έως την πλήρωση του ενταμιευτή), ακόμα και στην περίπτωση που ο χρήστης είχε διακόψει την αναπαραγωγή, επιφέροντας αχρείαστο δικτυακό φόρτο. Τέλος, η προοδευτική μεταφόρτωση αντιμετωπίστηκε διστακτικά από τους παρόχους περιεχομένου, καθώς το περιεχόμενο πρακτικά αποθηκεύτεται στο τερματικό του χρήστη.

Στη συνέχεια, και προκειμένου να αντιμετωπιστούν οι ανάγκες αυτές, υιοθετήθηκε το πρωτόκολλο Real-Time Transport Protocol (RTP) το οποίο υποστηρίζει Unicast και Multicast ροές, προσφέροντας αξιόπιστες υπηρεσίες πολυμέσων με αντίτιμο το κόστος εξειδικευμένων υποδομών εξυπηρετητών και την περιορισμένη διείσδυση σε

τείχη προστασίας (firewalls). Λόγω αυτών των ζητημάτων δεν κατόρθωσε να τύχει ευρείας αποδοχής σε βάθος χρόνου.

Με την εμφάνιση φορητών συσκευών όπως τα smartphones και τα tablets, ικανών να αποκωδικοποιούν και να αναπαράγουν σε συνεχή ροή ταινίες υψηλής ποιότητας, και με δεδομένα τα προβλήματα και τις ελλείψεις των προαναφερθεισών προσεγγίσεων, ήρθε στο προσκήνιο η τεχνολογία της προσαρμοσμένης μετάδοσης ροών πολυμεσικού περιεχομένου πάνω από HTTP, στην οποία η ποιότητα του πολυμέσου προσαρμόζεται δυναμικά ανάλογα με τις δυνατότητες των συσκευών και τις συνθήκες των υποκείμενων δικτύων. Η βασική ιδέα πίσω από το HTTP Adaptive Streaming είναι η κατάτμηση και διάθεση των πολυμέσων σε πολλαπλές ποιότητες και η ικανότητα του πελάτη να αιτείται ανά πάσα στιγμή την κατάλληλη ποιότητα, ανάλογα τις συνθήκες της μετάδοσης. Η τεχνική αυτή συνδυάζει τα οφέλη των δύο προηγούμενων προσεγγίσεων (χρήση κοινών εξυπηρετητών Διαδικτύου, παράκαμψη firewalls, πλήρεις λειτουργικότητες αναπαραγωγής).

Παραλλαγές της αρχιτεκτονικής πελάτη-εξυπηρετητή, οι οποίες στοχεύουν να παρακάμψουν τους περιορισμούς επεκτασιμότητας του αρχικού μοντέλου, αποτελούν η προσέγγιση των CDN και πολύ πρόσφατα η προσέγγιση των Δικτύων ICN, οι οποίες δίνουν έμφαση στο πολυμεσικό περιεχόμενο.

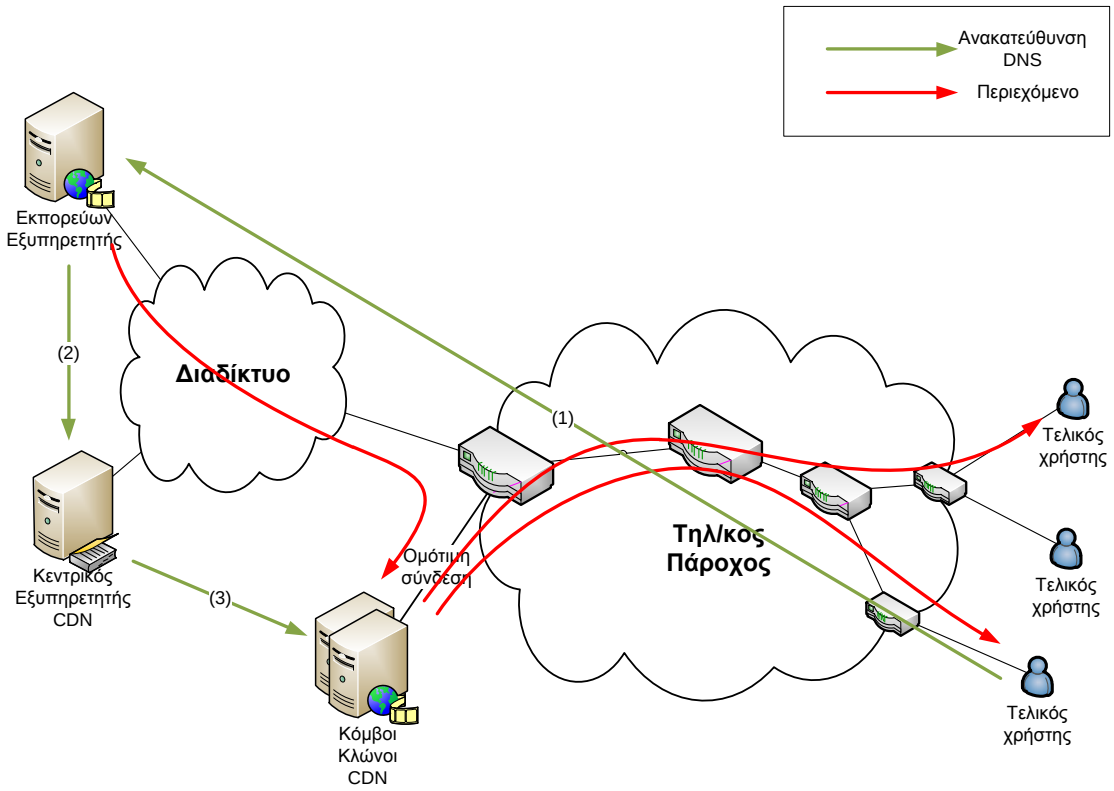
2.3 Δίκτυα Διανομής Περιεχομένου

Με την έκρηξη του παγκόσμιου ιστού, ένας αριθμός ιστοσελίδων παροχής περιεχομένου (ειδησεογραφικά portals, μηχανές αναζήτησης) έγιναν κεντρικά στην τοπολογία του Παγκόσμιου Ιστού (πολλοί σύνδεσμοι κατέληγαν σε αυτά). Καθώς η δημοφιλία των παρόχων περιεχομένου αυξανόταν, η —ολοένα και μεγαλύτερη— βάση χρηστών ερχόταν αντιμέτωπη με καθυστερήσεις (ή ακόμη και μη διαθεσιμότητα) λόγω του υπερβολικού φόρτου εργασίας του εξυπηρετητή και της κυκλοφοριακής συμφόρησης στο Διαδίκτυο. Το πρόβλημα έγινε πιο εμφανές, με την εισαγωγή των πολυμέσων και τις πρώτες ζωντανές μεταδόσεις που πραγματοποιήθηκαν [18]. Απλές λύσεις, όπως π.χ. η αύξηση της υποδομής του δικτύου και του αριθμού των διακομιστών δεν ήταν τεχνοοικονομικά βιώσιμες. Αφενός η ζήτηση είναι δύσκολο να προβλεφθεί και αφετέρου η προσθήκη εξυπηρετητών για την αντιμετώπιση της κυκλοφορίας αιχμής —ιδίως εάν λάβουμε υπόψη ότι τη συγκεκριμένη εποχή (1999) δεν υπήρχαν ιδεατά δίκτυα και

εξυπηρετητές, τα οποία κλιμακώνουν με ευκολία— ήταν μια ιδιαιτέρα δυσκίνητη και δαπανηρή διαδικασία.

Εκείνη την εποχή ήρθαν στο προσκήνιο οι πρώτοι πάροχοι CDN. Με την ανάπτυξη ενός δικτύου επικάλυψης κατανεμημένων ακραίων εξυπηρετητών (που ονομάζονται επίσης υποκατάστατα ή αντίγραφα) και τεχνικών ανακατεύθυνσης DNS ή, πιο σπάνια, ανακατεύθυνσης HTTP και επανεγγραφής των URLs, προκειμένου να ανακατευθύνουν τα αιτήματα σε ένα υποκατάστατο εξυπηρετητή, τα CDNs είναι σε θέση να αντιμετωπίσουν τις ακραίες περιπτώσεις ζήτησης, κάτι που επιτρέπει ταυτόχρονα την επεκτασιμότητα και την εγγυημένη απόδοση. Ένας χρήστης ανακατευθύνεται στο βέλτιστο υποκατάστατο εξυπηρετητή, βάσει κριτηρίων όπως η κατάσταση του δικτύου (π.χ. καθυστέρηση, απώλεια πακέτων), μετρήσεις του φορτίου του διακομιστή, καθώς και η γεωγραφική θέση του χρήστη. Η όλη διαδικασία —που απεικονίζεται στο Σχήμα 3— είναι διαφανής για το χρήστη, ο οποίος δε χρειάζεται να προβεί σε οποιαδήποτε ρύθμιση, όπως απαιτείται στην περίπτωση των δικτυακών διακομιστών μεσολάβησης (web proxies).

Οι πάροχοι περιεχομένου αρχικά και οι πάροχοι υπερκείμενων υπηρεσιών εν συνεχεία επωφελήθηκαν καθώς δεν απαιτούνταν πλέον επενδύσεις σε δαπανηρές υποδομές, ενώ και οι χρήστες τους βίωσαν βελτίωση της ποιότητας με όρους απόδοσης, καθυστέρησης κλπ. Οι τηλεπικοινωνιακοί πάροχοι καλωσόρισαν επίσης τα CDNs, καθώς, τους επέτρεπαν να μειώσουν τα λειτουργικά κόστη λόγω του τοπικά αποθηκευμένου περιεχομένου, αλλά και να ελαχιστοποιήσουν το ρυθμό απώλειας πελατών (churn rate) που οφείλεται σε ανεπαρκή ποιότητα των παρεχόμενων υπηρεσιών. Σε δεύτερο επίπεδο, τα CDNs ενισχύουν επίσης την ασφάλεια στο διαδίκτυο, καθώς η κατανομή των πόρων, που παρέχουν οι εξυπηρετητές υποκατάστατα, λειτουργεί ως φυσική ασπίδα σε επιθέσεις DoS. Το επικρατέστερο επιχειρηματικό μοντέλο συνεπάγεται επιμερισμό του κόστος στους παρόχους περιεχομένου, ενώ άλλα μοντέλα μοιράζουν τα κόστη μεταξύ των τηλεπικοινωνιακών παρόχων και των παρόχων περιεχομένου.



Σχήμα 3 Διανομή περιεχομένου με τη χρήση CDN

Τα CDNs εξυπηρετούν σήμερα ένα σημαντικό τμήμα της κίνησης στο Διαδίκτυο – η Akamai μόνο ισχυρίζεται ότι εξυπηρετεί το 15% με 30% της κίνησης στο Διαδίκτυο [19]. Ειδικά η διανομή πολυμέσων (κατά κύριο λόγο βίντεο) γίνεται εφικτή μέσω της εντατικής χρήσης των CDNs. Οι σημαντικές εμπορικοί πάροχοι CDN περιλαμβάνουν τις Akamai, EdgeCast, Limelight Networks, Level3, οι οποίες διαφέρουν τόσο στα επιχειρηματικά μοντέλα όσο και τη γεωγραφική κάλυψη. Ενώ οι ακαδημαϊκοί τους ομόλογοί τους όπως το CoDeen, και το CoralCDN – τα οποία στεγάζονται σε εξυπηρετητές PlanetLab, έχουν μια πιο πειραματική φύση και σκοπό τον εκδημοκρατισμό της διανομής περιεχομένου.

Στην πραγματοποιηθείσα έρευνα αναπτύχθηκαν εξελιγμένοι αλγόριθμοι για να παρέχουν λύσεις σε προβλήματα, όπως η τοποθέτηση των υποκατάστατων εξυπηρετητών (server placement), η συμπλήρωση της cache (cache population), η αντικατάσταση του περιεχομένου της αποθηκευτικής μνήμης (cache replacement), κλπ. Η τοποθέτηση εξυπηρετητών υποκατάστατων με βέλτιστο τρόπο στοχεύει στην ελαχιστοποίηση του συνολικού κόστους —στη βιβλιογραφία είναι γνωστό ως πρόβλημα ελάχιστου K-Median [20]. Από τους δημοφιλέστερους αλγορίθμους είναι ο άπληστος (greedy) —όπου οι εξυπηρετητές τοποθετούνται με διαδοχικές προσεγγίσεις, κάθε φορά

επιλέγεται αυτός με το ελάχιστο κόστος, ο βασισμένος σε δενδρική δομή (tree-based), ο οποίος τοποθετεί εξυπηρετητές με βέλτιστο τρόπο σε δενδρικές τοπολογίες, ο τυχαίος (random) και ο Hot-Spot, όπου οι εξυπηρετητές υποκατάστατα τοποθετούνται πλησίον των πελατών που δημιουργούν το μεγαλύτερο φόρτο.

Στην πράξη, η στρατηγική τοποθέτησης των εξυπηρετητών επηρεάζεται από τον επιλεχθέντα τρόπο ανάπτυξης του παρόχου CDN. Τα κατανεμημένα CDNs, που καλύπτουν πάνω από ένα πάροχο (multi-ISP) αναπτύσσουν στρατηγικά τους ακραίους εξυπηρετητές όσο το δυνατόν πιο κοντά στον τελικό χρήστη —σε datacenters των τηλεπικοινωνιακών παρόχων ή σημεία ανταλλαγής κίνησης (peering points) σε όλο τον κόσμο. Άλλοι πάροχοι CDN ακολουθούν μία πιο συγκεντρωτική προσέγγιση (single-ISP), όπου οι εξυπηρετητές υποκατάστατα τοποθετούνται εντός της περιοχής κάλυψης ενός ISP. Η δεύτερη προσέγγιση ακολουθείται κυρίως από παρόχους δικτύου που επεκτάθηκαν στην παροχή υπηρεσιών CDN, προκειμένου να βελτιώσουν τις υπηρεσίες που παρέχουν στους χρήστες τους.

Η πλήρης αναπαραγωγή του περιεχομένου των αρχικών εξυπηρετητών παρουσιάζεται ως η απλούστερη προσέγγιση, αλλά δεν είναι πρακτική από άποψη κόστους. Έτσι, τα προβλήματα της τοποθέτησης του περιεχομένου και της αντικατάστασής του είναι ζωτικής σημασίας για την αποτελεσματικότητα των CDNs, ειδικά εκείνων που έχουν επικεντρώνουν στο περιεχόμενο που δημιουργείται από τους χρήστες (User Generated Content - UGC). Η δημοτικότητα του περιεχομένου τείνει να τηρεί την αρχή του Pareto (γνωστή και ως κανόνας 80-20), η οποία αναφέρει ότι το 80% των αιτήσεων κατευθύνεται προς το 20% πιο δημοφιλές περιεχόμενο. Αυτό επιτρέπει την προσωρινή αποθήκευση του περιεχομένου που είναι πιο πιθανό να ζητηθεί από τους χρήστες. Οι αλγόριθμοι αντικατάστασης της μνήμης αποθήκευσης περιλαμβάνουν ενδεικτικά τους λιγότερο-συχνά-χρησιμοποιούμενη (Least Frequently Used - LFU), λιγότερο-πρόσφατα-χρησιμοποιημένη (Least Recently Used - LRU), και First In First Out - FIFO.

Παρά τα προαναφερθέντα οφέλη, η κλασσική προσέγγιση των CDNs εξακολουθεί να έχει μια σειρά από εγγενείς περιορισμούς, τόσο από τεχνικής όσο και από οικονομικής πλευράς. Οι πάροχοι CDN δεν διασυνδέονται —αυτό σημαίνει ότι το περιεχόμενο, το οποίο είναι διαθέσιμο (μέσω ενός CDN) προς τον τελικό χρήστη, εξαρτάται από τις συμφωνίες ανταλλαγής κίνησης του τηλεπικοινωνιακού παρόχου του

χρήστη. Ένα άλλο μειονέκτημα του επιχειρηματικού μοντέλου είναι ότι το παρεχόμενο περιεχόμενο καλύπτεται από συμβόλαιο. Το μη συμβεβλημένο περιεχόμενο είναι προσβάσιμο από το διακομιστή προέλευσης, με όλες τις συνέπειες που αυτό συνεπάγεται. Εκτός αυτών, νεότερες μελέτες δείχνουν ότι το κόστος για τους παρόχους OTT υπηρεσιών καθίσταται μη βιώσιμο, καθώς αυξάνει η ζήτηση των χρηστών, διότι, σε αντίθεση με την παραδοσιακή ευρυζωνική τηλεοπτική μετάδοση, κάθε επιπλέον χρήστης επιφέρει μια αύξηση του κόστους [21].

Αναγνωρίζοντας τα παραπάνω, μια πληθώρα εξελίξεων λαμβάνει χώρα στο οικοσύστημα της διανομής πολυμέσων. Βασικοί φορείς παροχής υπηρεσιών OTT (συμπεριλαμβανομένων των YouTube, Netflix και Amazon) επιλέγουν να εγκαταστήσουν ιδιόκτητα Δίκτυα CDN και σταδιακά να ανεξαρτητοποιηθούν από τα παραδοσιακά Δίκτυα CDN. Οι πάροχοι υπηρεσιών Διαδικτύου (ISPs) έχουν επίσης ξεκινήσει την ανάπτυξη ιδιόκτητων Δικτύων CDN, προκειμένου εισέλθουν στην αγορά της παροχής πολυμεσικών υπηρεσιών και να αποκτήσουν ένα μερίδιο των εσόδων της [22]. Μια τέτοια κίνηση επιτρέπει την προσωρινή αποθήκευση βαθύτερα στο δίκτυο και ολοένα και πιο κοντά στον τελικό χρήστη. Οι παραδοσιακοί πάροχοι CDN, από την άλλη πλευρά, επεκτείνουν την παρουσία τους στον τομέα των κινητών και του υπολογιστικού σύννεφου (cloud), ενώ στη διανομή πολυμέσων προσφέρουν ολοκληρωμένες λύσεις, οι οποίες δεν περιορίζονται σε απλή παράδοση του περιεχομένου, αλλά περιλαμβάνουν το σύνολο της αλυσίδας παραγωγής περιεχομένου. Οι λύσεις αυτές κυμαίνονται από την εξατομίκευση του περιεχομένου για multi-screen συσκευές, την υποστήριξη μια σειράς τεχνολογιών ABR και συστημάτων προστασίας DRM (με δυνατότητα κρυπτογράφησης του αποθηκευμένου περιεχόμενου στο τελικό στάδιο, κοντά στο χρήστη) μέχρι την δημιουργία λεπτομερών εκθέσεων και αναλύσεων σχετικά με την πελατειακή βάση και την χρήση της υπηρεσίας, που αποτελούν πολύτιμη πληροφορία για τους παρόχους περιεχομένου.

Τα CDNs αντιμετωπίζουν νέες προκλήσεις με την εκτίναξη του περιεχομένου που δημιουργείται από χρήστες (User Generated Content - UGC) και την επανάσταση των κοινωνικών δικτύων. Η ευκολία παραγωγής και δημοσίευσης περιεχομένου, και με δεδομένη την ολοκλήρωση των πολυμεσικών ροών στα κοινωνικά δίκτυα, εντείνει τη ζήτηση. Καθίσταται πλέον εύκολο για το περιεχόμενο για να γίνει υπερβολικά δημοφιλές (viral), μια τάση η οποία είναι δύσκολο να προβλεφθεί. Επιπλέον, η

αυξανόμενη ζήτηση για υψηλής ευκρίνειας περιεχόμενο τοποθετεί πρόσθετη επιβάρυνση στα δίκτυα των παρόχων CDN. Καθώς ένας αυξανόμενος αριθμός ISPs αναπτύσσει τα δικά του ιδιόκτητα CDN, πρωτοβουλίες, όπως η CDN-Interconnection Initiative της IETF (CDN-I) [23] αποκτούν ζωτική σημασία.

Αναφορικά με τη διανομή του περιεχομένου εσωτερικά στα CDNs, η τεχνολογία P2P υιοθετείται ολοένα και περισσότερο [24], μετά την επιτυχία των συστημάτων ανταλλαγής αρχείων P2P, η οποία έδωσε το κίνητρο για την χρήση των P2P συστημάτων στη διανομή πολυμεσικού περιεχομένου [25]. Ως αποτέλεσμα, εμφανίστηκε ένα νέο είδος υπηρεσιών γνωστό ως peercasting, οδηγώντας τις παραδοσιακές υπηρεσίες, όπως η τηλεόραση και το ραδιόφωνο στην εποχή P2P, π.χ. διαδικτυακή τηλεόραση βασισμένη σε P2P (P2PTV), P2P διαδικτυακό ραδιόφωνο και P2P ροές μουσικής. Όλες αυτές οι υπηρεσίες, μπορούν να ιδωθούν σαν εφαρμογές που παρέχονται από έναν πάροχο OTT, δημιουργώντας ένα νέο τοπίο στη βιομηχανία του θεάματος και των μέσων ενημέρωσης [26]. Στην επόμενη ενότητα, θα επικεντρώσουμε στα P2P συστήματα και στον τρόπο με τον οποίο μπορούν αυτά να εξυπηρετήσουν τη διανομή πολυμέσων μέσω διαδικτύου.

2.4 Δίκτυα Ομότιμων Κόμβων

Από την αρχή της εμφάνισης του Διαδικτύου έχουν εμφανιστεί αρκετά συστήματα, τα συμπεριφέρονται παρόμοια με τα δίκτυα ομοτίμων κόμβων (P2P), αλλά δεν υποδηλώνουν αυτό που σήμερα έχει επικρατήσει να ονομάζουμε P2P.

Τα συστήματα P2P είναι συνέπεια της ανάπτυξης του Διαδικτύου. Ένα σύστημα P2P είναι ένα κατανεμημένο περιβάλλον που αποτελείται από ένα υπόστρωμα επικοινωνίας που επιτρέπει την ανταλλαγή πληροφοριών μεταξύ ομότιμων κόμβων, εφαρμογές που τρέχουν πάνω από το κατανεμημένο περιβάλλον για την παροχή βασικών υπηρεσιών όπως η διευθυνσιοδότηση, και η δρομολόγηση (εντός του υπερκείμενου δικτύου), καθώς και αλγορίθμους εντοπισμού πόρων. Ένα υπερκείμενο δίκτυο P2P χαρακτηρίζεται συνεπώς ως μια λογική σύνδεση κόμβων, όπου ο ένας οδηγείται στον άλλο με χρήση του υποκείμενου δικτύου IP μέσω κατάλληλης διευθυνσιοδότησης και εξειδικευμένων πρωτοκόλλων διαχείρισης και ανάκτησης περιεχομένου (Σχήμα 4).

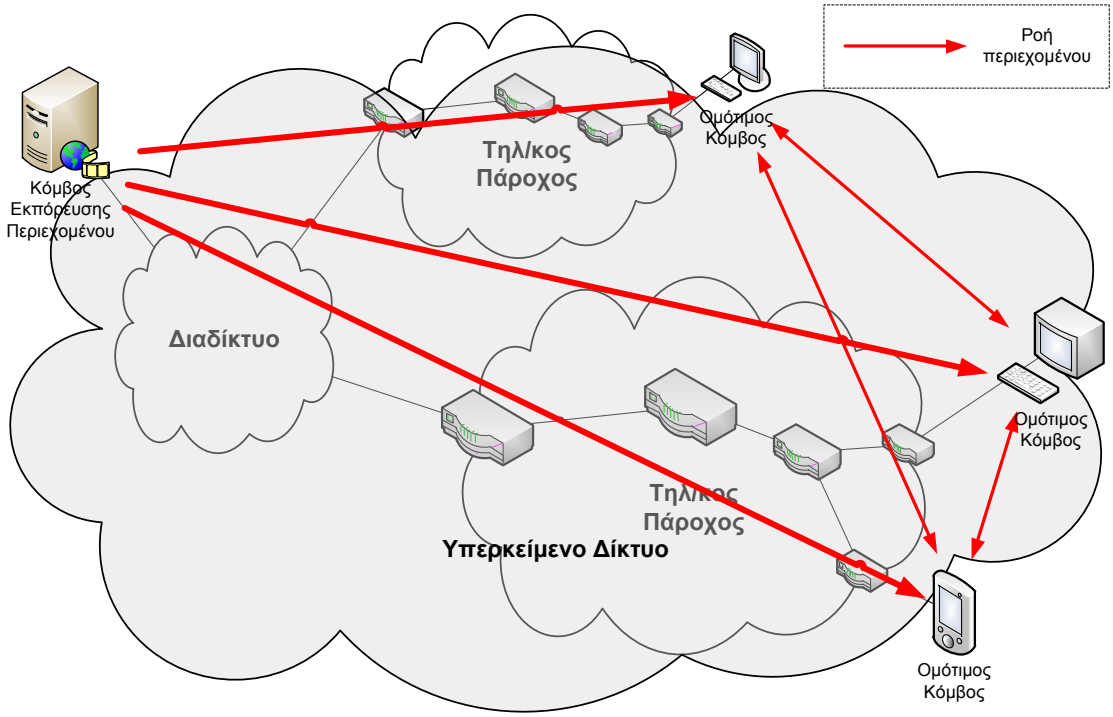
Σήμερα, η κίνηση που προέρχεται από ροές πολυμέσων (στη συντριπτική της πλειονότητα βίντεο) και η κίνηση από πρωτόκολλα P2P είναι μεταξύ των υψηλότερων

στο Διαδίκτυο. Η ραγδαία αύξηση των ροών πολυμέσων στο Διαδίκτυο, συνεπικουρούμενη από την ευκολία παραγωγής πολυμεσικού περιεχομένου από χρήστες, έχει οδηγήσει σε πολλαπλασιασμό της αντίστοιχης κίνησης, η οποία έχει ξεπεράσει εκείνη των P2P συστημάτων στη Β. Αμερική [4], όσον αφορά τις καθοδικές ροές (στις ανοδικές ροές το P2P εξακολουθεί να κρατά τα πρωτεία). Στην Ευρώπη, τα δίκτυα P2P παραμένουν οι φορείς του μεγαλύτερου ποσοστού της δικτυακής κίνησης. Το μεγαλύτερο μέρος της κίνησης που ανταλλάσσεται στα συστήματα P2P αντιστοιχεί σε περιεχόμενο ήχου και βίντεο, όπως μουσική και ταινίες.

Ως γνήσιοι εκπρόσωποι αποκεντρωμένων και κατανεμημένων αρχιτεκτονικών διαδικτύου, οι εφαρμογές P2P αποτελούν ελκυστικές λύσεις για τη μεταφορά των πολυμέσων μέσω του Διαδικτύου για μία σειρά λόγους:

- Δημιουργούν «επικαλύψεις» στο ευρυζωνικό δίκτυο, και δεν απαιτούν κανένα είδος αλλαγής στις υπάρχουσες υποδομές
- Έχουν ένα σχετικά χαμηλό κόστος των υπηρεσιών (ανά παραδιδόμενο GB) σε σύγκριση με τα CDNs
- Έχουν χαμηλό κόστος επένδυσης και συντήρησης (από την πλευρά του παρόχου)
- Είναι επεκτάσιμα σε εκατομμύρια ταυτόχρονους χρήστες —κάθε επιπλέον ομότιμος κόμβος αυξάνει τη διαθεσιμότητα των συνολικών πόρων
- Απουσία μοναδικών σημείων αποτυχίας
- Εισάγουν χαμηλότερο φόρτο στο δίκτυο σε σύγκριση με το Unicast για τον ίδιο σκοπό
- Μπορούν να χρησιμοποιήσουν Multicast τεχνικές —π.χ. ALM— για τη βελτίωση της αποτελεσματικότητας της παράδοσης.

Όπως συνέβη στα πρώτα χρόνια της διανομής πολυμέσων μέσω πρωτοκόλλου IP, η λύση «μεταφόρτωση και εν συνεχεία αναπαραγωγή» προηγήθηκε χρονικά των λύσεων του βίντεο κατά παραγγελία, της κωδικοποίησης σε πραγματικό χρόνο και της χρήσης πολυμεσικών ροών. Το ίδιο συνέβη και με τα συστήματα P2P, όπου η τεράστια επιτυχία των P2P συστημάτων ανταλλαγής αρχείων, αποτέλεσε κίνητρο για την χρήση των P2P προς εξυπηρέτηση της διανομής ροών πολυμεσικού περιεχομένου, κάνοντας πράξη τις υπηρεσίες peercasting.



Σχήμα 4 Ροές πολυμέσων σε σύστημα P2P

Η τεχνολογία P2P είναι σε θέση να αξιοποιήσει κάθε ομότιμο που εντάσσεται σε ένα δίκτυο επικάλυψης και ως κόμβο πελάτη και ως κόμβο εξυπηρετητή. Μια κοινή υπόθεση που γίνεται στα P2P συστήματα είναι ότι όλοι οι ομότιμοι μπορούν (και είναι επίσης πρόθυμοι) να συνεργάζονται για την αναμετάδοση των ροών, θέτοντας τους πόρους τους στη διάθεση του συστήματος (π.χ. ένα μέρος του εύρους ζώνης τους), προκειμένου αυτό να μεταδώσει τις ροές δεδομένων που ήδη κατέχουν σε άλλους κόμβους. Μια άλλη υπόθεση είναι ότι κάθε ροή του συστήματος αντιστοιχεί σε συνεχή ροή πολυμέσων, τα οποία κωδικοποιούνται στην πηγή της ροής. Η πηγή πρέπει να κατακερματίσει τα κωδικοποιημένα πολυμέσα σε μια σειρά από τμήματα, που συνήθως αντιστοιχούν σε διάρκεια λίγων δευτερολέπτων ή σε ένα ορισμένο εύρος bytes, και τα οποία προσδιορίζονται σε ένα αρχείο μεταδεδομένων. Τα τμήματα αυτά αποτελούν τα δομικά στοιχεία της ροής και θα εξαπλωθούν ώστε να είναι διαθέσιμα στους ομότιμους για την αναπαραγωγή της ροής.

Υπάρχουν δύο τυπικά σενάρια εφαρμογής P2P ροών:

- Το σενάριο πραγματικού χρόνου: Όταν οι ομότιμοι κόμβοι ενταχθούν στο δίκτυο, μπορούν να αιτηθούν μόνο για ένα μέρος του «προγράμματος» που διανέμεται,

που αντιστοιχεί στην ανά πάσα στιγμή (μελλοντική) μετάδοση. Το περιεχόμενο που διατίθεται εξαρτάται από τη στιγμή που οι ομότιμοι ενταχθούν στο δίκτυο.

- Το σενάριο βίντεο κατά παραγγελία (VoD): Οι ομότιμοι μπορούν να αιτηθούν όλο το διαθέσιμο περιεχόμενο, όταν θα ενταχθούν στο δίκτυο και, επιπλέον έχουν πρόσβαση σε διαδραστικές λειτουργίες επί του περιεχομένου (Fast Forward, Rewind, Pause, κ.λπ.).

Για τις εταιρίες που δρουν στο χώρο της διαδικτυακής τηλεόρασης, το VoD έχει θεωρηθεί ως το βασικό προϊόν για να προσελκύσουν τους καταναλωτές, δεδομένου ότι επιτρέπει ευελιξία και ευκολία παρακολούθησης, από οποιοδήποτε σημείο του πολυμέσου και ανά πάσα στιγμή.

Ωστόσο, το VoD σε συστήματα P2P έχει κάποια στοιχεία που διαφοροποιούν το σχεδιασμό του σε σχέση με την αντίστοιχη υπηρεσία ζωντανής μετάδοσης. Ενώ σε μια ζωντανή μετάδοση ένας πολύ μεγάλος αριθμός χρηστών παρακολουθούν την ίδια ροή συγχρόνως, στο VoD οι χρήστες μπορούν να παρακολουθούν την ίδια μεν ροή, αλλά με ασύγχρονο τρόπο ως προς τους άλλους χρήστες, βλέποντας δηλαδή διαφορετικά σημεία του ίδιου βίντεο σε οποιαδήποτε δεδομένη στιγμή. Επομένως και με δεδομένους περιορισμούς στη χωρητικότητα των κόμβων, η διαθεσιμότητα των τμημάτων του πολυμέσου στην περίπτωση VoD πιθανότατα δε θα είναι αντίστοιχα υψηλή (σε σχέση με τη ζωντανή μετάδοση).

Οι αρχιτεκτονικές διανομής ροών πολυμέσων πάνω από P2P ακολουθούν είτε δενδρική προσέγγιση είτε προσέγγιση πλέγματος (grid). Η δενδρική προσέγγιση δημιουργεί συνήθως δέντρα Multicast, όπου η ροή πολυμέσων ωθείται κατά μήκος του δένδρου, με αφετηρία την πηγή της ροής. Τα δέντρα Multicast δημιουργούνται στο στρώμα εφαρμογής (αποτελώντας ένα υπερκείμενο Multicast δομημένο πάνω από υποκείμενες Unicast συνδέσεις). Η προσέγγιση πλέγματος δεν παρέχει καμία δομή για την πορεία της διανομής και οι ομότιμοι αυτό-οργανώνονται σε «σμήνη» για να μοιραστούν το περιεχόμενο. Σε αυτή την προσέγγιση κάθε κόμβος διατηρεί έναν κατάλογο με τους ομότιμους με τους οποίους ανταλλάσσει πληροφορίες σχετικά με τη διαθεσιμότητα των δεδομένων και από τους οποίους θα λάβει τα επιθυμητά τμήματα των πολυμέσων.

Η δενδρική προσέγγιση, όπου το περιεχόμενο «σπρώχνεται» προς τον κόμβο που το αιτείται, έχει χρησιμοποιηθεί κυρίως σε εμπορικές εφαρμογές, όπως το PeerCast [27]. Αλλά οι πιο δημοφιλές λύσεις ροών πολυμέσων στηρίζονται στην προσέγγιση πλέγματος, όπου ο κάθε κόμβος «τραβάει» τη ροή που αναζητά, όπως είναι οι περιπτώσεις του SOPCast [28] και του PPLive [29].

Το περιβάλλον στο οποίο λειτουργούν οι περισσότερες εφαρμογές ροών πολυμέσων P2P χαρακτηρίζεται από τις ασύμμετρες ιδιότητες των δικτύων πρόσβασης των ομοτίμων (δηλαδή, το εύρος ζώνης για την καθοδική ζεύξη είναι σημαντικά υψηλότερο από αυτό που διατίθεται για την ανοδική ζεύξη). Αυτή η ασυμμετρία συνεπάγεται ότι το εύρος ζώνης της ανοδικής ζεύξης αποτελεί τον κύριο περιοριστικό παράγοντα για την αποστολή δεδομένων σε άλλους ομότιμους. Για τη μεταφορά αρχείων, ο περιορισμός αυτός αφορά μόνο τη διάρκεια της μετάδοσης, αλλά για τις ροές πολυμέσων έχει σημαντικό αντίκτυπο στην ποιότητα και τη μορφοποίηση των πολυμεσικών ροών.

Σε αυτά τα δίκτυα, οι απώλειες πακέτων συνήθως συμβαίνουν λόγω συμφόρησης του δρομολογητή, σφαλμάτων μετάδοσης στο φυσικό επίπεδο (σε ασύρματα και κινητά δίκτυα), αποχώρησης ενός κόμβου από το υπερκείμενο δίκτυο ή ακόμη και εξαιτίας του αυστηρού χρονικού ορίου λήξης που συνεπάγεται η οπτικοποίηση σε πραγματικό χρόνο.

Οι ραδιοτηλεοπτικοί σταθμοί έχουν το κίνητρο να χρησιμοποιήσουν τεχνολογίες P2P, καθώς αυτές κλιμακώνουν ικανοποιητικά κατά την ταυτόχρονη παροχή υπηρεσιών σε ένα μεγάλο αριθμό ομοτίμων (στην περίπτωσή αυτή τηλεθεατών). Οι επενδύσεις που απαιτούνται σε διακομιστές και εύρος ζώνης, είναι πολύ χαμηλότερες με τη χρήση P2P από ότι με άλλους μηχανισμούς διανομής περιεχομένου. Κατά συνέπεια, η τεχνολογία P2P μπορεί να είναι πιο προσιτή και αποδοτική από αντίστοιχα εναλλακτικά συστήματα διανομής περιεχομένου. Οι εταιρείες CDN, που διαθέτουν επικαλυπτικά δίκτυα με εξυπηρετητές κλώνους σε όλο τον κόσμο και οι οποίοι αντιγράφουν συνεχώς το περιεχόμενο μεταξύ τους, επίσης χρησιμοποιούν υβριδικά συστήματα P2P για τη μεταφορά αυτών των δεδομένων. Επίσης, κατά τη διαδικασία της εξισορρόπησης φορτίου μεταξύ των ακραίων εξυπηρετητών, οι χρήστες, αυτομάτως και διαφανώς, ανακατευθύνονται προς την πλησιέστερη διαθέσιμη «πηγή» έτσι ώστε το δίκτυο να μπορεί να αλλάζει δυναμικά χωρίς αυτό να γίνεται αντιληπτό από τους τελικούς

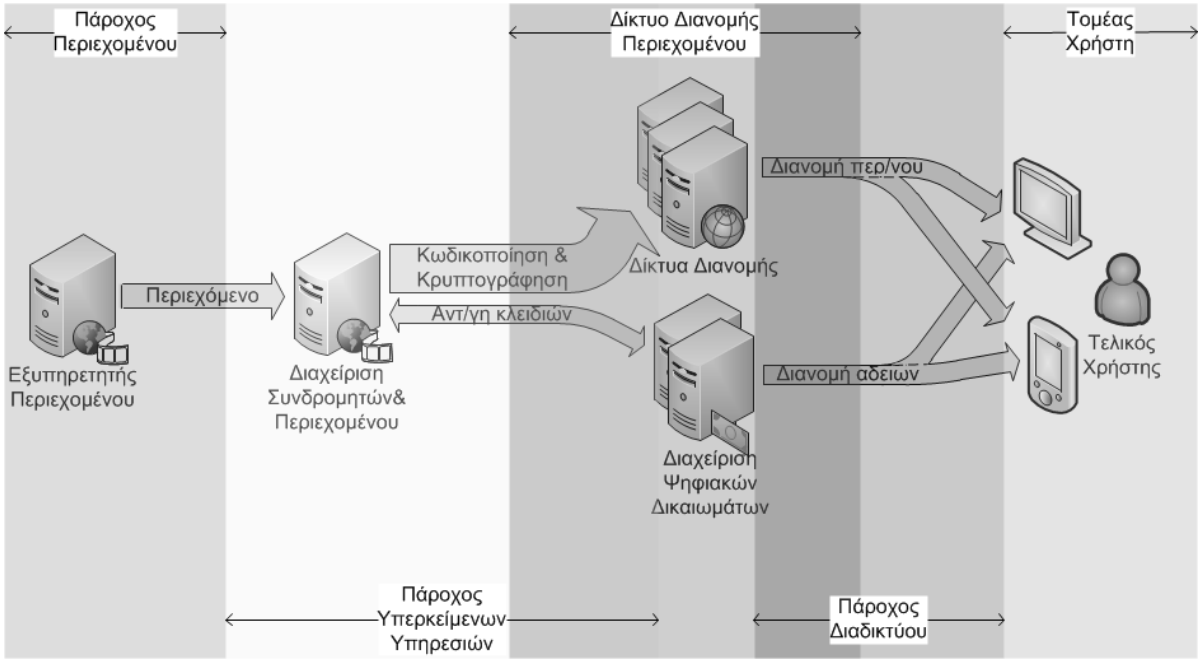
χρήστες (όπως και στην περίπτωση των P2P). Μία μείξη CDN και P2P μπορεί να αποτελέσει ιδανική λύση για την παροχή πολυμεσικού περιεχομένου, συνδυάζοντας τα πλεονεκτήματα των δύο επικαλυπτικών δικτύων. Σε αυτή τη λύση, ο κόμβος CDN θα θεωρείται ως ο προεπιλεγμένος ομότιμος, έχοντας πάντα διαθέσιμα όλα τα τμήματα περιεχομένου, έτσι ώστε όταν ένα τμήμα δεν μπορεί να ανακτηθεί εντός χρόνου από το δίκτυο P2P, να μπορεί να ανακτηθεί άμεσα από το πιο αξιόπιστο, αλλά και πιο δαπανηρό, δίκτυο CDN.

2.5 Τεχνολογίες αιχμής στη διανομή πολυμεσικού περιεχομένου

Στην παρούσα ενότητα παρουσιάζονται —εν συντομία— οι τεχνολογίες αιχμής που αφορούν τη διανομή και προστασία πολυμεσικού περιεχομένου, εστιάζοντας στην περίπτωση της μετάδοσης πολυμεσικών ροών κατά παραγγελία.

Στο Σχήμα 5 παρουσιάζεται μια τυπική αρχιτεκτονική τέτοιου συστήματος. Οι συμμετέχοντες στην αρχιτεκτονική αυτή είναι ο πάροχος περιεχομένου, ο πάροχος υπερκείμενων υπηρεσιών, το δίκτυο διανομής περιεχομένου (CDN), ο πάροχος υπηρεσιών Διαδικτύου και ο τελικός χρήστης. Ο πάροχος περιεχομένου —ως επί το πλείστον κινηματογραφικά στούντιο, ειδησεογραφικοί οργανισμοί ή πιο πρόσφατα και μεμονωμένοι χρήστες— διαθέτει πολυμεσικό περιεχόμενο σε πρωτόλεια μορφή. Ο πάροχος υπερκείμενων υπηρεσιών παρέχει υπηρεσίες πολυμεσικού περιεχομένου μέσω του Διαδικτύου και όχι μέσω ενός ιδιόκτητου δικτύου, το οποίο έχει αυτό τον αποκλειστικό σκοπό (π.χ. ένα δίκτυο IPTV). Ο πάροχος αυτός είναι υπεύθυνος για την κωδικοποίηση και την κρυπτογράφηση του ακατέργαστου περιεχομένου, σε κατάλληλη ποιότητα και μορφή, ώστε να ανταποκριθεί στις απαιτήσεις του τελικού χρήστη, ενώ παράλληλα διαχειρίζεται και τη συνδρομητική βάση. Ο πάροχος υπηρεσιών Διαδικτύου αποτελεί το κανάλι μέσω του οποίου φτάνει το περιεχόμενο στον τελικό χρήστη, αλλά λόγω της υπερκείμενης λειτουργίας του παρόχου OTT, αν και εμφανίζεται στο Σχήμα 5, δε συμμετέχει ενεργά στη διαδικασία διανομής. Άλλωστε, όπως θα τονισθεί και στη συνέχεια, οι πάροχοι Υπηρεσιών Διαδικτύου προσπαθούν να επαναπροσδιορίσουν το ρόλο τους και να αποκτήσουν κεντρικότερο ρόλο στην όλη διαδικασία. Επιπλέον, ασαφή είναι και τα όρια μεταξύ των παρεχόμενων λειτουργικοτήτων των παρόχων OTT και CDN. Τέλος, ο χρήστης θεωρείται ότι έχει στην κατοχή του τουλάχιστον μία συσκευή,

ικανή να καταναλώσει πολυμεσικό περιεχόμενο —αν και ο κανόνας είναι η κατοχή περισσότερων της μίας, ετερογενών συσκευών— ενώ σταδιακά όλο και περισσότεροι χρήστες γίνονται κάτοχοι μιας συνδεδεμένης ή υβριδικής τηλεόρασης (Connected or Hybrid TV). Υπό το πρίσμα της σύγκλισης των μέσων διανομής περιεχομένου, η συνδεδεμένη τηλεόραση αποτελεί έναν τεχνολογικά ουδέτερο όρο, ο οποίος καλύπτει όλο το εύρος συσκευών (συμπεριλαμβανομένων και κινητών συσκευών), που επιτρέπουν την πρόσβαση σε γραμμικό και μη-γραμμικό πολυμεσικό περιεχόμενο καθώς και άλλες υπηρεσίες OTT μέσω της ίδιας οθόνης, ενοποιώντας τα πεδία του εκπεμπόμενου και του δικτυακώς διανεμόμενου περιεχομένου .



Σχήμα 5 Τυπική αρχιτεκτονική διανομής πολυμεσικού περιεχομένου

Ενώ τα παλαιότερα περιβάλλοντα ήταν εξ ολοκλήρου διαχειριζόμενα από έναν πάροχο υπηρεσιών (σε συνεργασία με παρόχους περιεχομένου), σήμερα αυτό έχει ξεκινήσει να αλλάζει με ραγδαίο ρυθμό. Συγκεκριμένα η κυρίαρχη πρακτική συμπεριλάμβανε τη διάθεση στον τελικό χρήστη, ενός αποκωδικοποιητή (Set-Top Box), ο οποίος συνδεόταν με την τηλεόραση και μέσω ενός ιδιόκτητου δικτύου, ο πάροχος ήλεγχε από άκρο σε άκρο τη διανομή του πολυμεσικού περιεχομένου. Πλέον οι νέες αυξημένες απαιτήσεις, καθιστούν αυτό τον τρόπο διανομής ξεπερασμένο. Με τον πολλαπλασιασμό των διασυνδεδεμένων συσκευών που είναι ικανές να καταναλώνουν πολυμεσικό περιεχόμενο (έξυπνες τηλεοράσεις, υπολογιστές, κινητά, ταμπλέτες και

παιχνιδομηχανές) και αντίστοιχα νέων τεχνολογιών, οι καταναλωτές αναμένουν —αν όχι απαιτούν— την πρόσβαση στο περιεχόμενο, ανεξάρτητα από το είδος της συσκευής, του υποκείμενου δικτύου και της τοποθεσίας τους. Οι συσκευές δε διαφέρουν μόνο στο μέγεθος της οθόνης και τη διαθέσιμη υπολογιστική ισχύ, αλλά και στις υποστηριζόμενες τεχνολογίες· για παράδειγμα οι συσκευές της Apple δεν υποστηρίζουν την τεχνολογία Adobe Flash, η οποία μέχρι πρόσφατα ήταν η επικρατούσα τεχνολογία που επέτρεπε την κατανάλωση πολυμεσικού περιεχομένου σε υπολογιστές και κινητά. Κατά συνέπεια οι πάροχοι υπερκείμενων υπηρεσιών οφείλουν να απεγκλωβιστούν από τη λογική των κλειστών περιβαλλόντων (walled gardens) και να αναπτύξουν λύσεις που απευθύνονται σε μια πληθώρα συσκευών (multi-screen), προκειμένου να αυξήσουν κατά το δυνατόν τη συνδρομητική τους βάση.

Όπως αναλύθηκε και στην Ενότητα 2.3, οι πάροχοι υπερκείμενων υπηρεσιών απευθύνονται σε παρόχους Δικτύων CDN, με σκοπό την αξιόπιστη και αποδοτική διάθεση του περιεχομένου τους στους τελικούς χρήστες, καθώς η χρήση αποκλειστικά των εξυπηρετητών των παρόχων υπερκείμενων υπηρεσιών αποτελεί ανασταλτικό παράγοντα τόσο ως προς τη διαθεσιμότητα όσο και ως προς την επίδοση των υπηρεσιών αυτών. Αν και πρόσφατα η στρατηγική αυτή έχει αρχίσει να διαφοροποιείται, καθώς YouTube, Netflix και Amazon επιλέγουν σταδιακά την ανάπτυξη ιδιόκτητων CDN, αυτό δεν επηρεάζει την τεχνική προσέγγιση, αλλά μονάχα το επιχειρηματικό μοντέλο. Αντίστοιχα οι πάροχοι υπηρεσιών Διαδικτύου εισέρχονται στην αγορά αυτή, προσφέροντας και οι ίδιοι υπερκείμενες υπηρεσίες (προσαρμοσμένες στη συνδρομητική τους βάση) και αναπτύσσοντας μικρότερης κλίμακας CDN (ή MDN όπως αποκαλούνται τα —περιορισμένα εντός ενός ISP— CDN), ώστε αφενός να ικανοποιήσουν τις υψηλές απαιτήσεις των χρηστών και αφετέρου να καρπωθούν μέρος της κερδοφορίας.

Η παροχή πολυμεσικού περιεχομένου κυριαρχείται από ιδιόκτητες λύσεις, καθώς ελλείψει προτυποποιημένων λύσεων, κάθε πάροχος ανέπτυξε τη δική του λύση προσαρμοσμένη στις ανάγκες του. Η επικρατούσα τεχνολογία, αναφορικά με τη μετάδοση πολυμεσικών πακέτων, είναι αυτή του προσαρμοσμένου ρυθμού μετάδοσης (Adaptive Bit-Rate - ABR), η οποία υλοποιήθηκε ξεχωριστά από την Apple, με το HTTP Live Streaming (HLS) [30], τη Microsoft, που δημιούργησε το Microsoft Smooth Streaming (MSS) [31], και την Adobe, με το HTTP Dynamic Streaming (HDS) [32]. Δυστυχώς η διαλειτουργικότητα μεταξύ των πρωτοκόλλων αυτών δεν είναι εφικτή, με αποτέλεσμα οι

πάροχοι πολυμεσικού περιεχομένου να αναγκάζονται να υποστηρίζουν περισσότερα του ενός πρωτόκολλα, ώστε να ανταποκρίνονται στην ανομοιομορφία της συνδρομητικής βάσης. Στην πράξη, οι πάροχοι αναγκάζονται να κωδικοποιούν και να αποθηκεύουν κάθε ροή πολυμέσων σε πολλαπλές μορφές, με αντίστοιχη αύξηση του κόστους λειτουργίας τους.

Μία εξίσου σημαντική παράμετρος, η οποία πρέπει να ληφθεί υπόψη από τους παρόχους πολυμεσικών υπηρεσιών, είναι η προστασία του περιεχομένου. Οι πάροχοι περιεχομένου θέτουν αυστηρούς όρους, αναφορικά με την προστασία του περιεχομένου τους, προκειμένου να δώσουν άδεια για τη διανομή του στους παρόχους υπερκείμενων υπηρεσιών. Καθώς οι διασυνδεδεμένες συσκευές, αρκετές από τις οποίες στηρίζονται σε ανοιχτές πλατφόρμες, βρίσκονται εκτός του ελέγχου των παρόχων, απαιτείται η χρήση τεχνολογιών προστασίας περιεχομένου —ή όπως έχει επικρατήσει να λέγονται τεχνολογίες Διαχείρισης Ψηφιακών Δικαιωμάτων (Digital Rights Management – DRM). Οι διαθέσιμες λύσεις έχουν σχεδιαστεί και αυτές χωρίς προϋπάρχουσα προτυποποίηση, και με εστίαση σε συγκεκριμένες συσκευές, με αποτέλεσμα την ύπαρξη πολλών εναλλακτικών λύσεων. Ενδεικτικά αναφέρονται η PlayReady από τη Microsoft [33], η Widevine η οποία εξαγοράστηκε από τη Google [34], και η CMLA-OMA v2 [35], η οποία προωθήθηκε από την Open Mobile Alliance. Όπως και προηγουμένως οι πάροχοι, οι οποίοι επιθυμούν να απευθυνθούν στον ευρύτερο δυνατό αριθμό συσκευών, είναι αναγκασμένοι να ενσωματώσουν στις λύσεις τους, πλέον της μίας διαθέσιμων λύσεων προστασίας περιεχομένου. Προκειμένου να ενορχηστρώσουν την παράλληλη λειτουργία των λύσεων αυτών, οι πάροχοι καταφεύγουν σε επιπλέον ιδιόκτητες λύσεις [36].

Το πολυμεσικό περιεχόμενο προστατεύεται με τη χρήση κρυπτογραφίας και διαδικασίες απόκτησης αδειών, οι οποίες περιέχουν το κλειδί αποκτυπτογράφησης και ένα σύνολο περιορισμών και δικαιωμάτων, τα οποία έχει συμφωνήσει ο τελικός χρήστης με τον πάροχο. Οι κυριότερες γλώσσες προδιαγραφής δικαιωμάτων (Rights Expression Languages – REL) είναι η eXtensible rights Markup Language (XrML) [37], η οποία αποτελεί τη βάση της MPEG-21 [38], και η ODRL [39], στην οποία βασίζεται η γλώσσα προδιαγραφής δικαιωμάτων της OMA. Σε αυτές ορίζονται οι επιτρεπόμενες ενέργειες (permissions) και οι προϋποθέσεις κάτω από τις οποίες αυτές είναι εφικτές (conditions), τα οποία συνολικά καλούνται δικαιώματα.

Συν τοις άλλοις, η ανάπτυξη των πλατφορμών παροχής πολυμεσικού περιεχομένου έγινε αποσπασματικά και στοχεύοντας συγκεκριμένες συσκευές, κάτι το οποίο είχε σαν συνέπεια την υλοποίηση λύσεων, όπου η ζεύξη των τεχνολογιών ABR και DRM ήταν πολύ σφιχτή. Για παράδειγμα η Microsoft προσφέρει τη συνολική λύση MSS και PlayReady, η οποία απευθύνεται κυρίως σε προσωπικούς υπολογιστές, η Apple έχει ενσωματώσει στο HLS μια απλή λύση διαμοιρασμού αδειών που χρησιμοποιείται ως επί το πλείστον από τα κινητά και τις ταμπλέτες της, κλπ. Το αποτέλεσμα της όλης διαδικασίας είναι η δυσκολία ενσωμάτωσης νέων τεχνολογιών και υποστήριξης νέων συσκευών σε υφιστάμενα συστήματα.

Είναι σαφές ότι η έλλειψη προτύπων, ο μεγάλος αριθμός συσκευών με διαφορετικές δυνατότητες και η πολλαπλότητα των υφιστάμενων λύσεων συνεπάγονται εξαιρετικά πολύπλοκες και πολυδάπανες αρχιτεκτονικές, τόσο σε υλοποίηση και συντήρηση όσο και σε υπολογιστική ισχύ και αποθηκευτικό χώρο. Αντιλαμβανόμενοι αυτή την ανάγκη οι πάροχοι CDN έχουν αρχίσει να προσφέρουν ολοκληρωμένες λύσεις διανομής περιεχομένου, π.χ. [40], αλλά με ένα σεβαστό κόστος. Η περιγραφείσα κατάσταση καθιστά σαφές το μεγάλο κόστος της απαιτούμενης επένδυσης και αποτελεί τροχοπέδη για την περαιτέρω ανάπτυξη της συγκεκριμένης αγοράς, ιδίως για μικρομεσαίες επιχειρήσεις.

Προς την κατεύθυνση της απλούστευσης της υφιστάμενης πολυπλοκότητας, έχουν δημιουργηθεί διάφορες πρωτοβουλίες, όπως η DECE (Digital Entertainment Content Ecosystem). Η DECE αποτελεί μια κοινοπραξία εταιρειών, που στοχεύει στην προτυποποίηση της διαδικασίας διανομής πολυμεσικού περιεχομένου κάτω από την ταμπέλα του UltraViolet [41]. Στο πεδίο της προστασίας περιεχομένου, το Marlin DRM [42], είναι ένα «ανοιχτό» DRM, σκοπός του οποίου είναι η κάλυψη όσο το δυνατόν περισσότερων συσκευών και η υιοθέτησή του από τους παρόχους. Το UltraViolet υποστηρίζει το Marlin, μαζί με τέσσερις ακόμα τεχνολογίες DRM, ώστε τελικά ένα μοναδικά κρυπτογραφημένο περιεχόμενο να δύναται να αναπαραχθεί σε όλες πρακτικά τις διαθέσιμες συσκευές.

Παράλληλα, η ISO πρόσφατα δημοσίευσε το πρότυπο MPEG DASH [43] για τον προσαρμοσμένο ρυθμό μετάδοσης περιεχομένου. Το DASH περιλαμβάνει τα καλύτερα στοιχεία από τα HLS, MSS και HDS και υποστηρίζει τόσο ζωντανή όσο και κατά παραγγελία αναμετάδοση. Στην προσπάθεια να καλύψει όσο το δυνατόν περισσότερες

απαιτήσεις, υποστηρίζονται δύο μορφοποιήσεις, η Base Media File [44] του Διεθνούς Οργανισμού Τυποποίησης (International Organization for Standardization – ISO) [45] και η MPEG-2 Transport Stream [46] του Moving Picture Experts Group [47]. Παράλληλα ορίζει ένα δηλωτικό αρχείο το οποίο ονομάζεται Media Presentation Description (MPD) και το οποίο περιγράφει το περιεχόμενο της ροής πολυμέσου (τα διαθέσιμα τμήματα και το χρονισμό τους). Τέλος, στα πλαίσια του προτύπου, καθορίζονται κοινά μεταδεδομένα κρυπτογράφησης, επιτρέποντας τη διαλειτουργικότητα λύσεων DRM (παρομοίως με το UltaViolet).

3 Δίκτυα με Επίκεντρο την Πληροφορία

Το Κεφάλαιο αυτό παρουσιάζει τις αρχές και συνοπτικά τις πιο σημαντικές προσεγγίσεις που έχουν προταθεί στο πλαίσιο των Δικτύων με Επίκεντρο την Πληροφορία (Information-Centric Networking - ICN). Στη συνέχεια εμβαθύνει στην προσέγγιση του Content Centric Networking (CCN) [48] και, της βασισμένης σε αυτό, πρότυπης υλοποίησης CCNx [49], η οποία έχει χρησιμοποιηθεί σαν βάση της δικτυακής αρχιτεκτονικής, που προτείνεται από τη Διατριβή. Τέλος γίνεται μια εκτενής αναφορά σε ανοικτά θέματα, εστιάζοντας κυρίως στα θέματα προστασίας περιεχομένου και ιδιωτικότητας.

3.1 Εισαγωγή

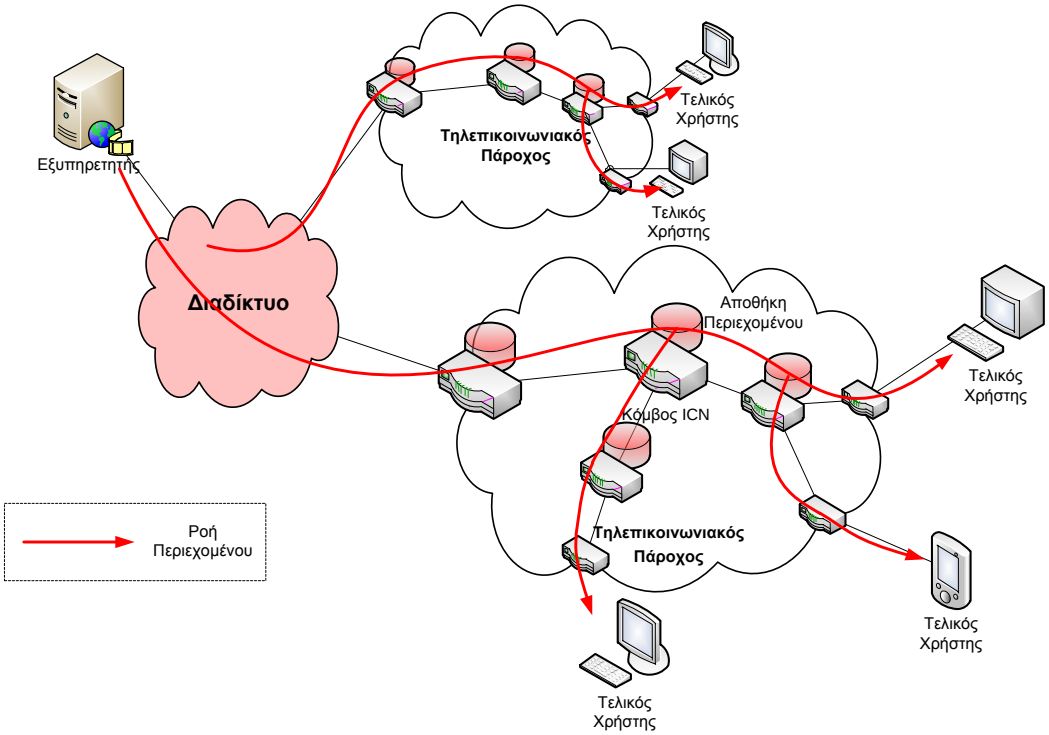
Όπως είδαμε και στο πρώτο Κεφάλαιο, η διανομή του (πολυμεσικού) περιεχομένου αποτελεί μία από τις μεγαλύτερες προκλήσεις, στις οποίες καλούνται να δώσουν απάντηση οι μελλοντικές αρχιτεκτονικές Διαδικτύου. Η ευρεία χρήση —η οποία αντικατοπτρίζει την επιτυχία και κατ' επέκταση την αναγκαιότητα— των Δικτύων CDN και P2P, μαζί με τις γνωστές αδυναμίες της κλασσικής προσέγγισης πελάτη-εξυπηρετητή, έχει στρέψει την έρευνα προς ένα νέο παράδειγμα δικτύωσης, με επίκεντρο την πληροφορία. Η έρευνα αυτή ωθείται από τη διαπίστωση ότι η παρούσα αρχιτεκτονική Διαδικτύου είναι ξεπερασμένη, καθώς η τυπική επικοινωνία δεν αφορά πλέον την επικοινωνία δύο απομακρυσμένων διαδικτυακών κόμβων, αλλά το διαμοιρασμό περιεχομένου, με επίκεντρο τις ροές πολυμέσων.

Τα Δίκτυα με Επίκεντρο την Πληροφορία (Information-Centric Networks - ICN) παρουσιάζουν μια διαφορετική προσέγγιση αναφορικά με τη δρομολόγηση του περιεχομένου λαμβάνοντας υπόψη το περιεχόμενο καθεαυτό και όχι την τοποθεσία του. Συγκεκριμένα, η πληροφορία προωθείται βάσει του ονόματός της και όχι της διεύθυνσης προορισμού της, προσεγγίζοντας τη δικτύωση με επίκεντρο την πληροφορία και όχι τον εξυπηρετητή που τη φιλοξενεί (ή την αιτείται). Ακολουθώντας το μοντέλο δημοσίευσης/συνδρομής (publish/subscribe), ο πάροχος του περιεχομένου δημοσιεύει στο Διαδίκτυο το περιεχόμενο αυτό, ενώ ο εκάστοτε ενδιαφερόμενος μπορεί να το αναζητήσει βάσει ονόματός. Μια βασική λειτουργία που καθίσταται δυνατή είναι ότι το

δίκτυο αποκτά επίγνωση του περιεχομένου που διακινεί και ως εκ τούτου, μπορεί να προβεί σε ενδοδικτυακή αποθήκευση.

Η έρευνα στην περιοχή των Δικτύων ICN γνωρίζει ιδιαίτερη άνθιση, όπως φαίνεται από τον αριθμό των ερευνητικών έργων παγκοσμίως, τα οποία εστιάζουν στην εν λόγω περιοχή, όπως τα 4WARD [50], SAIL [51], Named-Data Networking (NDN) [52],[53], PURSUIT [54], COMET [55], ANR-CONNECT [56] και CONVERGENCE [57] και τα οποία εξετάζουν εναλλακτικές αρχιτεκτονικές Δικτύων ICN υπό διαφορετικά πρίσματα. Σαν επιστέγασμα της ερευνητικής δραστηριότητας, έχει δημιουργηθεί μια ομάδα εργασίας στο Internet Research Task Force (IRTF) [58], η οποία στοχεύει στην προτυποποίηση της αρχιτεκτονικής.

Παρά τις θεμελιώδεις διαφορές που διέπουν τις προσεγγίσεις αυτές, ορισμένες έννοιες είναι κοινά αποδεκτές, όπως η δρομολόγηση βάσει ονόματος, η εγγενής αποθήκευση σε διαδικτυακά στοιχεία και ένα ριζικά επανασχεδιασμένο μοντέλο ασφαλείας. Οι αρχιτεκτονικές Δικτύων ICN έχουν δομηθεί γύρω από την έννοια του περιεχομένου που φέρει όνομα (named content)· ζητήματα όπως η ταυτότητα και η ασφάλεια του περιεχομένου έχουν αποσυνδεθεί από τις διαδικτυακές τοποθεσίες, από όπου αυτό εκπορεύεται.



Σχήμα 6 Ροές πολυμέσων σε Δίκτυα με Επίκεντρο την Πληροφορία

Το Σχήμα 6 απεικονίζει την αφηρημένη αρχιτεκτονική ενός Δικτύου ICN. Κάθε δρομολογητής εγκατεστημένος στον πάροχο υπηρεσιών διαδικτύου (ISP) περιλαμβάνει ένα χώρο προσωρινής αποθήκευσης, όπου αποθηκεύεται το περιεχόμενο πριν από την προώθησή του. Ως αποτέλεσμα, άλλοι πελάτες εξυπηρετούνται απευθείας από το διακομιστή περιεχομένου, ενώ άλλοι εξυπηρετούνται από τον αποθηκευτικό χώρο ενός δρομολογητή δικτύου, μέσω του οποίου έχει δρομολογηθεί προηγουμένως το ίδιο πακέτο. Με αυτό τον τρόπο, μέρος των αιτημάτων εξυπηρετείται εντός του Broadband Regional Network (BRN) του ISP, κάτι που αποφέρει οφέλη για όλους τους εμπλεκόμενους· τον ISP, τον πάροχο περιεχομένου και τον τελικό χρήστη. Οι εφαρμογές, οι οποίες είναι απαιτητικές σε εύρος ζώνης και ευαίσθητες στην καθυστέρηση, όπως οι ροές πολυμέσων, αναμένεται να αξιοποιήσουν τις εγγενείς δυνατότητες αποθήκευσης που παρέχονται από το στρώμα δικτύου και να βελτιώσουν τις επιδόσεις τους.

Η λειτουργικότητα ενός Δικτύου ICN μπορεί να θεωρηθεί ως ένας συνδυασμός ενός Δικτύου CDN και ενός Δικτύου P2P. Η ομοιότητα με τα δίκτυα CDN συνίσταται στην ύπαρξη αποθηκευτικού χώρου εντός του δικτύου, κάτι που οδηγεί σε λιγότερη κίνηση που διαβιβάζεται εκτός του BRN των ISPs. Ωστόσο, τα Δίκτυα ICN προχωρούν ένα βήμα παρακάτω από τα Δίκτυα CDN· στα Δίκτυα ICN όλοι οι ενδιάμεσοι δρομολογητές μπορούν να έχουν ένα χώρο αποθήκευσης, ενώ οι κλώνοι στα Δίκτυα CDN είναι συνήθως τοποθετημένοι στις παρυφές του δικτύου του ISP, όπως είδαμε στο προηγούμενο κεφάλαιο. Λαμβάνοντας υπόψη ότι το περιεχόμενο του αποθηκευτικού χώρου των δρομολογητών εξαρτάται από τις αιτήσεις που προέρχονται από τους πελάτες του δικτύου και ότι τα τμήματα του πολυμέσου μπορεί να προέρχονται από διαφορετική πηγή κάθε φορά (είτε το διακομιστή πηγή είτε διαφορετικούς δρομολογητές κατά μήκος της διαδρομής), η συμπεριφορά αυτή έχει ομοιότητες και με τα Δίκτυα P2P, ακόμη και αν σε αυτή την περίπτωση μιλάμε αυστηρά για μια προσέγγιση, στην οποία ο χρήστης εκκινεί τη διαδικασία απόκτησης του περιεχομένου (pull-based).

Παρ' όλες τις ομοιότητες, τα Δίκτυα ICN δεν είναι ένα ακόμα υπερκείμενο δίκτυο (overlay network), όπως τα Δίκτυα CDN και τα Δίκτυα P2P. Όπως υποστηρίζει και το [52], τα Δίκτυα ICN είναι μια υπέρθεση με τον ίδιο τρόπο που το πρωτόκολλο IP αποτελεί μια υπέρθεση πάνω από τα πρωτόκολλα του στρώματος μετάδοσης. Αντίθετα με τα Δίκτυα CDN, τα Δίκτυα ICN δεν περιορίζονται σε περιεχόμενο, για το οποίο υπάρχει σχετική συμφωνία μεταξύ δημιουργών και παρόχων υπηρεσιών CDN. Επιπλέον τα Δίκτυα CDN

δε συνεργάζονται μεταξύ τους και σαν αποτέλεσμα το καθένα περιορίζεται από τη γεωγραφική του επέκταση. Τα Δίκτυα ICN υπερβαίνουν τα εγγενή αυτά μειονεκτήματα των Δικτύων CDN και εκδημοκρατίζουν τη διανομή του περιεχομένου.

Συμπερασματικά, τα Δίκτυα ICN φαντάζουν σαν μια πολλά υποσχόμενη προσέγγιση, η οποία δείχνει ικανή να ανταποκριθεί στις προκλήσεις που καλείται να απαντήσει μια μελλοντική Διαδικτυακή αρχιτεκτονική. Ένα μεγάλο πλεονέκτημα που προκύπτει από τη δυνατότητα του δικτύου να γνωρίζει τι περιεχόμενο διέρχεται από τους κόμβους είναι η εφικτότητα χρήσης κρυφής μνήμης (cache), κάτι που έχει θετικό αντίκτυπο τόσο στους χρόνους απόκρισης όσο και στο χρησιμοποιούμενο εύρος ζώνης. Η άλλη πλευρά του νομίσματος είναι τα ευλόγα ζητήματα ασφάλειας και ιδιωτικότητας, που εγείρει η επίγνωση του περιεχομένου από το δίκτυο και τα οποία εξετάζονται πιο αναλυτικά σε επόμενη υποενότητα του Κεφαλαίου.

3.2 Αρχές λειτουργίας και προσεγγίσεις

Η ιδέα της δρομολόγησης βάσει ονόματος ετέθη πρώτη φορά το 1999 στα πλαίσια του προγράμματος TRIAD [59] του πανεπιστημίου Stanford σαν μία εναλλακτική της χρήσης εξυπηρετητών DNS στη διαδικασία διανομής περιεχομένου. Εν συνεχεία, και ενώ έδειχνε να έχει εγκαταλειφτεί, το 2007 επανήλθε στο προσκήνιο μέσω του προγράμματος Data Oriented Network Architecture (DONA) [60], το οποίο ενσωμάτωσε τη συγκεκριμένη αρχή σε ένα ευρύτερο πλαίσιο που δίνει έμφαση στην ασφάλεια, την αυθεντικότητα και τη διαθεσιμότητα του περιεχομένου, μέσω ενός εναλλακτικού τρόπου ονοματοδοσίας (μη ιεραρχικού). Το πρωτόκολλο δρομολόγησης του DONA έχει σχεδιαστεί ώστε να λειτουργεί πάνω από το IP. Εν συνεχεία, το 2009, το Palo Alto Research Center (PARC) παρουσίασε την αρχιτεκτονική Content-Centric Networking (CCN) [48], η οποία συνεισέφερε τα μέγιστα στην άνθιση της έρευνας στην περιοχή των Δικτύων ICN. Στο CCN ακολουθήθηκε ιεραρχικός τρόπος ονομασίας (κατά τα πρότυπα των URIs) και μελετήθηκαν συστηματικά η δομή των δρομολογητών και το πρωτόκολλο μετάδοσης δεδομένων (χωρίς χρήση της υποδομής του IP). Ακολούθησαν άλλες αξιοσημείωτες προσεγγίσεις όπως αυτές που προέκυψαν από τα Ευρωπαϊκά ερευνητικά προγράμματα PURSUIT/PSIRP [61] και 4WARD/SAIL (NetInf) [62]. Παρ' όλες τις διαφορές τους, όλα τα ερευνητικά προγράμματα συγκλίνουν στις ίδιες βασικές αρχές, οι οποίες μπορούν να συνοψιστούν στις εξής:

- Τεμαχισμός του περιεχομένου σε τμήματα με μοναδικό αναγνωριστικό/όνομα
- Πρωτόκολλο μετάδοσης που καθοδηγείται από τον αιτούντα (receiver-driven)
- Δρομολόγηση βάσει ονόματος
- Αποθήκευση τμημάτων του περιεχομένου εντός δικτυακών στοιχείων

Η πραγμάτευση, όμως, των συγκεκριμένων ζητημάτων διαφέρει μεταξύ των ερευνητικών προσπαθειών, όπως συνοψίζεται στην εργασία [63]. Μια σημαντική διαφορά εδράζεται στον τρόπο μετάβασης από την παρούσα κατάσταση του Διαδικτύου σε μία βασισμένη στις αρχές των Δικτύων ICN. Η προσέγγιση του «λευκού μητρώου» (clean slate) (η οποία ακολουθείται από το CCN) στηρίζεται στο επιχείρημα ότι χωρίς ριζικό επανασχεδιασμό του Διαδικτύου από μηδενική βάση δεν είναι δυνατό να ξεπεραστούν τα εγγενή προβλήματα της παρούσης αρχιτεκτονικής, ενώ αντίθετα οι υποστηρικτές της επικαλυπτικής (overlay) προσέγγισης (DONA) θεωρούν ανέφικτη την εκ των βάθρων αλλαγή του Διαδικτύου και εστιάζουν τις προτάσεις τους σε λύσεις που μπορούν να αναπτυχθούν πάνω από την υπάρχουσα υποδομή.

3.3 Η Αρχιτεκτονική Content-Centric Networking

Παρόλο που είναι δύσκολο να προβλεφθεί ποια από τις υπάρχουσες προσεγγίσεις θα επικρατήσει στο τέλος —το πιθανότερο άλλωστε είναι ότι στην πράξη θα προκύψει ένα αμάλγαμα των προσεγγίσεων αυτών— στην παρούσα Διατριβή στηριχθήκαμε στην προσέγγιση του Content-Centric Networking, η οποία εν συνεχεία υιοθετήθηκε και από το πρόγραμμα Named-Data Networking. Από την ερευνητική δραστηριότητα των προγραμμάτων αυτών έχει προκύψει και η —υπό ανάπτυξη— ανοιχτού κώδικα, υλοποίηση CCNx [49], η οποία αποτελεί τη βάση των πειραματικών δεδομένων μας.

Στο CCNx εισάγονται δύο είδη μηνυμάτων· το μήνυμα ενδιαφέροντος (Interest Message) και το μήνυμα περιεχομένου (Content Object). Το πρώτο αποστέλλεται από την πλευρά του πελάτη κάθε φορά που δημιουργείται ένα ονομαστικό αίτημα περιεχομένου στο Διαδίκτυο. Μαζί με τις επικεφαλίδες και τις υπόλοιπες πληροφορίες που απαιτούνται από τους δρομολογητές, το μήνυμα περιέχει το όνομα του περιεχομένου

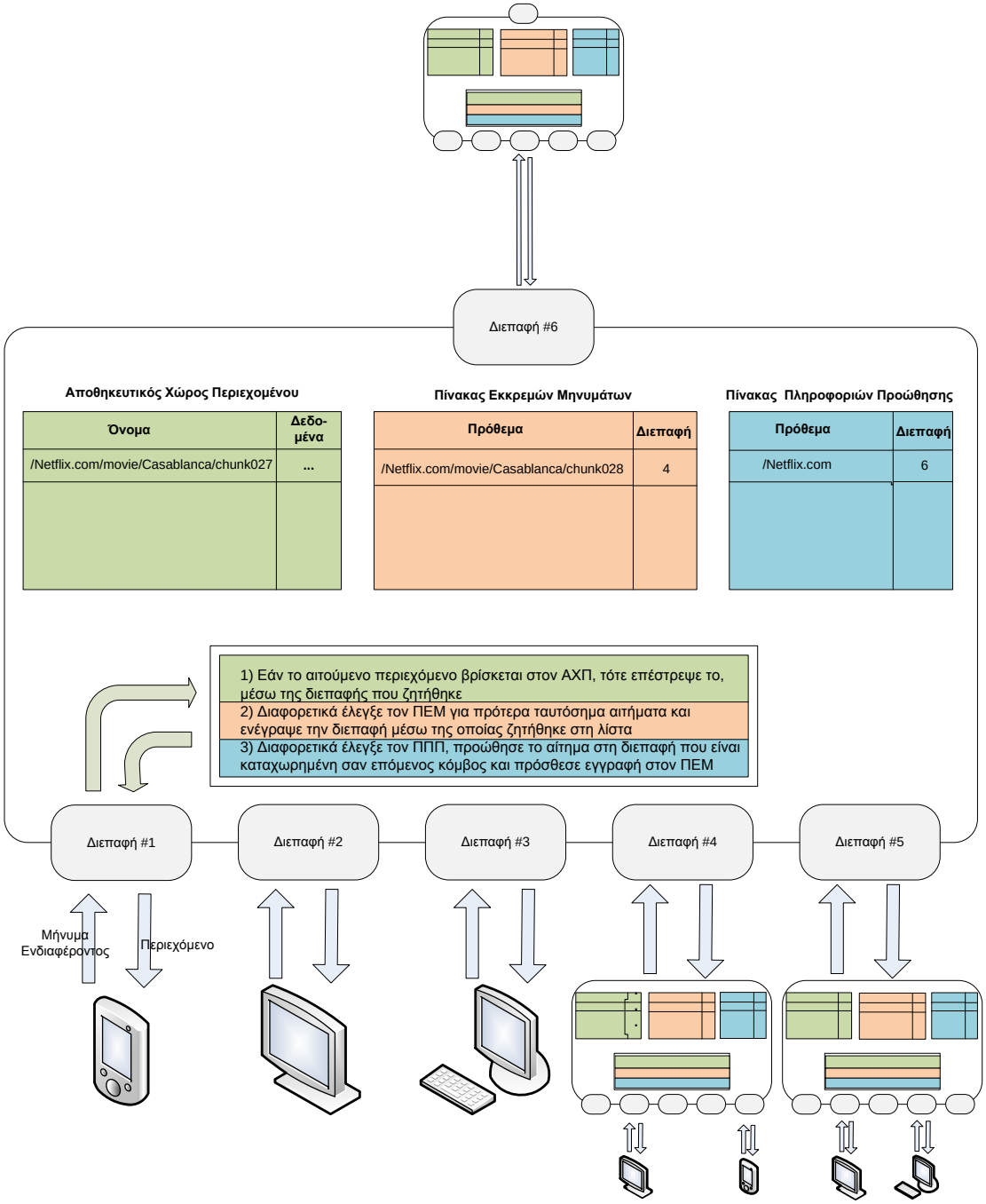
που ζητήθηκε από τον πελάτη. Το μήνυμα περιεχομένου είναι κατ' ουσία η απάντηση στο μήνυμα Interest, καθώς περικλείει το περιεχόμενο που φέρει το όνομα που ζητήθηκε.

Οι δομικές μονάδες ενός CCNx δρομολογητή είναι ο Πίνακας Πληροφοριών Προώθησης (Forward Information Base), ο Πίνακας Εκκρεμών Μηνυμάτων Ενδιαφέροντος (Pending Interest Table) και ο Αποθηκευτικός Χώρος Περιεχομένου (Content Store), όπως απεικονίζονται στο Σχήμα 7. Ο ΠΠΠ είναι πρακτικά το ισοδύναμο ενός πίνακα δρομολόγησης και περιέχει την αντιστοίχιση μεταξύ ενός ονόματος περιεχομένου και της διαδικτυακής διεπαφής, η οποία θα χρησιμοποιηθεί προκειμένου να προωθηθεί το μήνυμα Interest προς τον εξυπηρετητή που στεγάζει το περιεχόμενο αυτό. Ο ΠΕΜ είναι ένας πίνακας, όπου καταγράφονται όλα τα μηνύματα Interest, μαζί με την πληροφορία σχετικά με τη δικτυακή διεπαφή από την οποία προήρθαν. Τέλος ο ΑΧΠ είναι ο χώρος αποθήκευσης που διατίθεται σε ένα δρομολογητή, που καθιστά δυνατή τη βασική λειτουργικότητα της εγγενούς αποθήκευσης που προσφέρεται από τα Δίκτυα ICN.

Κάθε φορά που καταφθάνει ένα μήνυμα Interest σε ένα δρομολογητή, πρώτα ελέγχεται —βάσει του ονόματος— ο ΑΧΠ για τυχόν αποθηκευμένο αντικείμενο περιεχομένου, ώστε να αποσταλεί από εκεί προς τη διεπαφή που ήρθε το μήνυμα Interest. Εάν δε βρεθεί το περιεχόμενο στον ΑΧΠ, τότε ελέγχεται ο ΠΕΜ για τυχόν καταχωρήσεις (που αφορούν το ίδιο όνομα). Εάν βρεθεί αντίστοιχη εγγραφή τότε η διεπαφή από την οποία προήρθε το μήνυμα Interest προστίθεται στη συγκεκριμένη εγγραφή, ώστε, όταν φτάσει το περιεχόμενο στον κόμβο, αυτός να προωθήσει το περιεχόμενο προς την κατεύθυνση όλων των αιτούντων. Εάν δε βρεθεί εγγραφή ούτε στον ΠΕΜ, τότε και μόνο τότε ελέγχεται ο ΠΠΠ και δημιουργείται μια νέα εγγραφή στον ΠΕΜ. Η αντιστοίχιση στον ΠΠΠ γίνεται βάσει του μεγαλύτερου προθέματος και αν δεν υπάρχει αντίστοιχη εγγραφή, τότε δεν υπάρχει διαδρομή προς το συγκεκριμένο μήνυμα περιεχομένου. Η διαδικασία αυτή επαναλαμβάνεται σε κάθε δρομολογητή CCNx, στον οποίο φτάνει το μήνυμα Interest.

Τα μηνύματα περιεχομένου ακολουθούν την ακριβώς αντίστροφη διαδρομή από τα μηνύματα Interest. Αυτό επιτυγχάνεται μέσω της χρήσης του ΠΕΜ· το όνομα του περιεχομένου αναζητείται στον ΠΕΜ και η εγγραφή του ΠΕΜ «καταναλώνεται» υπό την έννοια ότι το μήνυμα περιεχομένου προωθείται στις διεπαφές που είναι καταγεγραμμένες στην εγγραφή του ΠΕΜ. Επιπλέον, όταν ένα μήνυμα περιεχομένου

φτάνει σε ένα δρομολογητή και σε συμφωνία με την πολιτική αντικατάστασης του αποθηκευτικού χώρου, αποθηκεύεται στον ΑΠΧ. Οι συνηθέστερες πολιτικές αντικατάστασης είναι η Αντικατάσταση με Βάση το Χρόνο Παραμονής (FIFO), η Αντικατάσταση με Βάση το Χρόνο της Τελευταίας Προσπέλασης (LRU), η Αντικατάσταση με Βάση τη Συχνότητα Προσπέλασης (LFU) και η Ψευδοτυχαία (Random).



Σχήμα 7 Δομή ενός δρομολογητή της αρχιτεκτονικής CCN

Η επίδοση των Δικτύων ICN έχει μελετηθεί ευρέως. Ορισμένες πρόσφατες μελέτες [64],[65] εστιάζουν στην αποδοτική χρήση του εύρους ζώνης και του αποθηκευτικού χώρου, ενώ άλλες στην επίδοση των πολιτικών ανανέωσης περιεχομένου στον ΑΧΠ, π.χ. στο [66] εξετάζεται μια παραλλαγή της προαναφερθείσας αντικατάστασης με βάση το χρόνο τελευταίας προσπέλασης. Τέλος, μία εναλλακτική πρόταση δρομολόγησης, η οποία εισάγει εννοιολογικά στοιχεία (semantics), προτείνεται στο [67].

3.4 Διανομή πολυμεσικού περιεχομένου πάνω από Δίκτυα ICN

Αναφορικά με τη διανομή πολυμεσικού περιεχομένου, στα πλαίσια του NDN έχει αναπτυχθεί η λύση NDNVideo [68], που βασίζεται σε ένα σχήμα ονομασίας, το οποίο επιτρέπει την εύκολη ενσωμάτωση στο CCNx υφιστάμενων εφαρμογών αναπαραγωγής βίντεο (VLC [69], GStreamer [70]) και ιδιαίτερα των πρωτοκόλλων ροής που βασίζονται σε HTTP. Σύμφωνα με την ιεραρχική προσέγγιση ονομασίας, τα ονόματα των μηνυμάτων περιεχομένου περιλαμβάνουν πληροφορίες δρομολόγησης (πρόθεμα δρομολόγησης), και γενικές πληροφορίες σχετικά με το βίντεο (την έκδοση, τον αύξοντα αριθμό του τμήματος του βίντεο και την κωδικοποίηση). Το πολυμέσο παρέχεται σαν μια συλλογή μηνυμάτων περιεχομένου, η οποία περιέχει τα εξής μηνύματα περιεχομένου —κλειδί, πληροφορίες ροής, τμήματα και δείκτη. Συγκεκριμένα, το κλειδί έχει χρησιμοποιηθεί για την υπογραφή των μηνυμάτων περιεχομένου. Οι πληροφορίες ροής περιέχουν μεταδεδομένα για το βίντεο, όπως η συχνότητα πλαισίου (frame rate). Τα τμήματα περιέχουν την πραγματική ροή του πολυμέσου και είναι αριθμημένα σειριακά. Τέλος ο δείκτης περιέχει την αντιστοίχιση μεταξύ τμημάτων και χρονοσφραγίδων (timestamps), οι οποίες θα χρησιμοποιηθούν από το πρόγραμμα αναπαραγωγής βίντεο.

Σύμφωνα με τις κατευθυντήριες γραμμές του NDN, ο διακομιστής βίντεο πρέπει να παραγάγει τα τμήματα του κωδικοποιημένου αρχείου βίντεο και, στη συνέχεια, να τα δημοσιεύσει ως ξεχωριστά αρχεία στο δίκτυο. Ανάλογα με το πρωτόκολλο δρομολόγησης, το δίκτυο θα πρέπει να ενημερωθεί με τις διαδρομές προς τα τμήματα αυτά, με αποτέλεσμα τη διαθεσιμότητα των τελευταίων βάσει των ονομάτων τους. Από την πλευρά του πελάτη, το πρόγραμμα αναπαραγωγής πολυμέσων θα κατεβάσει πρώτα το αρχείο με το δείκτη και (πιθανότατα) το αρχείο με τις πληροφορίες της ροής,

προκειμένου να λάβει τις απαραίτητες πληροφορίες για την αναπαραγωγή του βίντεο. Στη συνέχεια, με τρόπο παρόμοιο με τα βασισμένα στο HTTP πρωτόκολλα ροής (όπως π.χ. το Apple HTTP Live Streaming (HLS), και το Dynamic Adaptive streaming μέσω HTTP (DASH)), θα αρχίσει να ζητά τα τμήματα με την αποστολή των αντίστοιχων μηνυμάτων Interest. Τα τμήματα βίντεο θα μεταφορτωθούν είτε απευθείας από το διακομιστή βίντεο ή από τη μνήμη cache (CS) ενός CCNx router που βρίσκεται στη διαδρομή δρομολόγησης.

Μία νέα, πλέον πρόσφατη, κατεύθυνση της ερευνητικής δραστηριότητας είναι η συνέργια των τεχνολογιών Δικτύων ICN και προσαρμοζόμενης ροής πολυμέσων, όπως παρουσιάζεται στις εργασίες [71],[72],[73], με κύρια έμφαση στη διαλειτουργικότητα των προσεγγίσεων CCN και DASH. Οι δύο αυτές προσεγγίσεις μοιράζονται ορισμένες κοινές αρχές, με κυριότερες την ανάθεση της πρωτοβουλίας στο χρήστη, την τμηματική παράδοση του περιεχομένου, την υποστήριξη πολλαπλών πηγών, και την έλλειψη συνεδρίας μεταξύ χρήστη και παρόχου περιεχομένου. Παράλληλα, όμως, είναι εμφανής η ύπαρξη διαφορών, οι οποίες πρέπει να γεφυρωθούν, όπως η ονοματοδοσία του περιεχομένου, η αποδυνάμωση της ενδοδικτυακής αποθήκευσης λόγω πολλαπλών ποιοτήτων του ίδιου περιεχομένου, η απουσία προστασίας και ελέγχου του περιεχομένου εκτός της αρχικής πηγής κ.α. Ειδικά για το τελευταίο γίνεται ειδική μνεία και στην επόμενη υποενότητα. Τέλος, στο [74] παρουσιάζεται μια συνεργατική εφαρμογή μετάδοσης πολυμεσικού περιεχομένου πάνω από Δίκτυα ICN, με χρήση του πρωτοκόλλου HLS.

3.5 Ανοιχτά θέματα

Η ασφάλεια γενικότερα και η προστασία του περιεχομένου ειδικότερα είναι ανοικτά θέματα στα Δίκτυα ICN. Στα Δίκτυα ICN η ασφάλεια εδράζεται πάνω στο περιεχόμενο καθ' εαυτό και όχι σε σχέση με την τοποθεσία εκπόρευσής του ή τον τρόπο διαμοιρασμού του, όπως στο παρόν μοντέλο. Η χρήση ψηφιακών υπογραφών είναι απαραίτητη. Το περιεχόμενο, από κοινού με το όνομά του, υπογράφεται από το δημιουργό του, ώστε να τεκμηριώνεται με ασφάλεια η σύνδεση των δύο. Η υπογραφή, σε συνδυασμό με πληροφορίες για τον εκδότη της πληροφορίας, μπορούν να πιστοποιήσουν την προέλευση του περιεχομένου. Παράλληλα μπορούν να χρησιμοποιηθούν για την υποστήριξη σχέσεων εμπιστοσύνης σε λεπτομερές επίπεδο, καθώς —βάσει αυτών και του γενικότερου πλαισίου— ο αιτών μπορεί να συμπεράνει εάν ο κάτοχος της ψηφιακής

υπογραφής είναι ένας εύλογος εκδότης του συγκεκριμένου ψηφιακού περιεχομένου. Τα δημόσια κλειδιά μπορούν να κυκλοφορούν στα Δίκτυα ICN, όπως και τα υπόλοιπα τμήματα περιεχομένου. Βεβαίως, οι ερευνητές αναγνωρίζουν την έλλειψη χρηστικότητας και αποδοτικότητας στις ψηφιακές υπογραφές δημόσιου κλειδιού, κάτι που καθιστά την περαιτέρω έρευνα στο συγκεκριμένο τομέα απαραίτητη. Αλληλένδετο θέμα αποτελεί και η ανάκληση των κλειδιών, κάτι το οποίο στα Δίκτυα ICN καθίσταται πλέον πολύπλοκο, καθώς πρέπει να ληφθεί υπόψη και η εγγενής δυνατότητα αποθήκευσης των δεδομένων (άρα και των κλειδιών) σε ενδιάμεσους κόμβους.

Αναφορικά με την προστασία και την ιδιωτικότητα του περιεχομένου, το περιβάλλον των Δικτύων ICN είναι εξίσου απαιτητικό. Οι μηχανισμοί προστασίας περιεχομένου, οι οποίοι εφαρμόζονται στις υπηρεσίες διαμοιρασμού πολυμεσικού περιεχομένου σήμερα, δεν είναι συμβατοί με το μοντέλο των Δικτύων ICN, καθώς η κρυπτογράφηση ανά χρήστη εξουδετερώνει την αποτελεσματικότητα της αποθήκευσης στους δρομολογητές. Με δεδομένη την ευρεία χρήση των ενδιάμεσων αποθηκευτικών χώρων, οι εκδότες της πληροφορίας δεν μπορούν να εμπιστευτούν τις τοποθεσίες αποθήκευσης για την εφαρμογή του ελέγχου πρόσβασης, αλλά αναγκάζονται να καταφύγουν στη χρήση αλγορίθμων κρυπτογράφησης, όπως η κρυπτογράφηση εκπομπής (broadcast encryption) [75],[76] και άλλα σχήματα ελέγχου πρόσβασης βάσει κρυπτογράφησης [77],[78]. Οι προσεγγίσεις αυτές έχουν εξεταστεί στην παρούσα μορφή του Διαδικτύου και οφείλουν να επανεξεταστούν υπό το πρίσμα των Δικτύων ICN.

Η προστασία της ιδιωτικότητας στα Δίκτυα ICN αποτελεί με τη σειρά της ένα σύνθετο πρόβλημα, αν και με μια πρώτη ανάγνωση η πληροφορία που κυκλοφορεί στο δίκτυο αφορά το περιεχόμενο που ζητείται και όχι το ποιος το έχει αιτηθεί (η πληροφορία αυτή είναι δυνατό να εξαχθεί μόνο από τον ακραίο κόμβο με τον οποίο είναι συνδεδεμένος ο χρήστης). Παρόλα αυτά η χρήση ονομάτων που περιγράφουν με ακρίβεια το περιεχόμενο, συνιστά έναν ουσιαστικό κίνδυνο, καθώς επιτρέπει πιο εύκολα την αναζήτηση και την παρακολούθηση της διαδρομής του περιεχομένου. Αντίστοιχα η δυνατότητα αποθήκευσης του περιεχομένου στους ενδιάμεσους αποθηκευτικούς χώρους δημιουργεί επιπρόσθετους κινδύνους. Τέλος ιδιαίτερη μνεία πρέπει να δοθεί στην προστασία των ψηφιακών υπογραφών καθώς εν δυνάμει μπορούν να αποκαλύψουν στοιχεία για την ταυτότητα των υπογραφόντων. Τα παραπάνω καθίστανται ιδιαίτερα κρίσιμα στο σύγχρονο διεθνές περιβάλλον όπου ένα κράτος – το οποίο δεν φείδεται

υπολογιστικής ισχύος – επιθυμεί την παρακολούθηση των χρηστών του Διαδικτύου. Για την αποδυνάμωση των παραπάνω απειλών έχουν προταθεί λύσεις όπως η χρήση ιδεατών ιδιωτικών δικτύων (προσαρμοσμένων στο πλαίσιο των Δικτύων ICN), αλλά καθώς η προστασία της ιδιωτικότητας συγκεντρώνει τα φώτα της ερευνητικής κοινότητας, αναμένονται και άλλες προσεγγίσεις.

4 Κρυπτογραφία βάσει Χαρακτηριστικών

4.1 Εισαγωγή

Η Κρυπτογραφία Βάσει Χαρακτηριστικών (Attribute-Based Encryption - ABE) αποτελεί μια επέκταση της Κρυπτογραφίας Βάσει Ταυτότητας (Identity-Based Encryption - IBE), η οποία είχε προταθεί από τον Adi Shamir (εκ των εφευρετών του RSA) το 1984 [79], αλλά χρειάστηκε να περάσουν 17 χρόνια, έως ότου γίνει πράξη. Οι πρώτες υλοποιήσεις έγιναν εφικτές χάρη στις παράλληλες εργασίες των Boneh & Franklin [80] και Cocks [81] το 2001. Οι εργασίες αυτές στηριχτήκαν πάνω σε προόδους της επιστήμης των μαθηματικών στους τομείς της θεωρίας ομάδων και της θεωρίας πολυπλοκότητας.

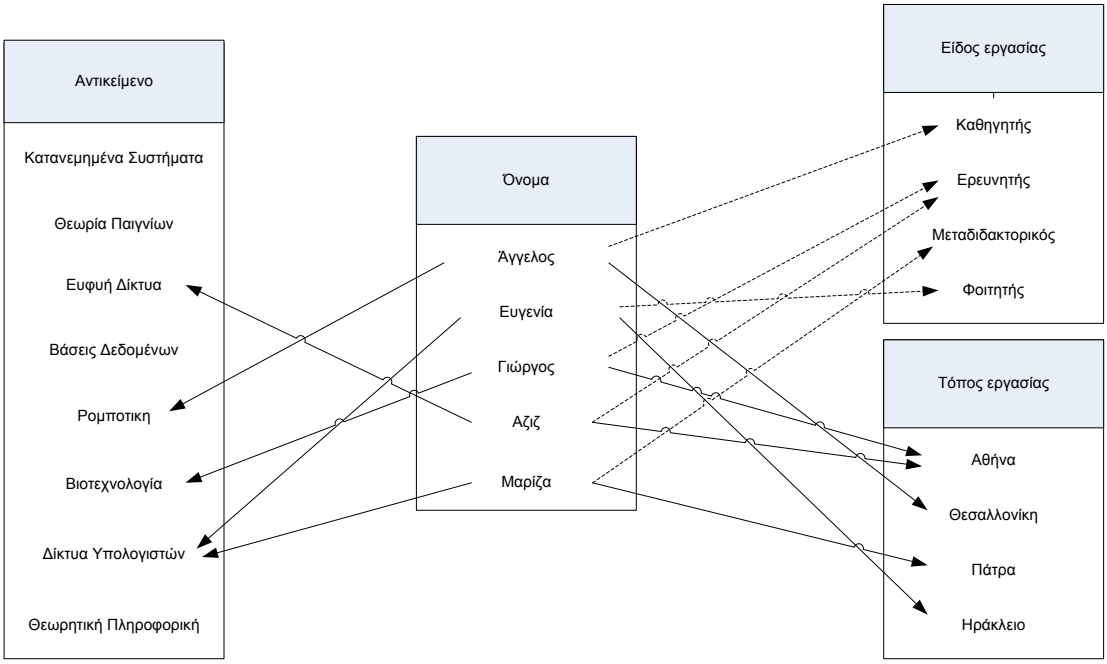
Η πολυπλοκότητα της διαχείρισης των πιστοποιητικών στα συστήματα ηλεκτρονικής αλληλογραφίας αποτέλεσε το κίνητρο του Shamir. Η κεντρική ιδέα της Κρυπτογραφίας IBE είναι η δυνατότητα κρυπτογράφησης ενός μηνύματος χωρίς να προαπαιτείται η πρόσβαση σε ένα πιστοποιητικό δημόσιου κλειδιού. Η δυνατότητα αυτή έχει πολλές πρακτικές εφαρμογές. Στην πράξη ο χρήστης/αποστολέας μπορεί να κρυπτογραφήσει ένα μήνυμα για έναν αποδέκτη, π.χ. τον john@otenet.gr, άνευ μιας υποδομής δημοσίου κλειδιού ή της απαίτησης ο αποδέκτης να είναι συνδεδεμένος την ώρα της κρυπτογράφησης (ώστε να υπάρξει κάποιο είδος διαπραγμάτευσης). Η ταυτότητα του χρήστη αποτελείται από μια αυθαίρετη συμβολοσειρά (στην παραπάνω περίπτωση το "john@otenet.gr"), βάσει της οποίας γίνεται η κρυπτογράφηση και για την οποία ο χρήστης έχει λάβει το κατάλληλο κλειδί από μια αρχή πιστοποίησης. Η ταυτότητα αυτή είναι το αντίστοιχο του δημοσίου κλειδιού του χρήστη σε συστήματα Υποδομής Δημοσίου Κλειδιού (Public Key Infrastructure - PKI).

Επεκτείνοντας την ιδέα αυτή οι Waters & Sahai πρότειναν το 2005 την Κρυπτογραφία ABE [2], θέτοντας στη θέση της ταυτότητας μια σειρά χαρακτηριστικών του χρήστη, προς τον οποίο γίνεται η κρυπτογράφηση. Η αρχική ονομασία της πρότασης αυτής ήταν Ασαφής (Fuzzy) Κρυπτογραφία IBE, ωστόσο επικράτησε η Κρυπτογραφία ABE. Με την επέκταση αυτή γίνεται δυνατή η κρυπτογράφηση ενός μηνύματος προς πολλούς χρήστες οι οποίοι μοιράζονται ένα σύνολο κοινών χαρακτηριστικών.

Ταυτόχρονα δεν είναι απαραίτητη η εκ των προτέρων γνώση των παραληπτών του μηνύματος. Μια σημαντική ιδιότητα της Κρυπτογραφίας ABE είναι η ανθεκτικότητα της σε «αθέμιτες συμπράξεις», δηλαδή η αποτροπή σύμπραξης χρηστών με συμπληρωματικά χαρακτηριστικά ώστε να αποκρυπτογραφήσουν ένα μήνυμα το οποίο από μόνοι τους δε θα μπορούσαν. Η Κρυπτογραφία IBE και η Κρυπτογραφία ABE μπορούν να κατηγοριοποιηθούν κάτω από την ευρύτερη ομπρέλα της Συναρτησιακής Κρυπτογραφίας (Functional Encryption).

Στο σημείο αυτό και για να γίνει κατανοητή η Κρυπτογραφία ABE παρατίθεται ένα σύντομο παράδειγμα. Ένα μήνυμα κρυπτογραφείται προς όλους τους ερευνητές (1ο κριτήριο), με αντικείμενο τη Βιοτεχνολογία (2ο κριτήριο) και οι οποίοι εδρεύουν στην Αθήνα (3ο κριτήριο). Η μόνη προαπαίτηση είναι η ύπαρξη μιας αρχής πιστοποίησης, η οποία θα είναι υπεύθυνη για την έκδοση των κατάλληλων —σύμφωνα με τα χαρακτηριστικά κάθε χρήστη— κλειδιών, π.χ. το αντίστοιχο πανεπιστήμιο-ερευνητικό κέντρο του καθενός. Στην αρχική πρόταση [2] προβλεπόταν η δυνατότητα αποκρυπτογράφησης, αν η ταυτότητα προς την οποία είχε κρυπτογραφηθεί το μήνυμα (ω) και η ταυτότητα του παραλήπτη (ω') απείχαν μια προκαθορισμένη απόσταση (threshold). Στο παραπάνω παράδειγμα αυτό θα σήμαινε ότι εάν ο χρήστης πληροί π.χ. τα 2 από τα 3 κριτήρια τότε έχει τη δυνατότητα αποκρυπτογράφησης του μηνύματος.

Στο Σχήμα 8 παρουσιάζεται το παράδειγμα. Εάν η επιθυμητή απόσταση μεταξύ των ταυτοτήτων είχε οριστεί μηδενική, δηλαδή ο χρήστης πρέπει να κατέχει και τα 3 χαρακτηριστικά-κριτήρια, τότε δυνατότητα αποκρυπτογράφησης έχει μόνο ο Γιώργος (Ερευνητής, Αθήνα και Βιοτεχνολογία), ενώ εάν αρκούν 2 από τα 3 χαρακτηριστικά τότε δύναται και ο Αζίζ (Ερευνητής, Αθήνα). Όπως θα δούμε στη συνέχεια, νεότερες εργασίες έχουν επιτρέψει τη χρήση τύπων Boolean, καθιστώντας δυνατή τη σύνταξη πολύπλοκων πολιτικών πρόσβασης με χρήση λογικών τελεστών AND, OR και NOT.



Σχήμα 8 Αντιστοίχιση χρηστών και χαρακτηριστικών

Τα τελευταία χρόνια η Κρυπτογραφία ΑΒΕ αποτελεί μία από τις πλέον ενεργές ερευνητικές περιοχές στο χώρο της κρυπτογραφίας. Η μελέτη εστιάζεται αφενός στη βελτιστοποίηση της εκφραστικότητας των πολιτικών πρόσβασης με διατήρηση της ασφάλειας της κρυπτογράφησης και αφετέρου σε πρακτικής φύσεως προβλήματα όπως η ανάκληση χαρακτηριστικών χρηστών ή/και αυτούσιων χρηστών, η βελτιστοποίηση της ταχύτητας κρυπτογράφησης και αποκρυπτογράφησης, η ύπαρξη πλέον της μιας αρχής πιστοποίησης χαρακτηριστικών, η χρήση ημιέμπιστων πληρεξούσιων για ανακρυπτογράφηση κλπ. Παράλληλα μελετώνται εφαρμογές της Κρυπτογραφίας ΑΒΕ με στόχο είτε την προστασία προσωπικών δεδομένων (άρα προστασίας της ιδιωτικότητας των χρηστών) είτε προστασίας περιεχομένου επιχειρήσεων. Ας σημειωθεί ότι οι εφαρμογές αυτή τη στιγμή περισσότερο στοχεύουν στην ανάδειξη της χρησιμότητας της Κρυπτογραφίας ΑΒΕ και την εφαρμοσιμότητα της σε υφιστάμενα ανοιχτά θέματα, παρά στην ανάπτυξη της σε λειτουργικά συστήματα, καθώς εκκρεμούν οι βελτιστοποιήσεις που προαναφέρθηκαν. Στις επόμενες παραγράφους θα παρουσιαστούν τόσο το θεωρητικό υπόβαθρο και τα ανοιχτά θέματα στα οποία εστιάζει η έρευνα, όσο προτάσεις εφαρμογής της Κρυπτογραφίας ΑΒΕ. Το μαθηματικό υπόβαθρο —το οποίο ξεφεύγει από τους στόχους της Διατριβής— παρουσιάζεται στο [82], στο οποίο γίνεται ευρεία χρήση μαθηματικών που χρησιμοποιούνται στην Κρυπτογραφία ΑΒΕ (διγραμμικές

απεικονίσεις, υπόθεση decisional-Bilinear Diffie-Hellman Exponent (d-BDHE), υπόθεση decisional-Bilinear Diffie-Hellman, Linear Secret-Sharing Schemes).

4.2 Παραλλαγές της Κρυπτογραφίας Βάσει Χαρακτηριστικών

Σε μεταγενέστερες εργασίες, οι Goyal, Pandey, Sahai, και Waters [83] προσδιόρισαν περαιτέρω την έννοια της Κρυπτογραφίας ABE. Ειδικότερα, πρότειναν δύο συμπληρωματικές μορφές Κρυπτογραφίας ABE. Οι δύο μορφές διαφέρουν στην τοποθέτηση της πολιτικής πρόσβασης στο κλειδί ή στο κρυπτογράφημα. Στην πρώτη, η οποία ονομάστηκε Κρυπτογραφία ABE Πολιτικής Κλειδιού (Key-Policy ABE ή KP-ABE), τα κρυπτογραφήματα υποσημειώνονται με τα χαρακτηριστικά, ενώ τα μυστικά κλειδιά των χρηστών περιλαμβάνουν τις πολιτικές πρόσβασης επί των χαρακτηριστικών αυτών. Η δεύτερη μορφή, που καλείται Κρυπτογραφία ABE Πολιτικής Κρυπτογραφήματος (Ciphertext-Policy ABE ή CP-ABE), είναι συμπληρωματική της πρώτης, υπό την έννοια ότι τα χαρακτηριστικά που περιγράφουν τα διαπιστευτήρια του χρήστη αποθηκεύονται στα κλειδιά, ενώ οι πολιτικές πρόσβασης συνδέονται με το κρυπτογράφημα. Επιπλέον στο [83] προτάθηκε μια κατασκευή για την Κρυπτογραφία KP-ABE η οποία επεκτείνει την εκφραστικότητα της, καθώς οι πολιτικές πρόσβασης (που βρίσκονται στα κλειδιά των χρηστών) εκφράζονται με έναν οποιοδήποτε μονοτονικό τύπο επί των κρυπτογραφημένων δεδομένων. Το σύστημα αποδείχθηκε επιλεκτικά ασφαλές υπό την διγραμμική υπόθεση Diffie-Hellman. Ωστόσο η δημιουργία μιας εκφραστικής Κρυπτογραφίας CP-ABE αφέθηκε ως ένα ανοικτό πρόβλημα.

Η πρώτη εργασία που ασχολήθηκε επισταμένα με το θέμα της Κρυπτογραφίας CP-ABE ήταν αυτή των Bethencourt, Sahai, και Waters [84]. Στο σύστημά τους επετεύχθη ανάλογη εκφραστικότητα και αποτελεσματικότητα με αυτή του [83]. Ενώ η κατασκευή των BSW είναι πολύ εκφραστική, το μοντέλο που χρησιμοποιήθηκε για την απόδειξη ασφαλείας απείχε πολύ από το ιδανικό —οι συγγραφείς απέδειξαν την ασφάλεια του συστήματος μόνο στο «μοντέλο γενικής ομάδας» (ένα ιδεατό μοντέλο που περιορίζει τις δυνατότητες του επιτιθέμενου). Αργότερα ο Waters [82] βελτίωσε την απόδειξη, ενώ παράλληλα διατήρησε την εκφραστικότητα του συστήματος.

Στις περισσότερες πρακτικές εφαρμογές, η Κρυπτογραφία CP-ABE αποδεικνύεται η πλέον κατάλληλη από τις δύο μορφές. Είναι δόκιμο η πολιτική

πρόσβασης, η οποία αποφαίνεται για τη δυνατότητα αποκρυπτογράφησης ενός κρυπτογραφήματος, να περιλαμβάνεται στο κρυπτογράφημα και όχι στο κλειδί του χρήστη. Αντίστοιχα το κλειδί κάθε χρήστη περιλαμβάνει το σύνολο των χαρακτηριστικών του, βάσει των οποίων αποκρυπτογραφεί ή όχι το κρυπτογράφημα. Στη συνέχεια του κειμένου όπου αναφερόμαστε στην Κρυπτογραφία ABE, θα αναφερόμαστε στην Κρυπτογραφία CP-ABE εκτός κι αν αναφέρεται ρητά διαφορετικά.

4.3 Η τεχνολογία CP-ABE

Ένα σχήμα Κρυπτογραφίας CP-ABE αποτελείται από τέσσερις αλγόριθμους: Εγκατάσταση, Κρυπτογράφηση, Δημιουργία κλειδιού και Αποκρυπτογράφηση.

Εγκατάσταση (λ, U). Ο αλγόριθμος εγκατάστασης δέχεται σαν είσοδο παραμέτρους ασφαλείας λ και το σύνολο των χαρακτηριστικών U. Εξάγει τις δημόσιες παραμέτρους PK και το κύριο κλειδί MK.

Κρυπτογράφηση (PK, M, A). Ο αλγόριθμος κρυπτογράφησης παίρνει ως είσοδο τις δημόσιες παραμέτρους PK, ένα μήνυμα M, και μια φόρμουλα πρόσβασης A επί των χαρακτηριστικών. Ο αλγόριθμος κρυπτογραφεί το μήνυμα M και παράγει ένα κρυπτογράφημα CT, τέτοιο ώστε μόνο ο χρήστης που διαθέτει ένα σύνολο από χαρακτηριστικά που ικανοποιούν τη φόρμουλα πρόσβασης να είναι σε θέση να αποκρυπτογραφήσει το μήνυμα. Θεωρούμε επιπλέον ότι το κρυπτογράφημα περιέχει και την πολιτική A.

Δημιουργία κλειδιού (MK, S). Ο αλγόριθμος δημιουργίας κλειδιού παίρνει ως είσοδο το κύριο κλειδί MK και ένα σύνολο χαρακτηριστικών S που περιγράφουν το κλειδί. Εξάγει ένα ιδιωτικό κλειδί SK.

Αποκρυπτογράφηση (PK, CT, SK). Ο αλγόριθμος αποκρυπτογράφησης παίρνει ως είσοδο τις κοινές παραμέτρους PK, ένα κρυπτογράφημα CT, το οποίο περιέχει μια πολιτική πρόσβασης A, και ένα ιδιωτικό κλειδί SK, το οποίο έχει εκδοθεί για ένα σύνολο χαρακτηριστικών S. Αν το σύνολο S των χαρακτηριστικών ικανοποιεί τη δομή πρόσβασης A τότε ο αλγόριθμος θα αποκρυπτογραφήσει το κρυπτογράφημα και θα επιστρέψει το μήνυμα M.

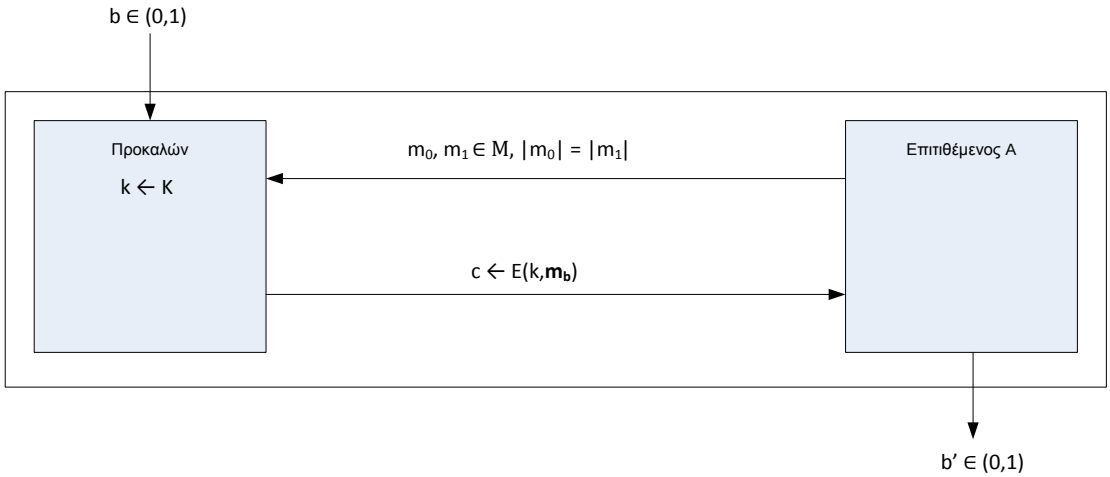
4.4 Ασφάλεια κρυπτογραφικών μοντέλων

Στην παρούσα υποενότητα πραγματοποιείται μια εισαγωγή στην ασφάλεια των κρυπτογραφικών μοντέλων (και δη των σχετικών με την Κρυπτογραφία ABE) και στον τρόπο απόδειξης της ασφαλείας αυτής. Η ανάλυση εστιάζει στις απαραίτητες έννοιες, παραλείποντας ευρείες αναφορές στο μαθηματικό υπόβαθρο ώστε να μη δυσκολευτεί ο —μη εξοικειωμένος με την κρυπτογραφία— αναγνώστης, αλλά παράλληλα να αποκτήσει μια καλύτερη αντίληψη που θα τον βοηθήσει στην κατανόηση των επόμενων παραγράφων.

Ο Claude Shannon ήταν ο πρώτος που εισήγαγε την έννοια της «τέλειας μυστικότητας» (perfect secrecy) το 1949 [85] και απέδειξε ότι το one-time-pad έχει αυτή την ιδιότητα, σύμφωνα με την οποία το κρυπτογραφημένο μήνυμα δεν παρέχει καμία πληροφορία σχετικά με το αρχικό μήνυμα. Δυστυχώς για να έχει ένα σύστημα αυτή την ιδιότητα πρέπει το μήκος του κλειδιού να είναι τουλάχιστον ίσο με μήκος του μηνύματος, κάτι μη πρακτικό.

Οι Goldwasser & Micali το 1984 προχώρησαν στον ορισμό της σημασιολογικής ασφάλειας ενός συστήματος, η οποία έχει την εξής σημασία. Ένα κρυπτογραφικό σύστημα μπορεί να οριστεί ως σημασιολογικά ασφαλές αν ένας επιτιθέμενος, ο οποίος γνωρίζει τον αλγόριθμο κρυπτογράφησης και έχει στην κατοχή του ένα κρυπτογράφημα δεν είναι σε θέση να εξακριβώσει καμία απολύτως πληροφορία σχετικά με το «καθαρό» κείμενο. Η διαφορά με την «τέλεια μυστικότητα» του Shannon έγκειται στο ότι εδώ ο επιτιθέμενος έχει πολυωνυμικά περιορισμένους πόρους. Για τυπικούς ορισμούς της σημασιολογικής ασφάλειας ο αναγνώστης παραπέμπεται στο [86].

Για την απόδειξη της ασφαλείας ενός κρυπτογραφικού σχήματος, χρησιμοποιείται μια μοντελοποίηση αυτού. Ένας προκαλών αλληλεπιδρά με έναν επιτιθέμενο, στον οποίο θέτει μια πρόκληση, την οποία ο επιτιθέμενος προσπαθεί να απαντήσει επιτυχώς. Στη βιβλιογραφία συνήθως αυτή η διαδικασία αναφέρεται και ως παίγνιο. Ο επιτιθέμενος κερδίζει το παίγνιο αυτό εάν μαντέψει σωστά με πιθανότητα μεγαλύτερη αυτής που θα είχε εάν επέλεγε στην τύχη (0.5). Στο Σχήμα 9 απεικονίζεται το παίγνιο στην περίπτωση της σημασιολογικής ασφαλείας για κρυπτογραφία με κλειδί μιας χρήσης.



Σχήμα 9 Παίγνιο στην περίπτωση της σημασιολογικής ασφαλείας (κλειδί μιας χρήσης)

Αρχικά ο επιτιθέμενος (A) διαλέγει δυο μηνύματα (ίσου μήκους) και τα στέλνει στον προκαλών. Ο προκαλών διαλέγει με τη βοήθεια ενός κέρματος ένα από τα δύο μηνύματα και το κρυπτογραφεί με τη χρήση του κλειδιού k. Το κρυπτογραφημένο μήνυμα στέλνεται πίσω στον επιτιθέμενο, ο οποίος επιχειρεί να ανακαλύψει ποιο ήταν το μήνυμα που κρυπτογραφήθηκε. Το πλεονέκτημα του επιτιθέμενου A ως προς τον αλγόριθμο κρυπτογράφησης E στην περίπτωσή αυτή ορίζεται ως εξής:

$$Adv_{ss}[A, E] = |Pr[W_0] - Pr[W_1]|,$$

όπου σαν W_b ορίζουμε το γεγονός το αποτέλεσμα του κέρματος (b) να είναι 0 ή 1.

Εάν οι πιθανότητες $Pr[W_0]$ και $Pr[W_1]$ είναι ίσες τότε το πλεονέκτημα είναι μηδενικό, διαφορετικά όταν το πλεονέκτημα δεν είναι αμελητέο τότε ο επιτιθέμενος έχει σπάσει τη σημασιολογική ασφάλεια του αλγορίθμου E.

Υπάρχουν πολλές παραλλαγές του παραπάνω παιγνίου, οι οποίες διαφέρουν ανάλογα με το υπό εξέταση κρυπτογραφικό σχήμα, το τι θέλει να επιτύχει ο επιτιθέμενος και τι δυνατότητες έχει. Οι κυριότερες μοντελοποιημένες επιθέσεις είναι αυτές του γνωστού κρυπτογραφήματος (COA), του επιλεγμένου αρχικού κειμένου (CPA) και του επιλεγμένου κρυπτογραφήματος (CCA), καθώς και παραλλαγές τους.

Στην πρώτη ο εισβολέας έχει πρόσβαση μόνο σε ένα σύνολο κρυπτογραφημάτων. Η επίθεση είναι απολύτως επιτυχής, εάν μπορούν να συναχθούν τα αντίστοιχα «καθαρά» κείμενα, ή ακόμη καλύτερα, το κλειδί της κρυπτογράφησης. Στην περίπτωση του επιλεγμένου αρχικού κειμένου, ο εισβολέας έχει τη δυνατότητα να επιλέξει αυθαίρετα μη κρυπτογραφημένα κείμενα και να λάβει τα αντίστοιχα

κρυπτογραφήματα. Ο στόχος της επίθεσης είναι να εξαχθεί κάποια επιπλέον πληροφορία η οποία θα μειώσει την ασφάλεια του συστήματος κρυπτογράφησης (ιδανικά το κλειδί της κρυπτογράφησης). Υπάρχουν δύο είδη αυτής της επίθεσης, η απλή και η προσαρμοστική. Στην πρώτη ο επιτιθέμενος έχει προεπιλέξει τα αρχικά κείμενα προς κρυπτογράφηση, ενώ στη δεύτερη μπορεί να τα επιλέγει στην πορεία, ανάλογα με τα αποτελέσματα των προηγούμενων ενεργειών.

Στο τρίτο μοντέλο επίθεσης, αυτό του επιλεγμένου κρυπτογραφήματος, ο επιτιθέμενος έχει πρόσβαση σε ένα «αποκρυπτογραφικό μαντείο» (decryption oracle). Επιλέγει δηλαδή ένα κρυπτογράφημα και αποκτά το αποκρυπτογραφημένο κείμενο (υπό ένα άγνωστο κλειδί). Αν και με μια πρώτη ματιά αυτό το είδος επίθεσης φαίνεται μη ρεαλιστικό (το σύστημα να επιτρέπει την αποκρυπτογράφηση κρυπτογραφημάτων), ωστόσο έχει χρησιμοποιηθεί στην πράξη αρκετές φορές. Για παράδειγμα το κρυπτοσύστημα RSA χρησιμοποιεί τον ίδιο μηχανισμό για την αποκρυπτογράφηση και την υπογραφή, επιτρέποντας την παραπάνω επίθεση. Και αυτή η επίθεση έχει δύο εκφάνσεις, την απλή (CCA) και την προσαρμοστική (CCA2) που είναι και η πλέον ισχυρή.

Η σημασιολογική ασφάλεια δεν είναι επαρκής και αυτό γιατί εξ ορισμού δεν καλύπτει την επίθεση επιλεγμένου κρυπτογραφήματος. Γι αυτό το λόγο έχει επινοηθεί η έννοια της αποδείξιμης ασφαλείας, η απόδειξη δηλαδή ότι δεν υπάρχει επιτιθέμενος που να μπορεί να παραβιάσει το σύστημα. Προϋπόθεση για την αποδείξιμη ασφάλεια ενός συστήματος είναι η διατύπωση όλων των παραμέτρων του παιγνίου με τυπικό τρόπο. Εν συνεχεία το σύστημα αποδεικνύεται ασφαλές εάν η ασφάλεια του μπορεί να αναχθεί σε ένα γνωστό μαθηματικό πρόβλημα που θεωρείται δισεπίλυτο (για παράδειγμα η παραγοντοποίηση ακεραίων ή ο διακριτός λογάριθμος).

Η ασφάλεια των παραπάνω μοντέλων επίθεσης αποδεικνύεται υπό διάφορες παραλλαγές, που εξαρτώνται από το κρυπτογραφικό μοντέλο. Στο κανονικό μοντέλο (standard model) ο επιτιθέμενος περιορίζεται μόνο από το χρόνο και τους υπολογιστικούς πόρους. Σε κάποιες περιπτώσεις όμως για να αποδειχτεί η ασφάλεια ενός συστήματος, χρησιμοποιούνται ιδεατές κατασκευές-συναρτήσεις οι οποίες περιορίζουν τις δυνατότητες του επιτιθέμενου. Τέτοια μοντέλα είναι το μοντέλο «γενικής ομάδας» (όπου ο επιτιθέμενος έχει πρόσβαση σε μια γενική ομάδα και όχι σε κάποια αποδοτική όπως οι ελλειπτικές καμπύλες ορισμένες στο $\mathbb{Z}_p$ ή σε σώματα Galois) και το μοντέλο «τυχαίου

χρησμού» (όπου μια κρυπτογραφική συνάρτηση κατακερματισμού αντικαθίσταται από μια αντίστοιχη ιδεατή συνάρτηση). Στην πράξη ένα σύστημα το οποίο έχει αποδειχτεί ασφαλές υπό το μοντέλο «γενικής ομάδας», συχνά αποδεικνύεται τετριμμένα ανασφαλές υπό το κανονικό μοντέλο.

Στην περίπτωση των Κρυπτογραφιών IBE και ABE έχει υιοθετηθεί μια περαιτέρω παραλλαγή των παραπάνω μοντέλων. Συγκεκριμένα πολλές φορές για την απόδειξη ασφαλείας ενός συστήματος η μοντελοποίηση περιορίζει τον επιτιθέμενο στη δήλωση της ταυτότητας του χρήστη (id) στον οποίο σκοπεύει να επιτεθεί πριν λάβει τις δημόσιες παραμέτρους του συστήματος. Αυτό το μοντέλο καλείται επιλεγμένης ταυτότητας (selective-ID ή s-ID) [87], σε αντίθεση με το προσαρμοστικής ταυτότητας (adaptive-ID), όπου ο επιτιθέμενος μπορεί να επιλέγει την ταυτότητα που θα επιτεθεί ανάλογα με τα πρότερα αποτελέσματα. Ανεξαρτήτως της προεπιλογής (ή όχι) της ταυτότητας, ο επιτιθέμενος μπορεί να πραγματοποιεί προσαρμοστική επίθεση στο κρυπτογράφημα.

Για λόγους πληρότητας ας τονιστεί ότι συνήθως η παραβίαση της ασφαλείας κρυπτογραφικών συστημάτων οφείλεται στην πλημμελή υλοποίηση τους (και όχι σε θεωρητικά κενά). Έτσι προκύπτουν διάφορες επιθέσεις που συνολικά αποκαλούνται «πλαγίου καναλιού», όπως για παράδειγμα η μέτρηση της καθυστέρησης απάντησης σε αλγόριθμους αποκρυπτογράφησης εγκατεστημένων σε εξυπηρετητές διαδικτύου ή η μέτρηση της κατανάλωσης ενέργειας σε έξυπνες κάρτες, τα οποία αποκαλύπτουν πληροφορίες σχετικά με την επιτυχή ή όχι αποκρυπτογράφηση.

4.5 Εφαρμοσμένη Κρυπτογραφία βάσει χαρακτηριστικών – Ανοιχτά θέματα

Η Κρυπτογραφία ABE αποτελεί μια από τις πιο ενεργές περιοχές έρευνας στον τομέα της κρυπτογραφίας, λόγω εν μέρει και της εγγενούς καταλληλότητας της για παροχή ασφαλείας στο νέφος (cloud). Η παραδοσιακή ασύμμετρη κρυπτογραφία (υποδομή δημοσίου κλειδιού) είναι «ένα προς ένα», δηλαδή κάθε ευαίσθητο έγγραφο κρυπτογραφείται προς έναν υποψήφιο αποδέκτη (με χρήση του δημόσιου κλειδιού του). Σε περιβάλλοντα υπολογιστικού νέφους, όπου η αποθήκευση ενός τέτοιου εγγράφου γίνεται σε ημιέμπιστους διαδικτυακούς εξυπηρετητές η κρυπτογράφηση προς κάθε χρήστη ξεχωριστά θα επέφερε μεγάλο διαχειριστικό κόστος, και βέβαια το αντίστοιχο κόστος σε χωρητικότητα. Η Κρυπτογραφία ABE με την «1 προς N» κρυπτογράφησή της

δίνει απάντηση σε αυτό το πρόβλημα. Για το λόγο αυτό, τυγχάνει και εκτενούς χρηματοδότησης, ιδιαίτερα στην Αμερική.

Βεβαίως στο δρόμο για την καθιέρωση της Κρυπτογραφίας ABE σαν μια πρακτική λύση, η έρευνα έχει πολλά ανοιχτά θέματα να επιλύσει. Ένα από τα κυρίαρχα είναι η επίδοση των αλγορίθμων κρυπτογράφησης και —κυρίως— αποκρυπτογράφησης. Η αποκρυπτογράφηση αποτελεί μεγαλύτερη πρόκληση καθώς αφενός πραγματοποιείται πολλαπλάσιες φορές από την κρυπτογράφηση και αφετέρου τα τελικά τερματικά πιθανότατα είναι κινητά ή άλλες συσκευές σχετικά περιορισμένων δυνατοτήτων. Σε κάθε (από)κρυπτογράφηση πραγματοποιείται ένας αριθμός υπολογισμών – αυτοί συνήθως είναι υψώσεις σε δύναμη και διγραμμικές απεικονίσεις, ο αριθμός των οποίων συνήθως εξαρτάται από παραμέτρους όπως ο αριθμός των χαρακτηριστικών των χρηστών που περιλαμβάνονται στο σύστημα ή ο αριθμός των χαρακτηριστικών που περιλαμβάνονται στην πολιτική πρόσβασης. Οι αρχικές υλοποιήσεις της Κρυπτογραφίας ABE σε πραγματικές συνθήκες (π.χ. με 100 διακριτά χαρακτηριστικά) είχαν αποτέλεσμα χρόνους αποκρυπτογράφησης της τάξης μερικών δευτερολέπτων, χρόνος απαγορευτικός για εφαρμογές πραγματικού χρόνου.

Ειδικότερα υπάρχει μια τριπλή διελκυστίνδα μεταξύ της επίδοσης της κρυπτογράφησης, της εκφραστικότητας της πολιτικής πρόσβασης καθώς και του επιτεύξιμου επιπέδου ασφαλείας. Ας εστιάσουμε στην ανταγωνιστική σχέση εκφραστικότητας και επίδοσης. Η εκφραστικότητα ενός σχήματος Κρυπτογραφίας ABE είναι συνάρτηση της δομής (ή φόρμουλας) πρόσβασης. Η δομή πρόσβασης μπορεί να παρασταθεί από μια Boolean φόρμουλα ή ένα δέντρο, τα φύλλα του οποίου είναι τα χαρακτηριστικά ενώ τα κλαδιά (εσωτερικοί κόμβοι) αναπαριστούν πύλες AND, OR και 1 από N. Στις πρώτες υλοποιήσεις, το μέγεθος του κρυπτογραφήματος και οι χρόνοι κρυπτογράφησης και αποκρυπτογράφησης ήταν γραμμικοί είτε ως προς το μέγεθος του δέντρου πρόσβασης [83] είτε ως προς το συνολικό αριθμό των χαρακτηριστικών που έχουν καθοριστεί στο σύστημα [88]. Επιπροσθέτως —όπως θα δούμε και στη συνέχεια— η δυνατότητα ανάκλησης συγκεκριμένων χρηστών επηρεάζει και αυτή τις επιδόσεις της Κρυπτογραφίας ABE.

Ο Waters [82] χρησιμοποιώντας στη θέση του δέντρου πρόσβασης ένα πίνακα γραμμικού διαμοιρασμού-μυστικών (Linear Secret-Sharing Scheme, LSSS) διατήρησε την εκφραστικότητα και τις επιδόσεις του [83], βελτιώνοντας το επίπεδο ασφαλείας σε

επιλεγμένης-ταυτότητας υπό το κανονικό μοντέλο. Η Lewko [89] κατάφερε πρώτη να αποδείξει την πλήρη ασφάλεια υπό το κανονικό μοντέλο, χρησιμοποιώντας τη μεθοδολογία απόδειξης «Κρυπτογράφησης Δυαδικού Συστήματος» [90]. Στην πρότασή της, το μέγεθος των κλειδιών και του κρυπτογραφήματος κλιμακώνονται γραμμικά ως προς τον αριθμό των χαρακτηριστικών.

4.6 Ανάκληση χρηστών

Η ανάκληση χρηστών είναι ένα πολύπλοκο θέμα ακόμα στην κλασσική Κρυπτογραφία PKI. Στην Κρυπτογραφία ABE είναι επιπλέον δύσκολο, λόγω της έλλειψης μοναδικών (για κάθε χρήστη) χαρακτηριστικών στα κλειδιά και στα κρυπτογραφήματα. Τα χαρακτηριστικά, βάσει των οποίων γίνεται η κρυπτογράφηση, κατά κανόνα είναι κοινά για τους αποδέκτες χρήστες. Έτσι, η ανάκληση ενός και μόνο χρήστη δεν είναι μια τετριμμένη διαδικασία, καθώς ανάκληση ενός χαρακτηριστικού συνεπάγεται πιθανή ανάκληση πολλών χρηστών.

Παρόλη την πολυπλοκότητα της διαδικασίας, ήδη από την εισαγωγή της Κρυπτογραφίας CP-ABE [84] προτάθηκε ένα πρώτο απλό σχέδιο ανάκλησης χρηστών. Μια ημερομηνία λήξης προσαρτάται σε κάθε ένα από τα χαρακτηριστικά, αναγκάζοντας το χρήστη να ανανεώνει περιοδικά κλειδιά του. Έτσι τυχόν ανακλημένοι χρήστες θα αποκλείονται από την ανανέωση των κλειδιών τους.

Στην εργασία των Piretti et al [91] έγινε η πρώτη προσπάθεια εφαρμογής της Κρυπτογραφίας ABE στην πράξη. Μελετήθηκαν κυρίως η υλοποίηση των δομών πρόσβασης και οι επιδόσεις της Κρυπτογραφίας ABE σε συνάρτηση με το είδος της ελλειπτικής καμπύλης που επιλέγεται. Από τα πρώτα συμπεράσματα ήταν η σημασία της εισαγωγής του αρνητικού τελεστή στη δομή πρόσβασης, η οποία μέχρι τότε δεν είχε καταστεί δυνατή. Οι Ostrovsky, Sahai, και Waters [92] ήταν οι πρώτοι που συμπεριέλαβαν και τον αρνητικό τελεστή στις δομές πρόσβασης, διατηρώντας τις επιδόσεις του συστήματος σε συγκρίσιμο επίπεδο σε σχέση με τις προηγούμενες προτάσεις. Είναι προφανής η σημασία του αρνητικού τελεστή για την ανάκληση καθώς πλέον θα μπορούσε να προστεθεί στο κρυπτογράφημα και η άρνηση ενός συγκεκριμένου χρήστη.

Αυτή η προσέγγιση βέβαια έχει το μειονέκτημα της γραμμικής μεγέθυνσης του κρυπτογραφήματος και παράλληλα της λογαριθμικής μεγέθυνσης των κλειδιών, καθώς η λίστα ανάκλησης μεγαλώνει. Σε κάθε περίπτωση όμως αυτό είναι προτιμητέο σε σχέση

με την περιοδική επανέκδοση των κλειδιών, η οποία μπορεί να ενεργεί σαν συμφόρηση σε συστήματα Κρυπτογραφίας ABE (ειδικά όταν έχουμε να κάνουμε με μία μόνο αρχή πιστοποίησης).

Μια επόμενη προσέγγιση βελτιώνει τις επιδόσεις αυτές. Η εργασία των Lewko et al [93] βελτίωσε την αποτελεσματικότητα του [92], μέσω της επίτευξης μικρότερων και σταθερών σε μέγεθος κλειδιών, αλλά η γραμμική κλιμάκωση του κρυπτογραφήματος ως προς το πλήθος των ανακληθέντων χρηστών εξακολουθεί. Και στα δύο παραπάνω συστήματα ο κρυπτογράφος υποτίθεται ότι έχει γνώση της λίστας ανάκλησης (κάτι που δεν είναι εφικτό σε όλες τις περιπτώσεις).

Στην πρόταση των Boldyreva et al [94] προτείνεται ένα σύστημα ανάκλησης σε Κρυπτογραφία IBE, το οποίο συνδυάζει δυαδικά δέντρα και Κρυπτογραφία ABE (αντιμετωπίζοντας τον χρόνο ως ένα «ειδικό» χαρακτηριστικό). Το σχέδιό τους βελτιώνει την απόδοση της ενημέρωσης των κλειδιών, με τη χρήση ενός «κλειδιού ενημέρωσης» σε συνδυασμό με το ιδιωτικό κλειδί του χρήστη. Για την επιτυχή αποκρυπτογράφηση απαιτούνται και τα δύο κλειδιά. Οι χρήστες λαμβάνουν περιοδικά το «κλειδί-ενημέρωσης», εκτός αν ανακληθούν. Αν και η εργασία γίνεται στο πλαίσιο της ανάκλησης χρηστών σε Κρυπτογραφία IBE γίνεται ειδική μνεία ότι ένα τέτοιο σύστημα μπορεί να εφαρμοστεί και στην Κρυπτογραφία ABE.

Στην τεχνική έκθεση [95], η οποία επεκτείνει τις προτάσεις της [94] σε συστήματα Κρυπτογραφίας ABE, οι συγγραφείς παρουσιάζουν το σύστημα τους ως Κρυπτογραφία CP-ABE με Ανάκληση. Ένα —μοναδικό για κάθε χρήστη— αναγνωριστικό εντάσσεται στην Κρυπτογραφία ABE. Αυτό χρησιμεύει μόνο για τους σκοπούς της ανάκλησης, η κρυπτογράφηση και η αποκρυπτογράφηση μπορεί να γίνουν χωρίς να ληφθεί υπόψη αυτό το αναγνωριστικό. Ο κρυπτογράφος δεν είναι υποχρεωμένος να γνωρίζει τους υπό ανάκληση χρήστες. Αυτό είναι ευθύνη του διαχειριστή του συστήματος, ο οποίος δημοσιεύει περιοδικά ενημερωμένα στοιχεία (με τη μορφή ενός δέντρου ανάκλησης).

Η εργασία των Attrapadung et al [96] συνδυάζει τα συστήματα των εργασιών [94] και [97] (προηγούμενη εργασία των ιδίων), για τη δημιουργία ενός υβριδικού συστήματος. «Άμεση ανάκληση» [97] σημαίνει ότι ο κρυπτογράφος περιλαμβάνει ρητά τη λίστα ανάκλησης στο κρυπτογράφημα, ενώ στην «έμμεση ανάκληση» [94] το έργο ανάκλησης ανατίθεται στο διαχειριστή του συστήματος. Οι συγγραφείς υποστηρίζουν ότι αν και η υπόθεση της «άμεσης ανάκλησης» μπορεί να μοιάζει μη ρεαλιστική, σε ορισμένες

περιπτώσεις, όπως στην Pay-TV είναι κοινή τακτική (ο πάροχος περιεχομένου / κρυπτογράφος γνωρίζει την λίστα ανάκλησης). Το υπόλοιπο της πρότασής τους επικεντρώνεται στον αποτελεσματικό συνδυασμό των δύο υποσυστημάτων.

Σε ένα παρόμοιο περιβάλλον (Pay-TV), όπου ο αποστολέας ανακρυπτογραφεί το κρυπτογράφημα λαμβάνοντας υπόψη την ανανεωμένη λίστα ανάκλησης, η εργασία [98] παρουσιάζει ένα σχέδιο ανάκλησης που δίνει τη δυνατότητα λεπτομερούς ανάκλησης. Έτσι δίνεται η δυνατότητα ανάκλησης ενός χαρακτηριστικού του χρήστη, χωρίς να ανακληθεί ο χρήστης συνολικά και χωρίς να επηρεαστούν οι άλλοι χρήστες που μοιράζονται το χαρακτηριστικό αυτό.

Σε ορισμένες πιο πρόσφατες εργασίες, η Κρυπτογραφία ABE συνδυάζεται με την τεχνική της ανακρυπτογράφησης σε πληρεξούσιο κόμβο (Proxy Re-Encryption - PRE) [99], προκειμένου να παρασχεθεί αποτελεσματική ανάκληση. Η κεντρική ιδέα πίσω από τις προτάσεις αυτές είναι η εκτέλεση των υπολογιστικά απαιτητικών εργασιών σε ημι-αξιόπιστους πληρεξούσιους κόμβους (στην περίπτωση ανάκλησης εκδίδονται νέα κλειδιά και τα κρυπτογραφήματα κρυπτογραφούνται εκ νέου). Οι εργασίες αυτές εκτελούνται σε πληρεξούσιους κόμβους.

Συγκεκριμένα η πρόταση των Yu et al [100] δίνει έμφαση σε πρακτικά σενάρια στα οποία είναι διαθέσιμοι ημιαξιόπιστοι online κόμβοι μεσολάβησης. Η εργασία τους επιτρέπει στην αρχή πιστοποίησης να ανακαλέσει οποιοδήποτε αριθμό χρηστών, ενώ ο υπολογιστικός φόρτος ανατίθεται σε εξωτερικούς πληρεξούσιους κόμβους.

Στην εργασία των Wang et al [101] εισάγεται η I-ABE (Ιεραρχική ABE) με κλιμακούμενη ανάκληση χρήστη. Το σύστημα ανάκλησης επιτρέπει την ανάθεση των πιο «έντονων» εργασιών στα πλαίσια της ανάκλησης σε φορείς παροχής υπηρεσιών Cloud (CSP), χωρίς να αποκαλύψει το περιεχόμενο των δεδομένων, συνδυάζοντας την προσέγγιση της ανακρυπτογράφησης σε πληρεξούσιο κόμβο (Proxy Re-encryption - PRE) και αυτήν της «οκνηρής» ανακρυπτογράφησης (Lazy Re-encryption - LRE).

Τα συστήματα των προτάσεων [100], [101] διαφέρουν σε αρκετά σημεία (στη δυνατότητά εφαρμογής τους στις Κρυπτογραφίες CP-ABE και KP-ABE, στην εκφραστικότητα των δομών πρόσβασης τους και στο επιτεύξιμο επίπεδο ασφαλείας τους).

4.7 Πολλαπλές αρχές πιστοποίησης

Ακόμα κι από τα πιο απλά σενάρια γίνεται σαφές ότι δεν είναι ρεαλιστικό, μια μοναδική αρχή πιστοποίησης να είναι υπεύθυνη για όλα τα χαρακτηριστικά των χρηστών. Για παράδειγμα η ικανότητα οδήγησης πιστοποιείται από το Υπουργείο Μεταφορών, η ασφαλιστική ενημερότητα από τον ασφαλιστικό φορέα και η φορολογική από την αρμόδια εφορία, δηλαδή έχουμε τρεις διακριτές αρχές πιστοποίησης χαρακτηριστικών. Η εισαγωγή περισσότερων της μίας αρχών πιστοποίησης όμως δεν είναι κάτι τετριμμένο, όπως θα δούμε παρακάτω.

Στο κλασσικό σχήμα με τη μοναδική αρχή πιστοποίησης η ιδιότητα της αποτροπής της κακόβουλης σύμπραξης χρηστών επιτυγχάνεται ως εξής. Το μυστικό κλειδί κάθε χρήστη δημιουργείται από διαφορετικά τυχαία μέρη του μυστικού. Έτσι καθίσταται αδύνατη η συνεργασία μεταξύ των χρηστών. Σε ένα περιβάλλον με πολλές αρχές πιστοποίησης, οι οποίες δεν επικοινωνούν μεταξύ τους (για λόγους πρακτικούς ή προστασίας των προσωπικών δεδομένων των χρηστών) η παραπάνω λύση δεν είναι εφικτή.

Η εργασία της Chase [102] έδωσε μια πρώτη ικανοποιητική λύση στο πρόβλημα αυτό εισάγοντας δύο νέες παραμέτρους. Πρώτον κάθε χρήστης ταυτοποιείται από ένα καθολικό αναγνωριστικό και δεύτερον η ύπαρξη μιας έμπιστης κεντρικής αρχής πιστοποίησης, η οποία συμμετέχει στη δημιουργία του κλειδιού κάθε χρηστή με βάση το αναγνωριστικό του. Στη συνέχεια, χρησιμοποιώντας ψευδοτυχαίες συναρτήσεις (PRFs) εξασφαλίζεται ότι τα κλειδιά των χρηστών δε μπορούν να συνδυαστούν. Η προτεινόμενη λύση παρόλα τα θετικά της, παρουσιάζει την εξής αδυναμία. Ενδεχομένως κακόβουλες αρχές πιστοποίησης να συνεργαστούν και με βάση το μοναδικό αναγνωριστικό του χρήστη να φτιάξουν ένα προφίλ του, κάτι που απειλεί την ιδιωτικότητα των χρηστών. Αναγνωρίζοντας αυτή την απειλή η μετέπειτα εργασία των Chase και Chow [103] βελτιώνει την αρχική λύση αφαιρώντας την έμπιστη κεντρική αρχή πιστοποίησης και εισάγοντας ένα πρωτόκολλο ανώνυμης έκδοσης κλειδιών (το οποίο στηρίζεται πάνω σε ένα πρωτόκολλο «ανυποψίαστου υπολογισμού» (oblivious computation)). Με αυτόν τον τρόπο το κλειδί παράγεται «ανυποψίαστα», χωρίς δηλαδή να χρειαστεί να αποκαλύψουν ευαίσθητες πληροφορίες ο χρήστης και η αρχή πιστοποίησης. Ένας πρακτικός περιορισμός των δύο παραπάνω προτάσεων είναι ότι απαιτείται από το χρήστη να έχει χαρακτηριστικά από όλες τις (προκαθορισμένες) αρχές πιστοποίησης.

Στην εργασία των Lin et al [104] παρουσιάζεται ένα σύστημα «κατωφλιού» το οποίο είναι επίσης μερικώς αποκεντρωμένο. Το σύνολο των αρχών πιστοποίησης είναι προκαθορισμένο εξ αρχής, ενώ απαιτείται η αλληλεπίδραση αυτών κατά τη διάρκεια της εγκατάστασης του συστήματος. Το σύστημα είναι ασφαλές εάν συμπράξουν έως m χρήστες, όπου το *m* είναι μία παράμετρος που επιλέγεται κατά τη ρύθμιση του συστήματος. Οι επιδόσεις του συστήματος και η αποθήκευση των κλειδιών συναρτώνται με την παράμετρο m.

Σε νεότερη εργασία των Lewko και Waters [105] παρουσιάστηκε ένα σύστημα, στο οποίο κάθε συμμετέχων μπορεί να γίνει αρχή πιστοποίησης. Επιπλέον δεν απαιτείται μια κεντρική έμπιστη αρχή, κάτι το οποίο θα δρούσε σαν συμφόρηση σε μεγάλα συστήματα. Σε σχέση με προηγούμενα συστήματα, επιτυγχάνεται μεγαλύτερη εκφραστικότητα – η δομή πρόσβασης μπορεί να περιλαμβάνει οποιαδήποτε Boolean φόρμουλα (με την εξαίρεση του τελεστή NOT) επί χαρακτηριστικών τα οποία έχουν εκδοθεί από ένα οποιοδήποτε υποσύνολο αρχών πιστοποίησης. Σε σχέση με την Κρυπτογραφία ABE που υποστηρίζει μία μοναδική αρχή πιστοποίησης, η Κρυπτογραφία ABE με πολλαπλές αρχές πιστοποίησης έχει στη θέση του αλγορίθμου εγκατάστασης, δυο αλγορίθμους εγκατάστασης, έναν συνολικό και έναν για κάθε αρχή πιστοποίησης.

4.8 Απόκρυψη χαρακτηριστικών

Μια άλλη ερευνητική κατεύθυνση εστιάζει στο πρόβλημα της απόκρυψης των χαρακτηριστικών. Τόσο στην Κρυπτογραφία IBE όσο και στην Κρυπτογραφία ABE αυτό που επιτυγχάνεται είναι η απόκρυψη του περιεχομένου. Τα χαρακτηριστικά των χρηστών βάσει των οποίων γίνεται η (από)κρυπτογράφηση δεν είναι αντίστοιχα προστατευμένα. Σε πολλές περιπτώσεις τα χαρακτηριστικά αυτά αποτελούν καθαυτά ευαίσθητα προσωπικά δεδομένα και θα ήταν επιθυμητή η απόκρυψή τους (π.χ. σε περιπτώσεις ασθενών).

Η Κρυπτογραφία Κατηγορήματος (Predicate Encryption) δίνει λύση σε αυτό το πρόβλημα. Η γενική ιδέα είναι η εξής, έστω ότι το κρυπτογράφημα έχει κρυπτογραφηθεί με βάση την πολιτική χ ενώ η παράμετρος υ χαρακτηρίζει το κλειδί του χρήστη. Η σχέση $P(\upsilon,\chi)$ ισχύει εάν το κλειδί (υ) αποκρυπτογραφεί το κρυπτογράφημα (χ). Ο χρήστης μαθαίνει μόνο εάν ισχύει αυτή η σχέση (ή όχι) χωρίς να πληροφορείται για τις παραμέτρους υ, χ. Η ευρύτερη τάξη σχέσεων τέτοιας μορφής στη βιβλιογραφία είναι

αυτή του εσωτερικού γινομένου. Σε αυτήν το κλειδί αναπαριστάται με ένα διάνυσμα v και το κρυπτογράφημα με ένα διάνυσμα χ. Η σχέση $P(v,\chi)$ ισχύει εάν και μόνο εάν $v \times \chi = 0$.

Η ασφάλεια της απόκρυψης των χαρακτηριστικών ταξινομείται σε σθεναρή και αδύναμη. Στην περίπτωση της σθεναρής δε διαρρέει καμία πληροφορία για τα v, χ είτε η $P(v,\chi)$ ισχύει είτε όχι, ενώ στην περίπτωση της αδύναμης, αυτό είναι εγγυημένο μόνο στην περίπτωση που η $P(v,\chi)$ δεν ισχύει.

Οι Boneh και Waters [106] κατέστησαν εφικτό ένα σύστημα ανώνυμης Κρυπτογραφίας IBE, ενώ στο [107] οι Katz, Sahai και Waters επεκτείνουν τα αποτελέσματα αυτά και στην περίπτωση της Κρυπτογραφίας ABE, επιτρέποντας την απόκρυψη των χαρακτηριστικών των χρηστών (υπό τη σθεναρή έννοια). Παρ' όλα αυτά το επίπεδο ασφαλείας της κρυπτογράφησης καθεαυτής δεν ήταν το επιθυμητό, στοιχείο που βελτιώνεται στην πρόσφατη εργασία των Okamoto και Takashima [108]. Δυστυχώς σε όλες τις προσεγγίσεις τα μεγέθη των κλειδιών (δημόσιο και ιδιωτικό) καθώς και του κρυπτογραφήματος κλιμακώνονται γραμμικά ως προς τον αριθμό των χαρακτηριστικών.

4.9 Εφαρμογές

Παρά το σύντομο χρόνο ζωής της, η Κρυπτογραφία ABE φαίνεται να βρίσκει πολλές πρακτικές εφαρμογές, λόγω των μοναδικών χαρακτηριστικών της. Οι περισσότερες προτάσεις βρίσκουν πεδίο εφαρμογής στην προστασία των προσωπικών δεδομένων σε πλατφόρμες κοινωνικής δικτύωσης [109], διαχείρισης ιατρικών δεδομένων [110], εξειδικευμένων δικτύων οχημάτων [111], ενώ άλλες στην προστασία ψηφιακού περιεχομένου σε συστήματα συνδρομητικής τηλεόρασης [112].

Αναλυτικά, στο [109] προτείνεται το κοινωνικό δίκτυο Persona —στα πρότυπα του Facebook, στο οποίο οι χρήστες διαχειρίζονται τα προσωπικά τους δεδομένα (τα οποία είναι αποθηκευμένα στο σύστημα) με τη χρήση Κρυπτογραφίας ABE, ώστε να τα προστατεύσουν από μη-εξουσιοδοτημένη πρόσβαση. Στην πρόταση των Akinyele et al [110], περιγράφεται η λύση τους για την προστασία ευαίσθητων ιατρικών δεδομένων με χρήση Κρυπτογραφίας ABE, όπου τα δεδομένα των ασθενών κρυπτογραφούνται βάσει πολιτικών πρόσβασης επί των ρόλων των εμπλεκομένων (ασθενείς, ιατροί, νοσοκόμοι,

ασφαλιστικοί πράκτορες). Στην εργασία [111] προτείνεται η Κρυπτογραφία ABE για την προστασία δεδομένων που ανταλλάσσονται σε δίκτυα που απαρτίζονται από οχήματα (Vehicular ad hoc networks), και στα οποία λόγω της ταχέως μεταβαλλόμενης σύνθεσής τους, η επίτευξη σχέσεων εμπιστοσύνης είναι προβληματική. Τέλος, στο [112], το οποίο είναι και το πιο παρεμφερές στο αντικείμενο της Διατριβής, καθώς αφορά την προστασία ψηφιακού περιεχομένου, οι Traynor et al εστιάζουν στην εφαρμοσιμότητα της Κρυπτογραφίας ABE στη συνδρομητική τηλεόραση, μελετώντας την επίδοση των συστημάτων αυτών (χρόνοι κρυπτογράφησης και αποκρυπτογράφησης) σε σχέση με τον αριθμό των χρηστών και των χαρακτηριστικών τους, τα οποία απαρτίζουν τις πολιτικές πρόσβασης.

Ας τονιστεί ότι καμία από τις παραπάνω προτάσεις δεν εξετάζει την Κρυπτογραφία ABE σε συνέργεια με τα Δίκτυα ICN, όπως η παρούσα Διατριβή. Επίσης, οι υλοποιήσεις βασίζονται στην αρχική κατασκευή CP-ABE [84] (με εξαίρεση την [110] που στηρίζεται στην βελτιωμένη πρόταση του Waters [90]), η οποία δεν ήταν προσανατολισμένη στην επίδοση, αλλά στην επιτευξιμότητα του κρυπτογραφικού συστήματος.

5 Διαδικασίες διανομής πολυμεσικού περιεχομένου

Το Κεφάλαιο παρουσιάζει τις διαδικασίες που συνθέτουν την προτεινόμενη λύση. Καταρχάς περιγράφεται το πρωτόκολλο απόκτησης της άδειας χρήσης πολυμεσικού περιεχομένου με χρήση πολλαπλών αρχών πιστοποίησης. Εξετάζονται δύο περιπτώσεις – με χρήση κεντρικού κόμβου και πλήρως αποκεντρωμένο σύστημα και επιλέγεται το δεύτερο, για λόγους που εξηγούνται αναλυτικά. Ακολουθεί η προτεινόμενη αρχιτεκτονική δικτύου που ενσωματώνει την Κρυπτογραφία ABE σε ένα —βασισμένο σε Δίκτυα ICN— σύστημα διανομής πολυμέσων. Τέλος διερευνάται η ανάκληση χρηστών υπό το πρίσμα της συνέργειας Κρυπτογραφίας ABE και Δικτύων ICN και προτείνεται ένα κατάλληλο σχέδιο ανάκλησης.

5.1 Απόκτηση άδειας

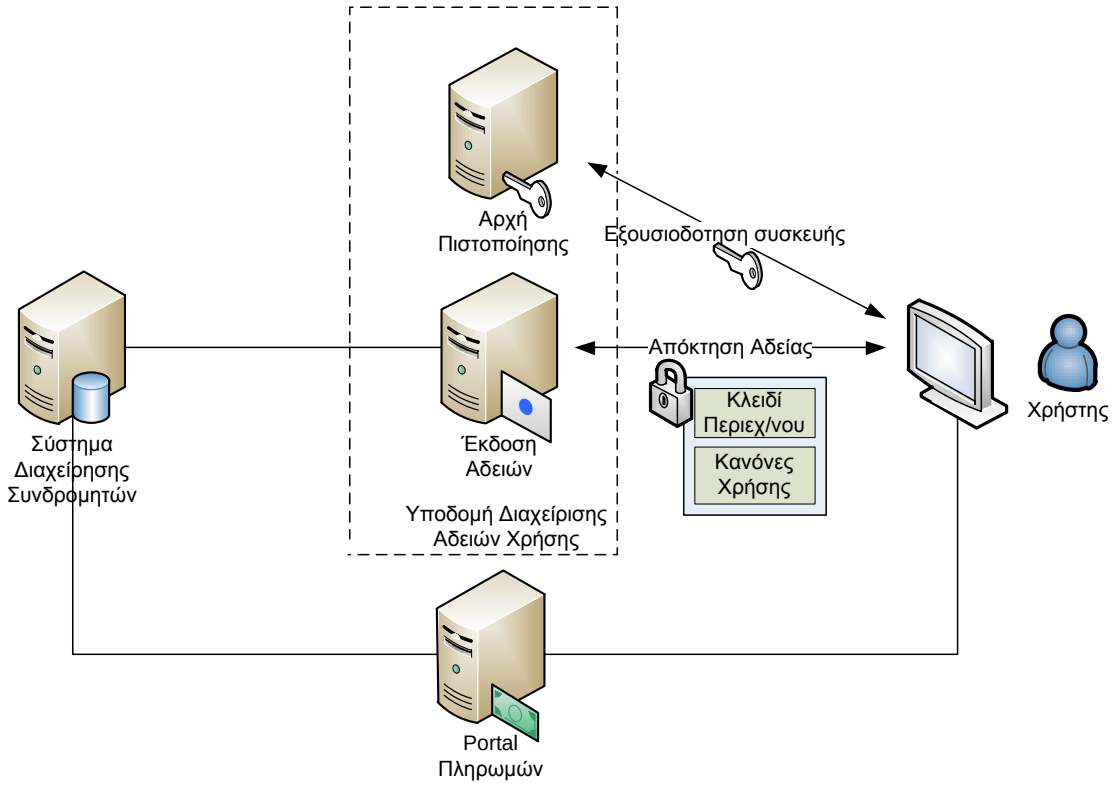
Η ενότητα αυτή εστιάζει στους μηχανισμούς της προτεινόμενης προσέγγισης αναφορικά με την απόκτηση άδειας χρήσης. Η Κρυπτογραφία ABE ενσωματώνεται σε συστήματα DRM, ώστε να επιτρέπει την ασφαλή απόκτηση άδειας πάνω από Δίκτυα ICN (αλλά πάνω και από την υφιστάμενη αρχιτεκτονική Διαδικτύου). Το σημείο εστίασης της προσέγγισής μας είναι η διαδικασία έκδοσης αδειών, σκιαγραφώντας ένα πρωτόκολλο το οποίο ανταποκρίνεται ρεαλιστικά στις απαιτήσεις των παρόχων.

Όπως σε κάθε αγορά, οι Πάροχοι Υπερκείμενων Υπηρεσιών προσπαθούν να βελτιώσουν τις υπηρεσίες τους και να αποκτήσουν, έτσι, ανταγωνιστικό πλεονέκτημα. Μεταξύ άλλων, αυτό επιτυγχάνεται προσφέροντας εξατομικευμένες υπηρεσίες σε κάθε χρήστη. Στην πράξη, συνήθως αυτό υλοποιείται μέσω της προώθησης πακέτων περιεχομένου, π.χ., «Προνομιακό Πακέτο», «Πακέτο Αθλημάτων», τα οποία συγκεντρώνουν περιεχόμενο από περισσότερους του ενός παρόχους περιεχομένου. Για την υλοποίηση αυτών των εξατομικευμένων υπηρεσιών, οι πάροχοι εστιάζουν στη δημιουργία υποδομών, όπως συστήματα διαχείρισης συνδρομητών και περιεχομένου. Παράλληλα επενδύουν σε συστήματα DRM για τη διασφάλιση του περιεχομένου από την πειρατεία και κατ' επέκταση την εξασφάλιση των εσόδων τους. Η κρυπτογράφηση των αδειών γίνεται συνήθως με χρήση ασύμμετρης κρυπτογράφησης (PKI) [113], ενώ η

κρυπτογράφηση του περιεχομένου γίνεται βάσει του πρωτοκόλλου Advanced Encryption Standard Chain Block Cipher (AES CBC) [114].

Οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση —μέσω ενός διακομιστή αδειών χρήσης— σε μια άδεια, η οποία περιλαμβάνει το κλειδί αποκρυπτογράφησης του περιεχομένου. Οι άδειες περιλαμβάνουν, εκτός από το κλειδί αποκρυπτογράφησης, και κανόνες που σχετίζονται με το μοντέλο χρήσης —για παράδειγμα, ποιες από τις συσκευές που βρίσκονται στην κατοχή ενός χρήστη επιτρέπεται να αναπαράγουν το περιεχόμενο και πόσες φορές. Οι κανόνες αυτοί αντανακλούν τους όρους στους οποίους συμφωνούν ο χρήστης και ο πάροχος. Οι συσκευές πρέπει να πληρούν ορισμένα πρότυπα εμπιστοσύνης, που καθορίζονται από τον πάροχο, ο οποίος αναλαμβάνει την έκδοση πιστοποιητικών PKI για τις αξιόπιστες συσκευές. Οι ευαίσθητες πληροφορίες αποθηκεύονται είτε σε ασφαλές λογισμικό (Sandbox) είτε αντίστοιχα σε ασφαλές υλικό (Trusted Platform Module) στη συσκευή. Η τεχνολογία PlayReady DRM της Microsoft, για παράδειγμα, δημιουργεί ένα δομικό στοιχείο εξατομίκευσης στο Silverlight Sandbox κάθε έμπιστης συσκευής, το οποίο αναλαμβάνει τη διαχείριση των αδειών χρήσης και λοιπών ευαίσθητων πληροφοριών [115]. Το αιτούμενο πολυμεσικό περιεχόμενο κρυπτογραφείται χρησιμοποιώντας το συμμετρικό κλειδί, το οποίο περιλαμβάνεται στην άδεια, επιτρέποντας στον κάτοχό της αδείας την αποκρυπτογράφηση του. Το τμήμα της διαχείρισης αδειών ενός παρόχου υπηρεσιών OTT παρατίθεται στο Σχήμα 10.

Στην προτεινόμενη λύση, τα συνδρομητικά πακέτα αντιστοιχίζονται σε χαρακτηριστικά. Για παράδειγμα, όταν ένας χρήστης αγοράζει ένα «Προνομιακό Πακέτο» αποκτά το σχετικό χαρακτηριστικό «Προνομιακός Χρήστης». Ο χρήστης μπορεί να επιδείξει στη συνέχεια, αυτό το χαρακτηριστικό σε μια Αρχή Πιστοποίησης, η οποία αποτελεί τμήμα της λύσης DRM, και να αποκτήσει ένα αντίστοιχο κλειδί. Ένας χρήστης μπορεί να αποκτήσει πρόσθετα χαρακτηριστικά σε μεταγενέστερο χρόνο και τα κλειδιά του θα επικαιροποιηθούν αναλόγως. Τα κλειδιά αυτά αποθηκεύονται σε μια ασφαλή μονάδα στη συσκευή του χρήστη. Στο διακομιστή έκδοσης αδειών χρήσης, οι άδειες κρυπτογραφούνται αναλόγως. Μία άδεια που αντιστοιχεί στο «Προνομιακό Πακέτο» μπορεί να κρυπτογραφηθεί υπό το «Προνομιακό» χαρακτηριστικό, επιτρέποντας εν συνεχεία στους χρήστες που κατέχουν αυτό το χαρακτηριστικό να την αποκρυπτογραφήσουν.

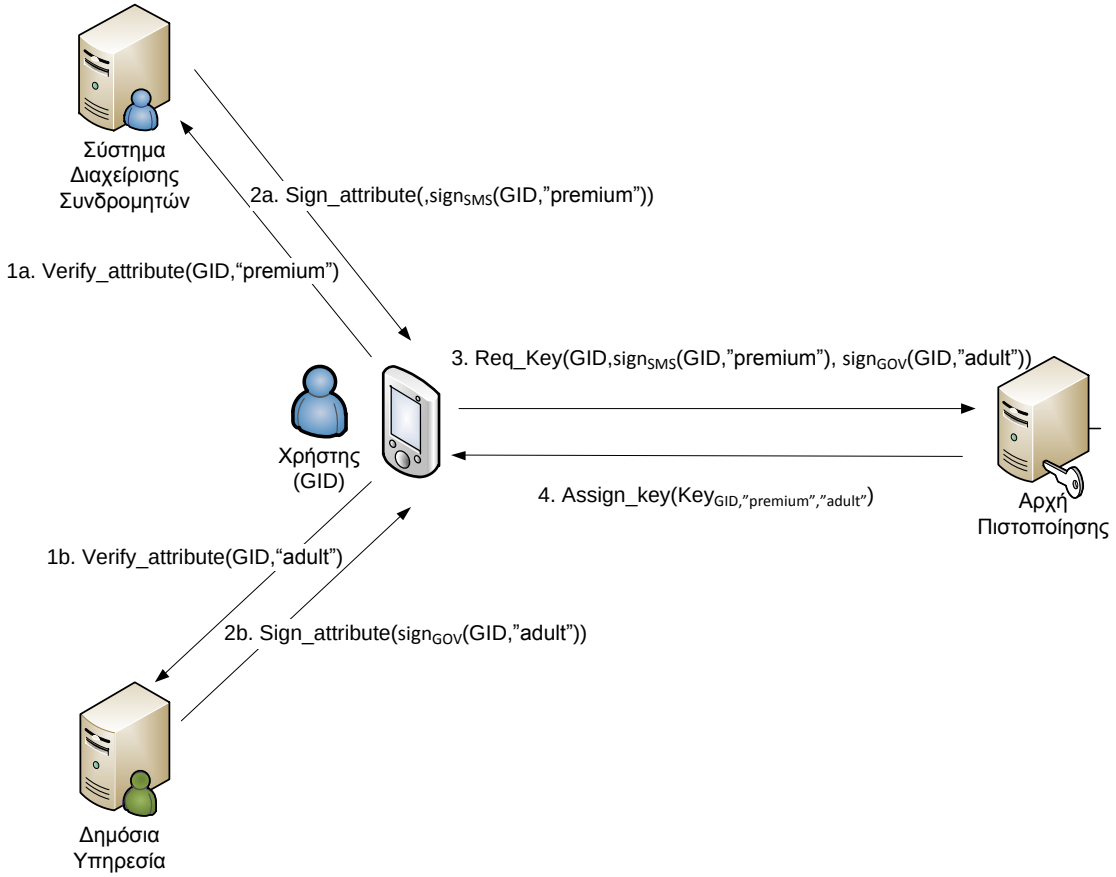


Σχήμα 10 Διαδικασία απόκτησης άδειας χρήσης πολυμεσικού περιεχομένου

Αυτή η φάση είναι παρόμοια με τα σημερινά συστήματα, με τη διαφορά ότι εφαρμόζεται κρυπτογράφηση ABE αντί για PKI, ενώ η υπόλοιπη διαδικασία αδειοδότησης παραμένει η ίδια, ελαχιστοποιώντας με αυτό τον τρόπο τις απαιτούμενες αλλαγές από τις τρέχουσες προσπάθειες τυποποίησης. Η ταυτότητα του χρήστη ελέγχεται μέσω του διακομιστή αδειών χρήσης, ενώ παράλληλα ελέγχεται η συσκευή ως προς την ασφάλειά της, και αν και τα δύο σκέλη του ελέγχου πετύχουν, ο χρήστης αποκτά την άδεια. Το ιδιωτικό κλειδί (ABE) χρησιμοποιείται για να αποκρυπτογραφήσει την άδεια και εν συνεχεία το κλειδί αποκρυπτογράφησης (AES), το οποίο εξάγεται από την άδεια, για να αποκρυπτογραφήσει το σχετικό περιεχόμενο.

Η λεπτομερής διαδικασία απόκτησης άδειας περιλαμβάνει τρία στάδια: Απόκτηση χαρακτηριστικού, κατόπιν κλειδιού και, τέλος, της ίδιας της άδειας. Στο Σχήμα 11 απεικονίζονται τα δύο πρώτα. Το πρώτο βήμα αφορά την απόκτηση χαρακτηριστικού. Είτε ο χρήστης μπορεί να αγοράσει ένα χαρακτηριστικό, όπως στην περίπτωσή μας με την αγορά του «Προνομιακού Πακέτου» και αντίστοιχα του «Προνομιακού» χαρακτηριστικού, είτε, εάν το χαρακτηριστικό είναι εγγενές (π.χ.

ημερομηνία γέννησης), ο χρήστης πρέπει είναι σε θέση να το αποδείξει, προκειμένου να λάβει το χαρακτηριστικό «Ενήλικας» από ένα δημόσιο οργανισμό. Τα χαρακτηριστικά υπογράφονται ψηφιακά από κάθε εκδότη. Μετά την απόκτηση των χαρακτηριστικών του, ο χρήστης μπορεί να απευθυνθεί σε μια Αρχή Πιστοποίησης Χαρακτηριστικών (ΑΠΧ) για να λάβει το αντίστοιχο κλειδί. Ο χρήστης παρέχει τα υπογεγραμμένα χαρακτηριστικά του στην ΑΠΧ, η οποία επαληθεύει τις υπογραφές και, εάν η επαλήθευση είναι επιτυχής, ο χρήστης θα λάβει το κλειδί που σχετίζεται με τα χαρακτηριστικά του.



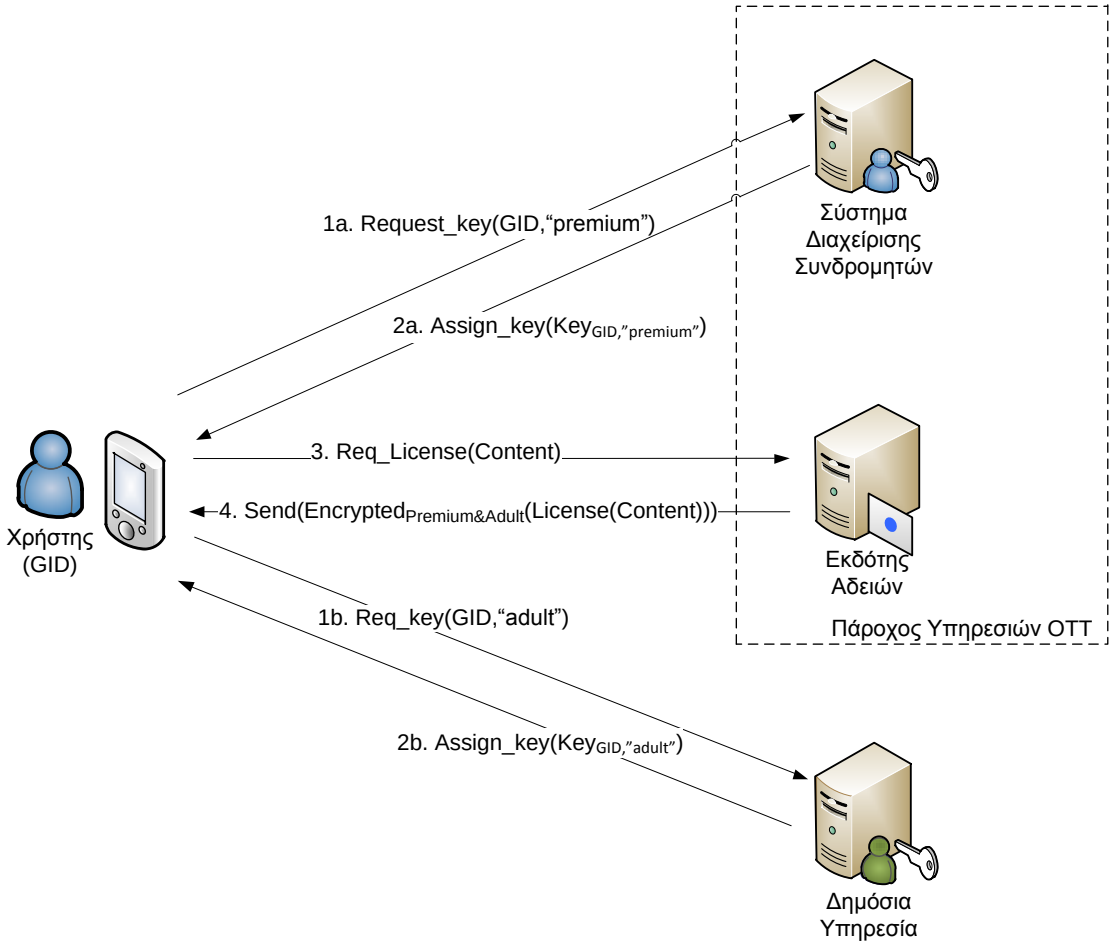
Σχήμα 11 Απόκτηση κλειδιού (συγκεντρωτικό σχήμα)

Το τελικό στάδιο περιλαμβάνει την απόκτηση της άδειας καθεαυτής. Ο διακομιστής αδειών χρήσης κρυπτογραφεί την άδεια σύμφωνα με τα προβλεπόμενα χαρακτηριστικά των χρηστών. Εάν το περιεχόμενο πρέπει να είναι προσιτό σε «Προνομιακούς» και «Ενήλικες» χρήστες, η άδεια περιεχομένου κρυπτογραφείται με χρήση πολιτικής «Προνομιακός ΚΑΙ Ενήλικας». Οι χρήστες χωρίς τα κατάλληλα κλειδιά δεν μπορούν να αποκρυπτογραφήσουν την άδεια και, κατά συνέπεια, δεν μπορούν να έχουν πρόσβαση στο πολυμεσικό περιεχόμενο. Σε εναλλακτικά, πιο σύνθετα, σενάρια ο

πάροχος υπηρεσιών OTT θα μπορεί να λαμβάνει υπόψη και άλλα χαρακτηριστικά των χρηστών, όπως για παράδειγμα τον τόπο κατοικίας και τις προτιμήσεις τους, ώστε να παρέχει εξατομικευμένο περιεχόμενο.

Ένα μειονέκτημα αυτής της προσέγγισης είναι ότι η μοναδική αρχή έκδοσης κλειδιών βάσει χαρακτηριστικών θα πρέπει να είναι σε θέση να επαληθεύσει τις υπογραφές όλων των άλλων αρχών. Επίσης, σε μεγάλα συστήματα ένα σφάλμα σε μια μοναδική τέτοια αρχή προκαλεί δυσλειτουργία του συστήματος συνολικά, ενώ έχει αρνητικό αντίκτυπο και στην επίδοση. Έτσι, ένα ρεαλιστικό σύστημα θα πρέπει να περιλαμβάνει αρκετές αρχές έκδοσης κλειδιών. Αντί της υπογραφής των χαρακτηριστικών και της ανάθεσης της δημιουργίας των κλειδιών σε μια ενιαία ΑΠΧ, κάθε αρχή (σύστημα διαχείρισης συνδρομητών, δημόσια υπηρεσία) μπορεί να λειτουργήσει ως αρχή έκδοσης κλειδιών. Τέτοια αποκεντρωμένα συστήματα μπορούν να εφαρμοστούν με τη χρήση πολλαπλών αρχών. Αποτελεσματικές τεχνικές, με χρήση Κρυπτογραφίας ABE και κοινών υπογραφών, επιτρέπουν την ασφαλή αυτόνομη δημιουργία του κλειδιού [105]. Ένας χρήστης αλληλεπιδρά με κάθε ΑΠΧ και αποκτά ένα κλειδί. Οι αρχές αυτές δεν επικοινωνούν μεταξύ τους. Η μεταξύ τους επικοινωνία εκτός από πρακτικές δυσκολίες ενέχει και κινδύνους για την ιδιωτικότητα των χρηστών (π.χ. συγκέντρωση στοιχείων για τα χαρακτηριστικά των χρηστών). Τα αποκτηθέντα κλειδιά δένονται σε ένα ενιαίο με τη χρήση ενός παγκόσμιου αναγνωριστικού χρήστη (Global User ID – GID), που αποτρέπει τους χρήστες από το να συνωμοτήσουν συνδυάζοντας επιμέρους κλειδιά τους. Στο Σχήμα 12 απεικονίζεται η διαδικασία απόκτησης άδειας χρήσης με χρήση πολλαπλών αρχών (ΑΠΧ).

Τα κλειδιά που έχουν εκδοθεί μπορούν να αποκρυπτογραφήσουν οποιαδήποτε άδεια, εφ' όσον αυτή είναι κρυπτογραφημένη υπό μια πολιτική πρόσβασης, η οποία ικανοποιείται από τα χαρακτηριστικά των χρηστών. Ο εξυπηρετητής έκδοσης αδειών δε χρειάζεται πλέον να διατηρεί τα δημόσια κλειδιά του κάθε συνδρομητή (όπως στην περίπτωση του PKI). Το σύστημα δίνει τη δυνατότητα κρυπτογράφησης, χωρίς να απαιτείται εκ των προτέρων γνώση των συγκεκριμένων χρηστών που θα έχουν πρόσβαση στο κρυπτογραφημένο περιεχόμενο, παρά μόνο των χαρακτηριστικών που θα πρέπει να πληρούν οι τελευταίοι. Έτσι, οι άδειες μπορούν να κρυπτογραφούνται για ομάδες χρηστών που μοιράζονται τις ίδιες ιδιότητες και όχι για κάθε μεμονωμένο χρήστη, αποφορτίζοντας τον εξυπηρετητή έκδοσης αδειών.



Σχήμα 12 Απόκτηση αδείας με χρήση αποκεντρωμένων ΑΠΧ

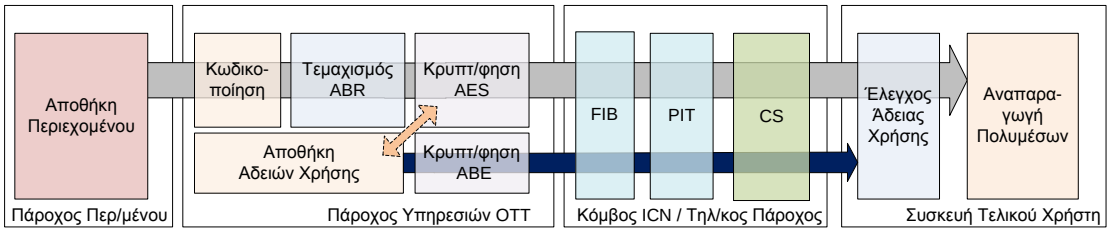
Η λεπτομέρεια του ελέγχου πρόσβασης που παρέχει το σύστημα, εξαρτάται αποκλειστικά από την επιλεχθείσα λεπτομέρεια των χαρακτηριστικών. Συνολικά, η αρχιτεκτονική μας έχει θετική επίδραση τόσο στην απαιτούμενη διαχειριστική προσπάθεια, όσο και στην χρήση των υπολογιστικών πόρων του παρόχου, δηλαδή λιγότερη επεξεργαστική ισχύς και αποθηκευτικός χώρος.

5.2 Διανομή αδειών και περιεχομένου

Τα συμμετρικά κλειδιά που περιλαμβάνονται στις δημιουργηθείσες άδειες χρησιμοποιούνται για την κρυπτογράφηση του πολυμεσικού περιεχομένου. Το κρυπτογραφημένο περιεχόμενο αποθηκεύεται αρχικά στους εξυπηρετητές του παρόχου, έτοιμο προς διανομή. Οι άδειες χρήσης αντιμετωπίζονται κι αυτές σαν δεδομένα που ακολουθούν τον ίδιο τρόπο ονομασίας και διανομής, όπως και το υπόλοιπο περιεχόμενο. Η προτεινόμενη αρχιτεκτονική ακολουθεί τις αρχές των Δικτύων ICN, προκειμένου να παράσχει επεκτάσιμη/κλιμακούμενη και οικονομικά αποδοτική διανομή πολυμεσικού

περιεχομένου. Η διαδικτυακή αρχιτεκτονική βασίζεται στην υλοποίηση ανοικτού κώδικα του CCN, η οποία διατίθεται στο [49].

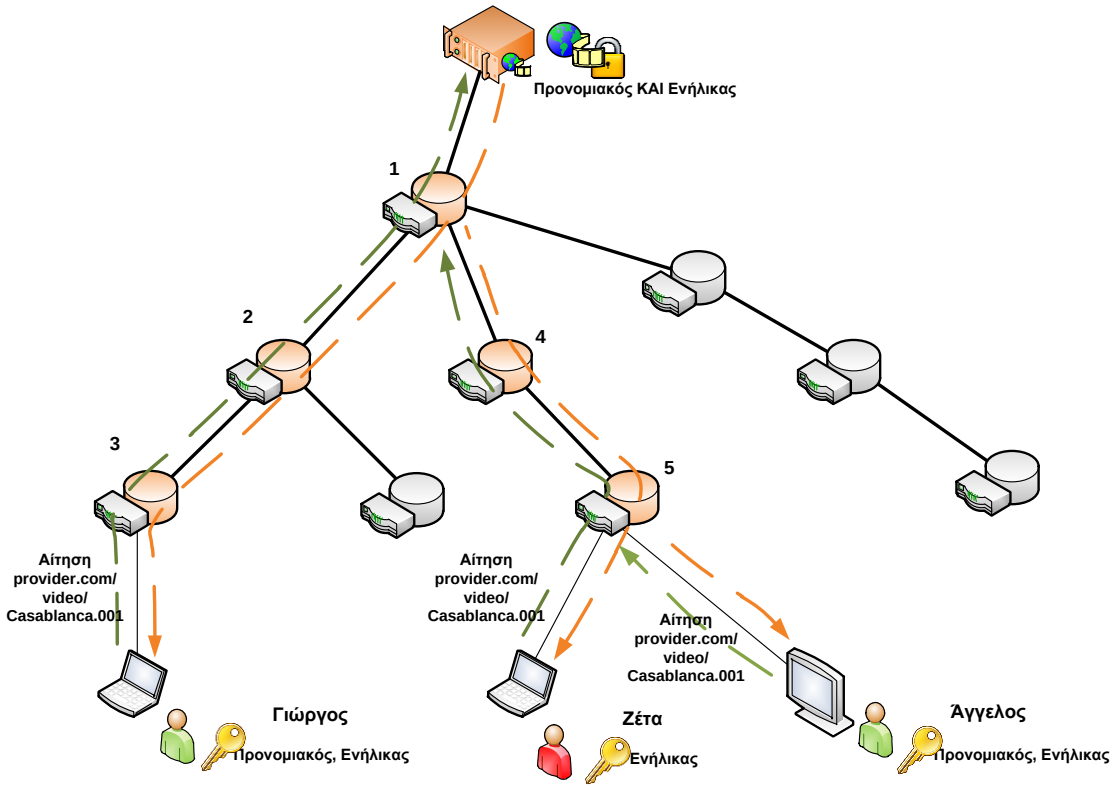
Το Σχήμα 13 παρουσιάζει τη διαδρομή του πολυμεσικού περιεχομένου καθώς αυτό διασχίζει τους εμπλεκόμενους της αρχιτεκτονικής μας. Ο Πάροχος Υπηρεσιών OTT κωδικοποιεί το ανεπεξέργαστο περιεχόμενο, το τεμαχίζει —χρησιμοποιώντας διαφορετικά προφίλ bitrate-αναλύσεων— σε κομμάτια και τελικά κρυπτογραφεί τα κομμάτια με χρήση συμμετρικού κλειδιού AES. Τα κρυπτογραφημένα τεμάχια περιεχομένου μεταφέρονται μέσω των κόμβων ICN προς τους αιτούντες χρήστες. Παράλληλα, μετά την απόκτηση άδειας σύμφωνα με το σχήμα που περιγράφεται στην προηγούμενη Ενότητα, η σχετική άδεια διαδίδεται μέσω των κόμβων ICN προς τους αιτούντες χρήστες. Η τερματική συσκευή του χρήστη λαμβάνει τα τμήματα και την άδεια, αποκρυπτογραφεί κάθε τμήμα του περιεχομένου στη βιβλιοθήκη DRM του πελάτη χρησιμοποιώντας το κλειδί που αποκτήθηκε από την άδεια, και, τέλος, τα αποκωδικοποιεί σε μορφή κατάλληλη για αναπαραγωγή.



Σχήμα 13 Πορεία του πολυμεσικού περιεχομένου από την παραγωγή στην κατανάλωση

Στην υλοποίηση CCNx, το σχήμα ονομασίας είναι ιεραρχικό και τα ονόματα είναι φιλικά προς τον άνθρωπο, π.χ., το όνομα `/Netflix/license/Casablanca.dcf` αντιστοιχεί σε ένα αρχείο άδειας χρήσης που παράγεται από τον πάροχο Netflix για την ταινία "Casablanca". Η λειτουργικότητα της δρομολόγησης-βάσει-ονόματος υποδηλώνει ότι τα αιτήματα των χρηστών δρομολογούνται με βάση το όνομα του επιθυμητού περιεχομένου, αντί της τοποθεσίας του στο δίκτυο. Όταν μια αίτηση φθάνει σε ένα κόμβο ICN, καταρχήν ελέγχεται ο αποθηκευτικός χώρος για τα ζητούμενα στοιχεία και, αν αυτά βρεθούν τοπικά, πραγματοποιείται η λήψη των δεδομένων από το συγκεκριμένο κόμβο. Σε διαφορετική περίπτωση η αίτηση προωθείται στον επόμενο κόμβο με κατεύθυνση την πηγή του περιεχομένου.

Το Σχήμα 14 απεικονίζει την προτεινόμενη αρχιτεκτονική του δικτύου, στην περίπτωση τριών χρηστών που ζητούν τα ίδια στοιχεία (άδεια ή τμήμα περιεχομένου). Αρχικά ο Γιώργος ζητά το στοιχείο βάσει του ονόματός του, και δεδομένου ότι δεν είναι ήδη προσωρινά αποθηκευμένο, το αίτημα του φτάνει στον πάροχο του περιεχομένου. Το περιεχόμενο αποθηκεύεται στους ενδιάμεσους κόμβους ICN (1, 2 και 3) από τους οποίους διέρχεται κατά την πορεία του. Στη συνέχεια, όταν η Ζέτα ζητά το ίδιο στοιχείο, το αίτημά της δρομολογείται προς τον πάροχο, έως ότου βρει τα δεδομένα αποθηκευμένα στον κόμβο 1. Τα τελευταία κατά τη λήψη τους αποθηκεύονται στους κόμβους 4 και 5. Τέλος, ο Άγγελος μπορεί να λάβει τα δεδομένα άμεσα από τον κόμβο (5).

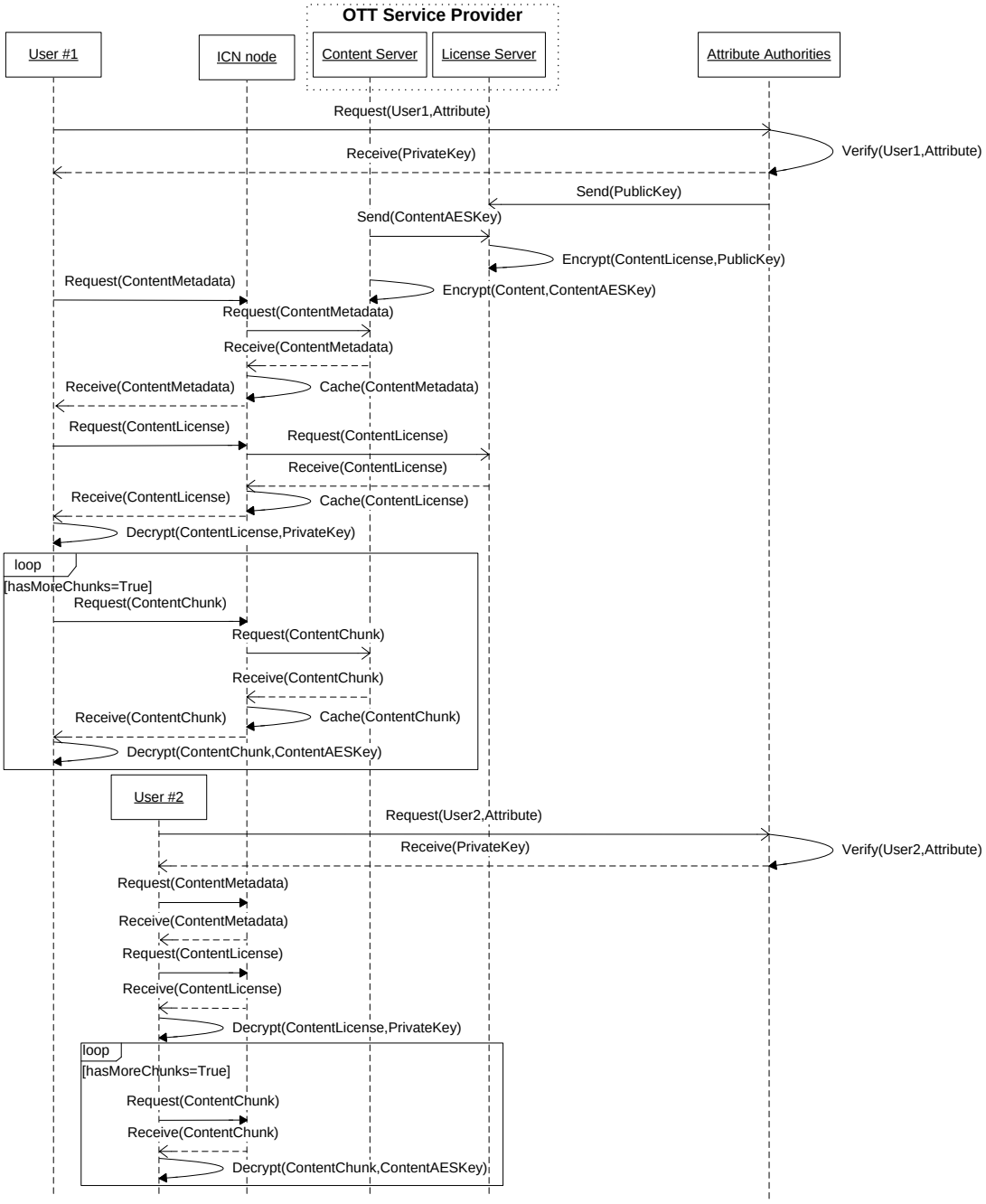


Σχήμα 14 Διαδικτυακή Αρχιτεκτονική

Εάν οι άδειες χρήσης έχουν κρυπτογραφηθεί ανά χρήστη, ο μηχανισμός αποθήκευσης περιεχομένου δε θα παρέχει καμία σημαντική βελτίωση, δεδομένου ότι κάθε χρήστης θα πρέπει να φτάσει το διακομιστή αδειών χρήσης για να αποκτήσει πρόσβαση στην άδειά του. Οι κρυπτογραφημένες με ABE άδειες επιτρέπουν σε κάθε χρήστη, που ικανοποιεί την πολιτική πρόσβασης, να αποκτήσει πρόσβαση στις κρυπτογραφημένες άδειες από τα αποθετήρια του δικτύου —δηλαδή χωρίς να

αλληλεπιδράσει με τον πάροχο του περιεχομένου. Έτσι, τα πλεονεκτήματα των Δικτύων ICN διατηρούνται, ενώ παράλληλα το περιεχόμενο είναι προστατευμένο.

Σημειώνεται ότι ο Γιώργος και ο Άγγελος ικανοποιούν την πολιτική πρόσβασης («Προνομιακός και Ενήλικας»), αποκτώντας πρόσβαση στην αποκρυπτογράφηση του περιεχομένου, ενώ στη Ζέτα δε χορηγείται πρόσβαση. Οι συνολικές αλληλεπιδράσεις μεταξύ των συμμετεχόντων στην αρχιτεκτονική σκιαγραφούνται στο διάγραμμα ακολουθίας του Σχήμα 15.



Σχήμα 15 Συνολικό διάγραμμα ακολουθίας

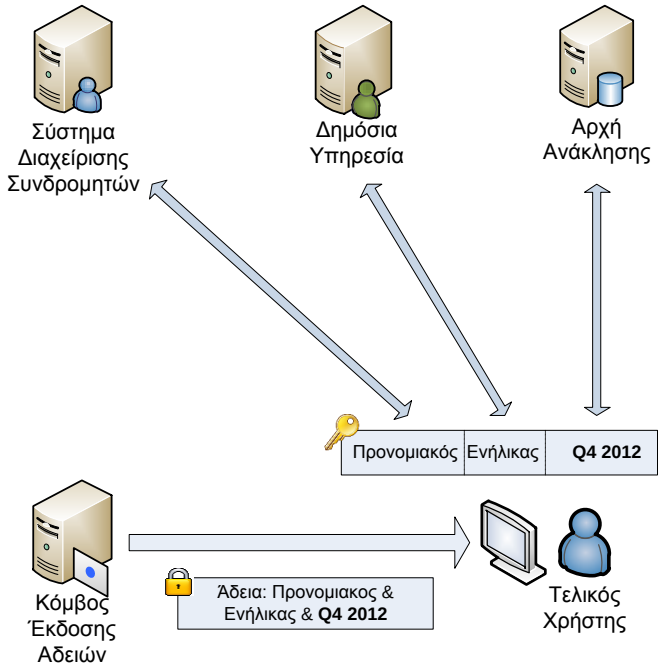
5.3 Ανάκληση χρήστη

Η ανάκληση ενός χρήστη είναι ένα άλλο ζήτημα που απαιτεί τη δέουσα προσοχή, ώστε να ανταποκριθεί στις πρακτικές απαιτήσεις της συνδρομητικής τηλεόρασης. Η ανάκληση είναι ένα δύσκολο θέμα, ακόμη και στα παραδοσιακά συστήματα PKI. Στην περίπτωση των κρυπτοσυστημάτων που βασίζονται σε Κρυπτογραφία ABE, η διαδικασία ανάκλησης είναι ακόμα πιο περίπλοκη, λόγω της έλλειψης εξατομικευμένων κλειδιών. Τα χαρακτηριστικά, βάσει των οποίων πραγματοποιείται η έκδοση των κλειδιών και εν συνεχεία η κρυπτογράφηση, είναι εν γένει κοινά για μια ομάδα χρηστών. Στις περισσότερες προσεγγίσεις με χρήση Κρυπτογραφίας ABE, η ανάκληση εστιάζεται στο επίπεδο των χαρακτηριστικών, αλλά στα σενάρια συνδρομητικής τηλεόρασης, παρόλο που η ανάκληση χαρακτηριστικών καθεαυτή θα μπορούσε να είναι χρήσιμη, η επικρατούσα πρακτική είναι η άμεση ανάκληση ενός χρήστη ή ενός πλήθους χρηστών. Υπό το πρίσμα αυτό, η Κρυπτογραφία ABE δυσχεραίνει την ανάκληση ενός μόνο χρήστη, λαμβάνοντας υπόψη ότι οι άλλοι χρήστες οι οποίοι μοιράζονται τις ίδιες ιδιότητες-χαρακτηριστικά με τον υπό ανάκληση χρήστη πρέπει να παραμείνουν ανεπηρέαστοι. Λόγω αυτού του περιορισμού, δεν είναι επιθυμητή η ανάκληση όλων των ιδιοτήτων που κατέχει ένας χρήστης.

Η συνέργεια με τα Δίκτυα ICN δημιουργεί πρόσθετες προκλήσεις, καθώς τα δεδομένα (συμπεριλαμβανομένων των αδειών) μπορούν να προσεγγιστούν απευθείας από τους ενδιάμεσους αποθηκευτικούς χώρους χωρίς περιορισμό. Ως εκ τούτου, οι μηχανισμοί ανάκλησης περιεχόμενου θα πρέπει να υλοποιηθούν είτε με την επιβολή ανάκλησης του περιεχομένου στους κόμβους Δικτύων ICN ή ορίζοντας ένα μέγιστο χρόνο αποθήκευσης του περιεχόμενου στους κόμβους αυτούς, με την πάροδο του οποίου θα διαγράφεται. Σε σενάρια συνδρομητικής τηλεόρασης ο πάροχος υπηρεσιών OTT θεωρείται ότι έχει λάβει γνώση της λίστας ανάκλησης. Κατά συνέπεια, κατ' αντιστοιχία με τις εργασίες [93], [96], το επόμενο βήμα είναι η ανακρυπτογράφηση του περιεχομένου υπό μια ενημερωμένη πολιτική πρόσβασης που θα αποκλείει τους ανακληθέντες χρήστες από την πρόσβαση στο περιεχόμενο. Ωστόσο, ένα μειονέκτημα αυτής της μεθόδου είναι ότι το μέγεθος του κρυπτογραφημένου περιεχομένου αυξάνεται γραμμικά με τον αριθμό των ανακληθέντων χρηστών [93], επιβαρύνοντας τη δικτυακή κίνηση. Επιπλέον η ανακρυπτογράφηση του περιεχομένου αναιρεί την αποδοτική χρήση των δικτυακών αποθηκευτικών χώρων των Δικτύων ICN. Το κρυπτογραφημένο, υπό τη

νεότερη πολιτική πρόσβασης, περιεχόμενο θα πρέπει να διαδοθεί σε ένα μεγάλο μέρος του δικτύου, προτού η προσωρινή αποθήκευση γίνει και πάλι αποτελεσματική.

Άλλες λύσεις προτείνουν τεχνικές ανακρυπτογράφησης με χρήση διακομιστών διαμεσολάβησης [100],[101], προκειμένου μέσω της ανακρυπτογράφησης του περιεχομένου να εξαιρεθούν οι ανακληθέντες χρήστες. Αυτό πραγματοποιείται με τη χρήση των ημι-αξιόπιστων κόμβων διαμεσολάβησης, αλλά η εκ νέου κρυπτογράφηση του περιεχομένου εμποδίζει και πάλι τη δυνατότητα αποθήκευσης στους κόμβους Δικτύων ICN, ενώ ταυτόχρονα εισάγονται και θέματα εμπιστοσύνης και εγκατάστασης επιπλέον εξυπηρετητών.



Σχήμα 16 Σχέδιο ανάκλησης χρηστών

Στην προτεινόμενη λύση, η ανάκληση των χρηστών γίνεται αναγκάζοντας το χρήστη να ανανεώσει τα κλειδιά του. Αυτό μπορεί να γίνει είτε με την προσάρτηση μιας ημερομηνία λήξης για κάθε χαρακτηριστικό, όπως στην εργασία των Bethencourt et al [84], είτε με τη χρήση μιας Αρχής Ανάκλησης η οποία εκδίδει «ενημερώσεις κλειδιού», στις οποίες οι μη ανακληθέντες χρήστες μπορούν περιοδικά να έχουν πρόσβαση [94]. Η δεύτερη επιλογή, η οποία προτιμήθηκε, δεδομένου ότι δεν απαιτεί περιττές ενημερώσεις για κάθε χαρακτηριστικό, αν και εισάγει μία επιπλέον Αρχή Πιστοποίησης, απεικονίζεται στο Σχήμα 16. Η Αρχή Ανάκλησης εκδίδει ένα κλειδί, που αντιστοιχεί σε ένα χαρακτηριστικό π.χ. «μη ανακληθείς 4ο τρίμηνο 2012», για όλους τους χρήστες, που

δεν έχουν ανακληθεί κατά τη διάρκεια της συγκεκριμένης χρονικής περιόδου. Ο εξυπηρετητής έκδοσης αδειών κρυπτογραφεί τις άδειες, λαμβάνοντας υπόψη το επιπλέον χαρακτηριστικό. Συνεπώς, μόνο ένας μη ανακληθείς χρήστης θα μπορεί να αποκρυπτογραφήσει την άδεια, η οποία έχει κρυπτογραφηθεί με τη νεότερη πολιτική πρόσβασης. Ένα προτέρημα της συγκριμένης προσέγγισης είναι η ευελιξία στον ορισμό του χρονικού διαστήματος. Υφίσταται όμως ένας συμβιβασμός μεταξύ της πραγματικής διάρκειας δικτυακής αποθήκευσης και του χρονικού παραθύρου από τη στιγμή που ανακαλείται ένας χρήστης μέχρι τη στιγμή που παύει να έχει πρόσβαση στο περιεχόμενο.

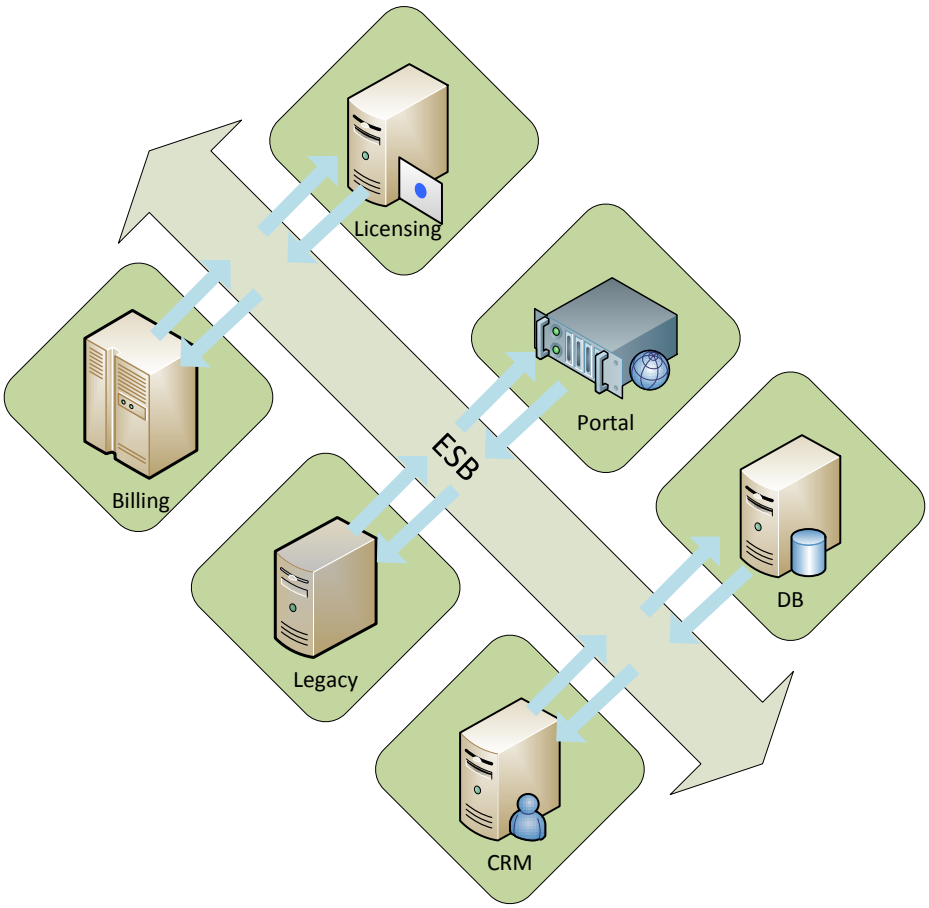
Επιπλέον, σε κάθε επικοινωνία με τις ΑΠΧ, η συσκευή του χρήστη ελέγχεται για κακόβουλο λογισμικό και ως προς τη συμμόρφωση εμπιστοσύνης, πριν μεταφερθούν σε αυτή τα κλειδιά. Υιοθετήθηκε αυτή η απλή λύση, καθώς δεν εμποδίζει τη χρήση ενδοδικτυακής κρυφής μνήμης ούτε προσθέτει μεγάλη πολυπλοκότητα στο προτεινόμενο σύστημα, με το κόστος όμως των περιοδικών ενημερώσεων των κλειδιών, οι οποίες μπορούν να μετριαστούν σε μια αποκεντρωμένη αρχιτεκτονική πολλαπλών αρχών.

6 Υπηρεσιοστραφής Παροχή Περιεχομένου

Το παρόν Κεφάλαιο εμβαθύνει στην υλοποίηση της προτεινόμενης λύσης και παρουσιάζει λεπτομερώς τις κυριότερες πτυχές της, με έμφαση στην αρχιτεκτονική του παρόχου υπηρεσιών OTT και τις διεπαφές του με τρίτα συστήματα (εξωτερικές Αρχές Πιστοποίησης Χαρακτηριστικών, συσκευές συνδρομητών και λοιπά τρίτα συστήματα).

Η λύση έχει δομηθεί βάσει του μοντέλου της Αρχιτεκτονικής Προσανατολισμένης στις Υπηρεσίες (Service Oriented Architecture – SOA). Σύμφωνα με την W3C [116] η SOA είναι ένα σύνολο στοιχείων λογισμικού, οι περιγραφές των διεπαφών των οποίων μπορούν να δημοσιευθούν και να ανακαλυφθούν, ώστε να καταστεί δυνατή η κλήση του λογισμικού από άλλα συστήματα. Ο συγκεκριμένος ορισμός είναι ελαφρώς περιοριστικός, καθώς αναφέρεται στα υλοποιημένα στοιχεία λογισμικού μιας αρχιτεκτονικής. Γενικότερα ως SOA —και υπό αυτή την έννοια θα χρησιμοποιείται εφεξής— έχει επικρατήσει να χαρακτηρίζονται όλες οι πολιτικές, οι πρακτικές και τα περιβάλλοντα ανάπτυξης και εκτέλεσης λογισμικού, τα οποία επιτρέπουν την παροχή και την κατανάλωση των λειτουργικοτήτων μιας εφαρμογής υπό τη μορφή υπηρεσιών [117],[118].

Η αρχιτεκτονική SOA αφορά κατανεμημένα συστήματα και στηρίζεται αφενός στη χρήση Υπηρεσιών Ιστού (Web Services) [119] και αφετέρου —συνήθως, αλλά όχι απαραιτήτως— στη χρήση μεσισμικού, το οποίο καλείται Επιχειρησιακός Δίαυλος Υπηρεσιών (Enterprise Service Bus – ESB). Η διάρθρωση ενός ESB παρουσιάζεται στο Σχήμα 17. Ο δίαυλος είναι υπεύθυνος για τη δρομολόγηση των μηνυμάτων που ανταλλάσσονται μεταξύ των υπηρεσιών, την ασφάλεια και την καταγραφή, καθώς και την παροχή στοιχειωδών υπηρεσιών, όπως η μετατροπή δεδομένων από τη μορφή που τα εξάγει μια υπηρεσία σε άλλη μορφή, κατάλληλη προς κατανάλωση από μια δεύτερη υπηρεσία.



Σχήμα 17 Επιχειρησιακός Δίαυλος Υπηρεσιών

Οι πλατφόρμες που στηρίζονται σε SOA γνωρίζουν μεγάλη αποδοχή την τελευταία δεκαετία και αποτελούν την υποδομή πάνω στην οποία στηρίζονται τα πληροφοριακά συστήματα μιας μεγάλης γκάμας εταιρειών (από παρόχους κινητής τηλεφωνίας και διαδικτύου μέχρι χρηματοπιστωτικούς οργανισμούς). Στην πράξη βέβαια, οι περισσότεροι οργανισμοί βρίσκονται σε μια διαρκή προσπάθεια συμμόρφωσης με τις αρχές της SOA κάτι το οποίο έχει αντίκτυπο τόσο στη σχεδίαση νέων λειτουργικοτήτων, όσο και στην επανασχεδίαση παλαιών.

Ενδεικτικά πλεονεκτήματα της SOA αποτελούν:

- η ευκολία ενσωμάτωσης επιχειρησιακών διαδικασιών μέσω γραφικών περιβαλλόντων σχεδίασης υπηρεσιών —τα περιβάλλοντα ανάπτυξης συμπεριλαμβάνουν στην υποδομή τους υλοποιήσεις των προδιαγραφών BPEL4WS [120] και BPMN [121], όπως η jBPM [122],

- η ύπαρξη ενσωματωμένων προσαρμοστών για ολοκλήρωση με δημοφιλή συστήματα διαχείρισης και χρέωσης συνδρομητών καθώς και βάσεις δεδομένων,
- η δυνατότητα επαναχρησιμοποίησης δομικών στοιχείων, το οποίο επιτρέπει την γρήγορη ανάπτυξη υπηρεσιών (fast time-to-market) και
- η παροχή στοιχειωδών υπηρεσιών, που επιτρέπει στους προγραμματιστές να επικεντρώσουν την προσπάθειά τους στην ανάπτυξη του πυρήνα της υπηρεσίας.

Τέλος η κατανεμημένη αρχιτεκτονική της SOA διευκολύνει την επικοινωνία με εξωτερικά συστήματα, κάτι που είναι ιδιαίτερα χρήσιμο, καθώς πολλές εταιρείες αποφασίζουν την ανάθεση των βοηθητικών λειτουργιών τους σε εξωτερικούς συνεργάτες.

Ιδιαίτερα σε εταιρείες όπως οι πάροχοι υπηρεσιών OTT, οι οποίες εξ ορισμού αποτελούν σημείο ολοκλήρωσης μεταξύ παρόχων περιεχομένου, λύσεων προστασίας περιεχομένου, συστημάτων για τη διαχείριση και τη χρέωση συνδρομητών και παρόχων υπηρεσιών CDN, η λύση της SOA παρουσιάζεται ως η πλέον κατάλληλη. Επιπλέον όπως είδαμε και στην Ενότητα 2.5, ο κλάδος των παρόχων υπηρεσιών OTT χαρακτηρίζεται από ένα διαρκώς μεταβαλλόμενο περιβάλλον, όπου μια πληθώρα τεχνολογικών λύσεων, συχνά μη διαλειτουργικών, προσπαθεί να ανταποκριθεί στις υψηλές απαιτήσεις των χρηστών. Είναι λοιπόν προς όφελος των παρόχων, η απεμπλοκή των επιχειρησιακών τους λειτουργιών από τις υποκείμενες τεχνολογίες, οι οποίες τείνουν να αντικαθίστανται σε σύντομο χρονικό διάστημα. Στην αρχιτεκτονική SOA, με τη χρήση διεπαφών που αποκρύπτουν την υλοποίηση, είναι δυνατή η αντικατάσταση των υποκείμενων τεχνολογιών, χωρίς να επηρεάζεται η λειτουργία των επιχειρησιακών ροών. Οι παραπάνω παρατηρήσεις τροφοδότησαν τη δημιουργία fora όπως το AMWA (Advanced Media Workflow Association), που μελετά την εφαρμογή της SOA σε εταιρίες που διαχειρίζονται ροές πολυμέσων [123]. Γι' αυτό το λόγο έχει δοθεί ιδιαίτερο βάρος στην εναρμόνιση της προτεινόμενης λύσης με τις αρχές της SOA.

Αξίζει να γίνει αναφορά και στον αντίλογο, ο οποίος εστιάζει σε δύο διαφορετικά θέματα. Πρώτον, υποστηρίζεται ότι η καθιέρωση και ευρεία αποδοχή προτύπων (όπως τα DASH, Marlin DRM, HEVC), θα δώσει τέλος στη διαρκή αλλαγή των τεχνολογιών. Ακόμα κι αν αυτό το σενάριο επαληθευτεί —κάτι καθόλου σίγουρο, καθώς οι τεχνολογίες συνεχώς εξελίσσονται— αυτό δεν αναιρεί τα πλεονεκτήματα της SOA. Μια δεύτερη

κριτική ματιά εστιάζει στην αδυναμία των SOA (και ιδιαίτερα του υποκείμενου ESB) να εξυπηρετήσουν αποδοτικώς μηνύματα ιδιαίτερα μεγάλου μεγέθους (όπως αρχεία πολυμέσων) εκ σχεδιασμού. Στην παρούσα λύση έχει ληφθεί υπόψη η συγκεκριμένη ανεπάρκεια και οι λειτουργίες που αφορούν διαχείριση μεγάλων αρχείων πολυμέσων, παρέχονται στο σύστημα σαν υπηρεσίες (που υλοποιούνται με χρήση υφιστάμενων ειδικά σχεδιασμένων εφαρμογών).

Όπως προαναφέρθηκε, η SOA είναι ένα σύνολο αρχών και μια κουλτούρα, η οποία δε χτίζεται σε μία μέρα, ιδίως σε εταιρίες οι οποίες έχουν αντικείμενο τα media και οι οποίες απέχουν από τον κόσμο του IT. Παραδείγματος χάριν, η ροή εργασιών στο πλαίσιο της SOA αφορά μια επιχειρησιακή ροή που περικλείει μια συγκεκριμένη λειτουργία της επιχείρησης, ενώ σε μια εταιρία παραγωγής τηλεοπτικού υλικού η ροή μεταφράζεται στην πορεία ενός πολυμέσου από την παραγωγή εώς την διανομή (απο/κωδικοποίηση, επεξεργασία εικόνας/ήχου κλπ). Σε συνέχεια του παραδείγματος, στις επιχειρήσεις που παράγουν πολυμεσικό υλικό είναι συνήθης ένας υψηλός βαθμός αυτοματοποίησης (προκειμένου να ανταποκριθούν στις απαιτήσεις του πραγματικού κόσμου), αλλά αυτή η αυτοματοποίηση αφορά και πάλι τα στάδια επεξεργασίας του πολυμεσικού υλικού και όχι των επιχειρησιακών διαδικασιών. Η αρχιτεκτονική SOA δεν έχει σχεδιαστεί για να αντικαταστήσει μια τέτοια αυτοματοποίηση και επομένως στην πράξη θα συνυπάρχει με αυτή – δίνοντας όμως έμφαση στην έκθεση αυτής της αυτοματοποίησης υπό τη μορφή υπηρεσιών.

Με βάση τις αρχές της SOA και λαμβάνοντας υπόψη τους περιορισμούς που αναφέρθηκαν, δομήθηκε η προτεινόμενη αρχιτεκτονική ενός παρόχου OTT, η οποία στοχεύει στην ενσωμάτωση λύσεων προστασίας περιεχομένου βασισμένων σε Κρυπτογραφία ABE. Στις επόμενες ενότητες θα προχωρήσουμε στη λεπτομερή περιγραφή των υποσυστημάτων, που εμπλέκονται στην ολοκλήρωση της τυπικής υποδομής ενός παρόχου υπηρεσιών OTT με την υποδομή που απαιτείται για την Κρυπτογραφία ABE, καθώς και των μεταξύ τους διεπαφών.

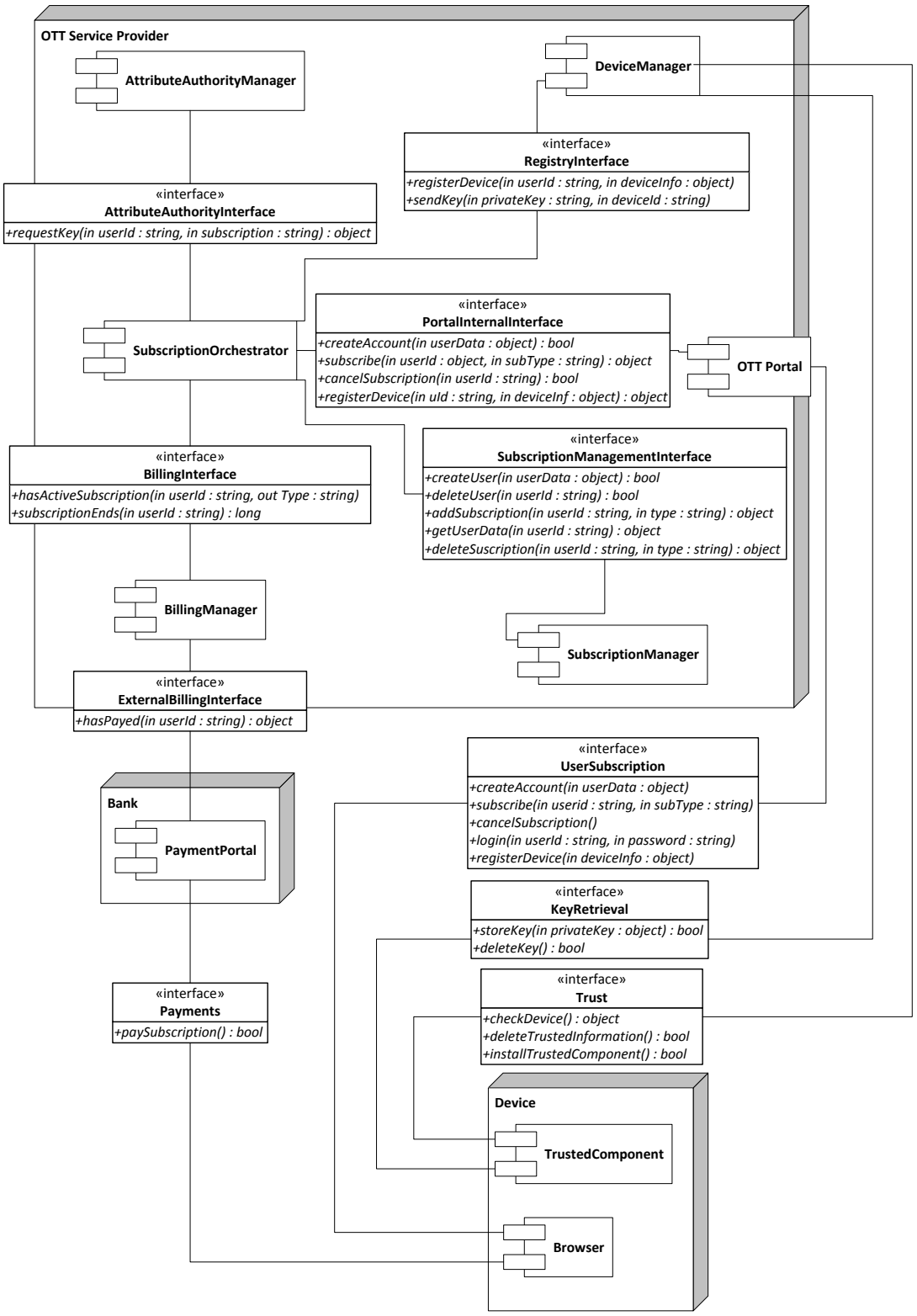
Πιο συγκεκριμένα θα παρουσιαστούν τα υποσυστήματα που εμπλέκονται στην πιστοποίηση του χρήστη και την έκδοση κλειδιού βάσει χαρακτηριστικών και τα υποσυστήματα που εμπλέκονται στη διαδικασία κρυπτογράφησης των αδειών με χρήση μιας πολιτικής πρόσβασης βάσει χαρακτηριστικών.

6.1 Διαδικασία πιστοποίησης και απόδοσης κλειδιού

Στο Σχήμα 18 παρουσιάζονται τα δομικά στοιχεία του παρόχου υπηρεσιών OTT, τα οποία συμμετέχουν στη διαδικασία εγγραφής ενός χρήστη και της απόδοσης σε αυτόν ενός κλειδιού ABE, το οποίο αντιστοιχεί στη συνδρομή του (ή γενικότερα στα πιστοποιημένα χαρακτηριστικά του). Τα δομικά αυτά στοιχεία αντιστοιχούν σε υποσυστήματα του παρόχου υπηρεσιών OTT και καθιστούν διαθέσιμες τις λειτουργίες αυτών υπό τη μορφή υπηρεσιών. Ταυτόχρονα απεικονίζονται και οι διεπαφές μεταξύ των δομικών στοιχείων με τις αντίστοιχες λειτουργίες τους. Η επικοινωνία με τα εξωτερικά συστήματα πραγματοποιείται με χρήση Υπηρεσιών Ιστού Simple Object Access Protocol (SOAP) [124], ενώ εσωτερικά στον πάροχο έχει ακολουθηθεί η αρχιτεκτονική SOA/ESB.

Συγκεκριμένα στον πάροχο OTT, τα κυριότερα στοιχεία είναι τα ακόλουθα:

- Ο Ενορχηστρωτής της Συνδρομητικής Υπηρεσίας (`SubscriptionOrchestrator`), ο οποίος ενθυλακώνει όλη την απαραίτητη λογική και συντονίζει τη λειτουργία του συστήματος. Σε μία αρχιτεκτονική SOA/ESB αυτή η διεργασία υλοποιείται με χρήση γλωσσών Business Process Execution Language (BPEL) και Business Process Model and Notation (BPMN).
- Το Υποσύστημα Χρέωσης (`BillingManager`), το οποίο είναι υπεύθυνο για τις χρεώσεις των υπηρεσιών και το οποίο παρέχει πληροφορίες σχετικά με το εάν ο χρήστης είναι ενήμερος ως προς τις υποχρεώσεις του.
- Το Υποσύστημα Διαχείρισης Συνδρομητών (`SubscriptionManager`), το οποίο διαχειρίζεται όλες τις πληροφορίες σχετικά με τους χρήστες και τις υπηρεσίες τους.
- Η Αρχή Πιστοποίησης Χαρακτηριστικών (`AttributeAuthorityManager`), η οποία εκδίδει κλειδιά για τους χρήστες ανάλογα με τα χαρακτηριστικά τους, στη συγκεκριμένη περίπτωση τον τύπο της συνδρομής.



Σχήμα 18 Δομικά στοιχεία του συστήματος εγγραφής χρήστη και έκδοσης κλειδιού

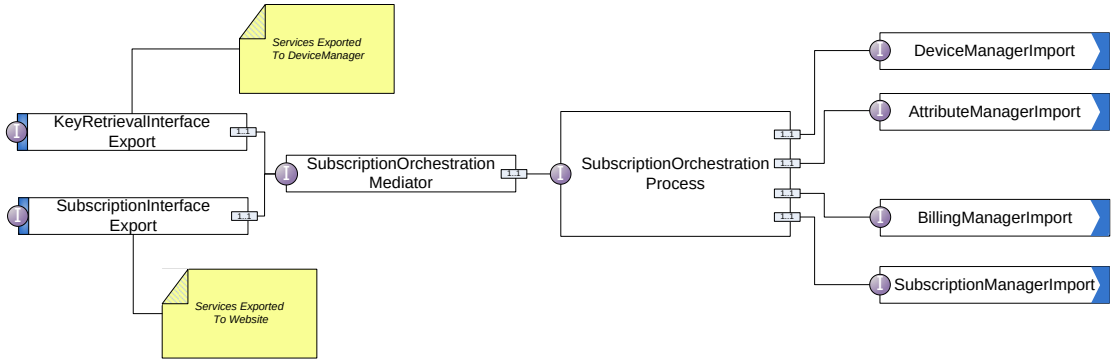
- Το Υποσύστημα Διαχείρισης Συσκευών (`DeviceManager`), το οποίο είναι υπεύθυνο για τον έλεγχο των συσκευών του συνδρομητή ως προς την ύπαρξη κακόβουλου λογισμικού και την πλήρωση λοιπών απαιτήσεων ασφαλείας.

- Το portal του παρόχου υπηρεσιών OTT, το οποίο αποτελεί το σημείο εισόδου για το χρήστη και το οποίο παρέχει με ενιαίο τρόπο πρόσβαση στις παρεχόμενες υπηρεσίες.

Για την ασφάλεια των πληρωμών γίνεται χρήση του portal πληρωμών μιας συνεργαζόμενης τράπεζας ή εναλλακτικού παρόχου ασφαλών πληρωμών (π.χ. PayPal[125]).

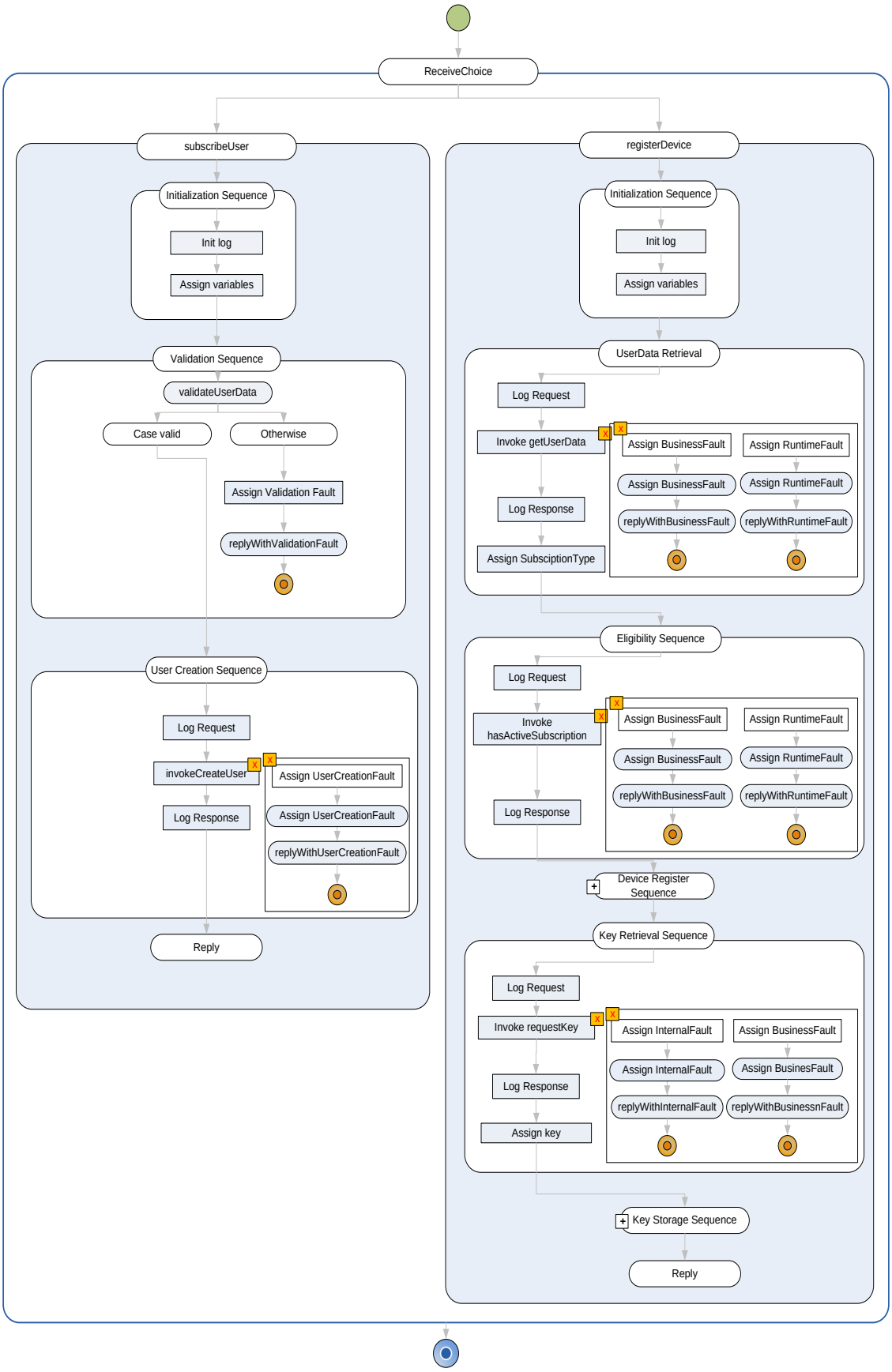
Στο Σχήμα 19 απεικονίζονται τα συστατικά του Ενορχηστρωτή Συνδρομητικής Υπηρεσίας. Στη δεξιά πλευρά του σχήματος βρίσκονται οι «εισαγωγείς» υπηρεσιών από άλλα υποσυστήματα, ενώ αντίστοιχα στην αριστερή πλευρά οι «εξαγωγείς» υπηρεσιών από το παρόν προς άλλα υποσυστήματα. Επιπλέον περιλαμβάνονται ένας διαμεσολαβητής, ο οποίος αφενός μετασχηματίζει τις εξαγόμενες υπηρεσίες σε μορφή κατάλληλη προς κατανάλωση και αφετέρου πραγματοποιεί δευτερεύουσες λειτουργίες όπως την καταγραφή (logging), και ο πυρήνας του ενορχηστρωτή.

Η δομή του πυρήνα του ενορχηστρωτή παρουσιάζεται αναλυτικά στο Σχήμα 20. Στο σχήμα αυτό αποτυπώνεται το διάγραμμα ροής δύο υπηρεσιών, οι οποίες δομούνται πάνω σε κλήσεις εισαχθεισών υπηρεσιών, ενώ δίνεται ιδιαίτερη έμφαση στη διαχείριση των σφαλμάτων και την καταγραφή της πορείας των υπηρεσιών, κάτι ιδιαίτερα σημαντικό σε πραγματικά συστήματα.

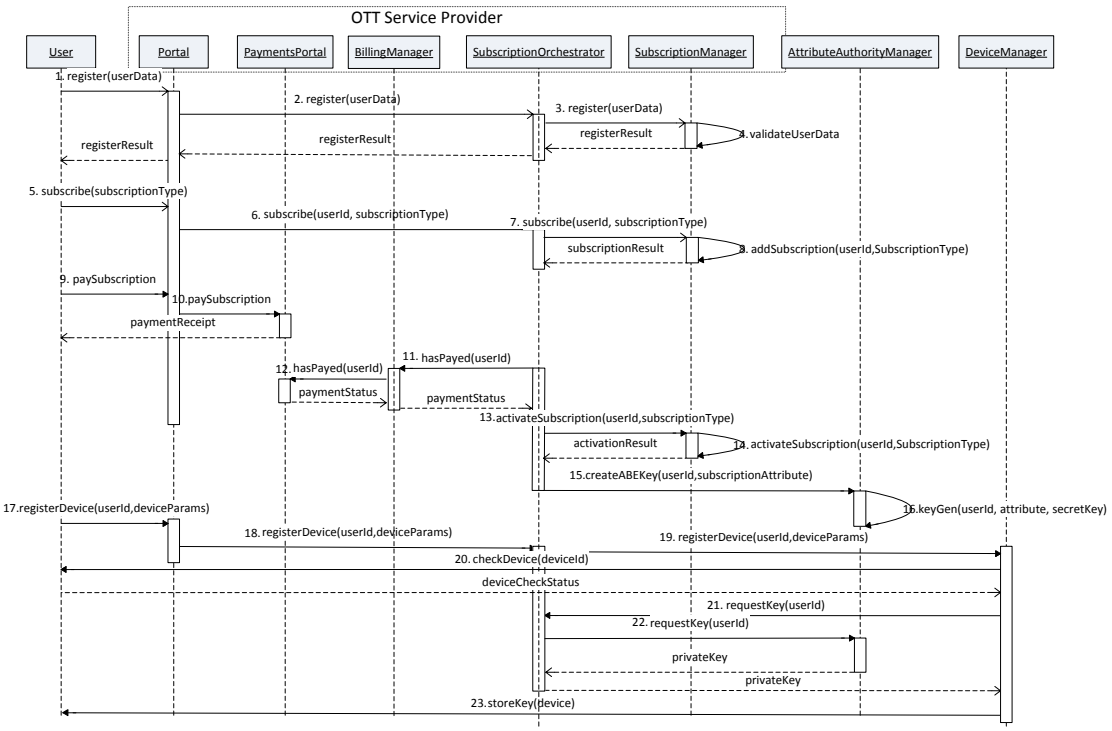


Σχήμα 19 Δομή του SubscriptionOrchestrator

Τέλος στο Σχήμα 21 παρουσιάζεται το συνολικό διάγραμμα ακολουθίας UML με τα εμπλεκόμενα υποσυστήματα, τα οποία συμμετέχουν στη διαδικασία εγγραφής ενός χρήστης και της ακόλουθης απόδοσης κλειδιού σε αυτόν.



Σχήμα 20 Εσωτερική λογική (Διάγραμμα BPEL) του SubscriptionOrchestrator



Σχήμα 21 Διάγραμμα ακολουθίας της εγγραφής χρήστη και απόδοσης κλειδιού

Τα υποσυστήματα επικοινωνούν μεταξύ τους μέσω των ορισμένων διεπαφών με τρόπο που συντονίζεται από τον Ενορχηστρωτή Συνδρομητικής Υπηρεσίας (ΕΣΥ), χωρίς απαραίτητα αυτό να σημαίνει ότι αποκλείεται η απευθείας επικοινωνία των υποσυστημάτων. Σε κάθε διεπαφή έχουν οριστεί οι αντίστοιχες λειτουργίες, π.χ. ο ΕΣΥ χρησιμοποιώντας τη λειτουργία `hasActiveSubscription(String userId)` λαμβάνει πληροφορίες για τη συνδρομή του χρήστη με χαρακτηριστικό userId.

Οι κλήσεις 1-4 αφορούν την εγγραφή του χρήστη, ενώ οι 5-14 τη διαδικασία συνδρομής και την πληρωμή αυτής. Στη συνέχεια οι κλήσεις 15-16 αφορούν τη δημιουργία κλειδιού Κρυπτογραφίας ABE, το οποίο αντιστοιχεί στο συγκεκριμένο χαρακτηριστικό (συνδρομή). Τέλος οι κλήσεις 17-20 πραγματοποιούν την εγγραφή και τον έλεγχο της τερματικής συσκευής του χρήστη, ενώ σε περίπτωση που η συσκευή κριθεί κατάλληλη, γίνεται η αποθήκευση του δημιουργηθέντος κλειδιού σε αυτή (κλήσεις 21-23).

6.2 Διαδικασία κρυπτογράφησης περιεχομένου βάσει χαρακτηριστικών

Στο Σχήμα 22 παρουσιάζονται τα δομικά στοιχεία του παρόχου υπηρεσιών OTT και των εξωτερικών ΑΠΧ, που λαμβάνουν μέρος στη διαδικασία κρυπτογράφησης αδειών χρήσης περιεχομένου. Η διαδικασία αυτή περιλαμβάνει τις αλληλεπιδράσεις μεταξύ παρόχου και ΑΠΧ, ήτοι τη διαχείριση των χαρακτηριστικών και των δημόσιων κλειδιών των ΑΠΧ, τη δημιουργία μιας συνδυαστικής πολιτικής πρόσβασης και — τελικά— την κρυπτογράφηση της άδειας χρήσης περιεχομένου υπό τη συγκεκριμένη πολιτική πρόσβασης. Τα αυτοτελή δομικά στοιχεία είτε εξάγουν τη λειτουργικότητα υποκείμενων συστημάτων και τα δεδομένα βάσεων υπό τη μορφή υπηρεσιών είτε ενθυλακώνουν τη λογική της συνολικής υπηρεσίας.

Συγκεκριμένα στη διαδικασία συμμετέχουν τα εξής αυτοτελή δομικά στοιχεία:

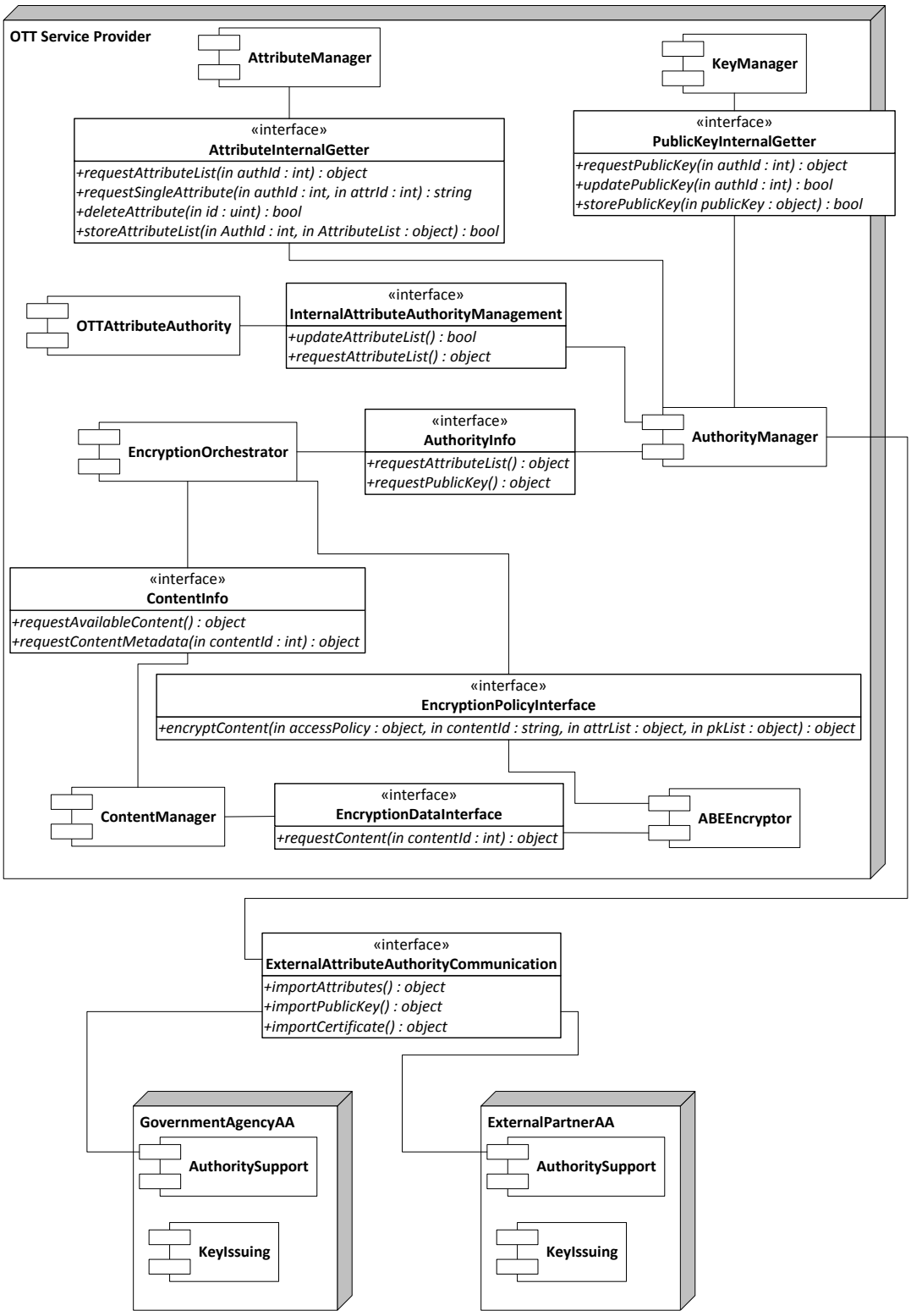
- Ο Ενορχηστρωτής Κρυπτογράφησης (`EncryptionOrchestrator`), ο οποίος συντονίζει την όλη διαδικασία.
- Το Υποσύστημα Διαχείρισης ΑΠΧ (`AuthorityManager`), το οποίο είναι υπεύθυνο για την επικοινωνία τόσο με την ΑΠΧ του παρόχου όσο και με τις εξωτερικές ΑΠΧ, αποκρύπτοντας λεπτομέρειες της επικοινωνίας τους από το υπόλοιπο σύστημα.
- Τα Υποσυστήματα Διαχείρισης Χαρακτηριστικών (`AttributeManager`) και Διαχείρισης Δημοσίων Κλειδιών (`KeyManager`) των ΑΠΧ, τα οποία αποθηκεύουν τα στοιχεία αυτά προκειμένου να είναι διαθέσιμα στο σύστημα.
- Το Υποσύστημα Διαχείρισης Πολυμεσικού Περιεχομένου (`ContentManager`), το οποίο διαχειρίζεται τις άδειες χρήσης και τα μεταδεδομένα πολυμεσικού υλικού προς κρυπτογράφηση.
- Το Υποσύστημα Κρυπτογράφησης Περιεχομένου βάσει Χαρακτηριστικών (`ABEEncryptor`), το οποίο είναι υπεύθυνο για την κρυπτογράφηση των αδειών χρήσης περιεχομένου.
- Τέλος τα Υποσυστήματα Υποστήριξης ΑΠΧ (`AuthoritySupport`), τα οποία εδράζονται στις εξωτερικές ΑΠΧ και τα οποία είναι υπεύθυνα για τις βοηθητικές

λειτουργίες μιας ΑΠΧ (π.χ. την παράθεση των χαρακτηριστικών και του δημοσίου κλειδιού της συγκεκριμένης ΑΠΧ)

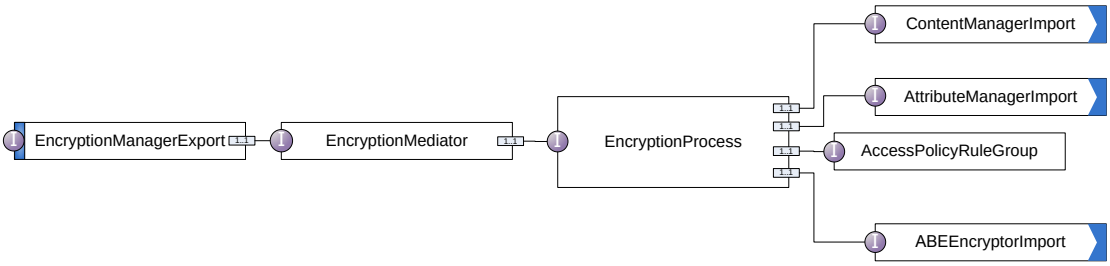
Ο Ενορχηστρωτής Κρυπτογράφησης είναι υπεύθυνος για τη ροή της διεργασίας κρυπτογράφησης αδειών χρήσης πολυμεσικού υλικού. Για την κρυπτογράφηση ενός πολυμέσου στην περίπτωση της αποκεντρωμένης Κρυπτογραφίας ABE απαιτούνται εκτός της άδειας χρήσης, μία πολιτική πρόσβασης βάσει χαρακτηριστικών, τα οποία μπορεί να «προέρχονται» από περισσότερες της μίας ΑΠΧ και τα αντίστοιχα δημόσια κλειδιά των ΑΠΧ αυτών. Επομένως σαν πρώτο βήμα, προκειμένου να καταστεί η κρυπτογράφηση εφικτή, κάθε πάροχος οφείλει να γνωρίζει τα χαρακτηριστικά τα οποία διαχειρίζεται κάθε ΑΠΧ, ώστε να μπορεί να συντάξει πολιτικές πρόσβασης χρησιμοποιώντας τα – και δευτερευόντως να μπορεί να ελέγξει τυχόν εννοιολογικές επικαλύψεις μεταξύ των χαρακτηριστικών της κάθε μίας ΑΠΧ. Κατόπιν για να προχωρήσει στην κρυπτογράφηση καθεαυτή, ο Ενορχηστρωτής Κρυπτογράφησης πρέπει να γνωρίζει και τα δημόσια κλειδιά των ΑΠΧ αυτών.

Ο Ενορχηστρωτής Κρυπτογράφησης αποτελείται από επιμέρους λειτουργικές μονάδες, οι οποίες εμφανίζονται στο Σχήμα 23. Μέσω του ESB πραγματοποιείται εισαγωγή των υπηρεσιών από τα υποσυστήματα Διαχείρισης Χαρακτηριστικών, Διαχείρισης Πολυμεσικού Περιεχομένου και Κρυπτογράφησης Περιεχομένου βάσει χαρακτηριστικών, ενώ έχει προβλεφθεί και εξαγωγή της υπηρεσίας (προς τον ESB), ώστε να δίνεται η δυνατότητα κλήσης της από μία άλλη υπηρεσία. Και στο συγκεκριμένο Ενορχηστρωτή περιλαμβάνεται ένας διαμεσολαβητής, για το μετασχηματισμό των υπηρεσιών. Επιπλέον στη διεργασία γίνεται χρήση ενός συνόλου κανόνων που αποσκοπούν στην παραγωγή των πολιτικών πρόσβασης (`AccessPolicyRuleGroup`).

Σε περίπτωση που είναι επιθυμητή η κρυπτογράφηση του ιδίου του περιεχομένου (και όχι της άδειας χρήσης του) με χρήση Κρυπτογραφίας ABE, τότε θα πρέπει να γίνει χρήση κατάλληλων υποσυστημάτων Διαχείρισης και Κρυπτογράφησης Πολυμεσικού Περιεχομένου. Οι λειτουργίες επί των τμημάτων του περιεχομένου δεν πραγματοποιούνται στο ESB, αλλά μέσω κατάλληλου διαύλου για την μετακίνηση μεγάλων αρχείων (αν και κατακερματισμένα τα αρχεία παραμένουν εξαιρετικά μεγάλα για το ESB). Παρόλα αυτά η ενορχήστρωση της κρυπτογράφησης μπορεί να πραγματοποιηθεί με τη συνδρομή του Ενορχηστρωτή Κρυπτογράφησης, χωρίς να αλλάξει η βασική λειτουργικότητα που έχει ήδη περιγραφεί στην Ενότητα αυτή.



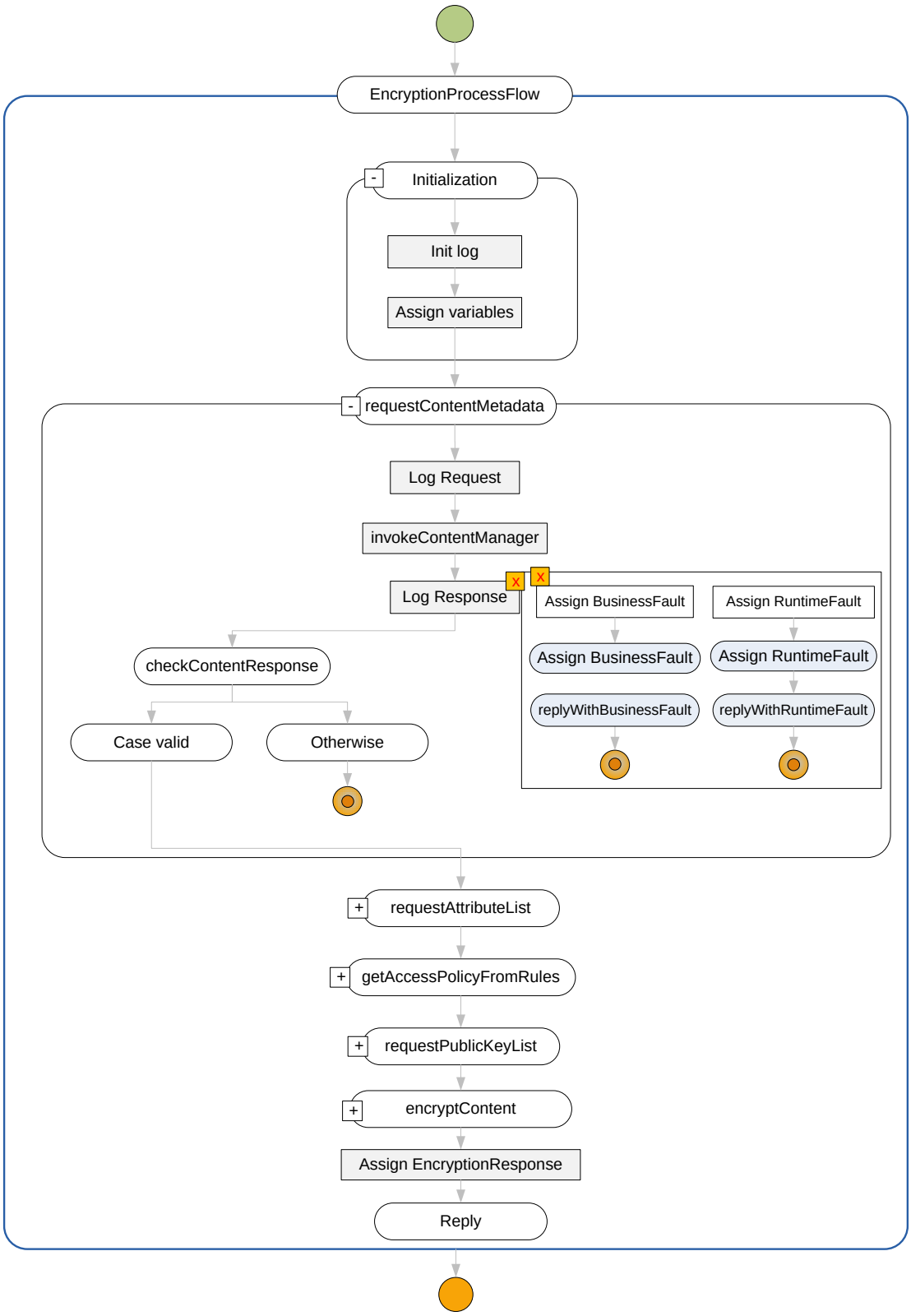
Σχήμα 22 Οργάνωση των δομικών στοιχείων που συμμετέχουν στη διαδικασία κρυπτογράφησης πολυμεσικού περιεχομένου



Σχήμα 23 Εσωτερική διάρθρωση του Ενορχηστρωτή Κρυπτογράφησης

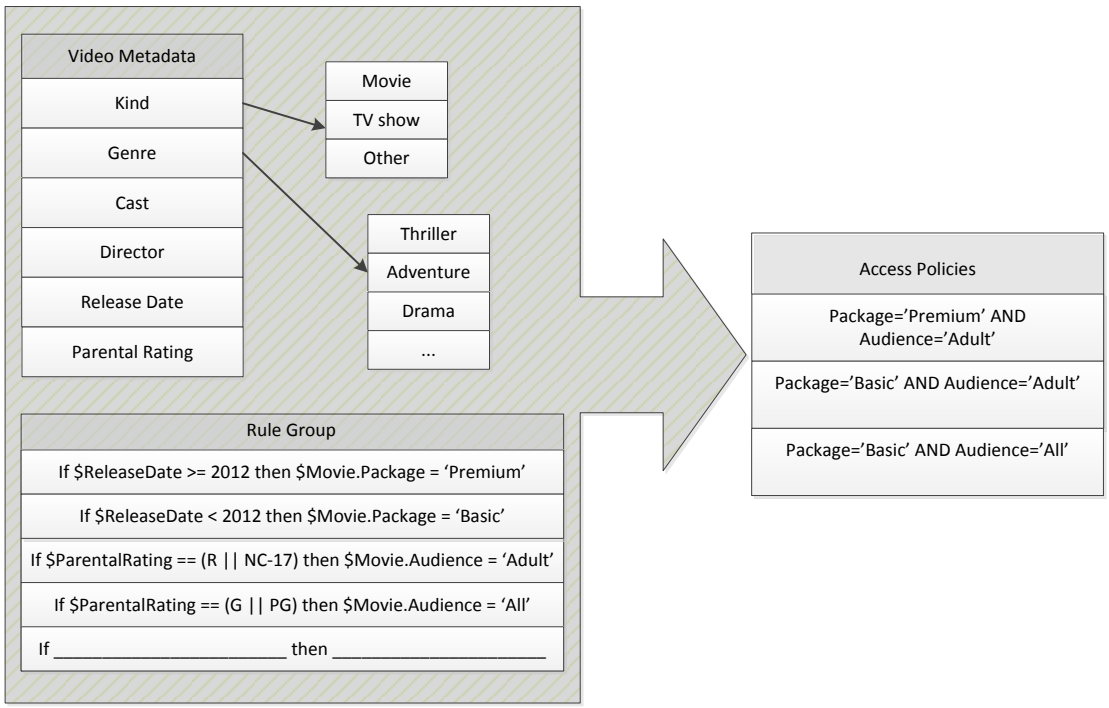
Η λογική της υπηρεσίας περιέχεται στη μονάδα Διεργασίας Κρυπτογράφησης (`EncryptionProcess`), η οποία αποτελεί τον πυρήνα του Ενορχηστρωτή και είναι κωδικοποιημένη σε γλώσσα BPEL. Η συγκεκριμένη μονάδα παρουσιάζεται στο Σχήμα 24.

Στη γραφική αναπαράσταση της ροής παρουσιάζονται τα διαδοχικά βήματα που ακολουθεί η διεργασία κρυπτογράφησης. Αναλυτικότερα παρουσιάζονται οι κλήσεις των υφιστάμενων υπηρεσιών, η καταγραφή της πορείας της διεργασίας, η διαχείριση των σφαλμάτων και άλλες λεπτομέρειες.



Σχήμα 24 Εσωτερική λογική (Διάγραμμα BPEL) του EncryptionOrchestrator

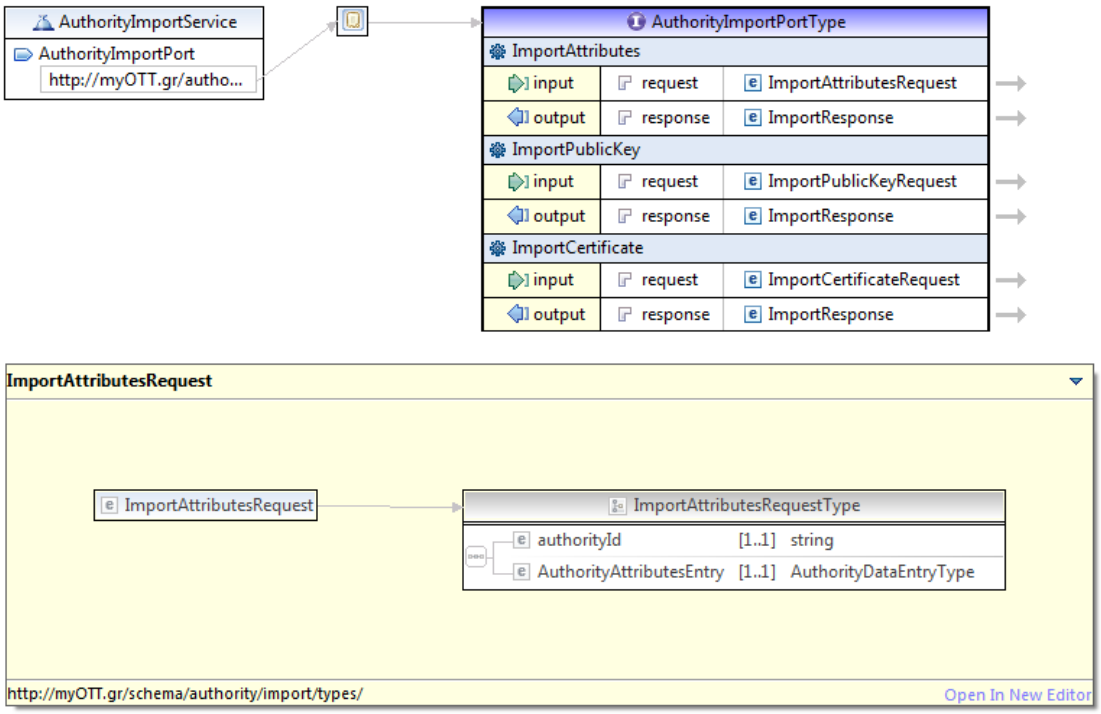
Η δημιουργία των πολιτικών πρόσβασης γίνεται με χρήση των μεταδεδομένων του περιεχομένου και κωδικοποιημένων κανόνων, όπως φαίνεται στο Σχήμα 25.



Σχήμα 25 Δημιουργία πολιτικών πρόσβασης

Στο Σχήμα 26 παρουσιάζεται ο σκελετός της διαδικτυακής υπηρεσίας, η οποία είναι υπεύθυνη για την επικοινωνία μεταξύ των εξωτερικών ΑΠΧ και του παρόχου υπηρεσιών OTT. Στην υπηρεσία έχουν προδιαγραφεί οι εξής τρεις λειτουργίες: η εισαγωγή λίστας χαρακτηριστικών, η εισαγωγή δημοσίου κλειδιού και η εισαγωγή πιστοποιητικού. Κάθε λειτουργία χρησιμοποιεί τους δικούς της τύπους δεδομένων για τις αιτήσεις εισαγωγής, π.χ. η εισαγωγή χαρακτηριστικών περιλαμβάνει ένα αναγνωριστικό της ΑΠΧ και εν συνεχεία μία λίστα μιας ή περισσότερων δομών δεδομένων (αντικειμένων), κάθε μία από τις οποίες περιγράφει ένα χαρακτηριστικό (αναγνωριστικό χαρακτηριστικού, ονομασία χαρακτηριστικού, περιγραφή χαρακτηριστικού).

Σε κάθε περίπτωση, ο πάροχος επιστρέφει απαντήσεις που χρησιμοποιούν τον ίδιο τύπο (ImportResponse), τα πεδία του οποίου παίρνουν διαφορετικές τιμές ανάλογα την υπηρεσία και την έκβασή της.



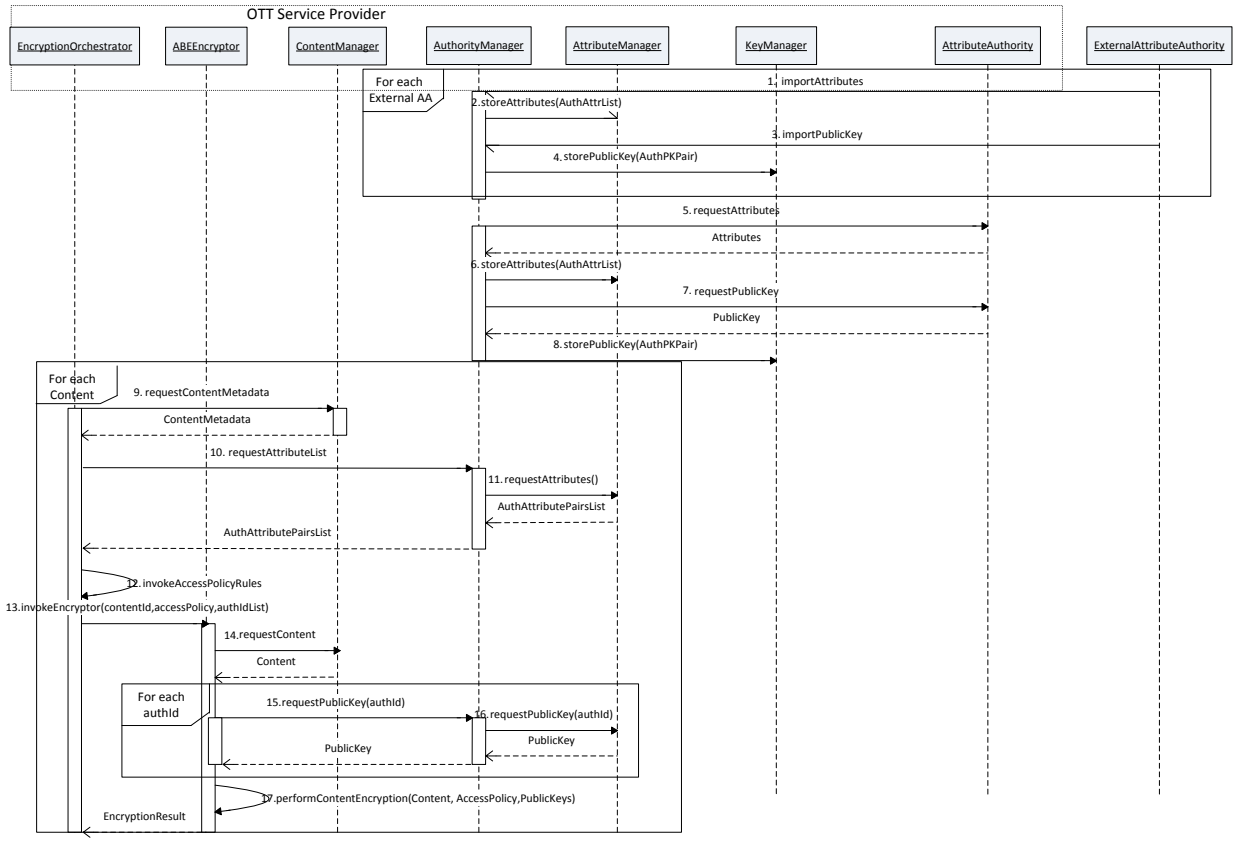
Σχήμα 26 Σκελετός διαδικτυακής υπηρεσίας υπεύθυνης για την επικοινωνία μεταξύ των ανεξάρτητων ΑΠΧ και του παρόχου υπηρεσιών ΟΤΤ.

Οι αλληλεπιδράσεις των συστημάτων που συμμετέχουν στη διαδικασία της κρυπτογράφησης παρουσιάζονται αναλυτικά στο διάγραμμα ακολουθίας υπηρεσίας (Σχήμα 27).

Οι κλήσεις 1-4 είναι επαναλαμβανόμενες για κάθε εξωτερική ΑΠΧ που συμμετέχει στη διαδικασία της κρυπτογράφησης και αφορούν την αποθήκευση του δημόσιου κλειδιού και των χαρακτηριστικών, τα οποία πιστοποιεί η κάθε μία, στον πάροχο υπηρεσιών ΟΤΤ. Αντίστοιχα οι κλήσεις 5-8 αφορούν την «εσωτερική» ΑΠΧ του παρόχου (η οποία βέβαια μπορεί και να έχει ανατεθεί σε εξωτερικό συνεργάτη, αν και δε συνηθίζεται για λόγους ασφαλείας). Συνολικά οι παραπάνω κλήσεις πραγματοποιούνται κατά την αρχικοποίηση του συστήματος και κατόπιν περιοδικά για την ανανέωση των στοιχείων.

Οι κλήσεις 9-17 πραγματοποιούν το κύριο μέρος της κρυπτογράφησης των αδειών χρήσης. Συγκεκριμένα πρώτα ζητούνται τα μεταδεδομένα του περιεχομένου (κλήση 9) και εν συνεχεία τα διαθέσιμα χαρακτηριστικά του συστήματος (κλήσεις 10-11). Με βάση τα παραπάνω και με χρήση προκαθορισμένων κανόνων, πραγματοποιείται η

δημιουργία της πολιτικής πρόσβασης (κλήση 12). Τέλος για την κρυπτογράφηση της άδειας, απαιτούνται (πλέον της πολιτικής πρόσβασης) η ανάκτηση της άδειας (κλήση 14), η ανάκτηση των δημοσίων κλειδιών των εμπλεκόμενων ΑΠΧ (κλήσεις 15-16), προτού πραγματοποιηθεί η καθεαυτή κρυπτογράφηση της (κλήση 17).



Σχήμα 27 Διάγραμμα ακολουθίας της διαδικασίας κρυπτογράφησης αδειών χρήσης πολυμεσικού περιεχομένου

7 Αξιολόγηση Διανομής Πολυμεσικού Περιεχομένου με χρήση Δικτύων ICN

Το παρόν Κεφάλαιο παρουσιάζει την αξιολόγηση της προτεινόμενης λύσης, η οποία πραγματοποιήθηκε με χρήση προσομοιωτή. Καταρχάς περιγράφεται η διάταξη του δικτύου και οι παράμετροι αυτής, ενώ δίνεται βάρος και στο υπό διανομή πολυμεσικό περιεχόμενο. Η αξιολόγηση πραγματοποιείται σε αντιπαραβολή με τα Δίκτυα CDN. Παρουσιάζονται τα οφέλη που επιφέρει η υιοθέτηση των Δικτύων ICN τόσο υπό το πρίσμα του παρόχου υπηρεσιών Διαδικτύου, μέσω της εξοικονόμησης διαδικτυακής κίνησης, όσο και από την πλευρά του τελικού χρήστη, μέσω της ελαχιστοποίησης των χρόνων αναμονής πριν και κατά τη διάρκεια της αναπαραγωγής του πολυμέσου.

7.1 Στρατηγική πειραμάτων

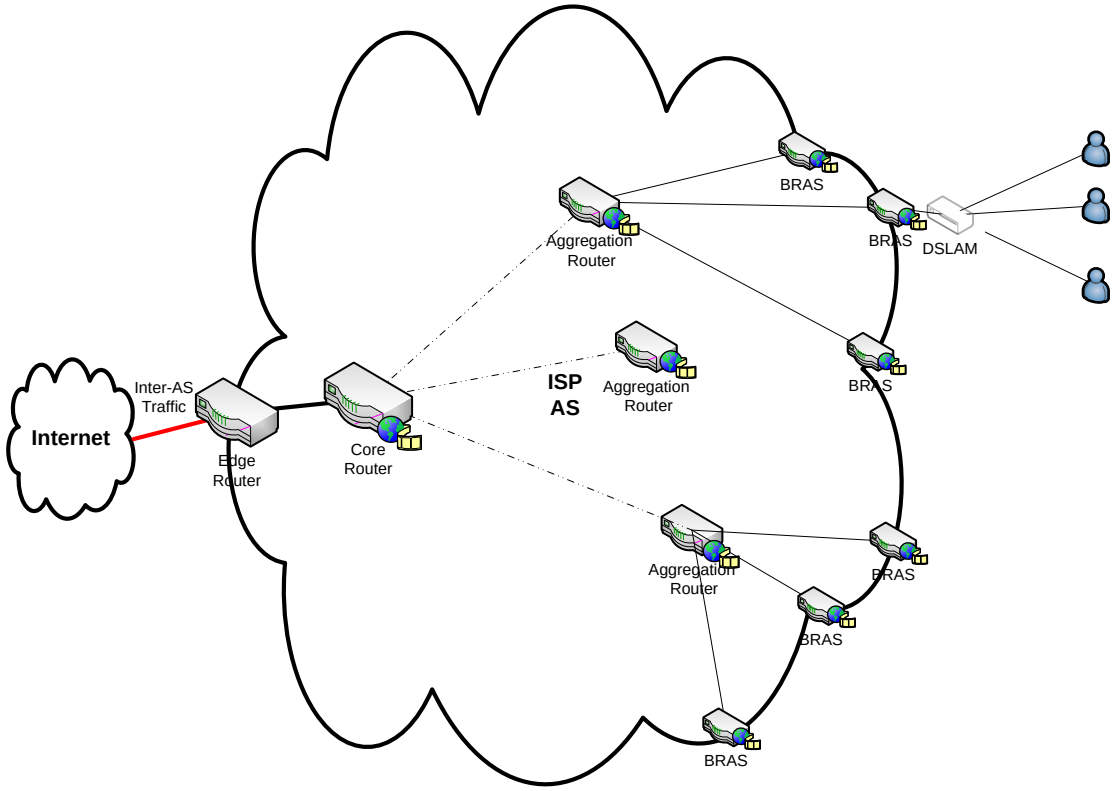
Η εκτίμηση της απόδοσης πολυμεσικών ροών σε Δίκτυα ICN έγινε με βάση τον προσομοιωτή JCCNxSim, ο οποίος αναπτύχθηκε στα πλαίσια της Διατριβής [126]. Ο JCCNxSim έχει στηριχθεί στο λογισμικό ανοιχτού κώδικα PeerSim [127], [128], το οποίο χρησιμοποιείται για τη διεξαγωγή προσομοιώσεων σε δίκτυα ομοτίμων κόμβων, με έμφαση σε ροές πολυμεσικού περιεχομένου. Ο PeerSim επεκτάθηκε ώστε να είναι δυνατή η χρήση του για προομοιώσεις Δικτύων ICN και ειδικότερα δικτύων που ακολουθούν το πρότυπο CCNx.

Προκειμένου να καταστούν σαφή τα πλεονεκτήματα των Δικτύων ICN σε σχέση με τις υφιστάμενες τεχνολογίες, η προσομοίωση εστιάζει σε προκαθορισμένα σενάρια διανομής πολυμεσικού περιεχομένου με χρήση Δικτύων ICN σε αντιπαραβολή με τη διανομή με χρήση Δικτύων CDN.

Για την αναπαράσταση του δικτύου χρησιμοποιήθηκε δενδρική τοπολογία, σε σύμπνοια με αντίστοιχες προσεγγίσεις της βιβλιογραφίας, όπως για παράδειγμα το [129], με τη διαφορά ότι στην παρούσα θεώρησή το δένδρο έχει έξι επίπεδα και κάθε κόμβος έχει τρία παιδιά. Το δένδρο αποτελεί ένα αυτόνομο σύστημα (Autonomous System - AS) ενός παρόχου υπηρεσιών Διαδικτύου. Ο κεντρικός διακομιστής του παρόχου (core network router) αναπαρίσταται από τη ρίζα του δένδρου, οι ενδιάμεσοι κόμβοι

αντιστοιχούν στην κύρια υποδομή του παρόχου (διακομιστές/μεταγωγείς) και, τέλος, τα φύλλα αντιπροσωπεύουν τους διακομιστές απομακρυσμένης ευρυζωνικής πρόσβασης (Broadband Remote Access Server- BRAS). Το δίκτυο μετάδοσης (Transport Network - TN), το οποίο αποτελεί τις ακμές του δένδρου, ακολουθεί τα πρότυπα τεχνολογίας ATM (Asynchronous Transfer Mode) [130],[131].

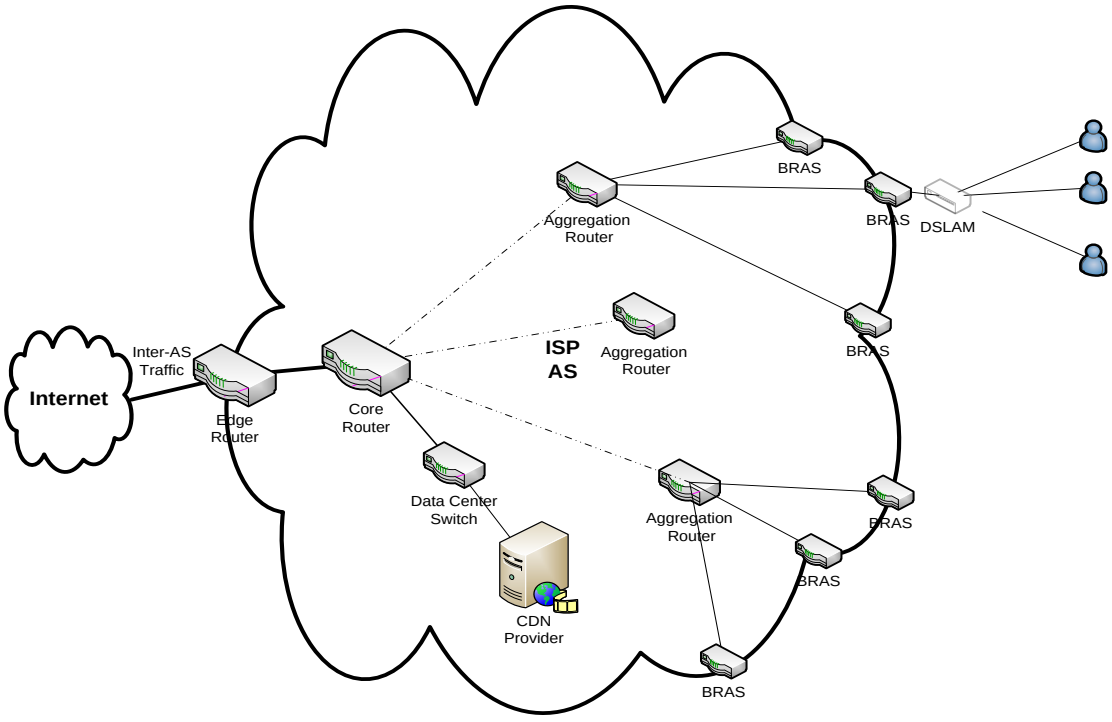
Για την περίπτωση των Δικτύων ICN θεωρήσαμε ότι οι κρυφές μνήμες είναι παρούσες σε όλα φύλλα του δένδρου (Σχήμα 28), ενώ στην περίπτωση της χρήσης Δικτύων CDN, ο εξυπηρετητής βρίσκεται απευθείας συνδεδεμένος με τον κεντρικό εξυπηρετητή του παρόχου και εντός του αυτόνομου συστήματος (βλ. Σχήμα 29).



Σχήμα 28 Τοπολογία παρόχου Διαδικτύου με χρήση Δικτύων ICN

Για την πραγματοποίηση των προσομοιώσεων επιλέχθηκαν οι εξής τιμές για τα παραμετροποιήσιμα χαρακτηριστικά του δικτύου. Η ταχύτητα του δικτύου του παρόχου είναι της τάξεως των 155 Mbps —η οποία υποστηρίζεται από τα δίκτυα ATM OC-3, ενώ οι συνδρομητές συνδέονται στο δίκτυο με ταχύτητα 6 Mbps (ταχύτητα μάλλον συντηρητική για συνδέσεις aDSL). Επιπροσθέτως, για την πιστότερη αναπαραγωγή των πραγματικών συνθηκών, έχει προβλεφθεί μεταβαλλόμενη κίνηση υποβάθρου με άνω όριο το 1 Mbps. Επομένως η εγγυημένη χωρητικότητα της γραμμής για την πολυμεσική ροή είναι 5

Mbps. Η κίνηση υποβάθρου θεωρείται ότι προέρχεται από περιήγηση σε ιστοσελίδες, διαδικτυακές κλήσεις κλπ.



Σχήμα 29 Τοπολογία παρόχου Διαδικτύου με χρήση Δικτύων CDN

Στην πλευρά του τελικού χρήστη προσομοιώνεται μία εφαρμογή αναπαραγωγής πολυμέσων, η οποία με την ολοκλήρωση της λήψης κάθε τμήματος του πολυμέσου, προχωρά σε ένα αίτημα για το επόμενο τμήμα του. Η μετάφραση των μηνυμάτων HTTP σε πακέτα Interest (βλέπε Ενότητα 3.3) γίνεται με τη χρήση πληρεξούσιου κόμβου κατ' αντιστοιχία με το [74]. Το ληφθέν τμήμα του πολυμέσου αποθηκεύεται —μέχρι την αναπαραγωγή του— σε ενταμιευτή, ο οποίος για λόγους απλότητας έχει θεωρηθεί επαρκώς μεγάλος.

Τα υπό εξέταση μεγέθη είναι η πιθανότητα ανάκτησης ενός τμήματος του πολυμέσου από την κρυφή μνήμη των κόμβων του Δικτύου ICN (ή του CDN) του αυτόνομου συστήματος όπου συνδέεται ο πελάτης (cache hit rate), ο χρόνος αναμονής κατά την εκκίνηση και κατά τη διάρκεια της αναπαραγωγής του πολυμέσου (οι δύο αυτοί χρόνοι, σε συνάρτηση και με το μέγεθος του διαθέσιμου ενταμιευτή, βρίσκονται στα άκρα μιας διελκυστίνδας, καθώς η αύξηση του αρχικού χρόνου αναμονής εν γένει βελτιώνει την αναμονή κατά τη διάρκεια της αναπαραγωγής του πολυμέσου, έχοντας επίδραση στην εμπειρία του χρήστη [132]) και τέλος η κίνηση (τα μηνύματα Interest), η

οποία εξέρχεται από το αυτόνομο σύστημα του παρόχου, και για την οποία —κατά την πάγια τακτική— ο πάροχος χρεώνεται. Τα δύο πρώτα μεγέθη επιλέχθηκαν κυρίως για την επίπτωσή τους στην ποιότητα υπηρεσίας του πελάτη, σε αντιστοιχία και με την προσέγγιση της εργασίας [133], ενώ το τρίτο επιλέχτηκε για να εξεταστούν τα πλεονεκτήματα της προσέγγισης των Δικτύων ICN από τη θέση του παρόχου υπηρεσιών Διαδικτύου – αν και ο πάροχος ωφελείται εμμέσως και από τη βελτιωμένη ποιότητα υπηρεσίας του πελάτη.

Στο προσομοιωθέν σύστημα είναι διαθέσιμες εκατό (100) πολυμεσικές ροές (βίντεο), διάρκειας τριάντα (30) λεπτών έκαστη, οι οποίες έχουν τεμαχιστεί σε τμήματα των δέκα (10) δευτερολέπτων, κατά τα πρότυπα του HLS [30]. Το όνομα κάθε τμήματος ακολουθεί την πρόταση του NDN [52] και είναι της μορφής `<MULTIMEDIA TITLE>/<SEGMENT>`. Στο σύστημα είναι συνδεδεμένοι πέντε χιλιάδες (5000) τελικοί χρήστες. Η δημοτικότητα των πολυμέσων ακολουθεί το νόμο του Zipf [134], όπου κάθε πολυμεσική ροή αποτελεί μία κλάση. Η δημοτικότητα κάθε κλάσης είναι αντιστρόφως ανάλογη της κλάσης της, σύμφωνα με τον τύπο

$$P_k = {}^{c}/_{k^{\alpha}}$$

, (όπου $\alpha = 0.82$, $c > 0$) δηλαδή υπάρχει ένας πολύ μικρός αριθμός πολυμέσων με μεγάλη δημοτικότητα και ένας μεγάλος αριθμός με μικρή, όπως προτείνεται στη βιβλιογραφία [134]. Οι ποιότητες των πολυμέσων επιλέχθηκαν ώστε να καλύψουν ένα ευρύ φάσμα· συγκεκριμένα η χαμηλή ποιότητα 1 Mbps αντιστοιχεί σε χαμηλής ποιότητας βίντεο (640x360), η μεσαία 2.5 Mbps σε SD βίντεο (854x480), ενώ η υψηλότερη 5 Mbps σε βίντεο HD (1280x720 ή 720p).

Οι προσομοιώσεις πραγματοποιήθηκαν μεταβάλλοντας σταδιακά το μέγεθος του αποθηκευτικού χώρου που διατίθεται στους κόμβους του δικτύου – και ο οποίος είναι ίδιος για όλους τους κόμβους. Ο αποθηκευτικός χώρος παρουσιάζεται σαν ποσοστό του συνολικού διατιθέμενου περιεχομένου και κατά κανόνα κυμαίνεται από 0.1% έως 1% του περιεχομένου αυτού (ώστε να ομοιάζει με πραγματικές συνθήκες).

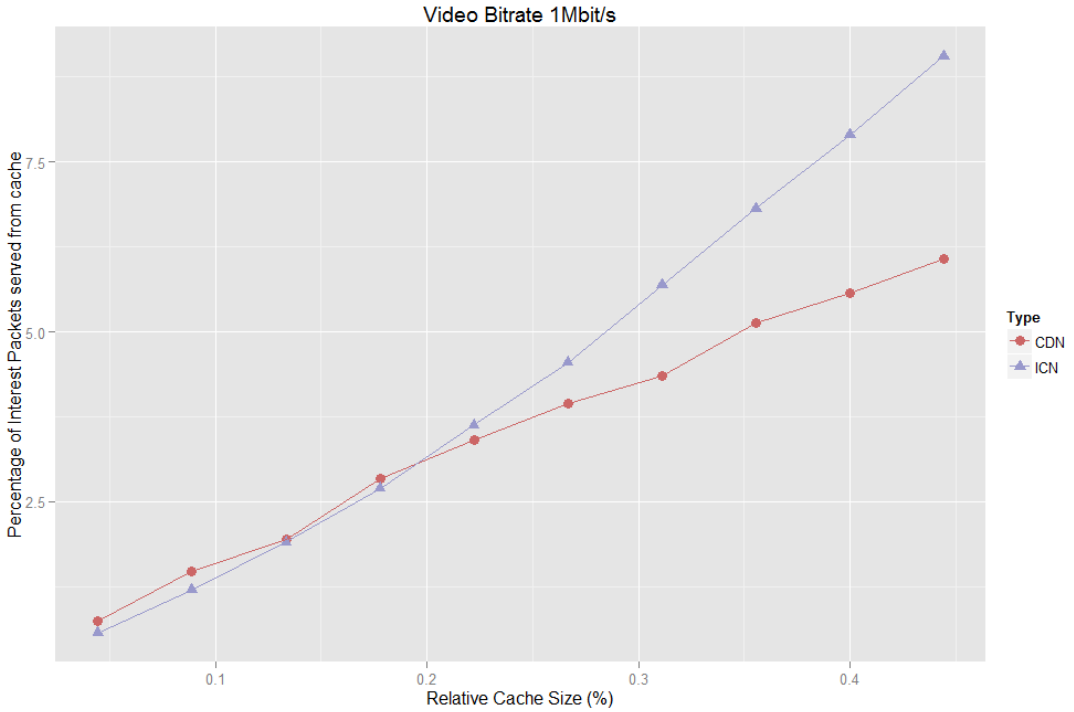
7.2 Ανάλυση αποτελεσμάτων

7.2.1 Αξιολόγηση από τη θέση του παρόχου Διαδικτύου

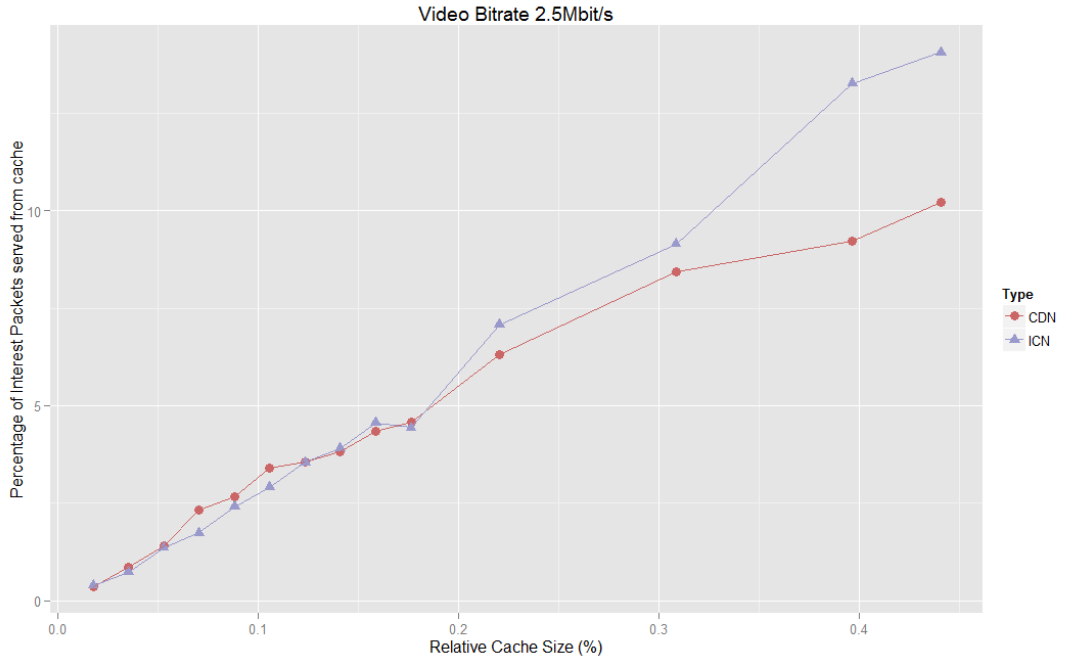
Ένα σημαντικό έξοδο των παρόχων υπηρεσιών Διαδικτύου είναι το κόστος της εξερχόμενης κίνησης προς άλλους παρόχους (με τους οποίους δεν έχουν προχωρήσει σε συμφωνία αμοιβαίας μη-χρέωσης). Επομένως, ένας από τους στόχους των παρόχων αυτών είναι η ελαχιστοποίηση της συγκεκριμένης κίνησης. Αυτός ήταν άλλωστε ένας από τους λόγους που η τεχνολογία των Δικτύων CDN γνώρισε τόσο μεγάλη επιτυχία. Όπως αναφέρθηκε και στο δεύτερο Κεφάλαιο, ένα από τα πλεονεκτήματα των Δικτύων ICN, και ιδιαίτερα της δρομολόγησης με βάση το όνομα, είναι ότι επιτρέπει τη χρήση αποθηκευτικού χώρου σε κάθε δρομολογητή. Τοιουτοτρόπως ένα μέρος των αιτήσεων εξυπηρετείται από τους διακομιστές που ανήκουν στο δίκτυο του παρόχου, με συνέπεια τη μείωση της εξερχόμενης κίνησης προς τρίτους παρόχους. Η κίνηση που εξέρχεται των ορίων του παρόχου καλύπτεται από συμβόλαια-συμφωνίες επιπέδου εξυπηρέτησης (Service License Agreement - SLA) και συνοδεύεται από αντίστοιχες χρεώσεις για τον πάροχο.

Στα Σχήματα 30, 31 και 32 παρουσιάζεται —για τις τρεις επιλεγμένες ποιότητες— η πιθανότητα εύρεσης ενός τμήματος του περιεχομένου στον αποθηκευτικό χώρο κάποιου δρομολογητή του αυτόνομου συστήματος όπου είναι συνδεδεμένος ο πελάτης, σε σχέση με το μέγεθος της μνήμης που έχει στη διάθεσή του ο εξυπηρετητής. Σύμφωνα με την προσομοίωση, η συγκεκριμένη πιθανότητα αυξάνεται σχεδόν γραμμικά σε σχέση με το μέγεθος της μνήμης. Τα δίκτυα ICN, ιδίως καθώς αυξάνεται η διαθέσιμη μνήμη, παρουσιάζουν μεγαλύτερη πιθανότητα εύρεσης τμήματος στον αποθηκευτικό χώρο σε σχέση με τα Δίκτυα CDN. Ταυτόχρονα, για ίδια (σαν ποσοστό σε σχέση με το συνολικό περιεχόμενο και όχι απόλυτα) μεγέθη μνήμης, παρατηρούμε ότι όσο αυξάνεται η ποιότητα, αυξάνεται το ποσοστό του περιεχομένου που εξυπηρετείται από τους αποθηκευτικούς χώρους, καθώς τα τμήματα του περιεχομένου παραμένουν περισσότερο χρόνο στον αποθηκευτικό χώρο —σε συμφωνία και με τα συμπεράσματα του [135], όπου ο χρόνος παραμονής στον αποθηκευτικό χώρο μειώνεται με την αύξηση του συνολικού ρυθμού αφίξεων. Στις χαμηλότερες ποιότητες οι αιτήσεις και άρα οι αντίστοιχες αφίξεις πραγματοποιούνται ταχύτερα, διότι κάθε αίτηση πραγματοποιείται με την ολοκλήρωση της μεταφόρτωσης του προηγούμενου τμήματος του περιεχομένου. Αυτό επιβεβαιώνεται και από επιπλέον προσομοίωση για την ποιότητα των 5 Mbps, όπου η χωρητικότητα της

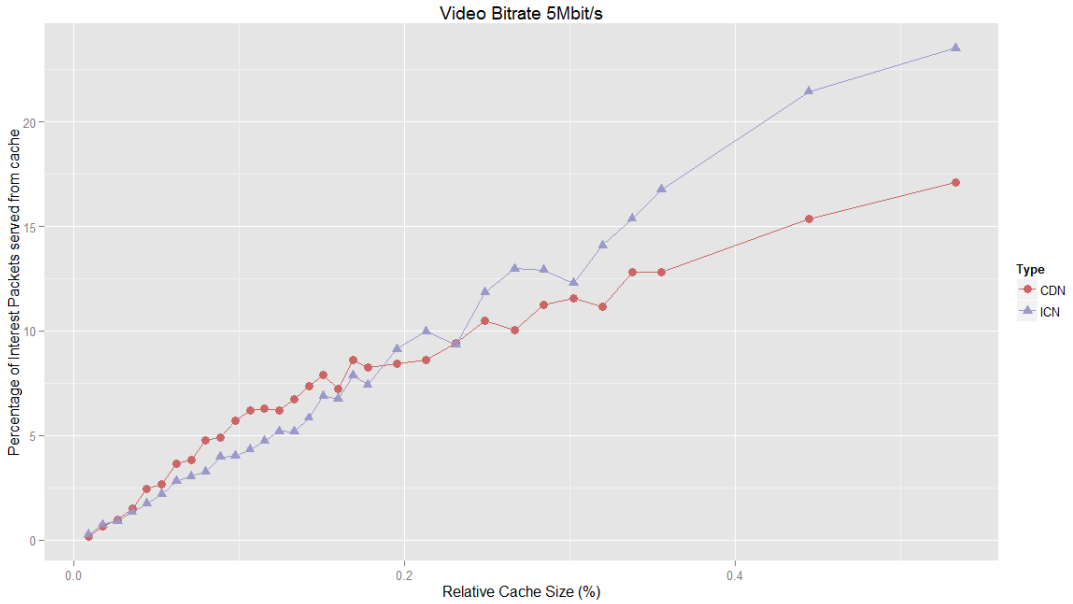
γραμμής του χρήστη ανέρχεται σε 12 Mbps. Η πιθανότητα εύρεσης τμήματος περιεχομένου στη μνήμη είναι μεγαλύτερη για τη γραμμή των 6 Mbps (Σχήμα 33).



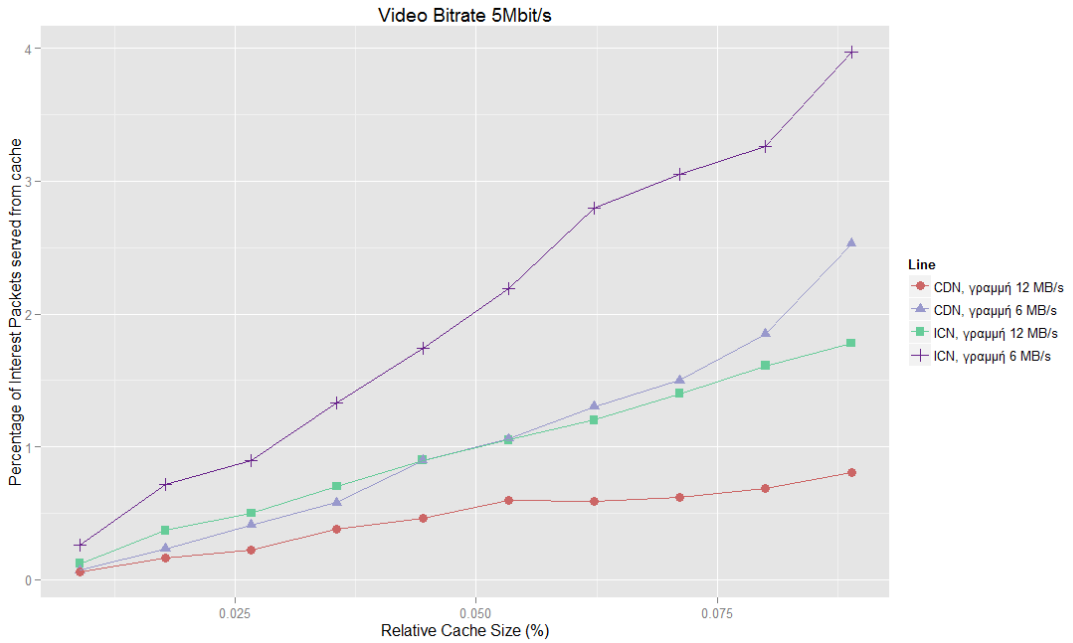
Σχήμα 30 Ποσοστό ανάκτησης περιεχομένου από την κρυφή μνήμη για ποιότητα 1 Mbit/s



Σχήμα 31 Ποσοστό ανάκτησης περιεχομένου από την κρυφή μνήμη για ποιότητα 2.5 Mbit/s



Σχήμα 32 Ποσοστό ανάκτησης περιεχομένου από την κρυφή μνήμη για ποιότητα 5 Mbit/s



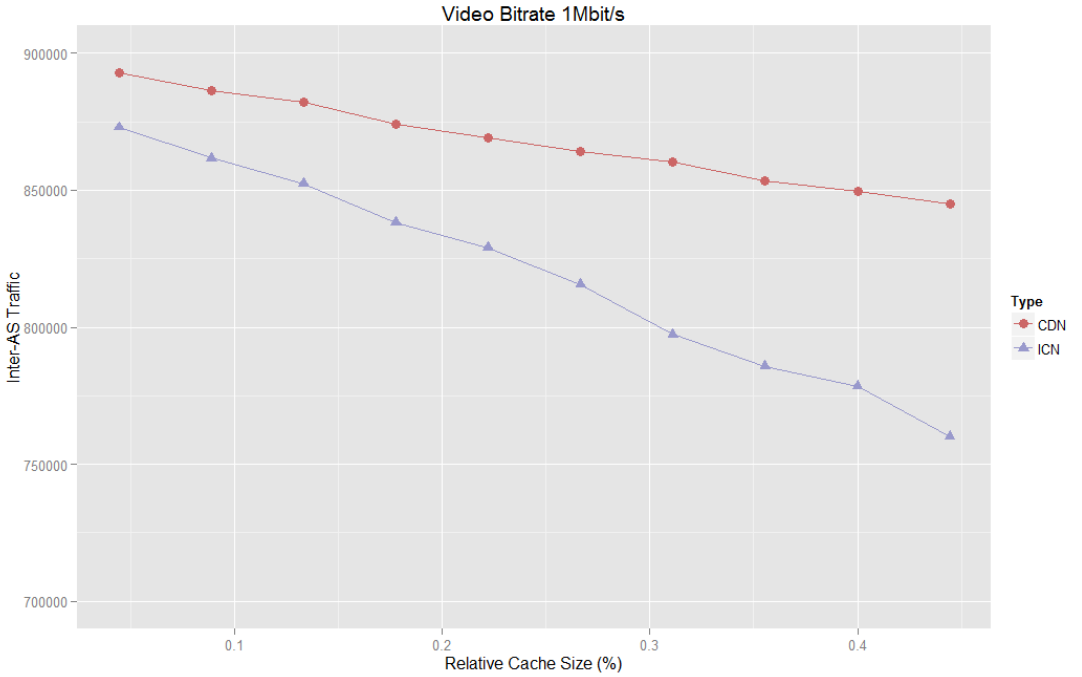
Σχήμα 33 Ποστοστό ανάκτησης περιεχομένου από την κρυφή μνήμη για ποιότητα 5 και γραμμές 5, 12 Mbps

Παρομοίως, στα Σχήματα 34, 35 και 36 παρουσιάζεται η δικτυακή κίνηση (εκφρασμένη σε αριθμό μηνυμάτων Interest) που εξέρχεται από το αυτόνομο σύστημα του παρόχου. Όπως μπορεί κανείς να παρατηρήσει, η εξερχόμενη κίνηση ελαττώνεται με την αύξηση του μεγέθους του αποθηκευτικού χώρου της μνήμης και στις δύο περιπτώσεις (Δίκτυα ICN και CDN). Αυτή η παρατήρηση είναι σε σύμπνοια με τα

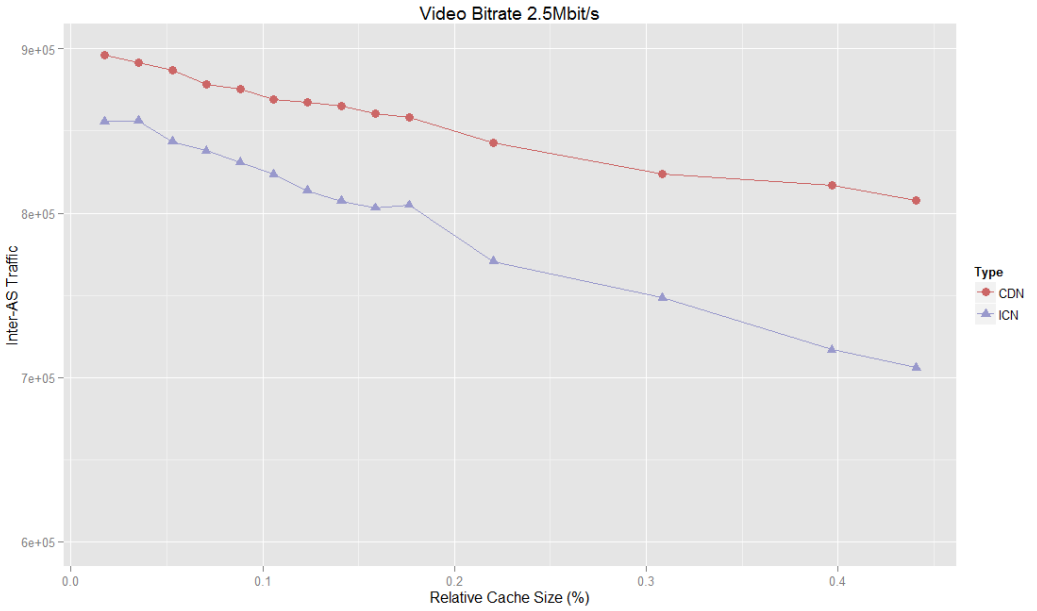
αποτελέσματα για τη χρήση των αποθηκευτικών χώρων, καθώς —όπως είδαμε προηγουμένως— η αύξηση του μεγέθους της διαθέσιμης μνήμης αυξάνει το ποσοστό του περιεχομένου που ανακτάται από αυτήν. Συνεπώς η εξερχόμενη του AS κίνηση ελαττώνεται. Επίσης, σε αντιστοιχία με τα αποτελέσματα για τη χρήση των αποθηκευτικών χώρων, παρατηρούμε ότι όσο υψηλότερη η ποιότητα, τόσο περισσότερη εξερχόμενη κίνηση «παγιδεύεται» εντός του δικτύου του παρόχου.

Τέλος, όσον αφορά τη σύγκριση των Δικτύων ICN με τα Δίκτυα CDN, παρατηρούμε ότι η εξερχόμενη κίνηση στα δίκτυα ICN είναι σημαντικά μικρότερη. Αυτό δεν οφείλεται τόσο στο ποσοστό ανάκτησης από τους αποθηκευτικούς χώρους —όπου τα Δίκτυα ICN και CDN δεν είχαν μεγάλες διαφορές— αλλά στη λειτουργικότητα του Πίνακα Εκκρεμών Αιτημάτων των Δικτύων ICN, ο οποίος αθροίζει τα εκκρεμή αιτήματα που αφορούν το ίδιο περιεχόμενο.

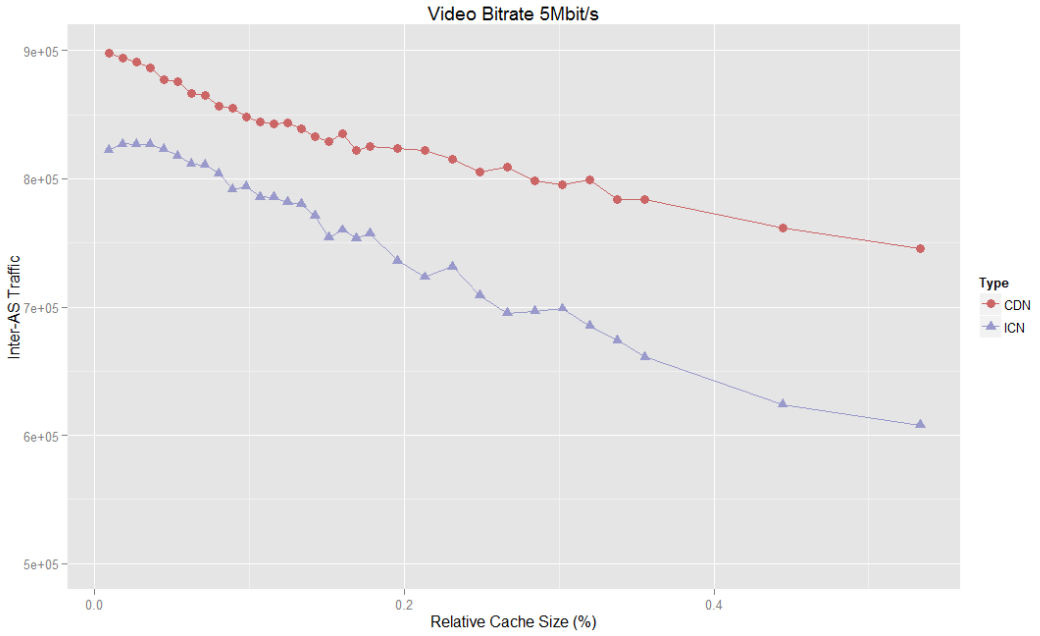
Εξετάζοντας το συμφέρον του παρόχου με βάση τις παραπάνω μετρήσεις, η προσέγγιση των Δικτύων ICN εκτιμάται θετικά – σε σχέση με την τεχνολογία αιχμής, η οποία χρησιμοποιείται στις σύγχρονες λύσεις διανομής πολυμεσικού περιεχομένου.



Σχήμα 34 Εξερχόμενη κίνηση (μηνύματα Interest) από το αυτόνομο σύστημα του παρόχου για ποιότητα βίντεο 1 Mbit/s



Σχήμα 35 Εξερχόμενη κίνηση (μηνύματα Interest) από το αυτόνομο σύστημα του παρόχου για ποιότητα βίντεο 2.5 Mbit/s



Σχήμα 36 Εξερχόμενη κίνηση (μηνύματα Interest) από το αυτόνομο σύστημα του παρόχου για ποιότητα βίντεο 5 Mbit/s

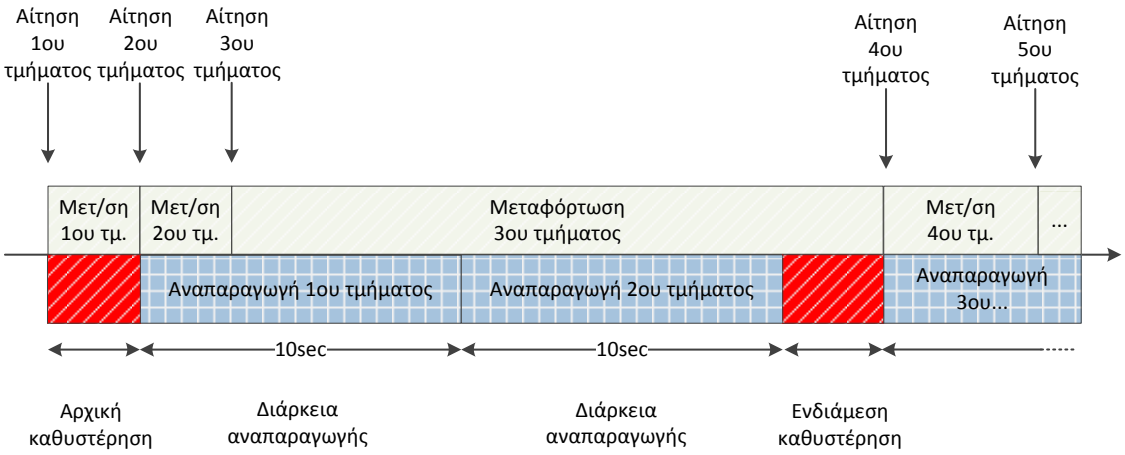
7.2.2 Αξιολόγηση από τη θέση του τελικού χρήστη

Η ποιότητας της εμπειρίας του χρήστη είναι στην πράξη ένας συνδυασμός τόσο του επιπέδου δικτυακής ποιότητας υπηρεσίας (καθυστέρηση, χαμένα πακέτα, κλπ) όσο

και παραμέτρων ανεξαρτήτων του δικτύου, όπως η κωδικοποίηση και συμπίεση του πολυμέσου, ο συγχρονισμός εικόνας και ήχου.

Καθώς ο στόχος της προσομοίωσης είναι η αξιολόγηση των Δικτύων ICN επιλέξαμε να επικεντρώσουμε τη μελέτη μας όχι γενικώς στην ποιότητα εμπειρίας του χρήστη, όσο σε ορισμένα αντικειμενικά μεγέθη που άπτονται της ποιότητας υπηρεσίας του δικτύου, όπως ο χρόνος αναμονής κατά την εκκίνηση και ο χρόνος αναμονής κατά τη διάρκεια της αναπαραγωγής του πολυμέσου (πάγωμα της εικόνας). Τα δύο παραπάνω μεγέθη εξετάζονται σε σχέση με την ποιότητα του πολυμέσου που λαμβάνει η εφαρμογή αναπαραγωγής, τη χωρητικότητα της γραμμής του χρήστη και τον αποθηκευτικό χώρο που είναι διαθέσιμος στο δίκτυο.

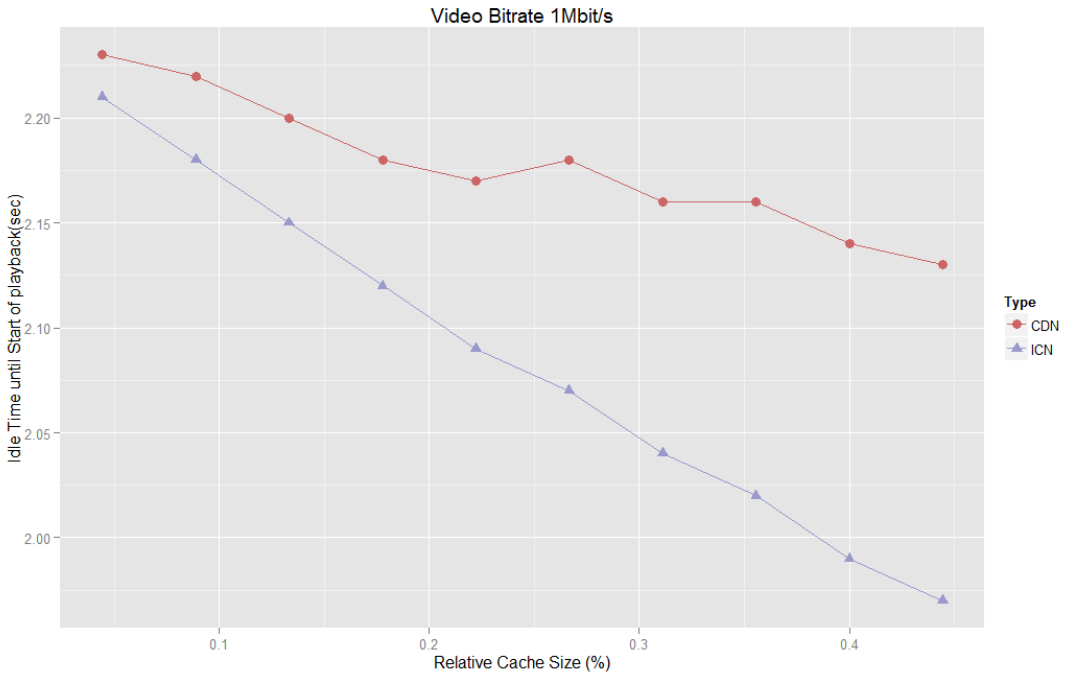
Ο χρόνος αναμονής κατά την εκκίνηση ορίζεται σαν η χρονική απόκλιση από τη στιγμή που ο χρήστης πραγματοποιεί μία αίτηση στο σύστημα για συγκεκριμένο περιεχόμενο έως ότου το λάβει. Στην περίπτωσή μας αυτό αντικατοπτρίζεται στο χρόνο αναμονής από τη στιγμή που ο χρήστης επιλέξει την έναρξη της αναπαραγωγής του πολυμέσου μέχρι αυτό να ξεκινήσει να αναπαράγεται στην οθόνη του τερματικού του. Ο χρόνος αναμονής κατά την εκκίνηση είναι μία από τις προτεινόμενες μετρικές της ποιότητας της εμπειρίας του χρήστη [136]. Στο Σχήμα 37 απεικονίζονται οι χρόνοι αναμονής κατά την εκκίνηση και κατά τη διάρκεια αναπαραγωγής ενός πολυμέσου.



Σχήμα 37 Καθυστερήσεις κατά την αναπαραγωγή πολυμεσικού περιεχομένου

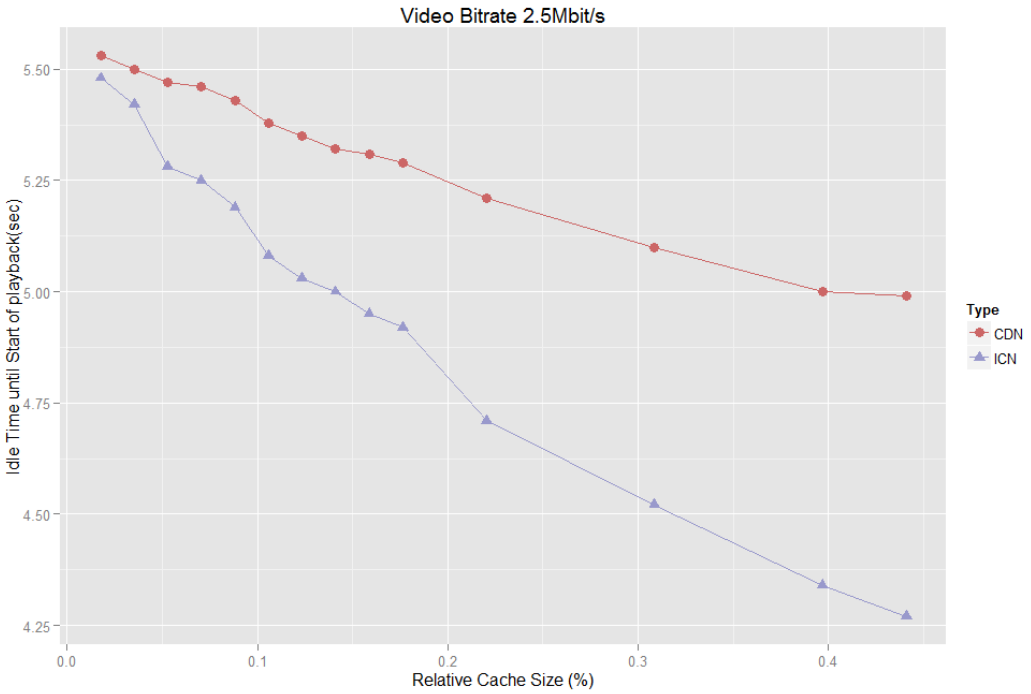
Σύμφωνα με πρόσφατη έρευνα [137], ο χρόνος αναμονής κατά την εκκίνηση της αναπαραγωγής πολυμεσικού περιεχομένου είναι κρίσιμος για τους παρόχους.

Ειδικότερα, τονίζεται ότι εάν ο χρόνος αναμονής κατά την εκκίνηση ξεπεράσει τα δύο δευτερόλεπτα, ο αριθμός των χρηστών που εγκαταλείπουν την αναπαραγωγή αυξάνεται σημαντικά. Πιο συγκεκριμένα, το ποσοστό των θεατών που εγκαταλείπουν αυξάνεται κατά 140% στην περίπτωση της αναμετάδοσης ζωντανού περιεχομένου και εκτινάσσεται στο 400% στην περίπτωση του βίντεο κατά παραγγελία μεγάλης διάρκειας. Όπως παρατηρούμε στη γραφική παράσταση του Σχήματος 38, για τους δεδομένους αποθηκευτικούς χώρους, ο χρόνος αναμονής κατά την εκκίνηση στην περίπτωση των Δικτύων ICN, τείνει να μειωθεί κάτω από δύο δευτερόλεπτα, ενώ οι αντίστοιχοι χρόνοι στα Δίκτυα CDN είναι οριακά μεγαλύτεροι. Αντίστοιχα στην περίπτωση της υψηλότερης ποιότητας (Σχήμα 39) οι χρόνοι αναμονής είναι μεν μεγαλύτεροι, αλλά με τη χρήση των Δικτύων ICN επιτυγχάνεται ταχύτερη μείωση του χρόνου αναμονής σε σχέση με τα Δίκτυα CDN.



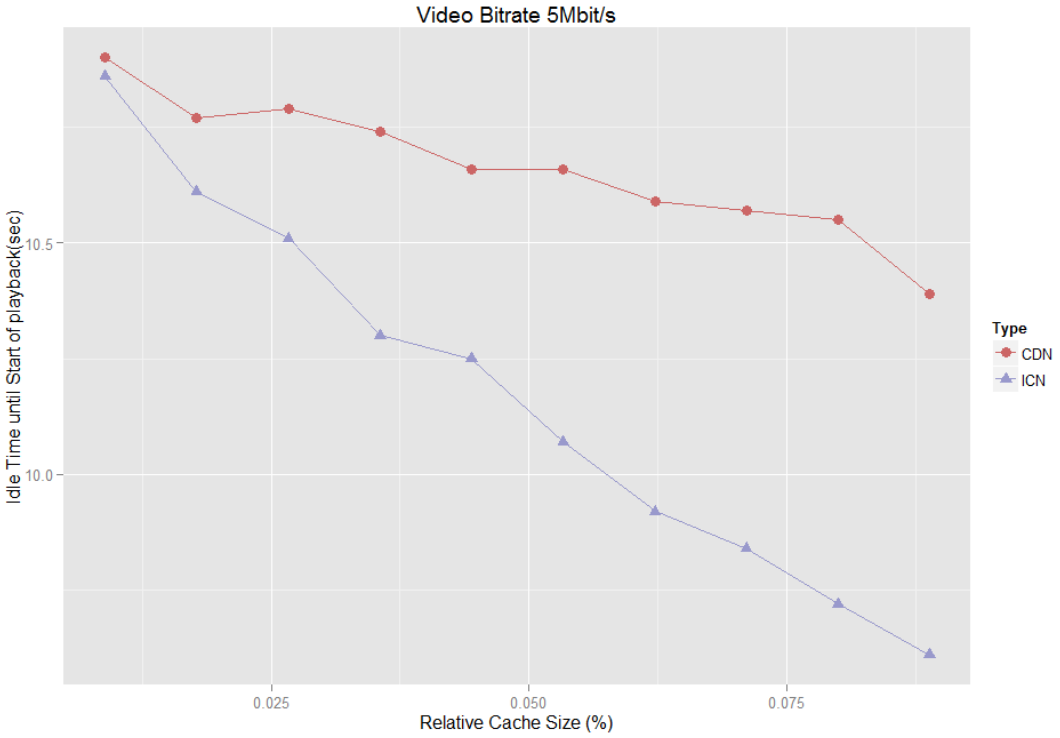
Σχήμα 38 Χρόνος Αναμονής μέχρι την Εκκίνηση Αναπαραγωγής (1 Mbit/s)

Αναφορικά με τους χρόνους αναμονής κατά τη διάρκεια της αναπαραγωγής του περιεχομένου, αυτοί στην περίπτωση των ποιοτήτων 1 Mbps και 2.5 Mbps είναι μηδενικοί (τόσο με χρήση Δικτύων ICN όσο και με χρήση Δικτύων CDN), επομένως η εμπειρία του χρήστη δεν επηρεάζεται αρνητικά από τη συγκεκριμένη μετρική.

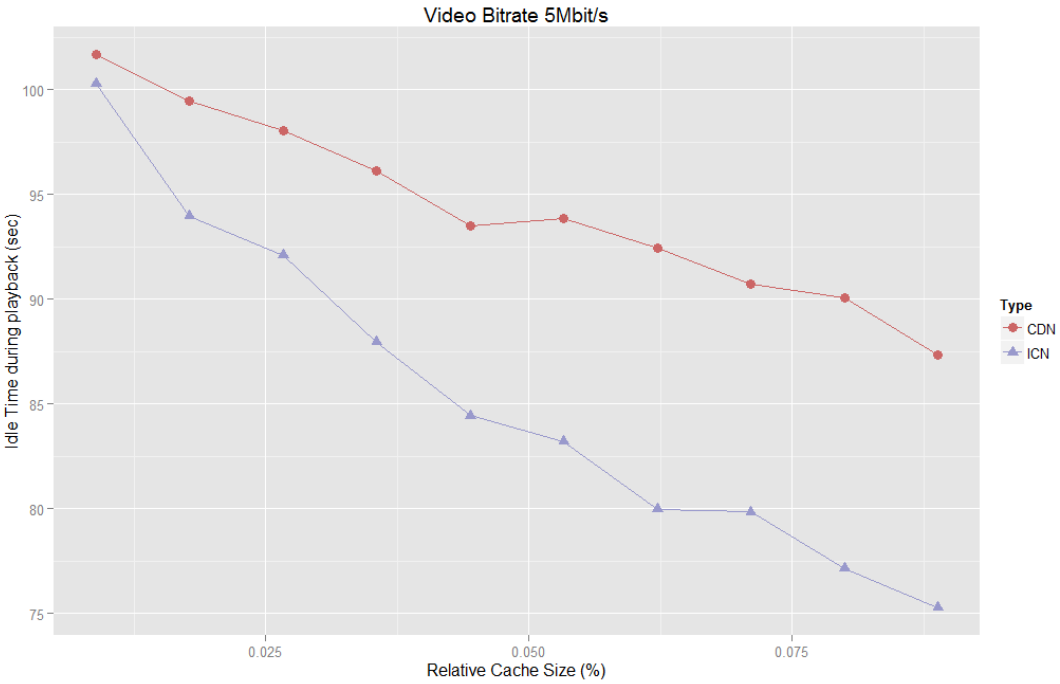


Σχήμα 39 Χρόνος Αναμονής μέχρι την Εκκίνηση Αναπαραγωγής (2.5 Mbit/s)

Στη περίπτωση της υψηλής ποιότητας (5 Mbps), οι ανενεργοί χρόνοι (μετρημένοι σε δευτερόλεπτα) μέχρι την εκκίνηση της αναπαραγωγής του βίντεο σε σχέση με το μέγεθος της κρυφής μνήμης των κόμβων του δικτύου καταγράφονται στο Σχήμα 40, ενώ οι αντίστοιχοι χρόνοι αναμονής κατά τη διάρκεια της αναπαραγωγής του βίντεο αποτυπώνονται στο Σχήμα 41. Όπως εύκολα παρατηρείται, οι χρόνοι αυτοί είναι ιδιαίτερα αυξημένοι σε σχέση με τις χαμηλότερες ποιότητες και επηρεάζουν αρνητικά την εμπειρία του χρήστη. Αυτό οφείλεται στον χρόνο που απαιτείται για τη μεταφόρτωση κάθε τμήματος, ο οποίος υπερβαίνει το χρόνο αναπαραγωγής, με συνέπεια καθυστερήσεις ανεξαρτήτως του υφιστάμενου δικτύου. Ωστόσο αξίζει να σημειωθεί ότι και σε αυτή την περίπτωση η μείωση που παρατηρείται στους χρόνους αναμονής είναι μεγαλύτερη με χρήση Δικτύων ICN σε σχέση με τη χρήση των CDN. Επιπλέον οι χρόνοι αναμονής αυξάνονται με την ποιότητα και μειώνονται με την αύξηση του μεγέθους της κρυφής μνήμης. Εντούτοις, η βελτίωση είναι σχετικά μικρή (στην περίπτωση της βέλτιστης ποιότητας υπάρχει μείωση του χρόνου αναμονής κατά την εκκίνηση της τάξης των δύο δευτερολέπτων) και απαιτούνται σημαντικά μεγαλύτερα μεγέθη κρυφής μνήμης προκειμένου ο τελικός χρήστης να παρατηρήσει αισθητή διαφορά.



Σχήμα 40 Χρόνος Αναμονής μέχρι την Εκκίνηση Αναπαραγωγής (5 Mbit/s)



Σχήμα 41 Χρόνος Αναμονής κατά τη διάρκεια της Αναπαραγωγής (5 Mbit/s)

8 Συμπεράσματα και Μελλοντική Εργασία

Στη Διατριβή προτείνεται ένα καινοτόμο σύστημα που στοχεύει να αντιμετωπίσει κάποιες από τις προκλήσεις αναφορικά με την παροχή περιεχομένου, και δη του πολυμεσικού, μέσω δικτύων επικοινωνιών. Καθώς η προστασία του διανεμόμενου πολυμεσικού περιεχομένου στα Δίκτυα ICN είναι ανοιχτό θέμα, προτείνεται η χρήση Κρυπτογραφίας ABE για το συγκεκριμένο σκοπό. Μεγάλο βάρος δόθηκε στη ρεαλιστικότητα της προσέγγισης. Υπό το πρίσμα αυτό, παρουσιάστηκε μια αρχιτεκτονική Πολλαπλών Αρχών Πιστοποίησης βάσει Χαρακτηριστικών, η οποία είναι κατάλληλη για πρακτικά συστήματα. Επίσης εξετάστηκε το εξίσου σημαντικό θέμα της ανάκλησης χρήστη και υιοθέτησε η πιο κατάλληλη λύση στο πλαίσιο των Δικτύων ICN. Η προτεινόμενη λύση είναι δομημένη σύμφωνα με τις αρχές της SOA, οι οποίες επιτρέπουν την ομαλή ενσωμάτωση νέων τεχνολογιών σε έναν πάροχο υπηρεσιών OTT.

Αν και ο κύριος στόχος της προτεινόμενης προσέγγισης ήταν η προστασία του πολυμεσικού περιεχομένου στο μελλοντικό διαδίκτυο (το οποίο πιθανώς να διαφέρει ριζικά από το σημερινό), μία σημαντική παράμετρος στο σχεδιασμό της προτεινόμενης αρχιτεκτονικής ήταν η συμβατότητα με τις υπάρχουσες προσπάθειες προτυποποίησης, με επίκεντρο τη διανομή του πολυμεσικού περιεχομένου, κατά κύριο λόγο δηλαδή τις τεχνολογίες Προσαρμοσμένου Ρυθμού Μετάδοσης (Adaptive Bit-Rate - ABR) και Διαχείρισης Ψηφιακών Δικαιωμάτων (DRM). Μεγάλη προσπάθεια επικεντρώθηκε στην ενσωμάτωση της Κρυπτογραφίας ABE σε συστήματα DRM, κάνοντας τη μετάβαση από τη χρήση κρυπτοσυστημάτων που βασίζονται σε υποδομές PKI προς αυτά που βασίζονται σε Κρυπτογραφία ABE ομαλή για τους παρόχους υπηρεσιών OTT. Παράλληλα, σύμφωνα με πρόσφατη έρευνα [74], οι τεχνολογίες ABR μπορούν να χρησιμοποιηθούν με υπόβαθρο το CCNx. Ένας πληρεξούσιος κόμβος HTTP μεταφράζει τα HTTP αιτήματα του χρήστη σε μηνύματα Interest, ενώ το σχήμα ονομασίας των τμημάτων του περιεχομένου λαμβάνει υπόψη του το bitrate του κάθε τμήματος.

Οι υφιστάμενες λύσεις DRM, χρησιμοποιούν εν γένει ασύμμετρη κρυπτογραφία για την προστασία των αδειών κατά τη μεταφορά τους —το Marlin DRM χρησιμοποιεί

TLS, ενώ το PlayReady DRM χρησιμοποιεί PKI— η οποία δεν είναι ενδεδειγμένη για την προστασία περιεχομένου σε Δίκτυα ICN, όπως έχει ήδη τονιστεί.

Οι άδειες χρήσης περιέχουν εκτός από το κλειδί που αποκρυπτογραφεί το περιεχόμενο και επιπλέον όρους χρήσης, οι οποίοι συμφωνούνται κατά τη διαδικασία εγγραφής και συνδρομής του χρήστη. Οι όροι αυτοί αφορούν τον αριθμό των επιτρεπόμενων αναπαραγωγών, το δικαίωμα στην αποθήκευση του περιεχομένου, κ.α. Η Κρυπτογραφία ABE δεν μπορεί να ελέγξει τη χρήση του περιεχομένου κατόπιν της αποκρυπτογράφησής του και συνεπώς δεν μπορεί να αντικαταστήσει ένα συνολικό σύστημα DRM. Η πρότασή μας αφορά τη χρήση της Κρυπτογραφίας ABE αντί της ασύμμετρης κρυπτογραφίας για την προστασία των αδειών κατά τη διανομή τους, ιδιαίτερα δε κατά την αποθήκευσή τους σε ενδιάμεσους αποθηκευτικούς κόμβους.

Στην υφιστάμενη διαδικτυακή αρχιτεκτονική, ο πάροχος του περιεχομένου έχει «πλήρη» έλεγχο αναφορικά με την πρόσβαση στο περιεχόμενο που διαθέτει. Στην περίπτωση των Δικτύων ICN, όπου το περιεχόμενο δε λαμβάνεται υποχρεωτικά από την τοποθεσία εκπόρευσής του, αλλά εν δυνάμει και από τους διαδικτυακούς αποθηκευτικούς χώρους, η Κρυπτογραφία ABE μπορεί να χρησιμοποιηθεί για την επιβολή περιορισμένης πρόσβασης. Στα Δίκτυα ICN, οι επιθυμητοί γεωγραφικοί περιορισμοί δεν μπορούν να εφαρμοστούν με βάση τον έλεγχο της διεύθυνσης IP του αιτούντα όπως στην υφιστάμενη υποδομή του Διαδικτύου, δεδομένου ότι πλέον δεν υπάρχει διεύθυνση IP. Επίσης, από τη στιγμή που το περιεχόμενο βρεθεί σε ένα διαδικτυακό αποθηκευτικό χώρο, πρέπει να εξασφαλιστεί το ίδιο από μη επιτρεπόμενη πρόσβαση. Μια επιλογή αποτελεί η κρυπτογράφηση του περιεχομένου βάσει μιας πολιτικής η οποία θα περιλαμβάνει ένα γεωγραφικό χαρακτηριστικό, έτσι ώστε μόνο οι χρήστες που διαθέτουν το απαιτούμενο χαρακτηριστικό να μπορούν να αποκρυπτογραφήσουν το περιεχόμενο. Βέβαια η τοποθεσία του χρήστη που έχει πιστοποιηθεί μία δεδομένη χρονική στιγμή είναι δυναμικό χαρακτηριστικό και γι' αυτό θα πρέπει να συνδυαστεί με συχνούς επανελέγχους και ένα ευέλικτο σύστημα ανάκλησης. Αυτή η προσέγγιση, σε συνδυασμό με τα τείχη προστασίας περιεχομένου (που αποτελούν μέρος της αρχιτεκτονικής του CCNx), τα οποία περιορίζουν το περιεχόμενο εντός των ορίων που έχουν καθοριστεί, μπορούν να περιορίσουν αποτελεσματικά την ανεπιθύμητη πρόσβαση.

Σε σύγκριση με την ασφάλεια που προσφέρεται μέσω των υπηρεσιών προστιθέμενης αξίας των Δικτύων CDN, η προτεινόμενη πρόταση δεν υποστηρίζει την κρυπτογράφηση του περιεχομένου ανά χρήστη —δηλαδή, εν προκειμένω το κλειδί AES που προστατεύει το περιεχόμενο είναι κοινό για όλους τους χρήστες. Τυχόν κρυπτογράφηση ανά χρήστη ακυρώνει την ικανότητα προσωρινής αποθήκευσης στους ενδιάμεσους κόμβους Δικτύων ICN και κατά συνέπεια η επιλογή αυτή δεν προτιμάται.

Η χρήση Κρυπτογραφίας ABE βελτιώνει σημαντικά τη διαχείριση των χρηστών. Συνήθως, οι δυνητικοί τελικοί χρήστες μπορούν να ομαδοποιηθούν σύμφωνα με κάποια κοινά χαρακτηριστικά – ιδιότητες, τα οποία αξιοποιεί η Κρυπτογραφία ABE. Σε συστήματα συνδρομητικής τηλεόρασης, τέτοια χαρακτηριστικά μπορεί να περιλαμβάνουν τη γεωγραφική θέση, την ηλικία, τον τύπο συνδρομής, το είδος του περιεχομένου που ενδιαφέρει το χρήστη, κλπ. Κάθε πάροχος υπηρεσιών OTT δύναται να εγκαταστήσει τη δική του ΑΠΧ και να διαχειρίζεται τα χαρακτηριστικά των συνδρομητών του ή εναλλακτικά μπορεί να καταφύγει στη χρήση εξωτερικών ΑΠΧ.

Η αποτελεσματικότητα των κρυπτοσυστημάτων ABE είναι ένα κρίσιμο ζήτημα, τόσο όσον αφορά το μέγεθος του κρυπτογραφήματος (το οποίο έχει κόστος σε εύρος ζώνης) όσο και τη χρήση των υπολογιστικών πόρων. Στα συστήματα αυτά, υφίσταται μια διελκυστίνδα μεταξύ της εκφραστικότητας (δηλαδή, του πλούτου του τύπου πολιτικής πρόσβασης), των μεγεθών των ιδιωτικών/δημόσιων κλειδιών, και του μεγέθους του κρυπτογραφήματος. Στην Κρυπτογραφία ABE, οι τυπικοί υπολογισμοί περιλαμβάνουν υψώσεις σε εκθέτη και ταιριάσματα-ζεύξεις (pairings). Το κόστος της κρυπτογράφησης δεν αποτελεί καθοριστικό παράγοντα, δεδομένου ότι οι άδειες μπορούν να κρυπτογραφηθούν προκαταβολικά για τη στοχοθετημένη ομάδα χρηστών. Το κόστος αποκρυπτογράφησης είναι πιο σημαντικό, διότι αυτή πραγματοποιείται στις τερματικές συσκευές του χρήστη, οι οποίες συχνά έχουν περιορισμένους υπολογιστικούς πόρους. Ωστόσο, η άδεια αποκρυπτογραφείται πριν από την έναρξη της αναπαραγωγής του περιεχομένου, οπότε δεν επηρεάζει αρνητικά την ποιότητα εμπειρίας του χρήστη (QoE). Το ζήτημα της ταχύτητας αποκρυπτογράφησης αποτελεί αντικείμενο νεότερων μελετών [138]. Επιπλέον, αν η χρήση Κρυπτογραφίας ABE πρόκειται να καθιερωθεί, είναι αναμενόμενη εξέλιξη η δημιουργία εξειδικευμένου υλικού, που θα παρέχει ταχύτερη αποκρυπτογράφηση.

Από την άλλη πλευρά, η εμπειρία του χρήστη είναι συναρτημένη με το διαθέσιμο εύρος ζώνης. Το μέγεθος του κρυπτογραφήματος της Κρυπτογραφίας ABE θα πρέπει να βελτιστοποιηθεί, προκειμένου να μην αναιρεί τα πλεονεκτήματα των Δικτύων ICN. Τα περισσότερα κρυπτοσυστήματα ABE, όπως το αρχικό CP-ABE [84], επάγουν κρυπτοκείμενα, το μέγεθος των οποίων αυξάνεται γραμμικά με τον αριθμό των χαρακτηριστικών. Για τη συγκεκριμένη κατασκευή CP-ABE, η αξιολόγηση δείχνει ότι ο χρόνος αποκρυπτογράφησης είναι μικρότερος από ένα δευτερόλεπτο για πολιτικές πρόσβασης που περιέχουν έως 100 χαρακτηριστικά. Όμως, θα πρέπει να λάβουμε υπόψη ότι, σε ρεαλιστικά συστήματα με μερικές εκατοντάδες χιλιάδες ή ακόμα και εκατομμύρια συνδρομητές (βλ. Netflix), ο αριθμός των χαρακτηριστικών ενός συστήματος μπορεί να είναι μεγάλος, εάν επιθυμούμε λεπτομερή έλεγχο πρόσβασης. Επομένως τμήματα περιεχομένου, το μέγεθος των οποίων αυξάνεται γραμμικά με τον αριθμό των χαρακτηριστικών, είναι ακατάλληλα. Πρόσφατες εργασίες [139], [140] έχουν επιτύχει σταθερό πλεόνασμα στο μέγεθος του κρυπτογραφήματος (δύο στοιχεία διγραμμικής ομάδας που οριοθετούνται από 300 bytes) ανεξαρτήτως του αριθμού των χαρακτηριστικών, ενώ τα ιδιωτικά κλειδιά αυξάνονται γραμμικά ή λογαριθμικά με τον αριθμό των χρηστών. Αυτό επιτυγχάνεται με τον περιορισμό της εκφραστικότητας των πολιτικών πρόσβασης. Στην εργασία [140] οι πολιτικές πρόσβασης περιέχουν αποκλειστικά και μόνο λογικοί τελεστές ΚΑΙ (AND) καθώς και τον τελεστή (*) που υποδηλώνει οποιοδήποτε χαρακτηριστικό. Διάφορες εναλλακτικές λύσεις μπορούν να εφαρμοστούν, προκειμένου να εμπλουτίσουν την εκφραστικότητα, για παράδειγμα η συνένωση αυτοτελών πολιτικών πρόσβασης, ώστε εμμέσως να υλοποιηθούν κατασκευές λογικού ΕΙΤΕ (OR).

Συνοψίζοντας τα συμπεράσματα των προσομοιώσεων είναι σαφές ότι, με βάση τα αποτελέσματα, η προσέγγιση των Δικτύων ICN προσφέρει βελτίωση σε όλα τα υπό εξέταση μεγέθη —διαδικτυακή κίνηση εκτός αυτόνομου συστήματος, χρόνοι αναμονής πριν και κατά τη διάρκεια της αναπαραγωγής του περιεχομένου— προσφέροντας έτσι ένα σημαντικό κίνητρο στους παρόχους υπηρεσιών Διαδικτύου για την υιοθέτησή της, καθώς αφενός θα προσφέρουν υπηρεσίες καλύτερης ποιότητας στους συνδρομητές τους και αφετέρου θα έχουν μικρότερα λειτουργικά κόστη, λόγω εξοικονόμησης δικτυακής κίνησης. Ωστόσο η ενδεχόμενη επιτυχία της προσέγγισης θα εξαρτηθεί σε μεγάλο βαθμό και από άλλους παράγοντες, όπως η ύπαρξη γρηγορότερων και ταυτόχρονα

οικονομικών μνημών, και άλλων τεχνοοικονομικών μεγεθών που σχετίζονται με την γενικότερη κατάσταση του Διαδικτύου, όπως υπογραμμίζεται και στη μελέτη [141].

Από τη Διατριβή προκύπτει ότι η υιοθέτηση του συνδυασμού Δικτύων ICN και Κρυπτογραφίας ABE είναι ευεργετική για κάθε φορέα που εμπλέκεται στη διανομή περιεχομένου μέσω Διαδικτύου. Η δικτυακή κίνηση στον κορμό του Διαδικτύου αναμένεται να μειωθεί, λόγω της αποτελεσματικής χρήσης των κρυφών αποθηκευτικών χώρων, με αποτέλεσμα να εξοικονομείται εύρος ζώνης. Οι ελλείψεις σε εύρος ζώνης θα μειωθούν ακόμη και σε περιπτώσεις υπερβολικά δημοφιλούς περιεχομένου. Επίσης, σε συνδυασμό με τις τρέχουσες προσπάθειες προτυποποίησης, η ζήτηση για ιδιόκτητα επικαλυπτικά δίκτυα θα μειωθεί, και οι πάροχοι υπηρεσιών OTT δε θα εξαρτώνται από τους παρόχους υπηρεσιών Δικτύων CDN για την αποδοτική παροχή περιεχομένου.

Από τη σκοπιά των χρηστών, η προτεινόμενη αρχιτεκτονική βελτιώνει τη συνολική ποιότητα της εμπειρίας τους, καθώς η προσωρινή αποθήκευση δεν περιορίζεται στο περιεχόμενο, που καλύπτεται από συμφωνία. Τέλος, με την προτεινόμενη προσέγγιση, αντιμετωπίζονται οι ανησυχίες των παρόχων περιεχομένου τόσο αναφορικά με την ποιότητα της υπηρεσίας που απολαμβάνουν οι χρήστες όσο και για την ασφάλεια του περιεχομένου τους.

Από οικονομικής απόψεως, η προτεινόμενη αρχιτεκτονική μπορεί επίσης να ενισχύσει τα υπάρχοντα επιχειρηματικά μοντέλα και τα μοντέλα τιμολόγησης. Οι πάροχοι υπηρεσιών OTT θα μπορούσαν να προσφέρουν στον τελικό χρήστη εκπτώσεις για pay-per-view πολυμεσικό περιεχόμενο που παρακολούθησαν άλλοι χρήστες σε μικρή απόσταση και ως εκ τούτου βρίσκεται προσωρινά αποθηκευμένο σε εγγείς διαδικτυακούς κόμβους.

Η προτεινόμενη προσέγγισή —η πρώτη που προτείνει την από κοινού χρήση των Δικτύων ICN και της Κρυπτογραφίας ABE για τη διανομή προστατευόμενου περιεχομένου— παρουσιάζει πολλά πλεονεκτήματα, και δίνει αφορμή για περαιτέρω έρευνα. Στην πραγματικότητα, τα Δίκτυα ICN δεν αποτελούν πανάκεια για τη διανομή περιεχομένου και διάφορα ζητήματα πρέπει να διερευνηθούν περαιτέρω, συμπεριλαμβανομένης της προέλευσης περιεχομένου, της υπογραφής του περιεχομένου, της ιδιωτικότητα της κρυφής μνήμης, καθώς και της ονομασίας. Η Κρυπτογραφία ABE, επίσης, εξελίσσεται και περνάει στην παραγωγή με τη δημιουργία πραγματικών κρυπτοσυστημάτων πέραν των θεωρητικών μοντέλων. Ωστόσο στον πραγματικό κόσμο,

οι εφαρμογές απαιτούν βέλτιση απόδοση και εκφραστικότητα. Αυτά τα θέματα θα είναι τα κομβικά σημεία μελλοντικών ερευνητικών προσπαθειών.

Βιβλιογραφία

[1] Mark Weiser, "The computer for the 21st century", Scientific American, 265(3), pp. 66–75, September 1991.

[2] G. Carofiglio, G. Morabito, L. Muscariello, I. Solis, M. Varvello, From content delivery today to information centric networking, Computer Networks, Volume 57, Issue 16, 13 November 2013, Pages 3116-3127, ISSN 1389-1286, http://dx.doi.org/10.1016/j.comnet.2013.07.002.

[3] Sahai A, Waters B. Fuzzy identity-based encryption. In Proceedings of Eurocrypt 2005. Springer-Verlag: Heidelberg, 2005; 457–473.

[4] Cisco Visual Networking Index: Forecast and Methodology, 2012–2017, White paper, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf

[5] https://twitter.com/NeelieKroesEU/status/328779137206587394

[6] Netflix, http://www.netflix.com

[7] YouTube, http://www.youtube.com/

[8] Schwarz, H.; Marpe, D.; Wiegand, T., "Overview of the Scalable Video Coding Extension of the H.264/AVC Standard," *Circuits and Systems for Video Technology, IEEE Transactions on* , vol.17, no.9, pp.1103,1120, Sept. 2007doi: 10.1109/TCSVT.2007.905532

[9] Sullivan, G.J.; Ohm, J.; Woo-Jin Han; Wiegand, T., "Overview of the High Efficiency Video Coding (HEVC) Standard," *Circuits and Systems for Video Technology, IEEE Transactions on* , vol.22, no.12, pp.1649,1668, Dec. 2012 doi: 10.1109/TCSVT.2012.2221191

[10] Hosseini, M.; Ahmed, D.T.; Shirmohammadi, S.; Georganas, Nicolas D., "A Survey of Application-Layer Multicast Protocols," *Communications Surveys & Tutorials, IEEE* , vol.9, no.3, pp.58,74, Third Quarter 2007 doi: 10.1109/COMST.2007.4317616

[11] BitTorrent, "BitTorrent Home Page," BitTorrent, Inc., 2011. [Online]. Available: http://www.bittorrent.com/

[12] Xinyan Zhang; Jiangchuan Liu; Bo Li; Yum, T.P., "CoolStreaming/DONet: a data-driven overlay network for peer-to-peer live media streaming," *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE* , vol.3, no., pp.2102,2111 vol. 3, 13-17 March 2005, doi: 10.1109/INFCOM.2005.1498486

[13] Open IPTV Forum, "Open IPTV Forum Home Page," Open IPTV Forum e.V., 2011. [Online]. Available: http://www.openiptvforum.org

[14] Ghinea, G.; Thomas, J.P., "Quality of perception: user quality of service in multimedia presentations," *Multimedia, IEEE Transactions on* , vol.7, no.4, pp.786,789, Aug. 2005 doi: 10.1109/TMM.2005.850960

[15] ITU-R Recommendation BS 1534-1: "Method for the Subjective Assessment of Intermediate Quality Level of Coding Systems"

[16] Decode-Encode Language (DEL) IETF. RFC 5 https://tools.ietf.org/html/rfc5

[17] Christos Douligeris, Aikaterini Mitrokotsa, DDoS attacks and defense mechanisms: classification and state-of-the-art, Computer Networks, Volume 44, Issue 5, 5 April 2004, Pages 643-666, ISSN 1389-1286, http://dx.doi.org/10.1016/j.comnet.2003.10.003.

[18] http://www.akamai.com/html/customers/case_study_victoria.html, last accessed 3/5/2013

[19] http://www.akamai.com/ericsson/akamai.html, last accessed 3/5/2013

[20] Lin Guo-Hui, Guoliang Xue, K-center and K-median problems in graded distances, Theoretical Computer Science, Volume 207, Issue 1, 28 October 1998, Pages 181-192, ISSN 0304-3975, http://dx.doi.org/10.1016/S0304-3975(98)00063-2.

[21] http://www.isuppli.com/Media-Research/News/Pages/OTT-Providers-Must-Address-Delivery-Network-Access-to-Remain-Competitive.aspx, last accessed 26 November 2013

[22] http://www.ericsson.com/ourportfolio/telecom-operators/media-delivery-network, last accessed 26 November 2013

[23] http://datatracker.ietf.org/wg/cdni/, last accessed 26 November 2013

[24] Dongyan Xu, Sunil Suresh Kulkarni, Catherine Rosenberg, Heung-Keung Chai, "Analysis of a CDN–P2P hybrid architecture for cost-effective streaming media distribution", Multimedia Systems (2006) 11(4): 383–399

[25] John Buford, Heather Yu, and Eng Keong Lua. 2008. *P2P Networking and Applications*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.

[26] Monteiro, Jânio M., Rui S. Cruz, Charalampos Z. Patrikakis, Nikolaos C. Papaoulakis, Carlos Tavares Calafate and Mário S. Nunes. "Peer-to-Peer Video Streaming." In Multimedia Networking and Coding, ed. Reuben A. Farrugia and Carl J. Debono, 254-313 (2013), doi:10.4018/978-1-4666-2660-7.ch010

[27] PeerCast.org, "PeerCast Home Page," PeerCast.org, 2010. Available: http://www.peercast.org/

[28] SopCast, "SopCast Home Page," SopCast.Com, 2010. Available: http://www.sopcast.org/

[29] PPLive, "PPTV Home Page," PPLive Inc., 2010. Available: http://www.pptv.com/

[30] R. Pantos, HTTP Live Streaming Internet draft. http://tools.ietf.org/html/draft-pantos-http-live-streaming-01, Last accessed: 26 November 2013.

[31] Microsoft Smooth Streaming. http://go.microsoft.com/?linkid=9682896, Last accessed: 26 November 2013.

[32] Adobe HTTP Dynamic Streaming. http://www.adobe.com/products/httpdynamicstreaming/, Last accessed: 26 November 2013.

[33] Microsoft PlayReady. http://www.microsoft.com/playready/, Last accessed: 26 November 2013.

[34] Widevine DRM. http://www.widevine.com/drm.html, Last accessed: 26 November 2013.

[35] OMA Digital Rights Management V2.0. http://technical.openmobilealliance.org/Technical/release_program/drm_v2_0.aspx, Last accessed: 26 November 2013.

[36] Verimatrix Multirights, http://www.verimatrix.com/solutions/verimatrix-multirights

[37] X. Wang, G. Lao, T. DeMartini, H. Reddy, M. Nguyen, E. Valenzeula. "XrML – eXtensible rights Markup Language". Proc. of the 2002 ACM Workshop on XML Security. Fairfax, VA, USA. pp. 71-79, Nov. 22-22, 2000.

[38] X. Wang, T. DeMartini, B. Wragg, M. Paramasivam, C. Barlas. "The MPEG-21 Rights Expression Language and Rights Data Dictionary", IEEE Trans. on Multimedia. 7(3), pp. 408-417, June 2005.

[39] W3C ODRL Community Group, http://www.w3.org/community/odrl/, Last accessed: 30 November 2013.

[40] Akamai SOLA Solutions. http://www.akamai.com/html/solutions/sola-solutions.html, Last accessed: 26 November 2013.

[41] UltraViolet Website. http://www.uvvu.com/, Last accessed: 26 November 2013.

[42] Marlin DRM. http://www.marlin-community.com/technology Last accessed: 26 November 2013.

[43] Dynamic Adaptive Streaming over HTTP (DASH), ISO/IEC 23009. http://standards.iso.org/ittf/PubliclyAvailableStandards/c057623_ISO_IEC_23009-1_2012.zip, Last accessed: 26 November 2013.

[44] ISO Base Media File, ISO/IEC 14496-12 (MPEG-4 Part 12)

[45] International Organization for Standardization (ISO), homepage: http://www.iso.org.

[46] MPEG-2 Transport Stream, ISO/IEC 13818-2

[47] Moving Picture Experts Group (MPEG), homepage: http://mpeg.chiariglione.org/

[48] Jacobson V, Smetters DK, Thornton JD, Plass MF, Briggs NH, Braynard RL. Networking named content. Proceedings of the 5th international conference on Emerging networking experiments and technologies, CoNEXT '09, ACM: New York, NY, USA, 2009; 1–12, doi:10.1145/1658939.1658941.

[49] CCNx, "CCNx", 2011. [Online]. Available: http://www.ccnx.org. Last accessed: 26 November 2013.

[50] 4WARD Project Website. http://www.4ward-project.eu/, Last accessed: 26 November 2013.

[51] Scalable and Adaptive Internet Solutions (SAIL).http://www.sail-project.eu/, Last accessed: 26 November 2013.

[52] Named Data Networking (NDN). http://www.named-data.net/index.html, Last accessed: 26 November 2013.

[53] NSF Announces Future Internet Architecture Awards. http://www.nsf.gov/news/news_summ.jsp?cntn_id=117611, Last accessed: 26 November 2013.

[54] Publish-Subscribe Internet Technology (PURSUIT). http://www.fp7-pursuit.eu/PursuitWeb/ , Last accessed: 26 November 2013.

[55] "COntent Mediator architecture for content-aware nETworks (COMET)." http://www.cometproject.org/, Last accessed: 14 August 2013.

[56] "Content-Oriented Networking: a New Experience for Content Transfer (ANR-CONNECT)."http://www.anr-connect.org/, Last accessed: 14 August 2013.

[57] CONVERGENCE Website. http://www.ict-convergence.eu , Last accessed: 26 November 2013.

[58] "Information-Centric Networking Research Group (ICNRG)." http://irtf.org/icnrg , Last accessed: 26 November 2013.

[59] TRIAD Project, http://gregorio.stanford.edu/triad/ , Last accessed 26 November 2013

[60] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica, "A data-oriented (and beyond) network architecture", SIGCOMM Comput. Commun. Rev. 37, 4 (August 2007), 181-192 doi:10.1145/1282427.1282402.

[61] Dimitrov V, Koptchev V. Psirp project – publish-subscribe internet routing paradigm: new ideas for future internet. Proceedings of the 11th International Conference on Computer Systems and Technologies and Workshop for PhD Students in Computing on International Conference on Computer Systems and Technologies, CompSysTech '10, ACM: New York, NY, USA, 2010; 167–171, doi:10.1145/1839379.1839409.

[62] Ahlgren B, D'Ambrosio M, Marchisio M, Marsh I, Dannewitz C, Ohlman B, Pentikousis K, Strandberg O, Rembarz R, Vercellone V. Design considerations for a network of information. Proceedings of the 2008 ACM CoNEXT Conference,

CoNEXT '08, ACM: New York, NY, USA, 2008; 66:1–66:6, doi:10.1145/1544012.1544078.

[63] Ahlgren, B.; Dannewitz, C.; Imbrenda, C.; Kutscher, D.; Ohlman, B., "A survey of information-centric networking," *Communications Magazine, IEEE* , vol.50, no.7, pp.26,36, July 2012, doi: 10.1109/MCOM.2012.6231276

[64] Diallo M, Fdida S, Sourlas V, Flegkas P, Tassiulas L. Leveraging caching for internet-scale content-based publish/subscribe networks. Communications (ICC), 2011 IEEE International Conference on, June; 1–5, doi:10.1109/icc.2011.5962666.

[65] Muscariello L, Carofiglio G, GalloM. Bandwidth and storage sharing performance in information centric networking. Proceedings of the ACM SIGCOMM workshop on Information-centric networking, ICN '11, ACM: New York, NY, USA, 2011; 26–31, doi: 10.1145/2018584.2018593.

[66] Detti A, Pomposini M, Blefari-Melazzi N, Salsano S. Supporting the web with an information centric network that routes by name. Computer Networks 2012; 56(17):3705 – 3722, doi:10.1016/j.comnet.2012.08.006.

[67] Lioudakis G, Anadiotis A, Mousas A, Patrikakis C, Kaklamani D, Venieris I. Routing in Content-Centric Networks: From Names to Concepts. New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on, May; 1–5, doi:10.1109/NTMS.2012.6208732.

[68] D. Kulinski, and J. Burke, "NDN Video: Live and Prerecorded Streaming over NDN", NDN Technical Report NDN-0007, September, 2012. Lederer, S., Müller, C., Rainer, B., Timmerer, C., Hellwagner, H., "An Experimental Analysis of Dynamic Adaptive Streaming over HTTP in Content Centric Networks", in Proceedings of the IEEE International Conference on Multimedia and Expo 2013, San Jose, USA, July, 2013

[69] "CCNx vlc plugin," part of the CCNx package. [Online]. Available: https://github.com/ProjectCCNx/ccnx/tree/master/apps/vlc Last accessed 26 November 2013

[70] J. Letourneau, "CCNxGST - GStreamer plugin used to transport media traffic over a CCNx network.", Available: https://github.com/johnlet/gstreamer-ccnx Last accessed 26 November 2013

[71] Lederer, S., Müller, C., Rainer, B., Timmerer, C., Hellwagner, H., "An Experimental Analysis of Dynamic Adaptive Streaming over HTTP in Content Centric Networks", in Proceedings of the IEEE International Conference on Multimedia and Expo 2013, San Jose, USA, July, 2013

[72] Liu, Y., Geurts, J., Point, J., Lederer, S., Rainer, B., Mueller, C., Timmerer, C., Hellwagner, H., "Dynamic Adaptive Streaming over CCN: A Caching and Overhead Analysis", in Proceedings of the IEEE international Conference on Communication (ICC) 2013 - Next-Generation Networking Symposium, Budapest, Hungary, June, 2013

[73] Grandl, R., Su, K., Westphal, C., "On the Interaction of Adaptive Video Streaming with Content-Centric Networks", eprint arXiv:1307.0794, July 2013.

[74] Detti A, Pomposini M, Blefari-Melazzi N, Salsano S, Bragagnini A. Offloading cellular networks with information-centric networking: The case of video streaming. World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a, June; 1–3, doi:10.1109/WoWMoM.2012.6263734.

[75] Dan Boneh, Craig Gentry, and Brent Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In CRYPTO '05: Proceedings of the 25th Annual International Cryptology Conference on Advances in Cryptology, pages 258–275. Springer-Verlag, 2005.

[76] Amos Fiat and Moni Naor. Broadcast encryption. In CRYPTO '93: Proceedings of the 13th annual international cryptology conference on Advances in cryptology, pages 480–491, New York, NY, USA, 1994. Springer-Verlag New York, Inc.

[77] Selim G. Akl and Peter D. Taylor. Cryptographic solution to a problem of access control in a hierarchy.ACM Trans. Comput. Syst., 1(3):239–248, 1983.

[78] Mikhail J. Atallah, Marina Blanton, Nelly Fazio, and Keith B. Frikken. Dynamic and efficient key management for access hierarchies. ACM Trans. Inf. Syst. Secur., 12(3):1–43, 2009.

[79] Shamir. Identity Based Cryptosystems and Signature Schemes. In Advances in Cryptology - CRYPTO, volume 196 of LNCS, pages 37-53. Springer, 1984.

[80] D. Boneh, M. Franklin Identity-Based Encryption from the Weil Pairing Proceedings of Crypto 2001, volume 2139 of Lecture Notes in Computer Science, pages 213{229, Springer-Verlag, 2001.

[81] Clifford Cocks, An Identity Based Encryption Scheme Based on Quadratic Residues, Proceedings of the 8th IMA International Conference on Cryptography and Coding, 2001

[82] Waters, B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In Cryptology ePrint Archive: Report 2008/290 (2008)

[83] Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: ACM Conference on Computer and Communications Security, pp. 89–98 (2006)

[84] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy, pp. 321–334 (2007)

[85] Communication Theory of Secrecy Systems, available online at http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf

[86] S. Goldwasser, S. Micali, Probabilistic Encryption, Journal of Computer and System Sciences, 28, pp. 270–299, 1984

[87] Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity-based encryption. In Advances in Cryptology|EUROCRYPT 2004, volume 3027 of LNCS, pages 207-22. Springer-Verlag, 2004.

[88] Ling Cheung and Calvin Newport. 2007. Provably secure ciphertext policy ABE. In Proceedings of the 14th ACM conference on Computer and communications security (CCS '07). ACM, New York, NY, USA, 456-465.

[89] Allison Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. 2010. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption. In *Proceedings of the 29th Annual international conference on Theory and Applications of Cryptographic Techniques* (EUROCRYPT'10), Henri Gilbert (Ed.). Springer-Verlag, Berlin, Heidelberg, 62-91.

[90] Brent Waters. 2009. Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions. In *Proceedings of the 29th Annual International Cryptology*

Conference on Advances in Cryptology (CRYPTO '09), Shai Halevi (Ed.). Springer-Verlag, Berlin, Heidelberg, 619-636.

[91] Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Brent Waters. 2006. Secure attribute-based systems. In Proceedings of the 13th ACM conference on Computer and communications security (CCS '06). ACM, New York, NY, USA, 99-112.

[92] Ostrovsky, R., Sahai, A., Waters, B.: Attribute-based encryption with nonmonotonic access structures. In: ACM Conference on Computer and Communications Security, pp. 195–203 (2007)

[93] Allison B. Lewko, Amit Sahai, Brent Waters: Revocation Systems with Very Small Private Keys. IEEE Symposium on Security and Privacy 2010: 273-285

[94] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation," *Proc. ACM Conf. Computer and Comm. Security*, pp. 417-426, 2008.

[95] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Ciphertext policy attribute based encryption with efficient revocation," Technical Report, University of Waterloo, 2010.

[96] Nuttapong Attrapadung, Hideki Imai: Attribute-Based Encryption Supporting Direct/Indirect Revocation Modes. IMA Int. Conf. 2009: 278-300

[97] Attrapadung, N., Imai, H.: Conjunctive broadcast and attribute-based encryption. In: Boyen, X., Waters, B. (eds.) Pairing 2009. LNCS, vol. 5671, pp. 248–265. Springer, Heidelberg (2009)

[98] Junbeom Hur, Chanil Park, Seong Oun Hwang: Fine-grained user access control in ciphertext-policy attribute-based encryption, Security and Communication Networks, Volume 5, Issue 3, pages 253–261, March 2012

[99] M. Blaze, G. Bleumer, and M. Strauss. Divertible Protocols and Atomic Proxy Cryptography. In Proc. of EUROCRYPT '98, Espoo, Finland, 1998.

[100] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," *Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '10)*, 2010.

[101] Guojun Wang, Qin Liu, Jie Wu, Minyi Guo: Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers. Computers & Security 30(5): 320-331 (2011)

[102] Melissa Chase. 2007. Multi-authority attribute based encryption. In *Proceedings of the 4th conference on Theory of cryptography* (TCC'07), Salil P. Vadhan (Ed.). Springer-Verlag, Berlin, Heidelberg, 515-534.

[103] Melissa Chase and Sherman S.M. Chow. 2009. Improving privacy and security in multi-authority attribute-based encryption. In Proceedings of the 16th ACM conference on Computer and communications security (CCS '09). ACM, New York, NY, USA, 121-130. http://doi.acm.org/10.1145/1653662.1653678

[104] H. Lin, Z. Cao, X. Liang, and J. Shao. Secure threshold multi authority attribute based encryption without a central authority. In INDOCRYPT, pages 426-436, 2008.

[105] Allison Lewko and Brent Waters. 2011. Decentralizing attribute-based encryption. In Proceedings of the 30th Annual international conference on Theory and applications of cryptographic techniques: advances in cryptology (EUROCRYPT'11), Kenneth G. Paterson (Ed.). Springer-Verlag, Berlin, Heidelberg, 568-588.

[106] Dan Boneh and Brent Waters. 2007. Conjunctive, subset, and range queries on encrypted data. In *Proceedings of the 4th conference on Theory of cryptography* (TCC'07), Salil P. Vadhan (Ed.). Springer-Verlag, Berlin, Heidelberg, 535-554.

[107] Jonathan Katz, Amit Sahai, and Brent Waters. 2008. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In Proceedings of the theory and applications of cryptographic techniques 27th annual international conference on Advances in cryptology (EUROCRYPT'08), Nigel Smart (Ed.). Springer-Verlag, Berlin, Heidelberg, 146-162.

[108] Tatsuaki Okamoto and Katsuyuki Takashima. 2012. Adaptively attribute-hiding (hierarchical) inner product encryption. In *Proceedings of the 31st Annual international conference on Theory and Applications of Cryptographic Techniques* (EUROCRYPT'12), David Pointcheval and Thomas Johansson (Eds.). Springer-Verlag, Berlin, Heidelberg, 591-608.

[109] Baden R, Bender A, Spring N, Bhattacharjee B, Starin D. Persona: an online social network with user-defined privacy. In Proceedings of the ACM Sigcomm 2009 Conference on Data Communication, SIGCOMM '09. ACM: New York, NY, USA, 2009; 135–146. DOI:10.1145/1592568.1592585.

[110] Akinyele JA, Pagano MW, Green MD, Lehmann CU, Peterson ZN, Rubin AD. Securing electronic medical records using attribute-based encryption on mobile devices. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, SPSM '11. ACM: New York,NY, USA, 2011; 75–86. DOI: 10.1145/2046614.2046628.

[111] Huang D, Verma M. ASPE: attribute-based secure policy enforcement in vehicular ad hoc networks. Ad Hoc Networks 2009; 7(8): 1526–1535. DOI:10.1016/j.adhoc.2009.04.011. Privacy and Security in Wireless Sensor and Ad Hoc Networks.

[112] Traynor P, Butler K, Enck W, McDaniel P. Realizing massive-scale conditional access systems through attribute-based cryptosystems, In Proceedings of NDSS, 2008. (Available from: http://www.internetsociety.org/sites/default/files/tray.pdf) [11 October 2013].

[113] Adams, Carlisle & Lloyd, Steve (2003). Understanding PKI: concepts, standards, and deployment considerations. Addison-Wesley Professional. pp. 11–15. ISBN 978-0-672-32391-1

[114] National Institute of Standards and Technology, "Advance Encryption Standard (AES)", Federal Information Processing Standard Publication 197, November 2001

[115] Microsoft White Paper: Using Silverlight DRM, Powered by PlayReady, with Windows Media DRM Content. http://download.microsoft.com/download/7/6/D/76D540F7-A008-427C-8AFC-BE9E0C0D8435/Using_Silverlight_with_Windows_Media_DRM-Whitepaper_FINAL.doc

[116] The World Wide Web Consortium (W3C), Web Services Glossary, http://www.w3.org/TR/ws-gloss/#defs

[117] Papazoglou, M.P., "Service-oriented computing: concepts, characteristics and directions," Web Information Systems Engineering, 2003. WISE 2003. Proceedings of the Fourth International Conference on , vol., no., pp.3,12, 10-12 Dec. 2003, doi: 10.1109/WISE.2003.1254461

[118] Papazoglou M. P. and Georgakopoulos D., 2003. Introduction: Service-oriented computing. Commun. ACM 46, 10 (October 2003), 24-28. DOI=10.1145/944217.944233 http://doi.acm.org/10.1145/944217.944233

[119] Curbera, F.; Duftler, M.; Khalaf, R.; Nagy, W.; Mukhi, Nirmal; Weerawarana, S., "Unraveling the Web services web: an introduction to SOAP, WSDL, and UDDI," Internet Computing, IEEE , vol.6, no.2, pp.86,93, March-April 2002, doi: 10.1109/4236.991449

[120] Web Services Business Process Execution Language Version 2.0, http://docs.oasis-open.org/wsbpel/2.0/wsbpel-v2.0.html

[121] Business Process Model and Notation (BPMN) Version 2.0, http://www.omg.org/spec/BPMN/2.0/

[122] Java Business Process Management , http://www.jboss.org/jbpm/

[123] White Paper: SOA for Broadcasters: How modern software systems can serve media businesses, http://www.amwa.tv/downloads/whitepapers/AMWA-WP-SOA_for_broadcasters-web.pdf, Last accessed: 17 December 2013

[124] The World Wide Web Consortium (W3C), SOAP Version 1.2 Part 1, http://www.w3.org/TR/soap12-part1/, Last accessed: 17 December 2013

[125] Paypal Website, https://www.paypal.com, Last accessed: 17 December 2013

[126] Α.-Χ. Γ. Αναδιώτης, "Διαχείριση Περιεχομένου με Χρήση Κατανεμημένου Συστήματος Αρχείων πάνω από Πληροφοριοκεντρικό Δίκτυο" Διδακτορική Διατριβή, Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Εθνικό Μετσόβιο Πολυτεχνείο, 2014.

[127] "PeerSim: A Peer-to-Peer Simulator." http://peersim.sourceforge.net/, Last accessed: 14 December 2013.

[128] A. Montresor and M. Jelasity, "PeerSim: A scalable P2P simulator," in *Proc. of the 9th Int. Conference on Peer-to-Peer (P2P'09)*, 2009.

[129] L. Muscariello, G. Carofiglio, and M. Gallo, "Bandwidth and storage sharing performance in information centric networking," in *Proceedings of the ACM SIGCOMM workshop on Information centric networking*, ICN '11, (New York, NY, USA), pp. 26–31, ACM, 2011.

[130] I.S. Venieris, E.N. Protonotarios, G.I. Stassinopoulos, R Carli, Bridging remote connectionless LAN/MANs through connection oriented ATM networks, Computer Communications, Volume 15, Issue 7, September 1992, Pages 418-428, ISSN 0140-3664, http://dx.doi.org/10.1016/0140-3664(92)90001-U.

[131] Stassinopoulos, G.I.; Venieris, I.S.; Petropoulos, K.P.; Protonotarios, E.N., "Performance evaluation of adaptation functions in the ATM environment," Communications, IEEE Transactions on , vol.42, no.6, pp.2335,2344, Jun 1994, doi: 10.1109/26.293685

[132] T Hossfeld, S Egger, R Schatz, M Fiedler, K Masuch, C Lorentzen, "Initial delay vs. interruptions: between the devil and the deep blue sea", In QoMEX 2012, Yarra Valley, Australia, July 2012.

[133] B. Wang, J. Kurose, P. Shenoy, and D. Towsley, "Multimedia streaming via tcp: An analytic performance study," *ACM Trans. Multimedia Comput. Commun. Appl.*, vol. 4, pp. 16:1–16:22, May 2008.

[134] L. Breslau, P. Cao, L. Fan, G. Phillips, and S. Shenker, "Web caching and zipf-like distributions: evidence and implications," in *INFOCOM '99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 1, pp. 126–134 vol.1, 1999.

[135] Ioannis Psaras, Richard G. Clegg, Raul Landa, Wei Koong Chai, and George Pavlou. 2011. Modelling and evaluation of CCN-caching trees. In Proceedings of the 10th international IFIP TC 6 conference on Networking - Volume Part I (NETWORKING'11), Jordi Domingo-Pascual, Pietro Manzoni, Ana Pont, Sergio Palazzo, and Caterina Scoglio (Eds.), Vol. Part I. Springer-Verlag, Berlin, Heidelberg, 78-91.

[136] R. Serral-Gracià, E. Cerqueira, M. Curado, M. Yannuzzi, E. Monteiro, and X. Masip-Bruin. 2010. An overview of quality of experience measurement challenges for video applications in IP networks. In *Proceedings of the 8th international conference on Wired/Wireless Internet Communications* (WWIC'10), Evgeny Osipov, Andreas Kassler, Thomas Michael Bohnert, and Xavier Masip-Bruin (Eds.). Springer-Verlag, Berlin, Heidelberg, 252-263. DOI=10.1007/978-3-642-13315-2_21 http://dx.doi.org/10.1007/978-3-642-13315-2_21

[137] Conviva 2013 Viewer Experience Report, http://www.conviva.com/reports/Viewer_Experience_Report.pdf, last accessed 04/12/2013

[138] Hohenberger S., Waters B. Attribute-based encryption with fast decryption. Kurosawa, Kaoru (ed.) et al., Public-key cryptography -- PKC 2013. 16th international conference on practice and theory in public-key cryptography, Nara, Japan, February 26--March 1, 2013

[139] Javier Herranz, Fabien Laguillaumie, and Carla Rafols. Constant size ciphertexts in threshold attribute-based encryption. In Public Key Cryptography, pages 19-34, 2010 http://dx.doi.org/10.1007/978-3-642-13013-7_2.

[140] Zhou Z, Huang D. On efficient ciphertext-policy attribute based encryption and broadcast encryption: extended abstract. Proceedings of the 17th ACM conference on Computer and communications security, CCS '10, ACM: New York, NY, USA, 2010; 753–755, doi:10.1145/1866307.1866420.

[141] Diego Perino and Matteo Varvello. 2011. A reality check for content centric networking. In *Proceedings of the ACM SIGCOMM workshop on Information-centric networking* (ICN '11). ACM, New York, NY, USA, 44-49. DOI=10.1145/2018584.2018596 http://doi.acm.org/10.1145/2018584.2018596

Παράρτημα Α' – Δημοσιεύσεις

Διεθνή Περιοδικά

[1] J. Papanis, S. Papapanagiotou, A. Mousas, G. V. Lioudakis, D. I. Kaklamani and I. S. Venieris. "On the Use of Attribute-Based Encryption for Multimedia Content Protection over Information Centric Networks", Transactions on Emerging Telecommunications Technologies. 2013.

[2] A. Mousas, A.-C. Anadiotis, G. V. Lioudakis, J. Papanis, P. Gkonis, D. I. Kaklamani and I. S. Venieris. "On Supporting Secure Information Distribution in Heterogeneous Systems using Standard Technologies", Wireless Personal Communications. 2013.

Πρακτικά Διεθνών Συνεδρίων

[3] E. A. Koutsoloukas, S. H. Kapellaki, N. D. Tselikas, N. Dellas, J. Papanis, G. N. Prezerakos and I. S. Venieris. "An event based communication middleware for personalized service provision: design & evaluation". Proceedings of the Next Generation Networking Middleware (NGNM 2006) Workshop in Networking 2006 Conference. 2006. pp. 14 - 22.

[4] J. Papanis, S. Kapellaki, E. Koutsoloukas, N. Dellas, G. N. Prezerakos and I. S. Venieris. "Facilitating context-awareness through hardware personalization devices: The Simplicity Device". Proceedings of the Second International Workshop MATA. 2005. pp. 252-262

[5] N. B. Melazzi, S. Salsano, G. Bartolomeo, F. Martire, E. Fischer, C. Meyer, C. Niedermeier, R. Seidl, E. Rukzio, E. Koutsoloukas, J. Papanis and I. S. Venieris. "The Simplicity System Architecture". Proceedings of 14th IST Mobile Communications Summit. 2005

[6] E. Koutsoloukas, S. Kapellaki, J. Papanis, N. Dellas, N. Tselikas, G. N. Prezerakos, D. I. Kaklamani and I. S. Venieris. "Specification of context-aware mobile services over a distributed brokerage framework: The ubiquitous Media Streaming example". Proceedings of the International Conference on Software, Telecommunications and Computer Networks (SoftCom) 2004. pp. 26 - 30.

[7] N. Blefari-Melazzi, G. Ceneri, G. Cortese, N. Davies, N. Dellas, A. Friday, J. Hamard, E. Koutsoloukas, C. Niedermeier, C. Noda, J. Papanis, C. Petrioli, E. Rukzio, O. Storz and J. Urban. "The Simplicity Project: easing the burden of using complex and heterogeneous ICT devices and services. Part II: State of the Art of Related Technologies". Proceedings of the 13th IST Mobile & Wireless Communications Summit 2004.

Κεφάλαια Βιβλίων

[8] N. B. Melazzi, G. Bianchi, G. Ceneri, G. Cortese, F. Davide, N. Davies, N. Dellas, E. Fischer, T. Frantti, A. Friday, J. Hamard, M. Helbing, S. Kapellaki, K. Kawamura, W. Kellerer, E. Koutsoloukas, C. Meyer, C. Niedermeier, C. Noda, J. Papanis, C. Petrioli, E. Rukzio, S. Salsano, R. Seidl, O. Storz, J. Urban, I. S. Venieris and R. Walker. "The Simplicity Project: Managing Complexity in a Diverse ICT World". In Ambient Intelligence: The Evolution of Technology, Communication and Cognition Towards the Future of Human-Computer Interaction. G. Riva, F. Vatalaro, F. Davide and M. Alcaniz eds. IOS press. 2005. pp. 179 - 211.