Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
στα Πληροφοριακά Συστήματα

Μία Επισκόπηση Και Ταξινόμηση Τεχνολογιών Ενίσχυσης Της Ιδιωτικότητας Στον Παγκόσμιο Ιστό

Φεβρωνία Βασιλείου

Επιβλέπων Καθηγητής
Στέφανος Γκρίτζαλης

Αύγουστος 2013

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μία Επισκόπηση Και Ταξινόμηση Τεχνολογιών Ενίσχυσης Της Ιδιωτικότητας Στον Παγκόσμιο Ιστό

Φεβρωνία Βασιλείου

Επιβλέπων Καθηγητής
Στέφανος Γκρίτζαλης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Αύγουστος 2013

Περίληψη

Τις τελευταίες δεκαετίες, η εισαγωγή των ηλεκτρονικών υπολογιστών και των άλλων μορφών ηλεκτρονικής επικοινωνίας στην καθημερινή ζωή, έχει αλλάξει δραματικά όχι μόνο την οργάνωση και λειτουργία της οικονομικής δραστηριότητας, αλλά και τον καθημερινό τρόπο επικοινωνίας των ανθρώπων. Η αυξανόμενη χρήση του διαδικτύου αλλά και ο αυξανόμενος αριθμός των παρεχόμενων προς τους χρήστες υπηρεσιών εγείρει ανησυχίες για την ιδιωτικότητα των ατόμων. Σε αυτήν την ανάγκη προστασίας της ιδιωτικότητας των ατόμων ανταποκρίνονται οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας που επιτρέπουν στα άτομα να αποκρύψουν την πραγματική τους ταυτότητα, ελαχιστοποιώντας τις πληροφορίες που συλλέγονται για αυτά.

Η σημαντική ανάπτυξη της ερευνητικής δραστηριότητας σε σχέση με την προστασία της ιδιωτικότητας έχει οδηγήσει στη δημιουργία πληθώρας Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας, οι οποίες διαφοροποιούνται ανάλογα με την αρχιτεκτονική τους αλλά και το είδος της προστασίας την οποία παρέχουν. Σκοπός της παρούσας μεταπτυχιακής διατριβής είναι η παρουσίαση και περιγραφή αφενός μεν των state-of-the-art Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας, δίδοντας έμφαση στα σημεία ευπάθειάς τους, και αφετέρου η συγκριτική τους επισκόπηση σε σχέση με την προστασία που παρέχουν απέναντι σε επιλεγμένες επιθέσεις κατά της ιδιωτικότητας.

Summary

Over recent decades, the introduction of personal computers, as well as of other means of electronic communication, in daily life has changed dramatically not only the organization and function of economic activity, but also the daily communication of people. The increasing use of internet along with the increasing number of services provided to users raises privacy concerns. Privacy Enhancing Technologies constitute the response to this need for privacy protection, allowing users to hide their true identity, minimizing the amount of personal data that are being collected.

The significant development of research activity in relation to privacy protection has led to the creation of a substantial number of Privacy Enhancing Technologies, which are differentiated based on their architecture and the kind of protection they provide. The aim of this dissertation is to present and describe the state-of-the-art Privacy Enhancing Technologies, emphasizing on their vulnerabilities, as well as to provide a comparative overview regarding the protection they provide against selected threats on privacy.

Ευχαριστίες

Η παρούσα μεταπτυχιακή διατριβή εκπονήθηκε στο πλαίσιο του Μεταπτυχιακού Προγράμματος Σπουδών «Πληροφοριακά Συστήματα» του Ανοιχτού Πανεπιστημίου Κύπρου.

Ιδιαίτερες ευχαριστίες αποδίδονται στον Επιβλέποντα Καθηγητή κ. Γκρίτζαλη Στέφανο για την καθοδήγηση που μου παρείχε στην εκπόνηση της μεταπτυχιακής διατριβής μου και για την άψογη συνεργασία που είχαμε.

Ευχαριστώ πολύ τον Δημήτρη Ντόντη για την υπομονή, τη στήριξη και την πολύτιμη συμβολή του.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Η ιδιωτικότητα είναι ένα από τα θεμελιώδη ανθρώπινα δικαιώματα, το οποίο προστατεύεται από Διεθνείς Συμβάσεις, καθώς επίσης και από τα Συντάγματα πολλών χωρών, κατέχοντας κεντρική θέση στο κοινωνικό γίγνεσθαι. Ταυτόχρονα όμως αποτελεί ένα ζήτημα το οποίο έχει προκαλέσει έντονη συζήτηση στους κόλπους των κοινωνικών επιστημόνων και των νομικών τόσο για την οριοθέτησή της όσο και για το περιεχόμενό της. Αυτό γίνεται εύκολα αντιληπτό από το γεγονός ότι δεν υπάρχει κοινά αποδεκτός ορισμός της ιδιωτικότητας. Η δυσκολία αυτή στην ύπαρξη κοινά αποδεκτού ορισμού οφείλεται εν μέρει στο ότι η ιδιωτικότητα είναι μια κοινωνική αξία που αφορά τον καθένα. Ως κοινωνική αξία λοιπόν δεν μπορεί να γίνει κατανοητή εάν δεν ληφθεί υπόψη το ευρύτερο κοινωνικό πλαίσιο μέσα στο οποίο αναδύεται και λαμβάνει περιεχόμενο. Όπως αναφέρει ο Moore «η ανάγκη για ιδιωτικότητα είναι μια κοινωνικά κατασκευασμένη ανάγκη. Χωρίς την κοινωνία, δεν θα υπήρχε η ανάγκη για ιδιωτικότητα» [50]. Υπό αυτή την οπτική, η κοινωνική εξέλιξη συνοδεύεται και από την προσαρμογή του περιεχομένου της έννοιας της ιδιωτικότητας, ανάλογα με τις εκάστοτε ισχύουσες κοινωνικές συνθήκες, πεποιθήσεις αλλά και απαιτήσεις των μελών της κοινωνίας.

1.1 Η Ιδιωτικότητα ως Δικαίωμα

Η ιδιωτικότητα ως θεμελιώδες ανθρώπινο δικαίωμα αναγνωρίστηκε το 1948 στη Διακήρυξη των Ανθρωπίνων Δικαιωμάτων των Ηνωμένων Εθνών [02]. Πράγματι, το άρθρο 12 αναφέρει:

«Κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε προσβολές της τιμής και της υπόληψης του. Καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους».

Επίσης, στην Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου που υπογράφηκε το 1950 στη Ρώμη [25], το άρθρο 8 αναφέρει:

«*α) Κάθε άνθρωπος δικαιούται τον σεβασμό της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του.*

β) Δεν επιτρέπεται να υπάρξει καμία επέμβαση δημόσιας αρχής εν τη ασκήσει αυτού του δικαιώματος εκτός και αν η επέμβαση αυτή προβλέπεται από το νόμο και είναι απαραίτητη σε μια δημοκρατική κοινωνία για την εθνική ασφάλεια, τη δημόσια ασφάλεια ή την οικονομική ευημερία της χώρας, την πρόληψη της αταξίας ή ενός εγκλήματος, την προστασία της υγείας ή της ηθικής, ή την προστασία των δικαιωμάτων και ελευθεριών άλλων».

1.1.1 Εννοιολογικός Προσδιορισμός και Διαστάσεις της Ιδιωτικότητας.

Ο πρώτος ορισμός της ιδιωτικότητας δόθηκε από τους Warren και Brandeis στο άρθρο τους "Το Δικαίωμα στην Ιδιωτικότητα" [53]. Οι δύο Αμερικανοί όρισαν την ιδιωτικότητα ως «το δικαίωμα να είναι κάποιος μόνος». Έκτοτε, διάφοροι είναι οι ορισμοί που έχουν χρησιμοποιηθεί στη διεθνή βιβλιογραφία. Ο πιο ευρέως διαδεδομένος ορισμός της ιδιωτικότητας προέρχεται από τον Westin σύμφωνα με τον οποίον «η ιδιωτικότητα είναι η αξίωση των ατόμων, των ομάδων και των ιδρυμάτων, να αποφασίζουν μόνοι τους για το πότε, πώς και μέχρι ποιο σημείο οι πληροφορίες που αφορούν αυτούς, θα διαβιβάζονται σε άλλους» [54] και αφορά όχι μόνο τα φυσικά αλλά και τα νομικά πρόσωπα (ομάδες και οργανισμούς).

Γενικά, η έννοια της ιδιωτικότητας μπορεί να προσεγγιστεί υπό την οπτική τριών συμπληρωματικών θεωρήσεων [01]:

- *Τη χωρική ιδιωτικότητα*, που αφορά την προστασία της στενής φυσικής περιοχής που περιβάλλει ένα πρόσωπο, δηλαδή οικιακά και άλλα περιβάλλοντα όπως ο εργασιακός ή ο δημόσιος χώρος.

- *Την ιδιωτικότητα του ατόμου*, που αφορά την προστασία ενός προσώπου από την αδικαιολόγητη παρέμβαση, όπως ο σωματικός έλεγχος, η δοκιμή φαρμάκων ή οι πληροφορίες που παραβιάζουν την ηθική αίσθηση του ατόμου.

- *Την πληροφοριακή ιδιωτικότητα*, που αφορά τον έλεγχο του αν και πώς τα προσωπικά δεδομένα μπορούν να συγκεντρωθούν, να αποθηκευτούν, να υποστούν επεξεργασία ή να διαδοθούν επιλεκτικά.

Ένας τρίτος ορισμός που εντοπίζεται στη βιβλιογραφία είναι του Clarke Roger [14], σύμφωνα με τον οποίον: «Ιδιωτικότητα είναι η απαίτηση που έχουν τα άτομα στη διατήρηση ενός «προσωπικού χώρου», ελεύθερου από παρεμβάσεις από άτομα και οργανισμούς» και περιλαμβάνει τις ακόλουθες διαστάσεις:

- *Ιδιωτικότητα του ατόμου*: αφορά στην ακεραιότητα του σώματος του ατόμου. Τα θέματα περιλαμβάνουν την υποχρεωτική ανοσοποίηση, τη μετάγγιση αίματος χωρίς τη συγκατάθεση, την υποχρεωτική παροχή δειγμάτων υγρών του σώματος καθώς επίσης και ιστών του σώματος, και την υποχρεωτική στείρωση.

- *Ιδιωτικότητα της προσωπικής συμπεριφοράς*: αφορά σε όλες τις πτυχές της συμπεριφοράς, αλλά κυρίως σε ευαίσθητα θέματα, όπως οι σεξουαλικές προτιμήσεις και συνήθειες, οι πολιτικές δραστηριότητες και οι θρησκευτικές πρακτικές.

- *Ιδιωτικότητα των προσωπικών επικοινωνιών*: Τα άτομα απαιτούν να επικοινωνούν μεταξύ τους ή με οργανισμούς χωρίς όμως να παρακολουθούνται αυτές οι επικοινωνίες.

- *Ιδιωτικότητα των προσωπικών δεδομένων*: Τα άτομα απαιτούν τα προσωπικά τους δεδομένα να μην είναι αυτόματα διαθέσιμα σε άλλα άτομα και οργανισμούς. Ακόμα όμως και αν τα δεδομένα αυτά βρίσκονται στη διάθεση κάποιου άλλου μέρους, το άτομο θα πρέπει να είναι σε θέση να ελέγχει σημαντικά τόσο τα εν λόγω δεδομένα όσο και τη χρήση τους.

Στο σημείο αυτό θα πρέπει να σημειωθεί ότι οι δύο τελευταίες διαστάσεις έχουν συνδεθεί στενά τα τελευταία χρόνια και ο όρος «πληροφοριακή ιδιωτικότητα» αναφέρεται ακριβώς σε αυτόν

τον συνδυασμό της ιδιωτικότητας των προσωπικών επικοινωνιών και της ιδιωτικότητας των προσωπικών δεδομένων.

1.1.2 Πληροφοριακή Ιδιωτικότητα

Με τον όρο «πληροφοριακή ιδιωτικότητα» νοείται «η απαίτηση ενός ατόμου να έχει έλεγχο ή τουλάχιστον να επηρεάζει σημαντικά το χειρισμό των προσωπικών του δεδομένων» [14]. Ως προσωπικά δεδομένα ορίζεται το σύνολο εκείνων των δεδομένων που συνδέονται ή μπορούν να συνδεθούν με το άτομο, όπως για παράδειγμα τα στοιχεία της ταυτότητάς τους, δεδομένα για τη συμπεριφορά του, κοινωνικά δεδομένα, οικονομικά στοιχεία, κτλ.

Η έννοια της πληροφοριακής ιδιωτικότητας εισήχθη στα μέσα της δεκαετίας του 1960 και συνοδεύεται από την ολοένα αυξανόμενη ανησυχία που σχετίζεται με την ανάπτυξη των δυνατοτήτων των ηλεκτρονικών υπολογιστών και την εφαρμογή τους στην επεξεργασία των προσωπικών δεδομένων. Η αύξηση αυτή βέβαια της δημόσιας ανησυχίας δεν θα πρέπει να θεωρηθεί ως αντίδραση στην τεχνολογία αυτή καθ' εαυτή, αλλά στον τρόπο με τον οποίον η τεχνολογία αυτή χρησιμοποιείται.

Στο πλαίσιο της Ευρωπαϊκής Ένωσης, η προστασία της πληροφοριακής ιδιωτικότητας των ατόμων εκφράζεται μέσα από διαφορετικές Οδηγίες [52]. Ενδεικτικά αναφέρονται οι ακόλουθες:

- Την 95/46/ΕΚ Οδηγία για την Προστασία των Δεδομένων
- Την 99/93/ΕΚ Οδηγία για την Ψηφιακή Υπογραφή
- Την 2002/58/ΕΚ Οδηγία για τις Τηλεπικοινωνίες

Οι Οδηγίες αυτές αναγνωρίζουν σαφώς το δικαίωμα των ατόμων που αφορά στα προσωπικά τους δεδομένα και ταυτόχρονα δημιουργούν υποχρεώσεις όσον αφορά στην επεξεργασία των δεδομένων αυτών από τρίτους. Ειδικότερα, η Οδηγία 95/46/ΕΚ έχει διττό στόχο: αφενός μεν την επίτευξη ενός υψηλού επιπέδου προστασίας των προσωπικών δεδομένων και αφετέρου την ενεργοποίηση της ελεύθερης κυκλοφορίας των δεδομένων εντός της Ευρωπαϊκής Ένωσης.

Ένα στοιχείο το οποίο πρέπει να επισημανθεί είναι ότι η σχετική νομοθεσία επικεντρώνεται κυρίως στην προστασία των προσωπικών δεδομένων και όχι της ιδιωτικότητας των ατόμων με

την ευρύτερη έννοια. Είναι γεγονός ότι αυτή η προσέγγιση είναι πιο ρεαλιστική και συνεπώς πιο εύκολο να παράγει αποτελέσματα, εν αντιθέσει με την προστασία της ιδιωτικότητας που είναι πιο αφηρημένη και συνεπώς πιο προβληματική προσέγγιση ως προς τα αναμενόμενα αποτελέσματα.

1.2 Βασικές Αρχές της Ιδιωτικότητας

Το σύνολο της νομοθεσίας για την προστασία της ιδιωτικότητας απαιτεί την διασφάλιση κάποιων βασικών αρχών ιδιωτικότητας, όταν πρόκειται να γίνει συλλογή ή επεξεργασία προσωπικών δεδομένων. Οι περισσότερες εξ αυτών διατυπώθηκαν στις «Αρχές Ιδιωτικότητας» του ΟΟΣΑ, οι οποίες απετέλεσαν και τη βάση για τις Παγκόσμιες Αρχές Προστασίας των Προσωπικών Δεδομένων (Global Privacy Standards), όπως αυτές διατυπώθηκαν στο «Ψήφισμα της Μαδρίτης» από τη διεθνή διάσκεψη των επιτρόπων προστασίας των δεδομένων και της ιδιωτικής ζωής (Νοέμβριος 2009). Ειδικότερα, η Οδηγία του ΟΟΣΑ αναφέρει τις ακόλουθες αρχές [39]:

1. *Αρχή του περιορισμού της συλλογής προσωπικών δεδομένων:* Θα πρέπει να υπάρχουν όρια στη συλλογή των προσωπικών δεδομένων. Η συλλογή αυτή θα πρέπει να πραγματοποιείται με νόμιμο και δίκαιο τρόπο και, όπου είναι εφικτό, με τη γνώση ή τη συγκατάθεση του ατόμου.

2. *Αρχή της ποιότητας των δεδομένων:* Τα προσωπικά δεδομένα που συλλέγονται θα πρέπει να είναι συναφή με τους σκοπούς για τους οποίους πρόκειται να χρησιμοποιηθούν, και, στο βαθμό που απαιτείται, θα πρέπει να είναι ακριβή, πλήρη και ενημερωμένα.

3. *Αρχή του προσδιορισμού του σκοπού:* Ο σκοπός για τον οποίον συλλέγονται τα προσωπικά δεδομένα θα πρέπει να έχει προσδιοριστεί το αργότερο μέχρι τη στιγμή που θα ξεκινήσει η διαδικασία συλλογής τους και η χρήση τους θα πρέπει να περιορίζεται στην εκπλήρωση του εν λόγω σκοπού.

4. *Αρχή του περιορισμού της χρήσης:* Τα προσωπικά δεδομένα δεν θα πρέπει να αποκαλύπτονται, διατίθενται ή να χρησιμοποιούνται για σκοπούς άλλους από αυτούς που καθορίζονται σύμφωνα με την «Αρχή του προσδιορισμού του σκοπού», εξαιρουμένων των περιπτώσεων όπου αυτό γίνεται με τη συγκατάθεση του ατόμου ή που προβλέπονται από το νόμο.

5. *Αρχή της διασφάλισης της ασφάλειας:* Τα προσωπικά δεδομένα πρέπει να προστατεύονται με ασφαλή τρόπο από κινδύνους όπως είναι η απώλεια ή η μη εξουσιοδοτημένη πρόσβαση, η καταστροφή, η χρήση, η τροποποίηση ή η αποκάλυψη των εν λόγω δεδομένων.

6. *Αρχή της διαφάνειας:* Θα πρέπει να υπάρχει μια γενική πολιτική διαφάνειας σχετικά με τις εξελίξεις, τις πρακτικές και τις πολιτικές σε σχέση με τα προσωπικά δεδομένα. Θα πρέπει να είναι άμεσα διαθέσιμη η απόδειξη της ύπαρξης και της φύσης των προσωπικών δεδομένων, των κύριων σκοπών της χρήσης τους, καθώς και η ταυτότητα και η συνήθης κατοικία του διαχειριστή των δεδομένων.

7. *Αρχή της συμμετοχής του ατόμου:* Το άτομο θα πρέπει να έχει το δικαίωμα να ενημερωθεί από τον διαχειριστή των δεδομένων αφενός μεν για το κατά πόσον αυτός διαθέτει δεδομένα για τον ίδιο και αφετέρου για το τι είδους δεδομένα έχει στην κατοχή του. Ταυτόχρονα, υπογραμμίζεται το δικαίωμα στη διόρθωση ή και τη διαγραφή ανακριβών ή παράνομα αποθηκευμένων δεδομένων.

8. *Αρχή της υπευθυνότητας:* Ο διαχειριστής των δεδομένων θα πρέπει να είναι υπεύθυνος για τη συμμόρφωσή του στις παραπάνω αρχές.

Οι προαναφερθείσες αρχές είναι αποτέλεσμα μιας διεθνούς προσπάθειας και συναίνεσης για την αποτελεσματική προστασία της ιδιωτικότητας, χωρίς ωστόσο να παρεμποδίζεται η ελεύθερη κυκλοφορία των προσωπικών δεδομένων, παρέχοντας το γενικό πλαίσιο που θα πρέπει να διέπει όλα τα μέσα (τεχνικά ή μη) προστασίας της ιδιωτικότητας.

Κεφάλαιο 2
Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας

Η κοινωνία έχει αλλάξει δραματικά τις τελευταίες δεκαετίες. Η εισαγωγή των ηλεκτρονικών υπολογιστών και των άλλων μορφών ηλεκτρονικής επικοινωνίας στην καθημερινή ζωή, έχει μεταβάλλει όχι μόνο την οργάνωση και λειτουργία της οικονομικής δραστηριότητας, αλλά και τον καθημερινό τρόπο επικοινωνίας των ανθρώπων. Έρευνες έχουν δείξει ότι η χρήση του διαδικτύου και των υπηρεσιών του έχει αυξηθεί ραγδαία τα τελευταία χρόνια. Σύμφωνα με στοιχεία του Global Finance [29], το 2011 ο αριθμός των ατόμων που είχαν πρόσβαση στο διαδίκτυο άγγιζε τα 2,3 δις και μάλιστα σε ορισμένες ευρωπαϊκές χώρες το ποσοστό των χρηστών ξεπέρναγε το 90% του συνολικού πληθυσμού των χωρών αυτών.

Με την ευρεία χρήση των ηλεκτρονικών υπολογιστών και των συνεχώς αυξανόμενων, πιο περίπλοκων και διασυνδεμένων υπηρεσιών που βρίσκονται στη διάθεση των χρηστών, αυξάνεται ο κίνδυνος παραβίασης της ιδιωτικότητας των ατόμων. Πράγματι, ολοένα και περισσότερα προσωπικά δεδομένα, σχετικά με την προσωπικότητα και τα ενδιαφέροντά τους, αποθηκεύονται σε διάφορους ιστότοπους, επιτείνοντας την ανησυχία των χρηστών για την ασφάλεια των προσωπικών τους δεδομένων, στοιχείο το οποίο αποδεικνύεται άλλωστε και από τα συμπεράσματα πολλών ερευνών. Ενδεικτικά αναφέρονται οι εξής έρευνες:

α) Η ειδική έκδοση του Ευρωβαρόμετρου για την στάση των Ευρωπαίων απέναντι στην προστασία των προσωπικών δεδομένων και την ηλεκτρονική ταυτότητα [24], υπογραμμίζει τα ακόλουθα στοιχεία:

- Το 74% των Ευρωπαίων θεωρεί ότι η αποκάλυψη προσωπικών πληροφοριών αυξάνεται συνεχώς.
- Προσωπικές πληροφορίες θεωρούνται πρωτίστως τα οικονομικά στοιχεία (75%), οι ιατρικές πληροφορίες (74%), καθώς και ο αριθμός της ταυτότητας ή των καρτών και το διαβατήριο (73%).
- Το 43% των χρηστών του διαδικτύου θεωρεί ότι τους έχουν ζητηθεί περισσότερες προσωπικές πληροφορίες από ότι χρειάζεται για να αποκτήσουν πρόσβαση σε μια ηλεκτρονική υπηρεσία.
- Το 70% των Ευρωπαίων ανησυχεί ότι τα προσωπικά τους δεδομένα μπορούν να χρησιμοποιηθούν για σκοπό άλλον από εκείνον για τον οποίο συλλέχθηκαν.
- Η πλειοψηφία των Ευρωπαίων ανησυχεί για την καταγραφή της συμπεριφοράς τους μέσω πιστωτικών καρτών (54%), κινητών τηλεφώνων (49%) ή πρόσβασης στο διαδίκτυο μέσω του κινητού (40%).
- Για να προστατεύσουν την ταυτότητά τους στην καθημερινή ζωή, το 62% των Ευρωπαίων παρέχει την ελάχιστη απαιτούμενη πληροφορία.
- Σχεδόν 6 στους 10 χρήστες του διαδικτύου συνήθως διαβάζουν τις δηλώσεις απορρήτου (58%) και η πλειοψηφία εξ αυτών προσαρμόζει τη συμπεριφορά του στο διαδίκτυο (70%).

β) Έρευνα του Centre for Internet Society (CIS) για τη στάση των Αυστραλών απέναντι στην ιδιωτικότητα στο διαδικτυακό περιβάλλον [09] έδειξε ότι ο τρόπος με τον οποίον τα άτομα αντιλαμβάνονται την ιδιωτικότητα επηρεάζει καθοριστικά τις διαδικτυακές τους δραστηριότητες και ιδιαίτερα την απόφασή τους να αγοράσουν ή να πουλήσουν αγαθά και υπηρεσίες ηλεκτρονικά. Πιο συγκεκριμένα:

- Το 85% των Αυστραλών χρηστών του διαδικτύου θεωρεί ότι η ενημέρωση για τις παραβιάσεις των προσωπικών δεδομένων θα πρέπει να είναι υποχρεωτική για τις επιχειρήσεις.

- Τα θέματα για τα οποία ανησυχούν περισσότερο είναι η κλοπή της ταυτότητάς τους (86%) και η απώλεια οικονομικών τους στοιχείων (83%).

- Ο οικονομικός τομέας είναι ο πιο έμπιστος όσον αφορά την προστασία της ιδιωτικότητας (42%).

- Τα μέσα κοινωνικής δικτύωσης είναι ο λιγότερο έμπιστος τομέας όσον αφορά την προστασία της ιδιωτικότητας (1%). Μάλιστα, το 61% των ερωτώμενων χαρακτήρισε τα μέσα κοινωνικής δικτύωσης ως τον τομέα με τις χειρότερες πρακτικές προστασίας της ιδιωτικότητας.

Αποτέλεσμα αυτής της ανησυχίας είναι η γενικευμένη επιθυμία των χρηστών για προστασία των προσωπικών τους δεδομένων, απαιτώντας συνεχώς πιο εξελιγμένους τρόπους προστασίας τους σε επίπεδο νομοθεσίας, πολιτικών, πρακτικών και εφαρμογών. Η ανάγκη αυτή οδήγησε στην ανάπτυξη των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας.

Η έρευνα για τις Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας ξεκίνησε από τον David Chaum το 1981, ο οποίος ανάπτυξε το «mix network», ένα μέσο για την επίτευξη ανώνυμης και μη παρατηρήσιμης επικοινωνίας μέσω δικτύου. Στην εν λόγω έρευνα στηρίζονται ορισμένα από τα ανώνυμα συστήματα επικοινωνίας και αλληλογραφίας που χρησιμοποιούνται μέχρι και σήμερα. Αποτέλεσμα της ευρύτερης ερευνητικής δραστηριότητας ήταν η δημιουργία ενός ικανού αριθμού τεχνολογιών που μπορούν να ενσωματωθούν στις διαδικτυακές υπηρεσίες και να παρέχουν προστασία των προσωπικών δεδομένων των χρηστών.

2.1 Ορισμός των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας

Ο όρος «Τεχνολογία Ενίσχυσης της Ιδιωτικότητας» (Privacy Enhancing Technologies - PET) εμφανίστηκε το 1995 από την ολλανδική Αρχή Προστασίας Δεδομένων. Σε διαβούλευση στο ολλανδικό Κοινοβούλιο για το Νόμο περί Προστασίας των Δεδομένων, ο Υπουργός Δικαιοσύνης διευκρίνισε ότι τεχνικά μέσα πρέπει να χρησιμοποιηθούν για την προστασία της ιδιωτικότητας,

υπογραμμίζοντας ότι οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας μπορούν να αποβούν εξαιρετικά χρήσιμες στη διασφάλιση τόσο της σωστής χρήσης των προσωπικών δεδομένων όσο και του σεβασμού των αρχών της ιδιωτικότητας. Ταυτόχρονα, σύμφωνα με την Ευρωπαϊκή Επιτροπή, η χρήση των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας μπορεί να συμβάλλει στο σχεδιασμό συστημάτων και υπηρεσιών που θα ελαχιστοποιούν τόσο τη συλλογή όσο και τη χρήση των προσωπικών δεδομένων, ενώ παράλληλα θα διευκολύνουν και τη συμμόρφωση με τις αρχές προσωπικών δεδομένων, καθιστώντας την παραβίαση των κανόνων προστασίας των προσωπικών δεδομένων πιο δύσκολη.

Παρά την ευρεία χρήση όμως του όρου «Τεχνολογία Ενίσχυσης της Ιδιωτικότητας», δεν υπάρχει κοινά αποδεκτός ορισμός. Εκείνο που πρέπει να σημειωθεί ωστόσο είναι ότι παρά τις διαφορές, οι περισσότεροι εμπεριέχουν παρόμοιες αρχές, οι οποίες συνοψίζονται ως εξής:

Οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας: α) μειώνουν ή εξαλείφουν τον κίνδυνο παράβασης των αρχών της ιδιωτικότητας και της νομοθεσίας, β) ελαχιστοποιούν την ποσότητα των δεδομένων που κατέχει κάποιος για τα άτομα και γ) ενδυναμώνουν τα άτομα στη διατήρηση του ελέγχου των προσωπικών τους δεδομένων ανά πάσα στιγμή.

Για το σκοπό της μεταπτυχιακής διατριβής θα υιοθετηθεί ο ορισμός της Ευρωπαϊκής Επιτροπής [35], σύμφωνα με τον οποίον οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας είναι «ένα συνεκτικό σύστημα μέτρων Τεχνολογιών των Πληροφοριών και Τεχνολογιών το οποίο προστατεύει την ιδιωτικότητα εξαλείφοντας ή μειώνοντας τα προσωπικά δεδομένα ή αποτρέποντας την μη απαραίτητη ή/και ανεπιθύμητη επεξεργασία των προσωπικών δεδομένων, χωρίς ωστόσο να χάνεται η λειτουργικότητα του συστήματος πληροφοριών».

2.2 Βασικά Χαρακτηριστικά και Κατηγοριοποίηση των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας

Από την πρώτη εμφάνιση των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας έως και σήμερα έχει υπάρξει μια πληθώρα ερευνητικών άρθρων και προτάσεων για το ποια πρέπει να είναι τα χαρακτηριστικά των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας. Ο Goldeberg [35] παραθέτει μια σειρά από γενικές ιδιότητες που απαιτούνται για να είναι χρήσιμες οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας. Ειδικότερα, αναφέρει τις ακόλουθες:

- *Ευχρηστία*: οι χρήστες πρέπει να είναι σε θέση να χρησιμοποιήσουν μια Τεχνολογία Ενίσχυσης της Ιδιωτικότητας δεδομένων των δυσκολιών και του κόστους.

- *Ικανότητα ανάπτυξης*: οι καθημερινοί χρήστες θα πρέπει να είναι σε θέση να αποκτήσουν και να επωφεληθούν από μια Τεχνολογία Ενίσχυσης της Ιδιωτικότητας, απαιτώντας συμβατότητα με τα προτιμώμενα λειτουργικά συστήματα, τα προγράμματα περιήγησης στο διαδίκτυο, κτλ.

- *Αποτελεσματικότητα*: οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας πρέπει να λειτουργούν και να παρέχουν τα οφέλη τα οποία υπόσχονται.

- *Ευρωστία*: ένα χρήσιμο σύστημα πρέπει να διατηρεί όσο το δυνατόν περισσότερη προστασία.

Ο βασικός σκοπός ωστόσο των περισσότερων Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας είναι να διασφαλίσουν ένα ή περισσότερα από τα ακόλουθα κύρια χαρακτηριστικά της ιδιωτικότητας [18]:

- *Ανωνυμία (anonymity):* Πάντα πρέπει να υπάρχει ένα κατάλληλο σύνολο υποκειμένων με δυνητικά τα ίδια χαρακτηριστικά για να είναι εφικτή η ανωνυμία ενός υποκειμένου. Η ανωνυμία συνεπώς ορίζεται ως η κατάσταση του να μην είναι αναγνωρίσιμο μέσα σε ένα σύνολο υποκειμένων το σύνολο ανωνυμίας. Το σύνολο ανωνυμίας είναι ένα σύνολο όλων των πιθανών υποκειμένων. Σύμφωνα με τον ορισμό της ανωνυμίας του Pfitzmann-Hansen, τα υποκείμενα που μπορεί να σχετίζονται με μια ανώνυμη συναλλαγή συνιστούν το σύνολο ανωνυμίας για τη συγκεκριμένη συναλλαγή. Ένα υποκείμενο διεκπεραιώνει τη συναλλαγή ανώνυμα, αν δεν μπορεί να διακριθεί από έναν αντίπαλο από άλλα υποκείμενα.

- *Μη συνδεσιμότητα (unlinkability):* Μη συνδεσιμότητα δύο ή περισσοτέρων αντικειμένων (π.χ. υποκειμένων, μηνυμάτων, γεγονότων, δράσεων κτλ.) σημαίνει ότι μέσα στο σύστημα, αυτά τα αντικείμενα δεν μπορούν να συνδεθούν περισσότερο ή λιγότερο σε σχέση με την εκ των προτέρων γνώση.

- *Μη παρατηρησιμότητα (unobservability):* είναι η κατάσταση κατά την οποία τα αντικείμενα ενδιαφέροντος είναι δυσδιάκριτα από κάθε αντικείμενο ενδιαφέροντος του ίδιου τύπου. Αυτό σημαίνει ότι τα μηνύματα δεν είναι διακριτά από τον τυχαίο θόρυβο.

- *Ψευδωνυμία (pseudonymity):* είναι η κατάσταση όπου χρησιμοποιείται ένα ψευδώνυμο ως αναγνωριστικό. Υποθέτουμε ότι κάθε ψευδώνυμο αναφέρεται σε ακριβώς έναν κάτοχο, δεν αλλοιώνεται στο χρόνο και δεν μεταφέρεται σε άλλα υποκείμενα.

2.2.1. Κατηγοριοποίηση των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας

Η ραγδαία αύξηση του αριθμού των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας οδήγησε στην προσπάθεια ταξινόμησής τους. Είναι γεγονός όμως ότι παρά την πληθώρα ταξινομήσεων καμιά δεν έχει τύχει κοινής αποδοχής, αντικατοπτρίζοντας τις διαφορές στις παραδοχές σχετικά με την έννοια και τον ορισμό της ιδιωτικότητας, καθώς επίσης και τον σκοπό της ταξινόμησης. Δύο από τις πιο ενδεικτικές ταξινομήσεις είναι οι εξής: α) η ταξινόμηση που χρησιμοποιείται στο Ευρωπαϊκό Πρόγραμμα για το Μέλλον της Ταυτότητας στην Κοινωνία της Πληροφορίας (Future of Identity in the Information Society – FIDIS) και β) η ταξινόμηση του METAgroup.

2.2.1.1 Ταξινόμηση FIDIS

Η κατηγοριοποίηση που παρουσιάζεται στο Ευρωπαϊκό Πρόγραμμα για το Μέλλον της Ταυτότητας στην Κοινωνία της Πληροφορίας (FIDIS) διακρίνει δύο κατηγορίες Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας [18]: α) τα εργαλεία αδιαφάνειας (opacity tools) και β) τα εργαλεία διαφάνειας (transparency tools).

Α) Η πρώτη κατηγορία αφορά σε εργαλεία που αποκρύπτουν την ταυτότητα ενός ατόμου ή τη σχέση του με τα δεδομένα, καθώς αυτά υπόκεινται επεξεργασία από κάποιον άλλον. Τεχνικά παραδείγματα αποτελούν το MixMaster (παρέχει ανώνυμη αλληλογραφία), το TOR (ανώνυμη περιήγηση στο διαδίκτυο) και τα ψευδώνυμα. Μη τεχνικά παραδείγματα είναι η ψευδώνυμη πρόσβαση σε διαδικτυακές υπηρεσίες και η μυστικότητα των εκλογών.

Β) Η δεύτερη κατηγορία αφορά σε εργαλεία που βοηθάνε το άτομο να δει τι προσωπικά δεδομένα υφίστανται επεξεργασία, με ποιον τρόπο και ποιος τα επεξεργάζεται. Τεχνικά παραδείγματα αποτελούν τα αρχεία log και οι ελεγκτικοί παράγοντες. Μη τεχνικά παραδείγματα είναι τα νομικά δικαιώματα για την πληροφόρηση σχετικά με τα προσωπικά δεδομένα του κάθε ατόμου που υφίστανται επεξεργασία και οι έλεγχοι της ιδιωτικότητας (privacy audits).

2.2.1.2 Ταξινόμηση METAgroup

Η κατηγοριοποίηση που παρουσιάζεται στην Έκθεση του METAgroup «Privacy Enhancing Technologies» στηρίζεται στην αρχή της λειτουργίας την οποία επιτελούν οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας και διακρίνει δύο μεγάλες κατηγορίες [37]:

Α) **Τεχνολογίες Προστασίας της Ιδιωτικότητας**: η κατηγορία αυτή περιλαμβάνει εργαλεία και τεχνολογίες οι οποίες συμμετέχουν ενεργά στην προστασία της ιδιωτικότητας (π.χ. με την απόκρυψη προσωπικών πληροφοριών ή με την εξάλειψη της ανάγκης για αναγνώριση του προσώπου). Η κατηγορία αυτή διακρίνεται στις ακόλουθες επιμέρους υποομάδες:

- *Εργαλεία για ψευδωνυμία*: Ο καλύτερος τρόπος για την προστασία των προσωπικών δεδομένων στις ηλεκτρονικές υπηρεσίες είναι να προβλεφθεί η απαίτηση της ιδιωτικότητας στο βασικό σχεδιασμό της υπηρεσίας και στην αρχιτεκτονική των συστημάτων που κατασκευάζονται για να την υποστηρίξουν. Η πιο συνήθης πρακτική είναι η αντικατάσταση του ονόματος του χρήστη με ένα ουδέτερο αναγνωριστικό. Σε περιπτώσεις όπου η αρχή της ιδιωτικότητας δεν έχει προβλεφθεί στον αρχικό σχεδιασμό μιας υπηρεσίας ή ενός συστήματος είναι εφικτή η ενσωμάτωση add on ή middleware για το διαχωρισμό των ευαίσθητων δεδομένων στις συναλλαγές.

- *Προϊόντα και υπηρεσίες ανωνυμίας*: Η παροχή ανώνυμης πρόσβασης είναι η μια από τις βασικές λειτουργίες των συστημάτων και υπηρεσιών ενίσχυσης της ιδιωτικότητας. Οι εν λόγω υπηρεσίες, που παρέχονται κυρίως στο διαδίκτυο, επιτρέπουν στα άτομα να στέλνουν μηνύματα και να αλληλεπιδρούν με ηλεκτρονικές υπηρεσίες χωρίς να αποκαλύπτουν την πραγματική τους ταυτότητα.

- *Εργαλεία κρυπτογράφησης*: Η χρήση τεχνικών κρυπτογράφησης για τη διασφάλιση του απορρήτου των πληροφοριών είναι ένα κεντρικό μέρος των εργαλείων ενίσχυσης της ιδιωτικότητας. Χρησιμοποιώντας τεχνικές κρυπτογράφησης, τα ευαίσθητα δεδομένα των συναλλαγών μπορούν να περάσουν μέσα από ανασφαλή δίκτυα και διακομιστές.

- *Φίλτρα και blockers*: Αυτή είναι μια κατηγορία εργαλείων που επικεντρώνεται στην εξάλειψη των αρνητικών επιπτώσεων της απώλειας της ιδιωτικότητας, προστατεύοντας τα στοχοθετημένα άτομα από την ανεπιθύμητη αλληλογραφία.

- *Track και evidence erasers*: Κατά την επικοινωνία ή τη χρήση υπηρεσιών στο διαδίκτυο ο χρήστης αφήνει ίχνη της δραστηριότητάς του κατά μήκος της διαδρομής της κίνησης

των δεδομένων. Μέρος αυτής της δραστηριότητας μπορεί να διαγραφεί με τη χρήση διαφόρων βοηθητικών προγραμμάτων. Αν και αυτά τα προγράμματα δεν συνιστούν Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας, μπορούν να αποτελέσουν μέρος ενός πλαισίου των προϊόντων και υπηρεσιών που υποστηρίζουν την ιδιωτικότητα.

Β) **Τεχνολογίες Διαχείρισης της Ιδιωτικότητας**: η κατηγορία αυτή περιλαμβάνει εργαλεία και τεχνολογίες που υποστηρίζουν τη διαχείριση των κανόνων της ιδιωτικότητας και διακρίνεται στις επιμέρους υποομάδες:

- *Ενημερωτικά εργαλεία*: Η ευαισθητοποίηση, η δημιουργία πολιτικών και ο έλεγχος της συμμόρφωσης δεν είναι ενεργές Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας, αλλά θεωρούνται ως αναπόσπαστο κομμάτι του πλαισίου των Τεχνολογιών αυτών. Για το σκοπό αυτό υπάρχει μια σειρά από εργαλεία τα οποία διευκολύνουν τη δημιουργία και τη διαχείριση των πολιτικών της ιδιωτικότητας και επαληθεύουν ότι οι υπηρεσίες, όπως οι ιστοσελίδες, συμμορφώνονται με τους ισχύοντες κανόνες.

- *Εργαλεία διαχείρισης*: Τόσο γενικά όσο και ειδικά εργαλεία υποστηρίζουν την διαχείριση της Ιδιωτικότητας από τις επιχειρήσεις. Τα γενικά εργαλεία έχουν μια σημαντική λειτουργική επικάλυψη με άλλες λειτουργίες ασφαλείας. Τα ειδικά εργαλεία για τη διαχείριση των θεμάτων ιδιωτικότητας προσφέρονται ως add-on ενότητες σε γενικές σουίτες διαχείρισης του συστήματος.

2.3 Απειλές κατά της Ιδιωτικότητας

Είναι γεγονός ότι η αυξανόμενη χρήση των ηλεκτρονικών υπηρεσιών, όπως αναφέρθηκε και στην αρχή του παρόντος κεφαλαίου, εγείρει σημαντικά ζητήματα ως προς την ασφάλεια των προσωπικών δεδομένων των χρηστών. Οι κυριότερες απειλές κατά της πληροφοριακής ιδιωτικότητας μπορούν να κατηγοριοποιηθούν ως εξής [37]: α) απώλεια της εμπιστευτικότητας, β) κλοπή της ταυτότητας του χρήστη και γ) ανεπιθύμητα μηνύματα. Αυτές τις απειλές επιχειρούν να αντιμετωπίσουν οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας, διασφαλίζοντας το απόρρητο των προσωπικών δεδομένων. Παρ' όλα αυτά, η ανάπτυξη νέων τεχνολογιών για την προστασία της ιδιωτικότητας συνοδεύεται από την ταυτόχρονη ανάπτυξη ολοένα και πιο εξελιγμένων επιθέσεων κατά αυτών των τεχνολογιών. Στην παρούσα μεταπτυχιακή διατριβή, η ανάλυση θα επικεντρωθεί στις ακόλουθες απειλές:

1. *Επίθεση Ανάλυσης Κίνησης*

Η εν λόγω επίθεση αφορά στην παρακολούθηση και επεξεργασία μηνυμάτων με στόχο την εξαγωγή πληροφοριών από πρότυπα επικοινωνιών. Γενικά, όσο μεγαλύτερος είναι ο αριθμός των μηνυμάτων που παρακολουθούνται τόσο περισσότερα μπορούν να συναχθούν από την κίνηση [57]. Η επίθεση αυτή μπορεί να πραγματοποιηθεί είτε παθητικά (απλώς παρατηρώντας) είτε ενεργά (προκαλώντας καταστάσεις όπου η ανάλυση κίνησης γίνεται πιο εύκολη).

2. *Ωτακουστής*

Η επίθεση του ωτακουστή αφορά στη διαδικασία συλλογής πληροφοριών από ένα δίκτυο παρακολουθώντας την κίνηση των δεδομένων (τα πακέτα που στέλνονται ή λαμβάνονται). Οι πληροφορίες των πακέτων μένουν ανέπαφες, ωστόσο η ιδιωτικότητα παραβιάζεται. Σκοπός του ωτακουστή είναι η αποκάλυψη του εκκινητή ή του παραλήπτη κάθε συνόδου.

3. *Επίθεση Χρονισμού*

Η επίθεση χρονισμού έχει ως στόχο να αποκαλύψει τα δύο μέρη μιας επικοινωνίας. Για να το πετύχει αυτό ο επιτιθέμενος αναλύει τα περιοδικά μεταδιδόμενα πακέτα (μετρώντας την καθυστέρηση της ανταπόκρισης των πακέτων) και πραγματοποιεί χρονικούς συσχετισμούς προκειμένου να αποκαλύψει την πηγή των πακέτων [01]. Επίσης παρατηρεί τη διάρκεια μιας συγκεκριμένης επικοινωνίας συνδέοντας τα πιθανά τελικά σημεία και περιμένει για κάποιο συσχετισμό με την δημιουργία ή την αποσύνδεση κάποιου κόμβου σε κάθε πιθανό τελικό σημείο.

4. *Επίθεση Κωδικοποίησης Μηνύματος*

Εάν τα μηνύματα δεν αλλάξουν την κωδικοποίησή τους κατά τη διάρκεια της μετάδοσής τους, τότε αυτά μπορούν να συνδεθούν ή να ιχνηλατηθούν. Πράγματι, τόσο το περιεχόμενο όσο και το μέγεθος ενός μηνύματος που μεταδίδεται μπορεί να ιχνηλατηθεί, επιτρέποντας στον επιτιθέμενο να συνδέσει συγκεκριμένα κανάλια, ακολουθίες και συνόδους με συγκεκριμένα ζεύγη αποστολέων - παραληπτών.

5. *Επίθεση Traceback Παθητική/Ενεργή*

Σε μία επίθεση traceback [49], ένας επιτιθέμενος ξεκινώντας από ένα γνωστό ανταποκριτή ιχνηλατεί το μονοπάτι πίσω στον εκκινητή κατά μήκος του μονοπατιού προώθησης ή του

αντίστροφου μονοπατιού. Υπάρχουν δυο είδη επιθέσεων traceback: οι ενεργές και οι παθητικές. Στην πρώτη περίπτωση, ο επιτιθέμενος αποκτά τον έλεγχο του δικτύου και μπορεί να ανιχνεύσει την προέλευση των μεταδιδόμενων πακέτων. Στη δεύτερη περίπτωση, ο επιτιθέμενος μπορεί να συγκεντρώσει πληροφορίες σχετικά με τα χαρακτηριστικά δρομολόγησης των μελών που συμμετέχουν στο πρωτόκολλο και να ιχνηλατήσει τη σύνδεση εντοπίζοντας τον εκκινητή του μηνύματος.

6. *Επίθεση Σήμανσης*

Η επίθεση σήμανσης επιτρέπει στον επιτιθέμενο να αναγνωρίσει την κίνηση σε μια μεταγενέστερη χρονική στιγμή μέσω της τροποποίησής της.

7. *Επίθεση Διασταύρωσης*

Ο αποτελεσματικότερος τρόπος για τον εντοπισμό της ταυτότητας ενός κόμβου σε ένα δίκτυο είναι η παρατήρηση της συμπεριφορά του για μεγάλο χρονικό διάστημα. Σε γενικές γραμμές, ο συγκεκριμένος κόμβος θα εμφανίσει τυπικές online/offline συνόδους, θα χρησιμοποιήσει παρόμοιους πόρους και συνήθως θα απευθύνει ερωτήματα στις ίδιες ιστοσελίδες σε διαφορετικές συνόδους. Έτσι, παρατηρώντας ένα σύνολο ενεργών χρηστών σε διαφορετικές χρονικές στιγμές μπορεί να παρέχει στον εισβολέα πληροφορίες όπως ποιοι χρήστες είναι ενεργοί σε μια συγκεκριμένη χρονική στιγμή και ποιοι χρήστες επικοινωνούν μεταξύ τους.

8. *Κακόβουλοι Κόμβοι*

Κακόβουλος θεωρείται εκείνος ο κόμβος του δικτύου, ο οποίος επικοινωνεί με άλλους με σκοπό την αποκάλυψη της ταυτότητας του εκκινητή ενός μηνύματος. Στο χειρότερο δυνατό σενάριο, όλοι οι κόμβοι εκτός από έναν είναι κακόβουλοι και συνεπώς για κάθε πακέτο που ξεκινάει από αυτόν τον κόμβο είναι γνωστή η προέλευσή του [01].

9. *Επίθεση Τύπου Ενδιαμέσου*

Η επίθεση τύπου ενδιαμέσου είναι μια μορφή επίθεσης ενεργού ωτακουστή κατά την οποία ένας επιτιθέμενος εισάγει τον εαυτό του ανάμεσα σε δύο άλλους κόμβους στο δίκτυο, δημιουργεί ανεξάρτητες συνδέσεις και αναμεταδίδει μηνύματα μεταξύ τους. Με αυτόν τον τρόπο όλη η επικοινωνία περνά μέσα από αυτόν και δίνεται η δυνατότητα να τροποποιήσει τα μηνύματα, να εισάγει ψευδείς πληροφορίες, αλλά και να ξεκινήσει μια επίθεση άρνησης υπηρεσίας.

10. Καθυστέρηση

Ο όρος καθυστέρηση αναφέρεται στην καθυστέρηση της επεξεργασίας των δεδομένων του δικτύου. Πιο συγκεκριμένα, αναφέρεται στο χρόνο που χρειάζεται για να σταλεί ένα πακέτο δεδομένων από ένα συγκεκριμένο σημείο σε ένα άλλο. Μερικές φορές μετράται ως ο χρόνος που απαιτείται για ένα πακέτο να επιστραφεί στον αποστολέα.

11. Άρνηση Υπηρεσίας

Μια επίθεση άρνησης υπηρεσίας είναι μια προσπάθεια να καταστεί ο πόρος ενός δικτύου μη διαθέσιμος στους χρήστες. Ανεξάρτητα από τον τρόπο με τον οποίον πραγματοποιείται, η εν λόγω επίθεση συνιστά προσπάθεια που στόχο έχει να διακόψει (προσωρινά ή επ' αόριστον) ή να αναστείλει τις υπηρεσίες ενός ξενιστή συνδεμένου στο διαδίκτυο.

12. Επίθεση Πλημμυρίδας

Υπό φυσιολογικές συνθήκες, κάθε αποστολέας, που ανήκει στο σύνολο ανωνυμίας, στέλνει ένα μήνυμα ανά κάποιο χρονικό διάστημα. Στις επιθέσεις πλημμυρίδας, ο επιτιθέμενος πλημμυρίζει το σύστημα με ένα σύνολο από μη έγκυρα πακέτα με στόχο να επηρεάσει αρνητικά την κίνηση του δικτύου και να προκαλέσει πρόβλημα στην επικοινωνία των μελών του.

Κεφάλαιο 3
Αρχιτεκτονική των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας

Οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας αφορούν σε λογισμικό και συστήματα που επιτρέπουν στα άτομα να αποκρύψουν την πραγματική τους ταυτότητα, την οποία και αποκαλύπτουν μόνο όταν είναι απολύτως απαραίτητο. Οι τεχνολογίες αυτές, οι οποίες παραδοσιακά περιορίζονταν σε «εργαλεία ψευδωνύμων», συμβάλλουν στην ελαχιστοποίηση των πληροφοριών που συλλέγονται για τα άτομα και περιλαμβάνουν ανώνυμα προγράμματα περιήγησης στο Web, ειδικευμένες υπηρεσίες e-mail, κτλ. Τα τελευταία χρόνια ωστόσο έχει αναπτυχθεί πληθώρα Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας, οι οποίες διαφοροποιούνται ανάλογα με την αρχιτεκτονική τους αλλά και το είδος της προστασίας την οποία παρέχουν.

3.1 Πληρεξούσιοι Εξυπηρετητές

Ο πληρεξούσιος εξυπηρετητής δρα ως ενδιάμεσος στην επικοινωνία του χρήστη με τον ιστότοπο που επιθυμεί να επισκεφτεί. Αναλαμβάνει να στείλει τα αιτήματα του χρήστη που αναζητούν πόρους από κάποιον εξυπηρετητή και, αντιστρόφως, αναλαμβάνει να μεταφέρει τις αποκρίσεις του εξυπηρετητή στον χρήστη. Πολλοί μηχανισμοί προστασίας της ιδιωτικότητας στηρίζουν την αρχιτεκτονική της λειτουργίας τους στην χρήση του πληρεξούσιου εξυπηρετητή προκειμένου να διευκολύνουν την ασφαλή περιήγηση του χρήστη στο διαδίκτυο.

3.1.1 LPWA

Πολλοί ιστότοποι προσφέρουν προσωποποιημένες υπηρεσίες παρέχοντας την δυνατότητα στους χρήστες να παρέχουν πληροφορίες για τον εαυτό τους και τις προτιμήσεις τους [28]. Το Lucent Personalized Web Assistant (LPWA) είναι ένα σύστημα λογισμικού σχεδιασμένο να ανταποκριθεί στα προβλήματα που προκύπτουν κατά την εγγραφή των προσωπικών στοιχείων του χρήστη στους διάφορους ιστότοπους, στους οποίους ο χρήστης παρέχει: όνομα χρήστη, κωδικό πρόσβασης και διεύθυνση ηλεκτρονικού ταχυδρομείου. Οι χρήστες μπορούν λοιπόν να περιηγηθούν στον ιστό με ένα προσωποποιημένο, απλό, ιδιωτικό και ασφαλή τρόπο, χρησιμοποιώντας τα ψευδώνυμα (persona) που παράγονται από το LPWA. Κάθε ψευδώνυμο αποτελείται από ένα όνομα χρήστη, κωδικό πρόσβασης και μία διεύθυνση ηλεκτρονικού ταχυδρομείου.

Τεχνική Περιγραφή Λειτουργίας/Αρχιτεκτονική: Το σύστημα LPWA αποτελείται από τρία λειτουργικά στοιχεία: το Persona Generator, τον Browsing Proxy και τον E-mail Forwarder [28].

Ο Persona Generator χρησιμοποιεί δύο στοιχεία ιδιωτικών πληροφοριών που παρέχονται από τον χρήστη: το USER ID που αποτελείται από μία έγκυρη διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη και το SECRET το οποίο λειτουργεί ως ένας καθολικός κωδικός πρόσβασης. Χρησιμοποιώντας λοιπόν τις δύο αυτές πληροφορίες που παρέχονται από τον χρήστη, και λαμβάνοντας υπόψη τον ιστότοπο που θέλει να επισκεφτεί ο χρήστης, παράγει ένα μοναδικό και σταθερό ψευδώνυμο (persona) του χρήστη για τον συγκεκριμένο ιστότοπο ως απάντηση στο αίτημα του.

Ο Persona Generator χρησιμοποιεί την συνάρτηση Janus η οποία μεταφράζει την πληροφορία που παρέχεται από τον χρήστη (διεύθυνση ηλεκτρονικού ταχυδρομείου, συνθηματική φράση),

σε ένα ψευδώνυμο (όνομα χρήστη, κωδικό πρόσβασης και μία διεύθυνση ηλεκτρονικού ταχυδρομείου) για κάθε ιστότοπο [06], βασιζόμενη σε έναν κατάλληλο συνδυασμό κρυπτογραφικών συναρτήσεων [01]. Πιο συγκεκριμένα, δέχεται στην είσοδο της το USERID, το SECRET, και το DOMAIN (του ιστότοπου) και παράγει στην έξοδο της ένα LPWA όνομα χρήστη και κωδικό πρόσβασης, ενώ η παραγόμενη LPWA ψευδώνυμη ταχυδρομική ηλεκτρονική διεύθυνση είναι μία κρυπτογράφηση του USER ID από ένα σταθερό μυστικό κλειδί.

Ο Persona Generator μπορεί να υλοποιηθεί μέσα στον φυλλομετρητή του χρήστη ή στον Browsing Proxy.

Ο Browsing Proxy ενισχύει την προστασία της ιδιωτικότητας του χρήστη φιλτράροντας τις κεφαλίδες στο HTTP επίπεδο και αναφέροντας έμμεσα την σύνδεση του χρήστη στο TCP επίπεδο, εφόσον δεν υφίσταται σύνδεση του χρήστη απευθείας με τον ιστότοπο αλλά πραγματοποιείται μέσω του πληρεξούσιου. Ο Browsing Proxy μπορεί να τοποθετηθεί σε ένα τοίχος προστασίας (firewall), σε ένα σημείο εισόδου του παρόχου Internet (ISP) ή σε κάποιο ιστότοπο στο Internet.

Ο Email Forwarder προωθεί το ηλεκτρονικό μήνυμα, από την ψευδώνυμη (persona) ηλεκτρονική διεύθυνση ταχυδρομείου στην αντίστοιχη πραγματική διεύθυνση του χρήστη. Δεδομένου ότι οι διάφορες ψευδώνυμες (persona) διευθύνεις ηλεκτρονικού ταχυδρομείου δεν πρέπει να είναι συνδέσιμες με τον χρήστη, θα πρέπει ο Email Forwarder να τοποθετηθεί μακριά από τον υπολογιστή του χρήστη.

Πλεονεκτήματα/Θετικά χαρακτηριστικά: Όταν ένας ιστότοπος ζητάει από τον χρήστη να παρέχει το όνομα χρήστη, τον κωδικό πρόσβασης ή την ηλεκτρονική διεύθυνση ταχυδρομείου, ο χρήστης απλά πληκτρολογεί τον κατάλληλο χαρακτήρα (\u. \p, \@) αντίστοιχα με τον χαρακτήρα διαφυγής και το LPWA παρέχει το κατάλληλο ψευδώνυμο. Ο χρήστης δεν χρειάζεται να θυμάται τα ψευδώνυμα για τον κάθε ιστότοπο που επισκέπτεται και επομένως δεν χρειάζεται να πληκτρολογεί μεγάλα username, password ή email address [28].

Οι χρήστες έχουν διαφορετικά ψευδώνυμα σε κάθε ιστότοπο και αυτό έχει ως αποτέλεσμα την αποφυγή της δημιουργίας των profile των χρηστών από τους ιστότοπους ή την ενδεχόμενη συνέργεια αυτών, ενώ προστατεύει επίσης και την αποκάλυψη της πραγματικής ταυτότητας των χρηστών. Ο χρήστης θα πρέπει να είναι ιδιαίτερα προσεκτικός στα στοιχεία που αποκαλύπτει στους ιστότοπους που επισκέπτεται και δεν πρέπει να δίνει ηλεκτρονικές

διευθύνσεις ταχυδρομείου, αριθμούς πιστωτικών καρτών και άλλες πληροφορίες που αποκαλύπτουν την ταυτότητά του.

Πληκτρολογώντας ο χρήστης /@ ο LPWA πληρεξούσιος δημιουργεί μία ψευδώνυμη διεύθυνση ηλεκτρονικού ταχυδρομείου για τον χρήστη, αποτελούμενη από ένα παραγόμενο ψευδώνυμο του χρήστη και το domain lpwa.com. Στη συνέχεια το σύστημα ηλεκτρονικού ταχυδρομείου αποθηκεύει όλα τα εισερχόμενα μηνύματα και ο πράκτορας του χρήστη (user agent) αναλαμβάνει να ανασύρει τα μηνύματα για όλα τα ψευδώνυμα που ανήκουν στον συγκεκριμένο χρήστη [28]. Αυτή η διάταξη έχει το πλεονέκτημα ότι δεν αποθηκεύεται στο σύστημα ηλεκτρονικού ταχυδρομείου καμία πληροφορία που θα μπορούσε να αποκαλύψει την ταυτότητα του χρήστη. Για την επίτευξη του στόχου προστασίας της ταυτότητας του χρήστη, μία τέτοια διάταξη αντιστοιχεί καλύτερα σε περιβάλλοντα όπου ο πληρεξούσιος τοποθετείται σε ένα τείχος προστασίας ή σε ένα σημείο πρόσβασης του φορέα παροχής Internet (ISP).

Η διαφορετική διεύθυνση που αποκτά ο χρήστης, ως παραγόμενη του Persona Generator, σε κάθε ιστότοπο που απαιτείται η διαδικασία της εγγραφής, συντελεί στο αποτελεσματικό φιλτράρισμα των ανεπιθύμητων μηνυμάτων (spam). Για παράδειγμα, ο χρήστης μπορεί να είναι γνωστός ως hwfyh_yocY_XUKm_t_OKvnNW_lpwa@com στο my.yahoo.com και ως lN_illidPtFk__SthNoXzGuS_lpwa@com στο www.expedia.com [28]. Λαμβάνοντας ένα ανεπιθύμητο μήνυμα από την διεύθυνση lN_illidPtFk__SthNoXzGuS_lpwa@com που έχει στον ιστότοπο www.expedia.com μπορεί να εγκαταστήσει ένα φίλτρο για το string lN_illidPtFk__SthNoXzGuS_ ενώ την ίδια στιγμή τα μηνύματα από τους άλλους ιστότοπους είναι ανεπηρέαστα. Ο χρήστης γνωρίζει από ποιον ιστότοπο λαμβάνει το μήνυμα διότι όταν ο LPWA E-mail Forwarder αποκρυπτογραφεί μία ψευδώνυμη διεύθυνση ηλεκτρονικού ταχυδρομείου ώστε να το προωθήσει στην πραγματική διεύθυνση του χρήστη συμπεριλαμβάνει στο πεδίο CC του μηνύματος την ψευδώνυμη διεύθυνση από όπου προέρχεται αρχικά το μήνυμα. Επίσης, είναι σημαντικό να επισημανθεί ότι εάν ο αποστολέας ανεπιθύμητης αλληλογραφίας έχει πρόσβαση στη βάση δεδομένων ενός ιστότοπου γνωρίζει το χρήστη μόνο με την ψευδώνυμη διεύθυνση και όχι με τα πραγματικά του στοιχεία. Επιπλέον, ο χρήστης μπορεί να κρατήσει μία τοπική βάση δεδομένων αντιστοιχώντας ψευδώνυμες ηλεκτρονικές διευθύνσεις ταχυδρομείου με τους ιστότοπους που δημιουργήθηκαν και με αυτό τον τρόπο έχει την δυνατότητα να γνωρίζει ποιος ιστότοπος είναι υπεύθυνος για την αποστολή ανεπιθύμητου μηνύματος ακόμα και αν έχει αποσταλεί από τρίτο μέρος (party). Ο χρήστης μπορεί να παραπονεθεί στο website ή ακόμα και να λάβει κάποια άλλη ενέργεια εάν χρειαστεί [28].

Στο LPWA, ο HTTP πληρεξούσιος, ο οποίος περιλαμβάνει τον Browsing Proxy και τον Persona Generator, δεν αποθηκεύει καμία πληροφορία ταυτότητας του χρήστη. Ο πληρεξούσιος σε κάθε HTTP αίτημα του χρήστη παίρνει την ταυτότητα του χρήστη από την κεφαλίδα HTTP (αυθεντικοποίηση πληρεξούσιου) την οποία στέλνει ο φυλλομετρητής του χρήστη κεφαλίδα ως μέρος της διαδικασίας εισόδου του στο LPWA. Ο Persona Generator υπολογίζει τα ψευδώνυμα του χρήστη από την πληροφορία της κεφαλίδας και του domain ονόματος του ιστότοπου προορισμού, αποφεύγοντας έτσι την ανάγκη να αποθηκεύσει οποιαδήποτε πληροφορία ταυτότητας του χρήστη στον πληρεξούσιο. Ο χρήστης πρέπει να συνδέεται στο LPWA με τα ίδια στοιχεία ταυτότητας κάθε φορά ώστε να λαμβάνει συνεπή LPWA ψευδώνυμα.

Ευπάθειες/μειονεκτήματα: Εάν κατά την υλοποίηση του LPWA χρησιμοποιηθεί ως κεντρικός πληρεξούσιος ο ιστότοπος www.lpwa.com τότε τίθεται θέμα εμπιστοσύνης των διαχειριστών του.

Επίσης, το LPWA παρέχει περιορισμένη ανωνυμία σύνδεσης χρησιμοποιώντας τον HTTP πληρεξούσιο εφόσον η επικοινωνία ανάμεσα στον φυλλομετρητή και στον LPWA πληρεξούσιο είναι μία δημόσια σύνδεση και δεν κρυπτογραφούνται τα δεδομένα που στέλνονται, με αποτέλεσμα να είναι ευπαθές στην ανίχνευση της επικοινωνίας από ωτακουστές και στο ενδεχόμενο αποκάλυψης της ταυτότητας του χρήστη.

Το LPWA δεν φιλτράρει εφαρμογές Java και Javascript από τις οποίες μπορεί να διαρρεύσουν πληροφορίες από τον φυλλομετρητή στον εξυπηρετητή.

Εάν η τοποθεσία του Browsing Proxy είναι «μακριά» σε σχέση με την διαδικτυακή σύνδεση του χρήστη τότε η υποβάθμιση/μείωση της απόδοσης κατά την περιήγηση γίνεται αντιληπτή στο χρήστη.

3.1.2 Anonymizer

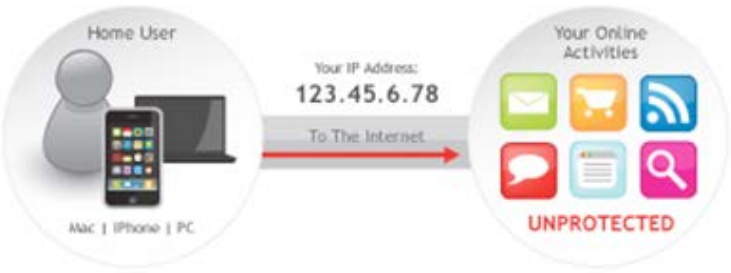
Ως γνωστό, οι δραστηριότητες στο διαδίκτυο μπορούν να αποκαλύψουν προσωπικές πληροφορίες για τους χρήστες όπως στοιχεία ταυτότητας, πιστωτικής κάρτας, προσωπικές προτιμήσεις και ενδιαφέροντα, το ιδιωτικό περιεχόμενο που μοιράζονται, καθώς επίσης και τις ιστοσελίδες που επισκέπτονται. Το Anonymizer Universal διασφαλίζει την ανωνυμία της ταυτότητας των χρηστών καθώς και την προστασία και ασφάλεια των προσωπικών δεδομένων των χρηστών κάθε φορά που χρησιμοποιούν το διαδίκτυο. Το Anonymizer Universal είναι μία

state-of-the-art υπηρεσία που επιτυγχάνει την ιδιωτικότητα, την ασφάλεια και την ανωνυμία της σύνδεσης.

Τεχνική Περιγραφή Λειτουργίας/Αρχιτεκτονική: Κάθε φορά που ο χρήστης συνδέεται στο διαδίκτυο, ο Anonymizer δρομολογεί όλη την διαδικτυακή κίνηση του χρήστη μέσα από ένα κρυπτογραφημένο «τούνελ», TLS σύνδεση, από τον υπολογιστή του στους ασφαλείς διακομιστές του Anonymizer. Ο Anonymizer είναι ένας πληρεξούσιος διακομιστής που ενεργεί ως ενδιάμεσος στην επικοινωνία του χρήστη με τον εξυπηρετητή και προστατεύει την ιδιωτική συμπεριφορά και τα προσωπικά δεδομένα, ενώ ταυτόχρονα αποκρύπτει τις πληροφορίες αναγνώρισης του υπολογιστή του χρήστη.

Πιο συγκεκριμένα όλες οι διαδικτυακές συνδέσεις που εκκινούνται από τον χρήστη προωθούνται μέσω του Anonymizer Universal στους διάφορους HTTP εξυπηρετητές [01]. Ο Anonymizer Universal αποτελείται από ομάδα πληρεξούσιων διευκολύνοντας την αποτελεσματική ανταπόκρισή του στις πολλές διαδικτυακές συνδέσεις των μελών του.

Για παράδειγμα, στην εικόνα 1 η ταυτότητα του χρήστη δεν προστατεύεται διότι η σύνδεσή του με τη διαδικτυακή του δραστηριότητα και πιο συγκεκριμένα με το URL που επισκέπτεται είναι εκτεθειμένη σε διάφορες επιθέσεις. Παρατηρείται ότι δεν υπάρχει προστασία της σύνδεσης και η IP του χρήστη είναι εκτεθειμένη και εμφανής καθ' όλη την διάρκεια της, ενώ και τα δεδομένα που ανταλλάσσονται δεν κρυπτογραφούνται.



Εικόνα 1: Σύνδεση του χρήστη με τις διαδικτυακές δραστηριότητες, ιστοτόπους του χωρίς προστασία

Στην εικόνα 2 παρατηρείται ότι ο χρήστης συνδέεται στο URL μέσω του δικτύου Anonymizer. Η σύνδεση αυτή προστατεύεται από το ασφαλή εικονικό ιδιωτικό δίκτυο που υφίσταται μεταξύ του χρήστη και του Anonymizer, δημιουργώντας ένα ασφαλή κρυπτογραφημένο τούνελ βασιζόμενο σε TLS σύνδεση. Στη συνέχεια, όλη η επικοινωνία του χρήστη πραγματοποιείται

διαμέσου του δικτύου Anonymizer το οποίο αλλάζει την πραγματική IP διεύθυνση του χρήστη με μία εικονική.

Εικόνα 2: Σύνδεση του χρήστη με τις διαδικτυακές δραστηριότητες με προστασία μέσω του δικτύου Anonymizer.

Πλεονεκτήματα/Θετικά χαρακτηριστικά: Ο Anonymizer Universal συνδυάζει την κρυπτογράφηση ενός Εικονικού Ιδιωτικού Δικτύου με μοναδικό εναλλασσόμενο και διαμοιραζόμενο IP [62]. Με την διαμεσολάβηση του Anonymizer πληρεξούσιου εξυπηρετητή προστατεύεται η σύνδεση του χρήστη με τον εξυπηρετητή, ενώ με τη δημιουργία κρυπτογραφημένου «τούνελ» μέσω του εικονικού ιδιωτικού δικτύου προστατεύεται η σύνδεση μεταξύ του χρήστη και του Anonymizer δικτύου. Επίσης, παρέχει προστασία και σε ασύρματες συνδέσεις του χρήστη μέσω του κρυπτογραφημένου εικονικού δικτύου του.

Οι καθημερινές δραστηριότητες του χρήστη στο διαδίκτυο ενδέχεται να αποκαλύψουν προσωπικά του δεδομένα, όπως τραπεζικές πληροφορίες και στοιχεία πιστωτικής κάρτας, ιατρικό ιστορικό, κωδικούς πρόσβασης, καθώς και ιδιωτική επικοινωνία. Ο Anonymizer χρησιμοποιεί υψηλού βαθμού κρυπτογράφηση για να δρομολογήσει την διαδικτυακή κυκλοφορία του χρήστη μέσω ενός «τούνελ» εικονικού ιδιωτικού δικτύου στους ασφαλείς διακομιστές του [62]. Επομένως, το κρυπτογραφημένο ιδιωτικό δίκτυο βοηθά στην προστασία των δεδομένων και την αποφυγή κλοπής της ταυτότητας.

Οι εισβολείς προσωπικών δεδομένων μπορούν να θέσουν σε κίνδυνο ευαίσθητες πληροφορίες του χρήστη. Εγκληματίες, εργοδότες, ακόμη και ο πάροχος του διαδικτύου (ISP) ενδέχεται να παρακολουθεί εύκολα τη μοναδική διεύθυνση IP του χρήστη στο διαδίκτυο καθώς επίσης και την δραστηριότητά του. Ο Anonymizer Universal αλλάζει την πραγματική διεύθυνση IP του χρήστη σε μία διαφορετική, μη ανιχνεύσιμη διεύθυνση IP κάθε μέρα, εξασφαλίζοντας έτσι την ιδιωτικότητα και την εμπιστευτικότητα των δραστηριοτήτων του χρήστη στο διαδίκτυο.

Η εγκατάσταση του Anonymizer Universal καθώς και η χρήση του είναι εύκολη. Εκτελείται στο παρασκήνιο και δεν απαιτεί ιδιαίτερες τεχνικές γνώσεις από τον χρήστη.

Ευπάθειες/μειονεκτήματα: Ο χρήστης πρέπει να εμπιστεύεται την υπηρεσία του εργαλείου Anonymizer [01]. Αν και όλοι οι πληρεξούσιοι του Anonymizer Universal καθώς και οι διαδικασίες αυθεντικοποίησης είναι απολύτως ασφαλείς και μπορούν να προσπελαστούν μόνο από εγκεκριμένο προσωπικό και όχι από τρίτα μέρη, τίθεται το θέμα εμπιστοσύνης και εμπιστευτικότητας του χρήστη προς τις παρεχόμενες υπηρεσίες του Anonymizer Universal.

3.2 Δίκτυα Mix

Το 1970 ο David Chaum εισήγαγε τα δίκτυα mix για την ασφαλή πρόσβαση του χρήστη σε διάφορες διαδικτυακές υπηρεσίες. Το Mix είναι ένα κομμάτι λογισμικού που δρομολογεί την επικοινωνία που λαμβάνει χωρίς να γνωρίζει την πηγή και τον προορισμό της. Η μεταφορά των δεδομένων πραγματοποιείται διαμέσου πολλών κόμβων Mix αφού πρώτα κρυπτογραφηθεί από τον εκκινητή, και στη συνέχεια διαδοχικά με το κλειδί του κάθε κόμβου Mix από τον οποίον θα διέλθει το μήνυμα, αποτελούμενο έτσι από πολλά στρώματα κρυπτογράφησης. Ο κάθε κόμβος που λαμβάνει το μήνυμα αφαιρεί το ένα στρώμα κρυπτογράφησης με το αντίστοιχο κλειδί που διαθέτει και το αποστέλλει στον επόμενο κόμβο mix του μονοπατιού δρομολόγησης κ.ο.κ. Έχουν αναπτυχθεί πολλοί μηχανισμοί προστασίας της ιδιωτικότητας βασιζόμενοι στους κόμβους Mix λόγω της ισχυρής κρυπτογράφησης που παρέχεται και της αποτελεσματικότερης εξασφάλισης της ιδιωτικότητας του χρήστη.

3.2.1 Mixminion

Το Mixminion είναι μία εφαρμογή του πρωτοκόλλου ανώνυμου επαναποστολέα τύπου III που παρέχει τη δυνατότητα στον χρήστη να στείλει και να λάβει μηνύματα ηλεκτρονικού ταχυδρομείου ανώνυμα [56]. Πιο συγκεκριμένα, επιτρέπει στον χρήστη: α) να προωθήσει μηνύματα ανώνυμα, β) να απαντήσει σε μήνυμα όπου ο παραλήπτης παραμένει ανώνυμος και γ) να απαντήσει σε μήνυμα όπου και ο αποστολέας και ο παραλήπτης παραμένουν ανώνυμοι. Χρησιμοποιεί την αρχιτεκτονική των δικτύων mix για την παροχή υψηλού βαθμού ανωνυμίας και αποτρέπει σε σημαντικό βαθμό διάφορες επιθέσεις που αποσκοπούν στη διασύνδεση του αποστολέα με τον παραλήπτη. Οι κόμβοι mix δεν μπορούν να διακρίνουν τα μηνύματα που

προωθούνται από το Mixminion από τα μηνύματα απάντησης και επομένως τα μηνύματα προώθησης και απάντησης μοιράζονται τον ίδιο βαθμό ανωνυμίας [19].

Τεχνική Περιγραφή Λειτουργίας/Αρχιτεκτονική: Το mixminion χρησιμοποιεί δίκτυα mix ελεύθερης δρομολόγησης. Εθελοντές εκτελούν στον υπολογιστή τους τα mixes, δηλαδή κόμβοι οι οποίοι αποκρυπτογραφούν, αναδιατάσσουν και αναμεταδίδουν τα μηνύματα που λαμβάνουν προς τον τελικό προορισμό τους [59]. Κάθε μήνυμα περνάει μέσα από διάφορα mixes και έτσι κανένα mix δεν μπορεί να συνδέσει τα μηνύματα του αποστολέα με τον παραλήπτη.

Κάθε μήνυμα που αποστέλλεται χωρίζεται από το mixminion σε μικρά πακέτα και συμπληρώνονται (pad) ώστε να έχουν το ίδιο μέγεθος. Το mixminion επιλέγει τη διαδρομή του δικτύου mix για κάθε πακέτο του μηνύματος που θα αποσταλεί. Κάθε πακέτο, ένα προς ένα, πριν αποσταλεί κρυπτογραφείται με τα αντίστοιχα δημόσια κλειδιά του κάθε κόμβου mix του μονοπατιού που θα ακολουθήσει. Στη συνέχεια, μεταδίδει το πακέτο στο πρώτο mix του μονοπατιού το οποίο μόλις το λάβει το αποκρυπτογραφεί, συμπληρώνει το πακέτο (repadding) ώστε να έχει το ίδιο μέγεθος με τα άλλα πακέτα και το αναμεταδίδει. Με αυτόν τον τρόπο το πακέτο φτάνει στο τελευταίο mix του μονοπατιού το οποίο το στέλνει στον τελικό προορισμό του, δηλαδή στον παραλήπτη.

Χαρακτηριστικό του mixminion είναι η παροχή του Single Use Reply Block (SURB) δηλαδή ενός μπλοκ απάντησης μίας χρήσης. Γενικά, ένα "reply block" είναι ένα κρυπτογραφημένο μήνυμα το οποίο περιέχει οδηγίες στον επαναποστολέα σχετικά με το πώς μπορεί να προωθήσει το μήνυμα στον χρήστη χωρίς να αποκαλυφθεί η διεύθυνσή του. Συμπεριλαμβάνοντας λοιπόν ένα reply block, επιτρέπει στους παραλήπτες του μηνύματος να απαντήσουν ανώνυμα, χωρίς να γνωρίζουν την πραγματική διεύθυνση του αποστολέα. Επομένως, το mixminion παρέχει την δυνατότητα στον χρήστη, με την χρήση των SURBs, να στέλνει μηνύματα προς τον παραλήπτη και να λαμβάνει απάντηση χωρίς να αποκαλύπτεται η ταυτότητά του. Το SURB περιέχει πληροφορίες οι οποίες είναι δυνατόν να αποκρυπτογραφηθούν από το πρώτο mix του μονοπατιού το οποίο προσδιορίζεται στο μπλοκ. Το mix αποκρυπτογραφεί τις πληροφορίες και βρίσκει σε αυτές ένα άλλο κρυπτογραφημένο μήνυμα το οποίο περιέχει το επόμενο mix που πρέπει να αποσταλεί. Στο τελικό mix, το τελευταίο μπλοκ περιέχει την πληροφορία για τον τελικό παραλήπτη που πρέπει να αποσταλεί. Το SURB μπορεί να χρησιμοποιηθεί μόνο μία φορά και καταστρέφεται μία εβδομάδα μετά την δημιουργία του. Δεν παρέχει τη δυνατότητα επαναληπτικών απαντητικών μηνυμάτων στον αποστολέα με αποτέλεσμα την καλύτερη

προστασία της ανωνυμίας του αποστολέα. Επομένως για να στείλει ο χρήστης κάποιο μήνυμα είναι απαραίτητη η δημιουργία ενός SURB.

Τα μηνύματα που ένας χρήστης λαμβάνει από το mixminion έχουν τρεις κωδικοποιημένες μορφές: α) δυαδικά, β) ανώνυμα μηνύματα απάντησης που στέλνονται στο SURB και απευθύνονται στον χρήστη και γ) μοναδικά τμήματα (fragments) μεγάλων ανώνυμων μηνυμάτων που εκτείνονται σε πολλαπλά πακέτα. Σε κάθε περίπτωση το mixminion παρέχει διαφορετικό τρόπο αντιμετώπισης: τα δυαδικά μηνύματα τα αποκωδικοποιεί σε πολύ μικρό βαθμό, τις ανώνυμες απαντήσεις με το SURB κλειδί του χρήστη και τα fragments τα αποθηκεύει μέχρι να είναι διαθέσιμα για την ανασύνθεση ολόκληρου του μηνύματος.

Είναι σημαντικό να επισημανθεί η swap λειτουργία του mixminion ως βασικό στοιχείο λειτουργίας του συστήματος που επιτρέπει στον χρήστη να στέλνει και να λαμβάνει ανώνυμα μηνύματα. Το κάθε κρυπτογραφημένο πακέτο του μηνύματος συμπεριλαμβάνει δύο τμήματα κεφαλίδας τα οποία αναστρέφονται (swap) κατά την διάρκεια μεταφοράς στο mixminion δίκτυο. Πιο συγκεκριμένα, όταν ο χρήστης δημιουργήσει το μήνυμά του, κρυπτογραφεί τη δευτερεύουσα κεφαλίδα με ένα τμήμα του ωφέλιμου φορτίου του, το μήνυμα μεταφέρεται στο δίκτυο mix, όπως περιγράφτηκε προηγουμένως (κάθε mix αποκρυπτογραφεί ένα στρώμα, επαληθεύει το τμήμα της τρέχουσας κεφαλίδας και συμπληρώνει κάποια σκουπίδια στο τέλος της επικεφαλίδας (pad)), μέχρι να φτάσει σε ένα mix που έχει επισημανθεί ως σημείο διασταύρωσης (crossover). Αυτό το σημείο διασταύρωσης εκτελεί μια "swap" (αναστροφή) αποκρυπτογραφώντας πρώτα τη δευτερεύουσα κεφαλίδα με το τμήμα του τρέχοντος ωφέλιμου φορτίου, και στη συνέχεια αναστρέφει (swap) τις δύο κεφαλίδες.

Πλεονεκτήματα/Θετικά χαρακτηριστικά: Λειτουργικό στοιχείο του mixminion αποτελεί το μπλοκ απάντησης μίας χρήσης (Single Use Reply Block, SURB). Λόγω του ότι δεν επαναχρησιμοποιείται και λήγει με την πάροδο κάποιου χρονικού διαστήματος αποτρέπεται, κατ' αυτόν τον τρόπο, ο εντοπισμός της διαδρομής του παραλήπτη από κάποιον αντίπαλο. Σε περίπτωση που το SURB χρησιμοποιηθεί αρκετές φορές για την αποστολή μηνυμάτων απάντησης στον αποστολέα, υπάρχει ο κίνδυνος ιχνηλάτισης του μονοπατιού και αποκάλυψης πολύτιμων πληροφοριών σε κάποιον κακόβουλο εισβολέα. Επίσης, το mixminion με τη χρήση του SURB παρέχει τον ίδιο βαθμό ανωνυμίας στα προωθημένα και στα μηνύματα απάντησης, τα οποία δεν είναι ευδιάκριτα ακόμα και από τους κόμβους mix.

Το mixminion για να προστατεύσει τους χρήστες από τις επιθέσεις χρονισμού, συγκεντρώνει κάποιο αριθμό πακέτων στην ουρά και έπειτα τα μεταδίδει στο μονοπάτι προς τον προορισμό τους. Κάθε υποκεφαλίδα του πακέτου περιλαμβάνει τη διεύθυνση του επόμενου κόμβου που θα προωθηθεί με την υπογραφή του (ταυτότητα) αποτυπώματος του κλειδιού και το mix αρνείται να παραδώσει το μήνυμα στον επόμενο κόμβο εάν δεν αποδείξει την ταυτότητά του. Με αυτήν την ενέργεια αν και ελλοχεύει ο κίνδυνος άρνησης υπηρεσίας (DoS), προστατεύει τους χρήστες από διάφορες επιθέσεις παραβίασης της ιδιωτικότητας του χρήστη. Επίσης, οι κόμβοι mix που παρεμβάλλονται δεν γνωρίζουν το μονοπάτι αλλά μόνο τους γειτονικούς τους κόμβους mix με αποτέλεσμα να μην μπορούν να συνδέσουν τον αποστολέα με τον παραλήπτη.

Το mixminion κρυπτογραφεί την σύνδεση μεταξύ των επαναποστολέων χρησιμοποιώντας TLS (Transport Layer Security) στο TCP επίπεδο και προσωρινά κλειδιά διασφαλίζοντας την ανωνυμία προώθησης σε κάθε μήνυμα και προστατεύοντας κατ' αυτόν τον τρόπο τη σύνδεση επικοινωνίας από ενεργές και παθητικές επιθέσεις. Αποτρέπει επίσης τις επιθέσεις σήμανσης (tagging attacks) με τη swap διεργασία, καθώς επίσης και με την ανίχνευση τροποποιημένων κεφαλίδων χρησιμοποιώντας τον έλεγχο αθροίσματος.

***Ευπάθειες/μειονεκτήματα*:** Το Mixminion δεν προστατεύει τα δεδομένα που ο χρήστης αποκαλύπτει στα μηνύματά του σε σχέση με τα προσωπικά του στοιχεία.

Για τη δημιουργία μονοπατιών, το mixminion θα πρέπει να είναι ενημερωμένο για τους διαθέσιμους κόμβους mix στο δίκτυο, το οποίο επιτυγχάνεται με τη λήψη ενός καταλόγου με μη αυτόματο τρόπο. Αυτό έχει σαν αποτέλεσμα ο αντίπαλος να είναι σε θέση να εκμεταλλευτεί το γεγονός ότι ο χρήστης ενδεχομένως να μην έχει ενημερωθεί πρόσφατα για τον ισχύον κατάλογο. Η διαφορά πληροφορίας που προκύπτει σε περίπτωση μη ενημερωμένου καταλόγου δημιουργεί προβλήματα στην επικοινωνία και αφήνει περιθώρια διαφόρων κακόβουλων επιθέσεων.

Ο αντίπαλος έχει τη δυνατότητα να «απορρίψει» μηνύματα που διασχίζουν το μονοπάτι προς τον προορισμό τους με στόχο οι χρήστες να το παρατηρήσουν και να ξαναστείλουν τα μηνύματα όχι στην ίδια διαδρομή αλλά σε μία ελεγχόμενη.

3.3 Δίκτυα Ομότιμων Οντοτήτων (Peer-to-Peer Networks)

Τα δίκτυα ομότιμων οντοτήτων αποτελούν διαμοιραζόμενα και αποκεντροποιημένα συστήματα αποτελούμενα από διασυνδεδεμένους κόμβους μεταξύ τους, οι οποίοι έχουν τη δυνατότητα αυτο-οργάνωσης στην τοπολογία των δικτύων με σκοπό τον διαμοιρασμό διαφόρων πόρων και μπορούν να ανταπεξέλθουν σε κάποια αποτυχία αλλά και να φιλοξενούν μετακινούμενο πλήθος κόμβων χωρίς την απαίτηση ύπαρξης ενός κεντρικού εξυπηρετητή ή κάποιας άλλης αρχής. Πολλοί μηχανισμοί προστασίας της ιδιωτικότητας αναπτύχθηκαν σε δίκτυα ομότιμων οντοτήτων προκειμένου να διασφαλίσουν την προστασία της ιδιωτικότητας του χρήστη και να αποφύγουν την κεντροποιημένη αρχιτεκτονική του πελάτη-εξυπηρετητή. Ακολουθούν μηχανισμοί και πρωτόκολλα προστασίας της ιδιωτικότητας του χρήστη στηριζόμενα σε δίκτυα ομότιμων οντοτήτων.

3.3.1 Crowds

Το Crowds συμβάλει στην ανωνυμοποίηση της περιήγησης του χρήστη, αποτρέποντας, στους εξυπηρετητές, την αποκάλυψη οποιασδήποτε προσωπικής πληροφορίας, όπως την διεύθυνση (IP), τις ιστοσελίδες που έχει επισκεφτεί και άλλες πληροφορίες που προσδιορίζουν το profile του. χρήστη Η ονομασία του βασίστηκε στην ιδέα υλοποίησής του: «ανάμειξη μέσα στο πλήθος», όπου ο χρήστης αποκρύπτει τα ίχνη του μέσα στο πλήθος και πιο συγκεκριμένα στην ομάδα μελών που εντάσσεται μέσα στο πλήθος "Crowds".

***Τεχνική Περιγραφή Λειτουργίας/Αρχιτεκτονική*:** Το Crowds λειτουργεί συγκεντρώνοντας τους χρήστες του ιστού σε μία γεωγραφικά διασπαρμένη ομάδα, γνωστή ως Crowd, η οποία πραγματοποιεί συναλλαγές στον ιστό εκ μέρους των μελών της [01]. Επομένως, το Crowds μπορεί να θεωρηθεί ως ένα σύνολο χρηστών [41]. Ο χρήστης για να εισέλθει στο crowds και να αποτελέσει ενεργό μέλος αυτού εκκινεί στον υπολογιστή του μία διεργασία που ονομάζεται jondo. Μόλις ξεκινήσει η εκτέλεση, το jondo επικοινωνεί με έναν εξυπηρετητή που ονομάζεται μπλέντερ και ζητάει την είσοδο στο Crowds. Εάν η αίτηση γίνει δεκτή τότε το μπλέντερ του παρέχει πληροφορίες σχετικά με τα άλλα μέλη του Crowd, ενώ ταυτόχρονα και τα άλλα μέλη του Crowd ενημερώνονται για το νέο μέλος. Επομένως, ο χρήστης για την ανώνυμη συμμετοχή του στο Crowds, και κατ΄ επέκταση στον παγκόσμιο ιστό, αντιπροσωπεύεται από το Jondo το οποίο λειτουργεί ως πληρεξούσιός του. Για να επιτευχθεί αυτό ο χρήστης ρυθμίζει τον φυλλομετρητή

του ώστε να χρησιμοποιεί το τοπικό jondo ως τον πληρεξούσιο του για όλες τις διαδικτυακές υπηρεσίες και κατά συνέπεια και όλα τα αιτήματα που προέρχονται από τον φυλλομετρητή του χρήστη στέλνονται στο jondo. Όταν ο χρήστης μέσω του φυλλομετρητή ζητήσει μία διεύθυνση URL τότε το HTTP αίτημα για αυτήν την διεύθυνση στέλνεται στο jondo το οποίο μόλις λάβει το αίτημα του χρήστη εκκινεί τη δημιουργία ενός τυχαίου μονοπατιού από jondos που μεταφέρουν το αίτημα προς τον εξυπηρετητή και αντίστροφα. Αναλυτικότερα, το Jondo επιλέγει ένα Jondo τυχαία και του προωθεί το αίτημα. Το jondo αυτό μόλις λάβει το αίτημα έχει δύο επιλογές: είτε να το προωθήσει σε ένα τυχαία επιλεγμένο jondo, είτε να το υποβάλει στον προορισμό του, δηλαδή στον τελικό εξυπηρετητή και στη συνέχεια ρίχνει ένα κέρμα για τον καθορισμό του επόμενου βήματος προώθησης ή υποβολής του αιτήματος. Συνοπτικά λοιπόν, το αίτημα του χρήστη ταξιδεύει από τον φυλλομετρητή του μέσω κάποιων Jondos προς τον τελικό εξυπηρετητή. Η απάντηση του εξυπηρετητή ακολουθεί το ίδιο μονοπάτι προς το Jondo του χρήστη, δηλαδή ακολουθεί το αντίστροφο μονοπάτι. Επίσης, τα επόμενα αιτήματα του ίδιου χρήστη ακολουθούν το ίδιο μονοπάτι, με εξαίρεση ίσως τον τελικό εξυπηρετητή. Δημιουργούνται επομένως στατικά μονοπάτια και το κάθε jondo γνωρίζει το προηγούμενο και το επόμενο jondo του μονοπατιού. Η πληροφορία που ανταλλάσσεται μεταξύ των Jondos κρυπτογραφείται με χρήση συμμετρικής κρυπτογράφησης, με διαμοιραζόμενα μεταξύ των jondos κλειδιά [01].

Πλεονεκτήματα/Θετικά χαρακτηριστικά: Όπως αναφέρθηκε παραπάνω, οι ενέργειες ενός μέλους κρύβονται μέσα στις ενέργειες των μελών του Crowd και αυτό έχει ως αποτέλεσμα την αδυναμία των εξυπηρετητών αλλά και των μελών του να εντοπίσουν και να καθορίσουν τον εκκινητή του μηνύματος δηλαδή τον αποστολέα. Το αίτημα προωθείται μεταξύ των συνεργαζόμενων μελών καθιστώντας σχεδόν αδύνατο την εύρεση του αποστολέα. Επομένως, ο εξυπηρετητής δεν δύναται να αποκτήσει πληροφορίες σχετικά με τον εκκινητή του αιτήματος. Οποιοδήποτε μέλος του Crowds είναι εξίσου πιθανό να είναι ο εκκινητής του μηνύματος, δηλαδή ο αποστολέας, εφόσον το κάθε μέλος είτε προωθεί το αίτημα που λαμβάνει είτε το υποβάλει στον εξυπηρετητή. Το κάθε jondo λαμβάνοντας ένα αίτημα δεν γνωρίζει αν ο προκάτοχός του είναι ο εκκινητής του αιτήματος ή απλά ένα μέλος.

Το Crowds κρυπτογραφεί όλη την επικοινωνία μεταξύ των jondos και αυτό καθιστά δύσκολη την εύρεση του παραλήπτη από έναν τοπικό ωτακουστή που παρακολουθεί την κίνηση του υπολογιστή του χρήστη. Η πιθανότητα να εντοπιστεί ο παραλήπτης από έναν τοπικό ωτακουστή μειώνεται όσο τα μέλη του πλήθους αυξάνονται.

Κάθε μονοπάτι που δημιουργείται παραμένει στατικό και τα μέλη αναγνωρίζονται μεταξύ τους με αποτέλεσμα τον αποκλεισμό της ενδεχόμενης παρέμβασης από κάποιο κακόβουλο συνεργό ή κόμβο ως μέλος της διαδρομής.

***Ευπάθειες/μειονεκτήματα*:** Το Crowds δεν μπορεί να προστατέψει το περιεχόμενο που αποκαλύπτει ο χρήστης στον εξυπηρετητή, π.χ. σε μια ηλεκτρονική φόρμα όπου παρέχει πληροφορίες σχετικά με την ταυτότητά του ή και οποιαδήποτε πληροφορία που σχετίζεται με τον ίδιο όπως ο αριθμός πιστωτικής κάρτας και επομένως η ανωνυμία του δεν μπορεί να προστατευτεί. Επίσης, τα περιεχόμενα της κάθε αίτησης είναι προσβάσιμα από τα ενδιάμεσα jondos του Crowd.

Ο χρήστης δεν προστατεύεται από τα εκτελέσιμα περιεχόμενα των Java εφαρμογών ή τα στοιχεία ελέγχου ActiveX που ενδέχεται να ανοίξουν δικτυακές συνδέσεις από τον φυλλομετρητή του χρήστη στον τελικό εξυπηρετητή που βρίσκονται. Προτείνεται, για την προστασία της ανωνυμίας από το ενεργό περιεχόμενο των ιστοσελίδων που επισκέπτεται, η απενεργοποίηση της Java και ActiveX από το πρόγραμμα περιήγησης, ενδεχομένως μέσω κάποιου διατιθέμενου μενού προτιμήσεων.

Το Crowds δεν προστατεύει από την επίθεση των κακόβουλων μελών του που προκαλούν «Άρνηση της Υπηρεσίας» (DoS). Επίσης, το Crowds αυξάνει την κίνηση του δικτύου, τον φόρτο εργασίας των συστημάτων που εκτελούν τα jondo και τον χρόνο ανάκτησης, επιβαρύνοντας κατ' αυτόν τον τρόπο την απόδοση του συστήματος.

3.3.1.1 AP3

Το AP3 (anonymizing peer to peer proxy) είναι ένα αποκεντρωμένο ανώνυμο δίκτυο ομότιμων οντοτήτων που παρέχει συνεργασία και διαμοιραζόμενες υπηρεσίες στους χρήστες του [36]. Πιο συγκεκριμένα, αποτελεί ένα δίκτυο επικάλυψης (overlay network) που χτίσθηκε πάνω από το δίκτυο ομότιμων οντοτήτων (peer to peer) Pastry [38]. Χρησιμοποιεί τις τεχνικές του Crowds με κάποιες διαφορές και παρέχει στους κόμβους του ανωνυμία παράδοσης των μηνυμάτων, ανωνυμία καναλιού επικοινωνίας και ασφαλή ανώνυμα ψευδώνυμα.

***Τεχνική Περιγραφή Λειτουργίας/Αρχιτεκτονική*:** Για την αποστολή ανώνυμων μηνυμάτων χρησιμοποιεί την τεχνική παράδοσης του Crowds όπου ο χρήστης κρύβεται μέσα σε ένα πλήθος από κόμβους και ο κάθε κόμβος δεν γνωρίζει αν παρέλαβε το μήνυμα από τον χρήστη (εκκινητή

του μηνύματος) ή απλά από κάποιον άλλο κόμβο που προωθεί το μήνυμα στο μονοπάτι [38]. Πιο συγκεκριμένα, για να στείλει ένας κόμβος ένα μήνυμα δημιουργεί ένα ανώνυμο αίτημα που συμπεριλαμβάνει το μήνυμα και την διεύθυνση του παραλήπτη στον οποίον προορίζεται το μήνυμα. Στη συνέχεια επιλέγει ένα τυχαίο κλειδί το οποίο προσδιορίζει τον κόμβο του δικτύου που θα προωθηθεί το μήνυμα. Το υποκείμενο υπόστρωμα δρομολόγησης εξασφαλίζει την αποτελεσματική παράδοση στον κόμβο που είναι υπεύθυνος για αυτό το κλειδί. Όταν ο κόμβος λάβει το μήνυμα εκτελεί μία «ρίψη νομίσματος» για να αποφασίσει εάν θα στείλει το μήνυμα στον προοριζόμενο παραλήπτη ή αν θα το προωθήσει σε κάποιον άλλο ομότιμο κόμβο τον οποίον θα επιλέξει τυχαία. Δημιουργείται λοιπόν ένα τυχαίο μονοπάτι από τυχαία hops με αποτέλεσμα η ταυτότητα του αποστολέα να κρύβεται τόσο από τον παραλήπτη του μηνύματος όσο και από τους άλλους κόμβους στο δίκτυο. Οι κόμβοι που λαμβάνουν ένα μήνυμα δεν είναι σε θέση να γνωρίζουν εάν ο κόμβος που τους έστειλε το μήνυμα είναι ο συντάκτης του. Ο κάθε κόμβος προωθεί το μήνυμα με πιθανότητα pf (πιθανότητα προώθησης). Για την προστασία της ανωνυμίας του αποστολέα η τιμή της πιθανότητας πρέπει να είναι τουλάχιστον 0,5. Αν η τιμή της πιθανότητας είναι μεγαλύτερη αυξάνεται ο κίνδυνος αποκάλυψης της ταυτότητας του χρήστη. Επίσης, η τιμή της pf (πιθανότητα προώθησης) πρέπει να είναι χαμηλότερη από 1 διότι τα μονοπάτια πρέπει να είναι πεπερασμένου μήκους.

Ο παραλήπτης που λαμβάνει ένα μήνυμα δεν γνωρίζει την ταυτότητα του αποστολέα με αποτέλεσμα να αδυνατεί να του στείλει απάντηση. Το AP3 παρέχει λύση στο πρόβλημα αυτό κατασκευάζοντας ανώνυμα κανάλια που επιτρέπουν σε έναν κόμβο να προσδιορίσει ένα μονοπάτι επιστροφής του μηνύματος χωρίς να αποκαλύπτεται η ταυτότητά του. Επομένως, κάθε κόμβος που επιθυμεί να στείλει μήνυμα ανώνυμα και να λάβει απάντηση επιλέγει αρχικά τυχαία ένα id και εγκαθιστά μονοπάτι στέλνοντας το ανώνυμο μήνυμα στον κόμβο που βρίσκεται πλησιέστερα στο επιλεγμένο id. Κάθε κόμβος στο μονοπάτι από το οποίο διέρχεται το μήνυμα γνωρίζει τον προηγούμενο κόμβο από τον οποίο έλαβε το μήνυμα και για να τον θυμάται τον καταγράφει στον τοπικό πίνακα προώθησης που διατηρεί. Εφόσον το μήνυμα φτάσει στον προορισμό του, ο τελικός κόμβος (id, endpoint) και κάθε κόμβος του μονοπατιού ανακατασκευάζουν το μονοπάτι προς τον αποστολέα ώστε να προωθηθεί η απάντηση.

Όταν το μονοπάτι έχει δημιουργηθεί, ο παραλήπτης προσδιορίζει μία χρονική περίοδος κατά την οποία οι καταχωρημένοι κόμβοι θα πρέπει να παραμείνουν στους πίνακες προώθησης. Εάν κάποιο κανάλι λήξει τότε ο κόμβος αποστολέας μπορεί απλά να δημιουργήσει ένα νέο ανώνυμο μονοπάτι για να εξυπηρετήσει το ανώνυμο κανάλι. Σε περίπτωση που κάποιος κόμβος του μονοπατιού βρεθεί εκτός λειτουργίας ο κόμβος που έχει αποστείλει το μήνυμα δεν μπορεί να

λάβει πλέον μηνύματα από αυτό το μονοπάτι. Με τη δημιουργία ανώνυμου καναλιού διατηρείται η ανωνυμία του δέκτη επειδή κανένας κόμβος στο μονοπάτι δεν γνωρίζει αν ο κόμβος στον οποίον προωθούν τα μηνύματα είναι ο δημιουργός του καναλιού.

Ο χρήστης έχει την δυνατότητα απόκρυψης της πραγματικής ταυτότητάς του και αυθεντικοποίησης των μηνυμάτων χρησιμοποιώντας ψευδώνυμα. Παράγει λοιπόν ένα ζεύγος κλειδιών, δημόσιο και ιδιωτικό (K_{pub}, K_{pri}), που αντιστοιχεί σε ένα ψευδώνυμο. Κάθε κόμβος έχει την δυνατότητα παραγωγής παραπάνω από ενός ψευδώνυμου, ανάλογα με την απαίτηση. Όταν ο κόμβος δημιουργήσει ένα ψευδώνυμο εγκαθιστά ένα ανώνυμο κανάλι σε μία θέση $H(K_{pub})$ όπου Η είναι μία ασφαλής συνάρτηση κατακερματισμού. Ο κόμβος που θέλει να στείλει μήνυμα με ασφάλεια σε ένα ψευδώνυμο, κρυπτογραφεί το μήνυμα, χρησιμοποιώντας το δημόσιο κλειδί του ψευδώνυμου, και στέλνει το μήνυμα στο ανώνυμο κανάλι. Με αυτόν τον τρόπο διασφαλίζεται ότι μόνο ο χρήστης που του ανήκει το ψευδώνυμο μπορεί να διαβάσει το μήνυμα, αποτρέποντας άλλους κόμβους να το διαβάσουν.

Πλεονεκτήματα/Θετικά χαρακτηριστικά: Το AP3 παρέχει μια συνεργατική, διαμοιραζόμενη ανώνυμη υπηρεσία επικοινωνίας. Χτίστηκε πάνω από μη αξιόπιστους κόμβους και έχει την δυνατότητα να χειρίζεται ομαλά την άφιξη και την αναχώρηση κάθε κόμβου, παρέχοντας ένα ευέλικτο, ελαφρύ γενικό μηχανισμό για την ανώνυμη μονή εκπομπή (unicast) και την επικοινωνία της ομάδας [38].

Επίσης, όταν ένας κόμβος συνδέεται ή αφήνει το δίκτυο επικάλυψης (overlay network) απαιτεί πολύ μικρή επεξεργασία, με αποτέλεσμα το AP3 να παρέχει τη δυνατότητα στήριξης δικτύων με υψηλούς ρυθμούς κύκλων εργασιών των κόμβων.

***Ευπάθειες/μειονεκτήματα*:** Η απλότητα σχεδιασμού του AP3 το καθιστά ευάλωτο σε διάφορες επιθέσεις. Ένας κόμβος που παρακολουθείται παθητικά από κάποιον ωτακουστή ο οποίος παρατηρεί τα πακέτα που εισέρχονται και εξέρχονται από αυτόν μπορεί να συμπεράνει αν ο κόμβος είναι ο αποστολέας ή ο παραλήπτης του πακέτου. Επίσης, τα πακέτα δρομολογούνται προς τις ταυτότητες των κόμβων που είναι "κοντά" στο ID προορισμού με αποτέλεσμα οι κοντινοί κόμβοι να μπορούν να κρυφακούσουν και να συμπεράνουν τον παραλήπτη.

Το AP3 δημιουργεί στατικά μονοπάτια για την κατασκευή ανώνυμων καναλιών, δίνοντας κατ' αυτόν τον τρόπο τη δυνατότητα σε έναν εισβολέα να αποκτήσει πληροφορίες δρομολόγησης.

Υπάρχουν χρονικοί περίοδοι όπου κάποιοι κόμβοι που συμμετέχουν σε μονοπάτια μένουν εκτός λειτουργίας με αποτέλεσμα αυτό να αποτελεί σημείο ευπάθειας του δικτύου. Σε περίπτωση λοιπόν που ένας κόμβος με ένα ανώνυμο ψευδώνυμο δεν λειτουργεί για κάποιο χρονικό διάστημα, τότε όλα τα πακέτα που στέλνονται σε αυτό το ψευδώνυμο, δηλαδή σε αυτόν τον κόμβο, χάνονται. Ο εισβολέας μπορεί να συσχετίσει τα ερωτήματα για το ψευδώνυμο και τις περιόδους μη λειτουργίας του κόμβου. Για παράδειγμα, ο εισβολέας μπορεί να στέλνει συνεχώς ερωτήματα στο συγκεκριμένο ψευδώνυμο μέχρι να σταματήσει να λαμβάνει απάντηση, με αποτέλεσμα να συμπεραίνεται ποιοι κόμβοι έφυγαν από το δίκτυο.

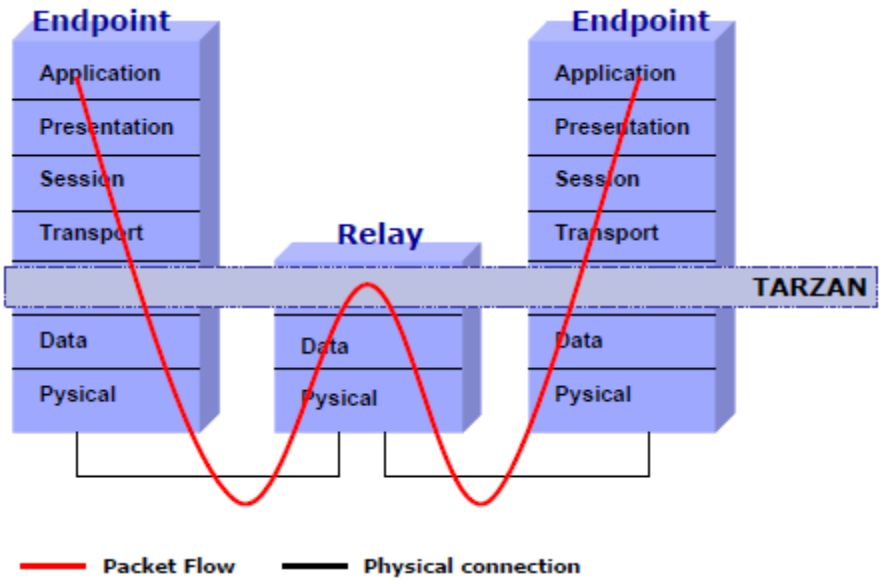
Το AP3 είναι ευπαθές σε επιθέσεις άρνησης υπηρεσίας (DoS). Για να συμβεί μια επίθεση άρνησης υπηρεσίας, ένας κακόβουλος κόμβος πρέπει να είναι σε κάποιο σημείο του μονοπατιού του πακέτου.

3.3.1.2 Tarzan

Το Tarzan είναι ένα peer-to-peer ανώνυμο στρώμα δικτύου (network layer) [27]. Στηρίχθηκε στην αρχιτεκτονική του Crowds αντλώντας αρκετά στοιχεία της λειτουργίας του. Παρέχει ανωνυμία σε διάφορες εφαρμογές, όπως η περιήγηση στο διαδίκτυο και ο διαμοιρασμός αρχείων, δημιουργώντας IP τούνελ μεταξύ των ανοιχτών (open-ended) συνόλων των peers, προσθέτοντας μία μικρή επιβάρυνση πάνω από μία αντίστοιχη, μη ανώνυμη διαδρομή επικάλυψης. Το Tarzan αποτελείται από ένα ανοιχτό σύνολο κόμβων χωρίς την ύπαρξη κάποιου κεντρικού, δίνοντας την δυνατότητα στους συμμετέχοντες κόμβους – πελάτες των εφαρμογών να επικοινωνήσουν με μη συμμετέχοντες εξυπηρετητές στο διαδίκτυο. Στο Tarzan, τα πακέτα δρομολογούνται μέσω τούνελ το οποίο δημιουργείται με την επιλογή τυχαίας σειράς από peers, χρησιμοποιώντας πολυεπίπεδη κρυπτογράφηση mix. Το ένα άκρο του τούνελ αποτελείται από έναν κόμβο που τρέχει μια εφαρμογή-πελάτη και το άλλο άκρο από έναν κόμβο που τρέχει την λειτουργία ενός μεταφραστή διεύθυνσης δικτύου. Ο τελευταίος κόμβος προωθεί την κίνηση του πελάτη στον τελικό προορισμό, έναν συνηθισμένο εξυπηρετητή του διαδικτύου. Στόχος της δημιουργίας του είναι, κυρίως, η χρησιμοποίηση του ως ένα υποκείμενο (underlying) στρώμα μεταφοράς με ανεκτή μείωση της αποδοτικότητας από διάφορες εφαρμογές, χωρίς την τροποποίησή τους, προσφέροντας ανωνυμία σε ικανοποιητικό βαθμό.

***Τεχνική Περιγραφή Λειτουργίας/Αρχιτεκτονική*:** Το Tarzan λειτουργεί στο στρώμα δικτύου (Nertwork Layer) υποκαθιστώντας το συνηθισμένο στρώμα – IP (Internet Protocol), χρησιμοποιώντας για τη μετάδοση των πακέτων πολυεπίπεδη κρυπτογράφηση, παρόμοια με τα

δίκτυα mix. Όπως απεικονίζεται στην εικόνα 3, τα συνηθισμένα πακέτα κατά την αναμετάδοσή τους, σύμφωνα με το μοντέλο διαστρωμάτωσης OSI, φτάνουν μέχρι το στρώμα δικτύου [47]. Ως αποτέλεσμα, οποιοδήποτε υψηλότερου επιπέδου πρωτόκολλο, συμπεριλαμβανομένου TCP και UDP, μεταδίδεται στο τούνελ με τον ίδιο τρόπο από το Tarzan.



Εικόνα 3: Στρωματοποίηση Μοντέλου OSI, ροή των πακέτων και στο στρώμα του Tarzan.

Κάθε κόμβος που επιθυμεί ανωνυμία ακολουθεί μία συγκεκριμένη διαδικασία αποτελούμενη από τρία στάδια. Πρώτον, εκτελεί μία εφαρμογή που επιλέγει ένα σύνολο από κόμβους οι οποίοι σχηματίζουν ένα μονοπάτι μέσω του δικτύου επικάλυψης. Δεύτερον, ο κόμβος αυτός που αποτελεί την πηγή δρομολόγησης, εγκαθιστά ένα τούνελ χρησιμοποιώντας τους επιλεγμένους κόμβους. Τρίτον, δρομολογεί τα πακέτα δεδομένων μέσω του εγκατεστημένου τούνελ. Το σημείο εξόδου του τούνελ είναι ένας NAT (Μεταφραστής Διευθύνσεων Δικτύου) ο οποίος προωθεί τα ανώνυμα πακέτα στους εξυπηρετητές οι οποίοι δεν γνωρίζουν σχετικά με το Tarzan.

Το Tarzan μεταδίδει στο τούνελ δύο διακριτούς τύπους μηνυμάτων, τα πακέτα δεδομένων και τα πακέτα ελέγχου τα οποία και ενθυλακώνει σε ένα UDP πακέτο. Τα πακέτα ελέγχου περιέχουν εντολές και απαντήσεις που εγκαθιστούν και διατηρούν τα τούνελ. Για την μετάδοση του πακέτου στο μονοπάτι προώθησης προς τον προορισμό, το σημείο εισόδου του τούνελ «καθαρίζει» την διεύθυνση IP της πηγής από το αντίστοιχο πεδίο της κεφαλίδας, εκτελεί μία ένθετη κρυπτογράφηση για κάθε άλμα (hop) στο τούνελ και ενθυλακώνει το αποτέλεσμα σε ένα UDP πακέτο [27]. Πιο συγκεκριμένα, αν το τούνελ αποτελείται από l κόμβους (h1, h2….., hl) και το κλειδί προώθησης για κάθε κόμβο είναι kh_i, ο αρχικός κόμβος παράγει το κρυπτογραφημένο

μπλοκ $\{\{....\{\{p\}_{khl}\}_{khl-1}.....\}_{kh2}\}_{kh1,}$ όπου p αποτελεί το πακέτο εισόδου. Είναι σημαντικό να επισημανθεί ότι μία ετικέτα ροής (flow tag) προσδιορίζει μοναδικά κάθε σύνδεσμο στο τούνελ (όπως στο MPLS). Συνεπώς, ο αρχικός κόμβος δεικτοδοτεί (tags) το μπλοκ που παράγει με το πρώτο αναγνωριστικό ροής και το προωθεί στον κόμβο h_1. Ο κόμβος h_1 αποκρυπτογραφεί τα δεδομένα, αφαιρώντας το ένα στρώμα της κρυπτογράφησης, δεικτοδοτεί ξανά το πακέτο (retags) και το προωθεί στον επόμενο κόμβο (άλμα) κ.ο.κ. μέχρι να φτάσει στον τελευταίο κόμβο του τούνελ ο οποίος αφαιρεί το τελευταίο στρώμα κρυπτογράφησης και αποκαλύπτεται η αρχική IP διεύθυνση του πακέτου.

Στο αντίστροφο μονοπάτι, ο κάθε κόμβος εκτελεί μία μοναδική κρυπτογράφηση με το αντίστοιχο αντίστροφο κλειδί, ξαναδεικτοδοτεί (retags) το πακέτο και το προωθεί πίσω στον αρχικό κόμβο με αποτέλεσμα ο κόμβος αυτός να εκτελεί τόσες αποκρυπτογραφήσεις όσες είναι αντίστοιχα και οι κρυπτογραφήσεις που εκτελέστηκαν από τον κάθε κόμβο του τούνελ.

Για τον σχηματισμό του τούνελ, το Tarzan επιλέγει τυχαία μία σειρά από υπάρχοντες κόμβους του δικτύου. Κάθε αναμεταδότης την πρώτη φορά που εισέρχεται στο δίκτυο παράγει τοπικά το δημόσιο κλειδί το οποίο και το δημοσιεύει, ενώ είναι ο μόνος που γνωρίζει το αντίστοιχο ιδιωτικό κλειδί. Το τούνελ δημιουργείται με επαναληπτικά άλματα (hop by hop). Για την εγκατάσταση κάθε άλματος στο τούνελ χρησιμοποιείται η ίδια διαδικασία. Ο αρχικός κόμβος h_1 στέλνει ένα ερώτημα εγκατάστασης με τη μορφή κανονικού πακέτου δεδομένων στον κόμβο h_i μέσω του κόμβου $h_{i-1,}$ συμπεριλαμβάνοντας το κλειδί αποκωδικοποίησης που θα χρησιμοποιήσει ο κόμβος h_{i-1} για να στείλει δεδομένα στον κόμβο $h_{i,}$ καθώς και το κλειδί κωδικοποίησης που θα χρησιμοποιήσει ο κόμβος h_i για τα πακέτα που θα λάβει από τον κόμβο h_{i+1}. Ο αρχικός κόμβος δημιουργεί το αίτημα εγκατάστασης χρησιμοποιώντας το δημόσιο κλειδί του h_i για να κρυπτογραφήσει το αρχικό κλειδί της συνόδου προώθησης και στη συνέχεια αυτό το κλειδί συνόδου χρησιμοποιείται για να κρυπτογραφήσει το μεταγενέστερο αντίθετο κλειδί, τις διευθύνσεις των κόμβων και τα αναγνωριστικά ροής. Όταν ο κόμβος h_i έχει επιτυχώς αποθηκεύσει την κατάσταση αυτού του αιτήματος απαντά στον αρχικό κόμβο με ένα end to end έλεγχο ορθότητας.

Το Tarzan, για την δημιουργία ανώνυμου τούνελ παρέχει για τον πελάτη έναν IP forwarder ο οποίος κρύβει την διεύθυνση IP και τον αριθμό της αρχικής θύρας (port) για τα TCP και UDP πακέτα των πελατών και τα αποστέλλει στο τούνελ, ενώ για τον εξυπηρετητή παρέχει έναν μεταφραστή διευθύνσεων δικτύου ψευδωνύμων (Pseudonymous Network Address Translator). Ο πελάτης μεταφράζει τη δική του διεύθυνση δικτύου σε μια τυχαία διεύθυνση που αποδίδεται

από τον PNAT από τον ανατεθειμένο χώρο ιδιωτικών διευθύνσεων. Ο PNAT μεταφράζει αυτή την ιδιωτική διεύθυνση σε μία από τις δικές του πραγματικές διευθύνσεις. Τα πακέτα απάντησης μεταφράζονται στην πραγματική τους διεύθυνση δύο φορές, μία σε κάθε τέλος του τούνελ [27].

Για την επιλογή των κόμβων το Tarzan χρησιμοποιεί τον αλγόριθμο αναζήτησης Chord [51]. Ο αλγόριθμος Chord είναι μία διαμοιραζόμενη συνάρτηση κατακερματισμού η οποία χαρτογραφεί τα κλειδιά σε κόμβους. Κάθε κόμβος Chord έχει ένα μοναδικό 160-bit αναγνωριστικό (ID) που λαμβάνεται με τον κρυπτογραφικό κατακερματισμό της IP διεύθυνσής του. Όλοι οι αναμεταδότες του Tarzan συμμετέχουν σε μοναδικό δακτυλίδι Chord. Οι νέοι αναμεταδότες λαμβάνουν μέρος στο δακτυλίδι επικοινωνώντας με έναν υπάρχων κόμβο για να ανακαλύψουν τους κατάλληλους γείτονες. Τα κλειδιά χαρτογραφούνται στο Chord σε ένα διάστημα 160-bit από μία καθολική συνάρτηση κατακερματισμού. Ο διάδοχος του κλειδιού είναι ο κόμβος με το μικρότερο ID που είναι μεγαλύτερο ή ίσο από το κλειδί. Η λειτουργία του Chord, lookup(K), ανακαλύπτει την διεύθυνση IP του διαδόχου του κλειδιού K με επαναληπτικές αποστολές Remote Procedure Calls στους κόμβους του δακτυλιδιού Chord μέχρι να φτάσουν στον επιθυμητό διάδοχο. Ένας κόμβος αποδοτικά επιλέγει έναν τυχαίο ομότιμο κόμβο (peer) παράγοντας ένα τυχαίο κλειδί αναζήτησης και βρίσκοντας τον διάδοχο αυτού του κλειδιού. Ο διάδοχος απαντάει με την IP διεύθυνση του και το δημόσιο κλειδί [27].

Πλεονεκτήματα/Θετικά χαρακτηριστικά: Το Tarzan παρέχει ανωνυμία σε επίπεδο IP και μπορεί να χρησιμοποιηθεί από διάφορες εφαρμογές προσδίδοντας στο δίκτυο χαμηλή καθυστέρηση. Η αρχιτεκτονική του ομότιμου δικτύου του Tarzan δεν απαιτεί κεντρική διαχείριση ή έλεγχο και οι κόμβοι έχουν τη δυνατότητα να συνδέονται και να αφήνουν το δίκτυο με δυναμικό τρόπο. Παρέχει ανωνυμία αποστολέα και παραλήπτη, ενώ η IP αρχιτεκτονική προώθησης που χρησιμοποιεί, επιτρέπει στους ανώνυμους εξυπηρετητές να αλληλεπιδρούν με τους πελάτες με τρόπο αφανή, εκτελώντας δυναμική μετάφραση ψευδώνυμων διευθύνσεων δικτύου και προώθηση θύρας.

Η δημιουργία του τούνελ είναι οδηγούμενη από τον πελάτη και με αυτό τον τρόπο επιτρέπει στους χρήστες να επιλέξουν και να δημιουργήσουν πιο αποδοτικά μονοπάτια. Επίσης, η δημιουργία των τούνελ επιτυγχάνεται με τυχαία επιλογή από ένα μεγάλο σύνολο ομότιμων κόμβων, με αποτέλεσμα ο αντίπαλος να μην μπορεί να προβλέψει τους κόμβους του τούνελ για να επιτεθεί. Τόσο οι παθητικοί ωτακουστές, όσο και οι κακόβουλοι συμμετέχοντες δεν μπορούν να ξεχωρίσουν εάν ένας κόμβος είναι ο εκκινητής του μηνύματος ή αν απλώς αναμεταδίδει το πακέτο.

Η κρυπτογράφηση που χρησιμοποιεί το Tarzan, ακολουθώντας τα δίκτυα mix, προστατεύει από την επίθεση κωδικοποίησης μηνύματος, καθώς επίσης και από άλλες επιθέσεις. Επίσης, ο μηχανισμός κάλυψης της κίνησης με την χρησιμοποίηση mimic κόμβων, ο έλεγχος ακεραιότητας και ο επανασχηματισμός ιδιωτικών συνδέσμων σε κάποια αποτυχία, και όχι ολόκληρων των μονοπατιών, προστατεύει σε ικανοποιητικό βαθμό από ένα σύνολο επιθέσεων.

***Ευπάθειες/μειονεκτήματα*:** Το Tarzan προσφέρει ανωνυμία σε επίπεδο δικτύου, αλλά δεν προσφέρει προστασία στα υψηλότερα επίπεδα δικτύου, με κίνδυνο την αποκάλυψη της πληροφορίας στο περιεχόμενο του ωφέλιμου φορτίου στο επίπεδο της εφαρμογής εάν δεν προστατευτεί από την εφαρμογή. Αυτό έχει ως αποτέλεσμα οι εφαρμογές που χρησιμοποιούν το Tarzan να πρέπει να εξασφαλίζουν την προστασία του περιεχομένου ώστε να μην τεθεί σε κίνδυνο από τους αντιπάλους. Ένας μη υποψιασμένος χρήστης θα πρέπει να χρησιμοποιήσει κάποιο εργαλείο ανωνυμοποίησης σε επίπεδο εφαρμογής για να εξασφαλίσει ανώνυμη επικοινωνία και μεταφορά δεδομένων στο Tarzan.

Επίσης, σε περίπτωση που ένας στατικός αντίπαλος διαφθείρει κάποιους κόμβους του συστήματος έχει τη δυνατότητα παρακολούθησης της συμπεριφοράς τους [26], όπως να διαβάζει πακέτα που εισέρχονται στους κόμβους που ελέγχει καθώς και να αναλύει τα δεδομένα, το μέγεθος, τους ρυθμούς και τον όγκο των μηνυμάτων. Ο αντίπαλος μπορεί να χρησιμοποιήσει την χρονική ανάλυση των πακέτων και να αποφασίσει αν τα πακέτα που αναμεταδίδονται από διαφορετικούς αναμεταδότες ανήκουν στο ίδιο τούνελ, αλλά δεν μπορεί να υπολογίσει την απόσταση που έχουν οι αναμεταδότες στο τούνελ. Επομένως, το Tarzan είναι ευάλωτο σε επιθέσεις χρονισμού αν και παρέχονται μηχανισμοί προστασίας.

3.3.2 Onion Routing Protocol

Το Onion routing αποτελεί ένα δίκτυο επικάλυψης προσφέροντας ανωνυμία στην επικοινωνία των μελών του και παρέχοντας ανωνυμία σε εφαρμογές που στηρίζουν την λειτουργία τους στο πρωτόκολλο TCP. Ο χρήστης επιλέγει ένα μονοπάτι στο δίκτυο που ονομάζεται κύκλωμα (“circuit”) στο οποίο κάθε κόμβος (“onion router”) γνωρίζει τον προκάτοχο και τον διάδοχό του, αλλά κανέναν άλλον κόμβο του μονοπατιού δρομολόγησης. Η κίνηση στο μονοπάτι αποτελείται από σταθερού μεγέθους κελιά. Ο κάθε onion router αφαιρεί ένα στρώμα κρυπτογράφησης από το κάθε κελί που διέρχεται από αυτόν με το συμμετρικό του κλειδί και το αναμεταδίδει στον μεταγενέστερο onion router κοκ. Αποτελεί σημαντικό πρωτόκολλο προστασίας της ιδιωτικότητας του χρήστη και παρέχει ικανοποιητική προστασία έναντι ισχυρών αντιπάλων.

Στοχεύει στην ασφαλή μεταφορά των δεδομένων στο δίκτυο, αποκρύπτοντας το περιεχόμενο που μεταφέρεται από την επίθεση των ωτακουστών και άλλων κακόβουλων αντιπάλων.

3.3.2.1 TOR

Το TOR αρχικά σχεδιάστηκε, υλοποιήθηκε και αναπτύχθηκε στα πλαίσια ενός έργου του εργαστηρίου ναυτικών ερευνών της Η.Π.Α., ως δεύτερη γενιά του Onion Routing, με σκοπό την προστασία της επικοινωνίας της κυβέρνησης [60]. Σήμερα χρησιμοποιείται καθημερινά από διάφορους ανθρώπους, από τον στρατό, από τους δημοσιογράφους κ.α. εξυπηρετώντας διάφορους σκοπούς. Αποτελεί μία circuit-based, χαμηλής καθυστέρησης, υπηρεσία ανώνυμης επικοινωνίας η οποία λειτουργεί στις υπάρχουσες υποδομές του διαδικτύου, δεν απαιτεί τροποποιήσεις του πυρήνα, απαιτεί μικρό συντονισμό ή συγχρονισμό μεταξύ των κόμβων και παρέχει μία λογική ανταλλαγή μεταξύ της ανωνυμίας, της χρηστικότητας και της αποτελεσματικότητας [22].

Τεχνική Περιγραφή Λειτουργίας/Αρχιτεκτονική: Το δίκτυο του TOR είναι ένα δίκτυο επικάλυψης. Δομικά στοιχεία του δικτύου TOR αποτελούν οι onion routers (ORs), onion proxies (OPs) και οι directory server. Το onion router λειτουργεί ως μια διεργασία επιπέδου χρήστη και κάθε OR διατηρεί μία TLS σύνδεση με κάθε άλλο onion router. Το onion router συνδέεται στους αιτούμενους προορισμούς και αναμεταδίδει τα δεδομένα. Κάθε OR διατηρεί ένα κλειδί – ταυτότητας μεγάλης διάρκειας και ένα κλειδί onion μικρής διάρκειας. Το κλειδί ταυτότητας το χρησιμοποιεί για να υπογράψει πιστοποιητικά TLS, τα ORs router descriptor (μία σύνοψη των κλειδιών, της διεύθυνσης, του εύρους ζώνης, της πολιτικής εξόδου κ.α.) και (από τους εξυπηρετητές καταλόγους) τους καταλόγους. Το κλειδί onion χρησιμοποιείται για να αποκρυπτογραφήσει αιτήματα των χρηστών, να εγκαταστήσει κυκλώματα και να διαπραγματευτεί τα ephemeral κλειδιά. Το πρωτόκολλο TLS εγκαθιστά ένα κλειδί συνδέσμου μικρής διάρκειας στην επικοινωνία μεταξύ των ORs. Γενικότερα, τα κλειδιά μικρής διάρκειας περιστρέφονται περιοδικά και ανεξάρτητα.

Κάθε χρήστης εκτελεί τοπικά ένα λογισμικό που ονομάζεται onion proxy για να ανακτήσει καταλόγους, να εγκαταστήσει κυκλώματα (circuits) στο διαδίκτυο και να διαχειριστεί συνδέσεις για τις εφαρμογές του χρήστη. Οι onion proxies δέχονται TCP streams και τα πολυπλέκουν (multiplex) στα κυκλώματα [22].

Οι directory servers διατηρούν πληροφορίες σχετικά με την κατάσταση του δικτύου. Το TOR χρησιμοποιεί ένα μικρό γκρουπ από έμπιστους onion routers που λειτουργούν ως directory servers και εντοπίζουν αλλαγές στην τοπολογία του δικτύου και στην κατάσταση των κόμβων, συμπεριλαμβανομένου τα κλειδιά και τις πολιτικές εξόδου. Κάθε directory server λειτουργεί ως HTTP server και οι πελάτες έχουν την δυνατότητα ανάκτησης της τρέχουσας κατάστασης του δικτύου και της λίστας των ORs. Επίσης, κάθε OR μπορεί να ανεβάσει πληροφορίες σχετικά με την κατάστασή του στον directory server δημοσιεύοντας υπογεγραμμένη δήλωση της κατάστασής του. Μόλις ο directory server λάβει αυτή την δήλωση ελέγχει εάν γνωρίζει το κλειδί ταυτότητας του OR. Εάν δεν το γνωρίζει δεν ανανεώνει τον κατάλογο με το συγκεκριμένο OR. Για να συμπεριληφθεί ένας καινούργιος OR στον directory server θα πρέπει να εγκριθεί από τον διαχειριστή του directory server. Η διαδικασία έγκρισης δεν έχει ακόμα αυτοματοποιηθεί [22].

Η επικοινωνία των onion routers μεταξύ τους αλλά και η επικοινωνία μεταξύ των onion router και των onion proxy πραγματοποιείται διαμέσου TLS συνδέσεων με την χρήση ephemeral κλειδιών. Στο δίκτυο του TOR η κίνηση μεταφέρεται με κελιά σταθερού μεγέθους 512 byte, τα οποία αποτελούνται από την κεφαλίδα και το ωφέλιμο φορτίο.

Η κεφαλίδα αποτελείται από:

- το αναγνωριστικό του κυκλώματος (circID) που προσδιορίζει το κύκλωμα στο οποίο αναφέρεται το κελί,
- μία εντολή που περιγράφει την ενέργεια που πρέπει να εκτελεστεί σχετικά με το ωφέλιμο φορτίο του κελιού.

Τα κελιά διαχωρίζονται σε:

- κελιά ελέγχου,
- κελιά αναμεταδότες τα οποία μεταφέρουν, άκρη-σε-άκρη, δεδομένα stream.

Οι εντολές των κελιών ελέγχου είναι:

- συμπλήρωση,
- δημιουργία (κυκλώματος)

- καταστροφή (κυκλώματος).

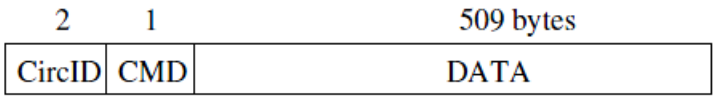
Τα κελιά αναμεταδότες έχουν:

- μια επιπρόσθετη κεφαλίδα (κεφαλίδα αναμετάδοσης) στην αρχή του ωφέλιμου φορτίου συμπεριλαμβάνοντας το streamID,
- έλεγχο αθροίσματος (άκρη-σε-άκρη) που χρησιμοποιείται για τον έλεγχο της ακεραιότητας,
- το μήκος του αναμεταδιδόμενου ωφέλιμου φορτίου,
- μία εντολή αναμετάδοσης.

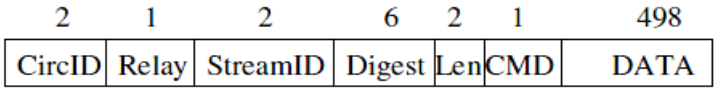
Ολόκληρο το περιεχόμενο της κεφαλίδας αναμετάδοσης και το κελί του ωφέλιμου φορτίου αναμετάδοσης, κρυπτογραφούνται και αποκρυπτογραφούνται μαζί, καθώς το κελί αναμετάδοσης μεταφέρεται στο κύκλωμα (circuit) χρησιμοποιώντας 128bit κρυπτογράφησης AES για την παραγωγή ενός κρυπτογραφημένου stream.

Οι εντολές αναμετάδοσης είναι:

- αναμετάδοση δεδομένων,
- αρχή αναμετάδοσης,
- καταστροφή αναμετάδοσης,
- συνδεδεμένη αναμετάδοση (για να ενημερώσει τον OP ότι μια αναμετάδοση που έχει ξεκινήσει έχει επιτύχει),
- επέκταση αναμετάδοσης (για να επεκτείνει το κύκλωμα ανά άλμα και για αναγνώριση),
- περικοπή αναμετάδοσης (για την καταστροφή ενός τμήματος του κυκλώματος και για γνωστοποίηση)
- αναμετάδοση αποστολής (sendme, για τον έλεγχο συμφόρησης)
- πτώση αναμετάδοσης (για την εφαρμογή long-range dummies).



Εικόνα 4: Πεδία Κελιού



Εικόνα 5: Πεδία Κελιού Αναμετάδοσης

Στο TOR, κάθε κύκλωμα που δημιουργείται μπορεί να χρησιμοποιηθεί από πολλά TCP streams. Για να αποφευχθούν οι καθυστερήσεις κατά την δημιουργία των κυκλωμάτων, οι OPs δημιουργούν κυκλώματα προληπτικά, ενώ για να περιορίσουν την συνδεσιμότητα μεταξύ των streams δημιουργούν καινούργια κυκλώματα περιοδικά εάν τα προηγούμενα έχουν χρησιμοποιηθεί και λήγουν τα παλιά κυκλώματα που δεν έχουν ανοιχτά streams. Οι OPs περιστρέφονται σε καινούργιο κύκλωμα ανά 1 λεπτό [22].

Ο OP του χρήστη δημιουργεί κυκλώματα "circuits" σταδιακά ακολουθώντας την παρακάτω διαδικασία (έστω ο OP αναφέρεται ως Alice):

- Η Alice στέλνει αρχικά κελί δημιουργίας (create) στον πρώτο κόμβο (έστω ότι αναφέρεται ως Bob) του μονοπατιού που έχει επιλέξει συμπεριλαμβάνοντας το circID: C_{AB} (επιλέγει κάποιο που δεν χρησιμοποιεί με την σύνδεσή της με τον Bob) και το ωφέλιμο φορτίο που περιέχει το πρώτο μισό της χειραψίας Diffie-Hellman (g^x) κρυπτογραφημένη με το onion κλειδί του onion router (Bob).

- Ο Bob ανταποκρίνεται με ένα κελί "created" συμπεριλαμβάνοντας το g^y με το διαπραγματευόμενο κλειδί $K=g^{xy}$.

- Μόλις εγκατασταθεί το κύκλωμα η Alice και ο Bob στέλνουν μεταξύ τους κρυπτογραφημένα κελιά αναμετάδοσης με το διαπραγματευόμενο κλειδί.

- Για την επέκταση του κυκλώματος η Alice στέλνει κελί επέκτασης αναμετάδοσης "relay extend cell" στον Bob προσδιορίζοντας την διεύθυνση του επόμενου OR (έστω ότι ονομάζεται Carol) και το κρυπτογραφημένο g^{x2}.

- Ο Bob αντιγράφει την μισή χειραψία στο κελί "create" και το στέλνει στον Carol για την επέκταση του κυκλώματος. Ο Bob επιλέγει ένα circID=C_{BC} το οποίο δεν χρησιμοποιεί με τον Carol και το οποίο δεν χρειάζεται να γνωρίζει η Alice.

- Όταν ο Carol ανταποκριθεί με το κελί "created" ο Bob αναδιπλώνει το ωφέλιμο φορτίο σε ένα κελί "relay extended" και το στέλνει στην Alice.

- Το κύκλωμα επεκτάθηκε έως τον Carol, η Alice και ο Carol μοιράζονται το κοινό κλειδί $K_2=g^{x2y2}$.

- Για περαιτέρω επέκταση του κυκλώματος η Alice ενεργεί κατά τον ίδιο τρόπο ενημερώνοντας τον τελευταίο κόμβο να στο κύκλωμα να επεκταθεί κατά έναν ακόμα κόμβο.

Για την αναμετάδοση των κελιών, εφόσον έχει εγκατασταθεί το κύκλωμα, η Alice δημιουργεί ένα κελί "relay" που προορίζεται να αποσταλεί σε μια συγκεκριμένη διεύθυνση, υπογράφει το digest (τα πρώτα 2 byte του ελέγχου ακεραιότητας) και κρυπτογραφεί διαδοχικά επαναλαμβανόμενα τα πεδία της κεφαλίδας και του ωφέλιμου φορτίου με τα συμμετρικά κλειδιά του κάθε OR του μονοπατιού. Όταν κάποιο OR παραλάβει ένα κελί "relay" ελέγχει το αντίστοιχα πεδίο circID και αποκρυπτογραφεί το ωφέλιμο φορτίο και την κεφαλίδα με το κλειδί συνόδου για αυτό το κύκλωμα. Για την καταστροφή ενός κυκλώματος η Alice στέλνει κελί ελέγχου "destroy".

Χαρακτηριστικό του δικτύου TOR αποτελεί η παροχή των κρυμμένων υπηρεσιών "hidden services". Το TOR επιτρέπει στους χρήστες του να προσφέρουν διάφορες υπηρεσίες TCP όπως έναν webserver χωρίς να αποκαλύψουν την IP διεύθυνση τους. Χρησιμοποιώντας τα "rendezvous points" του TOR οι άλλοι χρήστες του μπορούν να συνδεθούν στις κρυμμένες υπηρεσίες χωρίς να γνωρίζουν την ταυτότητα των άλλων στο δίκτυο [60].

Πλεονεκτήματα/Θετικά χαρακτηριστικά: Ο χρήστης στο δίκτυο του TOR, διαμέσου του λογισμικού που εκτελεί, δημιουργεί ένα μονοπάτι ιδιωτικού δικτύου με την σταδιακή εγκατάσταση ενός κυκλώματος αποτελούμενου από κρυπτογραφημένες συνδέσεις ανάμεσα

στους αναμεταδότες του δικτύου. Το κύκλωμα επεκτείνεται ανά ένα άλμα κάθε φορά και κάθε αναμεταδότης γνωρίζει μόνο τον προηγούμενο και τον επόμενο κόμβο του μονοπατιού. Πλεονέκτημα του δικτύου TOR, λοιπόν, αποτελεί το ότι κανένας αναμεταδότης δεν γνωρίζει ολόκληρο το μονοπάτι που ακολουθούν τα δεδομένα, με αποτέλεσμα να προστατεύει τους χρήστες από τους ωτακουστές και τους κακόβουλους αναμεταδότες που χρησιμοποιούν την ανάλυση της κίνησης για να συνδέσουν την πηγή με τον προορισμό [60].

Ο χρήστης διαπραγματεύεται σε κάθε άλμα του μονοπατιού ένα ξεχωριστό σύνολο από κρυπτογραφημένα κλειδιά διασφαλίζοντας τη μη ιχνηλάτιση των συνδέσεων [60]. Στο TOR, εφόσον εγκατασταθεί το κύκλωμα "circuit", μπορούν να αναπτυχθούν και να υποστηριχθούν διαφορές SOCKS εφαρμογές, διότι λειτουργεί με TCP streams, επιτυγχάνοντας την ανταλλαγή διαφόρων δεδομένων.

Ευπάθειες/μειονεκτήματα: Το TOR δεν προσπαθεί να λύσει όλα τα προβλήματα ανωνυμίας που προκύπτουν, αλλά επικεντρώνεται στην προστασία της μετάδοσης των δεδομένων. Στο δίκτυο του TOR δεν μπορούν να μεταδοθούν δεδομένα που βασίζονται σε nonstream πρωτόκολλα όπως το UDP. Σε αυτήν την περίπτωση θα χρειαστεί επιπλέον υπηρεσία η οποία δεν είναι διαθέσιμη. Επίσης το TOR δεν προσπαθεί να καλύψει ποιος συνδέεται στο δίκτυο και δεν προσφέρει προστασία ενάντια στους επιτιθέμενους που παρακολουθούν την κίνηση στα άκρα του δικτύου TOR π.χ. την κίνηση που εισέρχεται και εξέρχεται στο δίκτυο. Αν και αποτελεί ένα ανώνυμο σύστημα χαμηλής καθυστέρησης, παρ' όλα αυτά υπάρχουν καθυστερήσεις στην επικοινωνία των χρηστών του που είναι εμφανείς λόγω των εθελοντών κόμβων του δικτύου που βρίσκονται τοποθετημένοι σε διάφορες τοποθεσίες ανά τον κόσμο.

3.3.3 Υλοποιήσεις Δικτύων Mix

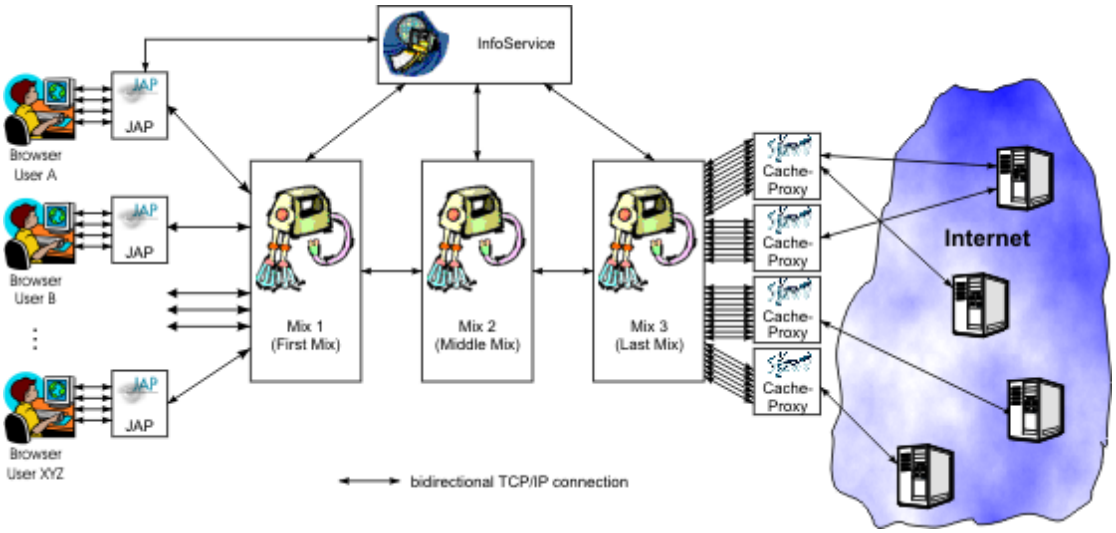
Αρκετοί μηχανισμοί προστασίας της ιδιωτικότητας αναπτύχθηκαν σε δίκτυα ομότιμων οντοτήτων και χρησιμοποίησαν ως λειτουργικό στοιχείο στην αρχιτεκτονική τους τους κόμβους mix. Παρατίθενται αναλυτικά οι μηχανισμοί JAP, Morphmix και I2P.

3.3.3.1 Java Anon Proxy (JAP)

Το JAP είναι ένα project ανοιχτού κώδικα του Πανεπιστημίου της Δρέσδης το οποίο υποστηρίζεται από το Ομοσπονδιακό Υπουργείο Οικονομικών. Πιο συγκεκριμένα, είναι ένα

πρόγραμμα το οποίο εγκαθίσταται στον υπολογιστή του χρήστη ως τοπικός πληρεξούσιος. Ο χρήστης ρυθμίζει κατάλληλα το πρόγραμμα περιήγησης που χρησιμοποιεί ώστε να χρησιμοποιήσει το JAP ως πληρεξούσιο, παρέχοντάς του ανωνυμία, δηλαδή διασφάλιση της επικοινωνίας με τον εξυπηρετητή χωρίς να αποκαλυφθεί η ταυτότητά του, καθώς αποκρύπτει τα δύο άκρα που επικοινωνούν ακόμα και από το στρώμα μεταφοράς (transport layer). Το JAP χρησιμοποιεί μία στατική διεύθυνση την οποία μοιράζεται με πολλούς χρήστες του. Με αυτό τον τρόπο αποκρύπτει την IP διεύθυνση του από την ιστοσελίδα που επισκέπτεται και προστατεύεται από κάποιον ωτακουστή [32].

***Τεχνική Περιγραφή Λειτουργίας/Αρχιτεκτονική*:** Το JAP λειτουργεί στο στρώμα της εφαρμογής. Η δομή της υπηρεσίας ανωνυμίας JAP απεικονίζεται σχηματικά στο ακόλουθο διάγραμμα.



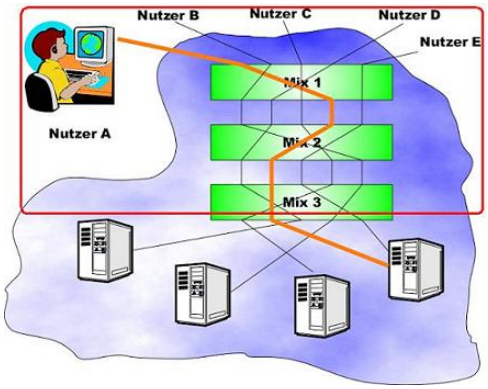
Εικόνα 6: Δομή λειτουργίας JAP

Με την εγκατάσταση του JAP ο χρήστης ρυθμίζει το πρόγραμμα περιήγησης που χρησιμοποιεί ώστε να στέλνει τα πακέτα των δεδομένων διαμέσου του JAP και όχι απευθείας στο διαδίκτυο. Επομένως συνδέεται με τον εξυπηρετητή διαμέσου μίας καθορισμένης ακολουθίας από κόμβους Mixes που ονομάζονται Cascade Mixes και έχει την δυνατότητα επιλογής ανάμεσα από διαφορετικές καθορισμένες ακολουθίες από κόμβους mix. Οι ενδιάμεσοι κόμβοι mix παρέχονται κυρίως από επίσημους οργανισμούς που δηλώνουν επισήμως ότι δεν κρατούν αρχεία log από τις συνδέσεις τους καθώς και δεν ανταλλάσουν δεδομένα αρχείων log με άλλους κόμβους mix [32]. Το JAP εμφανίζει την ταυτότητα και τον αριθμό των οργανισμών αυτών σε κάθε ακολουθία mix

cascade και επαληθεύει την πληροφορία με κρυπτογραφικά μέσα. Ο χρήστης έχει την δυνατότητα να επιλέξει αξιόπιστες ακολουθίες από Mix (mix cascade).

Ο χρήστης εκτελώντας το πρόγραμμα JAP στον υπολογιστή του, αρχικά συνδέεται με την υπηρεσία InfoService για να ελέγξει εάν η έκδοση που χρησιμοποιεί είναι ενημερωμένη. Στην περίπτωση που η έκδοση δεν είναι συμβατή με το πρόγραμμα των ενδιάμεσων κόμβων mixes ο χρήστης αναβαθμίζει την έκδοσή του ενώ στην αντίθετη περίπτωση η υπηρεσία του JAP δεν μπορεί να εκτελεστεί. Στη συνέχεια συνδέεται μόνιμα με τον πρώτο κόμβο mix μέχρι την αποσύνδεση του χρήστη. Το JAP κρυπτογραφεί τα δεδομένα που στέλνει με τα δημόσια κλειδιά των ενδιάμεσων κόμβων mixes και τα στέλνει στον πρώτο κόμβο mix, ο οποίος λαμβάνει τα πακέτα δεδομένων και από άλλους χρήστες που εκτελούν το JAP και αφαιρεί σε κάθε ένα από αυτά το ένα στρώμα κρυπτογράφησης τα αναδιατάσσει και τα στέλνει στον επόμενο κόμβο mix της ακολουθίας. Πρέπει να σημειωθεί ότι η ακολουθία των ενδιάμεσων mix είναι καθορισμένη με αποτέλεσμα η δρομολόγηση των πακέτων να είναι συγκεκριμένη και όχι ελεύθερη. Ο τελευταίος κόμβος mix αποκρυπτογραφεί πλήρως τα πακέτα που λαμβάνει και τα στέλνει στην κρυφή μνήμη του διαμεσολαβητή (proxy) ο οποίος αναλαμβάνει να τα στείλει στο διαδίκτυο, επίσης λαμβάνει απαντήσεις από τους εξυπηρετητές οι οποίες στέλνονται στον χρήστη με την αντίστροφη σειρά, διαμέσου της ίδιας ακολουθίας των κόμβων mixes.

Το JAP χρησιμοποιεί ισχυρή κρυπτογράφηση μεταξύ του υπολογιστή του χρήστη και των διακομιστών παρόχων του JAP κρυπτογραφώντας μόνο τα πακέτα δεδομένων ανάμεσα στον χρήστη και στους ενδιάμεσους κόμβους mix. Ο τελευταίος κόμβος mix στέλνει τα δεδομένα στον κατάλληλο εξυπηρετητή αποκρυπτογραφημένα. Στην παρακάτω εικόνα το κόκκινο περίγραμμα απεικονίζει το πλαίσιο κρυπτογράφησης του JAP [55].



Εικόνα 7: Πλαίσιο κρυπτογράφησης JAP

Πλεονεκτήματα/Θετικά χαρακτηριστικά: Το JAP παρέχει προστασία της διεύθυνσης IP του χρήστη ενάντια σε ισχυρούς αντιπάλους. Είναι εύκολο στην εγκατάσταση και στην χρήση του καθώς δεν απαιτεί ιδιαίτερες γνώσεις για την προστασία της ιδιωτικότητας.

Παρέχει προστασία από τους ωτακουστές οι οποίοι δύναται να παρακολουθήσουν το ένα σημείο του δικτύου ή να ελέγξουν έναν κόμβο mix [32].

Ο κάθε κόμβος mix συλλέγει τα πακέτα των χρηστών για μικρό χρονικό διάστημα και τα στέλνει στον επόμενο κόμβο με τυχαία σειρά προστατεύοντας με αυτό τον τρόπο τον χρήστη από διάφορες επιθέσεις συσχετισμού των πακέτων. Επίσης το JAP στέλνει σε τυχαία χρονικά διαστήματα ειδικά πακέτα, κρυπτογραφημένα, τα οποία αναγνωρίζονται από τον τελευταίο πληρεξούσιο και απορρίπτονται. Με αυτό τον τρόπο δημιουργεί εικονική κίνηση στο δίκτυο και αποτρέπει διάφορες επιθέσεις ανάλυσης της κίνησης καθώς και την καταμέτρηση των πακέτων από κάποιον αντίπαλο.

Το JAP παρέχει στον χρήστη μετρητή ανωνυμίας " anonym-o-meter", χρησιμοποιώντας λοιπόν, ως γνωστό, καθορισμένες διαδρομές από κόμβους mix (cascade) αθροίζοντας την κίνηση του χρήστη στο μοναδικό σημείο εισόδου της ακολουθίας και στο μοναδικό σημείο εξόδου της. Με αυτό τον τρόπο γνωστοποιεί στον χρήστη την κίνηση του δικτύου και πιο συγκεκριμένα τον αριθμό των χρηστών που χρησιμοποιούν την ίδια χρονική στιγμή, την ακολουθία των κόμβων mix (cascade) για την αποστολή των πακέτων.

Ευπάθειες/μειονεκτήματα: Μόνο δύο πρακτικές επιθέσεις είναι γνωστές εναντίον του JAP η (n-1) επίθεση δηλαδή η επίθεση όπου όλοι οι χρήστες συνεργάζονται εναντίων του ενός και στην περίπτωση που όλοι οι κόμβοι mix βρίσκονται υπό τον έλεγχο ενός εισβολέα [32].

Επιπλέον μειονέκτημα του JAP αποτελούν οι επιδόσεις του χρήστη στο διαδίκτυο οι οποίες είναι χαμηλότερες λόγω του ότι χάνετε λίγο εύρος ζώνης, μέσω του επιπλέον πρωτοκόλλου που χρησιμοποιείται και αυξάνετε η καθυστέρηση μετάδοσης σημαντικά [32].

3.3.3.2 Morphmix

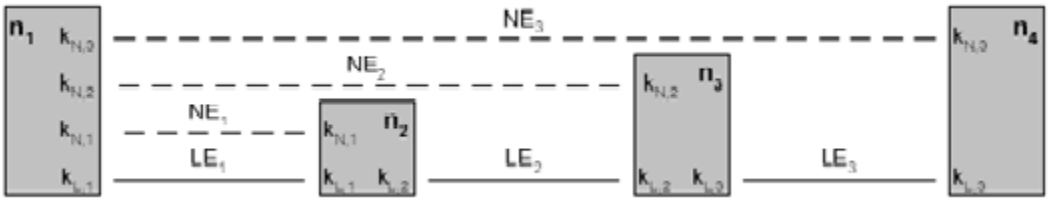
Το Morphmix είναι ένα ομότιμο, circuit – based, δίκτυο mix που στοχεύει στην παροχή ανώνυμης πρόσβασης στο διαδίκτυο με χαμηλή καθυστέρηση σε εκατομμύρια χρήστες [45]. Επιτρέπει λοιπόν σε εφαρμογές την ανώνυμη χρησιμοποίηση του διαδικτύου όπως είναι η περιήγηση στον

παγκόσμιο ιστό προσδίδοντας χαμηλή καθυστέρηση σε αυτές. Χαρακτηριστικό του Morphmix είναι το ότι κάθε χρήστης αποτελεί ταυτόχρονα και έναν κόμβο Mix με αποτέλεσμα να μην αποτελείται από καθορισμένους κόμβους αλλά από κόμβους που συμμετέχουν δυναμικά σε αυτό καθώς έχουν την δυνατότητα να εντάσσονται και να αποχωρούν από το δίκτυο οποιαδήποτε χρονική στιγμή.

***Τεχνική Περιγραφή Λειτουργίας/Αρχιτεκτονική*:** Το Morphmix αποτελείται από ένα ανοιχτό σύνολο από κόμβους όπου ο κάθε κόμβος i αναγνωρίζεται από την διεύθυνση ip_i. Επίσης κάθε κόμβος όταν τρέχει για πρώτη φορά στο δίκτυο του Morphmix παράγει ένα ζευγάρι κλειδιών το Δημόσιο κλειδί (PuKi) και το Ιδιωτικό (μυστικό) κλειδί (PrKi) [44]. Ο χρήστης προκειμένου να αποκτήσει πρόσβαση στο Internet ανώνυμα, εγκαθιστά ένα ανώνυμο τούνελ ξεκινώντας από τον ίδιο. Το ανώνυμο τούνελ αποτελείται από τον *εκκινητή κόμβο* τους *ενδιάμεσους κόμβους* και τον *τελικό κόμβο*.

Όλα τα μηνύματα που ανταλλάσσονται ανάμεσα στους κόμβους κρυπτογραφούνται όπως στην προτεινόμενη πολυεπίπεδη κρυπτογράφηση του Chaum [11] και έχουν το ίδιο μέγεθος. Η εικόνα 8 απεικονίζει την κρυπτογράφηση του μηνύματος {m} που αποστέλλεται από τον κόμβο n1 διαμέσου του ανώνυμου τούνελ και κρυπτογραφείται επαναλαμβανόμενα με τα συμμετρικά κλειδιά που αντιστοιχούν στις ένθετες κρυπτογραφήσεις $\{\{\{m\}_{kN,3}\}_{kN,2}\}_{kN,1}\}$. Η επικεφαλίδα του μηνύματος περιέχει ένα αναγνωριστικό του συνδέσμου μεταξύ των δύο κόμβων που εξυπηρετεί στην δρομολόγηση του μηνύματος στο τούνελ, επίσης περιέχει έναν αριθμό ακολουθίας και έναν τύπο για να διακρίνονται τα μηνύματα ελέγχου από τα μηνύματα δεδομένων.

Πριν αποσταλεί το μήνυμα από τον κόμβο n1 στον n2 η επικεφαλίδα κρυπτογραφείται σύμφωνα με το συμμετρικό κλειδί του συνδέσμου των δύο κόμβων $K_{L,1}$. Στη συνέχεια λαμβάνοντας ο κόμβος n2 το μήνυμα αφαιρεί την κρυπτογράφηση του συνδέσμου χρησιμοποιώντας το κλειδί $K_{L,1,}$ αφαιρεί ένα στρώμα κρυπτογράφησης χρησιμοποιώντας το κλειδί $K_{N,1}$, αποφασίζει για το επόμενο άλμα σύμφωνα με το αναγνωριστικό της επικεφαλίδας, θέτει τα πεδία στην επικεφαλίδα για τον επόμενο σύνδεσμο, κρυπτογραφεί την επικεφαλίδα σύμφωνα με το κλειδί του συνδέσμου μεταξύ των κόμβων n2 και n3, $K_{L,2,}$ και το στέλνει στον κόμβο n3. Αυτή η διαδικασία συνεχίζεται έως ότου φτάσει το μήνυμα στον τελικό κόμβο ο οποίος αναμεταδίδει τα δεδομένα στον τελικό εξυπηρετητή με τον οποίο ο χρήστης θέλει να επικοινωνήσει. Η απόκριση του εξυπηρετητή στον χρήστη στέλνεται πίσω στον κόμβο n1 ακολουθώντας την ίδια, αντίστροφη, διαδρομή με την διαφορά ότι κάθε κόμβος προσθέτει ένα στρώμα κρυπτογράφησης.



Εικόνα 8: Στρώματα κρυπτογράφησης

Αξιοσημείωτο είναι να αναφερθεί ότι το Morphmix υλοποιήθηκε ως δίκτυο Mix, επιπέδου εφαρμογής, χρησιμοποιώντας το πρωτόκολλο TCP για την μεταφορά των μηνυμάτων ανάμεσα στους κόμβους Mix.

Στο Morphmix ο κάθε κόμβος επιλέγει τον επόμενο κόμβο με αποτέλεσμα να γνωρίζει μόνο κάποιους κόμβους του δικτύου. Επίσης οι κόμβοι έχουν τη δυνατότητα να επικοινωνούν μεταξύ τους και να ανταλλάσσουν πληροφορία ελέγχου σχετικά με το αν έχουν ελεύθερους πόρους για να δεχτούν ένα νέο ανώνυμο τούνελ. Αυτή η δυνατότητα καθιστά το δίκτυο scalable εφόσον ο κάθε κόμβος διατηρεί μόνο το τοπικό περιβάλλον επικοινωνίας του δηλαδή τους κόμβους γείτονες του με τους οποίους είναι συνδεδεμένος.

Για την εγκατάσταση του συνδέσμου κρυπτογράφησης ανάμεσα σε δυο κόμβους προηγείται η TCP σύνδεση μεταξύ αυτών και στη συνέχεια ο πρώτος κόμβος, από αυτούς, επιλέγει ένα τυχαίο bit-string το οποίο εξυπηρετεί ως το συμμετρικό κλειδί για την κρυπτογράφηση του συνδέσμου. Το κλειδί κρυπτογραφείται με το δημόσιο κλειδί του δεύτερου κόμβου και στέλνεται σε αυτόν. Για να στηθεί μία ένθετη κρυπτογράφηση ανάμεσα στον κόμβο εκκινητή και στο επόμενο ενδιάμεσο κόμβο πρέπει να εγκατασταθεί το συμμετρικό κλειδί γνωστό μόνο στα δύο τελικά σημεία αυτών. Λόγω του ότι ο εκκινητής κόμβος δεν γνωρίζει τους άλλους κόμβους του τούνελ και επομένως τα δημόσια κλειδιά τους χρησιμοποιείται η Diffie-Hellman (DH) ανταλλαγή κλειδιών. Το Morphmix για να προστατεύσει την διαδικασία εγκατάστασης της ένθετης κρυπτογράφησης από κακόβουλους ενεργούς κόμβους χρησιμοποιεί την ιδέα του *μάρτυρα* κόμβου όπου σε κάθε άλμα ο εκκινητής επιλέγει έναν μάρτυρα τυχαία από τους κόμβους που γνωρίζει. Ο μάρτυρας έχει την ιδιότητα να ενεργεί ως τρίτο μέρος στη διαδικασία επιλογής του επόμενου άλματος ενός ανώνυμου τούνελ. Το θετικό στην διαδικασία αυτή είναι ότι ο δεύτερος κόμβος δεν γνωρίζει το μισό από το κλειδί που ανταλλάσσεται με τον πρώτο κόμβο αποτρέποντας έτσι τον δεύτερο κόμβο να υποκριθεί όλους τους επόμενους κόμβους καθώς

επίσης αποτρέπει τον δεύτερο κόμβο να επιλέξει το επόμενο άλμα. Αναλυτικά η διαδικασία περιγράφεται στο άρθρο [44].

Όπως αναφέρθηκε προηγουμένως στο Morphmix κάθε κόμβος στο τούνελ επιλέγει τον άμεσο διάδοχο στο τούνελ που εκτός από τα πλεονεκτήματα που προσθέτει στο δίκτυο έχει ως μειονέκτημα την επιλογή κακόβουλων κόμβων. Για να αντιμετωπίσει, λοιπόν, το Morphmix το πρόβλημα αυτό παρέχει τον μηχανισμό εντοπισμού σύγκρουσης ο οποίος βασίζεται στην υπόθεση ότι ο αντίπαλος μπορεί να χειριστεί κόμβους μόνο σε ένα μικρό σύνολο από όλα τα δημόσια /16 υποδίκτυα και ο μηχανισμός αυτός μπορεί να εντοπίσει επιλογές που περιέχουν πολλούς κακόβουλους κόμβους με υψηλή πιθανότητα. Εάν μία τέτοια επιλογή εντοπιστεί τότε το τούνελ θεωρείται κακόβουλο και απορρίπτεται από τον εκκινητή. Οι μη έντιμοι κόμβοι επιλέγουν τους γείτονες κόμβους από όλα τα /16 υποδίκτυα που περιέχουν κόμβους Morphmix [44].

Για την επίτευξη της επιλογής αυτής το Morphmix παρέχει τον μηχανισμό ανακάλυψης ομότιμων κόμβων βασιζόμενος στο ότι ο κάθε κόμβος αποθηκεύει την πληροφορία, σχετικά με τους άλλους κόμβους που έλαβε ως επιλογές, με τέτοιο τρόπο ώστε να επιτρέπει στους έντιμους κόμβους να επιλέξουν τους γείτονες κόμβους τους από ένα ευρύ φάσμα /16 υποδικτύων [42].

Πλεονεκτήματα/Θετικά χαρακτηριστικά: Στο Morphmix μπορεί να συμμετάσχει οποιοσδήποτε έχει πρόσβαση σε υπολογιστή με δημόσια διεύθυνση IP και είναι συνδεδεμένος στο διαδίκτυο. Το Morphmix μπορεί να χρησιμοποιηθεί για τον ανώνυμο διαμοιρασμό αρχείων, για FTP λήψεις αλλά σε περίπτωση που το τούνελ αποτύχει τα αρχεία θα πρέπει να ξαναληφθούν. Επίσης μπορεί να χρησιμοποιηθεί για την ενεργοποίηση ανώνυμης αναζήτησης και για τη λήψη αρχείων από άλλους ομότιμους κόμβους ομότιμων κοινοτήτων διαμοιρασμού αρχείων.

Η αποδοτικότητά του είναι ικανοποιητική παρόλη την ανομοιογένεια και την αναξιοπιστία των κόμβων και το δυναμικό περιβάλλον του και αντιμετωπίζει αποτελεσματικά έναν μεγάλο αριθμό από συμμετέχοντες κόμβους. Δεν χρησιμοποιεί κίνηση επικάλυψης και αυτό έχει ως αποτέλεσμα να μην επιβαρύνει το εύρος ζώνης.

Προστατεύει από τον αντίπαλο που ελέγχει αρκετούς κακόβουλους κόμβους και προσπαθεί να σπάσει την ανωνυμία των νόμιμων χρηστών και καθιστά δύσκολη την επίθεση της ανάλυσης

της κίνησης του δικτύου λόγω του μεγάλου φάσματος των κόμβων που ανήκουν σε διαφορετικά υποδίκτυα.

Ευπάθειες/μειονεκτήματα: Ο πιο σημαντικός περιορισμός του Morphmix είναι ότι σε περίπτωση που ένας κόμβος του τούνελ δεν λειτουργήσει σωστά τότε το τούνελ αποτυγχάνει έχοντας ως αποτέλεσμα όλη η ανώνυμη σχέση μεταξύ του εκκινητή και του εξυπηρετητή να τερματίζει. Επομένως το Morphmix δεν είναι κατάλληλο για μακροχρόνιες επικοινωνίες όπως απομακρυσμένες συνδέσεις.

Άλλο ένα πρόβλημα του Morphmix είναι η επίθεση άρνησης υπηρεσίας η οποία είναι αρκετά αποδοτική διότι εάν π.χ. αποτύχουν αρκετά τούνελ στο μισό χρονικό διάστημα κατά την λήψη ενός αρχείου η ποιότητα της υπηρεσίας που παρέχει το Morphmix μειώνεται με αποτέλεσμα οι χρήστες να μην το χρησιμοποιούν πλέον. Επίσης ένας αντίπαλος μπορεί να συμμετέχει με πολλούς κόμβους απλά για να διακόψει την υπηρεσία. Για να το επιτύχει αυτό δέχεται να εγκαταστήσει τούνελ που διέρχονται από αυτόν αλλά δεν δέχεται να προωθήσει τα δεδομένα ή σταματάει την μετάδοσή τους αφού το τούνελ έχει χρησιμοποιηθεί για μικρό χρονικό διάστημα.

Οι κόμβοι στο Morphmix συμμετέχουν με δυναμικό τρόπο με αποτέλεσμα ένας παρατηρητής να μην μπορεί να αποκτήσει καθολική εικόνα του δικτύου όμως εάν ο παρατηρητής παθητικά παρακολουθήσει τον κόμβο εκκινητή και τον τελευταίο κόμβο του τούνελ είναι σε θέση να παραβιάσει την ανωνυμία του χρήστη. Παρόλα αυτά όμως ο χρήστης μόλις μεταβεί σε άλλο τούνελ επανακτά την ανωνυμία του [43].

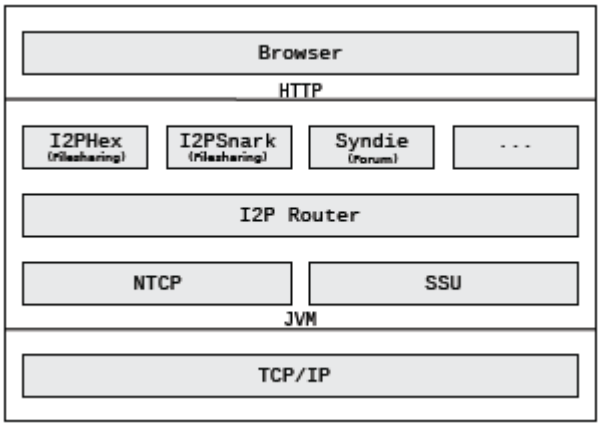
Επίσης το MorphMix προστατεύει από μακροχρόνιες επιθέσεις προφίλ, αλλά δεν εγγυάται την ανωνυμία της κάθε συναλλαγής [43].

3.3.3.3 I2P

Το I2P είναι ένα επεκτάσιμο, αυτό οργανωτικό, ανώνυμο στρώμα δικτύου μεταγωγής πακέτου (packet switched) στο οποίο μπορεί να λειτουργήσει ένας μεγάλος αριθμός από διαφορετικές ανώνυμες και ασφαλείς εφαρμογές όπως το Syndie ένα σύστημα ανώνυμου blogging και δημοσίευσης περιεχομένων, το I2P mail, το I2PSnark ένα σύστημα διαμοιρασμού αρχείων καθώς και άλλες εφαρμογές, επεκτείνοντας το και προσφέροντας τόσο λειτουργικότητα όσο και προστασία [63]. Αποτελεί, λοιπόν, ένα δίκτυο mix, χαμηλής καθυστέρησης, που χρησιμοποιεί, όπως το TOR [60], ως βάση για την παροχή ανώνυμων καναλιών επικοινωνίας, onion

δρομολόγηση για την δημιουργία τούνελ, ενσωματώνοντας ένα εύρος από ανώνυμες υπηρεσίες φιλοξενίας απευθείας με την πλατφόρμα του [33]. Το I2P αποτελεί μια προσπάθεια διαφόρων μηχανικών ανά τον κόσμο, χρηματοδοτούμενο από δωρεές και διαθέσιμο χωρίς περιορισμό σε όλους, για την κατασκευή, την ανάπτυξη και την διατήρηση της ανώνυμης και ασφαλής υποστήριξης του δικτύου και της επικοινωνίας των μελών του. Σχεδιάστηκε για να επιτρέπει στους ομότιμους κόμβους να το χρησιμοποιούν προκειμένου να επικοινωνούν μεταξύ τους ανώνυμα παρέχοντας ανωνυμία τόσο στον αποστολέα, στον παραλήπτη όσο και στα άλλα μέλη του επίσης.

Τεχνική Περιγραφή Λειτουργίας/Αρχιτεκτονική: Το I2P παρέχει ανωνυμία στους χρήστες διαμέσου ενός ανοιχτού δικτύου από δρομολογητές onion που εκτελούνται από εθελοντές [33]. Στην παρακάτω εικόνα παρατίθεται η αρχιτεκτονική του πλαισίου της πολυεφαρμογής I2P.



Εικόνα 9: I2P Αρχιτεκτονική

Το I2P δίνει την δυνατότητα χρησιμοποίησης, στην κορυφή του φυσικού Internet πρωτοκόλλου, δύο διαφορετικών πρωτοκόλλων μεταφοράς για ομότιμα δίκτυα το NIO-based TCP (NTCP), το NIO αναφέρεται στην νέα I/O βιβλιοθήκη της Java και το Secure Semireliable UDP (SSU) για την μεταφορά μηνυμάτων με το πρωτόκολλο UDP. Σημαντικός παράγοντας λειτουργίας του I2P αποτελεί ο δρομολογητής I2P που διατηρεί στατιστικά δεδομένα για τους ομότιμους κόμβους, εκτελεί την κρυπτογράφηση και την αποκρυπτογράφηση και δημιουργεί τα τούνελ στα οποία οι I2P εφαρμογές στηρίζουν την προστασία της ανωνυμίας τους. Σημαντικό είναι να σημειωθεί ότι πολλές διαδικτυακές εφαρμογές μπορούν να υλοποιηθούν πάνω από τον δρομολογητή I2P ενώ οι περισσότερες από αυτές ελέγχονται διαμέσου του φυλλομετρητή ιστού [33]. Η εφαρμογή που παρέχεται από κάποιο συγκεκριμένο ομότιμο κόμβο αναφέρεται ως υπηρεσία όπως η φιλοξενία

HTTP εξυπηρετητών, IRC επικοινωνία, μεταφορά ηλεκτρονικών μηνυμάτων βασιζόμενη στο POP/SMTP.

Χαρακτηριστικό στη λειτουργία του I2P αποτελεί η δομή δεδομένων routerInfo η οποία προσδιορίζει μοναδικά κάθε ομότιμο κόμβο του ομότιμου δικτύου και η leaseSet η οποία παρέχει την κατάλληλη πληροφορία στον δρομολογητή για την επικοινωνία του με έναν συγκεκριμένο προορισμό. Η routerInfo αποθηκεύει σημαντικές πληροφορίες σχετικά με τον ομότιμο κόμβο όπως τα δημόσια κλειδιά του, το 256bit αναγνωριστικό κατακερματισμού καθώς και το πώς ο ομότιμος κόμβο μπορεί να έρθει σε επαφή με άλλους κόμβους [33]. Η leaseSet περιέχει πληροφορίες για έναν συγκεκριμένο προορισμό και πιο συγκεκριμένα προσδιορίζει ένα σύνολο από σημεία εισόδου προς κάποια υπηρεσία. Τα σημεία εισόδου αποτελούν το αναγνωριστικό ενός εισερχομένου τούνελ προς τον ομότιμο κόμβο ο οποίος προσωρινά ενεργεί ως εισερχόμενη πύλη προς την υπηρεσία. Η routerInfo και η leaseSet αποτελούν ξεχωριστές οντότητες που αποθηκεύονται στην βάση δεδομένων netDB του δικτύου, στην οποία θα αναφερθούμε παρακάτω.

Το I2P αντιμετωπίζει το πρόβλημα της εύρεσης, αρχικά, άλλων ομότιμων κόμβων στο δίκτυο με την ανώνυμη HTTP λήψη, από μία συγκεκριμένη τοποθεσία, μίας λίστας από routerInfos που περιέχει τους διαθέσιμους I2P κόμβους. Αφού, λοιπόν, εντοπίσει τους ομότιμους κόμβους χρησιμοποιεί ένα super-peer διαμοιραζόμενο πίνακα κατακερματισμού (DHT) για να δημιουργήσει την netDB, μία βάση δεδομένων του δικτύου η οποία περιέχει πληροφορίες σχετικά με όλους τους ομότιμους κόμβους και τις υπηρεσίες του δικτύου που είναι διαθέσιμες. Οι super-peers [46] που διατηρούν την βάση δεδομένων netDB ονομάζονται floodfill peers και ο κάθε ένας είναι υπεύθυνος για την πληροφορία που βρίσκεται πλησιέστερα στο ID του. Η αναζήτηση και η αποθήκευση των routerInfos και των leaseSets πραγματοποιείται με την αποστολή αιτημάτων σε ένα floodfill εξυπηρετητή.

Χαρακτηριστικό στη λειτουργικότητα του I2P για την επίτευξη αμφίδρομης επικοινωνίας αποτελεί η δημιουργία εισερχόμενων (inbound) και εξερχόμενων (outbound) τούνελ για την μεταφορά του ωφέλιμου φορτίου. Το εισερχόμενο τούνελ χρησιμοποιείται για να μεταφέρει δεδομένα προς τον ομότιμο κόμβο για τον οποίο κατασκευάστηκε το τούνελ ενώ το εξερχόμενο τούνελ χρησιμοποιείται για να μεταφέρει δεδομένα από τον ομότιμο κόμβο για τον οποίο κατασκευάστηκε το τούνελ. Ο εκκινητής ομότιμος κόμβος επιλέγει την διαδρομή του μηνύματος το οποίο για να διέλθει από το εξερχόμενο τούνελ αρχικά κρυπτογραφείται σε πολλαπλά επίπεδα τα οποία το κάθε ένα από αυτά αφαιρούνται από τον αντίστοιχο ομότιμο κόμβο του

τούνελ που διέρχεται. Ενώ το μήνυμα που διέρχεται από το εισερχόμενο τούνελ προστίθεται σε αυτό από κάθε κόμβο του τούνελ ένα επίπεδο κρυπτογράφησης και αποκρυπτογραφείται από τον δημιουργό του τούνελ ο οποίος γνωρίζει τα κλειδιά του κάθε κόμβου του τούνελ.

Για την επιλογή των ομότιμων κόμβων στη δημιουργία των τούνελ το I2P τους κατηγοριοποιεί σε σειρές (tiers) με βάση συγκεκριμένα χαρακτηριστικά απόδοσης με πιο διακεκριμένες τις παρακάτω κατηγορίες:

- Fast – tier, κατατάσσονται οι ομότιμοι κόμβοι με υψηλό throughput.
- High – capacity tier, κατατάσσονται οι ομότιμοι κόμβοι που αποδέχονται με υψηλή πιθανότητα ένα αίτημα για τη δημιουργία τούνελ.

Ο εκκινητής κόμβος αφού επιλέξει τους ομότιμους κόμβους για τη δημιουργία του τούνελ τους στέλνει αίτημα οι οποίοι είτε αποδέχονται τη συμμετοχή τους στο τούνελ είτε την απορρίπτουν αναφέροντας τον λόγο απόρριψης. Η αποτυχία των τούνελ είναι σημαντικό κριτήριο ένταξης των κόμβων στην κατάλληλη σειρά (tier). Αξιοσημείωτο είναι να αναφερθεί πως όταν κάποιος ομότιμος κόμβος δεχτεί την συμμετοχή του στο τούνελ και αδυνατεί στην συνέχεια να διατηρήσει το τούνελ τότε οδηγεί σε αποτυχία του τούνελ. Το μήκος του τούνελ που δημιουργείται από τον εκκινητή ομότιμο κόμβο εξισορροπείται ανάμεσα στην ταχύτητα και την ανωνυμία δίνοντας στον χρήστη την δυνατότητα να ρυθμίσει αυτή την επιλογή.

Πλεονεκτήματα/Θετικά χαρακτηριστικά*:* Το I2P δίνει την δυνατότητα στους χρήστες να προστατεύουν την ανωνυμία τους συμμετέχοντας ενεργά σε ένα εχθρικό περιβάλλον. Οι ενέργειές τους καλύπτονται από την κίνηση των χρηστών που απαιτούν ανωνυμία σε μικρότερο βαθμό. Με αυτό τον τρόπο κάποιοι χρήστες προστατεύονται από πολύ ισχυρούς αντιπάλους σε ένα δίκτυο όπου τα μηνύματα των χρηστών δεν είναι ευδιάκριτα μεταξύ τους [63].

Ευπάθειες/μειονεκτήματα*:* Το I2P δεν παρέχει κάποιον κατάλληλο αλγόριθμο δρομολόγησης ώστε να αντιμετωπίσει την περίπτωση όπου οι περισσότεροι ομότιμοι κόμβοι είναι απρόσιτοι. Γι αυτό λοιπόν λειτουργώντας ως δίκτυο επικάλυψης πάνω σε ένα λειτουργικό δίκτυο μεταγωγής μπορεί να χρησιμοποιήσει έναν τέτοιο αλγόριθμο.

3.3.4 GNUnet Anonymity Protocol

Το GAP, GNUnet's Anonymity Protocol, είναι ένα πρωτόκολλο που προσφέρει ανωνυμία στην μεταφορά δεδομένων παρέχοντας σε κάθε κόμβο την δυνατότητα εξισορρόπησης της ανωνυμίας με την απόδοση συσχετίζοντάς τη με τις χαρακτηριστικές ανάγκες του. Χρησιμοποιείται κυρίως στο δίκτυο GNUnet, το οποίο αποτελεί ένα αποκεντροποιημένο, ανώνυμο δίκτυο ομότιμων κόμβων όπου οι χρήστες αναζητούν αρχεία, ιστοτόπους ή άλλα δεδομένα και εφόσον είναι διαθέσιμα σε αυτό τους παραδίδονται [17]. Ως κύρια χρήση του GAP [04] αποτελεί η αίτηση των αρχείων με ανώνυμο τρόπο στο δίκτυο GNUnet και στοχεύει στην προστασία του χρήστη από κάποιον αντίπαλο ο οποίος δεν μπορεί να αποδείξει τον αποστολέα ή τον παραλήπτη ενός μηνύματος που μεταδίδεται σε αυτό.

Τεχνική Περιγραφή Λειτουργίας/Αρχιτεκτονική: Στο δίκτυο GNUnet δεν υπάρχει κεντρικός κατάλογος υπηρεσίας και τα αρχεία που είναι διαθέσιμα σε αυτό αποθηκεύονται σε διαφορετικούς πελάτες με διαμοιραζόμενο τρόπο με αποτέλεσμα κανένας πελάτης να μην έχει αποθηκευμένο ολόκληρο το αρχείο αλλά ένα τμήμα του. Σε ένα πιο γενικό πλαίσιο το δίκτυο GNUnet παρέχει ανωνυμία σε αιτήσεις που στοχεύουν στους πόρους του δικτύου και όχι εκτός από αυτό. Η λειτουργία του πρωτοκόλλου GAP εστιάζεται κυρίως στην προστασία της ανωνυμίας για τον διαμοιρασμό αρχείων στο GNUnet δίκτυο.

Το GNUnet προσφέρει μηχανισμό εύρεσης άλλων ομότιμων κόμβων, κρυπτογράφηση συνδέσμων, message batching, αυθεντικοποίηση και χρησιμοποιεί ένα σύστημα κωδικοποίησης περιεχομένου το οποίο διασπά τα διαμοιραζόμενα αρχεία σε τμήματα του 1K τα οποία μεταδίδονται στο δίκτυο με τη χρήση του πρωτοκόλλου GAP. Οι κόμβοι επικοινωνούν μεταξύ τους με εμπιστευτικότητα και κανένας ξενιστής εκτός δικτύου δεν μπορεί να παρατηρήσει τα δεδομένα που ανταλλάσσονται μεταξύ των κόμβων καθώς και τον τύπο τους εφόσον όλα τα μηνύματα συμπληρώνονται και έχουν το ίδιο μέγεθος. Το GNUnet αποτελεί ένα αυστηρό, λοιπόν, δίκτυο ομότιμων κόμβων και κανένας κόμβος δεν έχει τη δυνατότητα ελέγχου όλου του δικτύου.

Το πρωτόκολλο GAP στοχεύει στην προστασία της ανωνυμίας του αποστολέα και του παραλήπτη από παθητικούς και ενεργούς αντιπάλους και από τους δρομολογητές του δικτύου GNUnet. Χαρακτηριστικό της λειτουργίας του αποτελούν οι δυσδιάκριτες ενέργειες μεταξύ της δημοσίευσης του περιεχομένου στο δίκτυο από τις ενέργειες απάντησης σε ερωτήματα καλύπτοντας έτσι η ανωνυμία του ανταποκριτή την ανωνυμία του εκδότη. Στοχεύει στην προστασία της ανωνυμίας εστιάζοντας στον μη συσχετισμό από κάποιον αντίπαλο του εκκινητή

κόμβου και της ενέργειας. Αυτό επιτυγχάνεται με την συμπεριφορά του εκκινητή κόμβου ως ενδιάμεσος κόμβος που απλά δρομολογεί δεδομένα. Επίσης αποτρέπει την άμεση δικτυακή σύνδεση του αποστολέα με τον παραλήπτη και διαφέρει από τα παραδοσιακά πρωτόκολλα mix που αντικαθιστούν την διεύθυνση πηγής σε κάθε άλμα. Οι κόμβοι που συμμετέχουν στο δίκτυο έχουν τη δυνατότητα να ορίζουν μία διεύθυνση επιστροφής διαφορετική από την δική τους.

Το GAP αποτελείται από δύο τύπους μηνυμάτων: τα ερωτήματα και τις απαντήσεις. Η ερώτηση αποτελείται από ένα αναγνωριστικό πόρων (Resource Identifier) και ένα αναγνωριστικό κόμβων (Node Identifier) που περιγράφει που πρέπει να αποσταλεί το μήνυμα σε αντίθεση με άλλα πρωτόκολλα όπως το Crowds και το Freenet στα οποία η απάντηση στέλνεται στον αποστολέα του ερωτήματος. Για την δρομολόγηση των μηνυμάτων χρησιμοποιεί το πεδίο time to live που παίρνει ψευδο-τυχαίες αρχικές τιμές οι οποίες μειώνονται από το πέρασμα κάθε δρομολογητή. Οι κόμβοι μεταξύ τους επικοινωνούν χρησιμοποιώντας κρυπτογράφηση ζεύξης (link encryption) και κάθε κόμβος συνδέεται με όσο το δυνατόν περισσότερους κόμβους. Το GAP ενημερώνεται για το αναγνωριστικό πόρου μίας ερώτησης από το επίπεδο εφαρμογής. Οι ερωτήσεις στο GAP είναι αναζητήσεις και στην περίπτωση που κάποιος πόρος δεν είναι διαθέσιμος και το ερώτημα δεν λάβει απάντηση για κάποιο χρονικό διάστημα τότε η ερώτηση αποστέλλεται ξανά έως ότου το επίπεδο εφαρμογής αποφασίσει για τον τερματισμό της λειτουργίας.

Ο κόμβος μόλις λάβει ένα ερώτημα το επεξεργάζεται με βάση την ακόλουθη διαδικασία [04]:

- Ελέγχει την διαθεσιμότητα της CPU και το εύρος ζώνης καθώς και τον ελεύθερο χώρο στον πίνακα δρομολόγησης και αποφασίζει εάν ο κόμβος είναι τελικά διαθέσιμος για την επεξεργασία του ερωτήματος. Σε περίπτωση που είναι απασχολημένος απορρίπτεται το ερώτημα.

- Προσδιορίζει εάν οι απαιτούμενοι πόροι είναι διαθέσιμοι τοπικά και σε περίπτωση διαθεσιμότητας τοποθετεί την απάντηση στην ουρά αποστολής του παραλήπτη που έχει οριστεί στο ερώτημα.

- Αποφασίζει σε πόσους κόμβους (n) θα στείλει το ερώτημα, εάν n>0 τότε μπαίνει στην ουρά για να αποσταλεί σε άλλους n κόμβους.

- Κάθε ουρά περιέχει ερωτήματα καθώς και απαντήσεις και μετά από ένα τυχαίο αλλά δεσμευμένο χρονικό διάστημα αποστέλλονται.

- Όταν παραλαμβάνεται μία απάντηση ελέγχεται ο πίνακας δρομολόγησης για το ταίριασμα του ερωτήματος και της ταυτότητας του επόμενου παραλήπτη. Η απάντηση τοποθετείται στην ουρά ή παραδίδεται το περιεχόμενο στο επίπεδο εφαρμογής. Εάν τα περιεχόμενα κρίνονται πολύτιμα, αντιγράφονται στον τοπικό αποθηκευτικό χώρο εφόσον είναι διαθέσιμος.

- Τα περιεχόμενα που βρίσκονται σε αποθηκευτικό χώρο και χρησιμοποιούνται σπάνια, διαγράφονται από αυτόν.

- Όταν το δίκτυο είναι ανενεργό στέλνονται τυχαία δεδομένα για την δημιουργία θορύβου στο υπόβαθρο.

Πλεονεκτήματα/Θετικά χαρακτηριστικά: Οι τεχνικές που χρησιμοποιεί το πρωτόκολλο GAP όπως η έμμεση αναφορά (indirection), οι καθυστερήσεις, η κρυπτογράφηση ζεύξης, η συμπλήρωση των μηνυμάτων ώστε να έχουν το ίδιο μέγεθος και ο διαμοιρασμός του περιεχομένου σε πολλούς κόμβους του δικτύου επιφέρουν ιδιαίτερα θετικά αποτελέσματα στην προστασία της ανωνυμίας των χρηστών του. Επίσης εφόσον το δίκτυο GNUnet αποτελεί ένα δίκτυο ομότιμων οντοτήτων στο οποίο ο κάθε κόμβος ελεύθερα συμμετέχει σε αυτό δεν διαδίδονται μηνύματα σε κόμβους που δεν αποτελούν τμήμα του δικτύου επικάλυψης (overlay) με αποτέλεσμα να μην προκύπτουν προβλήματα με τους κόμβους εξόδου του δικτύου που επικοινωνούν με τον τελικό παραλήπτη. Λόγω της μετανάστευσης του περιεχομένου, "content migration" ακόμα και αν αποκαλυφτεί η ταυτότητα του ανταποκριτή η ταυτότητα του εκδότη του περιεχομένου δεν αποκαλύπτεται με βεβαιότητα. Επίσης μία σκέψη που αυξάνει την αποδοτικότητα του δικτύου σε συνάρτηση με την εξασφάλιση της ανωνυμίας είναι ότι αυξάνοντας την απόδοση του συστήματος μειώνεται η ανωνυμία που προσφέρει στους χρήστες του αλλά το σύστημα γίνεται πιο εύχρηστο και επομένως αυξάνονται οι χρήστες του έχοντας ως αποτέλεσμα την αύξηση της κίνησης του δικτύου άρα και την καλύτερη προστασία της ανωνυμίας των χρηστών του.

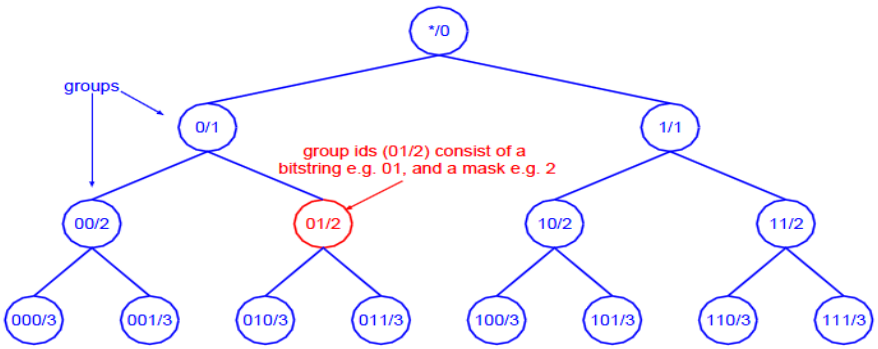
Ευπάθειες/μειονεκτήματα: Το πρωτόκολλο GAP έχει σχεδιαστεί για την προστασία της ανωνυμίας σε ένα συγκεκριμένο δίκτυο, το GNUnet και προσαρμόστηκε στην κάλυψη των αναγκών του δικτύου αυτού με αποτέλεσμα αυτή του η ιδιότητα να επιφέρει και την μεγαλύτερη αδυναμία του. Για παράδειγμα δεν μπορεί να εξασφαλίσει την παράδοση των πακέτων εφόσον σε περίπτωση υπερφόρτωσης οι κόμβοι αδειάζουν τους προσωρινά αποθηκευτικούς τους χώρους. Επίσης στο GNUnet δεν υπάρχει κάποιος χειριστής ως υπεύθυνος της λειτουργίας του δικτύου με αποτέλεσμα το ανοιχτό δίκτυο να γίνεται στόχος σε ισχυρούς

αντιπάλους στην διακοπή των διαδικτυακών συνδέσεων. Οι χρήστες διαμοιράζονται δεδομένα μεταξύ τους ώστε να αποκτήσουν διάφορα προνόμια και να αποδειχθούν νόμιμες οντότητες του δικτύου και αυτό έρχεται σε σύγκρουση με βασικές αρχές της ιδιωτικότητας όπως η απομόνωση [01].

3.3.5 P5 (Peer-to-Peer Personal Privacy Protocol)

Το P5, "Peer to Peer Personal Privacy Protocol", αποτελεί ένα πρωτόκολλο το οποίο εφαρμόζεται πάνω από το τρέχων διαδικτυακό πρωτόκολλο "Internet Protocol" και παρέχει ανωνυμία αποστολέα, παραλήπτη καθώς και αποστολέα – παραλήπτη [48]. Χαρακτηριστικό του πρωτοκόλλου αποτελεί η προσαρμοστικότητα του σε μια μεγάλη ανώνυμη ομάδα επιτρέποντάς τους την επιλογή του επιπέδου της ανωνυμίας που επιθυμούν συναλλάσσοντας το με την απόδοση της επικοινωνίας τους. Το πρωτόκολλο P5 μπορεί να παρέχει ανωνυμία σε εκατοντάδες χιλιάδες χρήστες που επικοινωνούν ταυτόχρονα.

Τεχνική Περιγραφή Λειτουργίας/Αρχιτεκτονική: Το πρωτόκολλο P5 δημιουργεί μία ιεραρχία των καναλιών μετάδοσης και εντάσσει τους χρήστες σε αυτά ανάλογα με το επίπεδο απόδοσης και ανωνυμίας που επιθυμούν. Παρέχει, λοιπόν, μία δομή ελέγχου για την ασφαλή και ανώνυμη σύνδεση των χρηστών σε ομάδες μετάδοσης διαφορετικών ιεραρχιών. Οι χρήστες οποιαδήποτε στιγμή μπορούν να μειώσουν το επίπεδο της ανωνυμίας που επιθυμούν και να αυξήσουν την αποδοτικότητα της επικοινωνίας τους. Το πρωτόκολλο P5 στηρίζεται στην κρυπτογραφία δημόσιου κλειδιού. Χρησιμοποιεί τα δημόσια κλειδιά, "communication keys" π.χ. K_0,……K_{N-1}, των κόμβων που θέλουν να επικοινωνήσουν ανώνυμα για να δημιουργήσει μία λογική ιεραρχία εκπομπής "logical broadcast hierarchy" . Η ιεραρχία εκπομπής είναι ένα δυαδικό δέντρο. Κάθε κόμβος του δυαδικού δέντρου αποτελείται από ένα bitstring συγκεκριμένου μεγέθους [48]. Για την αναπαράσταση των περιεχομένων μιας ομάδας χρησιμοποιείται ο συμβολισμός (b/m) όπου b απεικονίζει το bitstring και m απεικονίζει την μάσκα η οποία διευκρινίζει τον αριθμό των έγκυρων πιο σημαντικών bit του bitstring. Στην παρακάτω εικόνα απεικονίζεται το λογικό δέντρο μετάδοσης.



Εικόνα 10: Λογικό δέντρο μετάδοσης

Η εικονική δομή της εικόνας 10 βρίσκεται πάνω από την υφιστάμενη τοπολογία του διαδικτύου. Όπως παρατηρείται στην εικόνα η ρίζα του δέντρου απεικονίζεται ως (*/0) και αποτελείται από ένα άδειο (null) bitstring και μάσκα μηδενικού μήκους [48]. Το αριστερό παιδί της ρίζας του δέντρου περιέχει την ομάδα (0/1) και το δεξί την ομάδα (1/1) και το υπόλοιπο δέντρο συμπληρώνεται όπως απεικονίζεται στην εικόνα 10. Π.χ. η ομάδα (01/2) αναπαριστά το bitstring 01. Κάθε ομάδα αντιστοιχεί σε ένα κανάλι μετάδοσης του P5. Κάθε μήνυμα που στέλνεται σε μία ομάδα προωθείται και σε άλλες υποομάδες του συστήματος διενεργώντας πρώτα τον έλεγχο "min-common-prefix check". Αν π.χ. ο χρήστης A στείλει ένα μήνυμα στην ομάδα (b/m) τότε αυτό θα προωθηθεί στον χρήστη B (b'/m') αν και μόνο αν τα k πιο σημαντικά bit του b και του b' είναι τα ίδια, όπου k=min{m, m'}, γενικότερα η προώθηση στην ομάδα (b'/m') ενεργείται όταν έχουν μία σχέση προγόνου – απογόνου [48]. Κάθε χρήστης στο σύστημα συνδέεται με ένα σύνολο από τις προαναφερθείσες ομάδες μετάδοσης. Παρατηρείται ότι η αποδοτικότητα της επικοινωνίας αυξάνεται όσο αυξάνεται το μέγεθος της μάσκας των ομάδων ενώ μειώνεται το επίπεδο της ανωνυμίας των χρηστών.

Οι χρήστες απεικονίζονται στο λογικό δέντρο με τη χρήση μιας συνάρτησης κατακερματισμού των δημόσιων κλειδιών τους (H(.)). Όταν κάποιος χρήστης π.χ. η "Alice" συνδέεται στο σύστημα υπολογίζει "bAlice = H(PKAlice)" και επιλέγει μία τιμή mAlice ώστε να ισχύει: Lmin≤k≤ Lmax όπου k είναι ο αριθμός των χρηστών στο κανάλι (bAlice, mAlice), Lmin είναι το μικρότερο αποδεκτό μέγεθος ανώνυμου καναλιού και Lmax είναι το μεγαλύτερο αποδεκτό μέγεθος ανώνυμου καναλιού [48].

Το πρωτόκολλο P5 για να αντιμετωπίσει διάφορες παθητικές επιθέσεις προσθέτει στο σύστημα θόρυβο. Κάθε χρήστης στέλνει μηνύματα συγκεκριμένου μεγέθους σε κάποιο κανάλι που επιλέγει τυχαία. Επομένως κάθε κόμβος προωθεί είτε πακέτα θορύβου ή σήματος που έχει

παράγει ο ίδιος τοπικά είτε προωθεί πακέτα που λαμβάνει από κάποια διεπαφή σε κάποιο άλλο κανάλι. Επίσης εάν κάποιος κόμβος δεν έχει το κατάλληλο εύρος ζώνης ή την ικανότητα επεξεργασίας του λαμβανόμενου μηνύματος μπορεί να το απορρίψει εκτελώντας τον αλγόριθμο "dropping".

Πλεονεκτήματα/Θετικά χαρακτηριστικά: Το πρωτόκολλο P5 προσφέρει ανώνυμη επικοινωνία στο διαδίκτυο παρέχοντας ανωνυμία αποστολέα και παραλήπτη. Σχεδιάστηκε ως συμβατό με υπάρχον διαδικτυακά πρωτόκολλα (Internet protocols) και στοχεύει στην δημιουργία ενός επεκτάσιμου επιπέδου δικτύου (network layer) πάνω από το IP. Επιτρέπει σε ιεραρχημένες μικρές ομάδες μετάδοσης να συνδέονται με ασφαλή και ανώνυμο τρόπο. Κάθε χρήστης έχει τη δυνατότητα να ανταλλάξει το επίπεδο ανωνυμίας που επιθυμεί με την αποδοτικότητα της επικοινωνίας του στο δίκτυο. Τα πακέτα λόγω του ότι έχουν το ίδιο μέγεθος δεν είναι ευδιάκριτα σε σχέση με το περιεχόμενό τους εκτός από την πηγή και τον προορισμό ενώ από τους άλλους κόμβους αντιμετωπίζονται όπως και τα πακέτα δεδομένων.

Ευπάθειες/μειονεκτήματα: Το πρωτόκολλο P5 αν και παρέχει μηχανισμούς αντιμετώπισης ενός εύρους από παθητικές επιθέσεις παρ όλα αυτά αποτυγχάνει σε ενεργές επιθέσεις από ισχυρούς αντιπάλους. Αποτελεί τα πρώτα βήματα σχεδιασμού ενός επεκτάσιμου πρωτοκόλλου πάνω από τα τρέχοντα πρωτόκολλα διαδικτύου και χρειάζεται περαιτέρω έρευνα προς την αποτελεσματική αντιμετώπιση διαφόρων αντιπάλων που στοχεύουν στην παραβίαση της ανωνυμίας του χρήστη. Προσδίδει καθυστέρηση στο δίκτυο και δεν είναι κατάλληλο για την μεταφορά μεγάλων αρχείων.

3.3.6 Herbivore

Το Herbivore αποτελεί ένα πρωτόκολλο που παρέχει ανώνυμη επικοινωνία σε δίκτυα ομότιμων οντοτήτων [30]. Εκτελείται σε dining cryptography δίκτυα "DCnets", παρέχοντας ισχυρή ανωνυμία στους χρήστες. Προσφέρει ανωνυμία αποστολέα και παραλήπτη αποκρύπτοντας την ταυτότητα τους, προσαρμόζεται και ανταποκρίνεται αποδοτικά σε ένα μεγάλο αριθμό χρηστών επιτυγχάνοντας υψηλό εύρος ζώνης και χαμηλή καθυστέρηση. Επίσης προστατεύει τους χρήστες του ενάντια σε ισχυρούς αντιπάλους με απεριόριστες δυνατότητες υποκλοπών και παραβίασης της ανωνυμίας τους. Χαρακτηριστικό γνώρισμά του αποτελεί η αποδοτικότητα και η επεκτασιμότητα του. Οργανώνει το δίκτυο σε μικρά ανώνυμα cliques χρησιμοποιώντας μία αποκεντροποιημένη προσέγγιση ομότιμων οντοτήτων, παρέχοντας ανώνυμη επικοινωνία με αποδοτικό τρόπο και αποτρέποντας κάποιον αντίπαλο να παραβιάσει την ανωνυμία των

χρηστών του. Χρησιμοποιεί ως υπόστρωμα την υπάρχουσα μη αξιόπιστη δομή του διαδικτύου και διαρθρώνεται ως δίκτυο επικάλυψης σε αυτό.

Τεχνική Περιγραφή Λειτουργίας/Αρχιτεκτονική: Το Herbivore παρέχει δύο σημαντικούς μηχανισμούς λειτουργίας του, το πρωτόκολλο round και τον αλγόριθμο global topology control. Το πρωτόκολλο round, λειτουργεί στο χαμηλότερο επίπεδο και καθορίζει τον τρόπο με τον οποίο στέλνονται τα bits ανάμεσα στους συμμετέχοντες κόμβους [30]. Προσδίδει αποδοτικότητα στο σύστημα επεκτείνοντας το βασικό σχήμα του DCnet, εντοπίζει παραβιάσεις του συστήματος και διευκολύνει τις συναλλαγές, μεγάλης διάρκειας, των χρηστών. Η αποδοτικότητά του είναι αντιστρόφως ανάλογη με τον αριθμό των ταυτόχρονων ενεργών συνόδων.

Ο αλγόριθμος global topology control χωρίζει το δίκτυο σε μικρότερα ανώνυμα cliques. Με αυτόν τον τρόπο ενεργεί θετικά στην ανταπόκριση του πρωτόκολλο στο απεριόριστων διαστάσεων διαδίκτυο και στην αντιμετώπιση των κακόβουλων κόμβων. Κάθε clique αποτελείται από έναν προκαθορισμένο αριθμό k κόμβων ο οποίος αντιστοιχεί στον βαθμό ανωνυμίας που προσφέρει το σύστημα. Για την καλύτερη απόδοση του συστήματος όταν ο αριθμός των κόμβων που συμμετέχουν σε ένα clique μεγαλώσει αρκετά τότε αυτόματα δημιουργούνται καινούρια cliques ενώ αντίθετα όταν ο αριθμός των κόμβων ενός clique μειωθεί κάτω από τον προκαθορισμένο αριθμό κατωφλίου (k) τότε οι κόμβοι που το απαρτίζουν αναδιανέμονται σε όλο το δίκτυο. Το Herbivore προκειμένου να αποτρέψει τους αντιπάλους που στοχεύουν στην υπονόμευση του αλγορίθμου global topology control παρέχει το πρωτόκολλο ελέγχου ασφαλής εισόδου.

Καθοριστική σημασία στην γενική τοπολογία του Herbivore έχουν τα πρωτόκολλα ελέγχου εισόδου και συντήρησης. Το πρώτο αναθέτει τους νέους κόμβους του δικτύου σε clique και το δεύτερο αναδιατάσσει τους υπάρχων κόμβους στα clique ανάλογα με την αύξηση ή την μείωση των συμμετεχόντων. Ο κόμβος σύμφωνα με το πρωτόκολλο ελέγχου εισόδου “entry control protocol” δεν αποφασίζει σε ποιο clique θα συμμετάσχει. Στο Herbivore κάθε κόμβος έχει ένα μοναδικό κλειδί “node key” και κάθε clique έχει ένα μοναδικό κλειδί “clique key” έστω f και g αντίστοιχα οι συναρτήσεις που το παράγουν [30]. Για να εισέλθει στο δίκτυο ο νέος κόμβος παράγει ένα ζευγάρι κλειδιών το ιδιωτικό (Kprivate) και το δημόσιο (Kpublic). Στη συνέχεια παράγει τυχαίους φορείς (vectors) έως ότου βρει ένα y≠ Kpublic στο οποίο τα m_k μικρότερης σημασίας bits του f(Kpublic) να είναι ίδια με τα αντίστοιχα bits της f(y). Ο κόμβος εισέρχεται στο δίκτυο με το κλειδί που προκύπτει από την συνάρτηση g=(Kpublic, y) και στην συνέχεια το πλησιέστερο αριθμητικά κλειδί clique (clique key) στο κλειδί του κόμβου αποτελεί το clique στο οποίο εντάσσεται ο κόμβος. Για την ένταξη του κόμβου στο πλησιέστερο clique δεδομένου του

κλειδιού χρησιμοποιείται το off-the-shelf Chord protocol [51, 31]. Στη συνέχεια κάθε κόμβος του clique επαληθεύει την ορθότητα συμμετοχής του κόμβου υπολογίζοντας το f(Kpublic) και f(y) από το ζεύγος κλειδιών (Kpublic, y) που έχει γνωστοποιήσει ο κόμβος και επιβεβαιώνεται με αυτόν τον τρόπο αν τα mk bit ταιριάζουν και επίσης ελέγχουν αν το κλειδί g(Kpublic, y) του κόμβου αντιστοιχεί στο clique που συμμετέχουν. Εάν το (Kpublic, y) έχει παρουσιαστεί από άλλον συμμετέχοντα κόμβο τότε απορρίπτεται η είσοδος του κόμβου αυτού. Για την τελική αποδοχή του κόμβου το clique παράγει ένα τυχαίο vector v_{chat} και τον στέλνει στον νεοεισερχόμενο κόμβο ο οποίος παράγει ως απόκριση έναν vector (v_{resp}=Kprivate(v_{chat})). Όταν το clique επιβεβαιώσει ότι Kpublic(v_{resp})=v_{chat} μόνο τότε γίνεται αποδεχτός ο κόμβος στο clique. Με αυτή τη διαδικασία ένταξης ενός συμμετέχοντα κόμβου στο clique το Herbivore προστατεύει τον χρήστη από διάφορους αντιπάλους παραβίασης της ιδιωτικότητάς του.

Για την αύξηση του επιπέδου ασφαλείας οι κόμβοι δεν επιλέγουν τυχαία το y αλλά είναι αποτέλεσμα της κωδικοποίησης των λιγότερης σημασίας bits με την ημερομηνία. Το Herbivore προκειμένου να εξασφαλίσει την ασφάλεια της ανωνυμίας λόγω του ότι οι κόμβοι εισέρχονται και αποχωρούν από το δίκτυο σε διάφορες χρονικές στιγμές, διατηρεί τον αριθμό των συμμετεχόντων στα clique από k έως προσεγγιστικά 3k. Επίσης με την αύξηση του αριθμού των συμμετεχόντων κόμβων σε ένα clique μειώνεται η απόδοση του δικτύου, γι αυτό το Herbivore διαιρεί το clique σε μικρότερα clique για την αύξηση της απόδοσης και την εξασφάλιση υψηλού επιπέδου ανωνυμίας.

Στο Herbivore η συμπεριφορά των κόμβων καθορίζεται από το πρωτόκολλο round το οποίο διασφαλίζει την ανώνυμη μετάδοση των δεδομένων, το εύρος ζώνης εκπομπής τους καθώς και την ανίχνευση παραβίασης. Σε κάθε round ένας καθορισμένος αριθμός από δεδομένα που αντιστοιχούν σε πακέτα μεταφέρονται ανώνυμα σε διαδοχικά αριθμημένα slot καθώς για την μετάδοση των δεδομένων στα δίκτυα DCnet απαιτείται ένας τυχαίος αριθμός από stream. Το πρωτόκολλο round αποτελείται από τρεις φάσεις: 1η είναι η φάση δέσμευσης "reservation phase" στην οποία ανατίθεται σε κάθε κόμβο αντίστοιχα slots μετάδοσης ώστε να μειωθούν οι συγκρούσεις και να βελτιωθεί η αξιοποίηση του εύρους ζώνης, 2η είναι η φάση μετάδοσης "transmission phase" στην οποία μεταδίδονται τα δεδομένα και 3η η φάση είναι εξόδου "exit phase" στην οποία οι συναλλαγές μεγάλης διάρκειας προστατεύονται από την ανάλυση της κίνησης.

Τα ανώνυμα clique διατάσσονται σε τοπολογία αστεριού και αποτελούν ένα πλήρως συνδεδεμένο γράφημα όπου ο κάθε κόμβος έχει ένα διαμοιραζόμενο κλειδί και ένα αντίστοιχο

τυχαίο bit stream με κάθε άλλο συμμετέχοντα. Κάθε κόμβος μεταδίδει το XOR από το δικό του κλειδί του stream και το μήνυμά του στο κέντρο του αστέρα ο οποίος στη συνέχεια μεταδίδει το αποκρυπτογραφημένο μήνυμα σε κάθε k-1 συμμετέχοντα κόμβο [30].

Πλεονεκτήματα/Θετικά χαρακτηριστικά: Το Herbivore παρέχει ανωνυμία, επεκτασιμότητα και αποδοτικότητα σε ένα σύστημα ομότιμων οντοτήτων καθώς και ένα ανώνυμο κανάλι επικοινωνίας σε πολλές εφαρμογές. Λειτουργεί ως ένα εικονικό πρωτόκολλο επιπέδου δικτύου "network layer" και μεταφέρει ενσωματωμένη κίνηση IP στο ανώνυμο στρώμα [30]. Έχει την δυνατότητα υποστήριξης πολλών εφαρμογών με ελάχιστη ή καθόλου τροποποίηση του υπάρχοντος δικτυακού πρωτοκόλλου. Προστατεύει τον χρήστη από επιθέσεις publishing.

Το Herbivore χρησιμοποιεί την ανωνυμία που παρέχεται από τα DCnet δίκτυα και σε συνδυασμό των φάσεων reservation και exit αυξάνει αποδοτικά το εύρος ζώνης καθώς και διευκολύνει την ανώνυμη διεξαγωγή επικοινωνιών μεγάλης διάρκειας μεταξύ των συμμετεχόντων κόμβων. Επίσης διαχωρίζει το δίκτυο σε μικρότερα clique χρησιμοποιώντας τους αποκεντροποιημένους αλγορίθμους ελέγχου εισόδου και συντήρησης των clique επιτυγχάνοντας την προστασία της ανωνυμίας των χρηστών.

Προσφέρει υψηλό εύρος ζώνης και χαμηλή καθυστέρηση στους χρήστες του, διευκολύνοντάς τους στην περιήγησή τους στο διαδίκτυο, σε audio streaming και σε βίντεο υψηλής συμπίεσης με την παροχή υψηλού εύρους ζώνης και στις εφαρμογές ανταλλαγής μηνυμάτων με την χαμηλή καθυστέρηση. Το Herbivore μπορεί να αποτελέσει ένα πρακτικό σύστημα επίστρωσης επάνω στο υπάρχον διαδίκτυο παρέχοντας στους χρήστες υψηλού επιπέδου ανωνυμία.

Ευπάθειες/μειονεκτήματα: Το Herbivore δεν μπορεί να προστατεύσει την ταυτότητα των χρηστών όταν π.χ. οι φυλλομετρητές ιστού που χρησιμοποιούν έχουν ενεργοποιημένα τα cookies και μεταφέρουν στο ανώνυμο κανάλι το όνομα του χρήστη. Αν και παρέχει πρωτόκολλο end-to-end κρυπτογράφησης για να διασφαλίσει ότι οι άλλοι κόμβοι που συμμετέχουν στο clique δεν μπορούν να κρυφακούσουν τα περιεχόμενα παρ όλα αυτά οι ταυτότητες των υπηρεσιών ιστού που βρίσκονται εκτός του Herbivore είναι εκτεθειμένες. Το Herbivore προστατεύει την ταυτότητα των δύο επικοινωνούντων άκρων από τρίτα μέρη όταν και τα δύο άκρα είναι τμήμα του δικτύου του στην αντίθετη περίπτωση δεν μπορεί να προστατεύσει τους χρήστες από τρίτα μέρη όταν τα περιεχόμενα της επικοινωνίας τους ενδέχεται να εκθέτουν την ταυτότητά τους.

3.3.7 Mantis

Ως γνωστό πολλοί ιδιώτες που συμμετέχουν σε δίκτυα διαμοιρασμού αρχείων λειτουργούν ως εξυπηρετητές ή φιλοξενούν προσωπικές ιστοσελίδες. Το Mantis αποτελεί ένα δίκτυο ομότιμων οντοτήτων για αναζήτηση, αποτελούμενο από ανώνυμους κόμβους και στοχεύει στην προστασία της ιδιωτικότητας των χρηστών που λειτουργούν ως εξυπηρετητές στο δίκτυο [07]. Οι πελάτες δεν γνωρίζουν την ταυτότητα του εξυπηρετητή. Γενικότερα σε κάθε δίκτυο ομότιμων κόμβων ο κάθε συμμετέχων κόμβος αφιερώνει το μεγαλύτερο μέρος του εύρους ζώνης του προκειμένου να αναμεταδώσει κίνηση σε άλλους ομότιμους κόμβους του δικτύου. Το Mantis μειώνει σημαντικά αυτό το εύρος ζώνης ενισχύοντας έτσι την αποδοτική μεταφορά των δεδομένων. Στο Mantis κανένας κόμβος δεν γνωρίζει την ταυτότητα του κόμβου που έχει εκκινήσει μία υπηρεσία αιτήματος ή απάντησης.

Τεχνική Περιγραφή Λειτουργίας/Αρχιτεκτονική: Η αρχιτεκτονική του Mantis έχει ως πρότυπο το ανώνυμο σύστημα του Crowds που δημιουργήθηκε για την προστασία των συναλλαγών στο διαδίκτυο με την διαφορά ότι διατάσσεται σε δομή δέντρου όπως το Gnutella και επιτρέπει στους χρήστες την αναζήτηση στο δίκτυο ομότιμων οντοτήτων. Η δομή του δέντρου δημιουργείται με την μετάδοση των αιτημάτων αναζήτησης σε όλο το δίκτυο. Οι εξυπηρετητές στο Mantis μεταφέρουν τα δεδομένα απευθείας στους πελάτες μέσω ξεχωριστών ψευδο-πηγών UDP stream, επιτρέποντας μόνο τα δεδομένα ελέγχου να μεταφέρονται μέσω του τούνελ αποτελούμενο από το πλήθος "crowds". Το σύστημα του Mantis δεν περιορίζει την είσοδο και την έξοδο των κόμβων στο δίκτυο ενώ επιτρέπει την έξοδο των κόμβων από το μονοπάτι προώθησης οποιαδήποτε στιγμή.

Υιοθετεί την ορολογία του Crowds και χρησιμοποίει τα "Jondo" ως ονομασία των κόμβων στο δίκτυο που ενεργούν ως πελάτες, εξυπηρετητές ή αναμεταδότες των μηνυμάτων σε άλλους κόμβους, το "blender" ως ονομασία για τον εξυπηρετητή που επιτρέπει στα jondo να εντοπίσουν άλλους ομότιμους κόμβους, το "back channel" για να δηλώσει το μονοπάτι προώθησης των μηνυμάτων από πελάτες προς εξυπηρετητές και το "session" για να δηλώσει την επικοινωνία ενός ζευγαριού από jondos πάνω από ένα back-channel.

Κάθε Jondo κατά την αρχικοποίηση του εγγράφεται στον εξυπηρετητή κατάλογο του Blender αποκαλύπτοντας την διεύθυνση IP του καθώς και μία θύρα του (listening) για νέες συνδέσεις. Η εγγραφή του νεοεισερχόμενου κόμβου στο Blender είναι προαιρετική εφόσον το δίκτυο είναι λειτουργικό και χωρίς την παρουσία του Blender αλλά απαραίτητη για τον εντοπισμό άλλων

ομότιμων κόμβων. Το Blender μπορεί να είναι μία οντότητα αλλά ακόμα και ένα συγκεκριμένο φόρουμ που επιτρέπει στα jondos να εγγραφούν και να αντλήσουν λεπτομέρειες. Μόλις εισέλθει στον δίκτυο ο ομότιμος κόμβος στέλνει ερώτημα στο Blender για να λάβει μία λίστα από τις διαθέσιμες συνδέσεις. Μόλις εντοπίσει άλλον κόμβο που θέλει να συμμετάσχει εκτελούν μεταξύ τους ανταλλαγή κλειδιού χωρίς έλεγχο των ταυτοτήτων τους ώστε να συμφωνήσουν σε ένα κοινό κλειδί κρυπτογράφησης με το οποίο θα κρυπτογραφηθεί όλη η επικοινωνία μεταξύ τους. Η διαδικασία αυτή από το jondo επαναλαμβάνεται έως ότου αποκτήσει τον μικρότερο αριθμό συνδέσεων που έχουν καθοριστεί από τον χρήστη [07].

Τα μηνύματα που ανταλλάσσονται στο δίκτυο του Mantis έχουν τη μορφή {SRC_ID, DST_ID, TYPE, DATA} όπου τα πεδία SRC_ID και DST_ID περιέχουν τυχαία αναγνωριστικά της πηγής και του προορισμού αντίστοιχα που χρησιμοποιούνται για τις ατομικές συνόδους και με σκοπό την προστασία της ανωνυμίας τους, στο πεδίο TYPE δηλώνεται ο σκοπός του μηνύματος και στο πεδίο DATA περιέχεται οποιαδήποτε πληροφορία σχετική με το μήνυμα. Το DST_ID χρησιμοποιείται για την δρομολόγηση των μηνυμάτων διαμέσου του back-channel προς τον αποδέκτη ενώ όταν η τιμή του είναι 0 δηλώνει την μετάδοση των μηνυμάτων, όπως αιτήματα αναζητήσεων, και αναμεταδίδονται σε όλους τους γείτονες κόμβους.

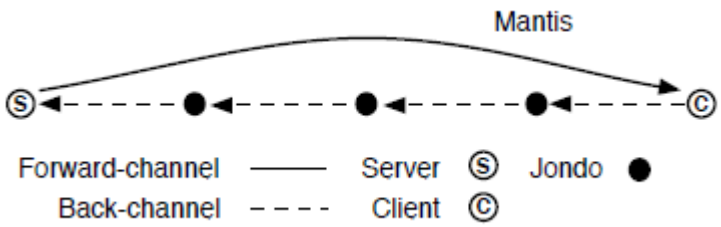
Ο πελάτης κόμβος παράγει με σκοπό την αναζήτηση ένα μήνυμα συμπεριλαμβάνοντας στο πεδίο SRC_ID την τιμή ενός τυχαίου αναγνωριστικού συνόδου το οποίο χρησιμοποιείται και για την αναγνώριση των απαντήσεων που λαμβάνει, στο πεδίο DST_ID το 0 για να δηλώσει την μετάδοση, στο πεδίο TYPE δηλώνει τον σκοπό της αναζήτησης και στο πεδίο DATA οποιοδήποτε όρο της αναζήτησης. Το μήνυμα κρυπτογραφείται σε αντίγραφα με το διαμοιραζόμενο κλειδί του πελάτη κόμβου και του κάθε γείτονά του και στη συνέχεια αναμεταδίδεται σε όλους τους γείτονες κόμβους που είναι συνδεδεμένος. Στη συνέχεια οι γείτονες κόμβοι αναμεταδίδουν το μήνυμα σε όλους τους συνδεδεμένους γείτονές τους και η αναμετάδοση συνεχίζεται κατ αυτόν τον τρόπο σχηματίζοντας ένα δέντρο με ρίζα τον εκκινητή κόμβο και κάθε κόμβο κάτω από τη ρίζα να αποτελεί τον παραλήπτη του αιτήματος χωρίς όμως να γνωρίζουν την θέση τους στο δέντρο σε σχέση με τον πελάτη κόμβο. Τα διπλά όμοια μηνύματα απορρίπτονται ώστε να αποφευχθεί η επανάληψη δρομολόγησης.

Το κάθε Jondo διατηρεί ένα πίνακα συσχετίζοντας τα αναγνωριστικά προορισμών με το επόμενο άλμα στην διαδρομή προώθησης. Μόλις το jondo λάβει ένα μήνυμα το αποκρυπτογραφεί με το διαμοιραζόμενο κλειδί και ενεργεί ανάλογα με την τιμή του πεδίου DST_ID. Εάν έχει άγνωστη τιμή το μήνυμα απορρίπτεται, εάν προορίζεται για το Jondo αυτό το δέχεται και συνεχίζει, εάν

έχει την τιμή 0 ενεργεί ανάλογα ώστε να το αναμεταδώσει στους γείτονές του διαφορετικά αντλεί από τον πίνακά που διατηρεί τον γείτονα κόμβο που πρέπει να προωθήσει το μήνυμα και εκτελεί τις απαραίτητες ενέργειες αποστολής. Εάν ένας κόμβος παραλάβει ένα μήνυμα που περιέχει ένα άγνωστο αναγνωριστικό του κόμβου πηγής συσχετίζει το jondo που αναμετάδωσε το μήνυμα αυτό ως το επόμενο άλμα στο μονοπάτι επιστροφής [07].

Σχετικά με τα μηνύματα απάντησης, ο εξυπηρετητής κόμβος παράγει ένα τυχαίο αναγνωριστικό συνόδου το οποίο και συμπεριλαμβάνει στο πεδίο SRC_ID, στο πεδίο DST_ID συμπεριλαμβάνει το αναγνωριστικό του κόμβου εκκινητή του μηνύματος, στο πεδίο TYPE συμπεριλαμβάνει το σκοπό του μηνύματος και στο πεδίο DATA οποιαδήποτε επιπρόσθετη πληροφορία όσον αφορά με τα αποτελέσματα της αναζήτησης. Το μήνυμα αναμεταδίδεται εφόσον πρώτα κρυπτογραφηθεί με το διαμοιραζόμενο κλειδί του εξυπηρετητή κόμβου και του Jondo του επόμενου άλματος που χαρτογραφείται από το DST_ID και έτσι αναμεταδίδεται πίσω στον κόμβο πηγή.

Ο πελάτης έχει την δυνατότητα επικοινωνίας απευθείας με τον εξυπηρετητή μέσω ενός τούνελ που δημιουργείται πάνω από το back-channel. Αυτό πραγματοποιείται με την ανταλλαγή μη αυθεντικοποιημένων κλειδιών προκειμένου να συμφωνήσουν το μυστικό κλειδί για την μεταξύ τους επικοινωνία και στη συνέχεια κρυπτογραφούν όλα τα άκρη προς άκρη μηνύματά τους με αυτό το μυστικό κλειδί και επιπρόσθετα γίνεται κρυπτογράφηση και σε κάθε άλμα από το αντίστοιχο jondo που το αναμεταδίδει. Επίσης το Mantis επιτρέπει την απευθείας επικοινωνία του εξυπηρετητή με τον πελάτη μέσω UDP καναλιού. Ο πελάτης όμως πρέπει να στείλει μέσω του κρυπτογραφημένου τούνελ την διεύθυνση IP του και ο εξυπηρετητής επικοινωνεί μαζί του μέσω ενός ψευδο-πηγής UDP stream. Το back-channel χρησιμοποιείται μόνο για την μεταφορά δεδομένων ελέγχου της αξιοπιστίας του stream μεταξύ του πελάτη και του εξυπηρετητή και αν χρειαστεί για οποιαδήποτε άλλη επικοινωνία.



Εικόνα 11: Κανάλι προώθησης και κανάλι επιστροφής

Το Mantis έρχεται αντιμέτωπο με το πρόβλημα της αποσύνδεσης κάποιου Jondo του back-channel με αποτέλεσμα την διακοπή της επικοινωνίας του εξυπηρετητή με τον πελάτη. Για την αντιμετώπιση του προβλήματος αυτού ο εξυπηρετητής κόμβος μπορεί να επαναδημιουργήσει το κανάλι επικοινωνίας εάν γνωρίζει την διεύθυνση IP του πελάτη στέλνοντας ένα μήνυμα αιτήματος καινούργιου καναλιού και συμπεριλαμβάνοντας την διεύθυνση του πελάτη και την πόρτα του. Το μήνυμα αυτό αναμεταδίδεται ανάμεσα στα jondo με την ρήξη ενός νομίσματος έως ότου φτάσει στον κόμβο που προορίζεται και έτσι επαναδημιουργείται το κανάλι μεταξύ τους και η επικοινωνία μπορεί να διεξαχθεί ομαλά και πάλι.

Πλεονεκτήματα/Θετικά χαρακτηριστικά: Το Mantis επιτρέπει στους χρήστες να αναζητήσουν αρχεία στο δίκτυο που παρέχονται από εξυπηρετητές εγκαθιστώντας ένα κρυπτογραφημένο τούνελ επικοινωνίας ώστε να μεταφέρεται ο μεγαλύτερος όγκος των δεδομένων και συγχρόνως προστατεύεται η ανωνυμία του εξυπηρετητή. Ο μεγαλύτερος όγκος της επικοινωνίας από τον εξυπηρετητή στον πελάτη στέλνεται μέσω ψευδο-πηγής UDP stream με αποτέλεσμα τα jondos να μην προωθούν μηνύματα για λογαριασμό των άλλων χρηστών και να επιβαρύνουν το δίκτυο με επιπλέον καθυστέρηση.

Ευπάθειες/μειονεκτήματα: Το Mantis αν και προστατεύει το περιεχόμενο της επικοινωνίας των κόμβων και συγχρόνως παρέχει ανωνυμία πελάτη και εξυπηρετητή παρόλα αυτά υπάρχουν ανοιχτά σημεία ευπάθειας στο δίκτυο. Η μη αυθεντικοποιημένη ανταλλαγή μυστικού κλειδιού μεταξύ των jondo για την μεταξύ τους επικοινωνία, η εγγραφή των κόμβων που επιθυμούν να συμμετάσχουν στο σύστημα σε μία οντότητα το Blender αποκαλύπτοντας την διεύθυνση IP και την διαθέσιμη θύρα τους καθώς και η χωρίς περιορισμό είσοδος και έξοδος των κόμβων από το σύστημα αποτελούν κάποια από τα ανοιχτά σημεία ευπάθειας του δικτύου Mantis.

3.3.8 Mute

Το Mute αποτελεί ένα ανώνυμο δίκτυο ομότιμων οντοτήτων και χρησιμοποιείται από εκατοντάδες χιλιάδες χρήστες για τον διαμοιρασμό αρχείων [16]. Στόχος του δικτύου είναι να αποκρύψει την διεύθυνση IP των χρηστών του. Στο δίκτυο Mute κάθε ομότιμος κόμβος επιλέγει τυχαία μία ψευδοδιεύθυνση με την οποία συμμετέχει στο δίκτυο καθώς και έναν πιθανολογικό μετρητή time-to-live ώστε να εμποδίσει έναν αντίπαλο από το να συμπεράνει κατά πόσο μία αναζήτηση έχει προχωρήσει ή πρέπει να προχωρήσει.

Τεχνική Περιγραφή Λειτουργίας/Αρχιτεκτονική: Οι χρήστες που επιθυμούν να συνδεθούν στο δίκτυο Mute συνδέονται με έναν μικρό αριθμό με άλλους γνωστούς κόμβους και μόνο οι απευθείας συνδεδεμένοι γείτονες γνωρίζουν την διεύθυνση IP. Κάθε κόμβος επιλέγει μία τυχαία διεύθυνση που χρησιμοποιεί για την αναγνώρισή του στο δίκτυο. Η επικοινωνία με κόμβους που βρίσκονται σε απόσταση μακρινή γίνεται με την αποστολή μηνυμάτων άλμα προς άλμα σε όλο το δίκτυο επικάλυψης.

Ο κάθε κόμβος στο δίκτυο Mute δημιουργεί έναν πίνακα δρομολόγησης καταχωρώντας σε αυτόν την σύνδεση από την οποία έλαβε το μήνυμα ως πιθανή δρομολόγηση προς την ψευδοδιεύθυνση αυτή. Το πρωτόκολλο δρομολόγησης του Mute περιγράφεται αναλυτικά στα παρακάτω βήματα [16]:

1. Η εφαρμογή κατά την εκκίνησή της παράγει ένα ψευδο-ID και ένα 1024bit RSA ζεύγος κλειδιών (ιδιωτικό/δημόσιο). Επίσης καθορίζει τις τιμές του μετρητή που θα χρησιμοποιήσει σε όλες τις αναζητήσεις που θα εκτελέσει.

2. Στη συνέχεια ο κόμβος προσπαθεί να δημιουργήσει συνδέσεις με άλλος κόμβους του δικτύου. Χρησιμοποιεί το δημόσιο κλειδί του ώστε να εγκαταστήσει ένα AES 128 bit συμμετρικό κλειδί συνόδου για κάθε σύνδεση.

3. Αφού εγκατασταθούν οι συνδέσεις επιλέγει ένα τμήμα με τους κόμβους που θα χρησιμοποιεί για να προωθεί τα μηνύματα με τους μετρητές που θα χρησιμοποιήσει και δημιουργεί μία άδεια λίστα με τα ID των κόμβων που «βλέπει» καθώς και έναν άδειο πίνακα δρομολόγησης.

Μετά από τις προηγούμενες ενέργειες ο κόμβος μπορεί να στείλει και παραλάβει μηνύματα ακολουθώντας την παρακάτω μορφοποίηση [16]:

MessageID: αποτελείται από 6 ψηφιακούς αριθμούς και μια χρονοσφραγίδα.

FromID: αποτελείται από το ψευδοID του αποστολέα.

ToID: αποτελείται από το ψευδοID του παραλήπτη ή το “ALL” για αναζητήσεις το οποίο στέλνεται σε όλους τους κόμβους γείτονες.

Flags: δηλώνει την φάση του μετρητή ή μπορεί να περιέχει ROUTE_ONLY το οποίο δηλώνει την προώθηση του μηνύματος αν έχει στον πίνακα δρομολόγησης το “To ID” ή το “FRESH_ROUTE”

το οποίο δηλώνει ότι πρέπει να διαγράψει από τον πίνακα δρομολόγησης και τον αποστολέα και τον παραλήπτη.

UtilityCounter: περιέχει μία ASCII, με βάση το 10, τιμή του μετρητή.

Length: περιέχει το μήκος του μηνύματος (ωφέλιμου φορτίου).

Body: περιέχει το κρυπτογραφημένο μήνυμα με κρυπτογράφηση AES.

Όταν ένας κόμβος λαμβάνει ένα μήνυμα έχει τις εξής επιλογές [16]:

- Εάν το ID του μηνύματος είναι στη λίστα των ID μηνυμάτων που έχει "δει" ο κόμβος ή αν η χρονοσφραγίδα είναι παλιά το μήνυμα απορρίπτεται, διαφορετικά το ID του μηνύματος προστίθεται στη λίστα του κόμβου με τα ID των μηνυμάτων που έχει «δει».

- Στον πίνακα δρομολόγησης εάν υπάρχει μία λίστα από κανάλια για το "From ID" τότε ο κόμβος προσθέτει το κανάλι επί το οποίο έλαβε το μήνυμα (απορρίπτοντας το παλιότερο κανάλι εάν υπάρχουν τώρα πάνω από 50). Εάν το "From ID" δεν είναι στον πίνακα δρομολόγησης προστίθεται με το κανάλι επί το οποίο φθάνει. Τα παλιότερα "From ID" απορρίπτονται εάν ο πίνακας δρομολόγησης περιέχει πάνω από 50 IDs.

- Εάν το ID πεδίο είναι ALL ή το "ToID" είναι άγνωστο και ο UtilityCounter δεν έχει λήξει, ο κόμβος μειώνει το time-to-live και προωθεί το μήνυμα σε όλους τους γείτονές του αποκρυπτογραφώντας το και κρυπτογραφώντας ξανά το μήνυμα με το κατάλληλο AES κλειδί. Εάν ο UtilityCounter έχει λήξει τότε το μήνυμα προωθείται στο υποσύνολο των κόμβων που επιλέγεται κατά την εκκίνηση.

- Εάν ο τοπικός πίνακας δρομολόγησης συμπεριλαμβάνει μία λίστα από κανάλια για το "ToID" τότε ο κόμβος επιλέγει τυχαία ένα από αυτά τα κανάλια τυχαία. Ο κόμβος στη συνέχεια προωθεί το μήνυμα στο κανάλι κρυπτογραφημένο με το AES κλειδί για αυτό το κανάλι.

Ο κόμβος μπορεί να συνεχίσει στην επεξεργασία απάντησης του μηνύματος εάν είναι απαραίτητο.

Πλεονεκτήματα/Θετικά χαρακτηριστικά: Στο Mute δίκτυο εφαρμόζεται το πρωτόκολλο Ants και ένας non-deterministic time-to-live μετρητής. Επίσης σχεδιάστηκε με χαρακτηριστικά που καθιστούν το σύστημα αποδοτικό και φιλικό προς τον χρήστη [15]. Το δίκτυο Mute

προσθέτει μεγάλο βαθμό δυσκολίας σε κάποιον αντίπαλο που στοχεύει στην σύνδεση της ψευδο-ID ενός κόμβου με την πραγματική διεύθυνσή του.

Ευπάθειες/μειονεκτήματα: Το Mute αντιμετωπίζει κυρίως επιθέσεις από κόμβους του συστήματος που στοχεύουν να συνδέσουν την IP διεύθυνση των γειτόνων κόμβων τους με ένα ψευδο-ID. Οι αντίπαλοι μπορούν να δημιουργήσουν πολλές συνδέσεις με κάποιον κόμβο αλλά το Mute δεν τους επιτρέπει να παρακολουθήσουν όλο το δίκτυο ή ακόμα όλες τις συνδέσεις που εισέρχονται ή εξέρχονται από τον κόμβο [15]. Στο δίκτυο Mute ο ρυθμός downloading είναι αρκετά χαμηλός λόγω της δρομολόγησης διαμέσου πολλών κόμβων και δεν είναι κατάλληλο για μεγάλα δίκτυα. Επίσης όλοι οι κόμβοι στο δίκτυο έχουν την δυνατότητα να διαβάσουν το περιεχόμενο του μηνύματος και αυτό αφήνει ανοιχτό σημείο ευπάθειας στο δίκτυο [36].

3.3.9 Τρίτη Γενιά Δικτύων Ομότιμων Οντοτήτων

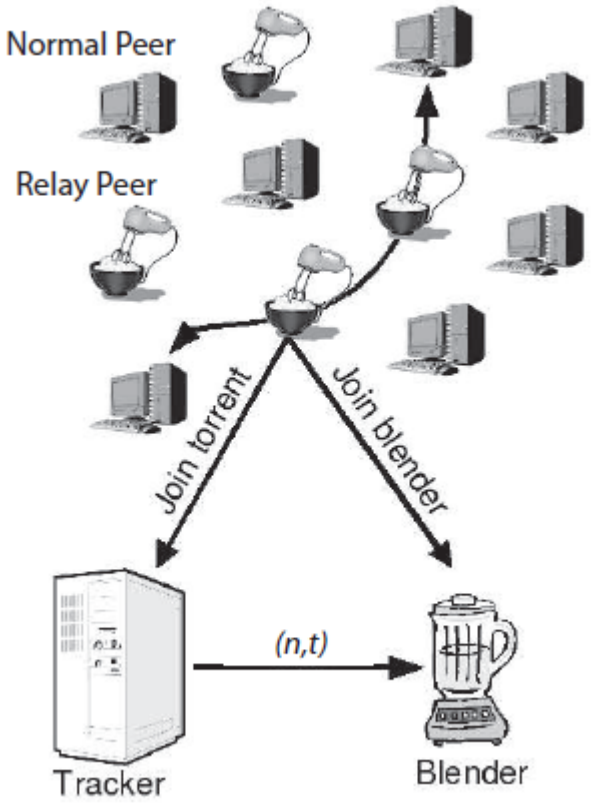
Η τρίτη γενιά των δικτύων ομότιμων οντοτήτων έχουν ενσωματωμένα ως λειτουργικά στοιχεία της αρχιτεκτονικής τους μηχανισμούς που συμβάλλουν στην προστασία της ιδιωτικότητας του χρήστη όπως κρυπτογράφηση και ανώνυμη επικοινωνία στο δίκτυο. Η εφαρμογή τους δεν είναι ιδιαίτερα διαδεδομένη λόγω της υπερφόρτωσης του δικτύου που προσθέτουν οι μηχανισμοί ανωνυμίας με αποτέλεσμα να προσδίδουν στο δίκτυο μεγάλη καθυστέρηση και δυσκολία στην χρήση τους. Το BitBlender εντάσσεται στην τρίτη γενιά των ομότιμων δικτύων προσφέροντας ανωνυμία στο BitTorrent (πρωτόκολλο, δικτύου ομότιμων κόμβων -διαμοιρασμού αρχείων που χρησιμοποιείται για τη διανομή μεγάλου όγκου δεδομένων).

3.3.9.1 BitBlender

Το BitBlender αποτελεί ένα πρωτόκολλο που παρέχει ένα ανώνυμο στρώμα στην κίνηση του BitTorrent [03]. Το BitTorrent αποτελεί ένα πρωτόκολλο διαμοιρασμού αρχείων σε δίκτυα ομότιμων κόμβων και δεν παρέχει ανωνυμία στους χρήστες εφόσον οι διευθύνσεις IP από όλους τους κόμβους που διαμοιράζονται το αρχείο δημοσιεύονται σε έναν γνωστό και δημόσια προσβάσιμο εξυπηρετητή που ονομάζεται tracker. Η λειτουργία του BitBlender στηρίζεται στην δημιουργία ενός ad-hoc πολλαπλών αλμάτων δίκτυο το οποίο αποτελείται από ειδικούς ομότιμους κόμβους “relay peers” που συμμετέχουν ως πληρεξούσιοι “proxy” στα αιτήματα και στις απαντήσεις εκ μέρους των άλλων ομότιμων κόμβων. Το BitBlender είναι εύκολο να εφαρμοστεί χωρίς να τροποποιηθεί το πρωτόκολλο BitTorrent.

Τεχνική Περιγραφή Λειτουργίας/Αρχιτεκτονική: Το πρωτόκολλο του BitBlender χρησιμοποιεί την κεντρική ιδέα παροχής ανωνυμίας του Crowd την οποία και την προσαρμόζει στην δική του αρχιτεκτονική [03]. Όπως αναφέρθηκε στο δίκτυο εκτός από τους κόμβους που διαμοιράζονται αρχεία υπάρχουν και οι κόμβοι "relay peers" οι οποίοι δεν ενεργούν κάποιο upload ή download αρχείου αλλά λειτουργούν ως πληρεξούσιοι της κίνησης εκ μέρους των κόμβων του δικτύου. Τα relay peers καθώς και τα ανώνυμα torrents οργανώνονται από μία οντότητα που ονομάζεται blender η οποία μπορεί να είναι ένας εξυπηρετητής καταλόγου, ένας εξυπηρετητής αντιγράφων καταλόγου ή ένας διανεμημένος πίνακας κατακερματισμού "DHT". Το Torrent είναι ένα metadata αρχείο που περιέχει στοιχεία απαραίτητα για το download του αρχείου στα οποία συμπεριλαμβάνεται και ένας δείκτης προς έναν εξυπηρετητή που ονομάζεται "tracker". Ο tracker περιέχει μία λίστα με τους κόμβους που συσχετίζονται με το συγκεκριμένο torrent αλλά και βοηθάει στην επικοινωνία μεταξύ των κόμβων. Τα relay peers μπορεί να είναι "seeders" δηλαδή να μπορεί να έχουν ένα ολοκληρωμένο αντίγραφο του αρχείου που διαμοιράζονται ή "leechers" δηλαδή μπορούν να διαθέτουν ένα υποσύνολο από τα κομμάτια ενός συγκεκριμένου αρχείου.

Η γενική περιγραφή της λειτουργίας του BitBlender έχει ως ακολούθως: Ο tracker προκειμένου να εισάγει στο δίκτυο relay peers για ένα συγκεκριμένο torrent επικοινωνεί με το blender στέλνοντας αίτημα για την εισαγωγή τους (στο συγκεκριμένο torrent) δίνοντας επιθυμητό βαθμό ανωνυμίας. Στη συνέχεια εφόσον εισαχθούν στο δίκτυο δέχονται αιτήματα και τα προωθούν σε άλλα μέλη του torrent. Οι κόμβοι αυτοί μπορεί να είναι και κόμβοι του δικτύου που συμμετέχουν στον διαμοιρασμό αρχείου. Οι απαντήσεις προωθούνται κατά τον ίδιο τρόπο από το ίδιο μονοπάτι αναμετάδοσης. Η διαδικασία αυτή δημιουργεί ένα δίκτυο ad-hoc.



Εικόνα 12: Αρχιτεκτονική BitBlender (όπου n: ο αριθμός των αιτούμενων κόμβων, t: μοναδικό αναγνωριστικό του tracker π.χ. URI)

Πλεονεκτήματα/Θετικά χαρακτηριστικά: Στο BitBlebder προκειμένου να επιτευχθεί ανωνυμία οι συμμετέχων κόμβοι του δικτύου απλά στέλνουν αιτήματα όπως στο BitTorrent ενώ τα relay peers απλά προωθούν τα αιτήματα που λαμβάνουν σε άλλους κόμβους και έτσι δημιουργείται ένα ad-hoc δίκτυο. Με αυτόν τον τρόπο είναι αρκετά δύσκολο σε κάποιον να αποκαλύψει ποιοι κόμβοι είναι relay peers και ποιοι πραγματικοί κόμβοι του δικτύου. Επίσης το πρωτόκολλο αυτό προσδίδει χαμηλή καθυστέρηση στο δίκτυο. Το χαρακτηριστικό στην αρχιτεκτονική λειτουργίας του αποτελεί το ότι η ανωνυμία που προσφέρει στους χρήστες δεν στηρίζεται στην κρυπτογραφία. Επιτυγχάνει επαρκή ανωνυμία στον διαμοιρασμό αρχείων και προστατεύει την ανωνυμία των εκκινητών των αιτημάτων. Όσοι περισσότεροι κόμβοι συμμετέχουν στο δίκτυο τόσο πιο δύσκολο είναι σε κάποιον αντίπαλο να αποκαλύψει τους πραγματικούς κόμβους που συμμετέχουν στη μεταφορά ενός torrent.

Ευπάθειες/μειονεκτήματα: Το BitBlender δεν χρησιμοποιεί κρυπτογράφηση στον διαμοιρασμό αρχείων και αυτό δημιουργεί κάποια μειονεκτήματα αν και δεν είναι απαραίτητο να παρέχει εμπιστευτικότητα στα περιεχόμενα που διαμοιράζεται εφόσον το BitTorrent είναι

ένα πρωτόκολλο που τα περιεχόμενά του δεν διαρρέουν πληροφορίες προσωπικών δεδομένων όπως στο HTTP και είναι προσβάσιμα από όλους.

3.4 Πρωτοβουλίες Ενίσχυσης των Πολιτικών Προστασίας

Στους μηχανισμούς προστασίας της ιδιωτικότητας που έχουν αναπτυχθεί εντάσσονται και οι υπηρεσίες ή συστήματα που στοχεύουν στην ενημέρωση του χρήστη σχετικά με την εφαρμοζόμενη πολιτική προστασίας που εφαρμόζει ο κάθε ιστότοπος που επισκέπτεται. Κύριος σκοπός τους αποτελεί η έγκαιρη πληροφόρηση του χρήστη και η οικοδόμηση ενός πλαισίου εμπιστοσύνης σχετικά με τα προσωπικά δεδομένα που συλλέγονται από τον εκάστοτε ιστότοπο και τον τρόπο που τα χειρίζεται και τα χρησιμοποιεί. Οι πρωτοβουλίες ενίσχυσης των πολιτικών προστασίας αποτελούν μία προσπάθεια δέσμευσης των εταιρειών που χρησιμοποιούν ιστοσελίδες να υλοποιούν συγκεκριμένες πολιτικές προστασίας ώστε ο χρήστης να έχει την δυνατότητα έγκρισης ή μη της χρήσης των προσωπικών του δεδομένων.

3.4.1 Truste

Το Truste αποτελεί μία αυτορυθμιζόμενη πρωτοβουλία προστασίας της ιδιωτικότητας [01]. Η Truste είναι μία εταιρεία διαχείρισης της προστασίας των προσωπικών δεδομένων στοχεύοντας στην ενίσχυση της εμπιστοσύνης των χρηστών στο διαδίκτυο. Παρέχει την δυνατότητα στις διάφορες ιστοσελίδες να συλλέγουν προσωπικά δεδομένα με ασφαλή τρόπο καθώς εναρμονίζονται στους όρους προστασίας της ιδιωτικότητας των χρηστών τους που καθορίζονται από την Truste. Κάθε πιστοποιημένη ιστοσελίδα που φέρει το σήμα της Truste αποτελεί διαπιστευτήριο στους επισκέπτες της ότι μετά την συλλογή των πληροφοριών, δεν αποκαλύπτονται στοιχεία της ταυτότητας τους σε τρίτα μέρη και τηρούνται οι κανόνες ασφάλειας των προσωπικών δεδομένων τους. Αποτελεί, λοιπόν μία ενέργεια ενδυνάμωσης των διαφόρων εταιρειών να εξασφαλίσουν τις καλύτερες και πιο ασφαλείς πρακτικές συλλογής και χρησιμοποίησης των προσωπικών πληροφοριών στις ιστοσελίδες τους και στις εφαρμογές τους [61].

Τεχνική Περιγραφή Λειτουργίας/Αρχιτεκτονική: Το Truste αρχικά αναλύει την πολιτική που εφαρμόζει ο εκάστοτε ιστότοπος κατά την χρήση του από τους επισκέπτες. Προκειμένου να

πιστοποιηθεί θα πρέπει να εναρμονιστεί με τις απαιτήσεις του προγράμματος πιστοποίησης Truste. Λόγω των αυξημένων αναγκών και των ποικίλων παρεχόμενων υπηρεσιών από τους διάφορους ιστοτόπους έχουν αναπτυχθεί διάφορα προγράμματα πιστοποίησης από την Truste. Ειδικότερα τα προγράμματα αυτά είναι τα ακόλουθα: Trusted Websites, Trusted Mobile Apps, Trusted Cloud, Trusted Data, Trusted Download, Children's Privacy, Trusted Smart Grid, APEC. Θα επικεντρωθούμε στο πρόγραμμα Trusted Websites στο οποίο οι ελάχιστες προϋποθέσεις που θα πρέπει να πληροί ένας ιστότοπος προκειμένου να πιστοποιηθεί από την Truste σχετικά με την πολιτική προστασίας της ιδιωτικότητας είναι οι παρακάτω:

- *Περιορισμός Συλλογής Στοιχείων* (Collection Limitation): Επιτρέπεται η συλλογή προσωπικών πληροφοριών μόνο με την ειδοποίηση και συγκατάθεση του ατόμου και συγκεντρώνονται μόνο οι προσωπικές πληροφορίες που είναι αναγκαίες για τον σκοπό που θα εξυπηρετήσουν και σύμφωνα με την Δήλωση προστασίας των προσωπικών δεδομένων των συμμετεχόντων που ισχύει κατά τον χρόνο της συλλογής.

- *Χρησιμοποίηση των προσωπικών δεδομένων*: Οι προσωπικές πληροφορίες μπορούν να χρησιμοποιηθούν για την παροχή των υπηρεσιών που προβλέπεται σύμφωνα με τη δημοσιευμένη δήλωση προστασίας προσωπικών δεδομένων που βρίσκεται σε ισχύ και για το χρονικό διάστημα της δήλωσης αυτής ή με προειδοποίηση και συγκατάθεση του χρήστη σύμφωνα με τις απαιτήσεις του προγράμματος.

- *Επιλογή* (Choice): Πρέπει να δίνεται η επιλογή στο συμμετέχοντα να αποσύρει την συγκατάθεσή του σχετικά με την συλλογή των προσωπικών του δεδομένων και την χρησιμοποίηση αυτών.

- *Συλλογή και χρησιμοποίηση προσωπικών στοιχείων από τρίτα μέρη* (Collection and Use of Third Party PII): Τα προσωπικά δεδομένα μπορούν να χρησιμοποιηθούν από τρίτα μέρη μόνο για την διευκόλυνση της ολοκλήρωσης της συναλλαγής για τον σκοπό που συλλέχθηκαν οι προσωπικές πληροφορίες. Στην περίπτωση που τα προσωπικά δεδομένα του χρήστη χρησιμοποιηθούν από τρίτα μέρη για σκοπό διαφορετικό από τον πρωταρχικό, θα πρέπει να υπάρχει ρητή συγκατάθεσή του. Επίσης θα πρέπει να υπάρχει δήλωση απορρήτου από το τρίτο μέλος που θα χρησιμοποιήσει τα δεδομένα αποσαφηνίζοντας τον τρόπο με τον οποίο συλλέγει τις πληροφορίες, τον προσδιορισμό των δεδομένων που συλλέγει, πως χρησιμοποιούνται τα δεδομένα αυτά και για ποιο σκοπό και με ποια άλλα μέλη, εάν υπάρχουν, διαμοιράζεται τα δεδομένα αυτά.

- *Μηχανή Αναζήτησης* (Search Engine): Μπορούν να περιέχουν προσωπικές πληροφορίες τρίτων μερών χωρίς την ειδοποίηση και τις απαιτήσεις που προαναφέρθηκαν εφόσον όμως οι πληροφορίες αυτές δεν δημιουργούν ένα μόνιμο προφίλ του ατόμου και έχουν αντληθεί από δημοσιευμένες και δημόσιες πηγές του διαδικτύου. Θα πρέπει όμως να παρέχεται ένας μηχανισμός απομάκρυνσης των αποτελεσμάτων αναζήτησης όταν τα δεδομένα αυτά βλάπτουν φυσικά το άτομο ή διαταράσσει δημόσια συμφέροντα συμπεριλαμβανομένης της εθνικής ασφάλειας, της άμυνας ή δημόσιας ασφάλειας.

- *Πρόσβαση* (Access): Θα πρέπει να παρέχεται η δυνατότητα στους χρήστες διαμέσου κάποιου μηχανισμού, εύκολου στην χρήση, να αλλάζουν τα μη έγκυρα προσωπικά δεδομένα, να αιτούνται την διαγραφή και την μη χρησιμοποίηση το δεδομένων αυτών πλέον. Θα πρέπει να δηλώνεται πως παρέχεται η πρόσβαση και σε περίπτωση που αρνείται την πρόσβαση αυτή από τρίτα μέρη θα πρέπει να δηλώνει τον λόγο της άρνησης.

- *Προωθητικά και ενημερωτικά μηνύματα ηλεκτρονικού ταχυδρομείου* (Promotional and Newsletter Email Communications): Όλα τα ενημερωτικά δελτία και διαφημιστικά μηνύματα e-mail που αποστέλλει ο κάθε συμμετέχων στο άτομο πρέπει να περιλαμβάνουν την ταχυδρομική διεύθυνση του αποστολέα και έναν μηχανισμό διαγραφής της εγγραφής ο οποίος θα πρέπει να είναι λειτουργικός και εύχρηστος.

- *Δημοσιοποίηση των προσωπικών δεδομένων* (Public Disclosure of PII): Ο ιστότοπος μπορεί να επιτρέπει στον χρήστη να δημοσιεύσει σε ένα φόρουμ, chat room ή άλλο δημόσιο φόρουμ προσωπικά του δεδομένα καθώς και να τα διαγράψει. Θα πρέπει να υπάρχει από τον ιστότοπο δήλωση ιδιωτικότητας προσδιορίζοντας τον τρόπο με τον οποίο ο χρήστης μπορεί να ζητήσει την διαγραφή των προσωπικών του δεδομένων από την δημόσια προβολή. Εάν ο ιστότοπος παρέχει κάποιον κατάλογο δημόσια προσβάσιμο ή κάποια παρόμοια υπηρεσία θα πρέπει να παρέχει την δυνατότητα στον χρήστη να ζητήσει την αφαίρεση των προσωπικών του δεδομένων από αυτόν.

- *Αλλαγές στο περιεχόμενο* (Material Changes): Ο ιστότοπος θα πρέπει να ενημερώσει τους χρήστες πριν προχωρήσει σε οποιαδήποτε ενέργεια αλλαγής στη συλλογή, χρησιμοποίηση και δημοσιοποίηση των προσωπικών δεδομένων τους και θα πρέπει να υπάρξει αντίστοιχη αποδοχή των ενεργειών αυτών για την επίτευξή τους.

- *Ασφάλεια δεδομένων* (Data Security): Ο ιστότοπος θα πρέπει να παρέχει μηχανισμούς προστασίας των προσωπικών δεδομένων από μη εξουσιοδοτημένη πρόσβαση, χρησιμοποίηση, δημοσιοποίηση και διαμοιρασμό από τρίτους.

- *Παράπονα και σχόλια χρηστών* (User Complaints and Feedback): Θα πρέπει να παρέχεται στους χρήστες να δηλώσουν τις ανησυχίες τους και τα σχόλιά τους σχετικά με την προστασία των προσωπικών τους δεδομένων.

- *Παραβίαση δεδομένων* (Data Breach): Ο ιστότοπος οφείλει να ενημερώσει εντός ενός χρονικού διαστήματος εάν ανιχνεύσει κάποια παραβίαση των προσωπικών δεδομένων των χρηστών του με τις απαραίτητες πληροφορίες της παραβίασης αυτών.

Πλεονεκτήματα/Θετικά χαρακτηριστικά: Η Truste αποτελεί μία υπηρεσία πιστοποίησης των πολιτικών προστασίας των προσωπικών δεδομένων που εφαρμόζουν οι ιστότοποι. Οι πιστοποιημένες ιστοσελίδες από την Truste παρέχουν στους χρήστες τους την δυνατότητα να ελέγχου τις πληροφορίες που συλλέγονται από αυτούς καθώς και τον τρόπο με τον οποίο χρησιμοποιούνται από αυτές τα δεδομένα. Ο κάθε ιστότοπος είναι υπεύθυνος και υπόλογος σχετικά με τις πρακτικές που περιγράφει στην πολιτική της προστασίας των ιδιωτικών δεδομένων. Στοχεύει στην εμπιστοσύνη των χρηστών προς τους πιστοποιημένους ιστοτόπους που επισκέπτονται σχετικά με την εξασφάλιση της προστασίας των προσωπικών τους δεδομένων και ελέγχει την τήρηση των πολιτικών αυτών.

Ευπάθειες/μειονεκτήματα: Το Truste αποτελεί μία πιστοποίηση των πολιτικών που εφαρμόζει ο ιστότοπος σχετικά με την προστασία των προσωπικών δεδομένων των χρηστών του. Δεν παρέχει μηχανισμούς προστασίας έναντι κακόβουλων επιθέσεων και δεν αποκρύπτει την διεύθυνση IP του χρήστη. Ο αντίπαλος διαμέσου διαφόρων επιθέσεων μπορεί να εντοπίσει τον εκκινητή ενός αιτήματος. Επίσης ο Dr. Benjamin Edelman του Harvard Business School ανακάλυψε τον Ιανουάριο του 2006 ότι πιστοποιημένοι ιστότοποι Truste παρουσιάζουν 50% πιθανότητα να παραβιάζουν την πολιτική προστασίας των προσωπικών δεδομένων σε σχέση με τους μη πιστοποιημένους ιστοτόπους. Επίσης ο Dr. Edelman έχει αναφέρει ότι η Truste δεν προχωράει σε ικανοποιητικά μέτρα αντιμετώπισης των πιστοποιημένων ιστοτόπων που παραβιάζουν την πολιτική προστασίας που έχουν δεσμευτεί να τηρούν και δεν ανακαλούν την πιστοποίηση από ιστοτόπους που παραβαίνουν την πιστοποιημένη πολιτική [58].

3.4.2 P3P (Platform for Privacy Preferences)

Το P3P (Platform for Privacy Preferences Project) αποτελεί μία πρωτοβουλία του W3C (World Wide Web Consortium). Το W3C επικεντρώνεται στην ανάπτυξη κοινών πρωτοκόλλων που προάγουν την εξέλιξη και διασφαλίζουν την διαλειτουργικότητα του Παγκόσμιου Ιστού (World Wide Web) ώστε να φτάσει στο μέγιστο των δυνατοτήτων του [34]. Το P3P προσπαθεί με αυτοματοποιημένο τεχνικό τρόπο να ενεργοποιήσει την προσωπική επιλογή και την ενημερωμένη συγκατάθεση των χρηστών καθώς και την δέσμευση των εκδοτών (publishers) σχετικά με την χρησιμοποίηση των δεδομένων. Σκοπός του είναι η εγκατάσταση ενός συμβολαίου μεταξύ του χρήστη και του εξυπηρετητή ώστε να διασφαλιστούν οι πρακτικές που εφαρμόζει ο εξυπηρετητής σχετικά με την προστασία της ιδιωτικότητας και να προσαρμοστούν στις προτιμήσεις του χρήστη.

Τεχνική Περιγραφή Λειτουργίας/Αρχιτεκτονική: Το P3P επιτρέπει στους ιστοτόπους να εκφράσουν τις πρακτικές προστασίας προσωπικών δεδομένων τους με τυποποιημένη μορφή ώστε να υπάρχει η δυνατότητα αυτόματης ανάκτησης και εύκολης κατανόησης από τους πράκτορες του χρήστη [64]. Ο πράκτορας ενεργεί εκ μέρους του χρήστη και γνωρίζει τις προτιμήσεις του, μπορεί να είναι ένα κομμάτι λογισμικού που ενσωματώνεται στο προγράμματα περιήγησης, μπορεί να λειτουργεί ως πρόσθετο στο πρόγραμμα περιήγησης, σε διακομιστές διαμεσολάβησης και μπορεί επίσης να εφαρμοστεί ως Java applets ή Javascript. Οι P3P πράκτορες του χρήστη επιτρέπουν στους χρήστες να ενημερώνονται για τις πρακτικές που εφαρμόζει ο ιστότοπος που επισκέπτονται (με μορφή αναγνωρίσιμη από τον χρήστη αλλά και αναγνωρίσιμη από την μηχανή) και αυτοματοποιούν τη λήψη αποφάσεων με βάση τις πρακτικές αυτές ώστε οι χρήστες να μην χρειάζεται να διαβάσουν τις πολιτικές απορρήτου σε κάθε ιστοσελίδα που επισκέπτονται.

Τα στοιχεία που χρησιμοποιούνται σε ένα P3P περιεχόμενο ιστού είναι τα παρακάτω [13]:

- Οι χρήστες του ιστού εκφράζουν τα προσωπικά δεδομένα και γνωστοποιούν τις προτιμήσεις τους. Μία προτίμηση είναι ένας κανόνας, ή ένα σύνολο από κανόνες που αποφασίζουν τις ενέργειες που πρέπει να διεξάγει ο πράκτορας του χρήστη ή τις ενέργειες που πρέπει να επιτρέψει όταν εμπλέκεται σε μια συζήτηση ή διαπραγμάτευση με μια υπηρεσία. Η προτίμηση μπορεί να εκφραστεί ως ένα συμβατικό κείμενο ή ως μία επίσημα καθορισμένη δήλωση επεξεργάσιμη από την μηχανή.

- Οι ιστότοποι εκφράζουν τα προσωπικά δεδομένα που χρησιμοποιούν καθώς και τις πρακτικές που γνωστοποιούν. Μία πρακτική είναι ένας P3P όρος που εκφράζεται από έναν ιστότοπο και περιγράφει τι προγραμματίζει να κάνει με τα δεδομένα.

- Το πρωτόκολλο P3P το οποίο παρέχει ένα πλαίσιο για την διαχείριση αυτών των πληροφοριών είναι μια απλή προέκταση του HTTP πρωτοκόλλου. Εμπλέκει το πρόγραμμα περιήγησης το οποίο εκδίδει το αίτημα με το οποίο ζητάει τις πρακτικές που εφαρμόζει ο ιστότοπος και τον ιστότοπο που απαντάει με τις προτάσεις. Μία πρόταση είναι μία σειρά από δηλώσεις. Μία δήλωση είναι μία περιγραφή των δεδομένων που ο ιστότοπος πρόκειται να ζητήσει και διευκρινίζει τι θα κάνει με αυτά τα δεδομένα και τι συνέπειες θα υπάρξουν στον χρήστη.

- Η συμμόρφωση του P3P είναι ενσωματωμένη στα προγράμματα περιήγησης, στους εξυπηρετητές ιστού και αν χρειάζεται στους διακομιστές διαμεσολάβησης ιστού (web-server proxies).

Μια απλοποιημένη περιγραφή της βασικής διαδικασίας του P3P είναι η ακόλουθη [13]:

- Ένα πρόγραμμα περιήγησης συμβατό με τοP3P αποκτά από έναν εξυπηρετητή που είναι επίσης συμβατός με το P3P την πρόταση του ιστοτόπου π.χ. τις δηλώσεις των πρακτικών του.

- Το πρόγραμμα περιήγησης συγκρίνει την πρόταση με τις προτιμήσεις του χρήστη.

- Εάν η πρόταση ικανοποιεί τις προτιμήσεις του χρήστη τότε το πρόγραμμα περιήγησης και ο εξυπηρετητής προχωρούν στην επικοινωνία διαμέσου του πρωτοκόλλου HTTP (όπως επεκτάθηκε με εργαλεία JavaScript, Java και cookies).

- Εάν οι πρακτικές που δηλώνονται δεν ικανοποιούν τις προτιμήσεις που έχουν δηλωθεί τότε ανάλογα με την εφαρμογή του προγράμματος περιήγησης και τις ρυθμίσεις των παραμέτρων του χρήστη, το πρόγραμμα περιήγησης μπορεί:

    - να προχωρήσει σε διαπραγμάτευση προκειμένου να καταλήξει σε σύμφωνη λύση με τις προτιμήσεις που έχουν δηλωθεί,

    - να γνωστοποιήσει στον χρήστη τη διαφωνία των προτιμήσεων επιτρέποντάς του:

- την ενημερωμένη συγκατάθεση για την παροχή δεδομένων παρά την διαφωνία των προτιμήσεων,
- να επιχειρήσει διαπραγμάτευση,
- να αποχωρήσει από την περαιτέρω επικοινωνία με τον εξυπηρετητή.

Η παραπάνω διαδικασία αποσκοπεί στην ενημερωμένη συγκατάθεση του χρήστη σχετικά με την επιλογή του. Το P3P θεωρεί δεδομένο την ύπαρξη κάποιου μηχανισμού ο οποίος θα διασφαλίζει ότι η πρακτική που συμφωνήθηκε μεταξύ του χρήστη και του εξυπηρετητή θα εφαρμοστεί. Ο μηχανισμός αυτό μπορεί να παρέχεται από τον ιστότοπο ή μπορεί να είναι κάποιο τρίτο ανεξάρτητο μέλος το οποίο στην ιδανική περίπτωση θα υπογράψει ψηφιακά τις προτάσεις και θα είναι οικονομικά υπεύθυνο για την παραβίαση.

Όπως αναφέρθηκε το πρωτόκολλο P3P είναι μία προέκταση του HTTP πρωτοκόλλου. Οι πράκτορες του χρήστη χρησιμοποιούν τις καθορισμένες αιτήσεις HTTP για να ανακτήσουν το P3P policy reference file από μία γνωστή τοποθεσία της ιστοσελίδας στην οποία ο χρήστης έστειλε το αίτημα. Το αρχείο policy reference υποδεικνύει την τοποθεσία του P3P policy file που εφαρμόζεται σε κάθε τμήμα της ιστοσελίδας εφόσον μπορεί να υπάρχει μία πολιτική για ολόκληρο την ιστοσελίδα ή διάφορες πολιτικές που κάθε μία καλύπτει και από ένα τμήμα της. Ο πράκτορας του χρήστη ανακτά την κατάλληλη πολιτική την αναλύει και ενεργεί ανάλογα με τις προτιμήσεις του χρήστη [67].

Πλεονεκτήματα/Θετικά χαρακτηριστικά: Το P3P επιτρέπει στους χρήστες να δημιουργήσουν τις δικές τους ρυθμίσεις ιδιωτικότητας σε ένα συγκεκριμένο επίπεδο παρέχοντας τη δυνατότητα στο P3P να μπλοκάρει αυτόματα cookies που δεν επιθυμεί ο χρήστης να βρίσκονται στον υπολογιστή του αλλά και να ενημερώνει τον χρήστη όταν η ιστοσελίδα που επισκέπτεται δεν εναρμονίζεται στις προτιμήσεις του [66].

Το πρόγραμμα περιήγησης του χρήστη είναι ενήμερο με απλοποιημένο και οργανωμένο τρόπο σχετικά με την πολιτική ιδιωτικότητας που επιθυμεί ο χρήστης και δεν αναζητά στην ιστοσελίδα που επισκέπτεται την πολιτική που εφαρμόζει αυτή. Συμπερασματικά αποτελεί μία προσπάθεια ανάπτυξης αυτόματης επικοινωνίας των πρακτικών διαχείρισης των δεδομένων και των προτιμήσεων των χρηστών του ιστού σχετικά με την προστασία της ιδιωτικότητάς τους.

***Ευπάθειες/μειονεκτήματα**:* Αν και το P3P παρέχει έναν τεχνικό μηχανισμό ενημέρωσης των χρηστών σχετικά με τις πολιτικές που εφαρμόζει ο ιστότοπος που επισκέπτεται σχετικά με την προστασία της ιδιωτικότητας πριν αποκαλύψει τα προσωπικά του δεδομένα δεν παρέχει, όμως, κάποιον τεχνικό μηχανισμό που να διασφαλίζει την τήρηση αυτών των πολιτικών προστασίας.

Επίσης δεν παρέχει κάποιον μηχανισμό προστασίας για την μετάδοση των δεδομένων ή για την εξασφάλιση της προστασίας τους κατά την μετάδοση ή την αποθήκευσή τους και δεν παρέχει καμία προστασία έναντι κακόβουλων επιθέσεων. Μπορεί όμως να λειτουργήσει συμπληρωματικά με άλλα εργαλεία που παρέχουν μηχανισμούς προστασίας έναντι διαφόρων κακόβουλων επιθέσεων.

Κεφάλαιο 4
Σύγκριση των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας

Στο παρόν κεφάλαιο θα παρουσιαστεί μία συγκριτική ανάλυση των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας σε σχέση με την προστασία που προσφέρουν απέναντι στις απειλές κατά της ιδιωτικότητας, όπως αυτές παρατέθηκαν στο 2ο κεφάλαιο.

4.1 Επίθεση Ανάλυσης Κίνησης

- ***LPWA***: Το LPWA είναι ευπαθές σε κάποιον αντίπαλο που παρακολουθεί και αναλύει την κίνηση παρόλο που η επικοινωνία μεταξύ του πληρεξούσιου και του εξυπηρετητή είναι δύσκολο να παρακολουθηθεί. Η επικοινωνία του χρήστη με τον πληρεξούσιο είναι εκτεθειμένη στην επίθεση αυτή.

- ***Anonymizer***: Η επικοινωνία του χρήστη με τον εξυπηρετητή πραγματοποιείται μέσω του πληρεξούσιου του Anonymizer. Ο χρήστης επικοινωνεί με τον Anonymizer διαμέσου ενός εικονικού ιδιωτικού δικτύου που δημιουργεί ένα κρυπτογραφημένο τούνελ εμποδίζοντας με αυτόν τον τρόπο την ανάλυση της κίνησης από κάποιον αντίπαλο. Στη συνέχεια ο Anonymizer προσδίδει στον χρήστη μία ψεύτικη διεύθυνση IP με την οποία επικοινωνεί με τον εξυπηρετητή αποκρύπτοντας την πραγματική διεύθυνση του χρήστη και εμποδίζοντας τον αντίπαλο να παρακολουθήσει και να αναλύσει την κίνηση προστατεύοντας από την επίθεση αυτή.

- ***Mixminion***: Αν και το mixminion χρησιμοποιεί το TLS πρωτόκολλο για την παροχή κρυπτογραφημένου καναλιού επικοινωνίας μεταξύ του χρήστη και μεταξύ των κόμβων του δικτύου που μετέχουν σε αυτό η προστασία έναντι αυτής της επίθεσης δεν είναι επαρκής. Οι κρυπτογραφημένες συνδέσεις μεταξύ των «τίμιων» κόμβων αποτρέπουν τον αντίπαλο να αναγνωρίσει ακόμα και τα δικά του μηνύματα αλλά χωρίς την συμπλήρωση και κίνηση του συνδέσμου επικοινωνίας με τεχνικό φορτίο "link padding", μπορεί να μετρήσει πόση κίνηση μεταφέρεται στο δίκτυο [20].

  Επίσης η πολιτική εξόδου που περιγράφει σε ποια διεύθυνση και με πια μέθοδο ένας κόμβος mix θα παραδώσει τα μηνύματά του αποτελεί ευπαθές σημείο για τους remailers [20]. Το mixminion αποτελείται από τις παρακάτω κατηγορίες κόμβων: οι ανοιχτοί κόμβοι εξόδου που μπορούν να παραδώσουν σε οποιοδήποτε εξυπηρετητή προορισμού, οι μεσάζοντες (middleman) κόμβοι οι οποίοι απλά αναμεταδίδουν κίνηση σε άλλους κόμβους επαναποστολείς και οι ιδιωτικοί κόμβοι εξόδου που απλά παραδίδουν τοπικά. Η ευπαθής ομάδα κόμβων είναι οι ανοιχτοί κόμβοι εξόδου. Όσο μικρότερος ο αριθμός τους τόσο πιο ευπαθές είναι το σύστημα στον αντίπαλο να παρακολουθήσει την κίνηση του δικτύου.

- ***Crowds***: Η δημιουργία τυχαίων μονοπατιών δρομολόγησης προσθέτει κάποιο βαθμό δυσκολίας στον αντίπαλο που παρακολουθεί και αναλύει την κίνηση του δικτύου παρ όλα αυτά η στατικότητα των μονοπατιών αυτών καθιστά ευπαθές τον μηχανισμό του Crowds στην επίθεση αυτή.

- ***AP3***: Το AP3 είναι ευπαθές σε παθητικές επιθέσεις. Ένας παθητικός αντίπαλος μπορεί να παρακολουθήσει την κίνηση στο δίκτυο και να συμπεράνει τον αποστολέα ή τον

παραλήπτη ενός μηνύματος. Επίσης ακόμα και αν παρακολουθεί την κίνηση ενός κόμβου του μονοπατιού, δηλαδή τα πακέτα που εισέρχονται και εξέρχονται από αυτόν μπορεί να συμπεράνει την ιδιότητά του κόμβου αυτού. Η δημιουργία ωστόσο ανώνυμων στατικών καναλιών για να καθίσταται δυνατή η απάντηση του παραλήπτη στον αποστολέα κάνει ακόμα πιο ευπαθές το σύστημα σε αυτή την επίθεση.

- ***Tarzan***: Οι Freedman και Morris δίνουν λύση στην επίθεση αυτή χρησιμοποιώντας εικονική κίνηση αποκαλούμενη και ως mimic traffic η οποία πραγματοποιείται σε μια σταθερή βάση ανάμεσα στους συμμετέχοντες ομότιμους κόμβους [47]. Ο κάθε κόμβος με την σύνδεση του στο δίκτυο εγκαθιστά συνδέσεις με k mimics κόμβους, από το σύνολο των επικυρωμένων κόμβων, ώστε να ανταλλάξει στη συνέχεια εικονική κίνηση. Ο κόμβος εγκαθιστά μία αμφίδρομη και χρονικά αμετάβλητη ροή πακέτων με τον κόμβο mimic στην οποία τα πραγματικά δεδομένα μπορούν να εισέλθουν. Τα πακέτα δεδομένων, σε αυτή την περίπτωση είναι δυσδιάκριτα από τα πακέτα κίνησης.

- ***TOR***: Το TOR προστατεύει από τους αντιπάλους που προσπαθούν να αναλύσουν την κίνηση στο δίκτυο. Δεν συνδέει απευθείας την πηγή με τον προορισμό αλλά τα πακέτα των δεδομένων μεταδίδονται στο δίκτυο του TOR διαμέσου διαφόρων κόμβων "relays" που καλύπτουν τα ίχνη τους ώστε κανένας παρατηρητής να μην μπορεί να εντοπίσει τον εκκινητή και τον προορισμό των δεδομένων. Σχεδιαστικά, όμως δεν προστατεύει από του επιτιθέμενους που ελέγχουν τα άκρα του.

- ***Java Anon Proxy***: Το JAP παρέχει προστασία σε ικανοποιητικό βαθμό σε αυτή την επίθεση με την αποστολή μηνυμάτων που δεν περιέχουν δεδομένα από το αρχικό σημείο της επικοινωνίας στο δίκτυο mix (πχ τον χρήστη) με αποτέλεσμα να καθίσταται δύσκολη η ανάλυση της κίνησης του δικτύου από κάποιον αντίπαλο. Με αυτό τον τρόπο δημιουργείται στο δίκτυο εικονική κίνηση. Τα εικονικά πακέτα ακολουθούν την κρυπτογράφηση των πακέτων του χρήστη που μεταδίδονται στο δίκτυο και ο αντίπαλος που ενδέχεται να παρατηρεί όλο το δίκτυο δεν μπορεί να διαχωρίσει ποιος χρήστης στέλνει πραγματικά δεδομένα που περιέχουν πληροφορία και ποιος εκονικά πακέτα [05].

- ***Morphmix***: Οι κόμβοι συμμετέχουν στο Morphmix με δυναμικό τρόπο, λαμβάνοντας μέρος και αποχωρώντας οποιαδήποτε χρονική στιγμή, παρέχοντας την δυνατότητα σε

κάθε χρήστη να αποτελεί ταυτόχρονα και έναν mix κόμβο καθιστώντας με αυτόν τον τρόπο δυσκολία στην ανάλυση της κίνησης από κάποιων αντίπαλο. Επίσης οι κόμβοι που συμμετέχουν στο δίκτυο του Morphmix δεν είναι αναγκαίο να βρίσκονται στο ίδιο υποδίκτυο αλλά σε διαφορετικά με αποτέλεσμα η ανάλυση της κίνησης σε ένα μεγάλο εύρος συνδέσεων μεταξύ των συμμετεχόντων κόμβων διαφόρων υποδικτύων να δυσχεράνει την ανάλυση της κίνησης σε αυτό.

- ***I2P***: Το δίκτυο καθίσταται ευπαθές στην ανάλυση της κίνησης από ισχυρούς παθητικούς εξωτερικούς παρατηρητές όπως και από έναν μεγάλο αριθμό από εσωτερικούς συνεργαζόμενους κακόβουλους παρατηρητές οι οποίοι απλά παρακολουθούν την συχνότητα των μηνυμάτων που διέρχονται ανάμεσα από τους δρομολογητές. Παρόλα αυτά ένα ευρύ ερευνητικό φάσμα υπαρχουσών ερευνών στην αντιμετώπιση των κακόβουλων αντιπάλων που προαναφέρθηκαν, έχει αναπτυχθεί και εστιάζουν στην μετατροπή των τούνελ σε δικό τους mix-cascade, προσθέτοντας χρονική καθυστέρηση στη διάδοση των μηνυμάτων, αναδιατάσσοντας τα μηνύματα και μεταδίδοντας εικονικά μηνύματα (μη ευδιάκριτα από τα μηνύματα ωφέλιμου φορτίου), μπορούν να εφαρμοστούν στις υπάρχουσες στρατηγικές.

- ***GNUnet***: Το GAP καθιστά δύσκολη την ανάλυση της κίνησης στο δίκτυο GNUnet. Οι ενέργειες των κόμβων επικαλύπτονται από την επιπρόσθετη κίνηση που προσδίδει ο κάθε κόμβος στο δίκτυο. Επίσης στο πρωτόκολλο GAP ο κόμβος εκκινητής ενεργεί όπως οι ενδιάμεσοι κόμβοι με αποτέλεσμα να μην διαχωρίζονται οι ενέργειές του στο δίκτυο από τους άλλους κόμβους και αυτό εμποδίζει κάποιον αντίπαλο από την ανάλυση της κίνησης του δικτύου. Αξιοσημείωτο είναι επίσης το ότι ένας αντίπαλος που ενδέχεται να αναλύει την κίνηση στο δίκτυο δεν μπορεί να ξεχωρίσει τα ερωτήματα από τις απαντήσεις που περιέχουν δεδομένα εφόσον έχουν το ίδιο μέγεθος.

- ***P5***: Τα πακέτα θορύβου που διαδίδονται στο δίκτυο ανά τακτά χρονικά διαστήματα καθιστούν ένα εμπόδιο δυσκολίας στην ανάλυση της κίνησης.

- ***Herbivore***: Το Herbivore παρέχει μηχανισμό προστασίας της ανάλυσης της κίνησης από κάποιον αντίπαλο. Στο πρωτόκολλο round στο οποίο καθορίζεται η συμπεριφορά των συμμετεχόντων κόμβων σε ένα clique, η φάση εξόδου προστατεύει τις συναλλαγές μεγάλης διάρκειας στο δίκτυο από την ανάλυση της κίνησης. Κυρίως οι συναλλαγές αυτές των χρηστών καθιστούν ευπαθές το σύστημα στην επίθεση της ανάλυσης της

κίνησης. Το Herbivore όμως προστατεύει ικανοποιητικά τους χρήστες του από μια τέτοια επίθεση.

- ***Mantis***: Στο Mantis ένας αντίπαλος παρακολουθώντας την κρυπτογραφημένη κίνηση κάποιων κόμβων που συμμετέχουν στο δίκτυο ενδέχεται να συμπεράνει τον εκκινητή ενός αιτήματος ή τον εξυπηρετητή. Εφόσον δεν εφαρμόζεται κάποιος μηχανισμός αποπροσανατολισμού του επιτιθέμενου που παρακολουθεί την κίνηση του δικτύου όπως η εικονική κίνηση καθίσταται ευπαθές στην επίθεση αυτή.

- ***Mute***: Κάποιος επιτιθέμενος έχει την δυνατότητα να παρακολουθήσει την κίνηση ενός τμήματος του δικτύου και να την ανάλυση οδηγώντας τον σε συμπεράσματα σχετικά με την δραστηριότητα των συμμετεχόντων κόμβων.

- ***BitBlender***: Το BitBlender με την εισαγωγή στο δίκτυο των κόμβων "relay peers" προσθέτει κάποιο βαθμό δυσκολίας σε κάποιον αντίπαλο που παρακολουθεί την κίνηση στο δίκτυο. Παρ όλα αυτά όμως ένας αντίπαλος που παρακολουθεί και καταγράφει την κίνηση του δικτύου μπορεί να αποκτήσει πληροφορίες σχετικά με την συμπεριφορά των χρηστών. Επομένως το BitBlender αν και παρέχει μηχανισμό προστασίας από την επίθεση αυτή δεν καθιστά αδύνατη την παραβίαση της ανωνυμίας των χρηστών καθώς και του περιεχομένου που διαμοιράζονται στο δίκτυο.

- ***Truste***: Δεν προσφέρει καμία υπηρεσία προστασίας έναντι της επίθεσης αυτής. Στοχεύει στην εξασφάλιση πολιτικών προστασίας προσωπικών δεδομένων από τους διάφορους ιστοτόπους με αποτέλεσμα να μην εστιάζεται σε μηχανισμούς προστασίας έναντι αυτής της επίθεσης.

- ***P3P***: Το P3P δεν προσφέρει καμία προστασία έναντι κακόβουλων επιθέσεων εφόσον κύριος στόχος του αποτελεί η ενημέρωση των χρήστη με αυτοποιημένο τρόπο σχετικά με τις πρακτικές που εφαρμόζει ο ιστότοπος που επισκέπτεται για την προστασία της ιδιωτικότητας και η ενημερωμένη συγκατάθεση και συμφωνία του σχετικά με τις προτιμήσεις προστασίας της ιδιωτικότητάς του.

4.2 Ωτακουστής

- ***LPWA***: Το LPWA είναι εκτεθειμένο σε κάποιον ωτακουστή ο οποίος μπορεί να παρακολουθήσει την επικοινωνία ανάμεσα στον πληρεξούσιο και στον χρήστη.

- ***Anonymizer***: Ένας ωτακουστής είναι πολύ δύσκολο να παρακολουθήσει την κίνηση λόγω του ότι πραγματοποιείται διαμέσου κρυπτογραφημένου τούνελ μεταξύ του χρήστη και του πληρεξούσιου του Anonymizer ο οποίος στη συνέχεια αλλάζει την IP του χρήστη για να επικοινωνήσει με τον εξυπηρετητή. Ο τρόπος επικοινωνίας είναι ασφαλής σε ικανοποιητικό βαθμό εμποδίζοντας έναν ωτακουστή να παρεμβληθεί στον δίαυλο επικοινωνίας.

- ***Mixminion***: Η κρυπτογράφηση του καναλιού επικοινωνίας με το πρωτόκολλο TLS, η χρησιμοποίηση προσωρινών κλειδιών, η χρησιμοποίηση της στρατηγικής δεσμών "dynamic pool", η αναδιάταξη των μηνυμάτων σε κάθε κόμβο mix πριν την αποστολή τους στον επόμενο κόμβο παρέχουν ικανοποιητικό βαθμό προστασίας από κάποιον ωτακουστή.

- ***Crowds***: Το Crowds κρυπτογραφεί όλη την επικοινωνία μεταξύ των jondo και αυτό καθιστά δύσκολη την εύρεση του παραλήπτη από έναν τοπικό ωτακουστή που παρακολουθεί την κίνηση του υπολογιστή του χρήστη. Η πιθανότητα να εντοπιστεί ο παραλήπτης από έναν τοπικό ωτακουστή μειώνεται όσο τα μέλη του πλήθους αυξάνονται.

- ***AP3***: Ένας ωτακουστής που παρακολουθεί την κίνηση ενός κόμβου, τα εισερχόμενα και τα εξερχόμενα μηνύματα που διέρχονται από αυτόν, μπορεί να συμπεράνει αν ο κόμβος αυτός είναι ο αποστολέας ή ο παραλήπτης. Επίσης η δημιουργία στατικών μονοπατιών καθώς και ότι το μήνυμα που διέρχεται από τους κόμβους δεν είναι κρυπτογραφημένο κάνει το σύστημα πιο ευπαθές στην επίθεση των ωτακουστών.

- ***Tarzan***: Το Tarzan με την εφαρμογή της εικονικής κίνησης (mimic traffic) παρέχει προστασία σε ικανοποιητικό βαθμό από την επίθεση αυτή. Οι επικεφαλίδες των πακέτων, το μέγεθος τους και οι ρυθμοί της εισερχόμενης κίνησης σε έναν κόμβο από τους κόμβους mimic είναι πανομοιότυπη με την εξερχόμενη κίνηση ώστε ένας

ωτακουστής να μην μπορεί να συμπεράνει αν ο κόμβος είναι ο αποστολέας του μηνύματος ή απλά αναμεταδότης στο τούνελ [26].

- ***TOR***: Η ισχυρή κρυπτογραφία που χρησιμοποιείται στο δίκτυο του TOR καθώς και το ότι ο κάθε αναμεταδότης γνωρίζει μόνο τον κόμβο που παρέλαβε τα δεδομένα και τον κόμβο που θα προωθήσει τα δεδομένα προστατεύει από κάποιον ωτακουστή που παρακολουθεί την κίνηση και δεν μπορεί να συνδέσει την πηγή με τον προορισμό των δεδομένων.

- ***Java Anon Proxy***: Παρέχει προστασία από τους ωτακουστές οι οποίοι παρακολουθούν ένα σημείο του δικτύου ή προσπαθούν να ελέγξουν έναν κόμβο mix [32].

- ***Morphmix***: Η πολυεπίπεδη κρυπτογράφηση και η κρυπτογράφηση του συνδέσμου (link encryption) μεταξύ των ομότιμων κόμβων εμποδίζει έναν ωτακουστή να συμπεράνει τον εκκινητή ή τον παραλήπτη. Επίσης το ότι ο κάθε ομότιμος κόμβος γνωρίζει μόνο τους γείτονές του και τον άμεσο διάδοχό του στο τούνελ δεν διευκολύνει τον ωτακουστή να αντλήσει πληροφορίες που παραβιάζουν την ανωνυμία του χρήστη. Μπορεί όμως να εκμαιεύσει πληροφορίες σχετικά με τον χρήστη εάν παρακολουθεί ταυτόχρονα τον εκκινητή και τον τελικό κόμβο του τούνελ αλλά παρόλα αυτά ο χρήστης επανακτά την ανωνυμία του μόλις η επικοινωνία του με τον εξυπηρετητή μεταβεί σε άλλο τούνελ.

- ***I2P***: Η πολυεπίπεδη κρυπτογράφηση των μηνυμάτων και η κρυπτογράφηση των συνδέσμων βοηθούν στην προστασία από κάποιον ωτακουστή. Ιδιαίτερα ευπαθές μετατρέπεται το δίκτυο από κάποιον ωτακουστή που παρακολουθεί τον πρώτο και τον τελευταίο κόμβο των τούνελ.

- ***GNUnet***: Το GAP παρέχει μηχανισμούς προστασίας από αυτή την επίθεση με τη χρήση κρυπτογράφησης ζεύξης (link encryption), με την συμπλήρωση των μηνυμάτων ώστε να έχουν όλα το ίδιο μέγεθος και την εικονική κίνηση που δημιουργείται στο δίκτυο.

- ***P5***: Τα πακέτα που μεταδίδονται με το πρωτόκολλο P5 συμπληρώνονται όλα ώστε να έχουν το ίδιο μέγεθος και διακρίνονται σε πακέτα θορύβου, σήματος και δεδομένων. Ένας ωτακουστής δεν μπορεί να διακρίνει τα πακέτα σήματος και θορύβου από τα πακέτα δεδομένων και αυτό προσθέτει ένα επίπεδο δυσκολίας στην επίθεση αυτή.

- ***Herbivore***: Είναι δύσκολο για κάποιον ωτακουστή να παρακολουθήσει το δίκτυο και να συμπεράνει τον αποστολέα ενός μηνύματος ή τον παραλήπτη εφόσον οι χρήστες του Herbivore ομαδοποιούνται σε cliques. Το πρωτόκολλο round καθορίζει την συμπεριφορά των κόμβων και διασφαλίζει την ανώνυμη μετάδοση των δεδομένων και ανιχνεύει τυχών ενέργεια παραβίασης. Εάν όμως κάποια από τα επικοινωνούντα άκρα σε μια επικοινωνία δεν αποτελούν τμήμα του Herbivore τότε τα δεδομένα εκτίθενται σε τρίτα μέρη και σε ωτακουστές αντίπαλους. Το Herbivore προστατεύει λοιπόν εντός του δικτύου που υποστηρίζει από την επίθεση των ωτακουστών.

- ***Mantis***: Το Mantis προστατεύει σε ικανοποιητικό βαθμό από έναν ωτακουστή που παρακολουθεί την κίνηση που διέρχεται σε ένα ή περισσότερα jondos. Λόγω των κρυπτογραφημένων μηνυμάτων και της αποστολής τους κατά την διαδικασία της αναζήτησης σε όλους τους γείτονες κόμβους δε μπορεί να συμπεράνει τον αποστολέα ή τον παραλήπτη καθώς και το περιεχόμενο των μηνυμάτων. Μόνο στην περίπτωση της αποστολής μηνυμάτων διαμέσου του καναλιού UDP όπου αποκαλύπτεται η διεύθυνση του πελάτη ή του εξυπηρετητή ενδέχεται ένας ωτακουστής να παραβιάσει την ανωνυμία του αποστολέα ή του παραλήπτη αλλά όχι το περιεχόμενο της επικοινωνίας του. Επίσης ενδέχεται ένας ωτακουστής να συμπεράνει τον εκκινητή ενός μηνύματος εάν διαπιστώσει ότι ο κόμβος που παρακολουθεί στέλνει μηνύματα αλλά δεν λαμβάνει από κάποιον γείτονα κόμβο. Υπάρχουν τεχνικές αντιμετώπισης όπως η εικονική κίνηση οι οποίες δεν έχουν εφαρμοστεί ακόμα.

- ***Mute***: Ένας ωτακουστής μπορεί να παρακολουθεί με παθητικό τρόπο την κίνηση που εισέρχεται και εξέρχεται από κάποιον κόμβο αλλά δεν μπορεί να γνωρίζει τα περιεχόμενα του μηνύματος λόγω της κρυπτογράφησής τους. Μπορεί να συμπεράνει με δυσκολία την ιδιότητα του κόμβου παρατηρώντας την δραστηριότητά του με βάση την κίνηση που διέρχεται από αυτόν. Το δίκτυο Mute δεν προστατεύει από κάποιον αντίπαλο που ενεργεί ως ωτακουστής.

- ***BitBlender***: Το BitBlender δεν εφαρμόζει κάποιον μηχανισμό προστασίας από κάποιον ωτακουστή που παρακολουθεί την κίνηση που εισέρχεται και εξέρχεται από κάποιον κόμβο. Δεν αποκρύπτει το περιεχόμενο των δεδομένων που διακινούνται στο δίκτυο εφόσον όλα τα δεδομένα "torrent" είναι διαθέσιμα δημοσίως επομένως δεν είναι απαραίτητο να χρησιμοποιήσει κάποιον μηχανισμό προστασίας των δεδομένων από τους τοπικούς ωτακουστές.

- ***Truste***: Στοχεύει στην διασφάλιση πολιτικών προστασίας προσωπικών δεδομένων και δεν προσφέρει μηχανισμούς προστασίας έναντι επιθέσεων. Τα δεδομένα που μεταδίδονται δεν αποκρύπτονται από τους ωτακουστές.

- ***P3P***: Το P3P δεν προσφέρει καμία προστασία έναντι κακόβουλων επιθέσεων εφόσον κύριος στόχος του αποτελεί η ενημέρωση των χρήστη με αυτοματοποιημένο τρόπο σχετικά με τις πρακτικές που εφαρμόζει ο ιστότοπος που επισκέπτεται για την προστασία της ιδιωτικότητας και η ενημερωμένη συγκατάθεση και συμφωνία του σχετικά με τις προτιμήσεις προστασίας της ιδιωτικότητάς του.

4.3 Επίθεση Χρονισμού

- ***LPWA***: Το LPWA είναι ευπαθές στην επίθεση αυτή καθώς μία τέτοια επίθεση δεν είναι εύκολο να αντιμετωπιστεί.

- ***Anonymizer***: Αν και μία τέτοια επίθεση είναι δύσκολο να αντιμετωπιστεί παρόλα αυτά το Anonymizer προσφέρει προστασία στην επίθεση αυτή με την παρεμβολή, στην επικοινωνία του χρήστη με τον εξυπηρετητή, του πληρεξούσιου διαμέσου ενός κρυπτογραφημένου τούνελ και την χρησιμοποίηση ψεύτικης διεύθυνσης IP, η οποία δεν είναι στατική αλλά δυναμική. Με αυτόν τον τρόπο δεν μπορεί να επιτευχθεί χρονικός συσχετισμός των συνδέσεων του χρήστη με τον εξυπηρετητή ούτε να υπάρξει χρονική ανάλυση των περιόδων σύνδεσης του χρήστη.

- ***Mixminion***: Το mixminion προστατεύει από την επίθεση αυτή γιατί στην προσπάθειά του να καλύψει τον χρονικό συσχετισμό των μηνυμάτων οι κόμβοι χρησιμοποιούν την στρατηγική επεξεργασίας δεσμών "timed dynamic pool", δηλαδή ο κάθε κόμβος mix δεν στέλνει το μήνυμα στον επόμενο προορισμό του αλλά αποκρυπτογραφεί το στρώμα που του αντιστοιχεί, τα συγκεντρώνει σε μία «πισίνα», τα αναδιατάσσει και μετά τα στέλνει στους επόμενους προορισμούς.

- ***Crowds***: Η επικοινωνία του χρήστη με τον εξυπηρετητή πραγματοποιείται διαμέσου των jondos δημιουργώντας με τυχαία επιλογή το μονοπάτι δρομολόγησης το οποίο παραμένει στατικό. Η στατικότητα του μονοπατιού δρομολόγησης αφήνει ανοιχτό

σημείο ευπάθειας στο σύστημα σε κάποιον αντίπαλο που εκτελεί χρονικούς συσχετισμούς των ερωτήσεων – αποκρίσεων και των περιόδων σύνδεσης.

- ***AP3***: Η δημιουργία ανώνυμων καναλιών καθιστά ιδιαίτερα ευπαθές το AP3 στον χρονικό συσχετισμό των πακέτων που αποστέλλονται σε κάποιον κόμβο. Τα ανώνυμα μονοπάτια που εγκαθίστανται ισχύουν για κάποια χρονική περίοδος και αντιστοιχίζονται σε κάποιο ψευδώνυμο, κόμβο, με αποτέλεσμα η συνεχή αποστολή μηνυμάτων αλλά και η παραλαβή τον αποκρίσεων διαμέσου αυτού του μονοπατιού ενδέχεται να συσχετιστεί χρονικά και να αποκαλύπτει η ιδιότητά του.

- ***Tarzan***: Ένας στατικός αντίπαλος μπορεί να διαφθείρει κάποιους κόμβους του συστήματος, προγενέστερα, ώστε να έχει τη δυνατότητα παρακολούθησης της συμπεριφοράς του [26]. Μπορεί να διαβάζει πακέτα που εισέρχονται στους κόμβους που ελέγχει καθώς και να αναλύσει τα δεδομένα, το μέγεθος, τους ρυθμούς και τον όγκο των μηνυμάτων. Ο αντίπαλος μπορεί να χρησιμοποιήσει την χρονική ανάλυση των πακέτων και να αποφασίσει αν τα πακέτα που αναμεταδίδονται από διαφορετικούς αναμεταδότες ανήκουν στο ίδιο τούνελ αλλά δεν μπορεί να υπολογίσει την απόσταση που έχουν οι αναμεταδότες στο τούνελ.

- ***TOR***: Το TOR δεν προστατεύει από την επίθεση αυτή. Εάν ο αντίπαλος μπορεί να παρακολουθήσει την κίνηση που εξέρχεται από τον χρήστη καθώς και την κίνηση που φτάνει στον επιλεγόμενο προορισμό μπορεί να χρησιμοποιήσει στατιστική ανάλυση ώστε να αποκαλύψει ότι είναι τμήμα του ίδιου κυκλώματος.

- ***Java Anon Proxy***: Το JAP παρέχει μηχανισμούς προστασίας από αυτή την επίθεση. Καταρχήν η εικονική κίνηση που δημιουργείται στο δίκτυο αποτελείται από κρυπτογραφημένα πακέτα με αποτέλεσμα να μην μπορούν να διαχωριστούν από τα πραγματικά πακέτα δεδομένων. Αυτό προσθέτει κάποιο βαθμό δυσκολίας στον χρονικό συσχετισμό των πακέτων από κάποιον παρατηρητή. Επίσης η αποστολή εικονικής κίνησης εγγυάται ότι όλοι οι χρήστες του JAP στέλνουν τον ίδιο αριθμό πακέτων κατά την διάρκεια κάθε χρονοσφραγίδας [05]. Κάθε mix αναδιατάσσει τα πακέτα που λαμβάνει και αλλάζει την κωδικοποίησή τους χρησιμοποιώντας ισχυρό μηχανισμό κρυπτογράφησης και δημιουργώντας με αυτόν τον τρόπο προστασία από τον χρονικό συσχετισμό της κίνησης του δικτύου από διενεργεί κάποιος αντίπαλος.

- ***Morphmix***: Οι ομότιμοι κόμβοι στο Morphmix συμμετέχουν δυναμικά στο δίκτυο και αυτό καθιστά κάποιο βαθμό δυσκολίας στην επίθεση χρονισμού. Ο αντίπαλος μπορεί ενδέχεται να συσχετίσει τα δεδομένα που εισέρχονται και εξέρχονται από κάποιον κόμβο Mix βασιζόμενος στον χρόνο. Αν και η πολυεπίπεδη κρυπτογράφηση και το σταθερό μέγεθος των κελιών προσθέτει κάποιο βαθμό δυσκολίας στην επίθεση αυτή είναι δύσκολο να αποτραπεί αποτελεσματικά.

- ***I2P***: Η μέθοδος garlic [63] που χρησιμοποιεί το I2P εμποδίζει σημαντικά έναν παρατηρητή που παρακολουθεί τα μηνύματα που εξέρχονται από τους κόμβους και συσχετίζει τους κόμβους που είναι συνδεδεμένοι μεταξύ τους, αλλά δεν καθιστά αδύνατη την επίθεση αυτή εάν παρακολουθεί όλους τους κόμβους που βρίσκονται κοντά στον χρήστη [23]. Η επίθεση λοιπόν αυτή είναι αρκετά ισχυρή αλλά αντιμετωπίζεται με τους διαφορετικούς χρόνους καθυστέρησης των μηνυμάτων στην ουρά, την επεξεργασία του μηνύματος και την διεργασία ρύθμισης του ρυθμού επεξεργασίας των μηνυμάτων (throttling). Λόγω του ότι οι έρευνες βελτίωσης και εξέλιξης του I2P συνεχίζονται δεν αποτρέπεται, προς το παρόν τουλάχιστον, η επίθεση αυτή αλλά παρέχεται προστασία σε ικανοποιητικό βαθμό.

- ***GNUnet***: Το GAP αντιμετωπίζει την επίθεση χρονισμού με την πρόσθεση σε κάθε άλμα τυχαίας καθυστέρησης των ερωτημάτων και των απαντήσεων. Επίσης το ότι ο κόμβος αποφασίζει τη διαδρομή του ερωτήματος προσθέτει ένα επίπεδο δυσκολίας στην επίθεση αυτή.

- ***P5***: Η προσθήκη θορύβου σε τυχαία χρονικά διαστήματα καθιστά δύσκολη την χρονική ανάλυση που ενεργείται από κάποιον επιτιθέμενο.

- ***Herbivore***: Η επίθεση αυτή είναι δύσκολη όταν οι χρήστες συμμετέχουν σε ασφαλείς ομάδες όπως στο πρωτόκολλο Herbivore που συμμετέχουν σε ομάδες ανώνυμων cliques. Εάν τα δύο άκρα που συμμετέχουν στην επικοινωνία καλύπτονται εντός του πρωτοκόλλου Herbivore προστατεύονται από αυτή την επίθεση εάν κάποιο από τα δύο άκρα βρίσκεται εκτός του πρωτοκόλλου τότε η επίθεση αυτή ενδέχεται να αποκαλύψει κάποια στοιχεία των επικοινωνούντων άκρων.

- ***Mantis***: Το Mantis είναι εκτεθειμένο σε έναν αντίπαλο που εκτελεί την επίθεση αυτή ο οποίος έχει την δυνατότητα να αποκαλύψει την ταυτότητα του εξυπηρετητή με την

ανάλυση των καθυστερήσεων των round-trip times (RTT) ανάμεσα στην αναμετάδοση των μηνυμάτων και στην απάντησή τους. Όσο πιο μακριά είναι ο εξυπηρετητής από τον χρήστη τόσο μεγαλύτερη θα είναι η καθυστέρηση ενώ αντίστροφα όσο πιο κοντά βρίσκεται η καθυστέρηση θα είναι μικρή. Επομένως οι εξυπηρετητές με την άμεση απάντηση τους εκτίθενται σε κάποιον επιτιθέμενο που ενεργεί την επίθεση αυτή [07]. Για να αντιμετωπιστεί αυτό το πρόβλημα θα πρέπει ο εξυπηρετητής να καθυστερεί την απάντηση του για ένα καθορισμένο χρονικό διάστημα και αυτή η καθυστέρηση να είναι ίδια για όλα τα μηνύματα.

- ***Mute***: Στο δίκτυο Mute αν και το περιβάλλον λειτουργίας του είναι δυναμικό, οι κόμβοι συμμετέχουν οποιαδήποτε στιγμή στο δίκτυο και αποχωρούν επίσης οποιαδήποτε στιγμή από αυτό, ο χρονικός συσχετισμός καθίσταται σχετικά δύσκολος να επιτευχθεί. Παρ όλα αυτά κάποιος αντίπαλος που παρακολουθεί ένα τμήμα του δικτύου μπορεί να συσχετίσει χρονικά τις αποκρίσεις στα ερωτήματα των κόμβων και να συμπεράνει την απόσταση του εξυπηρετητή κόμβου από την χρονική καθυστέρηση της απάντησης.

- ***BitBlender***: Στο BitBlender ο αντίπαλος συσχετίζοντας χρονικά τα δεδομένα που μετακινούνται ενδέχεται να αποκαλύψει την ταυτότητα του εκκινητή κόμβου καθώς και να προσδιορίσει κάποια relay peers. Ένας ενδιάμεσος κόμβος μπορεί να συσχετίσει την χρονική καθυστέρηση ενός αιτήματος έως ότου αυτό εκπληρωθεί και εάν ο χρόνος είναι μικρός τον οδηγεί στο συμπέρασμα ότι ο προηγούμενος κόμβος είναι ο εκκινητής. Για την αντιμετώπιση του προβλήματος αυτού προτείνονται τυχαίες καθυστερήσεις στην προώθηση των αιτημάτων ώστε να παρεμποδιστεί ο χρονικός συσχετισμός των αιτημάτων και των αποκρίσεων αλλά δεν έχουν εφαρμοστεί ακόμα.

- ***Truste***: Δεν προσφέρει καμία υπηρεσία προστασίας έναντι της επίθεσης αυτής. Στοχεύει στην εξασφάλιση πολιτικών προστασίας προσωπικών δεδομένων από τους διάφορους ιστοτόπους με αποτέλεσμα να μην εστιάζεται σε μηχανισμούς προστασίας έναντι αυτής της επίθεσης.

- ***P3P***: Το P3P δεν προσφέρει καμία προστασία έναντι κακόβουλων επιθέσεων εφόσον κύριος στόχος του αποτελεί η ενημέρωση των χρήστη με αυτοποιημένο τρόπο σχετικά με τις πρακτικές που εφαρμόζει ο ιστότοπος που επισκέπτεται για την προστασία της ιδιωτικότητας και η ενημερωμένη συγκατάθεση και συμφωνία του σχετικά με τις προτιμήσεις προστασίας της ιδιωτικότητάς του.

4.4 Επίθεση Κωδικοποίησης Μηνύματος

- ***LPWA***: Στο LPWA τα μηνύματα δεν κρυπτογραφούνται με αποτέλεσμα να παρουσιάζει σημεία ευπάθειας στην παραβίαση της ιδιωτικότητας διαμέσου της επίθεσης αυτής. Παρ όλα αυτά ο επιτιθέμενος δεν μπορεί να συσχετίσει τα δεδομένα με τον εκκινητή του αιτήματος.

- ***Anonymizer***: Αν και τα μηνύματα δεν κρυπτογραφούνται όμως η κίνηση που πραγματοποιείται διαμέσου κρυπτογραφημένου τούνελ και η αλλαγή της διεύθυνσης IP του χρήστη καθιστούν δύσκολο σε κάποιον αντίπαλο να συσχετίσει τα περιεχόμενα του μηνύματος με τον εκκινητή.

- ***Mixminion***: Η κρυπτογράφηση των πακέτων, η διαδικασία αναστροφής των κεφαλίδων "swap", η συμπλήρωση "padding" των πακέτων από κάθε κόμβο mix ώστε να έχουν όλα το ίδιο μέγεθος και η κρυπτογράφηση TLS του μηνύματος καθιστούν δύσκολη αυτή την επίθεση.

- ***Crowds***: Ο χρήστης προστατεύεται από την επίθεση κωδικοποίησης εφόσον η επικοινωνία μεταξύ των jondos πραγματοποιείται με την χρήση συμμετρικής κρυπτογράφησης, με διαμοιραζόμενα μεταξύ των jondos κλειδιά. Τα ενδιάμεσα jondos έχουν πρόσβαση στα περιεχόμενα στην επεξεργασία και ανταλλαγή τους αλλά κάποιος αντίπαλος εκτός δικτύου δεν έχει την δυνατότητα εκκίνησης μίας τέτοιας επίθεσης.

- ***AP3***: Αν και παρέχει μηχανισμό προστασίας μέσω της αυθεντικοποίησης των μηνυμάτων χρησιμοποιώντας ψευδώνυμα και κατ' επέκταση κρυπτογράφηση του μηνύματος με το δημόσιο κλειδί του ψευδωνύμου, η δημιουργία ανώνυμων καναλιών και η χρονική διάρκεια ύπαρξης αυτού προς ένα συγκεκριμένο ψευδώνυμο το καθιστά ευάλωτο σε αυτή την επίθεση.

- ***Tarzan***: Το Tarzan παρέχει μηχανισμούς προστασίας από τις επιθέσεις κωδικοποίησης μηνύματος. Ο μηχανισμός ελέγχου ακεραιότητας, η πολυεπίπεδη κρυπτογράφηση των πακέτων, καθώς και η εικονική κίνηση (mimic traffic) παρέχει στο Tarzan ικανοποιητικό βαθμό προστασίας σε αυτή την επίθεση.

- ***TOR***: Η ισχυρή κρυπτογράφηση που παρέχεται από το δίκτυο TOR προστατεύει από την επίθεση αυτή. Τα διαδοχικά στρώματα κρυπτογράφησης ανά κόμβο προσθέτουν κάποιο βαθμό δυσκολίας στην επεξεργασία των κρυπτογραφημένων μηνυμάτων.

- ***Java Anon Proxy***: Η ισχυρή πολυεπίπεδη κρυπτογράφηση των πακέτων που χρησιμοποιείται από τους ενδιάμεσους κόμβους καθιστά δύσκολη την επίθεση αυτή. Αν και η μετάδοση των πακέτων πραγματοποιείται διαμέσου καθορισμένων ακολουθιών από κόμβους mix και ο τελευταίος κόμβος αποστέλλει τα πακέτα αποκρυπτογραφημένα στον εξυπηρετητή παρόλα αυτά προστατεύεται από την επίθεση αυτή σε ικανοποιητικό βαθμό.

- ***Morphmix***: Το Morphmix προστατεύει από αυτή την επίθεση λόγω της ισχυρής πολυεπίπεδης κρυπτογράφησης. Επίσης η κρυπτογράφηση της κεφαλίδας ενός μηνύματος και του ωφέλιμου φορτίου με το κλειδί του αντίστοιχου εικονικού συνδέσμου και το ίδιο μέγεθος των μηνυμάτων προσθέτουν κάποιον βαθμό δυσκολίας στον επιτιθέμενο που ενεργεί την επίθεση αυτή.

- ***I2P***: Το I2P χρησιμοποιεί για την κρυπτογράφηση από άκρη σε άκρη δεικτοδότηση των συνόδων (session tags). Κάθε δεικτοδότηση της συνόδου χρησιμοποιείται μόνο μία φορά αποτρέποντας έτσι τους εσωτερικούς αντίπαλους από την επίθεση αυτή. Επίσης η ισχυρή πολυεπίπεδη κρυπτογράφηση του μηνύματος προστατεύει από την επίθεση αυτή.

- ***GNUnet***: Το πρωτόκολλο GAP προστατεύει το δίκτυο GNunet από την επίθεση κωδικοποίησης μηνυμάτων. Μηχανισμοί προστασίας έναντι της επίθεσης αυτής αποτελούν το ίδιο μέγεθος των μηνυμάτων που μεταφέρονται στο δίκτυο, με αποτέλεσμα τα πακέτα που περιέχουν δεδομένα να μην διακρίνονται από τα πακέτα που περιέχουν ερωτήματα και το ισχυρό πλαίσιο κρυπτογράφησης της ζεύξης που δημιουργείται στο πρωτόκολλο GAP.

- ***P5***: Στο P5 καθίσταται δύσκολη μία τέτοια επίθεση λόγω της ισχυρής κρυπτογράφησης των μηνυμάτων. Τα πακέτα που μεταδίδονται αποτελούνται από μικρά κρυπτογραφημένα τμήματα με το κάθε ένα από αυτά να κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη..

- ***Herbivore***: Η επίθεση αυτή καθίσταται δύσκολη στο πρωτόκολλο Herbivore εφόσον οι κόμβοι εντάσσονται σε ασφαλείς ομάδες cliques. Εάν όμως η επικοινωνία επεκτείνεται και εκτός των καλυπτόμενων κόμβων από το πρωτόκολλο τότε ο αντίπαλος ενδέχεται να αντλήσει κάποιος πληροφορίες από την επίθεση κωδικοποίησης.

- ***Mantis***: Τα μηνύματα που αναμεταδίδονται στο δίκτυο κρυπτογραφούνται από jondo σε jondo. Αν και δεν χρησιμοποιείται μέθοδος συμπλήρωσης των μηνυμάτων ώστε να έχουν όλα το ίδιο μέγεθος παρ όλα αυτά η κρυπτογράφησή τους σε κάθε άλμα με το συμφωνημένο μυστικό κλειδί μεταξύ των γειτόνων κόμβων καθιστά δύσκολη μία τέτοια επίθεση.

- ***Mute***: Το δίκτυο Mute δεν παρέχει μηχανισμό προστασίας σε αυτήν την επίθεση. Δεν χρησιμοποιείται κάποιος μηχανισμός συμπλήρωσης των μηνυμάτων ώστε να έχουν όλα το ίδιο μέγεθος και επίσης κάθε κόμβος έχει πρόσβαση στα περιεχόμενα των μηνυμάτων που λαμβάνει με αποτέλεσμα για κάποιον κακόβουλο συνεργό εντός δικτύου να μην τίθεται θέμα επίθεσης κωδικοποίησης ενώ κάποιος παθητικός αντίπαλος να έχει την δυνατότητα εκτέλεσης της επίθεσης αυτής.

- ***BitBlender***: Το BitBlender δεν χρησιμοποιεί κρυπτογράφηση στον διαμοιρασμό αρχείων αν και δεν είναι απαραίτητο να παρέχει εμπιστευτικότητα στα περιεχόμενα που διαμοιράζεται εφόσον το BitTorrent είναι ένα πρωτόκολλο που τα περιεχόμενά του δεν διαρρέουν πληροφορίες προσωπικών δεδομένων όπως στο HTTP και είναι προσβάσιμα από όλους. Επομένως δεν παρέχει μηχανισμό προστασίας σε αυτή την επίθεση εφόσον δεν αποτελεί σκοπός του πρωτοκόλλου η απόκρυψη των περιεχομένων των δεδομένων που διακινούνται στο δίκτυο.

- ***Truste***: Δεν προσφέρει καμία υπηρεσία προστασίας έναντι της επίθεσης αυτής. Στοχεύει στην εξασφάλιση πολιτικών προστασίας προσωπικών δεδομένων από τους διάφορους ιστοτόπους με αποτέλεσμα να μην εστιάζεται σε μηχανισμούς προστασίας έναντι αυτής της επίθεσης.

- ***P3P***: Το P3P δεν προσφέρει καμία προστασία έναντι κακόβουλων επιθέσεων εφόσον κύριος στόχος του αποτελεί η ενημέρωση των χρήστη με αυτοποιημένο τρόπο σχετικά με τις πρακτικές που εφαρμόζει ο ιστότοπος που επισκέπτεται για την προστασία της

ιδιωτικότητας και η ενημερωμένη συγκατάθεση και συμφωνία του σχετικά με τις προτιμήσεις προστασίας της ιδιωτικότητάς του.

4.5 Επίθεση Traceback Παθητική/Ενεργή

- ***LPWA***: Το LPWA δεν προστατεύει από επιθέσεις traceback. Τα μηνύματα δεν κρυπτογραφούνται με αποτέλεσμα η κίνηση από και προς τον μοναδικό πληρεξούσιο να είναι εκτεθειμένη σε επιθέσεις traceback.

- ***Anonymizer***: Το Anonymizer κατευθύνοντας την κίνηση του χρήστη προς τον εξυπηρετητή διαμέσου ενός εικονικού ιδιωτικού δικτύου δημιουργώντας με αυτόν τον τρόπο ένα κρυπτογραφημένο τούνελ και αντικαθιστώντας την IP του χρήστη με μια ψεύτικη διεύθυνση IP προστατεύει από επιθέσεις traceback είτε ενεργές είτε παθητικές. Ο αντίπαλος αδυνατεί να παρακολουθήσει την κίνηση που κατευθύνεται διαμέσου του κρυπτογραφημένου τούνελ προς τον πληρεξούσιο του Anonymizer καθώς και να ιχνηλατήσει τα μηνύματα από και προς τον χρήστη ή τον εξυπηρετητή.

- ***Mixminion***: Η κρυπτογράφηση του καναλιού επικοινωνίας, η χρήση προσωρινών κλειδιών, η χρησιμοποίηση της στρατηγικής δεσμών "dynamic pool" από κάθε κόμβο, η αναδιάταξη, η αποστολή πολλών πακέτων ταυτόχρονα και η χρησιμοποίηση SURBs για την αποστολή ανώνυμων μηνυμάτων καθιστά δύσκολη την ιχνηλάτιση του μονοπατιού από τον αποστολέα προς τον παραλήπτη και αντίστροφα και προστατεύει από ενεργές και παθητικές επιθέσεις ιχνηλάτισης μονοπατιού.

- ***Crowds***: Το Crowds λόγω της συμμετρικής κρυπτογράφησης που χρησιμοποιεί στην επικοινωνία μεταξύ των μελών του προστατεύει από ενεργές επιθέσεις traceback ενώ παρουσιάζει ευπάθεια στις παθητικές επιθέσεις traceback. Ο αντίπαλος εάν δεσμεύσει κάποιον αριθμό από Jondos ενδέχεται να εντοπίσει τον εκκινητή του μηνύματος και να αποκτήσει πληροφορίες δρομολόγησης.

- ***AP3***: Η δημιουργία ανώνυμων καναλιών μεγάλης χρονικής διάρκειας και η αντιστοίχησή τους με κάποιο ψευδώνυμο κόμβου καθιστούν δυνατή την ιχνηλάτιση του μονοπατιού τόσο ενεργά όσο και παθητικά.

- ***Tarzan***: Ο μηχανισμός κρυπτογράφησης ο οποίος είναι παρόμοιος με τα δίκτυα mix, που χρησιμοποιεί το Tarzan, η δημιουργία εικονικής κίνησης (mimic traffic) κατά την αποστολή και παραλαβή πακέτων πραγματικών δεδομένων καθώς και ο μηχανισμός ελέγχου ακεραιότητας καθιστά δύσκολη την ιχνηλάτιση των πακέτων για τον εντοπισμό είτε του αποστολέα, είτε του παραλήπτη, είτε και των δύο. Η κίνηση επικάλυψης που δημιουργείται μεταξύ των κόμβων mimic με σταθερό ρυθμό και η κρυπτογράφηση που πραγματοποιείται έχει ως αποτέλεσμα να μην διαχωρίζονται εύκολα τα πραγματικά δεδομένα από την κίνηση αυτή. Επομένως σε περίπτωση αποστολής δεδομένων δημιουργείται εικονική κίνηση (mimic traffic) η οποία μπορεί να απορριφθεί ή να εξισορροπηθεί οποιαδήποτε χρονική στιγμή καθώς επίσης και κατά την παραλαβή πραγματικών δεδομένων μπορεί να δημιουργηθεί εξερχόμενη εικονική κίνηση. Καμιά διαφοροποίηση δεν μπορεί να γίνει αντιληπτή σχετικά με την ποσότητα των δεδομένων που ανταλλάσσονται [26]. Επομένως καθίσταται αρκετά δύσκολη η ιχνηλάτιση των πακέτων τόσο με ενεργό τρόπο όσο και με παθητικό τρόπο.

- ***TOR***: Το TOR παρέχει προστασία σε ενεργές επιθέσεις traceback λόγω της ισχυρής πολυεπίπεδης κρυπτογράφησης που εφαρμόζει στην μετάδοση των δεδομένων και λόγω των onion routers που λειτουργούν ως αναμεταδότες των δεδομένων και συνδέονται μεταξύ τους διαμέσου TLS με την χρήση ephemeral κλειδιών. Στις παθητικές, όμως, επιθέσεις traceback δεν προσφέρει την ίδια προστασία, στην περίπτωση που κάποιος αντίπαλος δεσμεύσει αρκετούς πόρους του δικτύου θα μπορούσε να αντλήσει πληροφορίες σχετικά με την δρομολόγηση. Από την άλλη πλευρά οι onion router, αναμεταδότες του TOR, είναι διάσπαρτοι σε διάφορες τοποθεσίες ανά τον κόσμο και δεν είναι εφικτό η παρακολούθηση όλων αλλά μόνο ένα τμήμα από αυτούς. Επίσης το TOR σχεδιαστικά δεν προστατεύει τα δύο επικοινωνούντα άκρα με αποτέλεσμα να αποτελεί σημείο ευπάθειας σε παθητικές επιθέσεις traceback.

- ***Java Anon Proxy***: Το Jap προστατεύει από ενεργές επιθέσεις traceback με την χρησιμοποίηση των ενδιάμεσων κόμβων mix στην δρομολόγηση των πακέτων από τον χρήστη στον εξυπηρετητή και με την χρησιμοποίηση πολυεπίπεδης κρυπτογράφησης. Ένας παρατηρητής όμως που παρακολουθεί παθητικά την κίνηση του δικτύου ή ένα τμήμα του μπορεί να ιχνηλατίσει το μονοπάτι προς τον εξυπηρετητή ή προς τον χρήστη αν και η εικονική κίνηση που μεταφέρεται στο δίκτυο προσθέτει κάποιον βαθμό δυσκολίας. Η στατική δρομολόγηση των πακέτων και το γεγονός ότι ο τελευταίος

κόμβος mix στέλνει τα δεδομένα αποκρυπτογραφημένα στον κατάλληλο εξυπηρετητή το καθιστά ευπαθές σε παθητικές επιθέσεις traceback.

- ***Morphmix***: Το Morphmix δεν μπορεί να αποτρέψει τις παθητικές επιθέσεις traceback από κάποιον αντίπαλο που μπορεί να παρακολουθεί ένα μεγάλο υποσύνολο από όλους τους κόμβους π.χ. 20% και να παραβιάσει μερικά ανώνυμα τούνελ. Όμως δεν θεωρεί μία τέτοια επίθεση εφικτή να πραγματοποιηθεί διότι ο αντίπαλος δεν έχει τη δυνατότητα να παρατηρήσει ένα μεγάλο τμήμα του Morphmix το οποίο περιέχει έναν μεγάλο αριθμό από κόμβους διαμοιραζόμενους σε όλο τον κόσμο. Προστατεύει όμως από ενεργές επιθέσεις traceback λόγω της ισχυρής πολυεπίπεδης κρυπτογράφησης των μηνυμάτων εμποδίζοντας κάποιον αντίπαλο να αποκτήσει έλεγχο του δικτύου και να επιτεθεί ενεργά σε αυτό με σκοπό την παραβίαση της ανωνυμίας.

- ***I2P***: Το I2P δεν παρέχει ικανοποιητική προστασία από μια παθητική επίθεση traceback. Εάν κάποιος αντίπαλος δεσμεύσει πολλούς κόμβους του δικτύου τότε έχει τη δυνατότητα να αποκτήσει πληροφορίες δρομολόγησης και να αποκαλύψει τον χρήστη. Από την άλλη πλευρά προστατεύει από ενεργές επιθέσεις traceback με την ισχυρή πολυεπίπεδη κρυπτογράφηση των μηνυμάτων που μεταφέρονται στο τούνελ.

- ***GNUnet***: Το πρωτόκολλο GAP προστατεύει από ενεργές αλλά και παθητικές επιθέσεις traceback. Το δίκτυο GNUnet επιτρέπει την μετάδοση μηνυμάτων μόνο στα μέλη του με αποτέλεσμα να μην προκύπτουν προβλήματα κατά την επικοινωνία των κόμβων με τον τελικό παραλήπτη του μηνύματος εφόσον αποτελεί κόμβος του δικτύου GNUnet. Επίσης η τεχνική κάλυψης της κίνησης του δικτύου αποτελεί ισχυρός μηχανισμός στις επιθέσεις αυτές.

- ***P5***: Το P5 αν και παρέχει μηχανισμό προστασίας με την πρόσθεση θορύβου στο σύστημα, ανά τακτά χρονικά διαστήματα, δεν αποτρέπει κάποιον αντίπαλο που ενεργεί παθητική επίθεση traceback να αντλήσει κάποιες πληροφορίες. Αποτρέπει όμως από ενεργές επιθέσεις traceback λόγω της κρυπτογράφησης της ζεύξης από άλμα σε άλμα και της κρυπτογράφησης των πακέτων που μεταφέρονται στο δίκτυο.

- ***Herbivore***: Το Herbivore προστατεύει τους χρήστες του από επιθέσεις traceback είτε παθητικές είτε ενεργές. Αν και κάποιος αντίπαλος μπορεί να παρακολουθήσει την κίνηση του δικτύου παθητικά είτε να συμμετάσχει ενεργά στο πρωτόκολλο αλλά θα είναι

δύσκολο να συμπεράνει την προέλευση ή τον προορισμό του μηνύματος εντός του ανώνυμου clique.

- ***Mantis***: Το Mantis δεν προστατεύεται ικανοποιητικά από την παθητική επίθεση Traceback. Οι αντίπαλοι μπορεί να παρακολουθήσουν ένα μεγάλο τμήμα του δικτύου και να συμπεράνουν, σχετικά με την συμπεριφορά των κόμβων, τον εκκινητή ενός αιτήματος ή τον παραλήπτη. Λόγω όμως της κρυπτογράφησης του κάθε αναμεταδιδόμενου μηνύματος με το αντίστοιχο συμφωνημένο διαμοιραζόμενο μυστικό κλειδί του κάθε κόμβου το οποίο είναι ξεχωριστό για κάθε γείτονα με τον οποίον είναι συνδεδεμένος, δεν μπορεί να συμμετέχει ενεργά στο δίκτυο εάν δεν γνωρίζει το μυστικό κλειδί για την αποκρυπτογράφηση ή κρυπτογράφηση των μηνυμάτων που θα διέρχονται από αυτόν.

- ***Mute***: Το δίκτυο Mute δεν προστατεύει τους χρήστες από επιθέσεις traceback είτε είναι παθητικές είτε ενεργές. Ένας αντίπαλος έχει την δυνατότητα να παρακολουθήσει παθητικά την κίνηση του δικτύου και να εκμαιεύσει πληροφορίες σχετικά με ένα τμήμα των συμμετεχόντων κόμβων και επίσης έχει την δυνατότητα να επέμβει ενεργά σε αυτό.

- ***BitBlender***: Το BitBlender δεν προστατεύει τους χρήστες από την παθητική και ενεργή επίθεση traceback. Τα περιεχόμενα που διαμοιράζονται οι χρήστες δεν είναι κρυπτογραφημένα και δεν παρέχεται μηχανισμός ελέγχου πρόσβασης σε αυτά. Επομένως κάποιος αντίπαλος μπορεί να εκτελέσει είτε ενεργή είτε παθητική επίθεση traceback και να αντλήσει πληροφορίες σχετικά με την δραστηριότητα των χρηστών αλλά και να ανακαλύψει τον εκκινητή κάποιου αιτήματος.

- ***Truste***: Δεν προσφέρει καμία υπηρεσία προστασίας έναντι των επιθέσεων αυτών. Στοχεύει στην εξασφάλιση πολιτικών προστασίας προσωπικών δεδομένων από τους διάφορους ιστοτόπους με αποτέλεσμα να μην εστιάζεται σε μηχανισμούς προστασίας έναντι αυτών των επιθέσεων.

- ***P3P***: Το P3P δεν προσφέρει καμία προστασία έναντι κακόβουλων επιθέσεων traceback εφόσον κύριος στόχος του αποτελεί η ενημέρωση του χρήστη με αυτοποιημένο τρόπο σχετικά με τις πρακτικές που εφαρμόζει ο ιστότοπος που επισκέπτεται για την προστασία της ιδιωτικότητας και η ενημερωμένη συγκατάθεση και συμφωνία του σχετικά με τις προτιμήσεις προστασίας της ιδιωτικότητάς του.

4.6 Επίθεση Σήμανσης

- ***LPWA***: Η επικοινωνία ανάμεσα στον φυλλομετρητή και στον LPWA πληρεξούσιο είναι μία δημόσια σύνδεση και δεν κρυπτογραφούνται τα δεδομένα που στέλνονται με αποτέλεσμα να αποτελεί ανοιχτό σημείο ευπάθειας σε αυτή την επίθεση.

- ***Anonymizer***: Τα μηνύματα που μεταφέρονται από τον φυλλομετρητή του χρήστη προς τον εξυπηρετητή αλλά και αντίστροφα δεν κρυπτογραφούνται. Προκειμένου να τροποποιηθεί ένα μήνυμα θα πρέπει ο αντίπαλος να επέμβει στην επικοινωνία του χρήστη με τον πληρεξούσιο του Anonymizer. Η παρεμβολή ενός τρίτου ενδιάμεσου καθίσταται δύσκολη στο σύστημα αυτό με αποτέλεσμα να ανταποκρίνεται αποτελεσματικά στην περίπτωση μίας τέτοιας επίθεσης.

- ***Mixminion***: Το mixnminion προστατεύει από αυτή την επίθεση. Σε περίπτωση που το ωφέλιμο φορτίο τροποποιηθεί από τον αντίπαλο το mixminion με την διαδικασία αναστροφής "swap" και με την κρυπτογράφηση SPRP είναι σε θέση να την εντοπίσει. Επίσης τα mixes ανιχνεύουν τροποποιημένες κεφαλίδες άμεσα χρησιμοποιώντας τον έλεγχο αθροίσματος.

- ***Crowds***: Η επικοινωνία μεταξύ των jondos πραγματοποιείται διαμέσου συμμετρικής κρυπτογράφησης αλλά η ακεραιότητα του μηνύματος δεν επιβεβαιώνεται με αποτέλεσμα να μην αποτρέπεται ο αντίπαλος στην προσπάθεια τροποποίησης κάποιου τμήματος του μηνύματος.

- ***AP3***: Το AP3 δίνει την δυνατότητα στον χρήστη να αποκρύψει την πραγματική ταυτότητά του και να αυθεντικοποιήσει τα μηνύματα του χρησιμοποιώντας ψευδώνυμα. Ο κόμβος που θέλει να στείλει μήνυμα με ασφάλεια σε ένα ψευδώνυμο, κρυπτογραφεί το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του ψευδωνύμου και στέλνει το μήνυμα στο ανώνυμο κανάλι. Αυτό εξασφαλίζει ότι μόνο ο χρήστης που του ανήκει το ψευδώνυμο μπορεί να διαβάσει το μήνυμα και αποτρέπει άλλους κόμβους να το διαβάσουν και να το τροποποιήσουν.

- ***Tarzan***: Το Tarzan αντιμετωπίζει αυτή την επίθεση με τον μηχανισμό ελέγχου ακεραιότητας προστατεύοντας τα μεταδιδόμενα πακέτα από την επίθεση της

επισήμανσης από κάποιον αντίπαλο που στοχεύει στην αναγνωρισιμότητα τους κατά την έξοδό τους από το δίκτυο του Tarzan [26].

- ***TOR***: Στο δίκτυο του TOR οι onion routers επικοινωνούν μεταξύ τους και με τους onion proxies διαμέσου συνέσεων TLS με την χρήση ephemeral κλειδιών. Με την χρησιμοποίηση των TLS συνδέσεων τα δεδομένα καλύπτονται κατά την μεταφορά τους στο δίκτυο αποτρέποντας κάποιον αντίπαλο να τροποποιήσει τα δεδομένα στο κανάλι επικοινωνίας. Επομένως ένας αντίπαλος εκτός δικτύου είναι δύσκολο να επέμβει και να τροποποιήσει τα δεδομένα που μεταφέρονται σε αυτό. Εάν όμως ο αντίπαλος είναι εντός του δικτύου τότε η αντιμετώπιση της επίθεσης αυτής είναι πιο πολύπλοκη. Ως γνωστό το TOR σχεδιαστικά δεν προστατεύει από επιθέσεις στα άκρα του και είναι ευπαθές στην από άκρη-σε-άκρη επίθεση χρονισμού με αποτέλεσμα η τροποποίηση των κελιών που μεταφέρονται στο κύκλωμα του δικτύου να μην προσφέρει επιπρόσθετη πληροφορία στον αντίπαλο. Γι αυτό το λόγο ελέγχεται η ακεραιότητα στα άκρα του κάθε stream, δηλαδή της κάθε TCP σύνδεσης. Σημειώνεται ότι στην τοπολογία κυκλώματος leaky-pipe που χρησιμοποιείται στο TOR το άκρο του stream μπορεί να είναι οποιαδήποτε άλμα στο κύκλωμα. (stream: είναι οποιαδήποτε TCP σύνδεση, και leaky-pipe κύκλωμα: ο OP μπορεί να στείλει μήνυμα σε οποιαδήποτε OR του κυκλώματος και μπορεί να δημιουργήσει stream π.χ. TCP συνδέσεις, διαμέσου οποιουδήποτε OR).

- ***Java Anon Proxy***: Το Jap προστατεύει από αυτή την επίθεση με την μεταφορά των πακέτων διαμέσου καθορισμένων ακολουθιών από mixes που παρέχονται κυρίως από έμπιστους οργανισμούς. Στην περίπτωση που κάποιος κακόβουλος κόμβος τροποποιήσει κάποιο τμήμα του πακέτου ενδέχεται και να μην γίνει αντιληπτό από τους ενδιάμεσους κόμβους αν και χρησιμοποιείται ισχυρή κρυπτογράφηση των πακέτων.

- ***Morphmix***: Ο αντίπαλος μπορεί να τροποποιήσει ελαφρώς ένα κελί ώστε να το αναγνωρίσει κατά την μετάδοσή του, πιο μετά, από κάποιον άλλο κόμβο mix. Η δομή όμως του Morphmix κελιού που ανταλλάσσεται μεταξύ δύο γειτόνων κόμβων παρέχει την δυνατότητα ελέγχου της ακεραιότητας του κελιού με το πεδίο checksum. Επομένως το Morphmix παρέχει μηχανισμό αποτροπής της επίθεσης αυτής σε ικανοποιητικό βαθμό.

- ***I2P***: Το I2P καθιστά αδύνατη μία τέτοια επίθεση εφόσον κάθε μήνυμα που διέρχεται από το τούνελ είναι υπογεγραμμένο και κρυπτογραφημένο σε πολλαπλά στρώματα. Ένας

εξωτερικός παρατηρητής δεν μπορεί να παρακολουθήσει ή ακόμα να εντοπίσει το μήνυμα που έχει τροποποιήσει λόγω της κρυπτογράφησης του συνδέσμου και της υπογραφής που φέρει το μήνυμα.

- ***GNUnet***: Το GAP προστατεύει τον εκδότη του περιεχομένου σε ικανοποιητικό βαθμό. Ακόμα και αν κάποιο ερώτημα που έχει επισημανθεί από τον αντίπαλο αποκαλύψει τον παραλήπτη, η ταυτότητα του εκδότη δεν μπορεί να αποκαλυφτεί εφόσον το GAP χρησιμοποιεί μετανάστευση του περιεχομένου, content migration.

- ***P5***: Τα πακέτα που μεταδίδονται στο δίκτυο αποτελούνται από μικρά κρυπτογραφημένα τμήματα με το δημόσιο κλειδί του παραλήπτη. Αυτή η κρυπτογράφηση σε συνδυασμό με το πεδίο checksum με το οποίο ο παραλήπτης ελέγχει την ορθότητα αποστολής τους μηνύματος δυσκολεύουν την επίθεση αυτή.

- ***Herbivore***: Το πρωτόκολλο Herbivore παρέχει μηχανισμό προστασίας στην επίθεση αυτή. Πιο συγκεκριμένα στην φάση μετάδοσης του πρωτοκόλλου round η ακεραιότητα των δεδομένων που μεταδίδονται προστατεύονται από το MD5 checksum που επισυνάπτεται σε κάθε πακέτο.

- ***Mantis***: Το Mantis δεν παρέχει μηχανισμό αντιμετώπισης αυτής της επίθεσης. Ένας κακόβουλος κόμβος έχει τη δυνατότητα να παραποιήσει το περιεχόμενο ενός μηνύματος χωρίς να γίνει αντιληπτό εφόσον δεν υπάρχει κάποιος μηχανισμός ελέγχου ακεραιότητας των μηνυμάτων που αναμεταδίδονται από κόμβο σε κόμβο.

- ***Mute***: Στο δίκτυο Mute το περιεχόμενο των μηνυμάτων μπορεί να προσπελαστεί και να διαβαστεί από όλους τους κόμβους. Αυτό το καθιστά ευπαθές στην επίθεση αυτή.

- ***BitBlender***: Στο BitBlender τα περιεχόμενα είναι διαθέσιμα σε όλους τους κόμβους και δεν χρησιμοποιείται κρυπτογράφηση στα δεδομένα που διαμοιράζονται οι χρήστες με αποτέλεσμα να μην τίθεται ως πρόβλημα η μη ύπαρξη μηχανισμού σχετικά με την επίθεση αυτή.

- ***Truste***: Δεν προσφέρει καμία υπηρεσία προστασίας έναντι της επίθεσης αυτής. Στοχεύει στην εξασφάλιση πολιτικών προστασίας προσωπικών δεδομένων από τους διάφορους

ιστοτόπους με αποτέλεσμα να μην εστιάζεται σε μηχανισμούς προστασίας έναντι αυτής της επίθεσης.

- ***P3P***: Το P3P δεν προσφέρει καμία προστασία έναντι κακόβουλων επιθέσεων εφόσον κύριος στόχος του αποτελεί η ενημέρωση των χρήστη με αυτοποιημένο τρόπο σχετικά με τις πρακτικές που εφαρμόζει ο ιστότοπος που επισκέπτεται για την προστασία της ιδιωτικότητας και η ενημερωμένη συγκατάθεση και συμφωνία του σχετικά με τις προτιμήσεις προστασίας της ιδιωτικότητάς του.

4.7 Επίθεση Διασταύρωσης

- ***LPWA***: Το LPWA είναι ευπαθές σε αυτή την επίθεση λόγω του ότι τα μηνύματα δεν είναι κρυπτογραφημένα και κάποιος αντίπαλος μπορεί να παρακολουθεί την κίνηση ανάμεσα στον χρήστη και στον πληρεξούσιο και να αντλήσει πληροφορίες. Λόγω του ότι η παρακολούθηση ανάμεσα στον πληρεξούσιο και στον εξυπηρετητή είναι δύσκολο να επιτευχθεί προσδίδει στην επίθεση αυτή κάποιον βαθμό δυσκολίας αλλά δεν την αποτρέπει.

- ***Anonymizer***: Ο Anonymizer χρησιμοποιεί υψηλού βαθμού κρυπτογράφηση για να δρομολογήσει την διαδικτυακή κυκλοφορία του χρήστη μέσω ενός κρυπτογραφημένου «τούνελ», εικονικού ιδιωτικού δικτύου, στους ασφαλείς διακομιστές του και επίσης η επικοινωνία του χρήστη με τον εξυπηρετητή πραγματοποιείται με ψεύτικη διεύθυνση IP αποκρύπτοντας με αυτόν τον τρόπο την πραγματική του διεύθυνση. Επομένως ο τρόπος λειτουργίας του Anonymizer προσφέρει προστασία από την επίθεση αυτή.

- ***Mixminion***: Η χρησιμοποίηση της στρατηγικής δεσμών "dynamic pool" αυξάνει το σύνολο των πιθανών αποστολέων για ένα δεδομένο παραλήπτη αυξάνοντας ταυτόχρονα το κόστος μιας επίθεσης διασταύρωσης. Ωστόσο, μια ολοκληρωμένη λύση παραμένει ένα ανοικτό πρόβλημα [20].

- ***Crowds***: Το Crowds είναι ευπαθές στην επίθεση αυτή. Η δημιουργία τυχαίων μονοπατιών δρομολόγησης, αλλά στατικών, καθώς και η συμμετρική κρυπτογράφηση της επικοινωνίας μεταξύ των jondos προσθέτει κάποιον βαθμό δυσκολίας σε μία τέτοια επίθεση αλλά δεν την αποτρέπει.

- ***AP3***: Το AP3 είναι ιδιαίτερα ευπαθές σε παθητικές επιθέσεις με αποτέλεσμα να μην προστατεύεται ικανοποιητικά από την επίθεση διασταύρωσης. Αν και τα μονοπάτια δημιουργούνται με τυχαία επιλογή και κάποιος κόμβος δεν μπορεί να γνωρίζει αν ο προηγούμενος κόμβος είναι αποστολέας ή κόμβος προώθησης, η στατικότητά τους για ένα χρονικό διάστημα καθιστά το σύστημα ιδιαίτερο ευάλωτο στην επίθεση αυτή.

- ***Tarzan***: Το πρωτόκολλο αναδημιουργίας των τούνελ στο Tarzan προσφέρει κάποια προστασία στην επίθεση αυτή. Οι ενδιάμεση κόμβοι επανεμφανίζονται στα ανακατασκευασμένα τούνελ με αποτέλεσμα ο αντίπαλος να μην μπορεί να ξεχωρίσει τα ανακατασκευασμένα τούνελ από τα καινούργια τούνελ δρομολόγησης και να έχει λιγότερη εμπιστοσύνη στα συμπεράσματά του. Επίσης η αναδημιουργία των τούνελ κατά την οποία ο εκκινητής μπορεί να επαναχρησιμοποιεί, συνεχόμενα, τον πρώτο κόμβο για να τον εμπλέκει στις επιθέσεις διασταύρωσης παρέχει προστασία στην επίθεση αυτή [26]. Σε περίπτωση αποτυχίας επανασχηματίζονται ιδιωτικοί σύνδεσμοι και όχι ολόκληρα τα μονοπάτια προστατεύοντας σε ικανοποιητικό βαθμό από επιθέσεις διασταύρωσης.

- ***TOR***: Το TOR δεν προσφέρει αποτελεσματική προστασία από την επίθεση αυτή. Τα άκρα του δικτύου του TOR είναι εκτεθειμένα σε παθητικούς αντιπάλους που παρακολουθούν την κίνηση και επίσης στην περίπτωση που ο επιτιθέμενος δεσμεύσει αρκετούς πόρους του δικτύου είναι σε θέση να αντλήσει πληροφορίες δρομολόγησης και συμπεριφοράς των κόμβων του δικτύου.

- ***Java Anon Proxy***: Η εικονική κίνηση που αποστέλλεται από τους ενδιάμεσους κόμβους προσθέτει κάποιο εμπόδιο δυσκολίας στην επίθεση αυτή αλλά δεν την αντιμετωπίζει αποτελεσματικά. Δεν είναι σαφές πώς το Jap μπορεί να αντιμετωπίσει μία τέτοια επίθεση κυρίως αν ληφθεί υπόψη ένας παγκόσμιος παρατηρητής [05].

- ***Morphmix***: Το δυναμικό και ετερογενές περιβάλλον του Morphmix και οι διαφορετικοί κόμβοι που εμφανίζονται σε διαφορετικές χρονικές στιγμές δίνουν την δυνατότητα σε μια τέτοια επίθεση τον εντοπισμό του αποστολέα. Στην περίπτωση όπου ένα μικρό σύνολο από αποστολείς επικοινωνούν με έναν συγκεκριμένο παραλήπτη ή εξυπηρετητή η επίθεση αυτή καθίσταται πρακτικής σημασίας εφόσον μπορεί να παραβιάσει την ανωνυμία.

- ***I2P***: Το I2P δεν έχει πλήρη μηχανισμό προστασίας έναντι της επίθεσης αυτής. Αποτελεί, λοιπόν, σημείο ευπάθειας του συστήματος και όσο το δίκτυο επεκτείνεται τόσο αυξάνεται η ευπάθειά του στην επίθεση αυτή. Επίσης στο σενάριο όπου ο αντίπαλος βρίσκεται και στα δύο άκρα του τούνελ και ενεργεί επίθεση διασταύρωσης η πιθανότητα παραβίασης της ανωνυμίας του χρήστη.

- ***GNUnet***: Κάποιος αντίπαλος μπορεί να παρακολουθήσει για μεγάλο χρονικό διάστημα το δίκτυο και να καταλήξει σε σημαντικά συμπεράσματα σχετικά με την συμπεριφορά των κόμβων αν και είναι δύσκολο να διακρίνει τα ερωτήματα από τις απαντήσεις που διαδίδονται στο δίκτυο. Παρόλα αυτά είναι δύσκολο να επέμβει ενεργά σε αυτό.

- ***P5***: Μία τέτοια επίθεση δύσκολα αντιμετωπίζεται από το πρωτόκολλο P5. Ο χρήστης κατά την συμμετοχή του στο σύστημα εάν αλλάξει το σύνολο των καναλιών μετάδοσης στα οποία συμμετέχει, διευκολύνει την επίθεση αυτή ενώ αν μείνει σταθερός στο σύνολο των ομάδων που έχει ενταχθεί με την έναρξη της συμμετοχής του στο σύστημα προστατεύεται από την επίθεση αυτή. Επίσης όταν ο χρήστης συμμετέχει σε δύο σύνολα ομάδων έστω U και V τότε η πιθανότητα μιας τέτοιας επίθεσης να παραβιάσει την ανωνυμία είναι η τομή των δύο συνόλων $U \cap V$.

- ***Herbivore***: Αν και μία τέτοια επίθεση είναι δύσκολο να αντιμετωπιστεί το Herbivore παρέχει μηχανισμό προστασίας σε αυτή την επίθεση. Ένας αντίπαλος εάν εντοπίσει κάποια συναλλαγή που εκτελείται για μεγάλο χρονικό διάστημα ενδέχεται να υπονομεύσει την ανωνυμία του κόμβου με την επίθεση αυτή. Το Herbivore προστατεύει από την επίθεση αυτή με την exit φάση του πρωτοκόλλου round, στο οποίο καθορίζεται η συμπεριφορά των κόμβων στο clique. Η φάση αυτή αποτελείται από μια ψηφοφορία "vote" για να ελέγξει εάν είναι η κατάλληλη στιγμή για αλλαγές στους συμμετέχοντες κόμβους στο clique. Ο κόμβος μπορεί να χρησιμοποιήσει την φάση αυτή για να στείλει ανώνυμα σήμα σους άλλους κόμβους ώστε να τους ενημερώσει ότι είναι στη μέση μιας μεγάλης συναλλαγής και να καθυστερήσουν την αποχώρησή τους από το clique χωρίς όμως να τους δεσμεύει. Συμπερασματικά αναμένουμε οι συμμετέχοντες κόμβοι να παραμένουν στο clique κατά τη διάρκεια μεγάλων συναλλαγών προστατεύοντας την ανωνυμία των μερών της συναλλαγής. Επίσης ο κάθε κόμβος που εκτελεί μία συναλλαγή μεγάλης διάρκειας ελέγχει τον εαυτό του σε μια τέτοια επίθεση και αν πέσει κάτω από μία συγκεκριμένη τιμή κατωφλίου σταματάει την εκτέλεση της συναλλαγής αυτής προκειμένου να προστατεύσει την ανωνυμία του.

- ***Mantis***: Στο Mantis ένας αντίπαλος που παρακολουθεί παθητικά ένα τμήμα του δικτύου μπορεί να παρατηρεί την κίνηση των κόμβων και να συμπεράνει τον αποστολέα ή τον εξυπηρετητή και να εκμαιεύσει πληροφορίες σχετικά με την συμπεριφορά των κόμβων στο δίκτυο αλλά δεν μπορεί να γνωρίζει το περιεχόμενο των μηνυμάτων που αναμεταδίδονται εφόσον κρυπτογραφούνται από άλμα σε άλμα.

- ***Mute***: Στο δίκτυο Mute κάποιος αντίπαλος μπορεί να παρακολουθήσει την κίνηση του δικτύου με παθητικό τρόπο και παρόλο που τα μηνύματα που διαδίδονται είναι κρυπτογραφημένα μπορεί να συμπεράνει κάποια στοιχεία για τη συμπεριφορά των κόμβων και να τον οδηγήσει στον αποστολέα ή στον παραλήπτη κόμβο.

- ***BitBlender***: Στο BitBlender ένας αντίπαλος που παρακολουθεί την κίνηση σε κάποιους κόμβους του δικτύου μπορεί να αντλήσει πληροφορίες σχετικά με την συμπεριφορά των κόμβων καθώς και να παραβιάσει την ανωνυμία κάποιων χρηστών. Για να περιοριστεί η επίθεση αυτή προτείνεται η τεχνική της κίνησης κάλυψης "cover traffic" με την έκδοση των ίδιων αιτημάτων πολλές φορές με μη καθοριστικό "non deterministic" τρόπο ώστε να είναι δυσδιάκριτα από τα relay peers.

- ***Truste***: Δεν προσφέρει καμία υπηρεσία προστασίας έναντι της επίθεσης αυτής. Στοχεύει στην εξασφάλιση πολιτικών προστασίας προσωπικών δεδομένων από τους διάφορους ιστοτόπους με αποτέλεσμα να μην εστιάζεται σε μηχανισμούς προστασίας έναντι αυτής της επίθεσης.

- ***P3P***: Το P3P δεν προσφέρει καμία προστασία έναντι κακόβουλων επιθέσεων εφόσον κύριος στόχος του αποτελεί η ενημέρωση των χρήστη με αυτοποιημένο τρόπο σχετικά με τις πρακτικές που εφαρμόζει ο ιστότοπος που επισκέπτεται για την προστασία της ιδιωτικότητας και η ενημερωμένη συγκατάθεση και συμφωνία του σχετικά με τις προτιμήσεις προστασίας της ιδιωτικότητάς του.

4.8 Κακόβουλοι Κόμβοι

- ***LPWA***: Η λειτουργία στηρίζεται σε έναν πληρεξούσιο και στην περίπτωση μίας τέτοιας επίθεσης είναι ο μοναδικός που μπορεί να δράσει ως κακόβουλος κόμβος και συνεργός.

- ***Anonymizer***: Ο μοναδικός ενδιάμεσος στην επικοινωνία του χρήστη με τον εξυπηρετητή είναι ο πληρεξούσιος του Anonymizer με αποτέλεσμα να αποτελεί και τον μοναδικό κακόβουλο κόμβο εάν εντοπιστεί παραβατική ενέργεια.

- ***Mixminion***: Μηνύματα διασχίζουν πολλούς κόμβους mix και ο κάθε κόμβος γνωρίζει μόνο τους γειτονικούς του κόμβους και όχι ολόκληρο το μονοπάτι επομένως η διακύβευση ενός μόνο mix, ακόμη και ενός σημείου διασταύρωσης, δεν δύναται να αποκαλύψει επαρκής πληροφορίες σε κάποιον αντίπαλο.

- ***Crowds***: Οι χρήστες έχουν την δυνατότητα να επιλέξουν τα Jondos με αποτέλεσμα να ελαχιστοποιείται η πιθανότητα ύπαρξης κακόβουλων κόμβων στην διαδρομή. Το μονοπάτι δρομολόγησης δημιουργείται με τυχαίο τρόπο και παραμένει στατικό ώστε τα μέλη να γνωρίζουν τον προκάτοχό και τον διάδοχό τους χωρίς όμως να αποκλείεται η ύπαρξη κακόβουλου κόμβου ή συνεργού στην διαδρομή. Τα Crowds λοιπόν προστατεύει από κακόβουλους κόμβους χωρίς όμως να αποκλείει με αποτελεσματικό τρόπο την ύπαρξή τους στα μονοπάτια δρομολόγησης.

- ***AP3***: Δεν παρέχει κάποιον μηχανισμό προστασίας από κακόβουλους κόμβους, το AP3 χτίστηκε πάνω σε αναξιόπιστους κόμβους. Ένα μονοπάτι ενδέχεται να περιέχει και κακόβουλους κόμβους χωρίς να είναι δυνατός ο εντοπισμός τους από το σύστημα.

- ***Tarzan***: Η ομογένεια των αναμεταδοτών ενός μοντέλου ομότιμου δικτύου προλαμβάνει τον αντίπαλο από το να συμπεράνει την ταυτότητα του αποστολέα. Κάθε κόμβος στο τούνελ του Tarzan γνωρίζει τον προηγούμενο κόμβο και τον επόμενο κόμβο. Επομένως εάν ο κακόβουλος κόμβος βρίσκεται στην αρχή ή στο ενδιάμεσο του τούνελ υπάρχει πιθανότητα να συμπεράνει τη δραστηριότητα του αποστολέα αλλά δεν μπορεί να συμπεράνει την δραστηριότητα του παραλήπτη καθώς και το περιεχόμενο του αποστολέα και του παραλήπτη. Εάν ο κακόβουλος κόμβος βρίσκεται στο τέλος του τούνελ τότε υπάρχει πιθανότητα να συμπεράνει την δραστηριότητα του παραλήπτη και το περιεχόμενο του αλλά δεν μπορεί να συμπεράνει την δραστηριότητα του αποστολέα και το περιεχόμενο του. Εάν οι κακόβουλοι κόμβοι βρίσκονται στην αρχή και στο τέλος του τούνελ τότε υπάρχει πιθανότητα να συμπεράνουν την δραστηριότητα του αποστολέα και το περιεχόμενο του και έχουν την δυνατότητα να συμπεράνουν την δραστηριότητα του παραλήπτη και το περιεχόμενο του [26].

- ***TOR***: Το δίκτυο του TOR δεν μπορεί να αποκλείσει την ύπαρξη κακόβουλων κόμβων στο δίκτυο αλλά και στην περίπτωση που υπάρχουν κακόβουλοι κόμβοι και ενεργούν ως αναμεταδότες στο σύστημα δεν μπορούν να αποκαλύψουν τα δύο άκρα της επικοινωνίας λόγω του ότι γνωρίζουν μόνο τον αναμεταδότη από τον οποίο λαμβάνουν τα δεδομένα και τον αναμεταδότη στον οποίο αποστέλλουν τα δεδομένα.

- ***Java Anon Proxy***: Η επικοινωνία του χρήστη με τον εξυπηρετητή πραγματοποιείται διαμέσου διαφορετικών αλλά καθορισμένων ακολουθιών από κόμβους mixes. Οι ενδιάμεσοι κόμβοι mix παρέχονται κυρίως από επίσημους οργανισμούς που δηλώνουν επισήμως ότι δεν κρατούν αρχεία log από τις συνδέσεις τους καθώς και δεν ανταλλάσουν δεδομένα αρχείων log με άλλους κόμβους mix [32] αποτελώντας έτσι ένα μέσο προστασίας του συστήματος jap από την ύπαρξη κακόβουλων κόμβων.

- ***Morphmix***: Το Morphmix παρέχει τον μηχανισμό εντοπισμού σύγκρουσης "collusion detection" για την ανίχνευση κακόβουλων κόμβων στο δίκτυο και πιο συγκεκριμένα στα τούνελ επικοινωνίας του χρήστη με τον εξυπηρετητή. Για όσο χρονικό διάστημα οι κακόβουλοι συνεργοί παραμένουν λίγοι σε αριθμό ο μηχανισμός λειτουργεί σωστά στηριζόμενος στο ότι ο αντίπαλος δεν μπορεί ελέγξει σημαντικά πολλά τούνελ εκτός και αν ενεργήσει δίκαια. Εάν όμως ο αντίπαλος ελέγξει πάνω από το 1/3 όλων των κόμβων ο μηχανισμός εντοπισμού σύγκρουσης αρχίζει να αποτυγχάνει [44]. Συμπερασματικά το Morphmix παρέχει μηχανισμό ανίχνευσης των κακόβουλων συνεργών σε ένα τούνελ με αποτέλεσμα να απορρίπτεται το τούνελ αυτό, εάν ανιχνευθεί η συμμετοχή κακόβουλων κόμβων σε αυτό.

- ***I2P***: Το I2P παρέχει μηχανισμό προστασίας από κακόβουλους κόμβους δημιουργώντας το profile του κάθε συμμετέχοντα κόμβου. Χρειάζεται όμως περαιτέρω έρευνα και ανάπτυξη στην αντιμετώπιση της ύπαρξης των κακόβουλων κόμβων για την προστασία του δικτύου σε ικανοποιητικό βαθμό.

- ***GNUnet***: Το GAP προστατεύει σε ικανοποιητικό βαθμό από τους κακόβουλους κόμβους. Ένας κακόβουλος κόμβος μπορεί να παρακολουθήσει την κίνηση μεταξύ των κόμβων αλλά δεν μπορεί να αναλύσει την κρυπτογραφημένη κίνηση μεταξύ αυτών εφόσον δεν γνωρίζει τα μυστικά κλειδιά τους [01].

- ***P5***: Στο σύστημα ενδέχεται να ενταχθούν κακόβουλοι κόμβοι αν και η μέθοδος ένταξης των κόμβων στο λογικό δέντρο και η κρυπτογράφηση ζεύξης προσθέτουν κάποιο βαθμό δυσκολίας αλλά δεν αποτρέπουν την ύπαρξή τους.

- ***Herbivore***: Το Herbivore με το πρωτόκολλο ελέγχου ασφαλούς εισόδου στο δίκτυο προστατεύει σε ικανοποιητικό βαθμό από κακόβουλους κόμβους. Επίσης ο ασφαλής τυχαίος μηχανισμός εισόδου καθιστά σχεδόν αδύνατο από έναν αντίπαλο που συνεργάζεται με έναν αριθμό κακόβουλων κόμβων να αποκτήσει τον έλεγχο του clique. Για παράδειγμα ένας αντίπαλος που ελέγχει το 90% των κόμβων που συμμετέχουν στο Herbivore έχει μόνον $0,9^{127} \approx 1,5*10^{-6}$ πιθανότητα να αποκτήσει τον έλεγχο ενός clique με μέγεθος 128 κόμβων.

- ***Mantis***: Ανοιχτό σημείο πρόσβασης των κακόβουλων κόμβων στο δίκτυο αποτελεί η εγγραφή των κόμβων σε μία κεντρική οντότητα, στον Blender, η οποία είναι μεν προαιρετική αλλά αναγκαία για την αναζήτηση άλλων κόμβων σε αυτό. Από τη στιγμή που δεν παρέχεται κάποιος μηχανισμός ελέγχου των κόμβων που εγγράφονται παραμένει ανοιχτό σημείο πρόσβασης των αντιπάλων στο δίκτυο. Το Mantis αντιμετωπίζει το πρόβλημά αυτό με την χρησιμοποίηση διάφορων οντοτήτων ως Blender και όχι μόνο μία οντότητα.

- ***Mute***: Το δίκτυο Mute δεν αποκλείει την ύπαρξη κακόβουλων κόμβων οι οποίοι μπορεί ακόμα και να συνεργάζονται με κόμβους του δικτύου και να παρουσιάζονται ως έντιμοι κόμβοι.

- ***BitBlender***: Το BitBlender δεν παρέχει μηχανισμούς που αποτρέπουν κάποιον κακόβουλο κόμβο να συμμετάσχει στο δίκτυο. Επίσης εφόσον το περιεχόμενο που διαμοιράζονται οι χρήστες στο BitBlender είναι δημοσίως διαθέσιμο δεν είναι αυστηρή απαίτηση της λειτουργίας του η παροχή εμπιστευτικότητας περιεχομένου και ελέγχου πρόσβασης σε αυτό από τους κόμβους. Επομένως οι κακόβουλοι κόμβοι εφόσον συμμετέχουν στο δίκτυο μπορεί να έχουν πρόσβαση στο περιεχόμενο που διαμοιράζεται σε αυτό.

- ***Truste***: Η αρχιτεκτονική του στηρίζεται στη χρήση ενός μοναδικού πληρεξούσιου και είναι ο μόνος που μπορεί να ενεργήσει ως κακόβουλος συνεργός επομένως εάν υπάρξει μία τέτοια επίθεση μπορούν να ληφθούν νομικά μέτρα εναντίον του.

- ***P3P***: Το P3P δεν προσφέρει καμία προστασία έναντι κακόβουλων επιθέσεων εφόσον κύριος στόχος του αποτελεί η ενημέρωση των χρήστη με αυτοματοποιημένο τρόπο σχετικά με τις πρακτικές που εφαρμόζει ο ιστότοπος που επισκέπτεται για την προστασία της ιδιωτικότητας και η ενημερωμένη συγκατάθεση και συμφωνία του σχετικά με τις προτιμήσεις προστασίας της ιδιωτικότητάς του.

4.9 Επίθεση Τύπου Ενδιαμέσου

- ***LPWA***: Το LPWA είναι ευπαθές στην επίθεση αυτή διότι η επικοινωνία με τον πληρεξούσιο δε κρυπτογραφείται και αυτό επιτρέπει σε κάποιον αντίπαλο που παρακολουθεί την επικοινωνία να παρεμβληθεί.

- ***Anonymizer***: Δεν μπορεί να παρακολουθήσει αλλά και να παρεμβληθεί κάποιος αντίπαλος ανάμεσα στην επικοινωνία του χρήστη με τον εξυπηρετητή. Η κρυπτογραφημένη κίνηση μεταξύ του χρήστη και του πληρεξούσιο αλλά και η αλλαγή της διεύθυνσης IP του χρήστη σε μη ανιχνεύσιμη εμποδίζει μία τέτοια επίθεση να επιτευχθεί.

- ***Mixminion***: Κάθε μήνυμα παρέχει στον κόμβο mix την ταυτότητα του διάδοχού του στο μονοπάτι και αυτό καθιστά δύσκολο για έναν αντίπαλο να επιδιώξει μία τέτοια επίθεση, να τροποποιήσει το μήνυμα, να ενώσει μηνύματα σαν να είναι μέλος της επικοινωνίας ή ακόμα και να γίνει ενεργό μέλος της επικοινωνίας και να διαγράψει μηνύματα.

- ***Crowds***: Κάθε μονοπάτι που δημιουργείται παραμένει στατικό για όσο χρονικό διάστημα είναι δυνατόν και τα μέλη αναγνωρίζονται μεταξύ τους με αποτέλεσμα τον αποκλεισμό ενδεχομένης παρέμβασης κάποιου κακόβουλου συνεργού ή κόμβου ως μέλος της διαδρομής. Επίσης η επικοινωνία των jondos πραγματοποιείται διαμέσου συμμετρικής κρυπτογράφησης καθιστώντας δύσκολο κάποιων αντίπαλο να επέμβει στον δίαυλο επικοινωνίας τους.

- ***AP3***: Στο AP3 το αναγνωριστικό του καναλιού απάντησης δεν είναι κρυπτογραφημένο και αποστέλλεται σε μορφή απλού κειμένου. Ο κακόβουλος κόμβος μπορεί να δημιουργήσει το δικό του κανάλι και να αντικαταστήσει το αναγνωριστικό του καναλιού

απάντησης στο αρχικό πακέτο με το δικό του. Με αυτόν τον τρόπο ο κόμβος μπορεί να στήσει μια επίθεση Τύπου Ενδιάμεσου.

- ***Tarzan***: Το Tarzan προσφέρει μηχανισμούς προστασίας σε αυτή την επίθεση. Η πολυεπίπεδη κρυπτογράφηση των πακέτων, ο μηχανισμός εικονικής κίνησης (mimic), που είναι δύσκολο να διαχωριστεί από την πραγματική κίνηση των πακέτων και ο έλεγχος ακεραιότητάς τους καθιστά δύσκολη την ενεργό συμμετοχή κάποιου παρατηρητή ως ενδιάμεσου στην επικοινωνία των κόμβων που παρακολουθεί.

- ***TOR***: Το TOR δεν είναι ασφαλές σε αυτή την επίθεση. Σημείο ευπάθειας του δικτύου αποτελούν οι κόμβοι εξόδου οι οποίοι αποστέλλουν τα αιτήματα αποκρυπτογραφημένα προς τον τελικό προορισμό και κάποιος αντίπαλος μπορεί να διαβάσει και να επέμβει στην επικοινωνία. Το TOR παρέχει ανωνυμία με το να προστατεύει τον εκκινητή του αιτήματος αλλά η κίνηση μεταξύ του κόμβου εξόδου και του διαδικτύου είναι εκτεθειμένη στους αντιπάλους εφόσον δεν διαφέρει από την κανονική κίνηση του διαδικτύου.

- ***Java Anon Proxy***: Η επικοινωνία του χρήστη με τον εξυπηρετητή πραγματοποιείται διαμέσου διαφορετικών αλλά καθορισμένων ακολουθιών από κόμβους mixes. Κάποιος αντίπαλος που παρακολουθεί την επικοινωνία και την κίνηση κάποιων κόμβων mixes δεν μπορεί να παρεμβληθεί στην επικοινωνία τους.

- ***Morphmix***: Ένας αντίπαλος έχει την δυνατότητα να παρακολουθήσει την επικοινωνία κάποιων κόμβων και εφόσον δεν χρησιμοποιούνται ψηφιακά πιστοποιητικά δεν υπάρχει κάποια δέσμευση μεταξύ της IP του κόμβου και του δημόσιου κλειδιού της με αποτέλεσμα να καθίσταται δυνατή μία τέτοια απειλή. Αλλά από την άλλη πλευρά η εφαρμογή αυτής της επίθεσης δεν είναι εφικτή διότι ο αντίπαλος χρειάζεται ενεργό έλεγχο σε διάφορους συνδέσμους του δικτύου. Για να επιτευχθεί αυτό πρέπει να παραβιάσει όλους τους συνδέσμους ανάμεσα των κόμβων στο ανώνυμο τούνελ το οποίο είναι δύσκολο έως μη επιτεύξιμο [44].

- ***I2P***: Ένας αντίπαλος μπορεί να παρακολουθήσει τα μηνύματα που μεταδίδονται ανάμεσα σε κάποιους κόμβου του δικτύου αλλά λόγω της κρυπτογράφησης του συνδέσμου καθώς και της ιδιότητας των υπογεγραμμένων μηνυμάτων είναι δύσκολο να επέμβει ως ενδιάμεσος.

- ***GNUnet***: Ένας κακόβουλος κόμβος μπορεί να παρακολουθήσει την κίνηση μεταξύ δύο κόμβων αλλά δεν μπορεί να επέμβει ενεργά λόγο της ισχυρής κρυπτογράφησης ζεύξης που χρησιμοποιείται.

- ***P5***: Εάν κάποιος αντίπαλος παρακολουθεί την επικοινωνία κάποιων κόμβων μεταξύ τους δεν μπορεί να επέμβει ενεργά σε αυτή. Η παραγωγή θορύβου από τους κόμβους αλλά και η κρυπτογράφηση της ζεύξης καθιστούν δύσκολη την ενεργό συμμετοχή του.

- ***Herbivore***: Αν και ένας αντίπαλος μπορεί να παρακολουθήσει παθητικά την επικοινωνία κάποιων κόμβων παρ' όλα αυτά λόγω του ότι συμμετέχουν σε κάποιο clique είναι δύσκολο να αποκτήσει ενεργή συμμετοχή ανάμεσα στην επικοινωνία τους. Τα πρωτόκολλα ελέγχου εισόδου σε ένα clique και ο έλεγχος ακεραιότητας των μηνυμάτων με το επισυναπτόμενο πεδίο MD5 checksum σε κάθε μήνυμα που ανταλλάσσουν καθιστούν δύσκολη μια τέτοια επίθεση.

- ***Mantis***: Στο Mantis ένας αντίπαλος μπορεί παθητικά να παρακολουθήσει την επικοινωνία δύο κόμβων. Ως γνωστό τα μηνύματα που ανταλλάσσονται μεταξύ των γειτόνων – κόμβων είναι κρυπτογραφημένα με το μυστικό διαμοιραζόμενο κλειδί αλλά η ανταλλαγή του κλειδιού έγινε με τρόπο μη αυθεντικοποιημένο "unauthorized", χωρίς να γνωρίζουν οι δύο κόμβοι τις ταυτότητες μεταξύ τους, και αυτό αφήνει ανοιχτή την πρόσβαση ενός αντιπάλου να ξεκινήσει μία επίθεση τύπου ενδιάμεσου και να συμφωνήσει ένα διαφορετικό κλειδί με καθένα από τα μέρη που εμπλέκονται στην ανταλλαγή κλειδιών [40].

- ***Mute***: Το δίκτυο Mute είναι ευπαθές στην επίθεση αυτή. Αν και παρέχει κρυπτογράφηση συνδέσμου για την παροχή ασφάλειας των άμεσων συνδέσεων με τους γείτονες κόμβους παρ' όλα αυτά μπορεί κάποιος αντίπαλος να ξεκινήσει μία επίθεση τύπου ενδιάμεσου και να συμφωνήσει ένα διαφορετικό κλειδί με καθένα από τα μέρη που εμπλέκονται στην ανταλλαγή κλειδιών [40].

- ***BitBlender***: Το BitBlender δεν παρέχει μηχανισμό προστασίας στην αντιμετώπιση αυτής της επίθεσης. Κάποιος αντίπαλος ενδέχεται να παρακολουθεί την κίνηση κάποιων κόμβων και έχει την δυνατότητα να διαβάσει τα περιεχόμενα που μεταφέρονται εφόσον δεν είναι κρυπτογραφημένα και να επέμβει ενεργά στην επικοινωνία τους.

- ***Truste***: Δεν προσφέρει καμία υπηρεσία προστασίας έναντι της επίθεσης αυτής. Στοχεύει στην εξασφάλιση πολιτικών προστασίας προσωπικών δεδομένων από τους διάφορους ιστοτόπους με αποτέλεσμα να μην εστιάζεται σε μηχανισμούς προστασίας έναντι αυτής της επίθεσης.

- ***P3P***: Το P3P δεν προσφέρει καμία προστασία έναντι κακόβουλων επιθέσεων εφόσον κύριος στόχος του αποτελεί η ενημέρωση των χρήστη με αυτοματοποιημένο τρόπο σχετικά με τις πρακτικές που εφαρμόζει ο ιστότοπος που επισκέπτεται για την προστασία της ιδιωτικότητας και η ενημερωμένη συγκατάθεση και συμφωνία του σχετικά με τις προτιμήσεις προστασίας της ιδιωτικότητάς του.

4.10 Καθυστέρηση

- ***LPWA***: Με την εισαγωγή του πληρεξούσιου μεταξύ του προγράμματος περιήγησης και του εξυπηρετητή προσδίδεται καθυστέρηση στην επικοινωνία. Η καθυστέρηση αυτή προέρχεται από τον χρόνο που χρειάζεται ένα HTTP αίτημα να διαβαστεί από τον πληρεξούσιο και στη συνέχεια να αποσταλεί καινούργιο αίτημα στον εξυπηρετητή. Με αυτή την παρέμβαση του πληρεξούσιου ανάμεσα στον χρήστη και στον εξυπηρετητή προσδίδεται καθυστέρηση στο σύστημα.

- ***Anonymizer***: Το Anonymizer εκτελείται στο παρασκήνιο προσδίδοντας κάποια καθυστέρηση αρχικά στην επικοινωνία του χρήστη με τον εξυπηρετητή αλλά όχι σημαντική ώστε να αποθαρρύνει τους χρήστες στην χρησιμοποίηση της υπηρεσίας που παρέχει.

- ***Mixminion***: Το mixminion παρέχει στο σύστημα υψηλό βαθμό καθυστέρησης.

- ***Crowds***: Το Crowds αυξάνει την κίνηση του δικτύου, τον φόρτο εργασίας των συστημάτων που εκτελούν τα jondo και τον χρόνο ανάκτησης και επομένως επιβαρύνεται η απόδοση του συστήματος.

- ***AP3***: Το AP3 παρέχει ένα ευέλικτο, ελαφρύ γενικό μηχανισμό χαμηλής καθυστέρησης δεδομένου ότι οι επεξεργασία που υφίσταται το πακέτο σε κάθε κόμβο του μονοπατιού είναι ελάχιστη.

- ***Tarzan***: Το Tarzan για την αναμετάδοση προσφέρει γρήγορο ρυθμό προώθησης των πακέτων, υψηλή ροή και για την εγκατάσταση των τούνελ καθυστερεί σε λογικά πλαίσια [26]. Η καθυστέρηση διάδοσης του τούνελ κυριαρχείται ολοκληρωτικά από την καθυστέρηση διάδοσης της υποκείμενης διαδικτυακής διαδρομής λόγω του ότι κάθε αναμεταδότης στο τούνελ προσθέτει για τη διαχείριση του πακέτου επιβάρυνση μικρότερη του 1msec. Η καθυστέρηση των τούνελ του Tarzan εξαρτώνται από την ταχύτητα μετάδοσης μέσω του διαδικτύου. Το Tarzan προσθέτει μικρή επιβάρυνση πάνω σε μία μη ανώνυμη διαδρομή επικάλυψης. Συμπερασματικά ή καθυστέρηση που προσθέτει είναι χαμηλή.

- ***TOR***: Το TOR δίκτυο έχει σχεδιαστεί ως ένα ανώνυμο σύστημα χαμηλής καθυστέρησης. Παρόλα αυτά υπάρχουν καθυστερήσεις στην επικοινωνία των χρηστών με τους εξυπηρετητές διότι η κίνηση διακινείται διαμέσου από υπολογιστές εθελοντών που βρίσκονται σε διάφορες τοποθεσίες ανά τον κόσμο με αποτέλεσμα να παρουσιάζονται κάποια σημεία συμφόρησης και καθυστέρησης στο δίκτυο [60].

- ***Java Anon Proxy***: Το Jap προσδίδει καθυστέρηση στην επικοινωνία του χρήστη με τον εξυπηρετητή με αποτέλεσμα η απόδοση να είναι χαμηλή. Αυξάνεται σημαντικά η καθυστέρηση διάδοσης και χάνεται εύρος ζώνης διαμέσου του πρωτοκόλλου.

- ***Morphmix***: Το Morphmix προσθέτει χαμηλή καθυστέρηση στο δίκτυο και παρέχει πρόσβαση στο διαδίκτυο για ένα μεγάλο αριθμό από χρήστες, χαμηλής καθυστέρησης. Αν και το Morphmix αντιμετωπίζει το πρόβλημα του ανομοιογενούς περιβάλλοντος, των κόμβων οι οποίοι δεν έχουν όλοι τις ίδιες δυνατότητες και μπορεί σε κάποια χρονική στιγμή να μην είναι διαθέσιμοι λόγω τεχνικού προβλήματος ή μπορεί προσωρινά να μην είναι προσβάσιμοι λόγω προβλήματος του δικτύου ή να έχουν τερματιστεί από τους λειτουργούς τους η απόδοσή του να είναι αρκετά χαμηλή και οι χρήστες να απορρίπτουν το Morphmix για λόγους απόδοσης και καθυστέρησης. Επίσης η υπολογιστική υπερθέρμανση του δικτύου λόγω της κρυπτογραφικής διαδικασίας είναι σχετικά μικρή και μπορεί να διαχειριστεί από οποιοδήποτε συμμετέχοντα κόμβο [44].

- ***I2P***: Το I2P είναι χαμηλής καθυστέρησης. Υπάρχουν κάποιες τεχνικές για την βελτιστοποίηση της απόδοσής του, οι οποίες σχετίζονται με τον επεξεργαστή, με το εύρος ζώνης και με το πρωτόκολλο που χρησιμοποιείται, επηρεάζοντας την καθυστέρηση του δικτύου και την ροή της κίνησης. Όσο μειώνεται η χρησιμοποίηση των

προαναφερθέντων πόρων αυξάνεται η απόδοση του δικτύου, στοιχείο που γίνεται αντιληπτό από τους χρήστες.

- ***GNUnet***: Το GAP είναι χαμηλό σε καθυστέρηση και προσφέρει στον χρήστη την επιλογή της μείωσης του επιπέδου προστασίας της ανωνυμίας του με την αύξηση της αποδοτικότητας του δικτύου χωρίς να επηρεάζει όμως την απόδοση του πρωτοκόλλου.

- ***P5***: Το πρωτόκολλο παρέχει στον χρήστη την δυνατότητα επιλογής ανάμεσα στο επίπεδο ανωνυμίας που επιθυμεί και στην αποδοτικότητα της επικοινωνίας του. Αυτό έχει ως αποτέλεσμα την αύξηση της απόδοσης του συστήματος για τον χρήστη με κάποιο βαθμό επίπτωσης του επιπέδου προστασίας της ανωνυμίας του. Γενικότερα το πρωτόκολλο είναι σχετικά υψηλής καθυστέρησης και προσθέτει σημαντικό φορτίο στο δίκτυο.

- ***Herbivore***: Το Herbivore επιτυγχάνει υψηλό εύρος ζώνης και χαμηλή καθυστέρηση.

- ***Mantis***: Το Mantis αποτελεί ένα δίκτυο ομότιμων οντοτήτων χαμηλής καθυστέρησης εφόσον προστίθεται μικρή υπερθέρμανση στα κανάλια επικοινωνίας. Τα jondos μεταφέρουν αιτήματα αναζητήσεων, απαντήσεις και δεδομένα ελέγχου χωρίς να επιβαρύνουν το δίκτυο.

- ***Mute***: Στο δίκτυο Mute λόγω του ότι το downloading πραγματοποιείται διαμέσου πολλών κόμβων ο ρυθμός του είναι αρκετά χαμηλός και επομένως σε ένα μεγάλο δίκτυο υπάρχει αρκετή καθυστέρηση.

- ***BitBlender***: Το BitBlender προσδίδει χαμηλή καθυστέρηση στους χρήστες του.

- ***Truste***: Το Truste δεν προσδίδει καθυστέρηση στους χρήστες που επισκέπτονται πιστοποιημένους ιστοτόπους απλά πιστοποιεί την πολιτική προστασίας των προσωπικών δεδομένων που εφαρμόζεται από αυτούς.

- ***P3P***: Το P3P προσδίδει μία μικρή καθυστέρηση στον χρήστη την πρώτη φορά που επισκέπτεται την ιστοσελίδα έως ότου τοποθετήσει και ανακτήσει την πολιτική P3P. Παρ' όλα αυτά η καθυστέρηση αυτή είναι μικρότερη από την καθυστέρηση που προκαλεί η ανάκτηση εικόνας από μία ιστοσελίδα. Μεταγενέστερες όμως αιτήσεις στην ίδια

ιστοσελίδα δεν προσθέτουν καθυστέρηση για το χρονικό διάστημα που η συμφωνηθείσα εφαρμοζόμενη πολιτική είναι σε ισχύ και δεν έχει λήξει [65].

4.11 Άρνηση Υπηρεσίας

- ***LPWA***: Από τη στιγμή που η επικοινωνία του χρήστη με τον εξυπηρετητή πραγματοποιείται διαμέσου του πληρεξούσιου αποτελεί σημείο ευπάθειας στην επίθεση αυτή. Εάν ο πληρεξούσιος βρεθεί εκτός λειτουργίας για τεχνικούς λόγους τότε η επίπτωση άρνησης υπηρεσίας στην επικοινωνία είναι αναπόφευκτη.

- ***Anonymizer***: Η επικοινωνία είναι ευπαθής σε μία τέτοια επίθεση μόνο εάν ο ενδιάμεσος πληρεξούσιος για οποιοδήποτε λόγο δεν είναι διαθέσιμος ή βρεθεί εκτός λειτουργίας.

- ***Mixminio****n*: Το mixminion δεν παρέχει προστασία έναντι των επιθέσεων άρνησης της υπηρεσίας.

- ***Crowds***: Το Crowds δεν προστατεύει από την επίθεση των κακόβουλων μελών του που προκαλούν άρνηση της υπηρεσίας.

- ***AP3***: Το AP3 είναι ευπαθές σε επιθέσεις άρνησης υπηρεσίας. Για να συμβεί μια επίθεση άρνησης υπηρεσίας ένας κακόβουλος κόμβος πρέπει να είναι σε κάποιο σημείο του μονοπατιού δρομολόγησης ή το μονοπάτι να αποτελείται από πολλούς κακόβουλους κόμβους.

- ***Tarzan***: Ο μηχανισμός mimic που παρέχει το Tarzan αναθέτει σε ζεύγη των κόμβων να ανταλλάξουν εικονική κίνηση. Ο μηχανισμός αυτός προσφέρει προστασία από επιθέσεις άρνησης της υπηρεσίας.

- ***TOR***: Το TOR δίκτυο είναι ευπαθές στην άρνηση της υπηρεσίας εφόσον δεν αποκλείονται οι επιθέσεις που στοχεύουν στην κατανάλωση της CPU και εφόσον είναι πιθανό κάποιοι onion routers να βρεθούν εκτός λειτουργίας και να προκαλέσουν πρόβλημα στην επικοινωνία του χρήστη με τον εξυπηρετητή.

- ***Java Anon Proxy***: Η επικοινωνία του χρήστη με τον εξυπηρετητή πραγματοποιείται διαμέσου διαφορετικών αλλά καθορισμένων ακολουθιών από κόμβους mixes. Η

δρομολόγηση λοιπόν είναι στατική και συγκεκριμένη με αποτέλεσμα εάν κάποιος κόμβος Mix της διαδρομής βρεθεί εκτός λειτουργίας η επικοινωνία του χρήστη με τον εξυπηρετητή να διακοπεί.

- ***Morphmix***: Το Morphmix δεν μπορεί να αποτρέψει κάποιον αντίπαλο που μπλοκάρει την κίνηση των κόμβων που ελέγχει. Είναι δύσκολο να ελεγχθεί μία τέτοια επίθεση εκτός και αν χρησιμοποιηθεί το "reputation system" σύμφωνα με το οποίο οι κόμβοι που συνεχώς αποτυγχάνουν στην προώθηση των δεδομένων, αποκτούν κακή φήμη και δεν συμπεριλαμβάνονται στις εκτεταμένες επιλογές από τους ειλικρινείς κόμβους. Αλλά η έρευνα σε αυτόν τον μηχανισμό είναι ακόμα σε εξέλιξη και επομένως δεν θεωρείται αξιόπιστος προς το παρόν. Επίσης το Morphmix είναι ευπαθές σε τούνελ δρομολόγησης που αποτυγχάνουν. Στην περίπτωση αυτή εναλλάσσεται το τούνελ και εγκαθίσταται πάλι η επικοινωνία με τον εξυπηρετητή.

- ***I2P***: Το I2P δεν προστατεύει σε επαρκή βαθμό ενάντια στην επίθεση άρνησης υπηρεσίας. Αντιμετωπίζει την επίθεση αυτή, διατηρώντας τα προφίλ των κόμβων που συμμετέχουν αναγνωρίζοντας έτσι τους κόμβους με χαμηλή απόδοση με σκοπό την αγνόησή τους ή την σπάνια χρησιμοποίησή τους. Αν και η αναγνώριση των κόμβων που δυσλειτουργούν στο σύστημα έχει σημαντικά αποτελέσματα δεν επαρκεί για την αντιμετώπιση της άρνησης της υπηρεσίας και επομένως περαιτέρω έρευνα διενεργείται στο πεδίο της επίθεσης αυτής.

- ***GNUnet***: Ο κάθε κόμβος όταν λαμβάνει ένα ερώτημα παίρνει κάποιες αποφάσεις σχετικά με την αποστολή του και την διεκπεραίωσή του. Εάν όμως δεν λάβει απάντηση εντός συγκεκριμένου χρονικού διαστήματος, το επίπεδο της εφαρμογής αποφασίζει εάν θα το απορρίψει. Σε περίπτωση λοιπόν που κάποιος πόρος δεν είναι διαθέσιμος τότε αυτό αφήνει ανοιχτό το σύστημα στην άρνηση της υπηρεσίας.

- ***P5***: Το πρωτόκολλο P5 καθορίζει ένα όριο στην ουρά κάθε ζεύξης "per link queue limit" με αποτέλεσμα όταν κάποιος κακόβουλος κόμβος στείλει πολλά πακέτα αυτά να ξεπερνούν το όριο και να απορρίπτονται.

- ***Herbivore***: Στο δίκτυο του Herbivore, σε κάθε round, ο κάθε κόμβος χωρίζει τα δεδομένα σε πακέτα ίδιου μεγέθους και μεταδίδει το κάθε πακέτο σε διαδοχικά slots. Οι

κακόβουλοι κόμβοι ενδέχεται να προκαλέσουν άρνηση της υπηρεσίας είτε επιτυγχάνοντας μείωση του εύρους ζώνης με την δέσμευση πολλών slots, είτε με το να μεταδίδουν χωρίς να έχουν δεσμεύσει slots, είτε με την επιβράδυνση της συχνότητας round. Επίσης για την επίτευξη της άρνησης της υπηρεσίας απαιτείται μεγάλο εύρος ζώνης [30]. Για παράδειγμα εάν υπάρχουν 106 cliques που μεταδίδουν στα 100kb/s ένας αντίπαλος με το να μεταδώσει στα 10Gb/s μπορεί να κλείσει μόνο 10% του δικτύου. Ένας κακόβουλος κόμβος όπως αναφέρθηκε μπορεί να μειώσει το εύρος ζώνης με την μείωση της συχνότητας μετάδοσης η οποία σε κάθε round καθορίζεται από τον πιο αργό κόμβο του clique. Παρόλα αυτά το Herbivore μπορεί να περιορίσει τους κόμβους που μεταδίδουν πολύ αργά. Επομένως το Herbivore παρέχει μηχανισμούς προστασίας για την άρνηση της υπηρεσίας αλλά δεν περιορίζει την πιθανότητα ύπαρξης στο σύστημα.

- ***Mantis***: Στο Mantis μπορεί να προκληθεί άρνηση της υπηρεσίας σε περίπτωση που κάποιος κόμβος του αντίστροφου μονοπατιού, στο ενδιάμεσο της επικοινωνίας του εξυπηρετητή με τον πελάτη, διακόψει την επικοινωνία του και αποσυρθεί από το σύστημα. Αν και το Mantis έχει προβλέψει σε αυτή την περίπτωση ο εξυπηρετητής κόμβος να επαναδημιουργήσει κανάλι επικοινωνίας με τον πελάτη κόμβο γνωρίζοντας όμως την IP διεύθυνσή του και την θύρα του, δεν παύει να είναι ένα ανοιχτό σημείο ευπάθειας στο δίκτυο εφόσον προκειμένου να ενημερωθεί με τα στοιχεία του πελάτη κόμβου το Mantis πρέπει να μετριάσει τους περιορισμούς για την προστασία της ανωνυμίας του πελάτη [07].

- ***Mute***: Στο δίκτυο Mute οι κόμβοι δρομολογούν τα μηνύματα που λαμβάνουν βάσει του πίνακα δρομολόγησής τους. Το περιβάλλον λειτουργίας του Mute είναι δυναμικό και μπορεί να οδηγήσει σε άρνηση της υπηρεσίας λόγω των απρόοπτων προβλημάτων που ενδέχεται να προκύψουν όπως π.χ. σε περίπτωση που κάποιος κόμβος στον οποίον αποστέλλεται ένα μήνυμα βρίσκεται εκτός δικτύου για τεχνικούς λόγους, το μήνυμα δεν προωθείται προς τον προορισμό του.

- ***BitBlender***: Είναι δυνατόν να προκύψει άρνηση της υπηρεσίας καθώς ο χρήστης λαμβάνει ένα αρχείο που έχει αιτηθεί και κάποιος κόμβος που περιέχει ένα τμήμα του αρχείου βρεθεί εκτός λειτουργίας για τεχνικούς λόγους ή δεν είναι διαθέσιμος. Αυτό όμως προκύπτει από την αρχιτεκτονική λειτουργίας του BitTorrent που επηρεάζει και την λειτουργία του BitBlender. Επίσης άρνηση της υπηρεσίας μπορεί να επέλθει εάν το

Blender είναι ένας κεντρικός εξυπηρετητής καταλόγου αποτελώντας σημείο ευπάθειας και κεντρικό σημείο αποτυχίας της λειτουργίας του πρωτοκόλλου και κατ επέκταση του δικτύου.

- ***Truste***: Δεν εστιάζεται στην αντιμετώπιση άρνηση της υπηρεσίας εφόσον απλά πιστοποιεί την πολιτική προστασίας των προσωπικών δεδομένων που εφαρμόζεται από τον κάθε ιστότοπο. Η αντιμετώπιση αυτής της απειλής εξαρτάται από τους μηχανισμούς προστασίας του κάθε ιστοτόπου.

- ***P3P***: Το P3P δεν προσφέρει καμία προστασία έναντι κακόβουλων επιθέσεων. Η αντιμετώπιση της άρνησης υπηρεσίας εξαρτάται από τους μηχανισμούς προστασίας που παρέχεται από το κάθε σύστημα και όχι από το P3P το οποίο επικεντρώνεται στην διασφάλιση πολιτικών προστασίας της ιδιωτικότητας και στην ενημέρωση και συγκατάθεση του χρήστη για οποιαδήποτε χρήση των προσωπικών του στοιχείων που λαμβάνει η κάθε ιστοσελίδα.

4.12 Επίθεση Πλημμυρίδας

- ***LPWA***: Ο χρήστης επικοινωνεί με τον εξυπηρετητή διαμέσου του πληρεξούσιου ο οποίος αποτελεί κεντρικό σημείο της αρχιτεκτονικής του LPWA. Η επικοινωνία αυτή αποτελεί σημείο ευπάθειας στην επίθεση πλημμυρίδας.

- ***Anonymizer***: Η επικοινωνία του χρήστη με τον πληρεξούσιο του Anonymizer διαμέσου του εικονικού ιδιωτικού δικτύου προστατεύει από την επίθεση αυτή. Στο εικονικό ιδιωτικό δίκτυο τα δυο άκρα που επικοινωνούν πρέπει πρώτα να ελέγξουν την ταυτότητά τους, να διεξάγουν διαδικασία αυθεντικοποίησης, και στην συνέχεια να εγκατασταθεί το ασφαλές τούνελ επικοινωνίας. Επομένως το Anonymizer επιτρέποντας την απομακρυσμένη πρόσβαση σε αυθεντικοποιημένους χρήστες και χρησιμοποιώντας κρυπτογραφικές τεχνικές για την μεταξύ τους επικοινωνία ενεργεί αποτελεσματικά στην επίθεση της πλημμυρίδας.

- ***Mixminion***: Το mixminion δεν προστατεύει πλήρως από την επίθεση πλημμυρίδας, αν και η χρησιμοποίηση μίας τιμής ορίου σε κάθε κόμβο Mix κατά την συγκέντρωση των μηνυμάτων, πριν την αποστολή τους στον επόμενο κόμβο προορισμού, αποτρέπει εν

μέρει από αυτή την επίθεση παρέχοντας σε κάθε κόμβο έναν σταθερό ρυθμό αποστολής μηνυμάτων. Η λύση αυτή δεν παρέχει πλήρης προστασία και παραμένει ένα ανοιχτό πρόβλημα.

- ***Crowds***: Το Crowds δεν προστατεύει από την επίθεση πλημμυρίδας των κακόβουλων μελών του. Αν και η συμμετρική κρυπτογράφηση της επικοινωνίας μεταξύ των jondo ενεργεί, εν μέρει, ως μηχανισμός αυθεντικοποίησης δεν αποτρέπει όμως την επίθεση αυτή.

- ***AP3***: Δεν παρέχει καμία προστασία και κανέναν μηχανισμό αντιμετώπισης της επίθεσης πλημμυρίδας.

- ***Tarzan***: Το Tarzan προστατεύει από την επίθεση πλημμυρίδας που ένας αντίπαλος μπορεί να χρησιμοποιήσει αποστέλλοντας σε κάποιον κόμβο μεγάλο αριθμό πακέτων. Στόχος του αντιπάλου αποτελεί η μείωση του αριθμού των άλλων αποστολέων που ταυτόχρονα χρησιμοποιούν τον κόμβο και η αναγνώριση των δικών του πακέτων που εξέρχονται από τον κόμβο αυτό. Το Tarzan προστατεύει με τους παρακάτω μηχανισμούς: Πρώτον οι κόμβοι mimic κρυπτογραφούν τα μηνύματα μεταξύ τους καθιστώντας δύσκολο για τον αντίπαλο να διακρίνει τα πακέτα του, δεύτερον η κίνηση κάλυψης δεν διακρίνεται από την νόμιμη κίνηση των άλλων κόμβων και τρίτον η αυστηρή δομή της επικάλυψης mimic περιορίζει το σύνολο των κόμβων στους οποίους επιτίθεται ο αντίπαλος. Επομένως, ο μόνος τρόπος για να πλημμυρίσει ένας κακόβουλος κόμβος τους κόμβους mimic είναι μέσω ενός καλοσχηματισμένου τούνελ στο δίκτυο επικάλυψης [47].

- ***TOR***: Το δίκτυο του TOR εφαρμόζει αποκεντροποιημένο έλεγχο συμφόρησης ("congestion control") χρησιμοποιώντας από άκρη-σε-άκρη "acks" για τη διατήρηση της ανωνυμίας, επιτρέποντας στις άκρες του δικτύου να ανιχνεύσουν πλημμύρα ή συμφόρηση. Σε μια τέτοια περίπτωση αποστέλλονται λιγότερα δεδομένα έως ότου η συμφόρηση υποχωρήσει [22].

- ***Java Anon Proxy***: Το Jap προστατεύει από επιθέσεις πλημμυρίδας δεδομένου ότι ο κάθε χρήστης θα πρέπει να αποδείξει με την χρήση ενός έγκυρου εισιτηρίου ότι επιτρέπεται να χρησιμοποιήσει το σύστημα στο αντίστοιχο κομμάτι του χρόνου. Για την προστασία της ταυτότητας του χρήστη το εισιτήριο αυτό είναι μία τυφλή υπογραφή [10] που εκδίδεται

από το ανώνυμο σύστημα επικοινωνίας. Κάθε κόμβος εκδίδει έναν περιορισμένο αριθμό εισιτηρίων για κάθε κανάλι και χρήστη [05], προστατεύοντας κατ' αυτόν τον τρόπο από επιθέσεις πλημμυρίδας κακόβουλων αντιπάλων.

- ***Morphmix***: Το Morphmix παρέχει μηχανισμό ελέγχου ροής των μηνυμάτων ανάμεσα στους κόμβους του. Για την αποφυγή της συσσώρευσης μηνυμάτων στην μνήμη του, κάθε κόμβος προσδιορίζει τον μέγιστο αριθμό των μηνυμάτων που έχει την δυνατότητα να λαμβάνει από τον προηγούμενο γείτονα κόμβο στο τούνελ. Αυτό συμβαίνει σε κάθε περίπτωση όπου ο ρυθμός εισερχομένων μηνυμάτων στον κάθε κόμβο είναι μεγαλύτερος από τον ρυθμό εξερχομένων μηνυμάτων. Ο μηχανισμός ελέγχου ροής των μηνυμάτων συνιστά μηχανισμό προστασίας ενάντια στην επίθεση πλημμυρίδας, χωρίς ωστόσο να αποτρέπει τέτοιου είδους επιθέσεις.

- ***I2P***: Το I2P δεν παρέχει μηχανισμό προστασίας σε αυτή την επίθεση.

- ***GNUnet***: Το πρωτόκολλο GAP απορρίπτει τα ερωτήματα που προέρχονται από κόμβους, οι οποίοι παράγουν κίνηση πάνω από μία προκαθορισμένη τιμή κατωφλίου. Επίσης, ο συνδυασμός ασύμμετρης και συμμετρικής κρυπτογραφίας για τη δημιουργία της κρυπτογραφημένης ζεύξης συνιστά ένα ακόμα εμπόδιο στην επίθεση πλημμυρίδας.

- ***P5***: Το πρωτόκολλο P5 προστατεύει από την επίθεση πλημμυρίδας με την εφαρμογή του αλγορίθμου "dropping" σε κάθε κόμβο. Εάν κάποιος κόμβος λάβει έναν αριθμό μηνυμάτων και δεν διαθέτει την επεξεργαστική ικανότητα, καθώς επίσης και το διαθέσιμο εύρος ζώνης, τότε αυτά απορρίπτονται. Επίσης, ο καθορισμός ορίου στην ουρά κάθε ζεύξης και η απόρριψη μηνυμάτων όταν ο αριθμός αυτών υπερβεί το εν λόγω όριο, αποτελεί έναν ισχυρό μηχανισμό αποτροπής της συγκεκριμένης επίθεσης.

- ***Herbivore***: Ένας κακόβουλος κόμβος ενδέχεται να δεσμεύσει πολλά slots για την μετάδοση ενός μηνύματος μειώνοντας το εύρος ζώνης και προκαλώντας αρνητικά αποτελέσματα στο σύστημα. Το πρωτόκολλο round προσφέρει προστασία σε μια ομάδα clique από την επίθεση πλημμυρίδας χωρίς όμως να αποκλείει την ύπαρξή της.

- ***Mantis***: Το Mantis δεν προσφέρει μηχανισμό προστασίας σε αυτή την επίθεση.

- ***Mute***: Χαρακτηριστικός μηχανισμός του δικτύου Mute αποτελεί το UtilityCounter. Ο μετρητής αυτός ελέγχει τα άλματα των μηνυμάτων αναζήτησης στο δίκτυο το οποίο και προστατεύει από την επίθεση πλημμυρίδας.

- ***BitBlender***: Το BitBlender δεν παρέχει μηχανισμό προστασίας για την αντιμετώπιση αυτής της επίθεσης.

- ***Truste***: Δεν εστιάζεται στην αντιμετώπιση της επίθεσης αυτής εφόσον απλά πιστοποιεί την πολιτική προστασίας των προσωπικών δεδομένων που εφαρμόζεται από τον κάθε ιστότοπο. Η αντιμετώπιση αυτής της απειλής εξαρτάται από τους μηχανισμούς προστασίας του κάθε ιστοτόπου.

- ***P3P***: Η αντιμετώπιση της επίθεσης αυτής εξαρτάται από τους μηχανισμούς προστασίας που παρέχεται από το κάθε σύστημα και όχι από το P3P που επικεντρώνεται στην διασφάλιση πολιτικών προστασίας της ιδιωτικότητας και στην ενημέρωση και συγκατάθεση του χρήστη για οποιαδήποτε χρησιμοποίηση των προσωπικών του στοιχείων που λαμβάνει η κάθε ιστοσελίδα.

Η συγκριτική ανάλυση που προηγήθηκε συνοψίζεται στον ακόλουθο πίνακα:

Κατηγορία	PET	Επίθεση Ανάλυσης Κίνησης	Ωτακουστές	Επίθεση Χρονισμού	Επίθεση Κωδικοποίησης Μηνύματος	Επίθεση Traceback Παθητική	Επίθεση Traceback Ενεργή	Επίθεση Σήμανσης	Επίθεση Διασταύρωσης	Κακόβουλοι κόμβοι	Επίθεση τύπου ενδιάμεσου	Καθυστέρηση	Άρνηση υπηρεσίας	Επίθεση πλυμμηρίδας
Proxy	LPWA	-	-	-	-	-	-	-	-	-	-	X	-	-
Proxy	Anonymizer	+	+	+	+	+	+	+	+	+	+	X	-	+
Mix Networks	Mixminion	-	+	+	+	+	+	+	-	+	+	Y	-	-
P2P Networks	Crowds	-	+	-	+	-	+	-	-	+	+	M	-	-
P2P Networks	AP3	-	-	-	-	-	-	+	-	-	-	X	-	-
P2P Networks	Tarzan	+	+	-	+	+	+	+	+	+	+	X	+	+
P2P Networks	Onion Routing	+	+	-	+	-	+	-	-	+	+	X	-	-
P2P Networks	Tor	+	+	-	+	-	+	+	-	+	-	M	-	+
P2P Networks	JAP	+	+	+	+	-	+	-	-	+	+	M	-	+
P2P Networks	MorphMix	+	+	-	+	-	+	+	-	+	+	X	-	-
P2P Networks	I2P	+	+	+	+	-	+	+	-	-	-	X	-	-
P2P Networks	GAP	+	+	+	+	+	+	+	-	+	+	X	-	+
P2P Networks	P5	+	+	+	+	-	+	+	-	-	+	Y	+	+
P2P Networks	Herbivore	+	+	+	+	+	+	+	+	+	+	X	-	-
P2P Networks	Mantis	-	+	-	+	-	+	-	-	-	-	X	-	-
P2P Networks	Mute	-	-	-	-	-	-	-	-	-	-	Y	-	+
P2P Networks	Bit Blender	-	Ǿ	-	Ǿ	-	-	Ǿ	-	-	-	X	-	-
Privacy Policies	Truste	Ǿ	-	Ǿ	Ǿ	Ǿ	Ǿ	Ǿ	Ǿ	Ǿ	Ǿ	Ǿ	Ǿ	Ǿ
Privacy Policies	P3P	Ǿ	Ǿ	Ǿ	Ǿ	Ǿ	Ǿ	Ǿ	Ǿ	Ǿ	Ǿ	X	Ǿ	Ǿ

Πίνακας 1: Συγκριτική ανάλυση των PET βάσει των επιλεγμένων απειλών της ιδιωτικότητας.

4.13 Συμπεράσματα

Στην παρούσα μεταπτυχιακή διατριβή μελετήθηκε πληθώρα συστημάτων προστασίας της ιδιωτικότητας, τα οποία βασίζονται σε διαφορετικά κεντρικά δομικά στοιχεία αρχιτεκτονικής. Το κάθε σύστημα εστιάζει σε διαφορετικά στοιχεία εξασφάλισης της ιδιωτικότητας του χρήστη και αντιμετώπισης των διαφόρων κακόβουλων επιθέσεων με αποτέλεσμα τα σημεία ευπάθειάς τους αλλά και οι μηχανισμοί προστασίας που παρέχουν να μην συγκλίνουν μεταξύ τους. Για την καλύτερη αξιολόγηση των συμπερασμάτων της σύγκρισης, παρατίθενται οι μηχανισμοί προστασίας της ιδιωτικότητας κατηγοριοποιημένοι ως προς το βασικό λειτουργικό στοιχείο της αρχιτεκτονικής τους.

Τα συστήματα που η λειτουργία τους στηρίζεται σε έναν HTTP πληρεξούσιο, όπως το LPWA και ο Anonymizer, στοχεύουν στην διασφάλιση της ανώνυμης περιήγησης του χρήστη στο διαδίκτυο. Παρατηρείται όμως ότι ο πληρεξούσιος, ως κεντρικό δομικό στοιχείο της αρχιτεκτονικής τους, αποτελεί σημείο ευπάθειας σε κακόβουλες επιθέσεις είτε ενεργές είτε παθητικές. Η επικοινωνία του χρήστη με τον πληρεξούσιο αποτελεί στόχος των αντιπάλων, παρακολουθώντας την κίνηση που εισέρχεται και εξέρχεται από αυτόν. Για την καλύτερη και ασφαλέστερη επικοινωνία του χρήστη με τον πληρεξούσιο θα πρέπει το σύστημα να προσφέρει μηχανισμούς κρυπτογράφησης και προστασίας του διαύλου επικοινωνίας τους, όπως παρέχεται από τον Anonymizer, στον οποίον η επικοινωνία γίνεται μέσω σύνδεσης TLS δημιουργώντας ένα κρυπτογραφημένο τούνελ. Επομένως, οι μηχανισμοί προστασίας που στηρίζουν την λειτουργία τους σε έναν κεντρικό πληρεξούσιο, ο οποίος μεσολαβεί στην επικοινωνία του χρήστη με τον εξυπηρετητή του διαδικτύου, θα πρέπει να εξασφαλίζουν την ασφαλή επικοινωνία του πληρεξούσιου με τον χρήστη ώστε να αποτρέπονται οι κακόβουλες επιθέσεις των αντιπάλων σε αυτόν για την παραβίαση της ιδιωτικότητας του χρήστη.

Τα συστήματα που στηρίζουν τη λειτουργία τους στους κόμβους mix παρέχουν μηχανισμούς πολυεπίπεδης κρυπτογράφησης των δεδομένων εξασφαλίζοντας σε ικανοποιητικό βαθμό την προστασία του περιεχομένου τους, αλλά και την μη συνδεσιμότητα των μηνυμάτων με τον αποστολέα από τους αντιπάλους. Το mixminion, αν και παρέχει τη δυνατότητα στον χρήστη να στείλει και να λάβει ανώνυμα ηλεκτρονικά μηνύματα, ανταποκρινόμενο θετικά στην προστασία της ιδιωτικότητας του χρήστη διαμέσου των μηχανισμών που παρέχει ενάντια σε κακόβουλες επιθέσεις, παρ' όλα αυτά προσδίδει στο σύστημα υψηλή καθυστέρηση που είναι εμφανή στον χρήστη.

Το Crowds, αλλά και τα συστήματα που στηρίζουν την λειτουργία τους στην αρχιτεκτονική του, όπως το AP3 και το Tarzan, έχει ως χαρακτηριστικό στοιχείο του συστήματος για την προστασία της ιδιωτικότητας των χρηστών την απόκρυψη των ενεργειών τους ανάμεσα στις ενέργειες του πλήθους των κόμβων που συμμετέχουν στο δίκτυο. Ο κάθε κόμβος γνωρίζει μόνο τον προηγούμενο και τον επόμενο κόμβο και δεν γνωρίζει όλο το μονοπάτι προς τον τελικό προορισμό του μηνύματος, προσφέροντας κατ' αυτόν τον τρόπο προστασία από τους κακόβουλους αντιπάλους, είτε ενεργούς είτε παθητικούς. Επίσης, τα συστήματα αυτά προσφέρουν προστασία ως προς τη μη συνδεσιμότητα των μηνυμάτων με τον εκκινητή τους και αποτελούν ισχυρά εργαλεία αποτροπής διαφόρων κακόβουλων επιθέσεων. Το Crowds προσδίδει μέτρια καθυστέρηση στην επικοινωνία του χρήστη, ενώ το Tarzan και το AP3 προσδίδουν μικρή καθυστέρηση. Σε γενικές γραμμές, η απόδοση του συστήματος των μηχανισμών προστασίας της ιδιωτικότητας εναλλάσσεται ανάλογα με το παρεχόμενο επίπεδο ασφαλείας της ιδιωτικότητας του χρήστη. Για παράδειγμα, το AP3 προσδίδει μικρή καθυστέρηση αλλά η προστασία της ιδιωτικότητας που προσφέρει στον χρήστη, παρουσιάζει αρκετά σημεία ευπάθειας, ενώ το Tarzan προσδίδει μικρή καθυστέρηση με την προστασία της ιδιωτικότητας του χρήστη να περιορίζεται μόνο στο network layer. Αντίθετα, το Crowds το οποίο προσδίδει μέτριου βαθμού καθυστέρηση είναι πιο αποτελεσματικό στην αντιμετώπιση κακόβουλων επιθέσεων.

Το Onion Routing παρέχει προστασία της πληροφορίας που μεταδίδεται στο δίκτυο και αποτρέπει αποτελεσματικά διάφορες κακόβουλες επιθέσεις. Το TOR, δεύτερης γενιάς onion routing, προσφέρει μηχανισμούς βελτιστοποίησης που συμβάλλουν στην αποτελεσματικότερη προστασία της ιδιωτικότητας του χρήστη. Διατίθεται μόνο για εφαρμογές που βασίζονται στο πρωτόκολλο TCP, οι οποίες αποτελούν και την πλειοψηφία των υπαρχουσών εφαρμογών, και στοχεύει στην απόκρυψη των ενεργειών του χρήστη στο διαδίκτυο και στην ασφαλή μετάδοση των δεδομένων του. Δεν προστατεύει από επιθέσεις που πραγματοποιούνται στα άκρα του δικτύου του καθώς σχεδιαστικά είναι εκτεθειμένα σε επιθέσεις κακόβουλων αντιπάλων. Χαρακτηριστικό στοιχείο της λειτουργίας του αποτελεί το ότι οι αναμεταδότες κόμβοι του δικτύου παρέχονται από χρήστες-εθελοντές οι οποίοι είναι διασκορπισμένοι σε διάφορες τοποθεσίες ανά τον κόσμο. Το στοιχείο αυτό, εκτός από τα πλεονεκτήματα που προσφέρει στο δίκτυο, έχει αντίκτυπο στην καθυστέρηση της επικοινωνίας του χρήστη με τον προορισμό του.

Το Jap, το Morphmix και το I2P αποτελούν υλοποιήσεις δικτύου mix σε δίκτυα peer-to-peer. Προσφέρουν ανώνυμα κανάλια επικοινωνίας και παράλληλα επωφελούνται από την ισχυρή πολυεπίπεδη κρυπτογράφηση που προσφέρεται από τους κόμβους mix. Το περιεχόμενο των

μηνυμάτων προστατεύεται από κακόβουλες επιθέσεις και σε γενικά προσεγγιστικά πλαίσια προστατεύουν σε ικανοποιητικό βαθμό την ιδιωτικότητα του χρήστη, παρά το γεγονός ότι εντοπίζονται ευπαθή σημεία στην αρχιτεκτονική της λειτουργίας τους.

Το πρωτόκολλο GAP έχει σχεδιαστεί για να καλύψει τις ανάγκες του ομότιμου δικτύου GNUnet διασφαλίζοντας την ανωνυμία των συναλλαγών μεταξύ των μελών του. Επισημαίνεται ότι ανταποκρίνεται θετικά στην αντιμετώπιση των κακόβουλων επιθέσεων των αντιπάλων προσδίδοντας μικρή καθυστέρηση στο δίκτυο.

Το πρωτόκολλο P5 προσφέρει ανώνυμη επικοινωνία στο διαδίκτυο παρέχοντας ανωνυμία τόσο στον αποστολέα όσο και στον παραλήπτη. Επιτρέπει σε μικρές ιεραρχημένες ομάδες μετάδοσης να συνδέονται στο δίκτυο και να επικοινωνούν με ασφαλή και ανώνυμο τρόπο. Κάθε χρήστης έχει τη δυνατότητα να ανταλλάξει το επίπεδο ανωνυμίας που επιθυμεί με την αποδοτικότητα της επικοινωνίας του στο δίκτυο.

Το Herbivore αποτελεί ένα πρωτόκολλο που παρέχει ανώνυμη επικοινωνία σε δίκτυα ομότιμων οντοτήτων και εκτελείται σε dining cryptography δίκτυα “DCnets”. Προσφέρει ανωνυμία στην επικοινωνία των μελών και προστατεύει τα επικοινωνούντα άκρα από κακόβουλες επιθέσεις μόνο εφόσον συμμετέχουν εντός της ομάδας του clique. Σε κάθε άλλη περίπτωση οι υπηρεσίες εκτός του clique είναι εκτεθειμένες. Προσαρμόζεται και ανταποκρίνεται αποδοτικά σε ένα μεγάλο αριθμό χρηστών, επιτυγχάνοντας υψηλό εύρος ζώνης και χαμηλή καθυστέρηση.

Τα Mantis και Mute αποτελούν δίκτυα ομότιμων οντοτήτων τα οποία προσφέρουν ανώνυμο διαμοιρασμό αρχείων στους χρήστες του. Το Mantis παρέχει προστασία της ταυτότητας του χρήστη που εκκινεί ένα αίτημα ή μια υπηρεσία, προστατεύοντας τόσο την ανωνυμία του εξυπηρετητή όσο και το περιεχόμενο της επικοινωνίας των κόμβων. Το δυναμικό περιβάλλον λειτουργίας του, καθώς και η αποκάλυψη της διεύθυνσης IP και της διαθέσιμης θύρας των κόμβων του που συμμετέχουν σε μια κεντρική οντότητα, αφήνει ανοιχτά σημεία ευπάθειας σε διάφορες κακόβουλες επιθέσεις. Συγκριτικά, το δίκτυο Mute είναι περισσότερο ευπαθές στις διάφορες κακόβουλες επιθέσεις σε σχέση με το δίκτυο Mantis. Δεν παρέχει προστασία του περιεχομένου που συναλλάσσεται στο δίκτυο από τα μέλη του και δέχεται κυρίως επιθέσεις συσχετισμού της πραγματικής IP των κόμβων του αντιστοιχίζοντάς την με την ψευδο-ID με την οποία συμμετέχουν στο δίκτυο. Η καθυστέρηση στο δίκτυο του Mantis είναι μικρή σε σχέση με την καθυστέρηση του δικτύου Mute.

Το BitBlender αποτελεί ένα πρωτόκολλο παροχής ανωνυμίας στην κίνηση του BitTorrent. Το BitTorrent είναι ένα πρωτόκολλο διαμοιρασμού αρχείων σε δίκτυα ομότιμων κόμβων. Η ανωνυμία που παρέχει στο δίκτυο το BitBlender δεν στηρίζεται στην απόκρυψη και κρυπτογράφηση του διαμοιραζόμενου περιεχομένου των μελών του, εφόσον είναι δημόσια εκτεθειμένο, αλλά στον αριθμό των συμμετεχόντων κόμβων. Όσο μεγαλύτερος είναι ο αριθμός αυτός τόσο αυξάνει η δυσκολία σε κάποιον κακόβουλο επιτιθέμενο να αποκαλύψει τους κόμβους που εμπλέκονται στην μεταφορά των αρχείων torrent. Παρ' όλα αυτά είναι ευπαθές σε διάφορες κακόβουλες επιθέσεις.

Το Truste και το P3P αποτελούν υπηρεσίες ενημέρωσης του χρήστη σχετικά με τις πολιτικές προστασίας των προσωπικών του δεδομένων που εφαρμόζει ο κάθε ιστότοπος που επισκέπτεται. Δεν εστιάζουν και δεν παρέχουν μηχανισμούς προστασίας της ιδιωτικότητας του χρήστη από κακόβουλες επιθέσεις αλλά επικεντρώνονται στην διασφάλιση της σύμφωνης γνώμης του. Ο χρήστης πρέπει να είναι ενήμερος σχετικά με τα προσωπικά στοιχεία που αντλεί και καταχωρεί ο κάθε ιστότοπος στις βάσεις δεδομένων του, καθώς επίσης και για τον τρόπο με τον οποίον ο ιστότοπος τα διαχειρίζεται και τα χρησιμοποιεί. Ταυτόχρονα, ο κάθε ιστότοπος πρέπει να έχει την συγκατάθεση του χρήστη πριν προχωρήσει σε οποιαδήποτε ενέργεια αποθήκευσης και αξιοποίησης των προσωπικών δεδομένων του.

Κεφάλαιο 5
Επίλογος

Η ραγδαία ανάπτυξη του διαδικτύου και η διείσδυσή του στην καθημερινή ζωή των ανθρώπων είναι ένα αναμφισβήτητο γεγονός. Η μεταβολή που έχει επιφέρει στη λειτουργία της κοινωνίας και στον τρόπο επικοινωνίας των ανθρώπων, έχει καταστήσει τη χρήση του διαδικτύου αναγκαία και αναπόσπαστο κομμάτι της καθημερινής επικοινωνίας των ανθρώπων. Ταυτόχρονα όμως έχει συμβάλει στον πολλαπλασιασμό των προβλημάτων που αφορούν στην ιδιωτικότητα των ανθρώπων. Πράγματι, η χρήση του διαδικτύου διευκολύνει την συλλογή και επεξεργασία των προσωπικών δεδομένων των ατόμων σε ευρεία κλίμακα.

Πράγματι, ο τρόπος επικοινωνίας του χρήστη με τον εκάστοτε ιστότοπο που επισκέπτεται αφήνει εκτεθειμένη την διεύθυνση IP του και κατ' επέκταση την ταυτότητά του. Κατ' αυτόν τον τρόπο ο χρήστης έρχεται έμμεσα αντιμέτωπος με κακόβουλους επιτιθέμενους που στοχεύουν στην άντληση πληροφοριών σχετικά με τα ενδιαφέροντά του, για διαφημιστικούς και άλλους σκοπούς, παραβιάζοντας την ιδιωτικότητά του. Είναι επίσης γεγονός ότι οι χρήστες, έχοντας ελλιπή γνώση για τους κινδύνους, αποκαλύπτουν προσωπικά στοιχεία σε διάφορους

ιστότοπους, όπως αριθμός ταυτότητας, πιστωτικής κάρτας, κτλ, χωρίς να αντιλαμβάνονται ότι μπορεί να αποτελέσουν στόχο κακόβουλων επιθέσεων για την υποκλοπή προσωπικών τους στοιχείων.

Οι κίνδυνοι που διατρέχει ο χρήστης, με την εξέλιξη της τεχνολογίας και κατ' επέκταση του διαδικτύου, αυξάνονται συνεχώς καθιστώντας αναγκαία την ανάπτυξη αποτελεσματικών μηχανισμών προστασίας της ιδιωτικότητας. Πράγματι, τις τρεις τελευταίες δεκαετίες υπάρχει ενεργό ένα μεγάλο φάσμα ερευνητικής δραστηριότητας, η οποία οδήγησε στην ανάπτυξη πληθώρας μηχανισμών προστασίας της ιδιωτικότητας. Η παρούσα μεταπτυχιακή διατριβή περιέγραψε διάφορους μηχανισμούς προστασίας της ιδιωτικότητας και ανέλυσε τα σημεία ευπάθειάς τους έναντι διαφόρων κακόβουλων επιθέσεων. Από τον συγκριτικό πίνακα που παρατέθηκε στο κεφάλαιο 4 προκύπτει ότι οι μηχανισμοί προστασίας της ιδιωτικότητας δεν συγκλίνουν ως προς την αντιμετώπιση των κακόβουλων επιθέσεων αφενός μεν διότι η αρχιτεκτονική τους είναι ελλιπής και αφήνει σημεία ευπάθειας και αφετέρου διότι επικεντρώνονται σε διαφορετικά σημεία προστασίας της ιδιωτικότητας του χρήστη.

Αξιοσημείωτο είναι ότι, μέχρι σήμερα, για να προστατευθεί η ανωνυμία του χρήστη θα πρέπει να «θυσιαστεί» ένα μέρος της απόδοσης του συστήματος προστασίας της ιδιωτικότητας που χρησιμοποιεί. Επίσης, δεν έχει αναπτυχθεί και εφαρμοστεί, τουλάχιστον ακόμα, κάποιος μηχανισμός που να επιφέρει πραγματικά αποτελεσματική και ισχυρή προστασία στην ανωνυμία του χρήστη.

Είναι γεγονός ότι η εφαρμογή των τεχνολογιών αυτών συναντά διάφορα τεχνολογικά και μη προβλήματα. Σύμφωνα με τους Cas και Hafskjold [08]: «Μέχρι στιγμής οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας δεν συνέβαλαν όσο θα ήταν δυνατό για την προστασία της ιδιωτικότητας, εν μέρει λόγω της έλλειψης διαθεσιμότητας των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας και εν μέρει λόγω της έλλειψης φιλικότητας προς το χρήστη. Οι πολλές δυσκολίες που ένας χρήστης έχει να αντιμετωπίσει - από μικρές ενοχλήσεις μέχρι συνολική απώλεια της πρόσβασης σε ορισμένες υπηρεσίες - και η τεχνογνωσία που απαιτείται για να κάνουν χρήση των πολλών Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας, μπορεί σε κάποιο βαθμό να εξηγήσει επίσης τη συχνά παρατηρηθείσα απόκλιση μεταξύ των δεδομένων ανησυχιών για την προστασία της ιδιωτικότητας και την πραγματική συμπεριφορά». Οι Leisner και Cas [08] τόνισαν επίσης ότι «οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας δεν υποστηρίζονται επαρκώς από τους ισχύοντες κανονισμούς», ενώ ο Sommer [08] παρατήρησε ότι «εξακολουθούμε να αντιμετωπίζουμε σημαντικά εμπόδια για την ανάπτυξη των τεχνολογιών αυτών (PET) σε μεγάλη κλίμακα (...) το

κομμάτι του επηρεασμού των επιχειρήσεων να σχεδιάσουν τις επιχειρηματικές διαδικασίες τους με τέτοιο τρόπο, ώστε η ελαχιστοποίηση των δεδομένων να μπορεί να εφαρμοστεί όπως προβλέπεται στο PRIME θα είναι ακόμη πιο δύσκολο από ό, τι το τεχνολογικό μέρος».

Συνοψίζοντας, προκειμένου να είναι εφικτή η αποτελεσματική προστασία της ιδιωτικότητας των χρηστών του διαδικτύου καθίσταται αναγκαία αφενός μεν η εφαρμογή τεχνολογιών, σε ευρεία κλίμακα, οι οποίες να χαρακτηρίζονται από ευρωστία, ευχρηστία και αποτελεσματικότητα και αφετέρου η προσαρμογή του νομοθετικού πλαισίου με τέτοιο τρόπο που θα προστατεύει την ιδιωτικότητα των ατόμων σε μεγαλύτερο βαθμό.

Βιβλιογραφία

Ελληνόγλωσση βιβλιογραφία

[01] Λαμπρινουδάκης Κ., Γκρίτζαλης Σ. & Κάτσικας Σ. (2010), Μία Επισκόπηση Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας στον Παγκόσμιο Ιστό, στο Γκρίτζαλης Σ., Λαμπρινουδάκης Κ., Κάτσικας Σ. & Μήτρου Λ. (επιμ.), *Προστασία της ιδιωτικότητας και τεχνολογίες πληροφορικής και επικοινωνιών*, Αθήνα, Παπασωτηρίου.

[02] ΟΗΕ, *Διακήρυξη των Ανθρωπίνων Δικαιωμάτων*, 1948, Ανακτήθηκε από http://www.ohchr.org/EN/UDHR/Documents/UDHR Translations/grk.pdf

Ξενόγλωσση βιβλιογραφία

[03] Bauer K., McCoy D., Grunwald D. & Sicker D. (2008), BitBlender: *Light-Weight Anonymity for BitTorrent*, SecureComm '08, AIPACa Workshop (22 September 2008), Istanbul, Turkey.

[04] Bennett K. & Grothoff C., *GAP – Practical Anonymous Networking*, S^3 lab and CERIAS, Ανακτήθηκε από https://gnunet.org/sites/default/files/aff.pdf

[05] Berthold O., Federrath H. & Kopsell S. (2009), Web MIXes: A System for Anonymous and Unobservable Internet Access, in Federrath H. (ed.): *Designing Privacy Enhancing Technologies*, Proceedings of the Workshop on Design Issues in Anonymity and Unobservability, LNCS 2009, Springer-Verlag, Heidelberg.

[06] Bleichenbacher D., Gaber E., Gibbons P.B., Matias Y. & Mayer A. (1998), *On Secure and Pseudonymous Client-Relationships with Multiple Servers*, Proceedings of the 3rd USENIX Workshop on Electronic Commerce (August 31-September 3 1998), Boston, Massachusetts.

[07] Bono S. C., Soghoian C. A. & Monrose F. (2004), *Mantis: A Lightweight, Server-Anonymity Preserving, Searchable P2P Network*, Technical Report TR-2004-01-B-ISI-JHU, Ανακτήθηκε από http://files.dubfire.net/jhu/publications/mantis-tr-b.pdf

[08] Borking J. (2009), *Why Adopting Privacy Enhancing Technologies (PETs) Takes So Much Time*, Ανακτήθηκε από http://ec.europa.eu/justice/news/events/workshop_pets_2009/presentations/BORKING_John_paper.pdf

[09] Centre for Internet Society (2012 April), *Privacy and the Internet: Australian attitudes towards privacy in the online environment*, Ανακτήθηκε από http://www.canberra.edu.au/cis/storage/Australian%20Attitutdes%20Towards%20Privacy%20Online.pdf

[10] Chaum D. L. (1984), *Blind Signature System*, Crypto '83, Plenum Press, New York.

[11] Chaum D. L., *Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms*, Ανακτήθηκε από https://mirror.robert-marquardt.com/anonbib/cache/chaum-mix.pdf

[12] Cheng C. M., Kung H. T. & Tan K. S., *On-Demand Link Padding in Traffic Anonymizing*, Ανακτήθηκε από http://www.eecs.harvard.edu/~htk/publication/2005-jit-cheng-kung-tan.pdf

[13] Clarke R., *Platform for Privacy Preferences: An Overview*, Ανακτήθηκε από http://www.rogerclarke.com/DV/P3POview.html#ArchProc

[14] Clarke R., *Privacy*, Ανακτήθηκε από http://www.rogerclarke.com/DV/Intro.html#Priv

[15] Clothia T., *Analysing the MUTE Anonymous File-Sharing System Using the Pi-calculus*, Ανακτήθηκε από http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.107.7924

[16] Clothia T., *Securing Pseudo Identities in an Anonymous Peer-to-Peer File-Sharing Network*, Ανακτήθηκε από http://www.cs.bham.ac.uk/~tpc/Papers/MuteOutline.pdf

[17] Cvrcek D., Matyas V. & Berthold S. (eds) (2008 March), *D13.1: Identity and impact of privacy enhancing technologies,* Future of Identity in the Information Society (FIDIS), Report.

[18] Cvrcek D. & Matyas V. (eds) (2007 May), *D13.1: Identity and impact of privacy enhancing technologies*, Future of Identity in the Information Society (FIDIS), Report.

[19] Danezis G. & Borisov N., *Denial of Service or Denial of Security: How Attacks on Reliability can Compromise Anonymity*, Ανακτήθηκε από http://research.microsoft.com/en-us/um/people/gdane/papers/ccs0255-borisov.pdf

[20] Danezis G., Dingledine R. & Mathewson N., *Mixminion: Design of a Type III Anonymous Remailer Protocol*, Ανακτήθηκε από http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.107.2563&rep=rep1&type=pdf

[21] Dierks T. & Allen C. (1999 January), *The TLS Protocol — Version 1.0.,* IETF RFC 2246, Ανακτήθηκε από http://www.rfc-editor.org/rfc/rfc2246.txt

[22] Dingledine R., Mathewson N. & Syverson P., *Tor: The Second-Generation Onion Router*, Ανακτήθηκε από https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf

[23] Erkkonen H. & Larsson J., *Anonymous Networks*, Ανακτήθηκε από http://www.cse.chalmers.se/~tsigas/Courses/DCDSeminar/Files/onion_routing.pdf

[24] European Commission (2011 June), Attitudes on Data Protection and Electronic Identity in the European Union, *Special Eurobarometer 359*.

[25] European Court of Human Rights, *European Convention on Human Rights*, Rome, 1950.

[26] Freedman M. J. & Morris R., *Tarzan: A Peer-to-Peer Anonymizing Network Layer*, Ανακτήθηκε από http://pdos.csail.mit.edu/papers/tarzan:ccs9/tarzan:ccs9.pdf

[27] Freedman M. J., Sit E., Cates J. & Morris R., *Introducing Tarzan, a Peer-to-Peer Anonymizing Network Layer*, MIT Laboratory for Computer Science, Ανακτήθηκε από http://www.cs.rice.edu/Conferences/IPTPS02/182.pdf

[28] Gabber E., Gibbons P.B., Kristol D. M., Matias Y. & Mayer A. (1999), *Consistent yet Anonymous Web Access with LPWA*, Communication of the ACM, special section on Internet Privacy,.

[29] Global Finance, *Internet Users by Country*, Ανακτήθηκε από http://www.gfmag.com/tools/global-database/ne-data/11942-internet-users.html#axzz2ZnyRvdjr

[30] Goel S., Robson M., Polte M. & Gun Sirer E., *Herbivore: A Scalable and Efficient Protocol for Anonymous Communication*, Ανακτήθηκε από http://www.cs.cornell.edu/people/egs/papers/herbivore-tr.pdf

[31] Hazel S. & Wiley B. (2002), *Achord: A Variant of the Chord Lookup Service for Use in Censorship Resistant Peer-to-Peer Publishing Systems*, Proceedings of the First Workshop on Peer-to-Peer Systems, Cambridge, MA.

[32] Herdegard J., Steinmeyer S. & Zhang W., *Anonymity and Privacy in the Internet*, Ανακτήθηκε από http://www.it.uu.se/edu/course/homepage/sakdat/ht05/assignments/pm/programme/Anonymity and Privacy in the Internet.pdf

[33] Herrmann M. & Grothoff C., *Privacy-Implications of Performance-Based Peer Selection by Onion-Routers: A Real-World Case Study using I2P*, Technische Universitat Munchen, Ανακτήθηκε από http://grothoff.org/christian/i2p.pdf

[34] Lindskog H. & Lindskog S. (2003), *Web Site Privacy with P3P*, Wiley Publishing Inc.,

[35] London Economics (2010 July), *Study on the Economic Benefits of Privacy-Enhancing Technologies (PETs)*, Final Report to the European Commission, DG Justice, Freedom and Security.

[36] Manda D. R. (2007 January), *A Study on Anonymous P2P Networks and their Vulnerabilities*, Digital Media Lab, Department of Applied Physics and Electronics, Umea University, Sweden.

[37] METAgroup (2005 March), *Privacy Enhancing Technologies*, META Group Report v 1.1.

[38] Mislove A., Oberoi G., Post A., Reis C., Druschel P. & Wallach D. S., *AP3: Cooperative, Decentralized Anonymous Communication,* Ανακτήθηκε από http://www.cs.rice.edu/~druschel/publications/AP3-EW.pdf

[39] OECD, *Privacy Principles*, 1980, Ανακτήθηκε από http://oecdprivacy.org/

[40] Rahma A. M. S., Farhan R. N. & Mohammad H. J. (2011), Developed Protocol for Key Exchange Based on Irreducible Polynomial, *Journal of University of Anbar for Pure Science*, Vol. 5, No 3.

[41] Reiter M. K. & Rubin A. D., *Crowds: Anonymity for Web Transactions*, Ανακτήθηκε από http://avirubin.com/crowds.pdf

[42] Rennhard M. (2004), *MorphMix – A Peer-to-Peer based System for Anonymous Internet Access*, Swiss Federal Institute of Technology, Zurich, Dissertation, Ανακτήθηκε από https://home.zhaw.ch/~rer/publications/PhDMorphMix.pdf

[43] Rennhard M. (2003 May), *Anonymous Internet Access for the Masses with MorphMix*, Swiss Federal Institute of Technology, Technical Report TIK-Nr 159, Ανακτήθηκε από https://home.zhaw.ch/~rer/publications/morphmix_tr2.pdf

[44] Rennhard M. & Plattner B. (2002), *Introducing MorphMix: Peer-to-Peer based Anonymous Internet Usage with Collusion Detection*, Ανακτήθηκε από http://freehaven.net/anonbib/cache/morphmix:wpes2002.pdf

[45] Rennhard M. & Plattner B. (2004), *Practical Anonymity for the Masses with MorphMix*, Swiss Federal Institute of Technology, Ανακτήθηκε από https://gnunet.org/sites/default/files/morphmix-fc2004.pdf

[46] Saini A., *Super-peer Architectures for Distributed Computing*, Ανακτήθηκε από http://www.fiorano.com/whitepapers/superpeer.pdf

[47] Schott S. (2007), *Tarzan: Techniques of a Peer-to-Peer Anonymizing Network Layer with Security Analysis from a more Recent Perspective*, Ανακτήθηκε από http://archive.cone.informatik.uni-freiburg.de/teaching/seminar/p2p-networks-w06/submissions/Tarzan.pdf

[48] Sherwood R., Bhattacharjee B. & Srinivasan A., *P^5: A Protocol for Scalable Anonymous Communication*, Ανακτήθηκε από http://www.cs.umd.edu/projects/p5/p5.pdf

[49] Shields C. & Levine B.N. (2000), *A Protocol for Anonymous Communication over the Internet*, Ανακτήθηκε από http://www.cs.ucsb.edu/~ravenben/classes/595n-s07/papers/hordes-ccs00.pdf

[50] Solove D.J. (2006 January), A Taxonomy of Privacy, *University of Pennsylvania Law Review*, Vol. 154, No. 3.

[51] Stoica I., Morris R., Karger D., Kaashoek M. F. & Balakrishnan H. (2001), *Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications*, Proceedings of the ACM SIGCOMM '01 Conference, San Diego, California.

[52] Van Blarkom G.W., Borking J.J. & Olk J.G.E. (eds) (2003), *Handbook of Privacy and Privacy-Enhancing Technologies: The Case of Intelligent Software Agents*, PISA Consortium, The Hague.

[53] Warren S. D. & Brandeis L.D. (1890 December), The Right to Privacy, *Harvard Law Review*, Vol 4, No 5.

[54] Westin A. F. (2003), Social and Political Dimensions of Privacy, *Journal of Social Issues*, Vol 59, No 2.

Διαδικτυακές πηγές

[55] http://anon.inf.tu-dresden.de/index_en.html

[56] http://en.wikipedia.org/wiki/Mixminion

[57] http://en.wikipedia.org/wiki/Traffic_analysis

[58] http://en.wikipedia.org/wiki/TRUSTe

[59] http://mixminion.net/manpages/mixminion.1.txt

[60] https://www.torproject.org/

[61] http://www.truste.com/

[62] https://www.anonymizer.com/

[63] http://www.i2p2.de/

[64] http://www.w3.org/P3P/

[65] http://www.w3.org/P3P/p3pfaq

[66] http://en.wikipedia.org/wiki/P3P

[67] http://www.oreillynet.com/network/excerpt/p3p/p3p.html