ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ
ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΧΑΡΑΛΑΜΠΟΣ Α. ΛΕΟΝΤΙΔΗΣ

Διάχυση και συλλογή πληροφορίας ως μέθοδος κοινωνικής μηχανικής, με χρήση τηλεπικοινωνιακών δικτύων

Επιβλέπων: Ευστάθιος Συκάς

Καθηγητής Ε.Μ.Π

Αθήνα, 25 Σεπτεμβρίου 2018

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ
ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΧΑΡΑΛΑΜΠΟΣ Α. ΛΕΟΝΤΙΔΗΣ

Διάχυση και συλλογή πληροφορίας ως μέθοδος κοινωνικής μηχανικής, με χρήση τηλεπικοινωνιακών δικτύων

Επιβλέπων : Ευστάθιος Συκάς
Καθηγητής Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 20η Σεπτεμβρίου 2018.Αθήνα, Σεπτέμβριος 2018

.....	.....	.....
Ευστάθιος Συκάς	Μιλτιάδης Αναγνώστου	Γεώργιος Στασινόπουλος
Καθηγητής Ε.Μ.Π	Καθηγητής Ε.Μ.Π	Καθηγητής Ε.Μ.Π

Αθήνα, Σεπτέμβριος 2018

.....

ΧΑΡΑΛΑΜΠΟΣ Α. ΛΕΟΝΤΙΔΗΣ

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

Ευχαριστίες

Θέλω να ευχαριστήσω αρχικά θερμά τον κ. Συκά για την βοήθειά του στην εκπόνηση της διπλωματικής και ακόμα τους κυρίους Αναγνώστου και Θεολόγου που διέθεσαν τον χρόνο τους ως μέλη της τριμελούς επιτροπής.

Ακόμα ευχαριστώ τον Δρ. Δ. Ξενικό, ΣΕΜΦΕ ΕΜΠ, που με έβαλε στον κόσμο των δικτύων και με βοήθησε να κατανοήσω έννοιες και φαινόμενα. Δίχως την καθοδήγηση και τις συμβουλές του δεν θα είχε ολοκληρωθεί αυτή η εργασία.

Ακόμα θέλω να ευχαριστήσω όσους προσέφεραν τις συμβουλές τους και την βοήθειά τους, την οικογένειά μου που με βοήθησε σε περιόδους φόρτου εργασίας και την Χρύσα που έκανε τον χρόνο ελαφρύτερο.

Τέλος να ευχαριστήσω την Ισπανίδα καθηγήτρια πληροφορικής P. R, της οποίας το κοινωνικό δίκτυο αποδείχθηκε εξαιρετικό δείγμα μελέτης.

Περίληψη

Είναι αστείρευτη πλέον η πληροφορία που κινείται στα μέσα κοινωνικής δικτύωσης. Το γεγονός αυτό παρέχει μεγάλες δυνατότητες για οργανισμούς που μπορούν να την αξιοποιήσουν αλλά εγκυμονεί και κινδύνους για τους χρήστες των μέσων.

Σκοπός αυτής της εργασίας είναι η αποτύπωση και μελέτη του δικτύου επαφών ενός ατόμου στα μέσα κοινωνικής δικτύωσης. Συντίθενται τα δίκτυα των επαφών του facebook, του LinkedIn και του twitter σε ένα γράφο όπου κάθε κόμβος μπορεί να είναι φίλος του ατόμου σε ένα, δύο ή και στα τρία αυτά μέσα. Για την υλοποίηση του γράφου αυτού επιλέχθηκε ένα άτομο με μόνο κριτήριο να είναι παρόν και στους τρεις χώρους του διαδικτύου. Μετά την σύνθεση του δικτύου, ακολούθησε η ανάλυσή του, υπό το πρίσμα της επίθεσης spear phishing. Ερευνήθηκε δηλαδή από ποιον κόμβο του δικτύου αν εκκινηθεί η επίθεση, είναι πιο πιθανό για το θύμα να ενδώσει. Τα αποτελέσματα της έρευνας τονίζουν τον κίνδυνο μιας τέτοιας επίθεσης και την ευκολία με την οποία μπορεί να διεξαχθεί. Η περίπτωση της επίθεσης spear phishing ωστόσο έχει επιλεχθεί προς μελέτη ως μία απαιτητική διαδικασία που οι ανάγκες της είναι εξαιρετικά κοντά σε αυτές άλλων διαδικασιών, που αντλούν υλικό από τα μέσα κοινωνικής δικτύωσης. Τέτοιες είναι μία διαφημιστική καμπάνια, μία προεκλογική εκστρατεία και άλλες.

Λέξεις κλειδιά:

Κοινωνικά δίκτυα, ανάλυση δικτύου, spear phishing, phishing, επίθεση κοινωνικής μηχανικής, κοινωνική μηχανική, facebook, twitter, LinkedIn, ηλεκτρονικό ταχυδρομείο

Abstract

The information flowing throw the social media is endless. This fact offers great opportunities to the institutions able to handle it. But the exploitation of this information also encloses hidden dangers to the users of these media.

The goal of this research is the construction and study of the network of contacts of a person in the social media. The networks of its contacts in facebook, twitter and LinkedIn are composed in one graph, where every node can be friend of the person in one, two or all three social media. For the production of this graph, a person was chosen with only criteria its existence in all three of the social media mentioned. After the construction of the network started its analysis on the prism of a spear phishing attack. The object was finding from which node of the network a spear phishing attack would have greater possibility to succeed. The results of the research mention the dangers of a possible attack of this type and the easiness of organizing it through the social media. The spear phishing attack though was chosen as a study case because it is a demanding procedure, which needs are close to the needs of other procedures also exploiting the information in social media. Such procedures are marketing, political and other campaigns.

Key words:

Social media, network analysis, spear phishing, phishing, social engineering, social engineering attack, mail, facebook, twitter, LinkedIn

Περιεχόμενα

Σχήματα και Γραφήματα

Κεφάλαιο 1.

Κεφάλαιο 2.

Κεφάλαιο 3.

Παράρτημα 2.

Πίνακες

Κεφάλαιο 1.

Κεφάλαιο 3.

1. Ορίζοντας το Social Engineering

Το social engineering (SE) είναι ένας σημαντικός κλάδος του information security. Η πρώτη βιβλιογραφική αναφορά σε αυτό έγινε το 1987 (Quann, Belford, 1987). Σύμφωνα με αυτό, το SE, από την πρώτη στιγμή της γέννησης του, θεωρείται ως απόπειρα εκμετάλλευσης των βοηθητικών παροχών και των υπηρεσιών υποστήριξης που συνήθως συνδέονται με υπολογιστικά συστήματα. Το SE, αργότερα περιγράφεται ως «τέχνασμα και απάτη, γνωστό και ως social engineering» (Kluepfel, 1989) και (Kluepfel, 1991). Ακόμα και σε ένα από τα πιο ευρέως γνωστά περιοδικά γύρω από το hacking, το «2006:The Hacker Quarterly», ο όρος Social engineering δεν αναφέρεται ευρέως. Ένα από τα άρθρα του με τίτλο «Janitor privileges», εξηγεί με λεπτομέρεια πώς γίνεται μια επίθεση SE, παρ' όλα αυτά ο όρος δεν αναφέρεται ποτέ στο κείμενο. Στο διάστημα από το 1995 ως το 2013, πολλοί ορισμοί έχουν δοθεί. Ισάριθμο πλήθος αναφέρεται στο SE ως επιστήμη, ως τεχνική ή ως μέθοδο απάτης και χειρισμού.

Ένα καλός ορισμός του social engineering θα μπορούσε να είναι ο εξής: Η επιστήμη της χρήσης της κοινωνικής αλληλεπίδρασης ως μέσο πειθούς ενός ατόμου ή οργανισμού, προκειμένου αυτό να συναινέσει (Venter et al., 2014) σε ένα συγκεκριμένο αίτημα ενός επιτιθέμενου, όπου είτε η κοινωνική αλληλεπίδραση, είτε η μέθοδος πειθούς, είτε το αίτημα εμπλέκει κάποια μονάδα σχετιζόμενη με κάποιον υπολογιστή.

Το SE εφαρμόζεται για να εξυπηρετήσει δύο διακριτές σκοπιμότητες, η πρώτη είναι η προπαγάνδα και η δεύτερη η απάτη. Η πρώτη εξυπηρετείται από τεχνικές και δραστηριότητες στα μέσα κοινωνικής δικτύωσης. Η δεύτερη ικανοποιείται μέσω της επίθεσης SE. Οι δύο αυτές μέθοδοι μπορεί να αλληλοσυμπληρώνονται, καθώς δεν είναι λίγες οι περιπτώσεις όπου μία επίθεση SE διεξάγεται για τη συλλογή εμπιστευτικών δεδομένων γύρω από κάποιο πρόσωπο, προκειμένου, στη συνέχεια, να εκκινηθεί μία εκστρατεία προπαγάνδας εναντίον του.

1.1 Social engineering ως μέθοδος προπαγάνδας

Το SE αποτελεί την κατεξοχήν τεχνική προπαγάνδας στα μέσα κοινωνικής δικτύωσης. Τα μέσα κοινωνικής δικτύωσης ακόμα, αποτελούν έναν χώρο μεγάλης σώρευσης πληθυσμού από όλες τις κοινωνικές ομάδες. Στις ΗΠΑ για παράδειγμα, 81% του πληθυσμού έχει τουλάχιστον ένα λογαριασμό σε κάποιο μέσο δικτύωσης. Στον χώρο αυτό, ο πληθυσμός συμπυκνώνεται σε μεγάλο βαθμό καθώς καταργείται ο παράγοντας της χωρικής απόστασης. Μέσω της δικτυακής δομής του χώρου, μπορεί η πληροφορία να διατρέξει πολύ μεγάλο αριθμό κόμβων με μικρό πλήθος αναμεταδόσεων. Καθίστανται έτσι τα social media, ιδανικό πεδίο για τη διασπορά πληροφορίας, με οποιοδήποτε σκοπό κι αν αυτή επιτελείται, για λόγους πολιτικής προπαγάνδας ή διαφήμισης (marketing). Χαρακτηριστικό είναι το γεγονός ότι 88% των επιχειρήσεων στις ΗΠΑ χρησιμοποιούν τα μέσα δικτύωσης για τη διαφήμισή τους.

Η πολιτική προπαγάνδα έχει κάθε λόγο να στραφεί σε αυτό το ισχυρό μέσο επικοινωνίας με το αντικείμενό της, καθώς η δύναμη γεννιέται από τη δημιουργία συμβολισμών στο ανθρώπινο μυαλό μέσω των διαδικασιών επικοινωνίας. Σύμφωνα με τον M. Castells (Castells, 2009), το τι σκέφτεται ο κόσμος για την κυβέρνηση και πώς αυτή συνδέεται με την κουλτούρα του τόπου και την οικονομία, καθορίζει το ποιος θα μπορεί να ασκεί την εξουσία και πώς θα μπορεί να το κάνει. Για την αποτελεσματική άσκηση της πολιτικής βίας επίσης χρειάζεται η κατευθυνόμενη διαμόρφωση της ατομικής και συλλογικής συνείδησης. Για παράδειγμα για να διεξαχθεί ο πόλεμος του Ιράκ, παρουσιάστηκε στον αμερικανικό λαό μέσω της προπαγάνδας ως ένας πόλεμος εναντίον της τρομοκρατίας. Η βία και η απειλή της βίας πάντα συνδυάζονται με την κατασκευή συμβολισμών προκειμένου να δημιουργούνται και να αναπαράγονται σχέσεις εξουσίας σε όλους τους τομείς της καθημερινής ζωής. Το κοινό στοιχείο όλων των διαδικασιών δημιουργίας συμβολισμών, είναι ότι αυτές εξαρτώνται από τα μηνύματα και τα πλαίσια που διαμορφώνονται και διαδίδονται από τα μέσα επικοινωνίας. Και παρ' όλο που κάθε άτομο σημασιοδοτεί με δικό του τρόπο κάθε μήνυμα που προσλαμβάνει, η απόδοση νοήματος μπορεί να καθοδηγηθεί από το περιβάλλον της

επικοινωνίας. Μπορούμε να πούμε λοιπόν ότι εφόσον οι συσχετισμοί δυνάμεων διαμορφώνονται διαρκώς στο μυαλό του ανθρώπου ως αποτέλεσμα της δημιουργίας συμβολισμών και σημείων, και δεδομένου ότι η δημιουργία αυτή εξαρτάται κυρίως από τη ροή πληροφορίας και τις εικόνες των δικτύων επικοινωνίας, η εξουσία προέρχεται από τα δίκτυα επικοινωνίας και όσους παράγοντες σχετίζονται με τον έλεγχό τους.

Όσον αφορά την πολιτική, ο Baudrillard (Baudrillard, 1996), γράφει πως η πολιτική βία επίσης είναι κι αυτή μια μορφή επικοινωνίας που επιδρά στο μυαλό μέσω εικόνων με στόχο τον εκφοβισμό. Την ίδια τακτική ακολουθεί και η τρομοκρατία. Η τελευταία μέσω της δημιουργίας φαντασμαγορικών εικόνων τυχαίας καταστροφής, εγκαθιδρύει ένα κλίμα μόνιμης ανασφάλειας. Παράλληλα η διάδοση των εικόνων σε εξωφρενικό ρυθμό και ποσότητα εξυπηρετεί μία ακόμα λειτουργία: η είδηση και η σημασία της δεν παλιώνει και δεν εξαφανίζεται από τη φυσική φθορά της αλλά από την ανεξέλεγκτη διασπορά. Η άμετρη αναπαραγωγή του νέου και της εικόνας του, το απελευθερώνει από την έννοια και την ουσία του. Έτσι μια είδηση μπορεί να χάσει την σημασία της ταχύτατα μετά τη γέννησή της και πλέον το μόνο περιεχόμενό της να είναι η πληροφόρηση ως συμβάν. Έτσι τα μέσα δικτύωσης ως μέσα διάδοσης και διασποράς των εικόνων γίνονται όχημα της κουλτούρας του φόβου στην πρώτη περίπτωση και διαλύουν το περιεχόμενο της ενημέρωσης στην δεύτερη.

Οι τεχνικές που χρησιμοποιεί το social engineering για να προπαγανδίσει μέσω των social media μπορεί να είναι είτε αυτοματοποιημένες είτε να κινούνται από ανθρώπινες ενέργειες. Οι τρεις κυριότερες από αυτές είναι τα bots, trolls και fake news.

1.1.1 Bots

Είναι αυτοματοποιημένα accounts που δρουν βάσει κάποιου αλγορίθμου και έχουν πολλών ειδών δράσεις στα social media. Τα bots μπορεί να σχηματίσουν ένα δίκτυο πλασματικών accounts που συνδέονται μεταξύ τους (follow, φίλοι κλπ), προκειμένου να είναι πιο αληθοφανές το κάθε προφίλ. Χρησιμοποιούνται για να προωθούν κάποιες αναρτήσεις. Το facebook καταργεί χιλιάδες τέτοια προφίλ κάθε εβδομάδα. Υπάρχουν περιπτώσεις που κάποια τέτοια προφίλ μπορεί να αντιστοιχούν και σε υπαρκτά πρόσωπα, οι επιθέσεις τέτοιου τύπου ονομάζονται σιβυλλικές (Sybil).

Οι επιθέσεις αυτού του τύπου μπορούν και αυτοματοποιούνται με τη συλλογή δεδομένων από τα κοινωνικά δίκτυα στα οποία συμμετέχει το άτομο που στοχεύει η επίθεση και την κλωνοποίηση του δικτύου επαφών του προφίλ του στόχου. Δηλαδή κατασκευάζονται και περιφερειακά προφίλ τα οποία έχει ως φίλους ή ακολουθεί το προφίλ κλώνος. Στην πλειοψηφία των περιπτώσεων, ο χρήστης έχει και αληθινό προφίλ. Στις περιπτώσεις αυτές, οι ενημερώσεις ανακατευθύνονται και στο ψεύτικο για να προσδώσουν κι άλλη αληθοφάνεια. Οι στόχοι μπορεί να είναι πολιτικοί παράγοντες, δημοσιογράφοι και επιστήμονες.

1.1.2 Trolls:

Είναι είτε αυτοματοποιημένα είτε χειριζόμενα από ανθρώπους προφίλ, τα οποία χρησιμοποιούνται για να προκαλέσουν χάος και σύγχυση στα social media σε κρίσιμες περιόδους. Μία από τις περιπτώσεις στις οποίες έχουν εφαρμοστεί ευρέως, σύμφωνα με έρευνα του oxford university (Sanovich, 2017), (Bolsover, 2017), είναι οι εκλογικές περίοδοι των τελευταίων χρόνων σε χώρες όπως η Ρωσία και η Κίνα, όπου έχουν χρησιμοποιηθεί για να επαναδημοσιεύσουν αναρτήσεις και ειδήσεις που ανέβηκαν πριν την εκλογική περίοδο, προκαλώντας σύγχυση στο κοινό. Στην Κίνα τα περισσότερα άτομα που δουλεύουν ως trolls είναι υπάλληλοι της κυβέρνησης,

ενώ στην Ρωσία πληρώνονται ένα μικρό ποσό για κάθε δημοσίευση που κάνουν.

Επίσης άλλη περίπτωση χρήσης τους είναι η κοινοποίηση προσωπικών δεδομένων για πρόσωπα των οποίων τα email έχουν παραβιαστεί με σκοπό τη διαπόμπευσή τους. (πχ Ρωσία 2012 υπόθεση του Medvedev).

Η έρευνα πάνω στην βελτιστοποίηση των trolls υπαγορεύει πως ο στόχος δεν είναι απλώς το πλήθος των reposts και retweets. Είναι η σωστή διαχείριση των αποτελεσμάτων αναζήτησης και η αξιολόγηση των πιο δημοφιλών αναρτήσεων, με στόχο τη σύγκρουση μεταξύ των χρηστών και όχι μόνο τον αριθμό των views. Επίσης ακόμα και η δημιουργία του περιεχομένου της ανάρτησης καθοδηγείται από αλγορίθμους βελτιστοποίησης βάσει των αποτελεσμάτων αναζήτησης. Το βάρος που δίνεται στη δημοτικότητα της εικόνας, δεν είναι λιγότερο σοβαρό από το πολιτικό μήνυμα που περιέχει. Αυτό το κοινωνικό φαινόμενο έχει λειτουργήσει ως αφορμή για να χρησιμοποιούνται μέσα κενά πολιτικού περιεχομένου ώστε να τραβήξουν το κοινό στο μέσο προπαγάνδας. Αυτά μπορεί να αποτελούν οτιδήποτε έχει την τάση να γίνεται δημοφιλές (πχ βίντεο με γάτες).

Τα bots σε πολλές περιπτώσεις συνεργάζονται με τα trolls για να διαδίδουν τις αναρτήσεις που κοινοποιούν τα τελευταία, κάνοντας αποτελεσματικότερη την προπαγάνδα. Επιπλέον, σε περιπτώσεις όπου το κοινό των μέσων δικτύωσης έχει ψηλό μορφωτικό επίπεδο, ο στόχος δεν είναι η συζήτηση αλλά ο αποκλεισμός και η άσκηση πολεμικής. Τα bots τότε αποδεικνύονται πολύ αποτελεσματικά λόγω της φύσης των εύκολα κλιμακούμενων επιθέσεών τους.

1.1.3 Fake news:

Όπως παρουσιάζονται από το “The Fake News Machine” (Gu et al., 2017), είναι η περίπτωση διάδοσης πλαστών ειδήσεων και πληροφοριών στα social media. Είναι πλέον ξεκάθαρο πως δεν υπάρχει διαχωρισμός του υλικού κόσμου από τον διαδικτυακό. Ό,τι συμβαίνει στο διαδίκτυο επηρεάζει άμεσα

τις κοινωνικοπολιτικές εξελίξεις. Όταν συνδυάζεται η δύναμη δικτύωσης που προσφέρουν τα social media και οι θεωρίες περί χειραγώγησης της κοινής γνώμης, μια νέα παράμετρος παρουσιάζεται στις πολιτικές καμπάνιες και στην προβολή του δημοσίου προφίλ εταιριών και προσώπων. Η παράμετρος αυτή είναι τα fake news, τα οποία έχουν τρία συνθετικά συστατικά που με την απουσία ενός από αυτά δεν μπορούν να λειτουργήσουν αποτελεσματικά: τα social media (χρήστες), τις online υπηρεσίες των social media (bots, trolls, διαφήμιση) και την ύπαρξη στόχου και κίνητρου. Ο στόχος των fake news είναι πάντα το γενικό κοινό. Η ελπίδα για την δημιουργία άμυνας απέναντι στις πλαστές ειδήσεις έγκειται μόνο στην ανάπτυξη της κριτικής σκέψης και στην κατανόηση των τεχνικών που χρησιμοποιούνται για την χειραγώγηση.

1.2 Social engineering ως μέθοδος απάτης

Το SE πολύ πριν αναπτυχθεί το περιβάλλον των μέσων κοινωνικής δικτύωσης, έκανε την εμφάνισή του στον τομέα του hacking και της ασφάλειας δεδομένων. Το SE χαρακτηρίστηκε ως τεχνική απάτης που αποσκοπεί στον έλεγχο του ανθρωπίνου παράγοντα ασφάλειας (Kevin Mitnick: “The art of deception: controlling the human element of security” (Mitnick, 2002)). Η μέθοδός του είναι η επίθεση κοινωνικής μηχανής (SE attack) η οποία εφαρμόζεται από έναν ή ένα σύνολο Social Engineers σε έναν στόχο για κάποιον σκοπό, που συνήθως είναι είτε το οικονομικό όφελος, είτε η πρόσβαση σε εμπιστευτικές πληροφορίες, είτε η διακοπή κάποιας υπηρεσίας. Η επίθεση έχει έναν αριθμό μέσων, δια μέσω των οποίων διεξάγεται. Αυτά μπορεί συνήθως να είναι κάποιοι δίαυλοι επικοινωνίας όπως το ηλεκτρονικό ταχυδρομείο ή το τηλέφωνο ή κάποια μορφή μονομερούς επικοινωνίας όπως ένα διαφημιστικό φυλλάδιο ή μία ιστοσελίδα. Τέλος μία επίθεση SE βασίζεται σε ορισμένες αρχές συγκατάθεσης του θύματος (compliance principles) σύμφωνα με τις οποίες, αυτό θα ακολουθήσει κάποια προδιαγεγραμμένη συμπεριφορά ως απάντηση σε συγκεκριμένα ερεθίσματα.

Η επίθεση SE, μπορεί να ταξινομηθεί σε δύο μεγάλες κατηγορίες: Την έμμεση και την άμεση επίθεση (Venter et al., 2014).

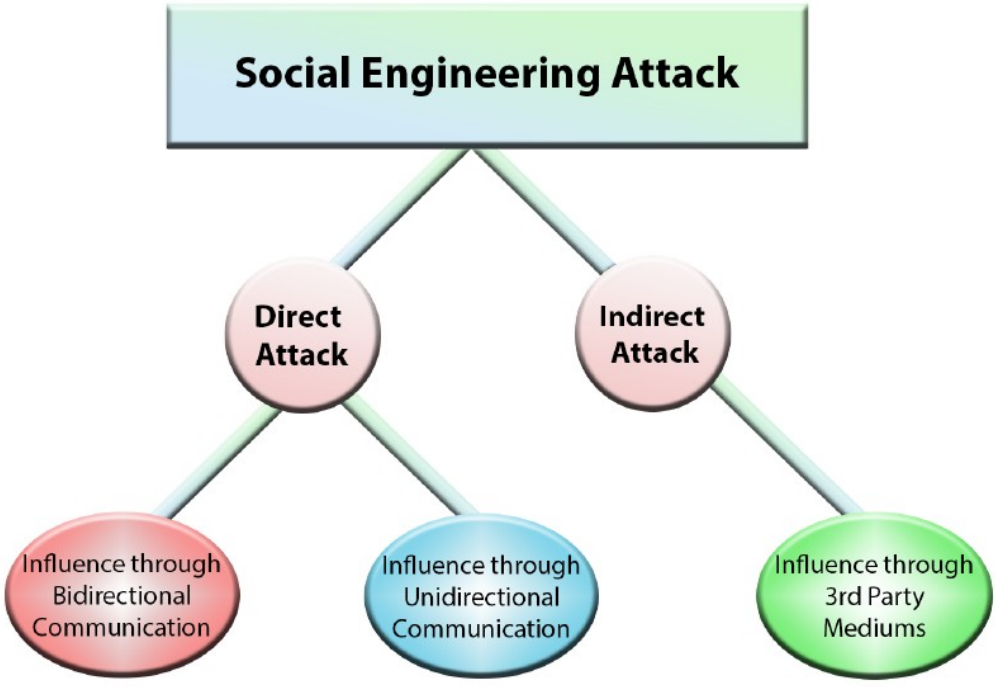
- Μια έμμεση επίθεση αναφέρεται σε ένα περιστατικό όπου ένα τρίτο μέσο χρησιμοποιείται ως μέθοδος επικοινωνίας. Ένα τρίτο μέσο θα μπορούσε να είναι συνήθως κάποιο flash disc, κάποιο cd-rom ή άλλα μέσα όπως μία ιστοσελίδα. Η επικοινωνία πραγματοποιείται με τη χρήση κάποιου τρίτου μέσου όταν αυτό είναι προσβάσιμο από τον στόχο, χωρίς να απαιτείται άμεση αλληλεπίδραση με τον social engineer.
    - Η έμμεση επικοινωνία ορίζεται ως επικοινωνία μέσω κάποιου επικοινωνιακού εργαλείου. Ο social engineer αλλά και ο στόχος μπορεί να είναι είτε ένα άτομο, μια ομάδα ατόμων ή ένας οργανισμός. Τα μέσα που χρησιμοποιούνται συχνά για έμμεση επικοινωνία είναι φυλλάδια, μονάδες flash disc και ιστοσελίδες. Κάθε τεχνική και στόχος μπορεί να συνδυαστεί με την έμμεση επικοινωνία. Ένα παράδειγμα μιας επίθεσης SE που χρησιμοποιεί έμμεση επικοινωνία είναι όταν ένας social engineer εγκαταλείπει ένα μολυσμένο flash disk σε μια επιλεγμένη τοποθεσία με την πρόθεση να συλλεχθεί από τον στόχο. Σε αυτό το παράδειγμα, ο social engineer, καθώς και ο στόχος, είναι άτομα. Η τεχνική που χρησιμοποιείται για αυτή την επίθεση είναι γνωστή ως δόλωμα (baiting), επειδή ένα φυσικό αντικείμενο αφήνεται σε σημείο φανερό από το στόχο.

- Μία άμεση επίθεση αποτελεί ένα περιστατικό στο οποίο δύο ή περισσότερα άτομα εμπλέκονται σε μία άμεση συζήτηση. Αυτή μπορεί να είναι μονομερής ή όχι. Λόγω αυτού, αυτού του είδους η επίθεση κατηγοριοποιείται περαιτέρω ως αμφίδρομη και μονόδρομη.

- Αμφίδρομη είναι η επικοινωνία όταν δύο ή περισσότερα μέλη παίρνουν μέρος σε αυτήν. Κάθε μέρος μπορεί να αποτελείται από ένα μεμονωμένο άτομο, ένα σύνολο ατόμων ή έναν οργανισμό. Ένα σύνηθες παράδειγμα επίθεσης αυτού του τύπου είναι η υπόδηση από τον επιτιθέμενο του ρόλου του θύματος με στόχο αυτός να αποκτήσει πρόσβαση σε κάτι στο οποίο το πραγματικό θύμα ήδη έχει. Η αμφίδρομη επικοινωνία ορίζεται ως μία συζήτηση ανάμεσα σε δύο άτομα. Σε αυτήν, ο social engineer μπορεί να είναι είτε μεμονωμένο άτομο είτε σύνολο ατόμων είτε οργανισμός. Ο στόχος της επίθεσης μπορεί να είναι επίσης άτομο ή οργανισμός. Τα μέσα που συνήθως χρησιμοποιούνται σε μία αμφίδρομη επικοινωνία, είναι το e-mail και οι συζητήσεις πρόσωπο με πρόσωπο ή μέσω τηλεφώνου. Κάθε τεχνική και στόχος μπορεί να συνδυαστεί με ένα μέσο αμφίδρομης επικοινωνίας. Ένα τέτοιο μέσο είναι phishing e-mail που φαίνεται πως προέρχεται από όπου ο στόχος κάποιο διαδικτυακό κατάστημα από όπου έχει κάνει κάποια παραγγελία το θύμα. Το mail είναι καμουφλαρισμένο ως ένα μήνυμα από το κατάστημα και τον πληροφορεί πως υπάρχει κάποια προσφορά διαθέσιμη σχετικά με την παραγγελία του. Ο στόχος αναγνωρίζει το σύνδεση ανάμεσα στο μήνυμα και την παραγγελία και κάνει κλικ στο σύνδεσμο. Ο στόχος επιλέγεται προσεχτικά. Το phishing χρησιμοποιεί στη συγκεκριμένη περίπτωση την αρχή της σπανιότητας (scarcity). Εφόσον το μήνυμα ισχυρίζεται ότι πρόκειται για μια περιορισμένη προσφορά, ο στόχος νιώθει πως πρέπει να ερευνήσει την περιορισμένη του ευκαιρία πριν αυτή πάψει να είναι διαθέσιμη.

- Μονόδρομη είναι η επικοινωνία στην οποία ο social engineer επικοινωνεί με τον στόχο αλλά ο στόχος δεν έχει κάποιο τρόπο με τον οποίο να μπορεί να επικοινωνήσει με τον social engineer. Αυτό συνήθως συμβαίνει μέσω κάποιου μέσου επικοινωνίας όπως μαζικά e-mail ή μηνύματα SMS. Ένα τέτοιο παράδειγμα αποτελούν τα e-mails που ανήκουν στην κατηγορία της

επίθεσης phishing. Η μονόδρομη επικοινωνία είναι πολύ παρόμοια με την αμφίδρομη, με τη διαφορά πως ο διάλογος διεξάγεται μόνο προς μία κατεύθυνση: από τον social engineer προς τον στόχο. Ο social engineer και ο στόχος μπορούν να είναι μεμονωμένα άτομα, σύνολα ατόμων ή οργανισμοί. Τα μέσα που χρησιμοποιούνται είναι συνήθως e-mails, sms ή γράμματα ταχυδρομείου. Κάθε τεχνική και στόχος μπορεί να συνδυαστεί με ένα μέσο μονόδρομης επικοινωνίας. Ένα παράδειγμα μίας επίθεσης SE η οποία χρησιμοποιεί μονόδρομη επικοινωνία είναι ένα flash disk με το οποίο ο engineer αποκτάει πρόσβαση στον υπολογιστή του στόχου.



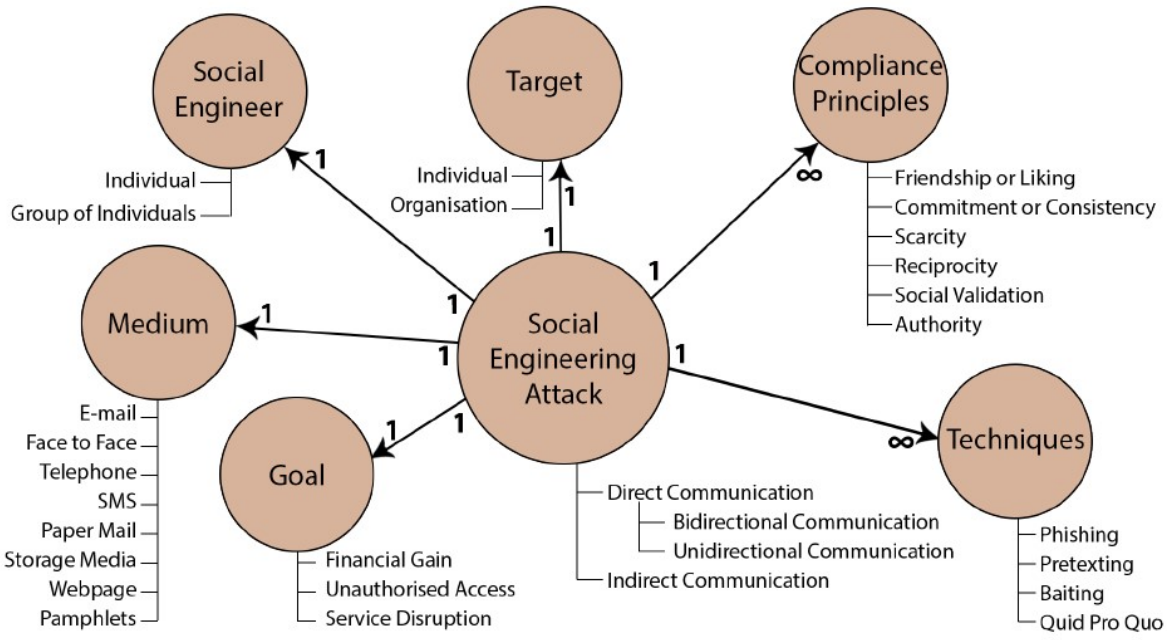
Σχήμα 1. Ταξινόμηση της επίθεση κοινωνικής μηχανής (Venter et al., 2014).

1.3 Οντολογία

Ορίζουμε μία επίθεση SE να έχει:

- ένα Social Engineer,
- ένα στόχο,
- μία ή περισσότερες αρχές συγκατάθεσης,
- μία ή περισσότερες τεχνικές,
- ένα μέσο,.

Συνθέτοντας τη θεωρία από τη βιβλιογραφία του μάρκετινγκ σχετικά με την εξήγηση της συμπεριφοράς των καταναλωτών, διεξήχθη μια εμπειρική μελέτη πεδίου για να διαπιστωθεί αν οι παράγοντες που συντελούν στις επιτυχημένες εκστρατείες μάρκετινγκ μπορούν να συντελέσουν επίσης και σε επιτυχείς επιθέσεις SE (Workman, 2008).



Σχήμα 2. Οντολογικό μοντέλο της επίθεσης κοινωνικής μηχανής (Venter et al., 2014).

Η θεωρία περί της θέσης του δημόσιου πλήθους σε σχέση με την επίγνωση και κατανόηση ενός προβλήματος (situational theory of the publics), ισχυρίζεται ότι ένας πληθυσμός μπορεί να κατακερματιστεί με βάση την ενεργότητα ή την παθητικότητα της επικοινωνιακής του συμπεριφοράς (Aldoory & Dyke, 2006). Οι παράγοντες που διακρίνει αυτή η θεωρία είναι η αναγνώριση προβλημάτων, το επίπεδο ενεργού συμμετοχής και η αναγνώριση των περιορισμών.

- Η αναγνώριση προβλημάτων αντικατοπτρίζει την έκταση στην οποία ένα άτομο αναγνωρίζει ένα πρόβλημα ως σχετικό προς αυτό· το οποίο σημαίνει, πως μία απειλή εκλαμβάνεται ως συμβάν με προσωπικές επιπτώσεις για το άτομο.
- Ο βαθμός της ενεργής συμμετοχής προκύπτει από την κατανόηση του τρόπου με τον οποίο εκλαμβάνεται συναισθηματικά το πρόβλημα. Όπως το κατά πόσο το άτομο εκλαμβάνει ως σοβαρές τις επιπτώσεις της απειλής.
- Η αναγνώριση των περιορισμών αντικατοπτρίζει τον βαθμό στον οποίο οι άνθρωποι αντιλαμβάνονται τις δράσεις τους ως περιορισμένες από παράγοντες πέραν της δύναμής τους.

Σύμφωνα με τον Grunig (Grunig, 1997), εάν αυτοί οι τρεις παράγοντες αντικατοπτρίζουν εξωτερικές συνθήκες, τότε το περιβάλλον πρέπει να αλλάξει προτού να ανταποκριθεί κάποιος. Αλλά εάν είναι αντιληπτοί ως παράμετροι που επηρεάζονται από το ίδιο το άτομο, μπορούν να αλλάξουν με επικοινωνιακή πειθώ. Οπότε η επικοινωνία είναι κεντρικό στοιχείο που επηρεάζει το κατά πόσο και πώς οι άνθρωποι ανταποκρίνονται σε μηνύματα σχετικά με μία απειλή (Petty & Cacioppo, 1986). Μετά από ανασκόπηση της κοινωνικής ψυχολογίας, του management και του security, τρεις ακόμη παράγοντες προκύπτουν: η εμπιστοσύνη (Wang & Emurian, 2005), ο φόβος (Straub & Welke, 1998) και η δέσμευση (Theoharidou et al., 2005). Το ΕΛΜ διακρίνει τις «κεντρικές» από τις «περιφερειακές» οδούς πειθούς, όπου μια κεντρική οδός συνιστά μια διεξοδική ανάλυση του περιεχομένου ενός μηνύματος και μια περιφερειακή είναι μια μορφή πειθούς που δεν ενθαρρύνει

την επεξεργασία (δηλαδή την εκτεταμένη γνωστική ανάλυση) του περιεχομένου των μηνυμάτων. Ο Cialdini (Cialdini, 2001) προσδιόρισε έξι παράγοντες που σχετίζονται με την περιφερειακή οδό: (α) αμοιβαιότητα, (β) συνέπεια, (γ) κοινωνική επιβολή, (δ) αρέσκεια, (ε) εξουσία και (στ) σπανιότητα.

α. Ένα παράδειγμα αμοιβαιότητας είναι το εξής: Όταν κάτι αξίας προσφέρεται, όπως ένα δωρεάν δείγμα, οι άνθρωποι νιώθουν υπόχρεοι να ανταποδώσουν τη χάρη, κάνοντας μία αγορά την οποία αρχικά δεν σκόπευαν (Allen & Meyer, 1990)
β. Η συνέπεια συνεπάγεται θεωρητικά δέσμευση συνέχισης, όπου οι άνθρωποι δεσμεύονται ψυχολογικά σε μια απόφαση που έχουν πάρει (Petty et al., 2002). Μια εκδήλωση της συνέπειας παρατηρείται σε περιπτώσεις όπου κάποιοι άνθρωποι συνεχίζουν να δαπανούν χρήματα για μη προσοδοφόρες επιχειρηματικές δραστηριότητες (Staw, 1981).
γ. Η κοινωνική επιβολή θεωρητικά περιλαμβάνει τη συναισθηματική δέσμευση, όπου οι άνθρωποι ακολουθούν τις συμπεριφορές των ομότιμων μελών της ομάδας, τους ρόλους που τους επιβάλλονται, συμπεριφορές σημαντικών άλλων ατόμων και γενικά την μόδα (Asch, 1946).
δ. Η αρέσκεια ενός ατόμου μπορεί να χρησιμοποιηθεί για την απόκτηση εμπιστοσύνης. Οι άνθρωποι εμπιστεύονται και συμμορφώνονται με αιτήματα από άλλους που βρίσκουν ελκυστικούς ή θεωρούν αξιόπιστους και έχουν ιδιαίτερες δυνατότητες και ικανότητες όπως αθλητές ή ηθοποιούς που τους αρέσουν (Giles & Wiemann, 1987).
ε. Η εξουσία μπορεί να χρησιμοποιηθεί για να προκαλέσει φόβο· οπότε οι άνθρωποι υπακούν σε εντολές για να αποφύγουν αρνητικές συνέπειες όπως η απώλεια προνομίου ή κάποιας αξίας ή ακόμη και από το φόβο τιμωρίας, ταπείνωσης ή καταδίκης (Milgram, 1983).
δ. Η σπανιότητα βασίζεται στην ανταπόκριση στις αντιληπτές ελλείψεις προσδίδοντας μεγαλύτερη ψυχολογική αξία στα σπανιότερα αντικείμενα (Brehm, 1966).

1.4 Μέθοδοι επίθεσης κοινωνικής μηχανής:

- Phishing. Η πιο συχνή μορφή επίθεσης, εκμεταλλεύεται τεχνικές κοινωνικής μηχανής. Οι επιτιθέμενοι χρησιμοποιούν mails, τα social media απευθείας μηνύματα και SMS. Στόχος είναι να εξαπατηθούν τα θύματα και να εξαχθούν από αυτά ευαίσθητες πληροφορίες ή να εγκατασταθεί κακόβουλο λογισμικό στον υπολογιστή τους. Με αυτόν το τύπο επίθεσης θα ασχοληθούμε και θα αναλυθεί στο επόμενο κεφάλαιο.

- Προσποίηση (pretexting): Ο επιτιθέμενος κατασκευάζει ένα σενάριο, ή μία καλή πρόφαση για να προσεγγίσει το θύμα, προσποιούμενος πως είναι κάποιος άλλος. Συνήθως ο επιτιθέμενος υιοθετεί περσόνες που έχει ξαναχρησιμοποιήσει κατά τη διάρκεια της καριέρας του κι έτσι μπορεί να εντοπιστεί. Η επιτυχία της επίθεσης βασίζεται κεντρικά στην ικανότητα του επιτιθέμενου να εγκαθιδρύσει μια σχέση εμπιστοσύνης με το θύμα.

- Επίθεση δολώματος (baiting). Το baiting εκμεταλλεύεται την ανθρώπινη περιέργεια. Συχνά συγχέεται με άλλου τύπου επιθέσεις. Κλασικό παράδειγμα είναι μία επίθεση κατά την οποία ο hacker αφήνει ένα usb stick μολυσμένο με κάποιο κακόβουλο λογισμικό στο parking του οργανισμού που στοχεύει.

- Η επίθεση Quid pro Quo (κάτι για κάτι). Σε αυτή την περίπτωση ο hacker υπόσχεται μία υπηρεσία ή ένα αγαθό σε αντάλλαγμα για πληροφορίες ή πρόσβαση. Η πιο συνήθης επίθεση είναι αυτή στην οποία ο επιτιθέμενος προσποιείται τον τεχνικό μίας μεγάλης επιχείρησης, καλεί τους εργαζόμενους και τους προσφέρει κάποιου είδους αναβάθμιση ή εγκατάσταση λογισμικού (ref. 42).

- Tailgating ή piggybacking. Περιλαμβάνει την πρόσβαση του επιτιθέμενου σε μία απαγορευμένη περιοχή για να συλλέξει

εμπιστευτικές πληροφορίες. Σύνηθες σενάριο είναι αυτό στο οποίο προσποιείται κάποιον υπάλληλο delivery και αιτείται πρόσβασης στον χώρο (ref. 42).

- Watering hole. Αποτελεί την τοποθέτηση κακόβουλου κώδικα στις δημόσιες ιστοσελίδες ενός ιστότοπου τον οποίο συνηθίζουν να επισκέπτονται οι στόχοι. Η τοποθέτηση κακόβουλου κώδικα σε μία σελίδα δεν είναι νέα τακτική και συχνά χρησιμοποιείται από hackers. Όταν ένα θύμα επισκεφτεί την ιστοσελίδα ένας δούρειος ίππος (Trojan) εγκαθίσταται στον υπολογιστή του δίνοντας στον επιτιθέμενο πρόσβαση. Επιθέσεις αυτής της μορφής συχνά χρησιμοποιούνται στην περίπτωση διαδικτυακής κατασκοπείας ή κρατικά επιχορηγούμενων επιθέσεων. Είναι υψηλού κόστους και δύσκολα υλοποιήσιμες γιατί χρειάζονται πολύ σχεδιασμό για την εμφύτευση του κώδικα στη σελίδα και την εκμετάλλευση κάποιου zero-day exploit στον υπολογιστή του θύματος (ref. 42).

1.5 Phishing

Σύμφωνα με τους (Dodge et al., 2007), (Miller, 2005) και (Mitnick & Simon, 2002), τα σενάρια επίθεσης SE μπορούν να λάβουν πολλές μορφές αλλά οι δύο πιο συνηθισμένες και ταχύτερα αναπτυσσόμενες είναι η προσποίηση (pretext) και το phishing. Με το δεύτερο κυρίως θα ασχοληθούμε στην έρευνα αυτή και θα αναλυθεί περαιτέρω παρακάτω.

Με την προσποίηση, ο επιτιθέμενος δημιουργεί ένα σενάριο σχεδιασμένο ώστε να επηρεάσει το θύμα να δώσει ευαίσθητες πληροφορίες, να πληρώσει κάποιο ποσό ή να πραγματοποιήσει κάποια πράξη που θέτει σε κίνδυνο την εμπιστευτικότητα πληροφοριών.

Το phishing είναι μία τεχνική που αποσκοπεί στην απόκτηση ευαίσθητων πληροφοριών από το ενδεχόμενο θύμα μέσω e-mails και ιστοσελίδων ή ταχυδρομικών γραμμάτων που φαίνεται να προέρχονται από κάποια αυθεντική επιχείρηση. Η επιχείρηση αυτή φαίνεται στο μήνυμα να ζητάει από το θύμα συγκεκριμένες πληροφορίες προκειμένου να αποτρέψει έναν λογαριασμό από το να κλείσει, ή σαν μέρος μιας προσφοράς που αποκαλείται gimmie. Ένα τυπικό παράδειγμα είναι ένα μήνυμα ηλεκτρονικού ταχυδρομείου που φαίνεται να προέρχεται από μια τράπεζα και περιέχει αυθεντικά λογότυπα της εταιρείας, ζητώντας από τα δυνητικά θύματα να κάνουν κλικ σε έναν σύνδεσμο που περιέχεται στο ηλεκτρονικό ταχυδρομείο και να ενημερώσουν τα προσωπικά τους δεδομένα σε μια τοποθεσία Web που φαίνεται να είναι νόμιμη επιχείρηση. Σε μια πρόσφατα δημοσιευμένη επίθεση, τα θύματα δέχτηκαν επιστολές με το ταχυδρομείο που παρουσίαζαν το λογότυπο της τράπεζάς τους, η οποία έδωσε εντολή στα θύματα να καλέσουν τον αριθμό τηλεφώνου που παρέχεται στην επιστολή. Στη συνέχεια, ένα διαδραστικό σύστημα φωνητικής εξυπηρέτησης ζήτησε αριθμούς κοινωνικής ασφάλισης, προσωπικούς αριθμούς αναγνώρισης και πληροφορίες επαλήθευσης, συμπεριλαμβανομένης της ημερομηνίας γέννησης και του πατρωνύμου της μητέρας, τα οποία στη συνέχεια χρησιμοποιήθηκαν για την ανάληψη χρημάτων και το άνοιγμα νέων λογαριασμών.

Μία επιτόπια μελέτη που διεξήχθη σε έναν μεγάλο οργανισμό παροχής υπηρεσιών ασφάλισης και χρηματοοικονομικών στις ΗΠΑ, έδειξε ότι υπάρχουν ορισμένοι ψυχολογικοί παράγοντες από τους οποίους εξαρτάται η επιτυχία μιας επίθεσης phishing. Αυτοί είναι (Workman, 2008):

(α) Δέσμευση λόγω της κοινωνικής κανονικότητας, στην οποία οι άνθρωποι τείνουν να επιβάλουν κατασκευασμένες υποχρεώσεις προς το πρόσωπό τους, όπως στην περίπτωση προσφοράς ενός αγαθού ή υπηρεσίας όπου υπονοείται η υποχρέωση της ανταπόδοσης.

(β) Δέσμευση λόγω της συνέπειας προς την συνέχιση μιας συμπεριφοράς που βασίζεται σε μία απόφαση που έχει κάποιος ήδη λάβει. Για παράδειγμα η τακτική αγορά της ίδιας μάρκας κάποιου προϊόντος για το οποίο το άτομο έχει κάνει έρευνα αγοράς στο παρελθόν ακόμα κι αν πλέον η αγορά του δεν συμφέρει συγκριτικά με τα υπόλοιπα.

(γ) Δέσμευση λόγω ανάγκης για κοινωνική αποδοχή (social proof), εκεί το άτομο ακολουθεί μοντέλα συμπεριφορών της ομάδας στην οποία ανήκει, είτε πρότυπα “σημαντικών” τρίτων ατόμων.

(δ) Εμπιστοσύνη προς άλλα άτομα που θεωρεί κάποιος ευρέως αποδεκτά και επιτυχημένα. Για παράδειγμα έναν ποδοσφαιριστή σε μία διαφήμιση κάποιου προϊόντος άσχετου με το ποδόσφαιρο ή τα αθλήματα γενικά.

(ε) Φόβος, συνήθως προς την εξουσία, υπό το καθεστώς του οποίου ένα άτομο ακολουθεί οδηγίες και εντολές προκειμένου να αποφύγει κάποια αρνητική συνέπεια όπως την καταδίκη, τον εξευτελισμό ή μία τιμωρία.

(στ) Αντίδραση στην έλλειψη ενός προϊόντος. Σε ένα προϊόν που βρίσκεται σε περιορισμένες και ανεπαρκείς ποσότητες, ο άνθρωπος συνηθίζει να τοποθετεί μεγαλύτερη συναισθηματική αξία.

Ο Πίνακας 1 εξηγεί τα χαρακτηριστικά που απαρτίζουν καθέναν από αυτούς τους παράγοντες.

Ψυχολογικός Παράγοντας.	Χαρακτηριστικά που τον συνθέτουν.
Δέσμευση στην κοινωνική κανονικότητα.	Ανταπόδοση ως υποχρέωση.
Δέσμευση λόγω συνέπειας.	Συνέπεια προς της αντιλήψεις του και γνωσιακή επένδυση για την οποία καταβλήθηκε κόπος.
Δέσμευση λόγω ανάγκης για κοινωνική αποδοχή.	Κοινωνική αποδοχή και επιβεβαίωση μέσα από τη συμμόρφωση με κάποιο αποδεκτό συμπεριφοριστικό μοντέλο
Εμπιστοσύνη.	Αξιοπιστία κατά κοινή αποδοχή και δημοτικότητα του ατόμου που ασκεί εμπιστοσύνη.
Φόβος.	Υπακοή στις αρχές και συναίνεση υπό την απειλή τιμωρίας ή αρνητικών συνεπειών.
Αντίδραση στην σπανιότητα.	Ανεπαρκής ποσότητα του αγαθού σε σχέση με τη ζήτηση και παρορμητικότητα στην εκτίμηση της αξίας του.

Πίνακας 1. Ψυχολογικοί παράγοντες και τα ποιοτικά μεγέθη από τα οποία εξαρτούνται,.

TABLE 2. Descriptive statistics, scale reliabilities, and intercorrelations of study variables.

	X	SD	1	2	3	4	5	6	7	8	9	10	11	12
1. Normative commitment	4.34	1.38	(.89)											
2. Continuance commitment	3.74	0.99	.55	(.80)										
3. Affective commitment	3.96	1.19	.44	.25	(.87)									
4. Trust	3.95	1.23	.45	.37	.54	(.82)								
5. Obedience	3.80	0.92	.42	.35	.35	.26	(.85)							
6. Reactance	3.91	1.05	.51	.34	.61	.54	.29	(.74)						
7. Employee age	37.96	11.25	.35	.17	.17	.16	.26	.05	—					
8. Employee gender	1.47	0.50	.31	.21	.13	.19	.18	.01	.09	—				
9. Employee education	2.65	0.88	.01	.04	.02	.04	−.01	.09	.01	−.09	—			
10. Previous victimization	2.93	1.30	−.17	.04	−.04	−.09	−.17	.19	−.24	−.15	.12	—		
11. Subjective behaviors	4.19	1.25	.47	.46	.48	.59	.38	.48	.32	.19	.09	−.09	(.89)	
12. Objective behaviors	.0000	3.39	.43	.43	.46	.51	.33	.43	.27	.15	.13	−.06	.84	(.87)

Note. $N = 588$. All correlations greater than $r = .14$ are significant at $p < .001$; correlations greater than .12 are significant at $p < .01$

Ο Πίνακας 2 παρουσιάζει τα αποτελέσματα του πειράματος. Οι κύριες εξεταζόμενες μεταβλητές έδωσαν αποτέλεσμα μεγαλύτερο από 0.8, εκτός από την αντίδραση που έδωσε .74, πράγμα που επιβεβαιώνει ότι οι άνθρωποι που χαρακτηρίζονται περισσότερο από αυτές τις ιδιότητες είναι ευκολότερο να υποκύψουν στο phishing.

Πίνακας 2.

Αποτελέσματα της έρευνας του Workman.

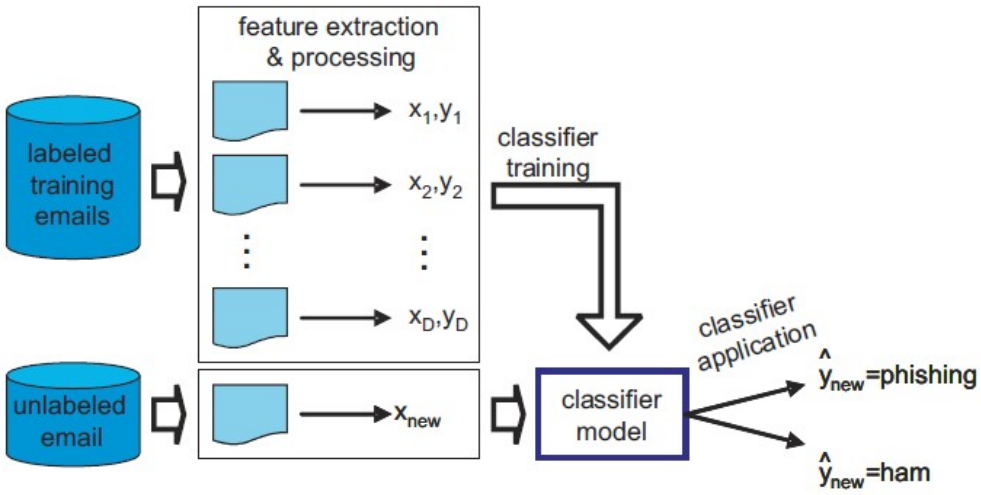
1.5.1 Εντοπισμός

Το 2006, μια έρευνα που ολοκληρώθηκε από τους R. Dhamija, J.D.Tygar και M. Hearst (Dhamija et al., 2006), έδειξε ότι ως και 90% των χρηστών ξεγελιούνται από ιστοσελίδες καλού phishing. Τα μηνύματα ηλεκτρονικού "ψαρέματος" (phishing) αποτελούν απειλή για την επικοινωνία μέσω διαδικτύου και την οικονομία παγκοσμίως. Προκειμένου να αντιμετωπιστεί αυτή, χρησιμοποιούνται μαύρες λίστες οι οποίες όμως δεν είναι αποτελεσματικές καθώς νέες απόπειρες απάτης διαφορετικής πηγής δημιουργούνται κάθε λεπτό. Έχουν γίνει κάποιες προτάσεις σχετικά με την πρόληψη μεταξύ των οποίων η χρήση μίας δυναμικής αλυσίδας Μάρκοφ και ενός μοντέλου λανθάνουσας κατανομής Dirichlet για την εκπαίδευση των ταξινομητών. Περεταίρω εφαρμογή ταξινομητών για την κατηγοριοποίηση phishing μηνυμάτων έχει γίνει από τον Chandrasekaran και τους συνεργάτες του (Chandrasekaran et al., 2006), ξεκινώντας με τα ακόλουθα χαρακτηριστικά: (1) ένα πλήθος δεικτών σχετικά με το στυλ των μηνυμάτων, (2) δομικά χαρακτηριστικά, και (3) λέξεις (π.χ. "κλικ"). Επίσης, ο Abu-Nihmeh και η ομάδα του (Abu-Nihmeh et al., 2007) διερεύνησε τις επιδόσεις διάφορων δημοφιλών ταξινομητών που χρησιμοποιούνται στην εξόρυξη κειμένου, π.χ., λογιστική παλινδρόμηση, τυχαία δάση και μηχανές διανυσμάτων υποστήριξης. Πέτυχαν βαθμό επιτυχίας f-measure 90% χρησιμοποιώντας τον ταξινομητή του τυχαίου δάσους. Τέλος, ο Fette και οι συνεργάτες του (Fette et al., 2007) ακολούθησαν μια παρόμοια προσέγγιση αλλά χρησιμοποιήστε ένα μεγαλύτερο δημόσια διαθέσιμο δείγμα με περίπου 7000 νόμιμα ηλεκτρονικά μηνύματα και 860 μηνύματα phishing. Κατά την επεξεργασία του προτείνουν δέκα διαφορετικά χαρακτηριστικά γνωρίσματα για τον εντοπισμό του phishing. Εννέα από αυτά τα χαρακτηριστικά μπορούν να εξαχθούν από το ίδιο το μήνυμα ηλεκτρονικού ταχυδρομείου, ενώ το δέκατο χαρακτηριστικό, η ηλικία των ονομάτων των domains που συνδέονται στο mail, πρέπει να λαμβάνεται από ένα αίτημα WHOIS τη στιγμή που λαμβάνεται το μήνυμα ηλεκτρονικού ταχυδρομείου. Πέτυχαν έτσι 0.13% ψευδώς θετικών ταξινομήσεων και 3.6% ψευδώς αρνητικών. Αυτό αντιστοιχεί σε βαθμό 97,6% f-measure.

Οι τεχνικές μηχανικής μάθησης, ιδιαίτερα η αυτόματη ταξινόμηση, έχουν γίνει δημοφιλείς στον τομέα της αναγνώρισης spam και phishing mails. Σε αντίθεση με τους χειροκίνητα κατασκευασμένους κανόνες φιλτραρίσματος, αυτοί αξιολογούν αυτόματα τη συνάφεια των χαρακτηριστικών εισόδου x = (x1, ..., xm) (π.χ. τα χαρακτηριστικά του email) και δημιουργούν μια συνάρτηση για την επιθυμητή ταξινόμηση y (π.χ. phishing ή nonphishing).

$$y = f(x, g)$$

Το διάνυσμα των αγνώστων τιμών των παραμέτρων καθορίζεται κατά τη φάση εκπαίδευσης με τέτοιο τρόπο ώστε η σχέση μεταξύ x και y στα εξεταζόμενα δεδομένα (x1, y1),. . . , (xD, yD) να αναπαράγεται με βάση κάποιο κριτήριο βελτιστοποίησης. Στη φάση της εφαρμογής, τα ίδια χαρακτηριστικά εξάγονται από ένα νέο εισερχόμενο μήνυμα. Με βάση αυτά τα χαρακτηριστικά και τη μοντελοποίηση, ο ταξινομητής παράγει μια ταξινόμηση του μηνύματος. Συνολικά, η προσέγγιση για τη μηχανική μάθηση συνοψίζεται στο Σχήμα.



Σχήμα 3. Το μοντέλο της μηχανικής μάθησης (Paass, 2008).

Για να προσεγγιστεί η επίδοση ενός ταξινομητή, διαφορετικά ποιοτικά μέτρα υπολογίζονται σε ένα ανεξάρτητο σύνολο που δεν έχει χρησιμοποιηθεί κατά τη φάση εκπαίδευσης. Παρακάτω παρουσιάζεται όπως προτάθηκε τον Gerhard Paass και τους συνεργάτες του, η ταξινόμηση αλυσίδας Markov (Paass et al., 2008). Αυτή μπορεί να περιγραφεί με τον εξής τρόπο:

Η εντροπία διασταύρωσης (cross-entropy (CE)) H(x,M) μεταξύ του μηνύματος x και της πηγής που προσεγγίζεται από το μοντέλο M, είναι ένα μέτρο της πιθανότητας ένα μήνυμα x με δυαδική αναπαράσταση (b_n), να έχει παραχθεί (b_1 . . . b_n) από αυτή την πηγή. Η εντροπία διασταύρωσης ορίζεται ως:

$$H(x, M) = -\frac{1}{n}\log\prod_{i=1}^{n} p(\, b_i | b_1^{i-1}, M)$$

όπου $p(b_i\,|b_1^{i-1}, M)$ είναι η πιθανότητα να συναντήσουμε το bit b_i βάσει των προηγούμενων bits b_1 . . . b_{i-1} του μηνύματος. Η τάξη στην οποία το μήνυμα x έχει την μικρότερη εντροπία, είναι αυτή από την οποία πιο πιθανά προήλθε. Επομένως η ταξινόμηση του x μπορεί να μοντελοποιηθεί βάσει της ελάχιστης εντροπίας διασταύρωσης σε όλες τις τάξεις C ως:

$$f(x) = arg\min_{c \in C} H(x, M_c)$$

όπου M_c είναι το μοντέλο για την τάξη $c \in C$. Μία εναλλακτική προσαρμογή της χρήσης της αλυσίδας Markov έγινε από τον Gerhard Paass και τους συνεργάτες του, κατά την οποία η μνήμη που απαιτείται για την εφαρμογή της τεχνικής ελαττώνεται κατά δύο τρίτα σε σχέση με την περίπτωση χρήσης του παραπάνω αλγορίθμου. Η εφαρμογή αυτή παρουσιάζεται παρακάτω:

Έστω ότι $M_c^{1,i-1}$ είναι το μοντέλο που προέκυψε μετά από την επεξεργασία των παραδειγμάτων εκπαίδευσης x_1, . . . , x_k μίας τάξης c. Κατά τη διάρκεια της παραγωγής όλων των μοντέλων, θεωρούμε την: $H(xi, M_c^{1,i-1})$ ως την αναμενόμενη εντροπία ενός μηνύματος διασταύρωσης x_i και του μοντέλου $M_c^{1,i-1}$. Έστω η εμπειρική τυπική απόκλιση των αναμενόμενων εντροπιών $\hat{\sigma}(k)$ του $M_c^{1,i-1}$, ίση με:

$$\hat{\sigma}(k) = \sqrt{\frac{1}{k-2} \cdot \sum_{i=1}^{k-1} \left(H\left(x_i, M_c^{1,i-1}\right) - \overline{H\left(x, M_c^{1,i-1}\right)} \right)^2}$$

Όπου $H\left(x, M_c^{1,i-1}\right) = \frac{1}{i-1} \sum_{j=1}^{i-1} H(x_j, M_c^{1,i-1})$. Για να επιλέξουμε ένα παράδειγμα για την εκπαίδευση βάσει της χρησιμότητάς του στην ακριβή ταξινόμηση, συγκρίνουμε την εντροπία του με τον μέσο και την τυπική απόκλιση από τα προηγούμενα βήματα της εκπαίδευσης. Με άλλα λόγια, θέλουμε να χρησιμοποιήσουμε μόνο εκπαιδευτικά παραδείγματα που το μοντέλο δεν μπορεί ήδη να ταξινομήσει ικανοποιητικά. Προσπερνάμε αλληλουχίες που είναι πιο πιθανές στο σύνολο των συνηθισμένων αλληλουχιών για μία πηγή. Για την ταξινόμηση των mails, κατασκευάζουμε δύο μοντέλα, ένα για τα ακίνδυνα μηνύματα (ham mails) και ένα για τα μηνύματα phishing. Εξάγουμε τέσσερα χαρακτηριστικά: τις τιμές H(x,M) για κάθε ένα από τα μοντέλα και δύο Boolean χαρακτηριστικά ως δείκτες κατάταξης σε κάθε μία από τις δύο τάξεις.

Τα σημασιολογικά χαρακτηριστικά είναι δείκτες περιεχομένου των e-mails και εξάγονται με χρήση μοντέλων λανθάνοντος θέματος. Τα λανθάνοντα αυτά θέματα είναι συστάδες λέξεων (clusters) που τείνουν να εμφανίζονται μαζί στα μηνύματα. Μπορούμε να περιμένουμε πως σε ένα phishing mail, οι λέξεις «κλικ», και «λογαριασμός» ή «account» συχνά εμφανίζονται μαζί, ενώ σε συνήθη οικονομικής φύσης μηνύματα, οι λέξεις «αγορά», «τιμές» και «πλάνο» μπορεί να συμπέσουν. Τα μοντέλα λανθάνοντος θέματος παράγουν τέτοια χαρακτηριστικά εκμεταλλευόμενα την συνύπαρξη λέξεων σε ένα εκπαιδευτικό σύνολο από mail. Ο Gerhard Paass και οι συνεργάτες του ανέπτυξαν ένα στατιστικό μοντέλο, το latent Class-Topic Model (CLTOM) το οποίο χρησιμοποιεί μπλοκ (clusters) λέξεων στα οποία η σειρά δεν παίζει ρόλο. Έτσι επικεντρώνεται περισσότερο στο διαχωρισμό των phishing από τα ακίνδυνα μηνύματα. Το μοντέλο εκπαιδεύεται σε ένα σετ μηνυμάτων όπου αναγνωρίζει την πιθανότητα να συνυπάρχουν διάφοροι συνδυασμοί λέξεων σε phishing και ακίνδυνα μηνύματα. Έτσι μπορεί να κατηγοριοποιεί τα mails βάσει του περιεχομένου τους.

1.5.2 Spear Phishing

Ως spear phishing ορίζεται η επίθεση phishing που στοχεύει ένα άτομο ή μία ομάδα με κάποιο κοινό χαρακτηριστικό. Αυτή διεξάγεται μετά από συλλογή στοιχείων για τον στόχο και σχεδιασμό προσαρμοσμένο στην περίσταση. Μπορεί να διεξάγονται είτε από πρόσωπα είτε ανώνυμα από εξειδικευμένα bots. Οι επιθέσεις αυτές έχουν πολλά κοινά με τις προαναφερθείσες επιθέσεις phishing αλλά συνήθως προέρχονται από κάποιον οργανισμό και όχι από μεμονωμένα άτομα.

Σε αντίθεση με την κλασική περίπτωση του phishing, όπως περιγράφηκε παραπάνω, για την οποία υπάρχουν αλγόριθμοι πρόβλεψης, το spear phishing, είναι μία επίθεση που εντοπίζεται και αποφεύγεται εξαιρετικά δύσκολα.

Τα mails αυτού του είδους επίθεσης είναι εξ ολοκλήρου κατασκευασμένα ώστε να έχουν παρουσιαστικό και περιεχόμενο που θα μπορούσε να προέρχεται από έναν νόμιμο οργανισμό. Μπορεί να είναι σε μορφή HTML και να περιλαμβάνουν λογότυπα, στοιχεία επικοινωνίας και copyright φαινομενικά πανομοιότυπα με αυτά που χρησιμοποιεί κάποια εταιρία ή ίδρυμα. Κάποιες από τις πιο συχνές απάτες περιλαμβάνουν μηνύματα αίτησης ανανέωσης των δεδομένων λογαριασμού του χρήστη, προειδοποιήσεις ότι ο λογαριασμός του θα διαγραφεί ή διαδικασίες επιβεβαίωσης στοιχείων. Το spear phishing έχει αποδειχθεί εξαιρετικά πιο αποδοτικό από την γενική μορφή phishing. Προκειμένου να χτιστεί μία σχέση εμπιστοσύνης με το θύμα, ο επιτιθέμενος παρατείνει το χρονικό διάστημα της επικοινωνίας. Η διαδικασία μίας επίθεσης spear phishing γενικά χωρίζεται σε πολλά στάδια και μπορεί να είναι χρονοβόρα και πολυέξοδη, έχει όμως μεγάλη πιθανότητα επιτυχίας.

Το ποσοστό ανάγνωσης των spear phishing mails είναι 70%. Ενώ για το μαζικό phishing είναι 3%. Ακόμα 50% από τους παραλήπτες που ανοίγουν spear phishing mails, κάνουν κλικ και στον σύνδεσμο που περιέχεται, σε αντίθεση με το 5% των χρηστών για το μαζικό phishing (Jagatic et al., 2007).

Τα δύο κεντρικά στάδια μίας επίθεσης spear phishing είναι τα εξής:

1. Επιλογή του θύματος και συλλογή πληροφοριών γύρω από αυτό και κατασκευή του μηνύματος. Το μήνυμα ράβεται στα μέτρα του στόχου με τρόπο που ο επιτιθέμενος δεν χρειάζεται να μιμηθεί κάποιον τρίτο ή να χρησιμοποιήσει λογότυπα και ονόματα γνωστών εταιριών. Αυτό προϋποθέτει τη γνώση προσωπικών δεδομένων για τον στόχο.

2. Κατασκευή ενός καμουφλαρισμένου ιστοτόπου για την συλλογή των προσωπικών δεδομένων του στόχου με domain name που δεν προδίδει την χρήση της σελίδας.

1.5.3 Mail spoofing

Πρόκειται για μία υποκατηγορία της επίθεσης spear phishing που αυξάνει την πιθανότητα να βρεθεί θύμα της επίθεσης ο στόχος. Στην περίπτωση του mail spoofing, η διεύθυνση mail από την οποία διεξάγεται η επίθεση είναι πανομοιότυπη με την διεύθυνση κάποιας από τις επαφές του στόχου, ιδανικά ενός φιλικού ή γνωστού ατόμου.

Σε έρευνα που έχει διεξαχθεί (Qingxiong, 2013) έχει αποδειχθεί ότι ένα άτομο είναι τέσσερις φορές πιθανότερο να πέσει θύμα μίας επίθεσης όταν αυτή γίνεται από κάποιον φαινομενικά γνωστό του. Στην ίδια έρευνα, περισσότερα από τα τρία τέταρτα των θυμάτων έδωσαν προσωπικά τους δεδομένα μετά από το spoofed mail που έλαβαν.

Η διαδικασία της μίμησης ενός mail είναι σχετικά απλή καθώς μπορεί ο server να ρυθμίσει να είναι άλλη η διεύθυνση που βλέπει ο παραλήπτης και άλλη η κανονική διεύθυνση. Έτσι όταν ο χρήστης που δέχτηκε επίθεση απαντήσει στο mail την απάντηση θα την λάβει ο επιτιθέμενος αντί για τον πραγματικό χρήστη στον οποίο ανήκει η διεύθυνση. Επίσης ο server επιτρέπει τον ορισμό του ονόματος το οποίο εμφανίζεται ως αποστολέας.

Το mail spoofing βασίζεται στην δομή ενός mail, όταν αυτό κατασκευάζεται από τον server.

Όταν ένα SMTP (simple mail transfer protocol) mail αποστέλλεται, η αρχική σύνδεση παρέχει δύο πληροφορίες:

- **MAIL FROM**: Παρουσιάζεται στον παραλήπτη ως η διαδρομή επιστροφής αλλά δεν είναι συνήθως ορατό από τον χρήστη. Δεν είναι προκαθορισμένο να ελέγχεται αν ο αποστολέας είναι εξουσιοδοτημένος να στείλει εκ μέρους αυτής της διεύθυνσης.
- **RCPT TO**: Προσδιορίζει σε ποιά διεύθυνση το mail παραδίδεται και είναι συνήθως ορατό από τον παραλήπτη.

Αυτά τα δύο μαζί ονομάζονται διεύθυνση φακέλου (envelope addressing). Αν ο server που λαμβάνει το mail δεν ανακοινώσει πως έχει πρόβλημα με κάποιο από τα δύο αυτά αντικείμενα, το σύστημα του αποστολέα στέλνει και την εντολή “DATA” και συνήθως στέλνει πολλές κεφαλίδες, συμπεριλαμβανομένων των:

- **From**: Η διεύθυνση που είναι ορατή ως διεύθυνση αποστολέα στον παραλήπτη. Επίσης δεν γίνεται αν δεν ζητηθεί έλεγχος για τα δικαιώματα του αποστολέα να στείλει από αυτή την διεύθυνση.
- **Reply-to**: Επίσης δεν ελέγχεται.

Ως αποτέλεσμα, ο παραλήπτης βλέπει το mail σαν να προέρχεται από τη διεύθυνση στην κεφαλίδα **From**:, μερικές φορές είναι δυνατό να βρεθεί η διεύθυνση **MAIL FROM**. Ωστόσο αν απαντήσει ο παραλήπτης στο μήνυμα η απάντηση θα σταλεί στη διεύθυνση **From** ή στη διεύθυνση **Reply-to**.

Ανάμεσα στα δύο στάδια του spear phishing λοιπόν, εμείς θα προσθέσουμε άλλα δύο που πραγματοποιούνται για μία επίθεση mail spoofing:

1^{α}. Καταγραφή του δικτύου φίλων του στόχου και επιλογή του ατόμου το οποίο ο επιτιθέμενος θα προσποιηθεί.

1^{β}. Εύρεση της διεύθυνσης mail του ατόμου που επιλέχθηκε και κατασκευή ή επιλογή ενός server για την κατασκευή του spoofed mail.

1.5.4 Πρόληψη

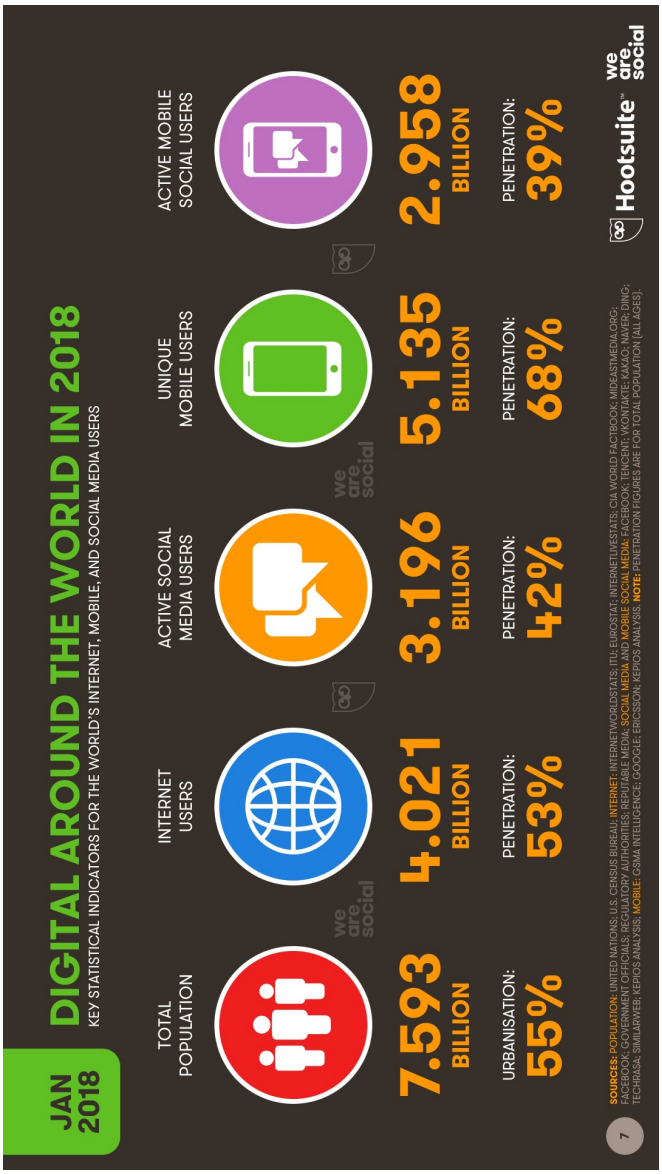
Πάνω από το 97% του παγκόσμιου πληθυσμού, δεν είναι σε θέση να αναγνωρίσει ένα καλά κατασκευασμένο email, σε μία επίθεση spear phishing, πόσο μάλλον αν χρησιμοποιεί mail spoofing. Η καλύτερη μορφή πρόληψης αυτή τη στιγμή είναι ένα σύστημα επικύρωσης της αξιοπιστίας των email, με το όνομα DMARC (Domain-based Message Authentication, Reporting and Conformance), το οποίο εντοπίζει και προλαμβάνει το mail spoofing. Επιτρέπει στον διαχειριστή ενός domain να εκδώσει μία πολιτική που να αναφέρει πως πρέπει να δράσει ο παραλήπτης σε περίπτωση αποτυχίας και κάτω από ποιες προϋποθέσεις το πεδίο **From**: πρέπει να θεωρηθεί αξιόπιστο. Ήδη πολλά σημαντικά και κομβικά domain names έχουν εκδώσει την πολιτική DMARC που χρειάζονται. Το DMARC ωστόσο είναι δύσκολο στην εγκατάστασή του και δημιουργεί πολλά προβλήματα στην επικοινωνία όσων δεν έχουν εκδώσει την πολιτική του domain τους. Επίσης πολλές μεγάλες ιστοσελίδες δεν έχουν εξασφαλίσει επαρκώς το domain τους. Στην περίπτωση του *facebook.com* για παράδειγμα, η διεύθυνση *fb.com* που παραπέμπει στην ίδια ιστοσελίδα δεν διαθέτει πιστοποιητικό που ορίζει την απόρριψη των spoofed mails από διευθύνσεις της μορφής *name@fb.com* .

Άλλο μέτρο πρόληψης που χρησιμοποιείται από ορισμένους παρόχους mail όπως το gmail, είναι η απλή σύγκριση του πεδίου **From** του μέρους DATA του μηνύματος, με το πεδίο **MAIL FROM** στο περιεχόμενο της αρχικής επικοινωνίας. Αν αυτά τα δύο διαφέρουν, το email σηματοδοτείται ως spam. Αυτή η μορφή πρόληψης ωστόσο δεν προστατεύει τον παραλήπτη ενός μηνύματος από ένα mail με ψευδές όνομα αποστολέα και διεύθυνση πολύ κοντινή στην αυθεντική. Για παράδειγμα: *John Marc <John_Marc@yahoo.com>* αντί για *John Marc <John_Marc@yaho.com>*.

2. Η έρευνα

2.1 Παγκόσμια δικτύωση

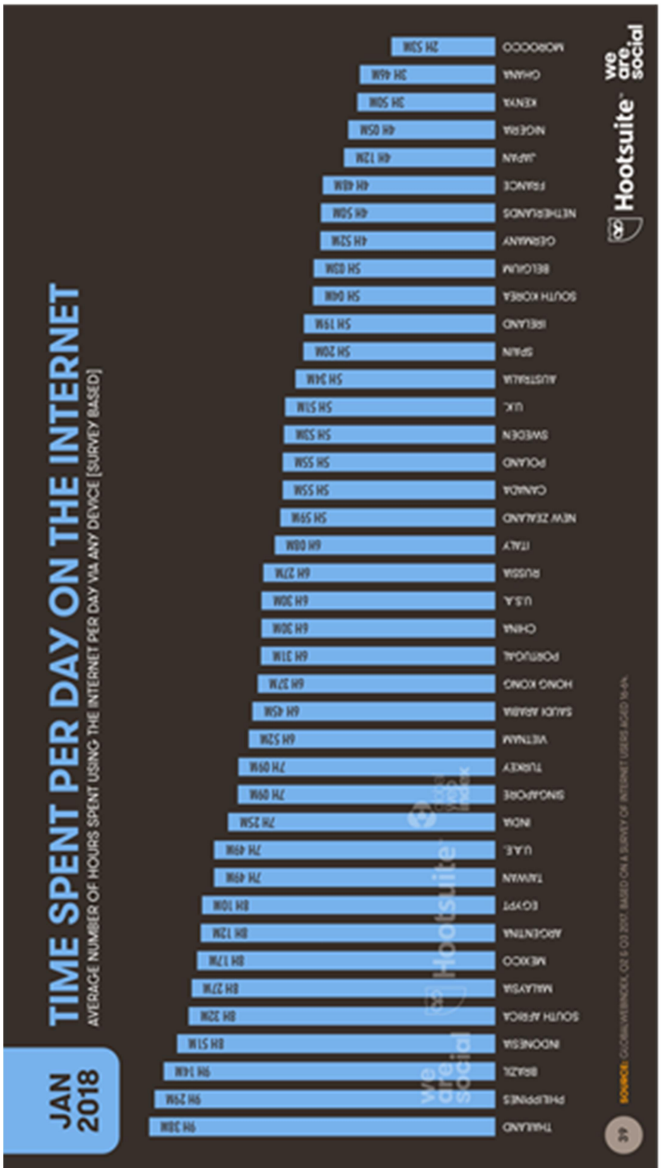
Τα ψηφιακά μέσα είναι πλέον προσβάσιμα από ένα πολύ μεγάλο μέρος του παγκόσμιου πληθυσμού. Ήδη το 53% του πληθυσμού έχει πρόσβαση στο διαδίκτυο και το 42% του πληθυσμού αποτελείται από ενεργούς χρήστες των μέσων κοινωνικής δικτύωσης (γράφημα 1). Οι άνθρωποι που ανήκουν στις ομάδες αυτές καταναλώνουν κατά μέσο όρο μεγάλο μέρος του χρόνου τους ημερησίως συνδεδεμένοι στο διαδίκτυο (γράφημα 2). Με τα δεδομένα αυτά μπορούμε με ασφάλεια να πούμε πως πλέον η διαδικτυακή διάσταση του κόσμου λαμβάνει διαστάσεις εφάμιλλες του υλικού κόσμου από άποψη ποσότητας πληροφορίας που κινείται και προσωπικών δεδομένων που εκτίθενται. Από πλευράς πυκνότητας της δικτύωσης, τα social media και ο κόσμος έξω από αυτά δεν έχουν πολύ μεγάλη διαφορά.



Γράφημα 1. Η ψηφιοποίηση παγκοσμίως (Ref. 47)

Το 1960 ο Stanley Milgram με ένα κοινωνικό πείραμά του στην Αμερική έβγαλε το συμπέρασμα πως το παγκόσμιο δίκτυο γνωριμιών έχει κατά μέσο όρο 6.2 βήματα (hops) από κάθε άνθρωπο προς έναν τυχαίο άλλο. Παρ' όλα αυτά ο Milgram διεξήγαγε το πείραμα μόνο μέσα στις ΗΠΑ. Η Microsoft το 2006 σε μία έρευνά της μέσα από 30 δισεκατομμύρια μηνύματα ηλεκτρονικού ταχυδρομείου που κινήθηκαν στο δίκτυό της σε ένα μήνα, έβγαλε το συμπέρασμα πως είναι 6.8 βήματα, πολύ κοντά στο αποτέλεσμα του Milgram. Το facebook το 2008 μίλησε για 5.28 hops, κοντά στο αποτέλεσμα της Microsoft. Ωστόσο σε νεότερες μετρήσεις, το 2011 το facebook ανέφερε 3.74 hops και το 2016, όταν είχε διπλασιαστεί ο πληθυσμός του site, σε νέα έρευνα αναφέρθηκαν σε 3.57 hops.

Αυτό το εξαιρετικά μικρό νούμερο σημαίνει πως οι ιδέες, οι δημιουργίες ή τα προσωπικά δεδομένα κάποιου, κατά τη διακίνησή τους, κατά μέσο όρο μπορούν να φτάσουν σε οποιονδήποτε άλλο άνθρωπο μόνο με τρία ή τέσσερα share ή like από τα κατάλληλα άτομα. Σε αυτό περιβάλλον έντονης δικτύωσης, είναι λογικό οργανισμοί, εταιρίες, επιχειρήσεις και μεμονωμένα άτομα να προσπαθήσουν να εκμεταλλευτούν προς όφελός τους την αστείρευτη ποσότητα πληροφορίας που διακινείται.



Γράφημα 2. Μέσος χρόνος online καθημερινά ανά χώρα. (Ref. 47)

Υπάρχουν περιπτώσεις οπού το μέσο για την επίτευξη ενός στόχου είναι η διακίνηση πληροφορίας, όπως στην περίπτωση μίας διαφημιστικής ή πολιτικής καμπάνιας. Στις περιπτώσεις αυτές, είναι εκμεταλλεύσιμη η ιδιότητα των μέσων κοινωνικής δικτύωσης να είναι scale free δίκτυα. Αυτό σημαίνει πως η κατανομή πιθανότητας του degree είναι εκθετική. Πρακτικά όσο αυξάνεται η τιμή του degree, τόσο εκθετικά λιγότεροι κόμβοι υπάρχουν που λαμβάνουν αυτή την τιμή. Με τον όρο degree σε έναν μη κατευθυνόμενο γράφο αναφερόμαστε στο πλήθος γειτόνων που συνδέονται άμεσα με έναν κόμβο. Εκμεταλλευόμενοι την ιδιότητα αυτή των scale free δικτύων, μπορούμε να καταστήσουμε αποδοτικότερη τη διάχυση της πληροφορίας στο δίκτυο. Αυτό επιλέγοντας να εισάγουμε στο δίκτυο την πληροφορία μέσω των λιγοστών κόμβων με πολύ υψηλό degree, όπου αυτό είναι δυνατό.

Στην πλειοψηφία των περιπτώσεων ωστόσο είναι απαραίτητη η συλλογή πληροφορίας από τα κοινωνικά δίκτυα. Μία τέτοια είναι η περίπτωση που θα μελετηθεί σε αυτή την εργασία.

2.2 Case study – Κοινό δίκτυο επαφών

Από τις πολλές διαθέσιμες επιλογές προς μελέτη, επιλέχθηκε ένα άτομο που είχε λογαριασμό στο facebook, στο twitter και στο LinkedIn. Αυτό τέθηκε ως κριτήριο γιατί από τη σύνθεση των τριών δικτύων είναι πιθανό να μπορούν να εξαχθούν ακριβέστερα αποτελέσματα και μία πιο ολοκληρωμένη εικόνα για το ευρύ κοινωνικό δίκτυο του ατόμου. Ως τώρα πολλές φορές έχουν μελετηθεί τα δίκτυα ατόμων σε κάθε ένα από τα τρία αυτά μέσα κοινωνικής δικτύωσης αλλά ποτέ δεν έχει γίνει η σύνθεση των τριών σε ένα δίκτυο. Αυτή είναι μία δουλειά που δεν μπορεί εύκολα να αυτοματοποιηθεί καθώς ένα άτομο μπορεί να έχει άλλο όνομα σε κάθε ένα από αυτά τα μέσα, άλλο email και διαφορετικές εικόνες προφίλ. Για τον λόγο αυτό η διασταύρωση των λογαριασμών και η κατασκευή του πρέπει να γίνεται με προσωπική προσπάθεια του ερευνητή ή με κάποιο πρόγραμμα που θα κατεβάσει όλα τα στοιχεία σε βάση δεδομένων και ύστερα θα αρχίζει να συσχετίζει προφίλ

διαφορετικών ιστοτόπων μεταξύ τους. Αυτός ο συσχετισμός θα απαιτεί αναγνώριση προσώπου και κάποιον αλγόριθμο που να αναγνωρίζει πόσο όμοια είναι δύο ονόματα. Πχ A. Hernandez και A. Hndz. Το παράδειγμα αυτό θα μπορούσε να είναι το όνομα στο facebook και στο twitter αντίστοιχα του ίδιου ατόμου. Η δυσκολία κατασκευής του δικτύου περιορίζει και το μέγεθος του δείγματος, για ένα άτομο με 1000 επαφές στο facebook και 350 στο twitter θα έπρεπε να δαπανηθεί πολλαπλάσια προσπάθεια από ότι στη συγκεκριμένη περίπτωση αφού θα κατασκευαζόταν ένα δίκτυο με περισσότερους από 500 κόμβους. Ωστόσο στην περίπτωσή μας (169 κόμβοι), αν και λιγότερο ακριβές στατιστικά το δείγμα, δεν επηρεάζεται το αποτέλεσμα της έρευνας γιατί τα μεγέθη που μετράμε δεν τα εξετάζουμε συγκριτικά με την μέση περίπτωση. Αυτό που έχει σημασία είναι να αποτυπωθεί με ακρίβεια ένα ικανοποιητικά μεγάλο τμήμα του κοινωνικού δικτύου του ατόμου που μελετάμε. Θέτοντας κριτήρια για την επιλογή των ατόμων που θέτουμε ως κόμβους διασφαλίζουμε την ποιότητα του δικτύου. Ο βρετανός ανθρωπολόγος Robin Dunbar, την δεκαετία του 90 είχε υποστηρίξει πως οι άνθρωποι που αποτελούν τον κοινωνικό περίγυρο ενός ατόμου κυμαίνονται μεταξύ των 100 και 250, κατά μέσο όρο όμως είναι περί τους 150 (Ref. 48). Εμείς έχοντας επιλέξει ως σημαντικούς και προς μελέτη 169 από τους συνολικά 230 κόμβους, μπορούμε να πούμε πως έχουμε ένα καλό κομμάτι του συνολικού κοινωνικού κύκλου του υπό μελέτη ατόμου.

2.3 Σκοπός της έρευνας

Η μελέτη του δικτύου αποσκοπεί στην εύρεση του ατόμου από το οποίο αν εκκινηθεί μία επίθεση spear phishing με τη χρήση mail spoofing προς το κεντρικό άτομο της μελέτης, οι πιθανότητες να πετύχει θα είναι οι μεγαλύτερες. Η επίθεση spear phishing έχει αρκετές γνωσιακές ανάγκες που θέτει γύρω από το κοινωνικό δίκτυο του στόχου. Για τον λόγο αυτό αποτελεί μία καλή αφορμή για την μελέτη και την εξαγωγή συμπερασμάτων για τις σχέσεις του στόχου με τα άτομα που απαρτίζουν το δίκτυο, μόνο βάσει της τοπολογίας του δικτύου. Θα ήταν ένα πολύ ισχυρό εργαλείο η γνώση άλλων

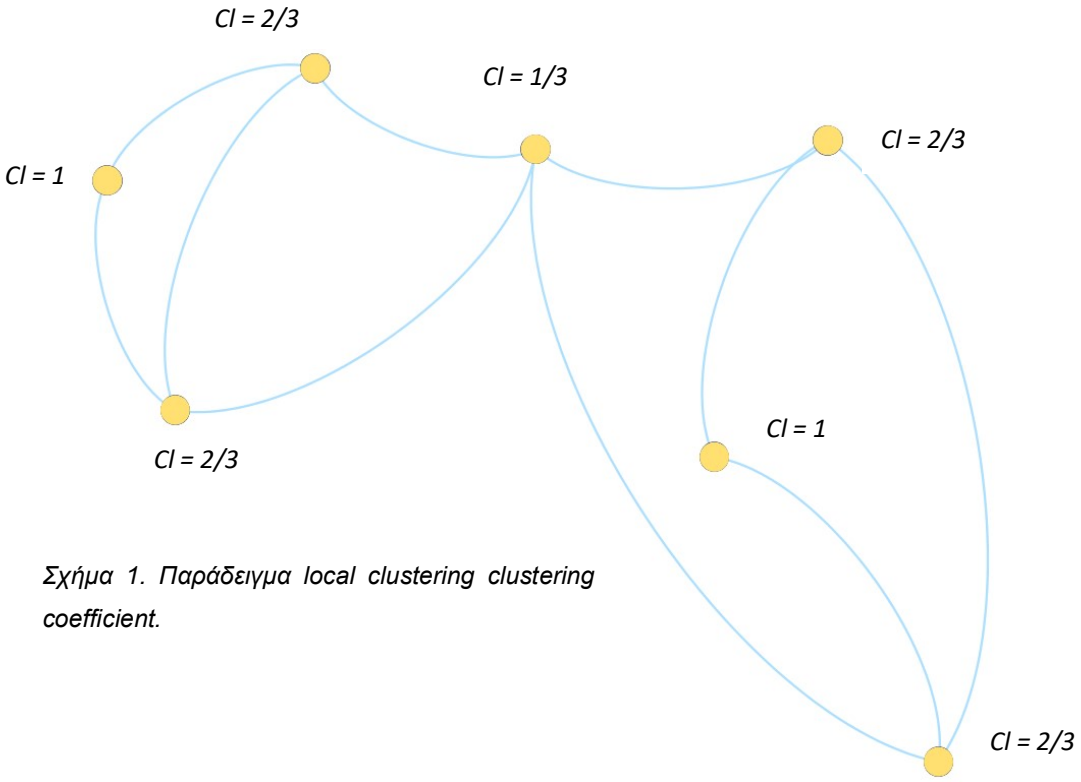
μεγεθών όπως ο ρυθμός επικοινωνίας μεταξύ των ατόμων ή ο όγκος δεδομένων που διακινούνται στο δίκτυο. Όμως η πρόκληση στην συγκεκριμένη μελέτη είναι η εξαγωγή συμπεράσματος με τη χρήση μόνο ελάχιστων δημόσιων δεδομένων. Μία προσθήκη που θα μπορούσαμε να κάνουμε στην παρούσα εργασία, θα ήταν να εξετάσουμε τους τοίχους των ατόμων με κάποιο software και έτσι να βάλουμε βάρη στο δίκτυο βάσει του πλήθους δημοσιεύσεων και tags μεταξύ των κόμβων.

Μπορούμε να πούμε λοιπόν πως στόχος της εργασίας είναι να εξαχθούν κάποια συμπεράσματα για τις σχέσεις του ατόμου με τους άλλους χρήστες των social media, μόνο βάσει της τοπολογίας του δικτύου. Της ελάχιστης πληροφορίας δηλαδή που μπορεί να μας δοθεί. Τελικά γίνεται μία ταξινόμηση των κόμβων ως προς την καταλληλότητά τους να γίνουν εφαλτήρια του spear phishing. Μέσα από τα στάδια που περνάμε κατά τον υπολογισμό των απαραίτητων παραμέτρων, μπορούμε να βγάλουμε και άλλα συμπεράσματα για τον κάθε κόμβο ανάλογα με τις τιμές που αυτές παίρνουν.

2.4 Οι παράμετροι του δικτύου

Η πρώτη παράμετρος που θα υπολογιστεί, είναι ο βαθμός (degree) του κάθε κόμβου. Αυτός μας δείχνει το πλήθος κοινών φίλων με τον κεντρικό κόμβο και κατ' επέκταση μπορούμε να πούμε το πόσο κοντινό άτομο είναι. Δύο άνθρωποι που τείνουν να περνάνε πολύ χρόνο μαζί έχουν μεγαλύτερη πιθανότητα να έχουν πολλές κοινές γνωριμίες. Επίσης δύο άτομα που έχουν πολλές κοινές γνωριμίες συνήθως συσχετίζονται σε περισσότερους από έναν χώρους. Πχ είναι συνεργάτες αλλά και φίλοι που έχουν κοινές παρέες. Στη συνέχεια υπολογίζουμε την τιμή του clustering. Μετράμε έτσι το πλήθος των τριγώνων που σχηματίζονται μεταξύ κάθε κόμβου και των γειτόνων του σε σχέση με το μέγιστο πλήθος τριγώνων που θα μπορούσε να σχηματιστεί. Έτσι αντιλαμβανόμαστε τον τρόπο με τον οποίο ένας κόμβος συσχετίζεται με το άτομο που μελετάμε. Αν έχει κοινούς φίλους οι οποίοι είναι κι αυτοί φίλοι μεταξύ τους (υψηλή τιμή clustering), συνήθως θα ανήκει σε έναν κοινωνικό κύκλο μέσω του οποίου συσχετίζεται με τον κεντρικό κόμβο. Αν αντιθέτως έχει έναν αριθμό κοινών φίλων με τον κεντρικό κόμβο οι οποίοι δεν γνωρίζονται

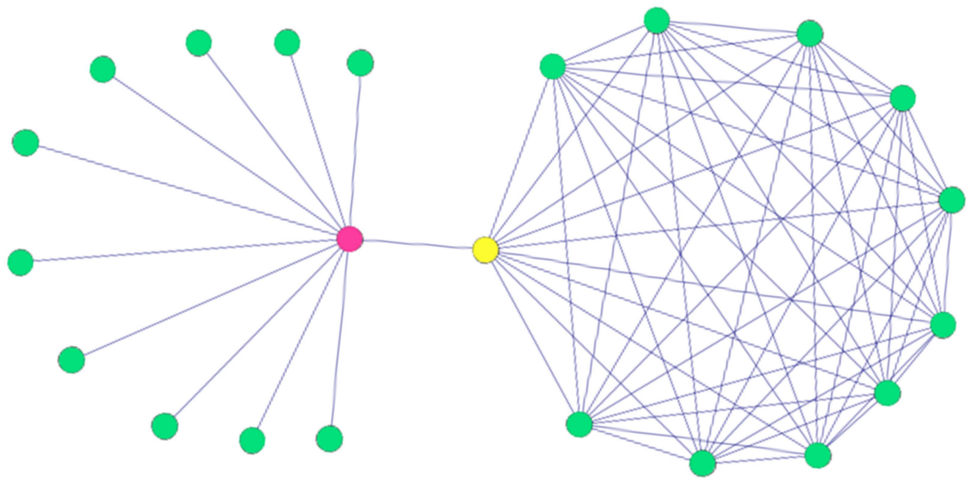
μεταξύ τους (μικρή τιμή clustering), η σύνδεση μπορεί να είναι ισχυρότερη καθώς συνυπάρχει με τον κεντρικό κόμβο σε πλήθος κοινωνικών κύκλων. Στην περίπτωση αυτή επίσης, ο κόμβος βρίσκεται σε θέση ισχύος όσον αφορά την πληροφορία που κινείται στο δίκτυο γιατί προκειμένου να διακινηθεί μεταξύ πολλών ατόμων πρέπει να διασχίσει τον ίδιο. Έτσι στο σχήμα 1 φαίνεται πως ο κόμβος με clustering ίσο με 1/3 είναι μονόδρομος για την κίνηση της πληροφορίας μεταξύ των τεσσάρων από τα έξι ζευγάρια που σχηματίζουν οι γείτονές του.



Σχήμα 1. Παράδειγμα local clustering clustering coefficient.

Ύστερα από το clustering, θα ασχοληθούμε με τέσσερα μέτρα της κεντρικότητας των κόμβων στο δίκτυο (centrality). Η κεντρικότητα μπορεί να μετρηθεί με περισσότερους από δέκα διαφορετικούς τρόπους, ωστόσο επιλέγουμε τέσσερα διαφορετικά μέτρα που βασίζονται μόνο σε τοπολογικά χαρακτηριστικά του δικτύου. Υπολογίζουμε αρχικά την betweenness centrality, η οποία παίρνει υψηλές τιμές για έναν κόμβο που είναι μέρος πολλών ελαχίστων μονοπατιών μεταξύ των κόμβων του δικτύου. Επίσης υπολογίζουμε και ένα παρόμοιο αλλά διαφορετικό μέγεθος, την pagerank

centrality. Αυτό το μέγεθος πρώτη φορά χρησιμοποιήθηκε από την google ώστε να ταξινομήσει βάσει της κεντρικότητάς τους τις σελίδες στο διαδίκτυο. Ένας κόμβος έχει υψηλή pagerank centrality όταν είναι ψηλή η πιθανότητα να είναι μέρος μίας τυχαίας διαδρομής μέσα στο δίκτυο. Ακόμα υπολογίζουμε την eigenvector centrality η οποία σχετίζεται με το degree και παίρνει υψηλή τιμή για έναν κόμβο ο οποίους συνδέεται με άλλους που έχουν υψηλό degree. Έτσι επίσης μπορούμε να κρίνουμε την στρατηγική σημασία ενός κόμβου μέσα στο δίκτυο. Τέλος υπολογίζουμε την closeness centrality, η τιμή της για έναν κόμβο εξαρτάται από το αντίστροφο της απόστασής του από όλους τους άλλους κόμβους στο δίκτυο. Στο σχήμα 2 φαίνεται ένα παράδειγμα όπου ο φούξια κόμβος μετέχει στα περισσότερα ελάχιστα μονοπάτια (50 περισσότερα από τον κίτρινο) και έχει υψηλή betweenness centrality. Οι δύο κόμβοι μετέχουν σε ίδιο πλήθος τυχαίων περιπάτων και έχουν ίση pagerank centrality. Ο κίτρινος ωστόσο επειδή συνδέεται με κόμβους μεγάλο degree έχει ψηλότερο eigenvector centrality. Η closeness centrality είναι ίση και για τους δύο κόμβους



Σχήμα 2.

Παράδειγμα centralities.

Φούξια:	*Κίτρινος:*
$E_c = 0.14$	$E_c = 1.0$
$B_c = Y+50$	$B_c = Y$
$P_c = 0.083$	$P_c = 0.083$

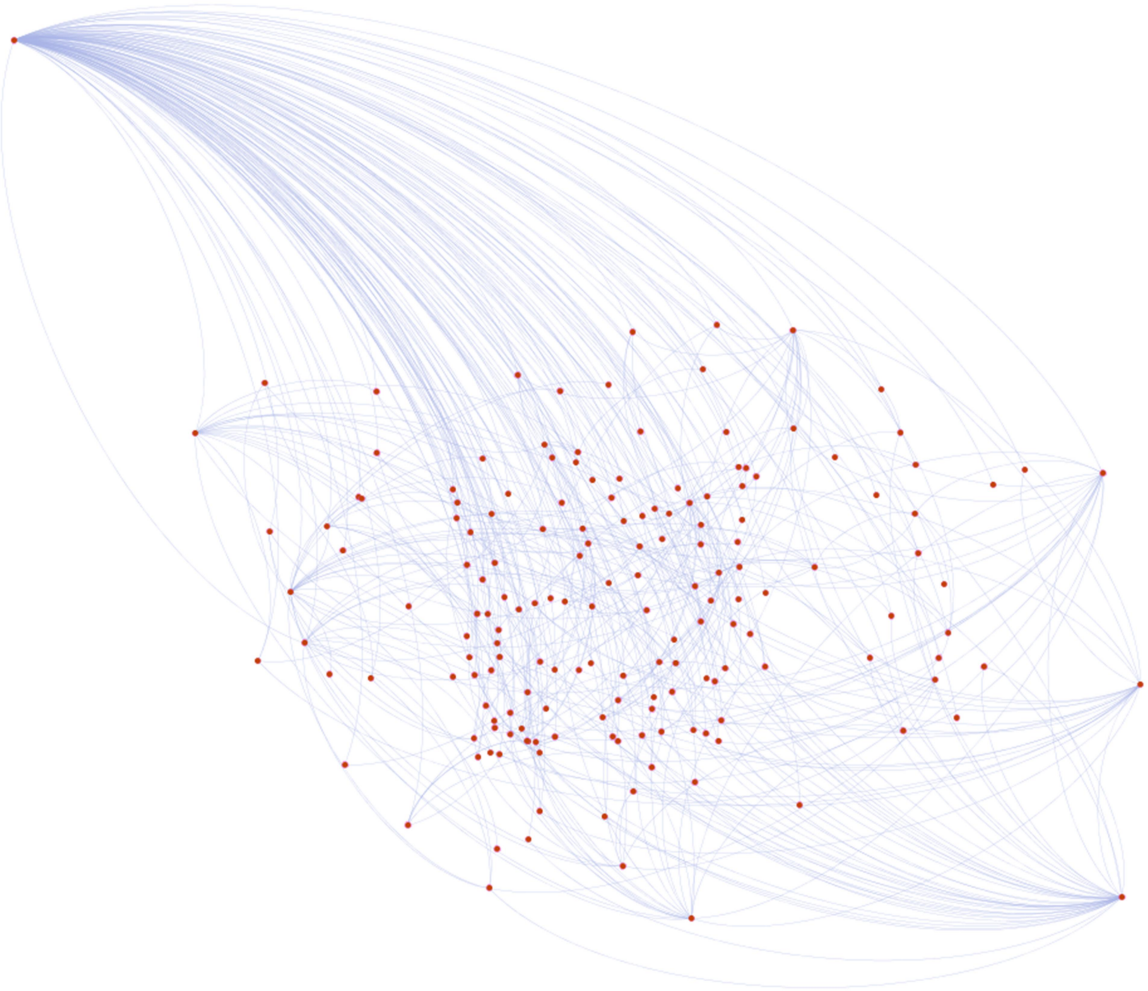
Στη συνέχεια, θα υπολογίσουμε την τιμή assortativity. Αυτό το μέγεθος μας δείχνει την τάση των κόμβων του δικτύου να συσχετίζονται με όμοιούς τους όσον αφορά το degree. Αυτό θα σήμαινε ότι άτομα με λίγους κοινούς φίλους με τον κεντρικό κόμβο, έχουν ως γείτονες κυρίως άτομα επίσης με λίγους κοινούς φίλους. Αυτό όμως θα μπορούσε να συμβαίνει μόνο αν το δίκτυο αποτελούταν από πολλές μικρές ομάδες συνδεδεμένων κόμβων με χαμηλό degree και λίγες μεγάλες ομάδες κόμβων με υψηλό degree. Επειδή κάτι τέτοιο δεν συμβαίνει, περιμένουμε ετερόφιλη τάση του δικτύου, δηλαδή χαμηλή τιμή του assortativity. Τέλος υπολογίζουμε την παράμετρο modularity του δικτύου. Η τιμή αυτή μας δείχνει το κατά πόσο εντός του δικτύου σχηματίζονται ομάδες ατόμων με μεγάλη πυκνότητα δεσμών εντός της ομάδας και μικρή εκτός. Στην περίπτωση του δικτύου που αναλύουμε είναι πολύ χρήσιμη αυτή η γνώση γιατί οι ομάδες αυτές αντιπροσωπεύουν τα διαφορετικά κοινωνικά σύνολα που ανήκει το άτομο υπό μελέτη. Γνωρίζοντας το μέγεθός τους και τον τρόπο που συνδέονται μεταξύ τους μπορούμε να βγάλουμε ορισμένα συμπεράσματα για την φύση τους, αν είναι εργασιακές, φιλικές ή οικογενειακές ομάδες. Με τα δεδομένα αυτά μπορούμε να βγάλουμε συμπεράσματα και για τα άτομα που τις απαρτίζουν.

3. Το δίκτυο

3.1 Κατασκευή του δικτύου

Για την κατασκευή του υπό μελέτη δικτύου, επιλέχθηκε ένα άτομο (κεντρικός κόμβος), με το οποίο δεν έχω καμία προσωπική σχέση ώστε να εξαχθούν από το διαδίκτυο όλα τα δεδομένα που είναι δυνατόν να συλλεχθούν υπό κανονικές συνθήκες. Στη συνέχεια καταγράφηκαν οι επαφές του σε τρία μέσα κοινωνικής δικτύωσης, στο facebook, στο twitter και στο LinkedIn.

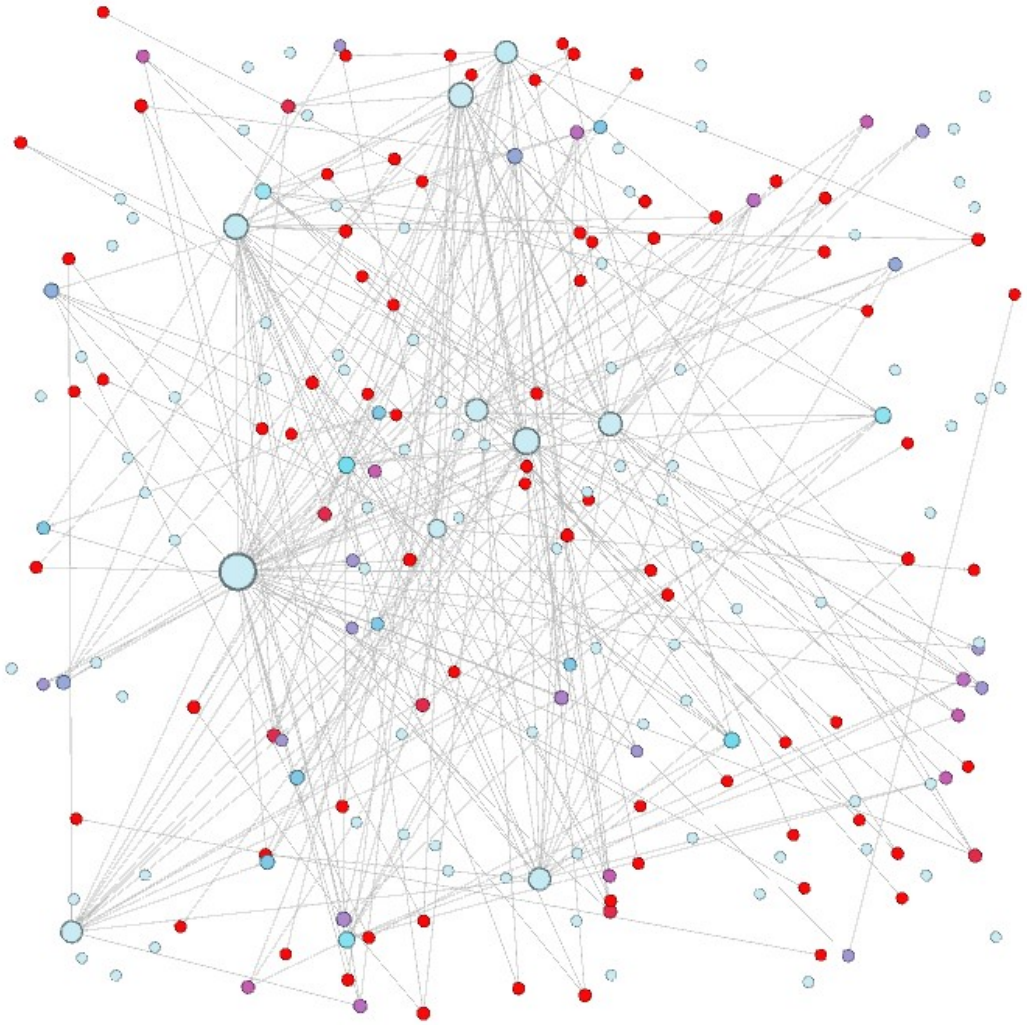
Συγκεκριμένα στο twitter επιλέχθηκαν όσοι ακολουθούν και ακολουθούνται από το άτομο που μελετάμε. Από το σύνολο των περιπτώσεων επίσης επιλέχθηκαν μόνο όσες συνυπάρχουν σε τουλάχιστον δύο από τα τρία αυτά δίκτυα. Αυτό το κριτήριο τέθηκε γιατί είναι πιο πιθανό να γνωρίζονται προσωπικά δύο άτομα ή να υπάρχει κάποιο ενδιαφέρον, εκτίμηση ή κάποιοι κοινοί τόποι μεταξύ τους όταν έχουν αναζητήσει ο ένας τον άλλο σε περισσότερα μέσα κοινωνικής δικτύωσης. Υπάρχουν σίγουρα και περιπτώσεις ατόμων που διαθέτουν λογαριασμό σε μόνο ένα δίκτυο. Αυτές όμως δεν λήφθηκαν υπόψη σε πρώτη φάση γιατί οι σημαντικές περιπτώσεις αυτού του τύπου θα αναδεικνύονταν από το ίδιο το δίκτυο λόγω του υψηλού degree τους. Στη συνέχεια κατασκευάστηκε το δίκτυο των ατόμων αυτών όπου κάθε ακμή αντιπροσωπεύει φιλία στο facebook ή στο LinkedIn ή σχέση αμοιβαίας ακολούθησης στο twitter. Οι ακμές του γράφου δεν έχουν ούτε κατεύθυνση ούτε βάρη. Στο δίκτυο αυτόν προστέθηκαν στη συνέχεια τα άτομα που αποτελούν κοινούς φίλους στους τρεις αυτούς χώρους μεταξύ κάποιου κόμβου και του κεντρικού ατόμου προς μελέτη και κατόπιν προστέθηκαν και οι ακμές μεταξύ των νεοεισαχθέντων κόμβων. Έτσι αναδείχθηκε ο τρόπος δικτύωσης των αρχικά επιλεγμένων ατόμων σε σχέση με το άτομο του οποίου το δίκτυο μελετάμε. Αξίζει να πούμε ότι από τις συνολικά 261 επαφές που είχε στα τρία μέσα δικτύωσης (104 LinkedIn, 140 facebook και 17 twitter), αφαιρώντας τις διπλές εγγραφές του ίδιου ατόμου σε πάνω από ένα μέσο,



Σχήμα 1. Το συνολικού δίκτυο, συμπεριλαμβανομένου του κεντρικού κόμβου που μελετάμε

μένουν συνολικά 230 άτομα. Το δίκτυο που κατασκευάστηκε με τη μέθοδο που προαναφέρθηκε έχει τελικά 169 κόμβους άρα 61 άτομα αποκλείστηκαν ως περιορισμένου ενδιαφέροντος για το πείραμά μας. Τελικά το δίκτυο που κατασκευάστηκε, έχει N = 169 κόμβους και k = 524 ακμές. Στο Σχήμα 2 αξίζει να παρατηρήσουμε πως, επιβεβαιώνοντας τον κανόνα, οι κόμβοι με υψηλό degree έχουν μικρό local clustering σε σχέση με τους κόμβους με μικρότερο degree. Για την περαιτέρω μελέτη του δικτύου επίσης, αφαιρέσαμε τον κεντρικό κόμβο, το άτομο δηλαδή του οποίου σχηματίσαμε το δίκτυο των φίλων, έτσι ώστε να λαμβάνουμε κανονικές τιμές για κάποια χαρακτηριστικά όπως η διάμετρος του δικτύου. Με τον κεντρικό κόμβο η διάμετρος ήταν ίση με 2, λογικό αφού μέσω αυτού μπορούσε να επιτευχθεί οποιοδήποτε μονοπάτι μεταξύ δύο τυχαίων κόμβων με 2 βήματα. Μετά από την αφαίρεσή

του, η διάμετρος είναι ίση με 8. Αυτό σημαίνει ότι το μεγαλύτερο ελάχιστο μονοπάτι μεταξύ δύο ατόμων στο συγκεκριμένο δίκτυο είναι ίσο με 8 βήματα, τόσο στο facebook όσο και στο twitter, η διάμετρος είναι ίση με 15. Ωστόσο η διαφορά αυτή εξηγείται καθώς το δίκτυο που μελετάμε αποτελεί ένα σύμπλεγμα κόμβων οι οποίοι έχουν εξ' ορισμού ως κοινό σημείο αναφοράς το κεντρικό άτομο της μελέτης. Η μέση απόσταση μεταξύ δύο κόμβων είναι ίση με L= 3.34 βήματα, επιβεβαιώνεται έτσι πως πρόκειται για ένα small world δίκτυο, αφού $L \propto \log N$. Επίσης υπάρχει ταύτιση με τη μέση απόσταση μεταξύ δύο ατόμων στο facebook, η οποία είναι ίση με 3.57 βήματα (ref. 35).



Σχήμα 2. Το δίκτυο που κατασκευάστηκε, οι κόμβοι είναι χρωματισμένοι ανάλογα με το τοπικό clustering, όσο πιο μικρό τόσο πιο ανοιχτό γαλάζιο και όσο πιο μεγάλο, τόσο πιο κόκκινο. Το μέγεθός τους είναι ανάλογο του degree τους.

Σχετικά με το δίκτυο ακόμα, υπολογίζουμε την πυκνότητά του, ίση με 0.036911 edges/vertex^2. Η πυκνότητα του facebook (ref. 33) και του twitter (ref. 34) είναι ίσες με 0.00040232 edges/vertex^2 και $6.061 * 10^{-5}$ edges/vertex^2. Η μεγαλύτερη κατά δύο τάξεις μεγέθους πυκνότητα από αυτή του facebook έχει να κάνει κυρίως με τον τρόπο κατασκευής του δικτύου, αφού χτίστηκε με κριτήριο την ύπαρξη ακμών (τουλάχιστον μίας) μεταξύ των κόμβων. Παρακάτω υπολογίζονται κάποια ακόμα χαρακτηριστικά του δικτύου που χρειάζονται για τον σκοπό μας.

3.2 Ανάλυση του δικτύου

3.2.1 Degree

Ύστερα από την κατασκευή του δικτύου, ως πίνακα μεγέθους 169x169, με άθροιση των στοιχείων της κάθε γραμμής, υπολογίστηκε το degree του εκάστοτε κόμβου. Αυτό κυμαίνεται από 0 για τους κόμβους που δεν συνδέονται με κάποιον άλλο (δεν έχουν κοινούς φίλους), έως 42. Η κατανομή της πιθανότητας του degree, είναι εκθετική, και προσεγγίζεται από την καμπύλη: $y = 0.3287 * x^{-1.233}$. Αλλιώς σε λογαριθμική κλίμακα, $y = -1.233 * x - 0.4832$. Η προσέγγιση έγινε στο excel. Επίσης με την μέθοδο των ελαχίστων τετραγώνων για την εκθετική κατανομή, κάνοντας τους υπολογισμούς στο matlab, προέκυψε αρκετά κοντινό αποτέλεσμα, $y = 0.8958 * x^{-1.66}$, σύμφωνα με τον τύπο:

$$y = e^{\alpha} * x^{\beta}$$

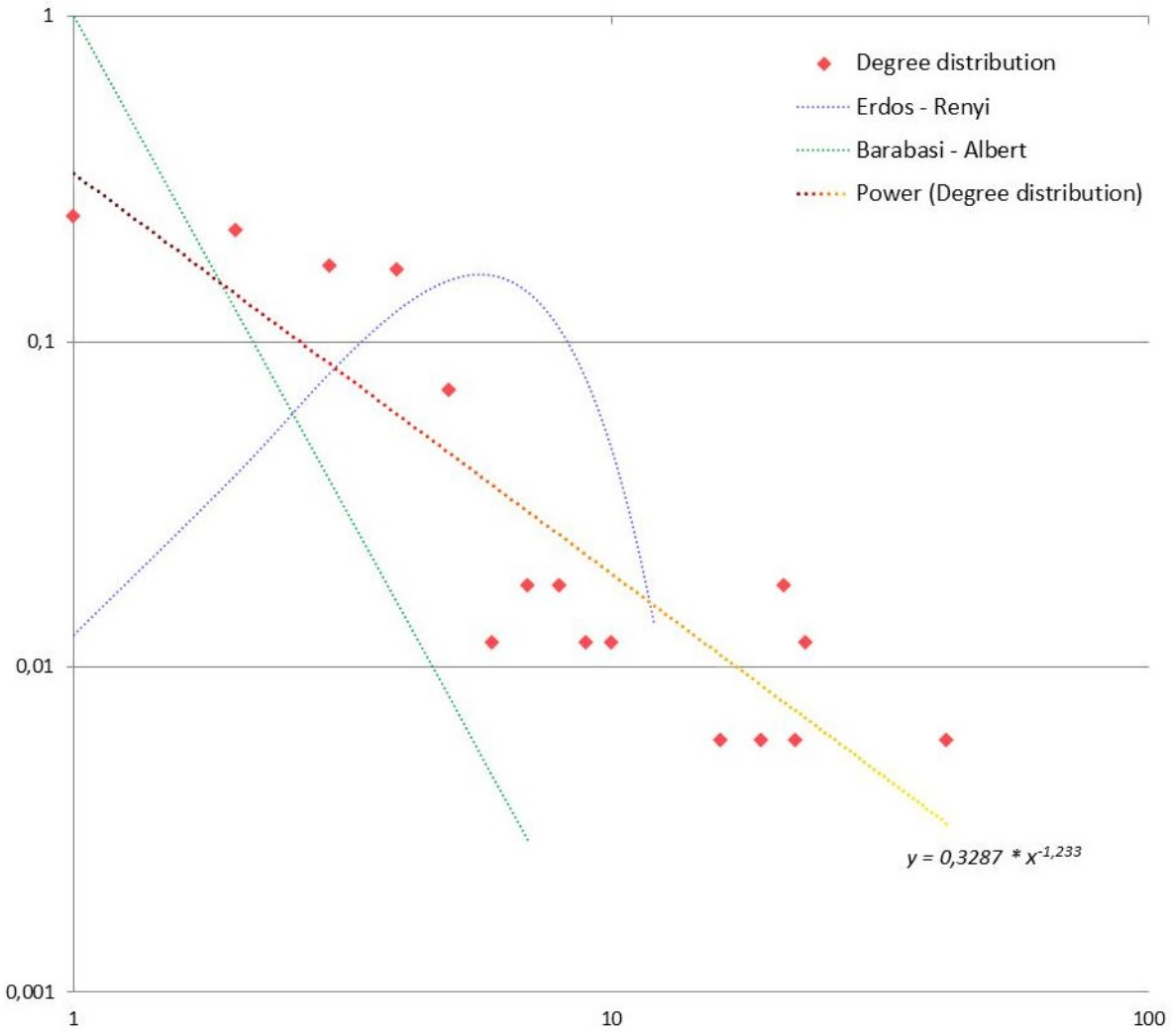
Όπου:

$$\beta = \frac{N * \sum_{i=1}^{N}(lnx_i * lny_i) - \sum_{i=1}^{N}(lnx_i) * \sum_{i=1}^{N}(lny_i)}{N * \sum_{i=1}^{N}(lny_i)^2 - \left(\sum_{i=1}^{N} lnx_i\right)^2}$$

και

$$\alpha = \frac{\sum_{i=1}^{N}(lny_i) - \beta * \sum_{i=1}^{N}(lnx_i)}{N}$$

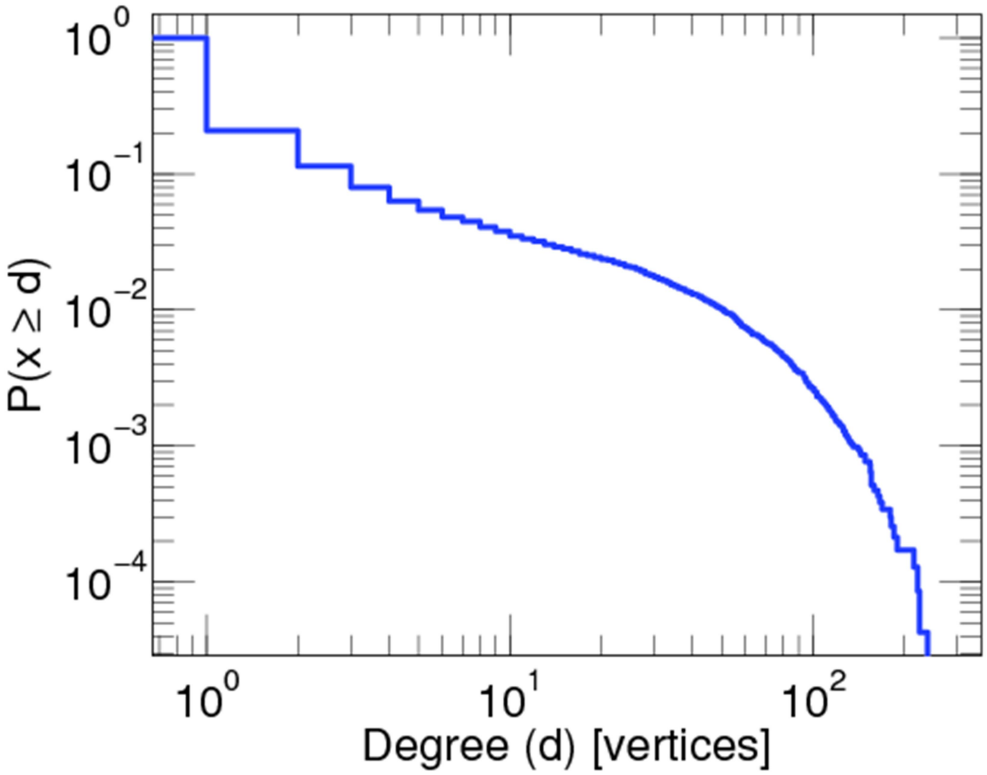
Όπου x_i, οι τιμές που λαμβάνει το degree και y_i οι αντίστοιχες πιθανότητες.



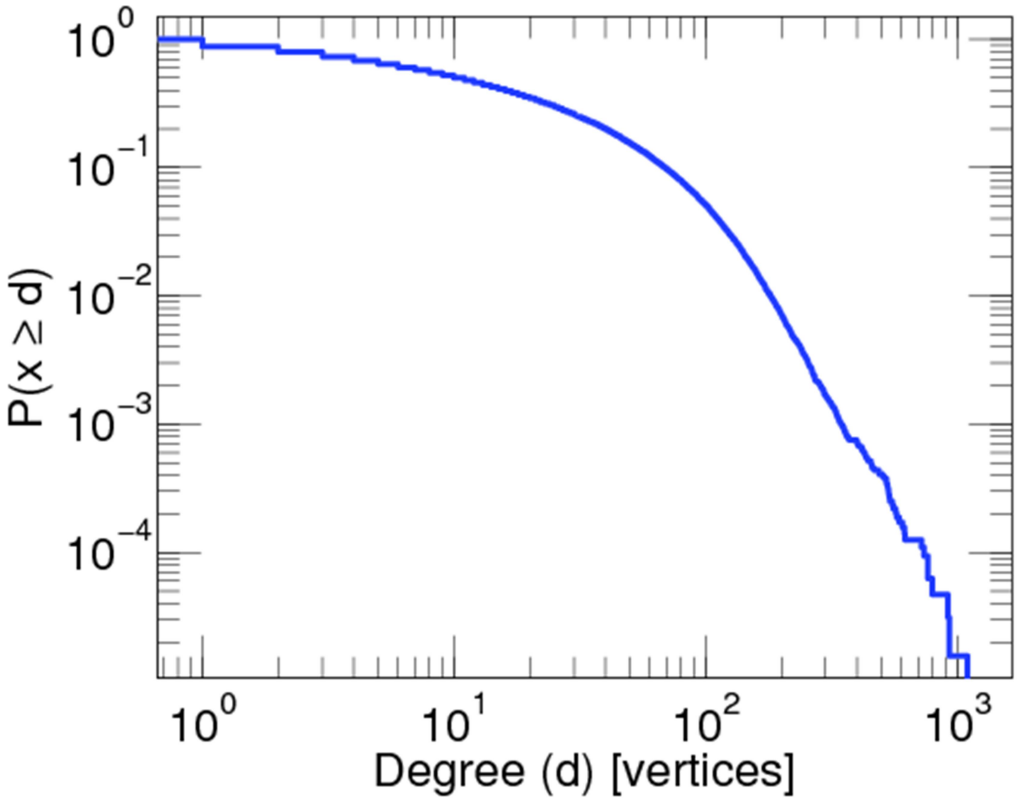
Σχήμα 3. Σε λογαριθμική κλίμακα, στον οριζόντιο άξονα βρίσκεται το degree d και στον κατακόρυφο η πιθανότητα P(x ≥ d).

Στο σχήμα 3, συγκρίνεται η κατανομή της πιθανότητας του degree με τις κατανομές δύο αντίστοιχων τυχαίων δικτύων. Το Erdos-Renyi, δεν ακολουθεί εκθετική κατανομή αλλά κατανομή poisson, σε αντίθεση το Barabasi Albert ακολουθεί εκθετική κατανομή. Παρατηρούμε πως είναι πολύ πιο κοντά στην ιδανική περίπτωση της ευθείας $y = x^{-1}$ η κατανομή του δικτύου που εξετάζουμε από αυτή του τυχαίου. Στα σχήματα 4 και 5 παρατίθενται οι κατανομές των δικτύων φιλίας στο facebook και ακολούθων στο twitter. Παρατηρούμε πως υπάρχει απόκλιση μεταξύ των κατανομών στα δίκτυα αυτά

και του δικτύου που μελετάμε. Αυτή θα την αποδώσουμε κυρίως στην κλίμακα των υπό μελέτη δικτύων, καθώς αυτά από τα οποία έχουν εξαχθεί τα γραφήματα έχουν πολύ μεγαλύτερο πλήθος κόμβων και προσεγγίζουν καλύτερα στατιστικά την καμπύλη. Επίσης το δίκτυο που μελετάμε περιέχει τις συνδέσεις μεταξύ ατόμων και στο facebook αλλά και στο twitter γεγονός που οδηγεί στην εξαγωγή μιας κοινής καμπύλης. Το μέσο degree ακόμα είναι 3.101 edges/vertex. Εδώ η σύγκριση με το facebook ή το twitter δεν έχει νόημα καθώς δεν πρόκειται για ολοκληρωμένα συμπλέγματα γύρω από τον κάθε κόμβο αλλά για μια σύνθεση επιλεγμένων ατόμων. Για τον λόγο αυτό παρατηρούμε και μεγάλη απόκλιση από το μέσο degree στο facebook (25.64 edges/vertex). Σε σχέση με το twitter, υπάρχει σχετική ταύτιση αλλά είναι τυχαία (2.8328 edges/vertex).



Σχήμα 4. Facebook (ref. 33)

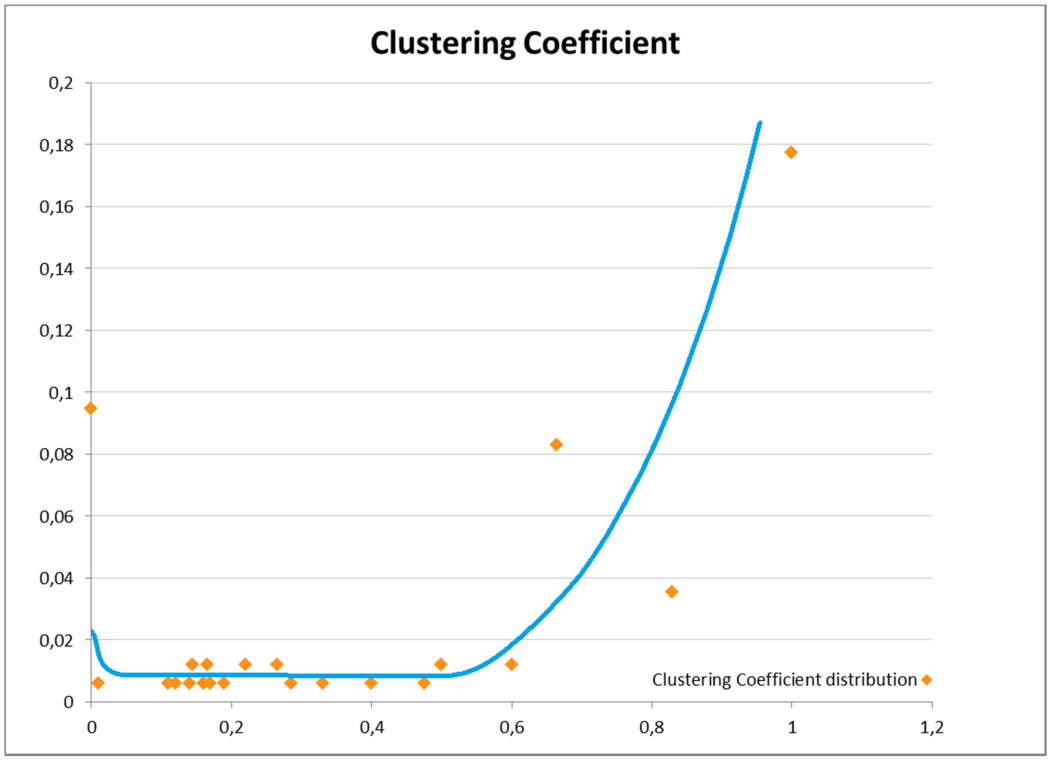


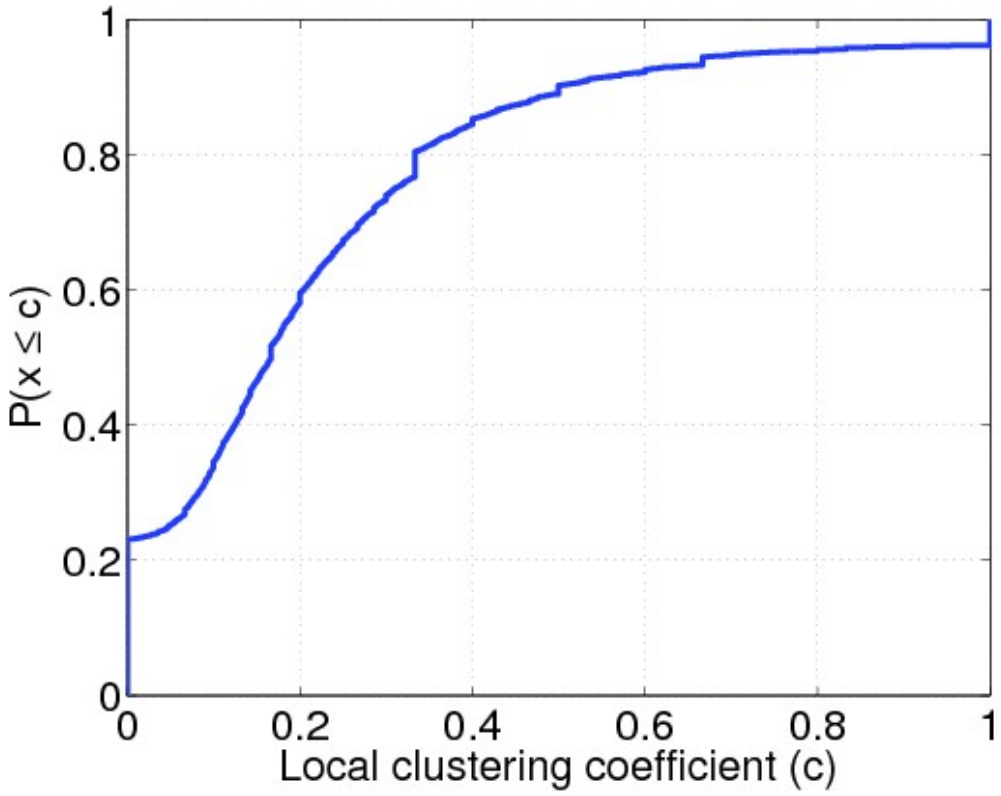
Σχήμα 5. Twitter (ref. 34)

3.2.2 Clustering

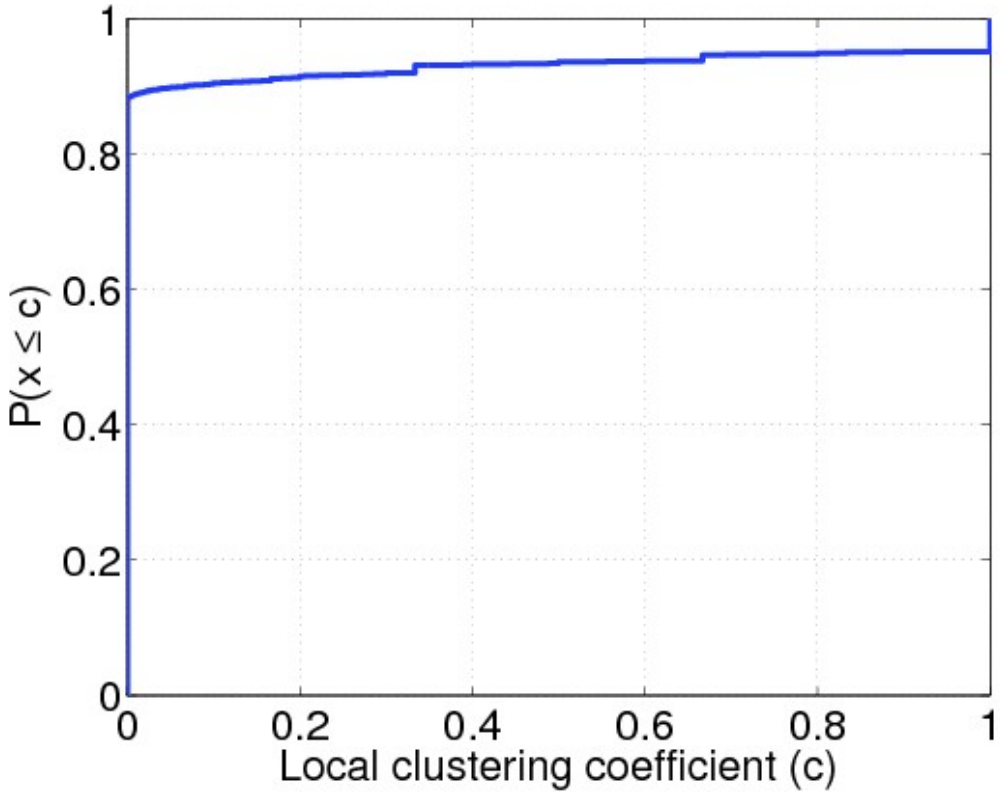
Ο τοπικός συντελεστής clustering, συμβολίζει το κατά πόσο σχηματίζονται τρίγωνα μεταξύ των φίλων του εκάστοτε κόμβου. Αυτός υπολογίστηκε κατά μέσο όρο ίσος με 29.98%. Στην περίπτωση του facebook, ισούται με 14.8% (ref. 33) και σε αυτή του twitter ισούται με 2.15%. Η απόκλιση οφείλεται κυρίως στο κοινό σημείο αναφοράς των ατόμων που απαρτίζουν το δίκτυο. Αυτό καθιστά πολύ πιθανότερη την μεταξύ τους αλληλεπίδραση.

Σχήμα 6. Προσέγγιση της κατανομής του local clustering coefficient, κάτω σε λογαριθμικό κατακόρυφο άξονα. Η καμπύλη χαράχτηκε προσεγγιστικά ως οπτικός οδηγός στον αναγνώστη.





Σχήμα 7. Facebook (ref. 33)



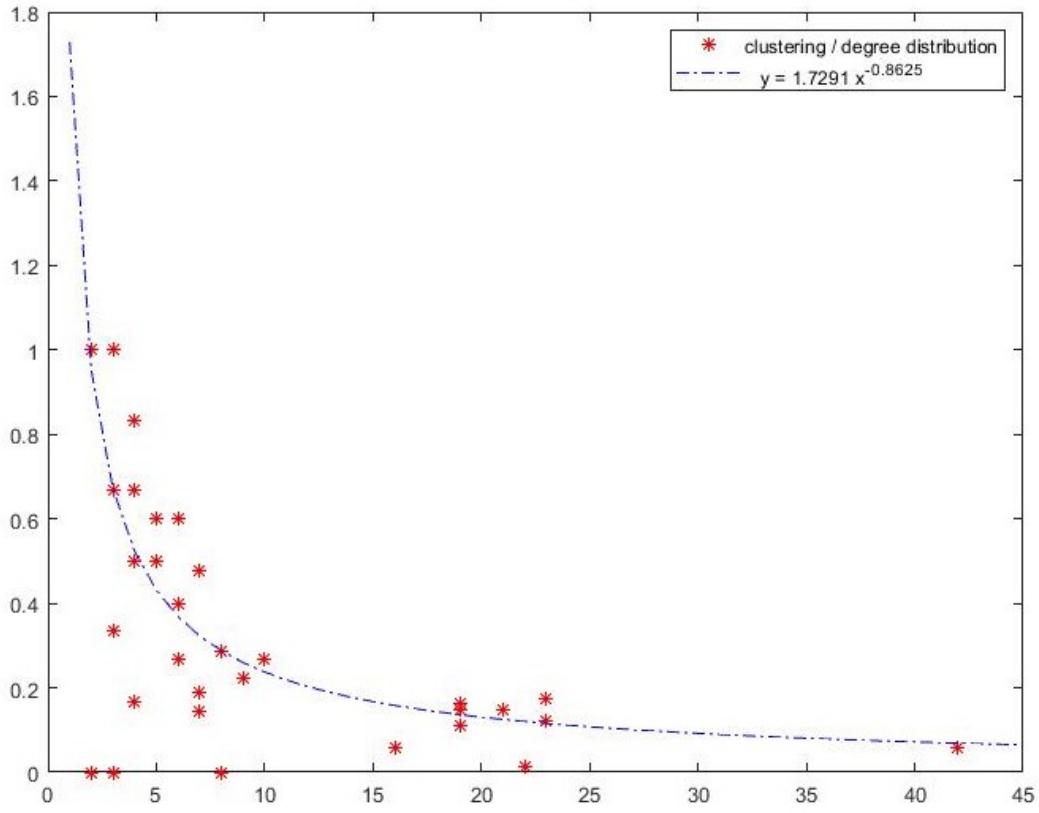
Σχήμα 8. Twitter (ref. 34)

Παρατηρούμε μεγάλη απόκλιση από τις αντίστοιχες κατανομές των facebook και twitter, την οποία αποδίδουμε στα ίδια αίτια με την περίπτωση του degree.

Στο σχήμα 9, φαίνεται η εξάρτηση του local clustering coefficient από το degree. Σύμφωνα με την προσέγγιση που κάναμε, αυτή προκύπτει ως:

$$C(k) = 1.7291 * k^{-0.8625}$$

Η εκθετική εξάρτηση του clustering coefficient από το degree, $C(k) \sim k^{-\gamma}$, έχει συσχετιστεί με μία ιεραρχική δομή στο δίκτυο, με τον εκθέτη γ να αποκαλείται ιεραρχικός εκθέτης (hierarchical exponent). Έχει βρεθεί πως η συγκεκριμένη εξάρτηση οφείλεται σε κάποιο βαθμό στον συσχετισμό των degree εντός του δικτύου, όπου κόμβοι με υψηλό degree συνδέονται με κόμβους με χαμηλό degree (ref. 36).

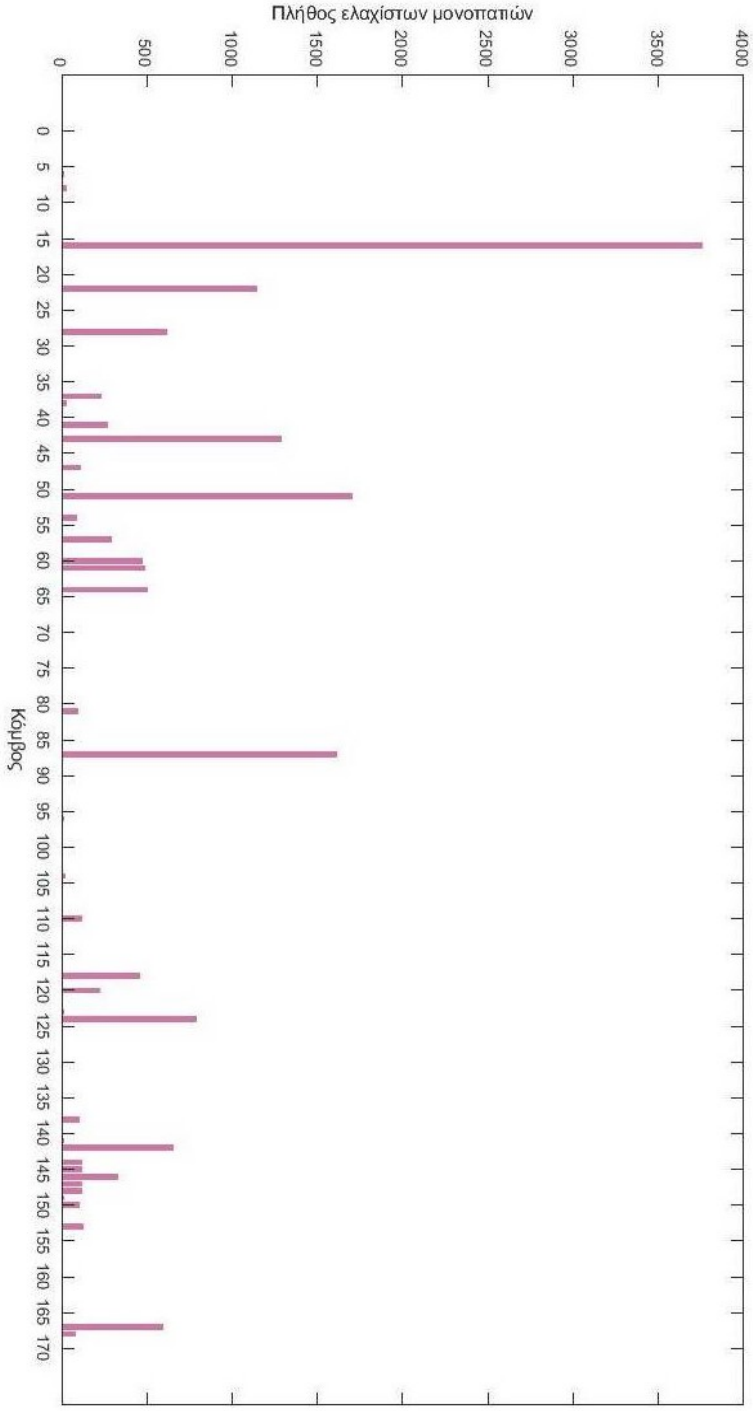


Σχήμα 9. Στον κατακόρυφο άξονα έχουμε το local clustering coefficient και στον οριζόντιο το degree.

Παρακάτω υπολογίζουμε μερικά χαρακτηριστικά του δικτύου που θα μας βοηθήσουν να ξεχωρίσουμε ορισμένους κόμβους βάσει της σημαντικότητάς τους μέσα στο δίκτυο. Για τον λόγο αυτό θα χρησιμοποιήσουμε ορισμένα μέτρα της κεντρικότητας (centrality) των κόμβων. Υπάρχουν πολλά διαφορετικά μέτρα για την κεντρικότητα ενός κόμβου εντός του δικτύου. Εμείς επιλέγουμε μόνο τέσσερα συγκεκριμένα τα οποία έχουν να κάνουν μόνο με την τοπολογία του δικτύου, για την οποία έχουμε δεδομένα. Παράλληλα όμως προσεγγίζουμε την έννοια της κεντρικότητας από διαφορετικές σκοπιές όπως φαίνεται παρακάτω.

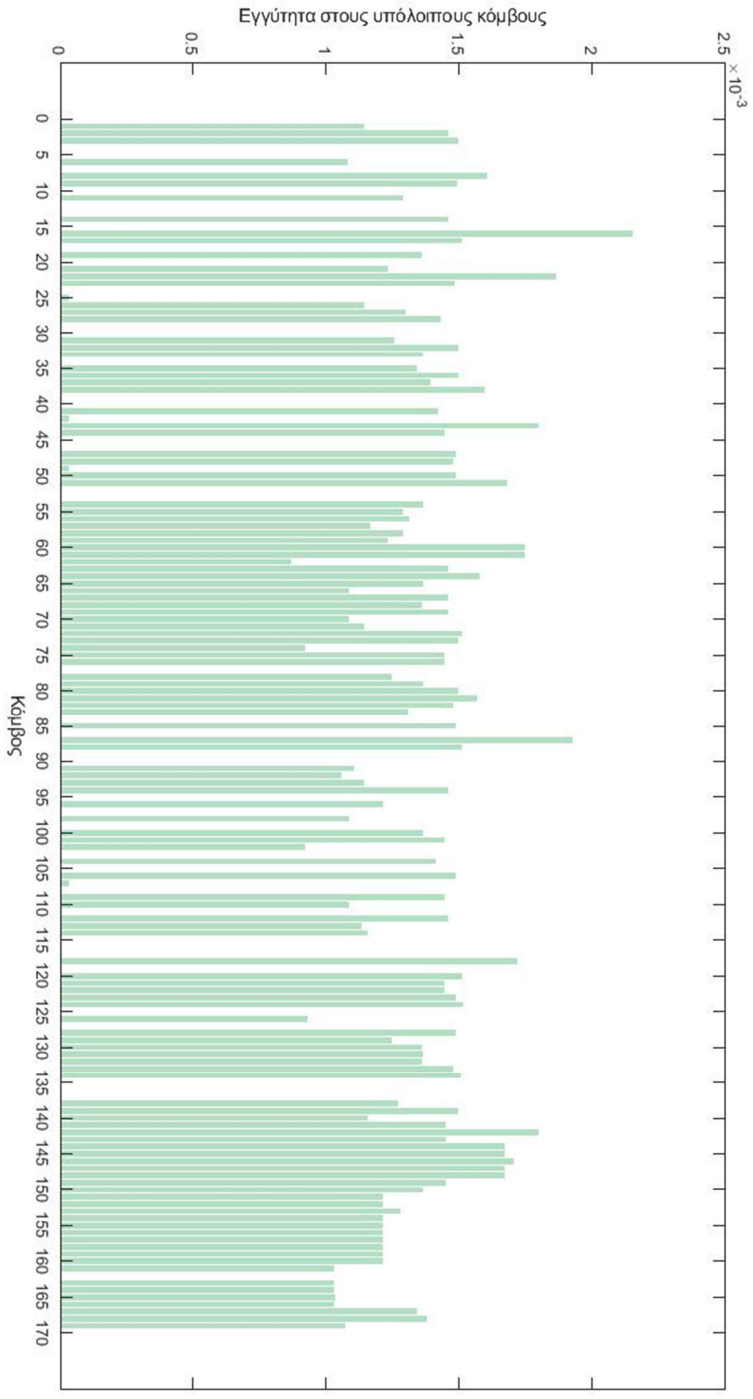
3.2.3 Betweenness centrality

Στον υπολογισμό της betweenness centrality, μετράμε πόσο συχνά ένας κόμβος εμφανίζεται στο ελάχιστο μονοπάτι μεταξύ δύο άλλων κόμβων του γράφου. Δεδομένου ότι μπορεί να υπάρχουν πολλά ελάχιστα μονοπάτια μεταξύ των κόμβων *s* και *t*, η κεντρικότητα ενός κόμβου *u* είναι ίση με (ref. 45): $c(u) = \sum_{s,t \neq u} \frac{n_{st}(u)}{N_{st}}$. Όπου $n_{st}(u)$ είναι το πλήθος ελαχίστων μονοπατιών μεταξύ των κόμβων *s* και *t* που διέρχονται από τον *u*, και N_{st} είναι το συνολικό πλήθος ελαχίστων μονοπατιών που συνδέουν τους *s* και *t*. Στην περίπτωση του δικτύου που μελετάμε, θα δούμε μεγάλες διακυμάνσεις γιατί υπάρχουν λίγοι εξαιρετικά κεντρικοί κόμβοι ενώ μεγάλο πλήθος λιγότερο δικτυωμένων. Είναι ακόμα πολλοί αυτοί με degree ίσο με 0 ή 1, οι οποίοι μπορούν να μετέχουν σε 0 ή 1 ελάχιστα μονοπάτια αντίστοιχα.



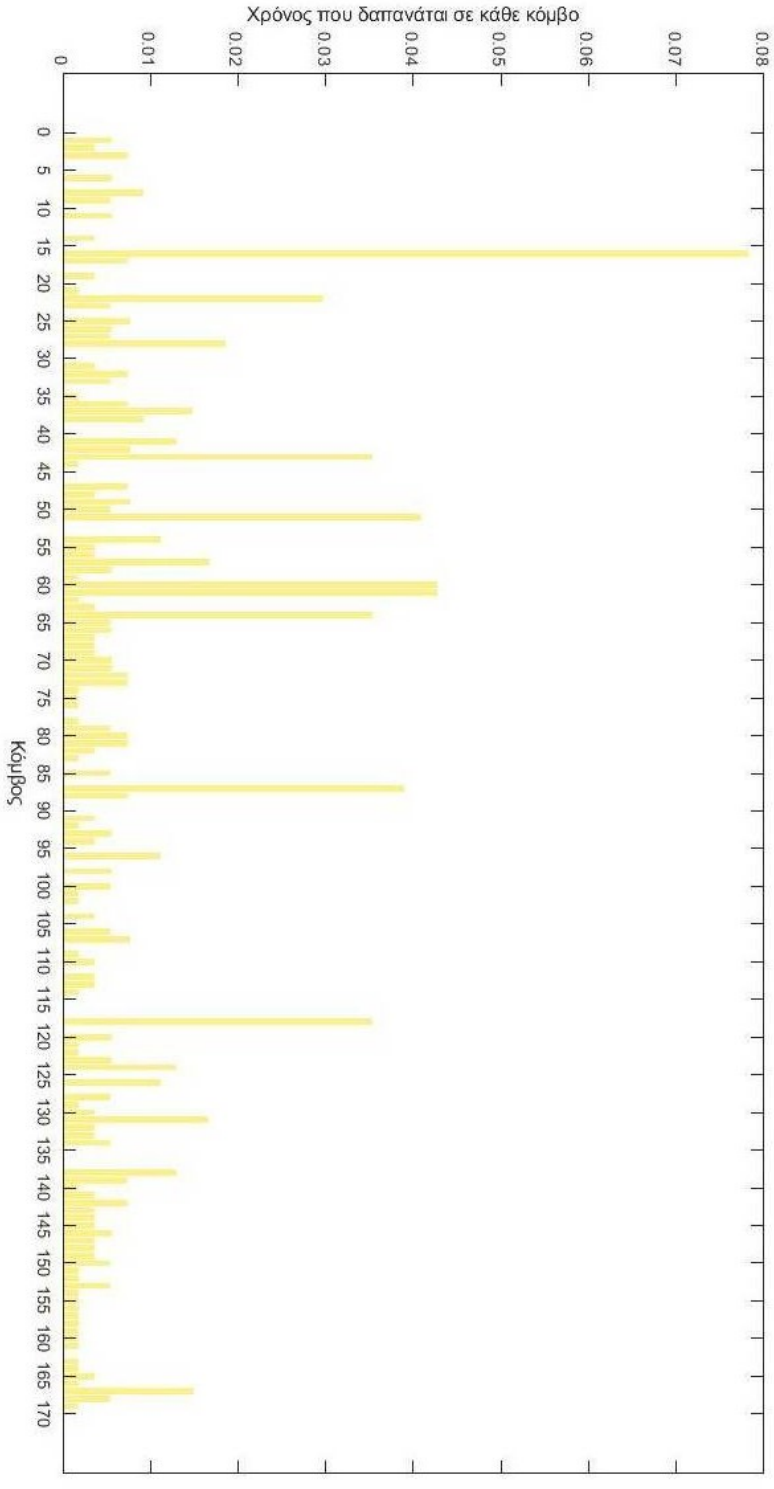
3.2.4 Closeness centrality

Για να υπολογίσουμε τον βαθμό εγγύτητας ενός κόμβου, υπολογίζουμε το αντίστροφο της απόστασης του κόμβου από όλους τους προσβάσιμους από αυτόν κόμβους. Αν δεν είναι όλοι οι κόμβοι προσβάσιμοι, όπως στο δίκτυο που εξετάζουμε, το μέτρο της εγγύτητας υπολογίζεται ως (ref. 45): $c(i) = (\frac{A_i}{N-1})^2 \frac{1}{c_i}$. Όπου A_i το πλήθος των προσβάσιμων κόμβων από τον κόμβο *i*, *N* το συνολικό πλήθος κόμβων, και c_i είναι το άθροισμα των αποστάσεων από τον *i* προς όλους τους προσβάσιμούς του κόμβους. Αν κανένας κόμβος δεν είναι προσβάσιμος από τον *i*, το $c(i)$ προκύπτει ίσο με 0. Η διάμετρος είναι ίση με 8 και η μέση απόσταση μεταξύ δύο κόμβων ίση με 3.34. Τα δύο μεγέθη είναι κοντινά μεταξύ τους οπότε οι αποκλίσεις θα είναι μικρές για τους κόμβους με μη μηδενικές τιμές.



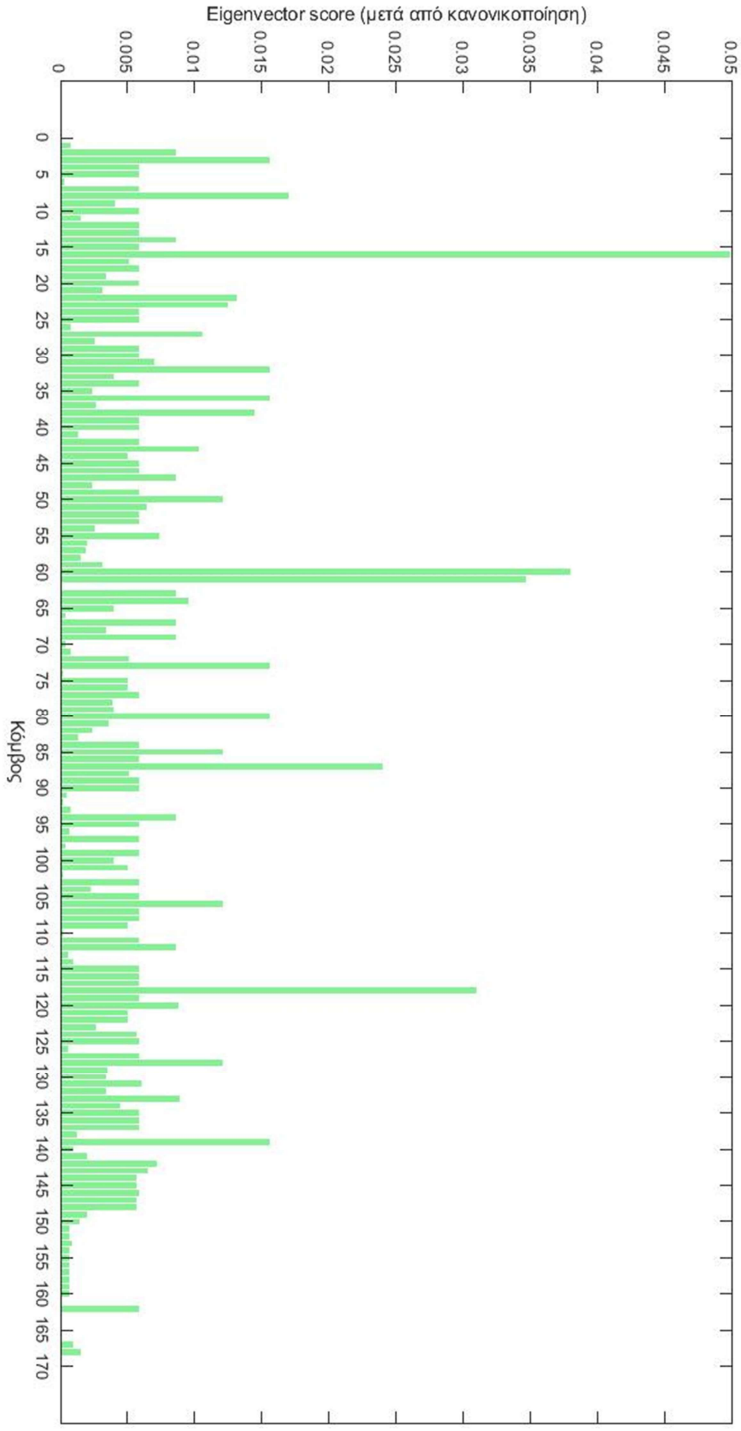
3.2.5 Pagerank centrality

Εδώ υπολογίζουμε τον μέσο χρόνο που δαπανάται σε κάθε κόμβο κατά τη διάρκεια ενός τυχαίου περίπατου στο δίκτυο (ref. 44). Σε κάθε κόμβο του δικτύου, είτε επιλέγεται ισοπίθανα ένας από τους γείτονές του ως επόμενος, με πιθανότητα *p*, είτε επιλέγεται ισοπίθανα ένας από τους μη γείτονές του, με πιθανότητα *1 – p*. Για τον δικό μας σκοπό, επιλέξαμε *p = 1*, ώστε να επιλέγεται πάντα ένας από τους γείτονες κατά τη διάρκεια του περιπάτου στο δίκτυο. Η pagerank centrality σαν ιδέα είναι κοντά στην betweenness centrality. Έχει όμως την διαφορά πως μετράει τη συμμετοχή του κόμβου στο σύνολο των μονοπατιών του δικτύου και όχι μόνο στα ελάχιστα. Πάντως δεν παύουμε να περιμένουμε αποτελέσματα κοντινά με αυτά του 3.2.3.



3.2.6 Eigenvector centrality

Αυτός ο τύπος μέτρησης της κεντρικότητας τέλος, χρησιμοποιεί το ιδιοδιάνυσμα που αντιστοιχεί στην μέγιστη τιμή του πίνακα του δικτύου. Σχετικές τιμές δίδονται σε όλους τους κόμβους, με βάσει το κριτήριο πως η τιμή ενός κόμβου είναι μεγαλύτερη όταν αυτός συνδέεται με πιο υψηλόβαθμους κόμβους. Οι τιμές κανονικοποιούνται ώστε το συνολικό τους άθροισμα να είναι ίσο με 1. Αν υπάρχει πλήθος αποσυνδεδεμένων τμημάτων, τότε υπολογίζεται η κεντρικότητα ξεχωριστά για το κάθε τμήμα. Στη συνέχεια προσαρμόζεται το αποτέλεσμα βάσει του ποσοστού τον κόμβων που συμμετέχουν στο συγκεκριμένο τμήμα. Στο δικό μας δίκτυο υπάρχουν δύο μικρά αποσυνδεδεμένα τμήματα. Επίσης η κεντρικότητα των απομονωμένων κόμβων ισούται με $^1/_N$ όπου *N*, το πλήθος όλων των κόμβων (ref. 45).



3.2.7 Assortativity

Η τιμή του assortativity για το δίκτυο, υποδηλώνει το κατά πόσο οι κόμβοι τείνουν να συνδέονται με άλλους που έχουν παρόμοια συμπεριφορά με τους ίδιους. Οι τιμές που παίρνει κυμαίνονται μεταξύ -1 και 1 και προκύπτουν από την σχέση του degree ενός κόμβου με αυτό των γειτόνων του. Για μεγάλες τιμές το δίκτυο παρουσιάζει ομοιοφιλία (highly assortative), οι κόμβοι δηλαδή τείνουν να συνδέονται με όμοιούς τους κόμβους. Για τιμές κοντά στο 0 παρουσιάζει ουδέτερη συμπεριφορά και για μικρές τιμές παρουσιάζει ετεροφυλία. Για το δίκτυο που μελετάμε, η τιμή assortativity προκύπτει ίση με A = -0.4319. Πρόκειται λοιπόν για ένα δίκτυο με έντονη τάση ετεροφιλίας. Η τιμή υπολογίστηκε από τον τύπο (Shao, 2010):

$$r = \frac{\frac{1}{E}\sum_{j>i} k_i k_j k_{ij} - \left[\frac{1}{E}\sum_{j>i}\frac{1}{2}\left(k_i + k_j\right)A_{ij}\right]^2}{\frac{1}{E}\sum_{j>i}\frac{1}{2}\left(k_i^2 + k_j^2\right)A_{ij} - \left[\frac{1}{E}\sum_{j>i}\frac{1}{2}\left(k_i + k_j\right)A_{ij}\right]^2}$$

Όπου *E* Το συνολικό πλήθος ακμών του στοιχείου, A_{ij}, τα στοιχεία του πίνακα του δικτύου (adjacency matrix) και k_i το degree του κόμβου *i*. Στη συνέχεια, υπολογίστηκε ο τοπικός παράγοντας του assortativity για κάθε κόμβο *n* του δικτύου. Αυτός υπολογίζεται ως (*Reik & Donges, 2012*):

$$\rho_n = \frac{j(j+1)(\bar{k} - \mu_q)}{2M\sigma_q^2}$$

Όπου *j*, ο πλεονάζων βαθμός (excess degree) του κόμβου *n*, ίσος με $k_n - 1$, $\bar{k}$ το μέσο degree των γειτόνων του *n*, μ_q η αναμενόμενη τιμή της κατανομής του excess degree, *M* το συνολικό πλήθος ακμών και σ_q^2, η διασπορά της κατανομής του excess degree. Αλλιώς ο τοπικός παράγοντας του assortativity, μπορεί να περιγραφεί ως: $\rho_n = \frac{\alpha_n - \beta_n}{\sigma_q^2}$, όπου $\beta_n = (j+1)\frac{\mu_q^2}{2M}$. Ο όρος αυτός κανονικοποιήθηκε ώστε να ισχύει $r = \sum_{n=1}^{N}\rho_n$. Η κανονικοποίηση αυτή δεν επηρεάζει το αποτέλεσμα της έρευνάς μας καθώς μας ενδιαφέρει η σύγκριση μεταξύ των κόμβων. Πολλαπλασιάζοντας τον όρο β_n με μία σταθερά, για κάθε n, μετατοπίσαμε την καμπύλη προς τα πάνω σε βαθμό ανάλογο της τιμή του local assortativity (Σχήμα 10).

Παρατηρούμε (σχήμα 11), ότι οι κεντρικοί κόμβοι (hubs), αυτοί δηλαδή με το μεγαλύτερο degree, όπως επιβεβαιώνεται από μελέτη σε πραγματικά δίκτυα μεγάλης κλίμακας, τείνουν να έχουν μικρή τιμή assortativity. Αυτό αποτελεί πρόβλημα της μεθόδου υπολογισμού του local assortativity (Piraveenan et al., 2010). Για τον λόγο αυτό, εξετάζουμε τους κεντρικούς κόμβους μεμονωμένα για να διαπιστώσουμε αν υπάρχει το φαινόμενο του ισχυρού κλαμπ. Αν δηλαδή τείνουν να έχουν πολλούς δεσμούς μεταξύ τους. Γι' αυτούς μετράμε το πλήθος ακμών προς τους υπόλοιπους κεντρικούς κόμβους (Πίνακας 1).

Ταυτότητα Κόμβου	**16**	**22**	**43**	**51**	**60**	**61**	**64**	**87**	**112**
Πλήθος ακμών	**5**	**2**	**4**	**1**	**3**	**4**	**2**	**5**	**2**

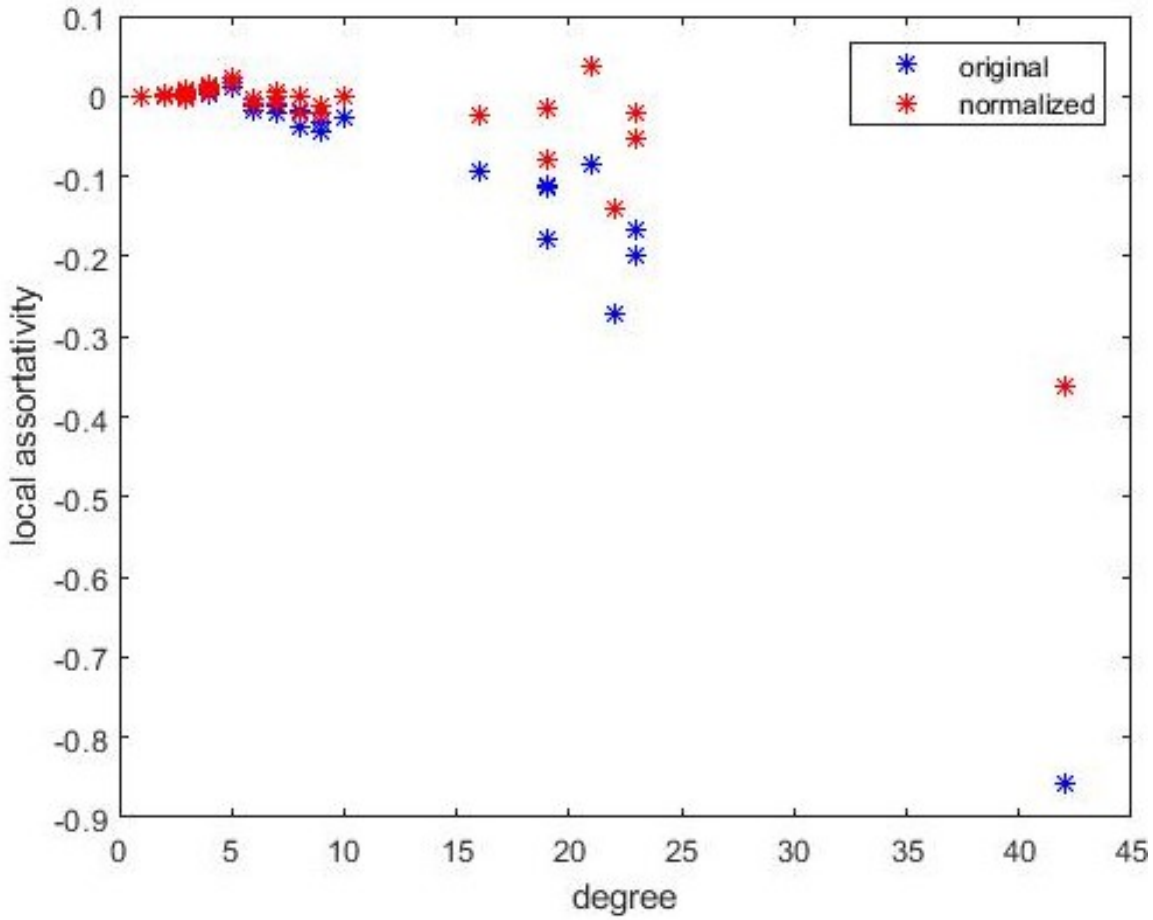
Πίνακας 1. Πλήθος ακμών κεντρικών κόμβων προς άλλους κεντρικούς κόμβους.

Έχουμε επιλέξει ως κεντρικούς εννιά κόμβους, με το κριτήριο να έχουν degree > 10. Για κάθε έναν από αυτούς υπάρχουν δυνητικά οκτώ ακμές προς τους υπολοίπους. Έτσι κατασκευάζουμε σαν νέο μέτρο του local assortativity, για τις ανάγκες της έρευνας μας, το $\hat{\rho} = (\hat{\kappa} - 4)/4$, όπου $\hat{\kappa}$, το πλήθος ακμών προς άλλους κεντρικούς κόμβους. Παρατηρούμε στον πίνακα 2 πως όντως υπάρχει σημαντική απόκλιση ανάμεσα στην προσέγγισή μας $(\hat{\rho})$ και στην τυπική τιμή (ρ). Για τον λόγο αυτό θα λάβουμε υπόψη την τιμή που υπολογίστηκε βάσει της βιβλιογραφίας, μόνο για τους μη κεντρικούς κόμβους με degree < 11 (Σχήμα 12).

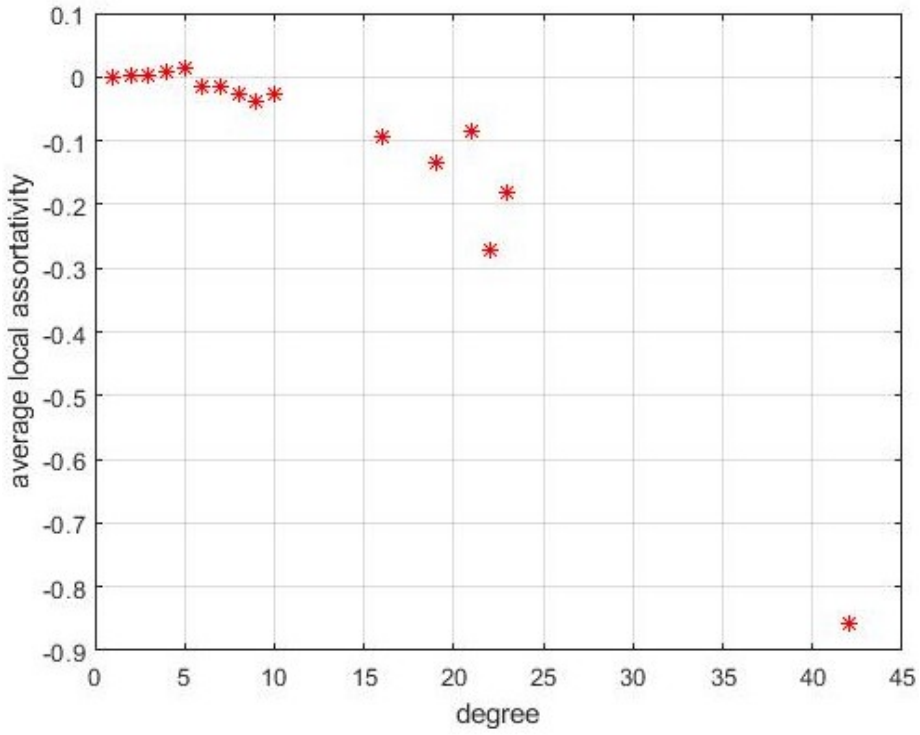
Το αξιοπερίεργο στην κατανομή του assortativity, είναι πως μεγαλύτερη τιμή λαμβάνουν οι κόμβοι με degree ίσο με 5 (σχήμα 12), ενώ η πιθανότητα να συναντήσουμε κόμβο με *k = 5* είναι μικρότερη από κάθε άλλη περίπτωση μονοψήφιας τιμής *k* και ίση με τις πιθανότητες των *k = 8* και *9.* Αυτό μπορεί να οφείλεται στην ύπαρξη κάποιων ομάδων συνδεδεμένων μεταξύ τους ατόμων με degree ίσο με 5.

Ταυτότητα Κόμβου	16	22	43	51	60	61	64	87	112
Local Assortativity $\widehat{\rho}$	0.25	-0.5	0	-0.75	-0.25	0	-0.5	0.25	-0.5
Local Assortativity $\boldsymbol{\rho}$	-0.363	-0.024	-0.014	-0.143	-0.021	-0.053	-0.079	0.036	0.003

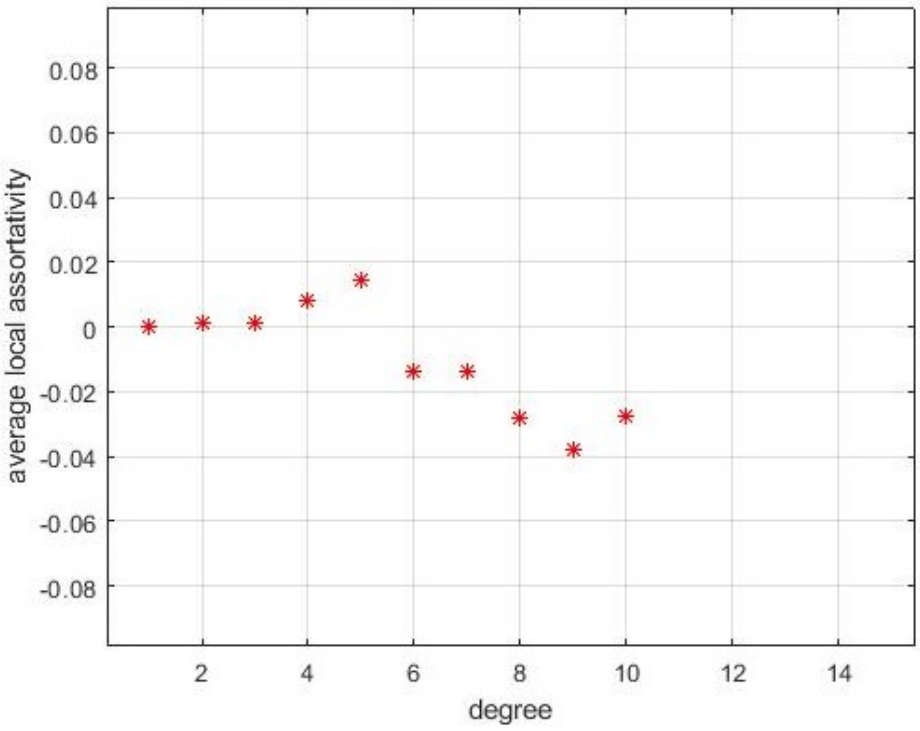
Πίνακας 2. Σύγκριση μέτρων Local assortativity για το μοντέλο που κατασκευάσαμε και αυτό που προτείνει η βιβλιογραφία.



Σχήμα 10.



Σχήμα 11.



Σχήμα 12. Λεπτομέρεια του γραφήματος στο σχήμα 11.

3.2.8 Modularity

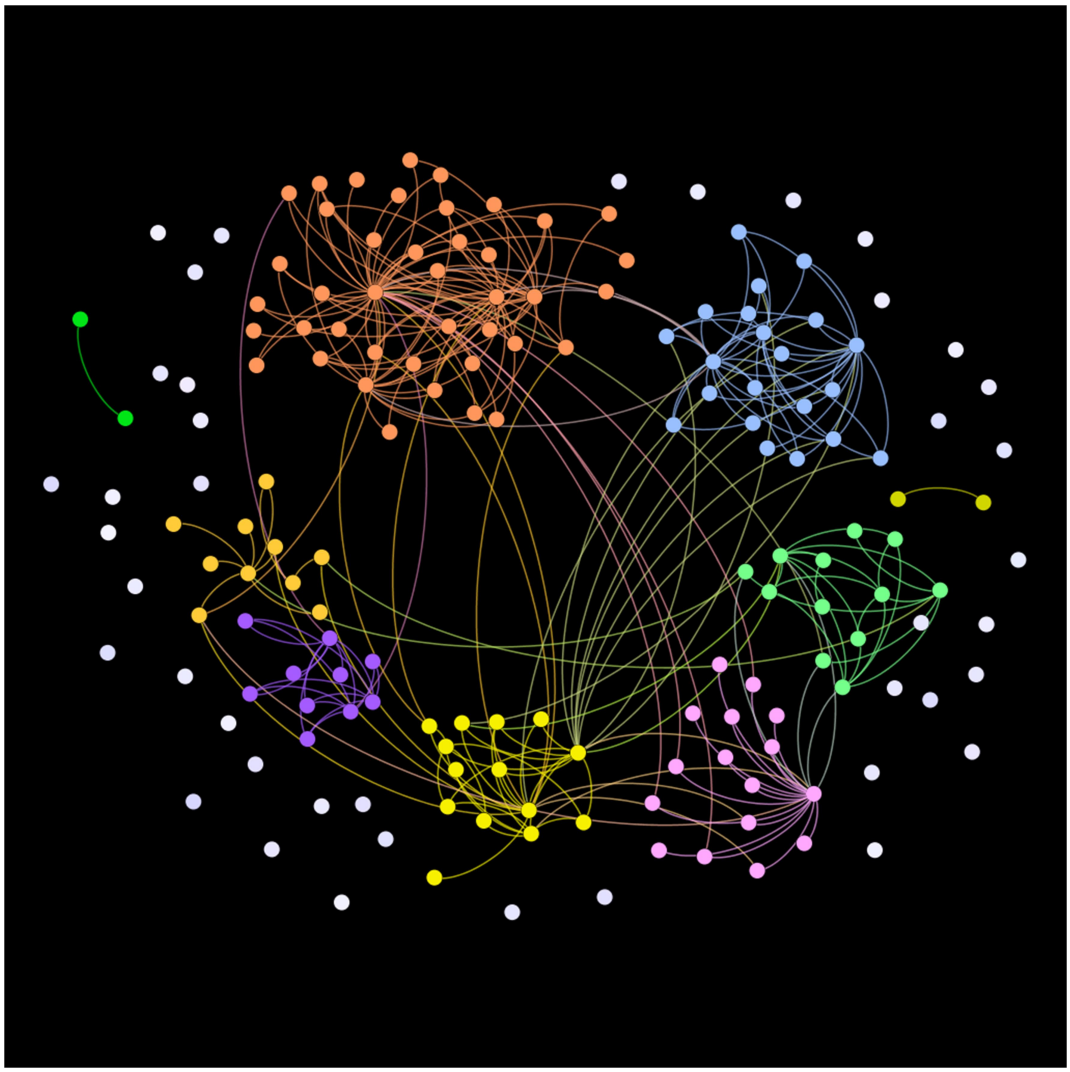
Είναι η τελευταία παράμετρος του δικτύου που υπολογίζουμε, πρόκειται για τον δείκτη της διαιρετότητας του δικτύου σε ομάδες ισχυρά συνδεδεμένες στο εσωτερικό τους και ασθενέστερα μεταξύ τους. Σε ένα κοινωνικό δίκτυο σαν αυτό που μελετάμε είναι αναμενόμενο να υπάρχει εμφανής κατακερματισμός σε ομάδες. Αυτό γιατί ένα άτομο έχει πολλά σύνολα γνωριμιών στα οποία εντάσσεται, εργασία, φίλοι από τη σχολή, φίλοι από τη γειτονιά ή τον τόπο καταγωγής, ευρύτερη οικογένεια, και άλλα. Οι ομάδες αυτές φυσικά περιπλέκονται και μεταξύ τους και είναι πολλές οι περιπτώσεις που ένα άτομο δεν θα ανήκει μόνο σε μία. Βλέποντας τις ομάδες είναι πιθανό να μπορούμε να βγάλουμε και κάποια συμπεράσματα για την φύση τους, βάσει στατιστικών δεδομένων. Ο Αμερικανός κοινωνιολόγος Charles Cooley, έκανε πρώτος την διάκριση σε πρωτεύουσες ομάδες και δευτερεύουσες (ref 46). Μία πρωτεύουσα ομάδα είναι ένα συνήθως μικρό σύνολο του οποίου τα μέλη μοιράζονται στενές και προσωπικές σχέσεις που διαρκούν στον χρόνο. Μία δευτερεύουσα ομάδα είναι ένα μεγάλο σύνολο του οποίου οι σχέσεις είναι απρόσωπες και αποσκοπούν σε κάποιο όφελος. Έτσι μπορούμε εκ πρώτης όψεως να αποκλείσουμε κάποια ενδεχόμενα, όπως για παράδειγμα το ότι μία ομάδα 40 ατόμων στο σύνολο των 169 που έχει το παράδειγμα μας, δεν μπορεί να είναι πρωτεύουσα. Μάλιστα αν δεν υπάρχει δεύτερη στο ίδιο μέγεθος πιθανά είναι ο εργασιακός κύκλος του ατόμου που μελετάμε.

Η τιμή του modularity υπολογίζεται ως το άθροισμα για όλες τις ομάδες του δικτύου, της διαφοράς των κόμβων εντός της ομάδας από το αναμενόμενο πλήθος κόμβων τυχαία τοποθετημένων σε ένα ισοδύναμο δίκτυο. Για να την υπολογίζουμε, τοποθετούμε αρχικά κάθε κόμβο σε μια διαφορετική ομάδα. Ύστερα για τον κόμβο *i*, εξετάζουμε κάθε γειτονικό κόμβο *j* και εκτιμάμε το κέρδος στο modularity στην περίπτωση που τον τοποθετούσαμε στην ομάδα του κόμβου *j* τον *i*. Ο *i* τοποθετείται στην κοινότητα στην οποία το κέρδος αυτό είναι μέγιστο. Η διαδικασία επαναλαμβάνεται για όλους τους κόμβους, συνήθως περισσότερες από μία φορές για τον κάθε κόμβο μέχρι το κέρδος να μεγιστοποιηθεί. Το αποτέλεσμα της ομαδοποίησης του δικτύου που εξετάζεται φαίνεται στο σχήμα 13. Η σειρά εξέτασης των κόμβων δεν φαίνεται να έχει

σημαντικό αντίκτυπο στο αποτέλεσμα. Το κέρδος της μεταφοράς ενός απομονωμένου κόμβου *i* σε μία κοινότητα *C*, δίνεται από τον τύπο (Piraveenan et al., 2014):

$$\Delta Q = \left[\frac{\Sigma_{in} + K_{i,in}}{2m} - \left(\frac{\Sigma_{tot} + k_i}{2m}\right)^2\right] - \left[\frac{\Sigma_{in}}{2m}\left(\frac{\Sigma_{tot}}{2m}\right)^2\left(\frac{k_i}{2m}\right)^2\right]$$

Στην περίπτωσή μας που δεν υπάρχουν βάρη, Σ_{in} είναι το πλήθος των ακμών μέσα στην *C*, Σ_{tot} οι συνολικές ακμές συδεδεμένες με κόμβους της *C*, k_i το πλήθος ακμών μεταξύ του *i* και της *C* και *m*, το συνολικό πλήθος ακμών στο δίκτυο.



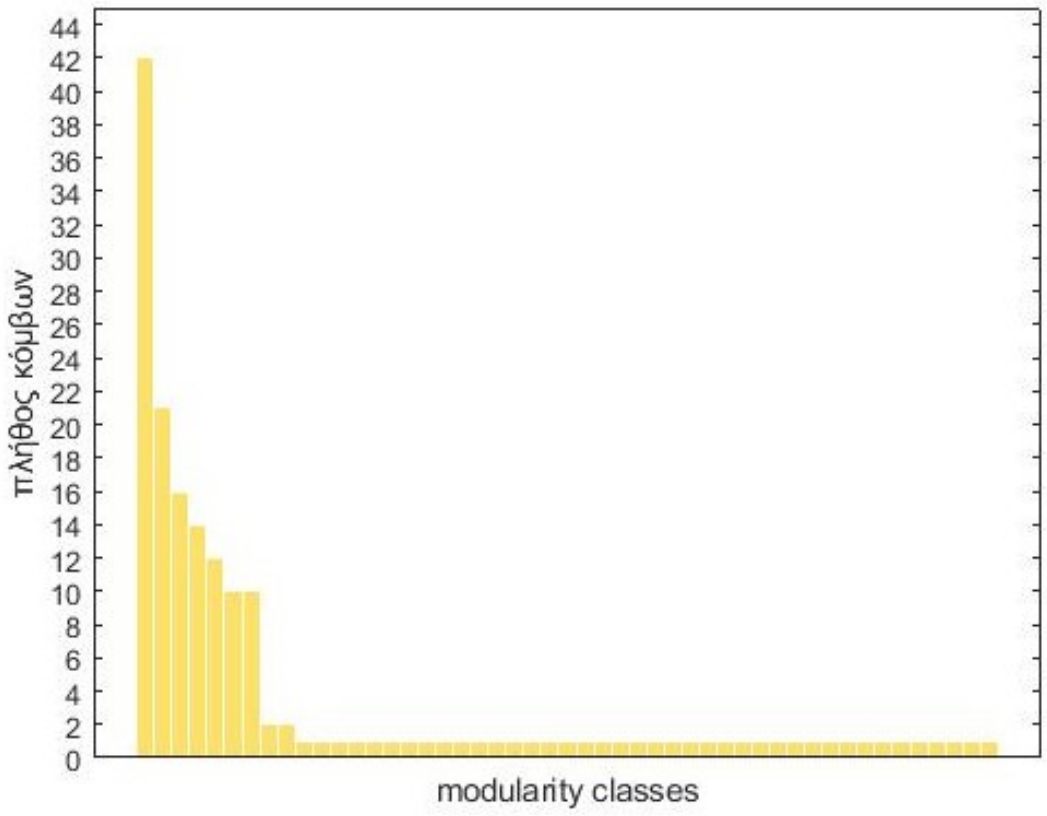
Σχήμα 13. Modularity classes του δικτύου.

Σε όλο το δίκτυο, το μέτρο του modularity προκύπτει ως:

$$Q = \frac{1}{2m}\sum_{i,j}\left[A_{ij} - \frac{k_i k_j}{2m}\right]\delta(c_i, c_j)$$

Όπου A_{ij} ο adjacency matrix του δικτύου, k_i το degree του κόμβου i, c_i η κοινότητα στην οποία έχει ενταχθεί ο i στην παραπάνω διαδικασία και η συνάρτηση δ είναι ίση με 1 αν $c_i = c_j$ και με 0 αλλιώς. Έτσι στο δίκτυό που εξετάζουμε προκύπτει πως $Q = 0.622$, τιμή αρκέτα υψηλή που υποδηλώνει ισχυρό κατακερματισμό σε κοινότητες. Οι κοινότητες που προέκυψαν είναι 49 εάν λάβουμε υπόψη και τους απομονωμένους κόμβους αλλά πρακτικά είναι επτά αυτές που μας ενδιαφέρουν, στις οποίες συμμετέχουν από 10 ως 42 κόμβοι (Σχήμα 14). Μπορούμε βάσει όσων είπαμε για τις πρωτεύουσες ομάδες, να συμπεράνουμε πως η ομάδα με τα 42 άτομα είναι πιθανά το ευρύ εργασιακό περιβάλλον του υπό μελέτη ατόμου και οι μικρότερες δεκαμελής ομάδες κάποιες παρέες. Το ότι εντάσσονται βάσει του αλγορίθμου τα συγκεκριμένα δέκα άτομα στην ομάδα, δεν σημαίνει πως είναι ενεργά μέλη της πρωτεύουσας ομάδας και τα δέκα. Για παράδειγμα μπορεί να αποτελείται από τέσσερα άτομα η πρωτεύουσα ομάδα και τα άλλα έξι να υπάρχουν ως κοινοί γνωστοί. Σίγουρα όμως σε κάθε πρωτεύουσα ομάδα υπάρχει ένας πυρήνας ατόμων ανάλογα μεγάλος με το μέγεθός της. Στις δευτερεύουσες ομάδες πάλι, καθώς οι σχέσεις μπορεί να είναι περισσότερο απρόσωπες, ενδέχεται να μην υπάρχει κάποιος πυρήνας.

Στη συνέχεια μπορούμε να υπολογίσουμε ακόμα το πλήθος κοινοτήτων με τις οποίες συνδέεται ο κάθε κόμβο. Αυτό μπορεί επίσης να ληφθεί υπόψη ως μέτρο της κεντρικότητας του κόμβου στο δίκτυο. Αυτό το μέτρο της κεντρικότητας ονομάζεται cross-clique centrality. Δεν παρουσιάζεται εδώ αλλά ο υπολογισμός του γίνεται στο script για το modularity, στο παράρτημα 3.



Σχήμα 14.

3.3 Ανάλυση των δεδομένων

3.3.1 Ταξινόμηση των δεσμών

Στην εργασία αυτή, ο στόχος είναι η εύρεση του κόμβου εντός του δικτύου από τον οποίο μία επίθεση spoofing προς το άτομο του οποίου το δίκτυο έχουμε κατασκευάσει θα έχει την μεγαλύτερη επικινδυνότητα. Για την εύρεσή του, θα κατασκευάσουμε μία μέθοδο ταξινόμησης όλων των ατόμων του δικτύου βάσει της επικινδυνότητας τους και θα επιλέξουμε το πρώτο στην κατάταξη. Την επικινδυνότητα την ορίζουμε ως την πιθανότητα να αντιδράσει ο στόχος δεκτικά προς ένα phishing mail, δηλαδή αρχικά να το ανοίξει και στη συνέχεια να ακολουθήσει τον σύνδεσμο που αυτό περιλαμβάνει. Ένα μήνυμα που κατασκευάζεται για μια επίθεση mail spoofing, όταν δεν γνωρίζουμε ακριβώς λεπτομέρειες για τα ενδιαφέροντα του θύματος, πρέπει να έχει γενικό

τίτλο και περιεχόμενο μηνύματος αλλά να φαίνεται παράλληλα ενδιαφέρον και ελκυστικό. Έτσι ώστε το άτομο που θα το λάβει να υποθέσει πως περιέχει κάποια ενδιαφέρουσα πληροφορία. Επομένως το πρόβλημα κατάταξης των κόμβων στο δίκτυο ανάγεται στο εξής πρόβλημα: «Από ποιο κόμβο εντός του δικτύου φίλων στα μέσα κοινωνικής δικτύωσης είναι πιο πιθανό να φτάσει μια αξιόπιστη ενδιαφέρουσα πληροφορία;». Η πληροφορία είναι το αντικείμενο που κινείται εντός του δικτύου που εξετάζουμε. Έτσι κατατάσσουμε τους κόμβους βάσει τις ικανότητάς τους να διαδώσουν την πληροφορία πρώτοι στον κεντρικό κόμβο του δικτύου, της ικανότητας τους να προσλάβουν μια πληροφορία πριν αυτή ταξιδέψει πολύ μέσα στο δίκτυο και βάσει της αξιοπιστίας ή του ενδιαφέροντος που φαινομενικά μπορεί να έχει μία πληροφορία από αυτούς. Τα τρία αυτά μεγέθη αν και είναι εξίσου σημαντικά, δεν μπορεί να ληφθούν εξίσου υπόψη στην κατάταξη των κόμβων γιατί δεν μπορούν να προβλεφθούν με την ίδια ακρίβεια.

- Πιο σημαντική θεωρούμε την ικανότητα του κόμβου να μεταφέρει την πληροφορία πρώτος στον κεντρικό κόμβο. Αυτό για λόγους ψυχολογικούς όσο και υπολογιστικούς. Το κεντρικό άτομο του δικτύου είναι πιο πιθανό να ανοίξει ένα μήνυμα από μία επαφή του από την οποία ξέρει πως υπάρχει μεγαλύτερη πιθανότητα να ακούσει κάτι πρωτότυπο. Επίσης η ικανότητα ενός κόμβου να διαδώσει στον κεντρικό κόμβο πρώτος μία πληροφορία που ήδη κατέχει, δεν εξαρτάται από το υπερδίκτυο στο οποίο ανήκει το δίκτυο που εξετάζουμε οπότε είναι πιο άμεσα προσεγγίσιμη με τα δεδομένα που έχουμε.

- Στη συνέχεια λαμβάνεται υπόψη η αξιοπιστία ή το ενδιαφέρον των πληροφοριών που προέρχονται από τον κόμβο. Δεύτερη έρχεται γιατί δεν επηρεάζει δραματικά την πιθανότητα να πέσει θύμα spoofing κάποιος από το συγκεκριμένο άτομο. Κυρίως όμως γιατί δεν μπορούμε να έχουμε πολύ καλή πρόβλεψη της αξιοπιστίας ή του ενδιαφέροντος που μία πληροφορία προερχόμενη από το συγκεκριμένο άτομο μπορεί να έχει. Ο μόνος τρόπος να την υπολογίσουμε είναι να την συσχετίσουμε με το πρεστίζ του ατόμου στο δίκτυο.

- Τελευταία, προσμετράμε την πιθανότητα η πληροφορία να φτάσει νωρίς στον κόμβο, ανεξάρτητα από το σημείο γέννησής της μέσα στο δίκτυο. Η συγκεκριμένη ποσότητα έρχεται τρίτη αφού για μία πληροφορία που προέρχεται από κάποιο σημείο εκτός του υπό μελέτη δικτύου, εξαρτάται κυρίως από τη θέση του ατόμου μέσα στο συνολικό υπερδίκτυο. Έτσι δεν μπορούμε να την προβλέψουμε με ακρίβεια. Επίσης θεωρούμε πως το κεντρικό άτομο γνωρίζει τη διασύνδεση του κάθε φίλου του με το υπερδίκτυο.

3.3.2 Μοντελοποίηση

Στο μοντέλο που κατασκευάζουμε, θα χρησιμοποιήσουμε τρία κεντρικά μεγέθη:

a. Την πιθανότητα ο κόμβος να μεταφέρει πρώτος την πληροφορία στον κεντρικό, στην οποία θα αναφερόμαστε ως *F.*

b. Την αξιοπιστία/ενδιαφέρον του κόμβου *P*.

c. Την πιθανότητα η πληροφορία να φτάσει νωρίς στον συγκεκριμένο κόμβο σε σχέση με τους υπολοίπους *T*.

- Για την πιθανότητα *F*:

θα συνυπολογίσουμε θετικά το degree σε σχέση με το πλήθος διαφορετικών modularity classes με τις οποίες συνδέεται ο κόμβος. Το degree στο δίκτυο αντιπροσωπεύει το πλήθος κοινών φίλων με τον κεντρικό κόμβο, όσο περισσότεροι κοινοί φίλοι υπάρχουν με αυτόν οι οποίοι προέρχονται από διαφορετικές κοινότητες κόμβων, τόσο πιο πιθανό είναι να είναι στενότερος φίλος ο κόμβος που εξετάζουμε και όχι μία απλή γνωριμία. Ωστόσο το degree δεν θέλουμε να είναι πολύ υψηλό αλλά να παίρνει τιμές πιο ψηλές από τη μέση τιμή, αφού με ένα πολύ κοντινό άτομο υπάρχει περίπτωση να υπάρχει

συχνή επικοινωνία άρα και μεγάλη πιθανότητα να υποψιαστεί το spoofing ο παραλήπτης. Έτσι ιδανική τιμή για το degree, θεωρούμε την τιμή k = 20. Επίσης θα συνυπολογίσουμε θετικά το closeness centrality, καθώς μετράει την γεωγραφική κεντρικότητα του ατόμου στο δίκτυο. Τέλος θα συνεισφέρει αρνητικά το local clustering coefficient καθώς όσο μικρότερο είναι τόσο περισσότερες δομικές τρύπες (structural holes) υπάρχουν γύρω από τον κόμβο στο δίκτυο και τόσο μεγαλύτερη ισχύ αποκτά στην διακίνηση της πληροφορίας. Σχετικά με το degree και το modularity, έχουμε τον πρώτο όρο:

$$F_1 = \frac{k}{1 + |20 - k|} * m_c^2$$

Όπου k το degree του κόμβου, εξασφαλίζουμε την λήψη ως βέλτιστης της τιμής k = 20 διαιρώντας με $1 + |20 - k|$. m_c είναι το πλήθος των modularity classes με τις οποίες συνδέεται ο κόμβος. Αυτό το υψώνουμε στο τετράγωνο για να του δώσουμε μεγαλύτερο βάρος. Σχετικά με τον παράγοντα local clustering coefficient (l_{cc}) και την closeness centrality (C_c)έχουμε τον δεύτερο παράγοντα:

$$F_2 = \frac{10}{9l_{cc} + 1} * C_c$$

Με τον τύπο $\frac{10}{9l_{cc}+1}$ εξασφαλίζουμε πως αν ο l_{cc} είναι ίσος με 1 δεν επηρεάζει το αποτέλεσμα, διαφορετικά αν είναι μικρότερος το αυξάνει. Στην περίπτωση που ο l_{cc} δεν ορίζεται, η τιμή της F_2 τίθεται ίση με 0. Συνθέτουμε ύστερα τους δύο παράγοντες και κανονικοποιούμε πολλαπλασιάζοντας με 100.7. Έχουμε λοιπόν:

$$F = 100.7 * F_1 * F_2$$

Που ισούται με:

$$F = 1007 * \frac{k * m_c^2 * C_c}{(1 + |20 - k|)(9l_{cc} + 1)}$$

Η πιθανότητα *F*, κανονικοποιημένη παίρνει τιμές από 0 για τους κόμβους με *k = 0* έως 100.

- <u>Για την αξιοπιστία/ενδιαφέρον του κόμβου *P*:</u>

Θα συνυπολογίσουμε θετικά την eigenvector centrality η οποία λειτουργεί ως μέτρο του πόσο κεντρικούς γείτονες έχει ένας κόμβος και το degree, το οποίο όσο υψηλότερο είναι τόσο μεγαλύτερο πρεστίζ έχει ο κόμβος στο δίκτυο. Το degree όμως, για τον ίδιο λόγο όπως και στην προηγούμενη περίπτωση, θα προτιμήσουμε να παίρνει σχετικά μεγάλες τιμές, γύρω από το $k = 20$. Έχουμε λοιπόν

$$P_1 = \frac{k}{1 + |20 - k|}$$

Και

$$P_2 = E_c$$

Όπου E_c η τιμή της eigenvector centrality. Όπως και πριν κανονικοποιούμε την τιμή P, πολλαπλασιάζοντας με 339.8. Έχουμε έτσι:

$$P = 339.8 * P_1 * P_2$$

Δηλαδή:

$$P = 339.8 * \left(\frac{k * E_c}{1 + |20 - k|}\right)$$

Η τιμή *P*, κανονικοποιημένη κυμαίνεται μεταξύ 0 και 100.

- <u>Για την ταχύτητα με την οποία φτάνει η πληροφορία στον κόμβο *T*:</u>

Για να φτάσει γρήγορα μία πληροφορία σε έναν κόμβο, είναι πολύ σημαντικό να συνδέεται με μεγάλο πλήθος κεντρικών κόμβων (hubs), έτσι θα βρίσκεται σε κάποιο σταυροδρόμι ροής πληροφορίας. Για αυτό το λόγο, θέλουμε υψηλό μέσο degree των γειτόνων σε συνδυασμό με πλήθος γειτόνων και μεγάλο πλήθος modularity classes με τις οποίες συνδέεται ο κόμβος. Επίσης είναι επιθυμητή η υψηλή τιμή της pagerank centrality που υποδηλώνει πως συχνά στην τυχαία πορεία της πληροφορίας μέσα στο δίκτυο θα βρεθεί διαμεσολαβητής ο συγκεκριμένος κόμβος. Θέλουμε ακόμα ψηλή τιμή της betweenness centrality. Αυτή εξασφαλίζει την συχνή ύπαρξη του κόμβου στο ελάχιστο μονοπάτι μεταξύ δύο άλλων κόμβων, αν και η πληροφορία δεν τείνει να ακολουθήσει απαραίτητα το ελάχιστο μονοπάτι. Τέλος ζητάμε να είναι μικρή η τιμή του local clustering coefficient. Στην περίπτωση αυτή υπάρχουν πολλές δομικά κενά (structural holes) γύρω από τον κόμβο, αυξάνοντας την πιθανότητα να βρεθεί φορέας πληροφορίας πρωτότυπης για πολλούς από τους γείτονές του.

Σε σχέση με το μέσο degree των γειτόνων $\bar{k}$ και το πλήθος των modularity classes (m_c), έχουμε τον πρώτο όρο:

$$T_1 = \left(\bar{k} * m_c\right)^2$$

Υψώνουμε στο τετράγωνο για να δώσουμε μεγαλύτερο βάρος. Σε σχέση με το degree, έχουμε τον δεύτερο όρο:

$$T_2 = \begin{cases} 0\,, & \gamma\iota\alpha\ k = 1\ \acute{\eta}\ k = 2 \\ \dfrac{k}{1 + |20 - k|}\,, & \alpha\lambda\lambda\iota\acute{\omega}\varsigma \end{cases}$$

Στην περίπτωση αυτή θέλουμε να αποφύγουμε να λάβουν εξαιρετικά μεγάλες τιμές για κόμβους που έχουν υψηλό $\bar{k}$ επειδή έχουν μόνο έναν ή δύο γείτονες με υψηλό degree. Για τον λόγο αυτό συνυπολογίζουμε το k ίσο με 0 στις περιπτώσεις μόνο ενός ή δύο γειτόνων. Σε σχέση με την κεντρικότητα, έχουμε:

$$T_3 = P_c * \sqrt{B_c}$$

Όπου P_c η pagerank centrality και B_c η betweenness centrality. Για την τελευταία υπολογίζουμε την τετραγωνική της ρίζα γιατί δεν θέλουμε να της δώσουμε μικρότερο βάρος από τα άλλα μεγέθη. Τέλος για τον local clustering coefficient, όπως και στην περίπτωση της *F*, έχουμε:

$$T_4 = \frac{10}{9l_{cc} + 1}$$

Συνθέτουμε τους τέσσερις παράγοντες και κανονικοποιούμε πολλαπλασιάζοντας με $3.2 * 10^{-5}$. Έτσι τελικά έχουμε:

$$T = 3.2 * 10^{-5} * T_1 * T_2 * T_3 * T_4$$

Δηλαδή:

$$T = \begin{cases} 0, & \gamma\iota\alpha\ k = 1\ \eta\ k = 2 \\ \dfrac{3.2 * (\bar{k} * m_c)^2 * k * P_c * \sqrt{B_c}}{10^5 * (9 * l_{cc} + 1) * (1 + |20 - k|)}, & \alpha\lambda\lambda\iota\acute{\omega}\varsigma \end{cases}$$

Η τιμή *T*, κανονικοποιημένη επίσης κυμαίνεται μεταξύ 0 και 100.

- Τελική αξιολόγηση των κόμβων:

Για να εξάγουμε ένα τελικό αποτέλεσμα για την αξία του κάθε κόμβου μέσα στο δίκτυο, θα αθροίσουμε τις τρεις τιμές, *P*, *T* και *F*, δίνοντας διαφορετικό βάρος στην κάθε μία ανάλογα με την σημασία που έχουμε αξιολογήσει πως έχει. Θέλουμε ακόμα να ξεχωρίσουν οι κόμβοι που έχουν τιμές ψηλότερες από τον μέσο όρο, οπότε και τις τρεις παραμέτρους τις διαιρούμε με την μέση τιμή που λαμβάνουν. Ακόμα υψώνουμε στο τετράγωνο τις τιμές *P* και *F* αλλά όχι την *T*. Ο πρώτος όρος που αφορά την τιμή *F*, είναι:

$$S_1 = \left(\left(\overline{\left(\frac{F}{P} \right)} + 1 \right) * \frac{F}{\bar{F}} \right)^2$$

Για να δώσουμε μεγαλύτερο βάρος στην *F*, θα πολλαπλασιάσουμε τον όρο που την περιλαμβάνει με την μέση τιμή του πηλίκου $\frac{F}{P} + 1$ ώστε να βαραίνει στο τελικό αποτέλεσμα περισσότερο όταν είναι μεγαλύτερη από την τιμή *P*.

Ο δεύτερος όρος που αφορά την τιμή *P*, θα είναι:

$$S_2 = \left(\frac{P}{\bar{P}} \right)^2$$

Τέλος για τον όρο που αφορά την τιμή *T*, έχουμε:

$$S_3 = \frac{T}{10 * \bar{T}}$$

Την τελευταία διαιρούμε με 10 ώστε να έχουν οι δύο πρώτοι παράγοντες την ίδια τάξη μεγέθους ενώ η *T* να είναι μία τάξη μεγέθους μικρότερη αφού μας ενδιαφέρει σημαντικά λιγότερο στον υπολογισμό του τελικού αποτελέσματος.

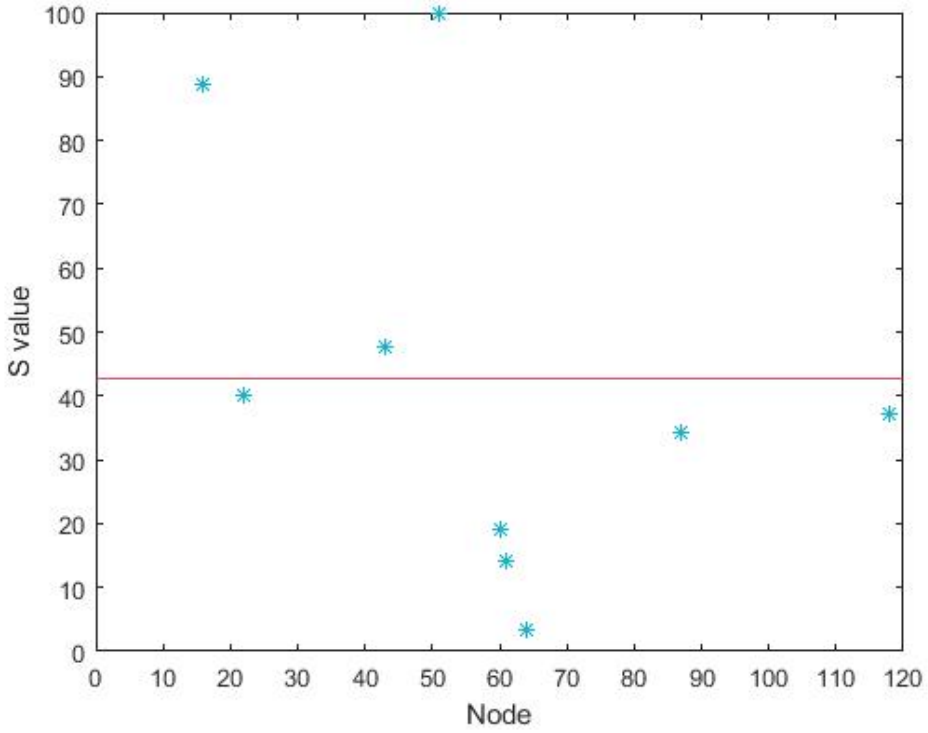
Συνθέτουμε τους τρεις παράγοντες και κανονικοποιούμε πολλαπλασιάζοντας με 0.025:

$$S = 0.025 * S_1 * S_2 * S_3$$

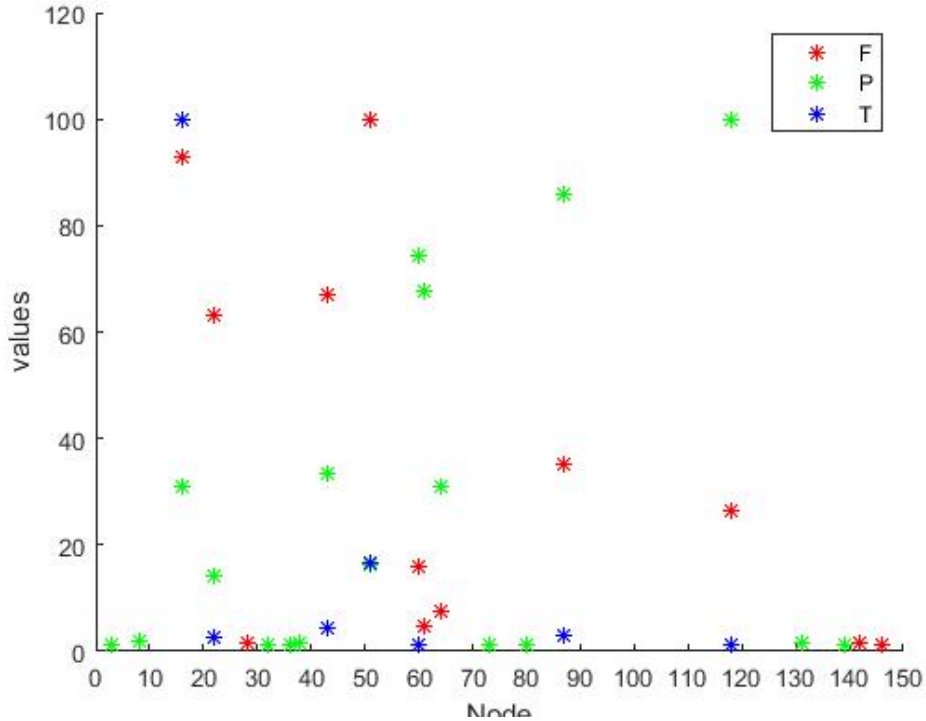
Αντικαθιστώντας:

$$S = 0.025 * \left(\left(\left(\overline{\frac{F}{P}} \right) + 1 \right) * \frac{F}{\overline{F}} \right)^2 * \left(\frac{P}{\overline{P}} \right)^2 * \left(\frac{T}{10 * \overline{T}} \right)$$

Μετά την κανονικοποίηση έχουμε $max(S) = 100$. Από τον υπολογισμό προέκυψαν τα εξής γράφημα για της τιμές *S* (15) και *F,P,T* (16).



Σχήμα 15. Τελική κατάταξη των κόμβων.
Η κόκκινη γραμμή βρίσκεται στη μέση τιμή της S.



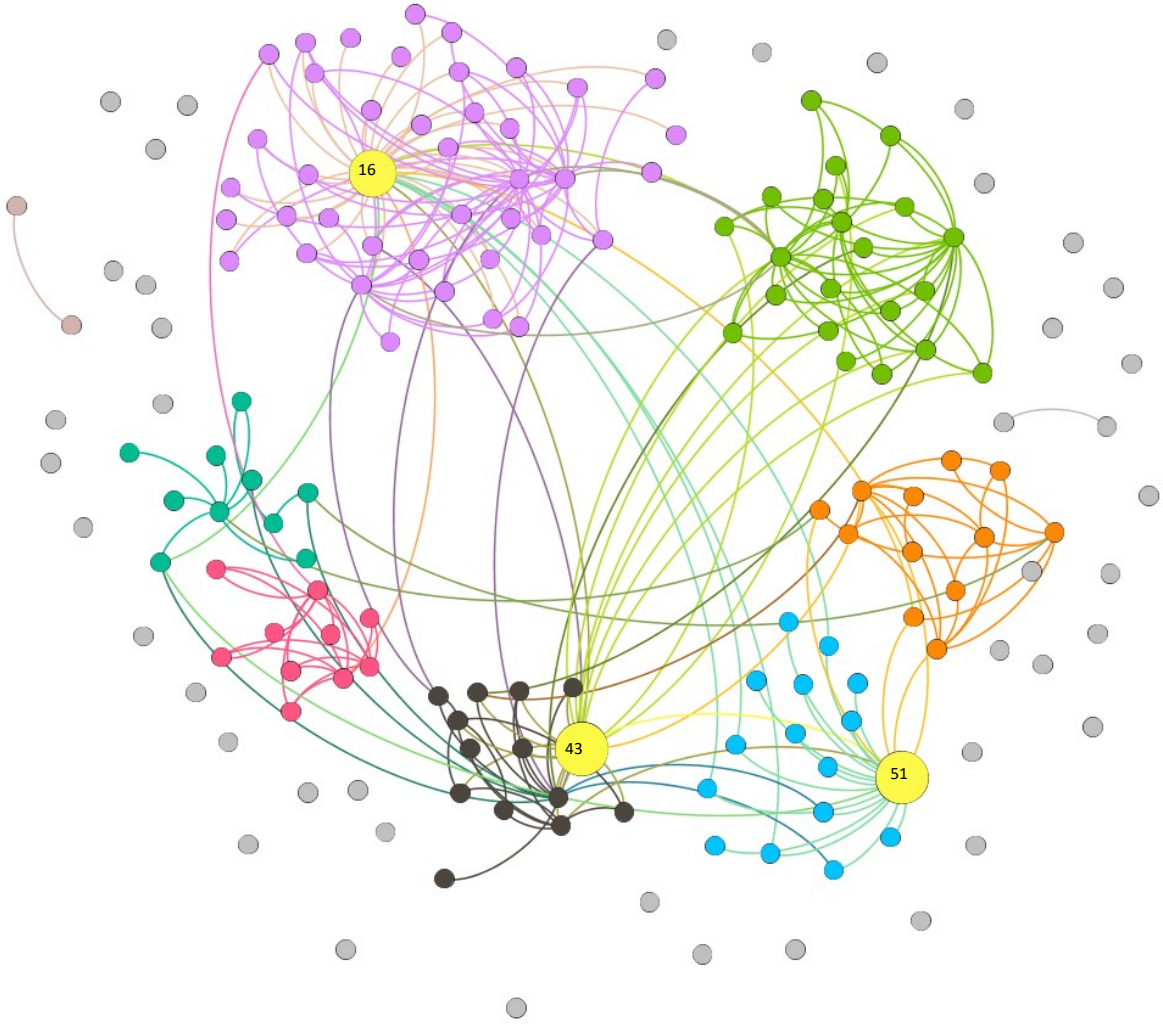
Σχήμα 16. Τιμές F, P, T για κάθε κόμβο.

- Τελικό αποτέλεσμα

Ταυτότητα κόμβου	Τιμή S
16	88.9
22	40.17
43	47.7
51	100
60	19
61	14.1
64	3.4
87	34.3
118	37.1

Πίνακας 3. Παρουσίαση των τελικών αποτελεσμάτων.

Παρατηρούμε ότι τρεις κόμβοι είναι πάνω από τον μέσο όρο (42.75). Οι 16, 43 και 51. Από αυτούς, οι δύο με τις πιο υψηλές τιμές είναι ο 51 και λίγο χαμηλότερη τιμή ο 16. Επομένως από τους κόμβους του δικτύου, θα επιλέγαμε ιδανικά έναν από αυτούς τους δύο, προτιμητέα τον 51. Η θέση των κόμβων φαίνονται μέσα στο δίκτυο παρακάτω (Σχήμα 17). Ο κόμβος 16 είναι πολύ κεντρικότερος των άλλων δύο και αρκετά πιο διασυνδεδεμένος στο δίκτυο. Όμως λόγω του κριτηρίου που θέσαμε για την ταξινόμηση των κόμβων, το degree ιδανικά να είναι κοντά στην περιοχή του 20, έχει μεγαλύτερη τελικά τιμή ο 51. Ο 16 έχει degree ίσο με 42, ο 43 ίσο με 19 και ο 51 ίσο με 22.



Σχήμα 17. Η θέση των κόμβων με την υψηλότερη κατάταξη στο δίκτυο.

4. Συμπεράσματα

Η μέθοδος που χρησιμοποιήθηκε για την εξαγωγή του τελικού αποτελέσματος φαίνεται πως δίνει μία σαφή κατάταξη των κόμβων του δικτύου. Μπορούμε να πούμε με πως μία προσπάθεια mail spoofing για τον πρώτο ή τον δεύτερο κόμβο στην ταξινόμηση θα έχει μεγαλύτερη πιθανότητα επιτυχίας από την περίπτωση στην οποία θα επιλέξουμε κάποιον άλλο κόμβο στην κατάταξη. Ακόμα μπορούμε με βεβαιότητα να αποκλείσουμε όλους τους κόμβους που δεν βρίσκονται στον πίνακα 3. Από τους κόμβους που παρουσιάζονται στον πίνακα 3, ο κόμβος 16 εμφανίζεται σε: facebook, twitter και LinkedIn, οι κόμβοι 22, 51 και 61, εμφανίζονται σε: facebook και twitter, ο 43 μόνο στο facebook και οι 60, 64, 87 και 118, μόνο στο LinkedIn. Από τους πέντε κόμβους που εμφανίζονται στο LinkedIn, οι τρείς (16, 60, 118) ανήκουν στην ίδια modularity class, η οποία είναι η μεγαλύτερη του δικτύου. Η παρατήρηση ενισχύει την υπόθεση πως η συγκεκριμένη ομάδα αποτελεί το εργασιακό περιβάλλον του υπό μελέτη ατόμου. Έτσι λοιπόν μπορεί ο επιτιθέμενος να έχει μία πρώτη ιδέα για το περιεχόμενο του spoofed mail.

Με την ολοκλήρωση αυτής της εργασίας, εύκολα καταλήγουμε στο συμπέρασμα, πως από λίγα εύκολα συλλέξιμα δημόσια δεδομένα, μπορούν να εξαχθούν πολλαπλάσια συμπεράσματα για τους συσχετισμούς ενός ατόμου με τα γύρω του. Σε περιπτώσεις όπου τα δεδομένα, παραμένοντας δημόσια, είναι περισσότερα και έχουν να κάνουν με το περιεχόμενο δημοσιεύσεων μεταξύ των κόμβων του δικτύου, μπορούμε να μιλήσουμε με ασφάλεια για τις θέσεις των ατόμων πάνω σε κοινωνικοπολιτικά ζητήματα ή για τις προτιμήσεις και τις ανάγκες τους. Συνειδητοποιούμε λοιπόν την ισχύ του social engineering ως εργαλείου ανάλυσης κοινωνικών συνόλων οποιουδήποτε μεγέθους αλλά και τους κινδύνους που ενέχει η χρήση του.

Σε επόμενο στάδιο αυτής της εργασίας, θα μπορούσε να γίνει μία ανάλυση σε σχέση με τις ομάδες που σχηματίζονται κατά την κατηγοριοποίηση σε modularity classes. Θα ήταν ενδιαφέρον επίσης να δοκιμάσουμε και άλλες μεθόδους ομαδοποίησης των κόμβων του δικτύου και να προσπαθήσουμε να εξάγουμε συμπεράσματα για την φύση των ομάδων στον υλικό κόσμο.

Μετά από την ανάλυση των δεδομένων της συγκεκριμένης έρευνας, θεωρώ πως η ανάλυση ενός δικτύου σαν αυτό, όταν παραλληλίζεται με την ανάλυση κοινωνικών συμπεριφορών, μπορεί να αποκαλύψει πολύ περισσότερες πληροφορίες από τις προφανείς. Αυτού του είδους η ανάλυση μπορεί να αποτελέσει ένα ισχυρό εργαλείο για την επιστήμη της κοινωνιολογίας.

Το social engineering θα δώσει σίγουρα τέτοια εργαλεία στο μέλλον στις ανθρωπιστικές επιστήμες. Ωστόσο, η έρευνα γίνεται και θα γίνεται στον χώρο του marketing σε σχέση με την μεγιστοποίηση του κέρδους. Ακόμα υπάρχει άνθιση των μεθόδων του social engineering σε περιόδους κρίσης όπου οι πολιτικές παρατάξεις πρέπει να καταφύγουν στην προπαγάνδα. Αυτές λοιπόν τις περιπτώσεις πρέπει να μελετήσουμε ώστε να βγάλουμε ωφέλιμα συμπεράσματα σε σχέση με τον κοινωνικό βίο του ανθρώπου.

Βιβλιογραφία

1. *Quann, J., Belford, P.: The hack attack - increasing computer system awareness of vulnerability threats. In: 3rd Applying Technology to Systems; Aerospace Computer Security Conference, United States, American Institute of Aeronautics and Astronautics (December 1987) 155-157*

2. *Kluepfel, H.: Foiling the wiley hacker: more than analysis and containment. In: Security Technology, 1989. Proceedings. 1989 International Carnahan Conference on. (1989) 15-21*

3. *Kluepfel, H.: In search of the cuckoo's nest [computer security]. In: Security Technology, 1991. Proceedings. 25th Annual 1991 IEEE International Carnahan Conference on. (1991) 181-191*

4. *Venter H. S. et al.: Towards an Ontological Model Defining the Social Engineering Domain. Conference paper in: IFIP Advances and communication Technology, July 2014. (2014) 5*

5. *Workman, M.: Wisecrackers: A Theory-Grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security. In: Journal of the American Society for Information and Technology, 59(4). (February 15, 2008) 1-12*

6. *Castells, Manuel: (2009) Comunicación y poder. Alianza Editorial/Madrid, Alianza Editorial*

7. *Baudrillard, Jean: (1996) Η Διαφάνεια του Κακού: Δοκίμιο πάνω στα ακραία φαινόμενα. Εξάντας/Αθήνα, Εξάντας Εκδοτική Α.Ε.*

8. *Sergey Sanovich, "Computational Propaganda in Russia: The Origins of Digital Disinformation." Samuel Woolley and Philip N. Howard, Eds. Working Paper 2017.3. Oxford, UK: Project on Computational Propaganda. comprop.oii.ox.ac.uk. 32 pp.*

9. *Gillian Bolsover, "Computational Propaganda in China: An Alternative Model of a Widespread Practice." Samuel Woolley and Philip N. Howard, Eds. Working Paper 2017.2. Oxford, UK: Project on Computational Propaganda. comprop.oii.ox.ac.uk. 32 pp.*

10. *Gu Lion, Kropotow Vladimir and Yarochkin Fyodor: The Fake News Machine: How propagandists abuse the internet and manipulate the public. A TrendLabs Research Paper. www.trendmicro.com (2017)*

11. *Mitnick, K.D., Simon, W.L.: The art of deception: controlling the human element of security. Wiley Publishing, Indianapolis (2002)*

12. *Aldoory, L., & Van Dyke, M.A. (2006). The roles of perceived shared involvement and information overload in understanding how audiences make meaning of news about bioterrorism. Journalism & Mass Communication Quarterly, 83, 346–361*

13. *Grunig, J. E. (1997). A situational theory of publics: Conceptual history, recent challenges and new research. In D. Moss, T. MacManus, & D. Vercic (Eds.), Public relations research: An international perspective (pp. 3–48). London: International Thomson Business Press*

14. *Petty, R.E., & Cacioppo, J.T. (1986). Communication and persuasion: Central and peripheral routes to attitude change. New York: Springer-Verlag*

15. *Wang, Y.D., & Emurian, H.H. (2005). An overview of online trust: Concepts, elements, and implications. Journal of Computers in Human Behavior, 21, 105–125*

16. *Straub, D.W., & Welke, R.J. (1998). Coping with systems risk: Security planning models for management decision-making. MIS Quarterly, 22, 441–469*

17. *Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. Computers and Security, 24, 472–484*

18. *Cialdini, R.B. (2001). Influence: Science and practice. Boston: Allyn & Bacon*

19. *Allen, N.J., & Meyer, J.P. (1990). The measurement and antecedents of affective, continuance and normative commitment to the organization. Journal of Occupational Psychology, 63, 1–18*

20. *Petty, R.E., Briñol, P., & Tormala, Z. L. (2002). Thought confidence as a determinant of persuasion: The self-validation hypothesis. Journal of Personality and Social Psychology, 82, 722–741*

21. *Staw, B.M. (1981). The escalation of commitment to a course of action. The Academy of Management Review, 6, 577–587*

22. *Asch, S.E. (1946). Forming impressions of personality. Journal of Abnormal and Social Psychology, 41, 258–290*

23. *Giles, H., & Wiemann, J.M. (1987). Language, social comparison and power. In C.R. Berger & S.H. Chaffee (Eds.), The handbook of communication science (pp. 350–384). Newbury Park, CA: Sage*

24. *Milgram, S. (1983). Obedience to authority: An experimental view. New York: Harper-Collins*

25. *Brehm, J.W. (1966). A theory of psychological reactance. NY: Academic Press.*

26. *Dodge,R.C., Carver, C., & Ferguson, A.J. (2007). Phishing for user security awareness. Computers & Security, 26, 73–80*

27. *Miller, K. (2005). Communication theories: Perspectives, processes, and contexts. New York: McGraw-Hill*

28. *M. Chandrasekaran, K. Narayanan, and S. Upadhyaya. Phishing email detection based on structural properties. In Proceedings of the NYS Cyber Security Conference, 2006.*

29. *R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in Computing Systems, pages 581–590, 2006*

30. *S. Abu-Nimeh, D. Nappa, X. Wang, and S. Nair. A comparison of machine learning techniques for phishing detection. In Proceedings of the eCrime Researchers Summit, 2007*

31. *I. Fette, N. Sadeh, and A. Tomasic. Learning to detect phishing emails. In Proceedings of the International World Wide Web Conference (WWW), pages 649–656, 2007*

32. *Gehrard Paass et al. Improved Phishing Detection using Model-Based Features. Conference paper, January 2008.*

33. *http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.216.4317&rep=rep1&type=pdf*

34. *http://konect.uni-koblenz.de/networks/facebook-wosn-links*

35. http://konect.uni-koblenz.de/networks/ego-twitter

36. https://research.fb.com/three-and-a-half-degrees-of-separation/

37. Shao, Z.-G. (2010), Network analysis of human heartbeat dynamics, Appl. Phys. Lett. 96, 073703, DOI: 10.1063/1.3308505.

38. Reik V. Donner and Jonathan F. Donges. Visibility Graph Analysis of Geophysical Time Series: Potentials and Possible Pitfalls. In Acta Geophysica, vol. 60, no. 3, Jun. 2012, pp. 589-623, DOI: 10.2478/s11600-012-0032-x

39. M. Piraveenan, M Prokopenko and A. Y. Zomaya. Classifying Complex Networks using Unbiased Local Assortativity. Proc. of the Alife XII Conference, Odense, Denmark, 2010

40. M. Piraveenan, U. Senanayake and G. Thedchanamoorty. Node Assortativity in Complex Networks: An Alternative Approach. In Procedia Computer Science, December 2014, DOI: 10.1016/j.procs.2014.05.229.

41. V. D. Blondel, J.L. Guillaume, R. Lambiotte and E. Lefebvre, Fast unfolding of communities in large networks. J. Stat. Mech. (2008) P10008, DOI: 10.1088/1742-5468/2008/10/P10008.

42. https://resources.infosecinstitute.com/common-social-engineering-attacks/#gref

43. Qingxiong Ma, The process and characteristics of phishing attacks: A small international trading company case study, Journal of Technology Research;Jul2013, Vol. 4, p1, July 2013

44. T. Jagatic, N. Johnson and F menczer, Social Phishing, in Communications of the ACM, Volume 50 Issue 10, Pages 94-100,October 2007.

45. https://www.mathworks.com/help/matlab/ref/graph.centrality.html

46. https://courses.lumenlearning.com/boundless-sociology/chapter/types-of-social-groups/

47. https://wearesocial.com/us/blog/2018/01/global-digital-report-2018

48. https://en.wikipedia.org/wiki/Dunbar%27s_number

Παράρτημα 1

Οι υπολογισμοί για τα μεγέθη του δικτύου, έγιναν στην matlab, εκτός του modularity. Το τελευταίο μέγεθος, υπολογίστηκε αυτόματα από το πρόγραμμα gephi με τον αλγόριθμο που περιγράφεται στο υποκεφάλαιο modularity. Ακολουθούν τα scripts της matlab για τον υπολογισμό του κάθε μεγέθους.

A.1 Degree distribution

Το script δέχεται ως είσοδο από το ιστόγραμμα ps, το οποίο είναι σε μορφή διανύσματος σαράντα τριών στοιχείων και περιέχει την πιθανότητα εμφάνισης της κάθε τιμής του degree από 0 έως 42. Προκύπτει εύκολα από τον adjacency matrix του δικτύου. Έχουμε:

degree = sum('Adj');

nbins = 43;

ps = hist(degree, nbins);

Στο script ακόμα γίνεται προσέγγιση της ευθείας που ταιριάζει καλύτερα στα σημεία με τη μέθοδο των ελαχίστων τετραγώνων. Ο πίνακας x, προέκυψε από τις πιθανές τιμές που λαμβάνουν τα στοιχεία του διανύσματος degree όπως υπολογίζεται παραπάνω. Τέλος ως έξοδος του script είναι ένα γράφημα σε λογαριθμικούς άξονες που παρουσιάζει τα σημεία του ps και αντιπαραβάλει την ευθεία που προκύπτει από τη μέθοδο των ελαχίστων τετραγώνων με τις καμπύλες Erdos - Renyi και Barabasi – Albert για τα ίδια σημεία.

```
x = [0 1 2 3 4 5 6 7 8 9 10 16 19 21 22 23 42]; % Τιμές που λαμβάνει το degree

j = 1;

for i = 1:43        % Δεν λαμβάνουμε τις τιμές 0 υπόψη, δηλαδή τους αποκομμένους κόμβους
        if (ps(i) == 0)     % Το ps είναι το διάνυσμα με την πιθανότητα εμφάνισης της κάθε
        τιμής του degree

      i = i+1;
```

```
    elseif (ps(i) ~= 0)
        y(j) = ps(i);
        j = j+1;
    end
end
v1 = 0;
v2 = 0;
v3 = 0;
v4 = 0;
for i = 2:17
    v1 = v1 + log(x(i)) * log(y(i));
    v2 = v2 + log(x(i));
    v3 = v3 + log(y(i));
    v4 = v4 + (log(x(i)))^2;
end
b = (43 * v1 - v2 * v3) / (43 * v4 - (v2)^2);
a = (v3 - b * v2) / 43;
c = 0:42;
e = exp(1);
f = (e^a) * (c.^b);
loglog(f,'b-.');      % Σχεδίαση του γραφήματος
hold on;
loglog(ps,'ro');
axis([1 100 0.001 1]);
z = 6.201183;                % Κλίση της Barabasi Albert για δίκτυο σαν το συγκεκριμένο
k = 0:42;
for i = 1:43
    d(i) = exp(-z) * (z^k(i))/factorial(k(i));
end
loglog(d,'g-*');
```

```
for i = 1:43
    d(i) = k(i)^(-3);
end
loglog(d,'y-');
legend('y = -1.66x - 0.0478' , 'degree distribution', 'Erdos-Renyi','Barabasi Albert');
hold off;
clear v1 v2 v3 v4 a b c d e f i j k x y z ;
```

A.2 Clustering coefficient

Το script για τον υπολογισμό του clustering coefficient δέχεται ως είσοδο τον adjacency matrix του δικτύου και στην έξοδο επιστρέφει ένα γράφημα με λογαριθμικό άξονα Y, στο οποίο παρουσιάζεται η κατανομή των τιμών του clustering. Για τους κόμβους με degree ίσο με 0 ή 1, δεν ορίζεται το clustering coefficient. Σε αυτές τις περιπτώσεις προκύπτει τιμή NaN για τον συγκεκριμένο κόμβο η οποία δεν τυπώνεται στο γράφημα. Επίσης δεν τυπώνουμε και όλες τις τιμές που έχουν μηδενική πιθανότητα στην κατανομή.

```
c  = 1:169;
k = sum(Adj,2);  % Υπολογισμός degree κάθε κόμβου απ' τον Adjacency matrix
k = transpose(k);
for i = 1:169      % Υπολογισμός του local clustering coefficient για κάθε κόμβο
   c(i) = 0;
   for j = 1:169
      for h = 1:169
         c(i) = c(i) + (Adj(i,j) * Adj(i,h) * Adj(j,h));
      end
   end
   c(i) = c(i) / k(i)/(k(i) - 1);
end
c_avg = 0;        % Υπολογισμός του μέσου local clustering coefficient
for i = 1:169      % Αποφεύγουμε να λάβουμε υπόψη τους κόμβους με Local cc = NaN
```

```
    if isnan(c(i))
    else
        c_avg = c_avg +c(i);
    end
end
c_avg = c_avg / 169
h = 1;
prop = 1:20;
for i = 0:0.005:1
        prop(h) = 0;
    for j = 1:169                       % Κατασκευή του ιστογράμματος, μετράμε πόσοι
if ((c(j)>=i) && (c(j)<(i+0.005)))    % κόμβοι έχουν clustering που ανήκει σε κάθε ένα από τα
            prop(h) = prop(h) + 1;      % διαστήματα πλάτους 0.005 μεταξύ 0 και 1.
        end
    end
    prop(h) = prop(h) / 169;      % Διαιρούμε με το πλήθος για να υπολογίσουμε την πιθανότητα
    h = h + 1;
end
axisx = 0:0.005:1;
j = 1;
for i = 1:200                           % Δεν τυπώνουμε τα μηδενικά
    if (prop(j) == 0)
        prop(j) = [];
        axisx(j) =[];
    else
        j = j+1;
    end
end
semilogy(axisx,prop,'m*')
legend('clustering coefficient distribution');
```

A.3 Centralities

Όλα τα μεγέθη centrality υπολογίστηκαν με τους τύπους που περιγράφονται αυτόματα από την matlab. Η συνάρτηση με την οποία υπολογίζει τις τιμές η matlab αναφέρεται στις παραγράφους 3.1.3 έως 3.1.6 για κάθε μέτρο centrality. Ως είσοδο δέχονται οι εντολές της το γράφο G που προκύπτει από τον adjacency matrix ως

G = graph(Adj);

Για τον υπολογισμό:

centrality('betweenness', G);

centrality('closeness', G);

centrality('pagerank', G);

centrality('eigenvector', G);

Η έξοδος κάθε εντολής είναι ένα διάνυσμα μήκους όσοι και οι κόμβοι του δικτύου, με την τιμή για κάθε έναν από αυτούς.

A.4 Assortativity

Επειδή ο τύπος για την assortativity, όπως παρουσιάζεται στην παράγραφο 3.1.7 έχει πολλούς επιμέρους υπολογισμούς, γι' αυτό και στο script τον χωρίζουμε στους παράγοντές του οι οποίοι υπολογίζονται χωριστά και στο τέλος συντίθεται το τελικό αποτέλεσμα. Είσοδος του script είναι ο adjacency matrix του δικτύου και έξοδος η τιμή A της assortativity.

```
K = sum(Adj);                    % Degree
A1 = 0;
A2 = 0;
A3 = 0;
for i = 1:169                    % Υπολογισμός του r στην παράγραφο 3.1.7
   for j = 1:169
```

```
      if(j>i)
         A1 = A1 + K(i) * K(j) * Adj(i,j);
         A2 = A2 + (K(i) + K(j)) * Adj(i,j) / 2;
         A3 = A3 + (K(i)^2 + K(j)^2) * Adj(i,j) / 2;
      end
   end
end
E = sum(K) / 2;
A1 = A1 / E;
A2 = (A2 / E)^2;
A3 = A3 / E;
A = (A1 - A2) / (A3 - A2)          % Assortativity
clear A1 A2 A3 K E I j ;
```

A.4.1 Local assortativity

Χρησιμοποιούμε τον τύπο για τον υπολογισμό της τιμής ρ_n στο κεφάλαιο 3.1.7. Με είσοδο τον adjacency matrix υπολογίζουμε χωριστά όλες τις επιμέρους παραμέτρους του τύπου και στο τέλος σε μορφή διανύσματος την τιμή για κάθε κόμβο.

```
k = sum(Adj);
ex_k = k - 1;                      % Excess degree
dev = std(ex_k)^2;                 % Τυπική απόκλιση
M = sum(k)/2;
m_square = (sum(ex_k)^2 + sum(ex_k.^2)^2 + 2 * sum(ex_k) * sum(ex_k.^2)) / (4 * M^2);
local_ass = zeros(1,169);
k_avg = zeros(1,169);
for i = 1:169                      % Υπολογισμός του local assortativity βάσει του τύπου
   for j = 1:169                   % στο υποκεφάλαιο assortativity
      if(Adj(i,j) ~= 0)
```

```
        k_avg(i) = k_avg(i) + ex_k(j);
      end
    end
   k_avg(i) = k_avg(i) / k(i);
   local_ass(i) = (k(i) * ex_k(i) * (k_avg(i) - sqrt(m_square))) / (2 * M * dev);
end
clear k ex_k dev m M k_avg i j ;
```

A.5 Τελικό αποτέλεσμα

Οι υπολογισμοί της παραγράφου 3.3 έγιναν στην matlab με το script που παρατίθεται. Σαν είσοδο δέχεται τις εξόδους των παραπάνω scripts. Δηλαδή τον πίνακα external από το script που υπολογίζει τις modularity classes, τον πίνακα c, από το script που υπολογίζει τον local clustering coefficient. Ακόμα δέχεται τον adjacency matrix του δικτύου. Ως έξοδο υπολογίζει τις τιμές *F, P* και *Τα* και την τελική τιμή *S* για κάθε κόμβο.

```
T = zeros(1,169);
g = graph(Adj);        %Δημιουργία του γραφήματος απ' τον adjacency matrix
b = centrality(g, 'betweenness');
p = centrality(g, 'pagerank');
ec = centrality(g, 'eigenvector');
cl = centrality(g, 'closeness');
count = 0;
countf = 0;
sav = 0;
for i = 1:169          %Όπου δεν ορίζεται το local clustering, δηλαδή ο
   if isnan(c(i))      %κόμβος είναι απομονωμένος, έχουμε T = F = 0
       T(i) = 0;
       F(i) = 0;
```

```
    else
        F(i) = 1007.07731689290310*k(i)*(external(2,i))^2*cl(i)/((1+abs(20-k(i)))*(9*c(i)+1));
        if (k(i) > 2)
            T(i) = 3.156834695445477e-05*(k(i)*external(2,i))^2 * (k(i)/(1+abs(20-k(i)))) * p(i) *
sqrt(b(i))*(10/(9*c(i) + 1));
        else
            T(i) = 0;
        end
    end
    P(i) = 339.8434325821883*(k(i)*ec(i))/(1 + abs(20 - k(i)));
    if (P(i) == 0)      %Υπολογισμός των μέσων F/P και 10 * T/P
        a(i) = 0;
        fct(i) = 0;
        count = count+1;
        countf = countf+1;
    else
    a(i) = F(i)/P(i);
    fct(i) = 10 * T(i) / P(i);
    end
end
fc = (169-countf)/sum(fct); %Μέσο 10 * T/P
med = sum(a)/(169-count);   %Μέσο F/P
S = ((1+med) * F/mean(F)).^2 + (P/mean(P)).^2 + T/(10*mean(T));
S = 100*S/max(S);           %Κανονικοποίηση
for i = 1:169
    if (S(i)<1)             %Δεν θέλουμε να τυπώσουμε τις μικρές τιμές που
        S(i) = NaN;         %δεν μας ενδιαφέρουν
    else
        sav = sav + S(i);
    end
```

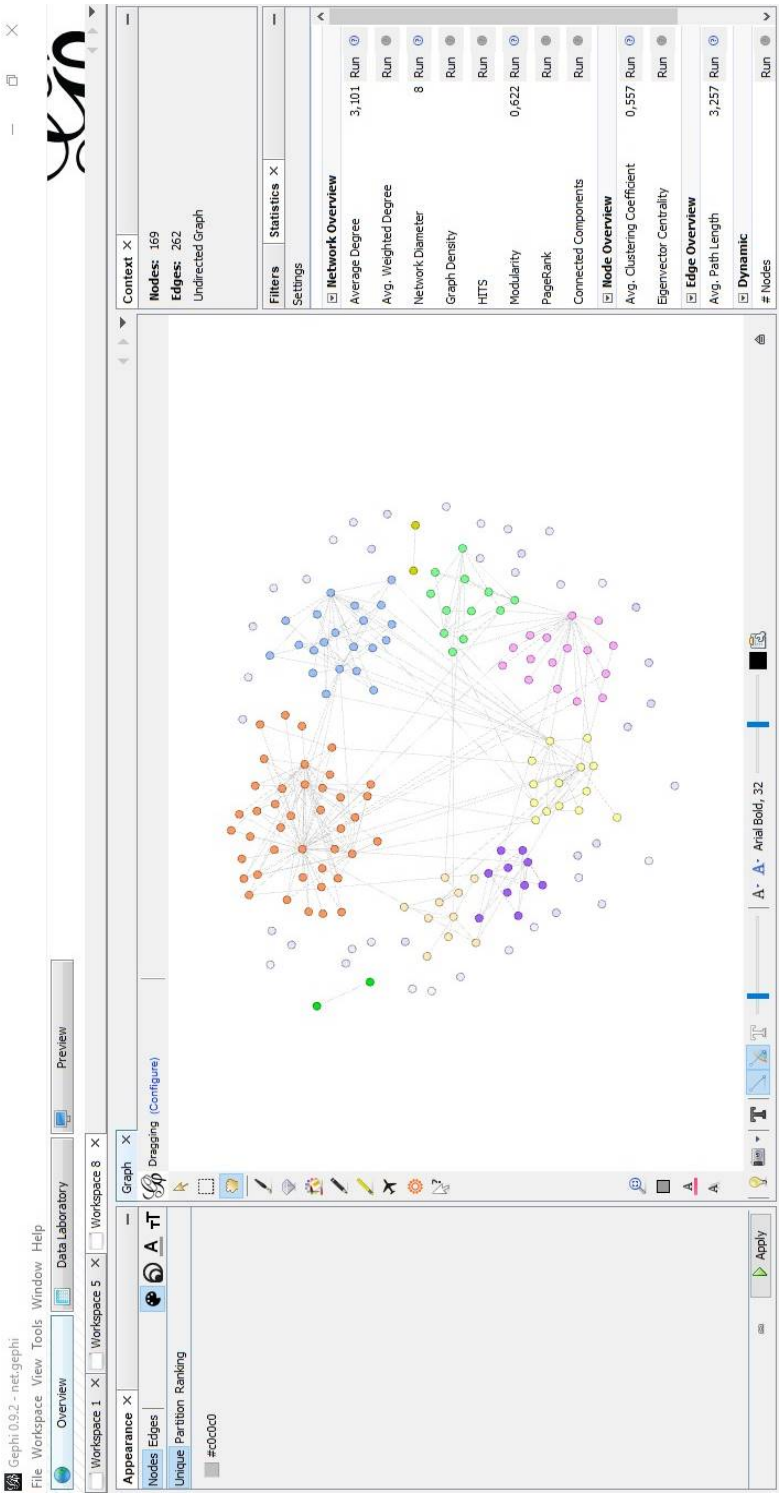
```
    if (T(i)<1)
        T(i) = NaN;
    end
    if (P(i)<1)
        P(i) = NaN;
    end
    if (F(i)<1)
        F(i) = NaN;
    end
end
plot(S,'*','Color',[0.1,0.7,0.8])   %Τύπωση για το σχήμα 15
xticks(0:10:150);
xlabel('Node');
ylabel('S value');
sav = sav/9;
hline = refline([0 sav]);
hline.Color = '[0.9,0.1,0.2]';

                %Εναλλακτικά τύπωση για το σχήμα 16
hold on
plot(F,'*r');
plot(P,'g*');
plot(T,'b*');
ylabel('values');
legend('F','P','T');
hold off

clear T g b p ec cl count countf  i fc fct a med  P F
```

Παράρτημα 2

Οι γραφικές απεικονίσεις των δικτύων καθώς και η εξαγωγή του modularity έγινε με το πρόγραμμα gephi. Αυτό είναι μία διαδραστική πλατφόρμα απεικόνισης και εξερεύνησης για δίκτυα και γράφους οποιουδήποτε τύπου ή μεγέθους. Το gephi είναι open source λογισμικό και σε μεγάλο βαθμό καλύπτονται οι ελλείψεις του από τη συνεισφορά διαφόρων προγραμματιστών. Η πλατφόρμα της απεικόνισής του χρησιμοποιεί 3D rendering ώστε ο χρήστης να αλληλεπιδρά με την απεικόνιση του δικτύου σε πραγματικό χρόνο, μέσα από τον χειρισμό των δομών, σχημάτων και χρωμάτων ώστε να αποκαλυφθούν οπτικά οι ιδιότητες του δικτύου. Το gephi είναι ένα συμπληρωματικό εργαλείο στην στατιστική ανάλυση του δικτύου που βοηθάει την κατανόηση και επεξήγηση των ιδιοτήτων και φαινομένων.

Έχει τρία κεντρικά μενού, το overview απ' όπου ο χρήστης ρυθμίζει τις ιδιότητες του δικτύου οι οποίες θα αποτυπώνονται στην οπτικοποίησή του. Μπορεί κανείς να ρυθμίσει το μέγεθος, χρώμα και την διαφάνεια των κόμβων και των ακμών, ανάλογα με μεγέθη που έχει ήδη υπολογίσει. Επίσης το menu του overview έχει πολλά χρήσιμα εργαλεία όπως την εύρεση ελαχίστων μονοπατιών, τον υπολογισμού των degree, clustering, centralities και modularity. Μέσα από αυτό τέλος δίνεται στο δίκτυο το σχήμα που θα έχει καθώς εκεί μπορούν να μετακινηθούν χειροκίνητα ή αυτοματοποιημένα οι κόμβοι του δικτύου. Η αυτοματοποιημένη μετακίνησή τους ωστόσο δεν είναι πολύ καλά υλοποιημένη. Το δεύτερο κεντρικό μενού είναι το data laboratory. Εκεί δύναται κανείς να επεξεργαστεί τους κόμβους και τις ακμές του δικτύου και τα στατιστικά μεγέθη που έχουν υπολογισθεί. Επίσης είναι δυνατό να εισαχθεί στο gephi κάποιος πίνακας σε αρχείο .csv που να αναπαριστά το δίκτυο. Αυτός μπορεί είτε να έχει την μορφή ενός adjacency matrix, είτε να έχει σε δύο στήλες όλα τα ζευγάρια κόμβων που συνδέονται. Μπορεί ακόμα μετά την επεξεργασία των δεδομένων στο gephi, να εξαχθούν κάποιες στήλες που απεικονίζουν τιμές κάποιων στατιστικών μεγεθών (degree, modularity κλπ) για κάθε κόμβο, πάλι σε αρχείο .csv. Το τρίτο menu 'preview', έχει να

κάνει με την απεικόνιση του δικτύου και εκεί ρυθμίζεται ο τρόπος που θα απεικονίζονται οι κόμβοι και οι ακμές βάσει είτε κάποιον προκαθορισμένων στυλ είτε αυτού που διαμορφώνει ο χρήστης.



Σχήμα 1. Το περιβάλλον του Gephi

Παράρτημα 3

Το script της matlab που παρατίθεται εδώ δεν χρησιμοποιήθηκε για τον σκοπό της εργασίας όμως μπορεί να φανεί χρήσιμο για την περεταίρω μελέτη ενός δικτύου. Χρησιμοποιείται για να υπολογίσει σε πόσες και ποιες modularity classes ανήκει ένας κόμβος. Η μεταβλητή modularity, είναι ο πίνακας όπως αυτός εξάγεται από το πρόγραμμα Gephi που χρησιμοποιήθηκε, που περιλαμβάνει για τον κάθε κόμβο, τον κωδικό του, “Id” στην πρώτη στήλη και την modularity class στην οποία ανήκει στην δεύτερη. Κατά την εισαγωγή του στη matlab, επιλέγουμε μόνο αυτές τις δύο στήλες. Η έξοδος του script είναι ο πίνακας external του οποίου κάθε στήλη αντιστοιχεί σε έναν κόμβο. Στην πρώτη γραμμή βρίσκεται το πλήθος δεσμών προς διαφορετικές από τη δική του modularity classes. Στην δεύτερη γραμμή Το πλήθος modularity classes πέραν αυτής στην οποία ανήκει ο κόμβος, με τις οποίες συνδέεται. Τέλος στην Τρίτη γραμμή, βρίσκεται ένας δεκαδικός αριθμός όπου κάθε του ψηφίο αντιστοιχεί σε μία modularity class και μας δείχνει με πόσα άτομά της συνδέεται ο κόμβος. Δεν εξετάζουμε πάλι αυτή στην οποία ανήκει. Το script μπορεί να δουλέψει μόνο για αυτής της κλίμακας δίκτυα, με λίγες modularity classes και λιγότερους από δέκα γείτονες ανά κόμβο σε κάθε διαφορετική από την δική του τάξη.

```
modularity = table2array(modularity);
k = sum(Adj);                       %Υπολογισμός degree
mod_class = zeros(1,169);
count = 9;
   for j = 1:169
      if (modularity(j,1) < 170)
         mod_class(modularity(j,1)) = modularity(j,2);
      end
      if (k(j) == 0)                %Μετράμε πόσοι κόμβοι έχουν degree = 0
```

```
            mod_class(j) = count;
            count = count + 1;
        end
    end
external_who = zeros(1,169);
external_count = zeros(1,169);
external_diff = zeros(1,169);
for i = 1:169
    for j = 1:169
        if((Adj(i,j) ~= 0) && (mod_class(i) ~= mod_class(j)))
%Μετράμε με πόσους από κάθε τάξη συνδέεται ο i
            external_who(i) = external_who(i) + 10^(-mod_class(j));
%Και με πόσους συνολικά
            external_count(i) = external_count(i) + 1;
        end
    end
end
external = zeros(3,169);
external(1,:) = external_count;
external(3,:) = external_who;
for i = 1:169                       %Υπολογίζουμε με ποιές τάξεις συνδέεται
    st = num2str(external_who(i),9);
    st = char(st);
    sz = size(st,2);
    for j = 1:sz
        if (st(j) == 'e')
            break
        end
        if ((st(j) ~= '0') && (st(j) ~= '.'))
            external_diff(i) = external_diff(i) + 1;
```

```
        end
    end
end
external(2,:) = external_diff;
%clear('external_count', 'external_who', 'external_diff', 'i', 'j', 'k', 'mod_class', 'count');
```

Ο κόσμος είναι δίκτυο κι εσύ ο μόνος κόμβος
Να μη με βγάλει μια ακμή που 'μαι έρημος και μόνος