**HY-335 – Δικτυα Υπολογιστων**

**Project Spring 2016**

“Building Short Anonymous Networks”

**Report**

Ομάδα :

* Ατζαμής Ιωσήφ , 3094
* Δεδούσης Ανδρέας , 3018
* Καρδουλάκης Νίκος , 3086

Το project αποτελειται από τα εξης αρχεια :

* Client.py
* Relay\_node.py
* End\_servers.txt
* Files2download.txt
* Relay\_nodes.txt

**Client.py**

Ο client ειναι ο βασικος παραγοντας και υπευθυνος για την ροη του προγραμματος. Παιρνει σαν παραμετρο 2 αρχεια, το πρωτο (end\_servers.txt) περιεχει το Url των end servers καθως και το allias τους και το δευτερο (relay\_nodes.txt) το οποιο περιεχει πληροφοριες σχετικα με τους relay\_nodes , δηλαδη IP και port.Αρχικα διαβαζει τα 2 αυτα αρχεια και τα αποθηκευει σε αναλογα dictionaries.Στην συνεχεια ζηταει απο τον χρηστη να δωσει ενα allias αριθμο ping και κριτηριο για την επιλογη καλυτερης διαδρομης (latency/hops).

Μετα, με την χρηση sockets και threads ξεκιναει direct συνδεση με τον end server και με καθε relay node καθως και συνδεσεις αναμεσα σε relay\_node και end\_server και υπολογιζει το RTT και τον αριθμο των hops σε καθε συνδεση.

Με βαση το κριτηριο που εχει εισαγει ο χρηστης επιλεγεται η καλυτερη διαδρομη και τελικα γινεται η ληψη του αρχειου και υπολογιζουμε τον χρονο που χρειαστηκε.

* def ping(num ,ip2,direct):

Παιρνει σαν παραμετρο τον αριθμο ping που εχει εισαγει ο χρηστης (num), ip προς την οποια θα υπολογιστουν ping και traceroute( ip2) και μια μεταβλητη που καθοριζει αν προκειται για direct συνδεση ή relay.Υπολογιζει τις αντιστοιχες τιμες και τις επιστρεφει.

* def connect\_relay(user\_alias,

relay\_ip,port,

ip,user\_ping,down):

Η συναρτηση αυτη καλει την προηγουμενη και υπολογιζει traceroute για την συνδεση client < -- > relay node και ανοιγει συνδεση μεταξυ τους.Στελνει καποια δεδομενα στον relay και στην συνεχεια περιμενει την απαντηση του στην οποια περιεχονται Ping και traceroute απο το relay στον end\_server.Τελος υπολογιζει το συνολικο ping και αριθμο hops αναμεσα σε client και end server και τα επιστρεφει.

* def find\_min\_RTT(y) :

Η συναρτηση αυτη καλειται οταν ο χρηστης εχει επιλεξει ως κριτηριο επιλογης το latency ή στην περιπτωση που εχει επιλεγει το hops ως κριτηριο αλλα δεν υπαρχει μοναδικη καλυτερη διαδρομη.Αυτο καθοριζεται απο την παραμετρο y (η οποια παιρνει τιμες 0 ,1 ).

* def find\_min\_HOPS(y):

Η συναρτηση αυτη καλειται οταν ο χρηστης εχει επιλεξει ως κριτηριο επιλογης το Hops ή στην περιπτωση που εχει επιλεγει το latency ως κριτηριο αλλα δεν υπαρχει μοναδικη καλυτερη διαδρομη.Αυτο καθοριζεται απο την παραμετρο y (η οποια παιρνει τιμες 0 ,1 ).

* def download():

Η συναρτηση αυτη κατεβαζει το αρχειο που ζητηθηκε και υπολογιζει τον χρονο που χρειαστηκε.

* def relay\_download(user\_alias,

relay\_ip,port,

ip,user\_ping,down):

Η συναρτηση αυτη χρησιμοποει sockets για την συνδεση client και relay\_node . Η συναρτηση αυτη τρεχει στον client και στελνει δεδομενα στον relay node οπως IP ,ping και url και στην συνεχεια περιμενει σαν απαντηση το αρχειο απο τον relay\_node

**Relay\_node.py**

Αρχικα ο relay node υπολογιζει random το port ου θα γινει η συνδεση. Στην συνεχεια ανοιγει ενα TCP socket και κανει bind την ΙP του υπολογιστη και την port που μας εδωσε η random. Επειτα περιμενει μεχρι να γινει καποια συνδεση.Οταν τελικα εχουμε συνδεθει γινεται η μεταφορα των δεδομενων απο τον Client στον relay ( IP, USER\_PING,URL,DOWN).Αναλογα μετην τιμη που θα εχει το flag down, o relay ειτε υπολιγιζει το PING και τα hops και στελνει πισω τις τελικες μετρησεις ειτε κατεβαζει το αρχειο με βαση το url.

* def ping(num , ip2):

Παιρνει σαν παραμετρο τον αριθμο ping που εχει εισαγει ο χρηστης (num), ip προς την οποια θα υπολογιστουν ping και traceroute( ip2).Υπολογιζει τις αντιστοιχες τιμες και τις επιστρεφει.

* def download(url):

Η συναρτηση αυτη κατεβαζει στον relay το αρχειο που ζητηθηκε και υπολογιζει τον χρονο που χρειαστηκε.

**BONUS**

“File protection via encryption and e-mail authentication”

Βασικη ιδεα του bonus είναι η ασφαλης ληψη του αρχειου. Αυτό επιτυγχανεται με χρηση κρυπτογραφησης μεσω της βιβλιοθηκης AES.

Ο αλγοριθμος που περιγραφεται από την ΑΕS είναι ενας με συμμετρικα κλειδια, το οποιο σημαινει ότι χρησιμοποιει τα ιδια κλειδια για κρυπτογραφηση του αρχειου και αποκρυπτογραφηση του.

Στο relay\_node, στη συναρτηση download η οποια πραγματοποιει τη ληψη του αρχειου, καλειται η συναρτηση encrypt\_file με παραμετρους το ονομα του αρχειου και το κλειδι κωδικοποιησης. Αυτή καλει την encrypt, η οποια αρχικα καλει την pad , στην οποια κωδικοποιειται το μυνημα με βαση το AES.block\_size, και στη συνεχεια δημιουργει ένα καινουργιο κρυπτογραφημενο αντικειμενο.

Η ασφαλεια ενισχυεται επιπροσθετα με την απόστολη ενός e-mail από τον relay\_node το οποιο περιεχει έναν τυχαιο κωδικο απαραιτητο για την αποκωδικοποιηση του κρυπτογραφημενου αρχειου.

Ο client, απο την πλευρα του, μετα τη ληψη του αρχειου, καλειται να εισαγει τον κωδικο που εχει λαβει σε e-mail. Με τον σωστο κωδικο, καλουνται οι απαραιτητες συναρτησεις για την αποκωδικοποιηση του αρχειου.