iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** IV **Month of publication:** April 2020

DOI: http://doi.org/10.22214/ijraset.2020.4051

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

Traffic Analysis and Relay finding in Tor

Keyur Rathod[1], Hepi Suthar[2]
[1]*M. Tech Student, Department of Computer Engineering, Marwadi University, India*
[2] *Assistant Professor, Department of Computer Engineering, Marwadi University, India*

Abstract: ***Tor browser is mostly used by Hackers, Dark Web visitors, Fraudsters, Cybercriminals. It's popularly known for its anonymity and strong encryption mechanism which safeguards the communication and leaves no trace behind it. For adversary, Tor is crucial service for doing online illicit work, traffic analysis of tor is too difficult because all message is encrypted and no present software is capable of capturing the whole communication and decode it to the identified initiator. The motto for the research is if any hackers or adversaries use Tor service for performing an illegal activity which causes govt. or people. Most of the techies and Tor users know that finding illicit communication in a Tor network is quite difficult. The aim of the research is to identify illicit communication by analyzing the relay packets interaction inside the Tor network with the help of network traffic analysis. The crucial part is it's very difficult to locate the relay inside the Tor network. So if any crime happens then to locate the source is hard, this research is useful in that direction. The research works in two phases and this research is helpful for those who want to study and get deep knowledge about Tor and also for those who are deucedly to penetrate Tor.***

Keywords: Traffic analysis, relay finding, Tor Traffic analysis and network attacks, relay attack, cryptographic attacks, Tor network attacks, finding relay location

I. INTRODUCTION

As technology era is evolving day by day each activity of every person and every organization is under the surveillance of either government's secret agency, individual who is spying online activities, or by the unorganized committee whose only motto is to track all the activities of targeted person or organization and leak crucial information to the civilized people for just creating chaos. So, to secure every online activity of each person is a challenging task for the government as well as for profound companies who are providing security to their clients because information and data are a vital part of today's era. For a Cyber Security person information is very useful and vital, if a person knows how to play with data it can create chaos or it can stop the chaos. In an online world, information is the base of every organization and government. So it's necessary and very crucial to secure each data and defend against surveillance systems from an outsider like hackers who can monitor and record every activity and sell it to the illegal online committee like dark web or deep web with the purpose of earning money. The structure of the internet is mostly divided into 3 parts first part is a surface web which we familiar and commonly used by all the people on the internet, it compromises only 10% of the total size of information available on the internet. Largely unfiltered and cluttered sites are indexed on this surface like Facebook, Twitter, etc.

The rests 90% of the information is extremely well organized and filtered. It's popularly known as Dark Web and Deep Web among hackers and techies.

Deep Web holds the information on the internet which is not indexed by the standard search engines and mostly innocuous content like academic data, medical records, etc. while Dark Web is the most dangerous and deepest layer of Deep Web because the nature of the content is criminal and have illegal documents and some are very confidential govt. records. While diving into Dark and Deep Web to much security concern is there and protect own identity is crucial. So, Deep and Dark web users use VPN (Virtual Private Network), Tor Browser, etc. for anonymity purposes.

For a hacker, information is a very vital and benign source of earning money. For adversary or hacker to defend against a surveillance system is very crucial and becoming anonymous is very aider for hackers. Anonymity and Tor are very popular in the hacking world.

Tor (The Onion Routing) is very popular amongst hackers, techie's, online criminals and fraudsters because it provides anonymity, safeguard communication and leave no traces at the end. So for security surveillance, it's very hard to identify online criminal activities. The onion routing is originally developed in the 1990s by U.S. Naval Research Laboratory. The mathematician Paul Syverson, scientist Michael G. Reed, and David Goldschlag developed Onion Routing Protocol for providing better security and protecting online data privacy with the purpose of strong protection against network surveillance. Tor is very popular low latency based anonymous communication network used for licit and illicit activities.

As we talked earlier, available info. on the internet is mostly unindexed so techies and hackers utilize the Tor for illicit online activities like accessing govt. confidential data, unauthorized news leaks of sensitive information (ex. WikiLeaks), buying, selling, smuggling drugs, and weapons, stolen credit card numbers, money laundering, bank and credit card fraud, Gain access to censored information, distribution of illegal sexual content, exchange of counterfeit currency, etc.

Cyber World heavily depends on security work as technology evolves security concern is also evolving because if any person uses any online medium like Tor for doing crime then it's very hard to trace them and identify the person behind it As a security researcher, every technology and security mechanism has loopholes even Tor community has issued regarding research and needs improvement as Tor users know that every Onion site under Onion service is slightly different from normal websites. The address of each onion site is different and difficult to memorize and become a headache for daily visitors. Tor also uses the Onion routing technique and strong encryption mechanism so, it's difficult to trace illicit activities online. The main issues are Onion services are slower i.e. Tor slower than normal network and uses high bandwidth for network usage.

II. RELATED WORK

In the past decades there is a lot of work done against on traffic analysis of Tor network, previous researchers had done traffic analysis on either entry node or on exit node and in some cases both S. Chakravarty, M. V. Barbera et al. [5] worked on the effectiveness of active traffic analysis attack against Tor network using a statistical correlation method and Cisco NetFlow data to reveal a source of anonymous traffic which done in two phases and they monitor both entry and exit node relay data. [9] S. Chakravarty, G. Portokalidis et al. shows using two decoy servers they inject traffic pattern that exposes bait credentials for decoy services and deployed prototype implantation into the Tor network. Much research on traffic analysis happens on entry or exit points but this [6] R. Jansen, M. Juarez, et al. research conducted solely with middle relays and also worked on website fingerprinting to detect onion service usage. [8] Y. Gilad and A. Herzberg give methods to identify clients without eavesdrop on the communication to the server and also without relying on the traffic pattern using different network attacks and side channels attack based on two scenarios. P. Mittal et al. [7] showed that Tor (anonymity system) provide efficient service to its users by using full use of forwarding capacity and also this facility sometime leaks information about Tor relays in the circuit so, they present stealthy attacks based on throughput information can reduce uncertainty about bottleneck relay of any circuit whose throughput is observed to identify guard relays and whether 2 concurrent TCP connection belongs to the same user. Tor is always vulnerable against traffic analysis attack S. J. Murdoch and G. Danezis [10] present new traffic analysis technique shows which nodes are being used by Tor having a partial view of the network, this research gives a very good and brief idea about how to reduce the anonymity provided by Tor. The actual creator of Tor P. Syverson et al. [1] talks about second-generation onion router (Tor) and gives a brief idea about how Tor network work and motto behind creating this extraordinary low latency, popularly used anonymous network and also talk about limitation in original design with improvements.

The hidden server nowadays known as onion servers are a very crucial part of the Tor network because it allows clients(users) to interact with onion services L. Øverlier and P. Syverson [2] shows attacks on these hidden servers which reveals the location, there are the first actual intersection attacks on any anonymous deployed network. [4] P. Winter, A. Edmundson et al. studied and conduct an online survey of 517 users and 17 semi-structured interviews of Tor users on how they use onion services, network communication of Tor, problems regarding onion addresses and improvements needed in Tor and onion service. [3] Remembering onion service address is difficult so, J. Victors et al. introduce Onion Name System (OnionNS) which allows Tor users to reference any onion service by a meaningful globally unique verifiable name by the administrator.

III.RESEARCH METHODOLOGY

A. Architectural Diagram And Description Of The Proposed Work

The onion routing protocol (Tor) is out-turn of a P. Syverson, M. G. Reed and D. Goldschlag which is created for protecting the user's anonymity in Tor while using the internet.

Tor network is different from the traditional network, the backbone of Tor is onion servers and volunteer relays because onion server provides different onion services and volunteer relay helps in connecting to the onion servers, more the onion servers better the faster reply client get. Working of Tor is very stiff because first, it needs onion servers which provide different onion services (OS) to Tor users.

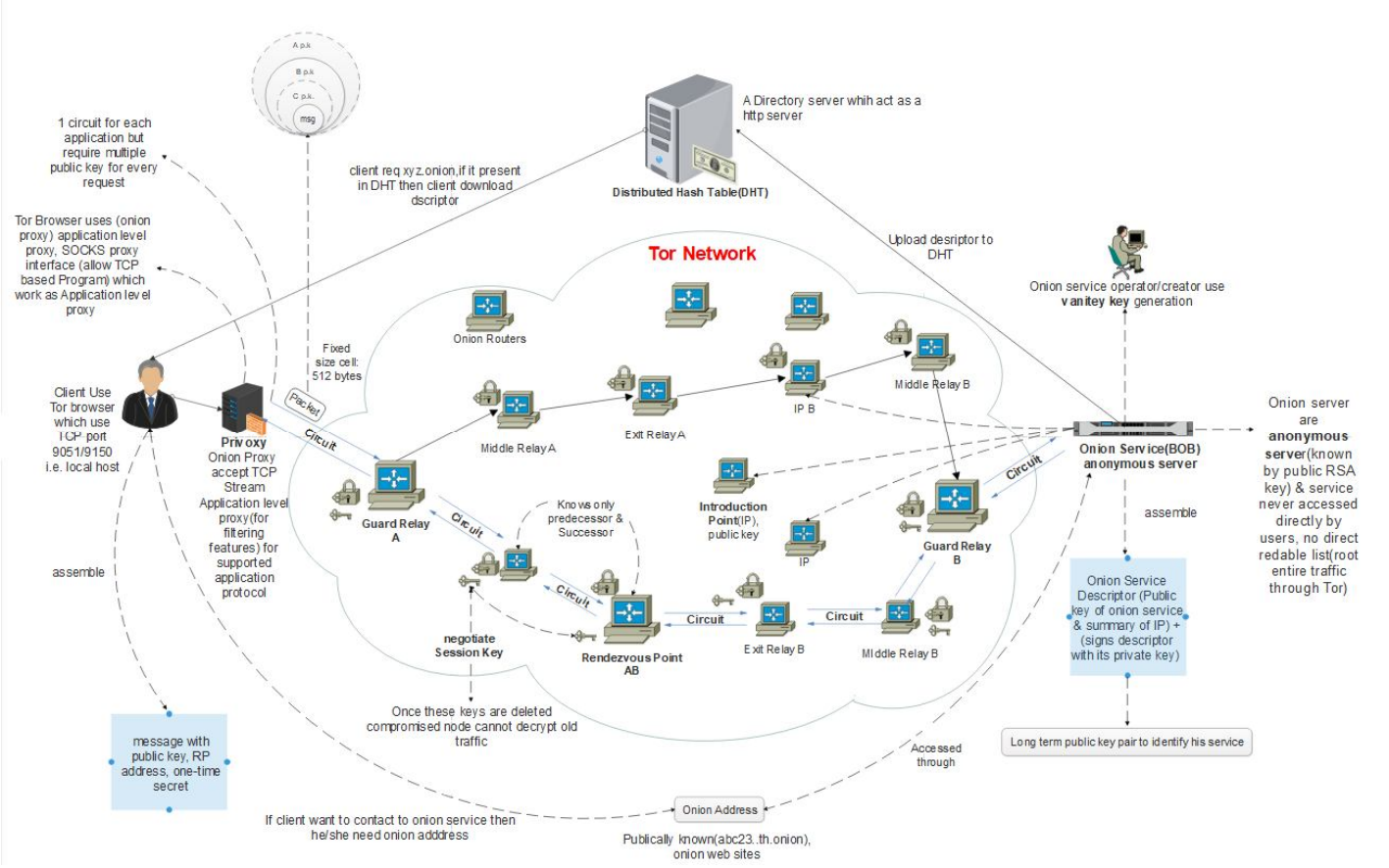


Fig. 1.Tor Architectural setup

Onion service creates a public key to advertise its existence inside Tor because a public key worked as an onion address through which users interact with different onion sites. OS creates an OS descriptor and uploads it to the Distributed Hash Table (DHT), now client/user download the DHT and knows about 16 characters long onion service address which is derived from services public key, after knowing onion address now client request to the DHT and ask services for connection. If the onion service exist and free to receive connection then client learns about onion service public key (onion service address) and IP-address, meanwhile client picks a random relay to build a circuit and assemble an introduction message (which contain one-time secret, address of Rendezvous Point) encrypt it with a public key of OS and send it back to an OS till now 1st half is completed. 2nd half involves actual communication, OS receives the message and decrypts it with its own private key and learns about RP, OS creates a circuit through RP and further communication done through that circuit, here RP tells the client that connection established. Here the important part is RP doesn't know the OS and also the client, it only worked as a tunnel between client and OS, and 6 hopes are used in entire communication.

This research is about finding relays location using traffic analysis of Tor, the main agenda for this research is criminal uses dark web and deep web for accessing govt. confidential data, gain access to censored information, and other illegal online activities in which the black market utilizes the Tor infrastructure. The expected outcome of this research is to find relay location inside the Tor network with the help of traffic analysis to identify cyber-criminal illicit activities and malicious payload which gives how many numbers of relays used for illicit communication, and their location. As discussed Tor is very popular among those cyber buddies who hire hackers or criminals to do illicit activities which scathe govt. or other legitimate organizations, it directly affects the black market because it revels the relay location inside the Tor network so, for govt. defense department it becomes easy to trace them. To achieve the goal of the research, the researcher divided the process flow into two different phases, phase-1 and phase-2. Both uses in the analysis of tor network phase-1 are about simulation setup of tor middle relay and gathering logs, analyze it and payload injection in normal network second phase directly deals with actual tor network and traffic analysis of Tor, network attacks, payload injection and result in analysis..

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

B. Detailed Operational Plan

While research is work in two phases both phases covers the analysis of Tor network, the first phase is a simulated bed environment in which tor middle relay is set up in two different Operating System (OS), Kali GNU/Linux kali-rolling version 2019.4, Ubuntu Bionic-Beaver version 18.04.3 LTS and to monitor relay utilization in Tor nyx version 2.1.0 is installed which gives a very good idea about relay working in a graph format, by this setup researcher get a good idea about the behaviour of middle relay and analyze logs. This setup is to run day and night for gathering good information and generating results, these results use in analyzing tor network for finding crucial information, here payload is a vital part of the research and test-bed setup because of payload helpful in locating the relay location, it's written in python language, first researcher test the payload in the normal network to gather router location (IP-address) to check whether it successfully penetrate the normal network or not, according to the researcher speculation if the payload failed to penetrate the normal network then it won't be able to penetrate complex and strong Tor network. To get the IP-address of a router which is connected in peer-to-peer network researcher to perform ethical attack here researcher make an assumption to check whether the payload is able to bypass the firewall of network and router without revealing itself, if successfully worked and give a list of routers IP-address in the whole network then this payload is mounted in Tor network, here payload is injected with https/http request to perform an ethical attack, using those statistic researchers generate a result which is helpful in phase two.

Phase two is an actual emulated bed setup in which researcher perform the real task on live Tor network, here phase-1 statistic and results are guide researcher in performing the attacks on Tor network, phase two describes the live Tor network in which middle relay is also needed to observe and capture traffic for analysis purpose. According to the statistic of each relay, the researcher generates the results and using those results graph is generated to describe the process. Here payload plays the vital role in the process because the payload is used for generating an attack on Tor network and furthermore it's also used in monitoring the behavior of itself, here researcher assumes that payload is strong enough to penetrate the Tor network and give at least 1st relay location i.e. first middle relay location place after guard relay. Here the main agenda of this phase is a researcher first check the possibility of the payload whether it's powerful enough to give the location of the relay then researcher attach the payload with http/https request and send it to the live Tor network here payload is programmed in such a way that it reverts back IP-address of the particular relay and spreading automatically inside the Tor network because the first middle relay broadcast the payload to other relays which are connected to the first middle relay and those relays also broadcast the payload to the further relays. And according to the results researcher creates a graph that describes the desired output.

C. Simulation Setup

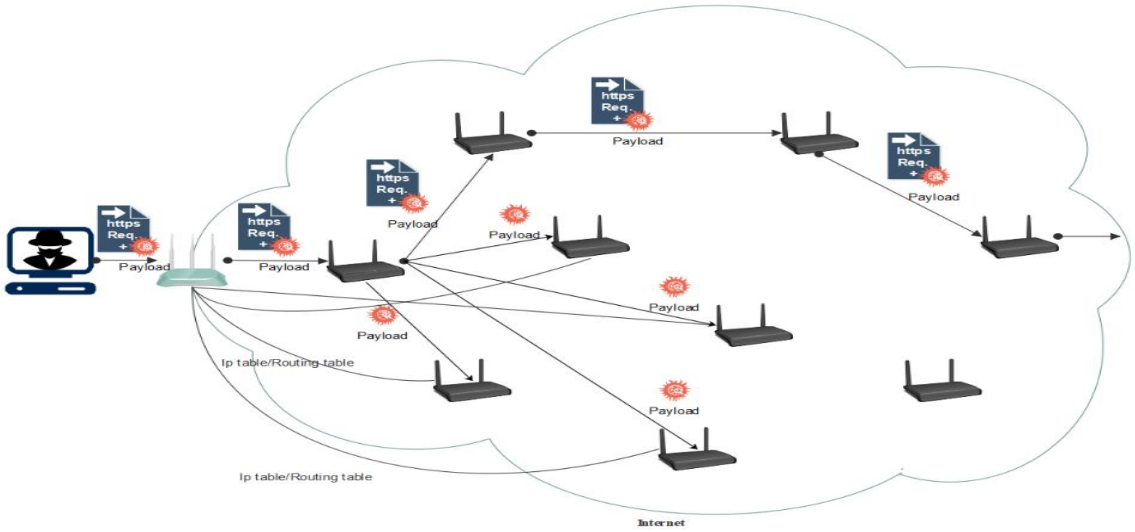


Fig. 2. Attack setup

The whole research practical is divided into two phases, the first is simulation testbed setup and second is the emulated testbed setup, in the simulation phase researcher first penetrates the network (a normal network which we used for accessing the internet). The first researcher creates a payload (a malicious payload) which used for exploiting the router. Here adversary (user) uses the payload to penetrate the router.

The first adversary creates a payload and then attach the payload to the web request (normal web request) i.e. http using Kali Linux tool, then every packet travels through the adversary router i.e. local router which connects to the other router in a network and together all routers establishes the profound network in which every router can communicate with each other router and decide the shortest path for any web request to the server for a host (user) in less time. The important part is how this works? So, each router has two things stored inside it, 1st is routing table/IP table 2nd is forwarding table. The routing table is responsible for choosing the best path because the routing table has the list of the connected routers i.e. IP address and it has multiple routing tables, in short, the routing table has the routing information, after deciding the best path for a prefix is selected. Now, the forwarding table comes into the picture, it has destination information i.e. where a packet is routed for a given IP (MAC address). After receiving the truthful information packet is routed through the nearest router (in networking it's called hopes or nodes) for the best and shortest path. This way routers are communicating inside the network. So when adversary (user) sends the http/https request (web request) first it visits the router (local router/home router) which connects adversary to the internet with the help of other routers in a network. The router gets the information and decides the shortest path by checking the routing tables and forwarding tables and then send to the next hope (nearest router). After that, the next hope receives the packets and also sends it to the next hope (nearest router) and goes on until it reaches the server (destination). This is how a path is established to the server and also the request-response is Travers by the same path. This is how our traditional network or internet is working, here we have to notice that there is no encryption mechanism is used by default so any powerful adversary can look up to the communication and infer it and can modify or change packets information completely, anything can be done but here researcher focuses on exploiting the router in a network. The researcher wants to exploit the router in order to get the routing table information (IP address) which gives a clear idea about how many routers are communicating with the researcher (adversary) router i.e. local router and send the payload to the nearest all routers. The work of payload is to return the routing table information to the adversary (researcher). So, only by penetrating (exploiting) half of the router in a network researcher (adversary) get the whole network idea i.e. how many routers in a network and it connects to the other router in a whole network. Here, by exploiting the few routers we get information on other routers. The important thing which we clear into our mind that if any user wants to find the routing path of request then simply go to the command prompt if you are Windows OS user and type tracrt command, if you are Linux OS user then go to terminal and type traceroute command both command will give you the same output i.e. routing path of your request so you can get an idea about how many routers (nodes) is in your path The main motto for performing this experiment. Here the vital part is any adversary can exploit its local router and get an idea about the routing table and see the list of a router but when packets visit the next node t also have routing tables inside it but adversary cannot identify that. Simply we get information about the local routing table but not get an idea about other routing tables. So payload work is to get the routing table which holds the list of IP address of other routers in a network and also researcher want to check the possibility of the payload whether it is powerful enough to penetrate the router or not and if it gets the successful attempt then how many routers it can exploit. Second, is payload pingback routing table information i.e. a list of IP addresses to the researcher or not i.e. simply to check whether the payload does the work what it made for or not. The third is if it is powerful enough to exploit the normal network if it is, then the researcher can deploy against the Tor network and check the workability inside Tor.

D. Tor Attack Setup

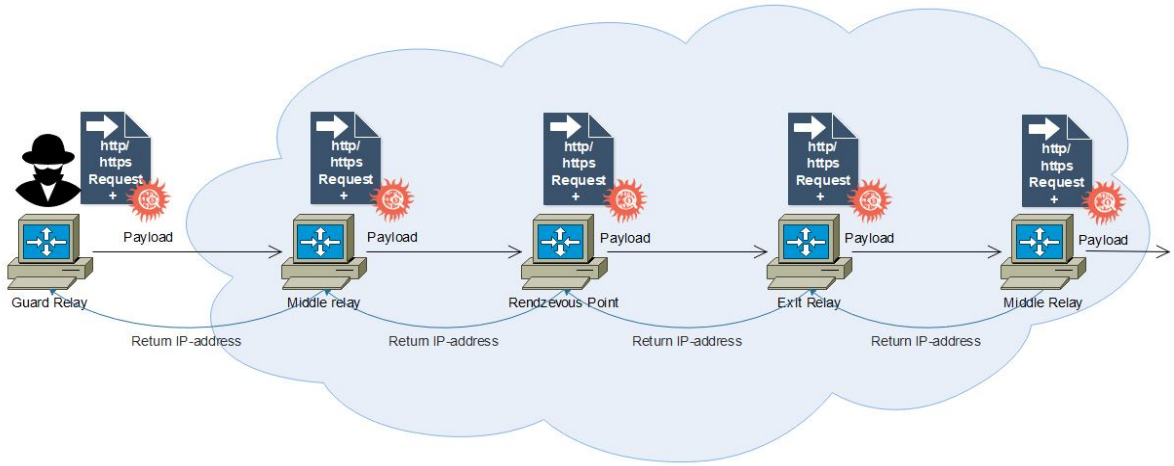


Fig. 2.1 Attack setup

Tor is quite tricky and different from the normal network because each relay in a circuit knows its successor and predecessor, no other relay in a circuit knows how many relays are there and the selection of each relay happens randomly. So it's tough to trace all relays in a circuit and its multilayer encryption technique i.e. like onion have multilayer same concepts and phenomena use it here and makes it more difficult to trace a request, and it uses a very strong connection TCP/TLS and this connection is not persistent. So for an adversary, this is a challenge to penetrate it, here the researcher creates one powerful malicious payload to penetrate the network, before deploying the payload in the Tor first it wants to perform into the normal network and check the feasibility of the payload according to the how much cause it can be done in a normal network according to that payload will be modified so, the first adversary creates a payload and bind it with http/https request (web request) and send it to Tor network. When the request (here at the bottom level request is divided into the chunks of packets and travels and visit each relay in a circuit) with payload enters into the Tor network it 1st connects with middle relay and then with rendezvous point (RP), exit, middle and finally goes to the exit relay which connects to the respected onion services according to request. So payload travels to the whole chain of a circuit when packets along with payload arrive at 1st relay its search for the IP-address of the machine and pingback to the adversary, then it shifts to RP, here it also searches for the IP-address and pingback to the middle relay and that relay pingback to the adversary, and so on. Here an important thing is each relay knows successor and predecessor and no other relays in a circuit that's why payload creates a 1 temporary persistence connection in a circuit because when packets along with the payload reach to a relay, each relay pingback its own IP-address to the adversary this way we can know the IP-address of each relay in a circuit. Here payload is useful in many ways first it creates a temporary persistence connection, it pings back IP-address of each relay. One important part in Tor is if any relay does not understand the message then it simply discard it or ignore it and doesn't allow a message to go further. So, the researcher designs a payload in such a way that if any relay discards the request then it pings back its last location in a network. This way adversary (researcher) knows the exact location of the last relay who discards the request and through this researcher or any adversary knows the full path with each relay location.

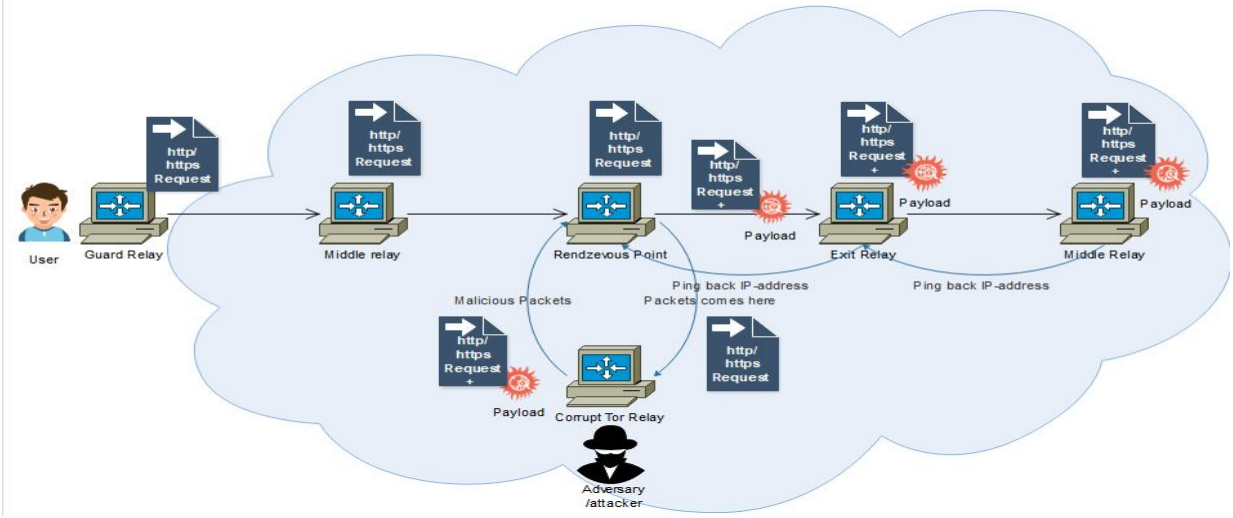


Fig. 2.2 Attack setup

The second stage is if 2.1 attacks setup does not successfully give the list of IP-address then an attacker has another attack setup i.e. in this setup attacker will create a corrupt middle realy as Tor users and researcher knows that each realy in a circuit knows either predecessor and successor no other relay in the circuit so by creating a corrupt realy and put it in between the circuit makes the concept useful because attaching corrupt realy in a circuit it knows predecessor and successor so, packets moves in a regular path but by attaching the attacker realy every packet changes the regular path and visit the attacker realy here attacker (adversary) check the previous relay IP-address and that previous realy also know its predecessor and successor so by this attacker get an idea about 3 realy in a circuit. Here corrupt realy attach the payload with packets and send back to the regular, that packets move forwards along with the payload when the packet reaches to the next realy it ping back the IP-address of that realy and next node IP-address by this attacker get the IP-address of other 4 relays. So in this way we can also identify the whole circuit and get each realy IP-address but the important thing is that is Tor circuit allows corrupt realy to be fit in to the circuit if it can then the second challenge comes that if RP forward packets to the corrupt realy? And corrupt relay ping the IP-address of realy or not. There is much concern that comes in the research. but through this way, we can identify each realy IP-address and detect the whole circuit.

IV. RESULTS

Analysis of Tor browser w.r.t other browser is showing up here. Each column represents different information with different values and also each column colour represents different information. Here Yellow box represents that .onion site is not able to open in normal browsers, and Red box represents connection time out. Green colour represents search string and Orange, Grey, Blue colour represents a different search engine. Here some test uses college internet and some test uses home internet (GTPL network).

Time delay analysis

Search string	Duckduckgo	Tor Browser	Google Browser
	Time format MM:SS:MS		
List of onion sites (general search)	00:03:83, 00:03:85, 00:00:53, 00:00:61	00:13:20	00:00:41 (4 times same result)
PROPUBLICA www.propub3r6espa33w.onion		00:55:50, 00:03:45, 00:01:31, 00:01:25	
thedarkweblinks.com	00:03:69, 00:02:86, 00:02:66, 00:02:58	00:06:78, 00:02:57, 00:02:63, 00:02:43	00:02:11, 00:01:90, 00:01:91, 00:01:90, 00:00:67, 00:01:61, 00:00:60
Facebook facebookcorewwwi.onion		00:03:45, 00:01:04, 00:00:99, 00:00:97	
Facebook (.com site)	00:01:06, 00:01:08, 00:00:70, 00:00:74	00:01:30, 00:01:10, 00:00:98, 00:00:89	00:01:40, 00:01:10, 00:01:02, 00:00:93, 00:00:92, 00:00:73, 00:00:64
sci-hub.tw/#about	00:01:33, 00:00:77, 00:00:74, 00:00:70	00:03:70, 00:00:99, 00:00:98, 00:00:86	00:03:51, 00:02:31, 00:01:93, 00:01:46, 00:01:32, 00:00:90, 00:00:79
Types of server (general search)	00:02:12, 00:00:89, 00:00:53, 00:00:63	00:02:55	00:00:63, 00:00:50, 00:00:46, 00:00:44, 00:00:48, 00:00:43 (4 times same result)
Dark web links (general search)	00:01:38, 00:01:92, 00:01:14, 00:00:75	00:09:33	00:00:40 (4 times same result)
thedarkweblinks.com	00:03:84, 00:03:13, 00:03:14, 00:02:76	00:05:20, 00:04:10, 00:04:12, 00:07:02	00:02:75, 00:01:92, 00:01:86, 00:01:78, 00:01:82
Drugs dark web link www.thedarkweblinks.com/page/7/	00:03:70, 00:03:44, 00:03:60, 00:02:40	00:02:99, 00:04:22, 00:03:01, 00:02:53	00:02:15, 00:03:22, 00:01:83, 00:02:40, 00:02:04
Drug website: Global Dreams www.zvz4ruc5b5q5yqz5.onion		03:01:99, 03:01:61 (connection timeout)	

Table 1. Time delay analysis

NOTE: There are some conditions which were considered while performing the practical:
The researcher did not use any VPN (Virtual Private Network) while performing the task, there are other factors which also have to be considered in this practice like human error, Internet speed, Website responding time, well-known sites take less time than less known sites.

Attacks observation

Research Paper	*Traffic Analysis Attacks*	*Network Attacks*	*Injection of Traffic*	*Traffic Pattern Analysis*	*End-to-end Encryption Attack*	*Cryptography Attacks*	*Side-channel Attack*	*Decoy traffic injection*	*Payload injection*
[1]	NO	NO	NO	NO	NO	NO	NO	NO	NO
[2]	NO	YES	NO	YES	NO	NO	NO	NO	NO
[3]	NO	YES	NO	NO	NO	YES	NO	NO	NO
[4]	NO	NO	NO	NO	NO	NO	NO	NO	NO
[5]	YES	YES	NO	YES	YES	YES	NO	NO	NO
[6]	YES	YES	NO	NO	YES	YES	NO	NO	NO
[7]	YES	YES	NO	NO	YES	YES	NO	NO	NO
[8]	YES	YES	NO	YES	YES	YES	YES	NO	NO
[9]	YES	YES	YES	YES	YES	YES	YES	YES	NO
[10]	YES	YES	NO	YES	YES	YES	NO	NO	NO
[11]	YES	YES	NO	YES	YES	YES	NO	NO	NO
[12]	NO	NO	NO	NO	NO	NO	NO	NO	NO

Table 2. Attack Observation

The researcher study Tor network and on the basis of some research paper researcher make a list of common attacks which can be used to analyze or penetrate the Tor network. The observation table is the analysis of the attacks which are helpful in the previous research.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

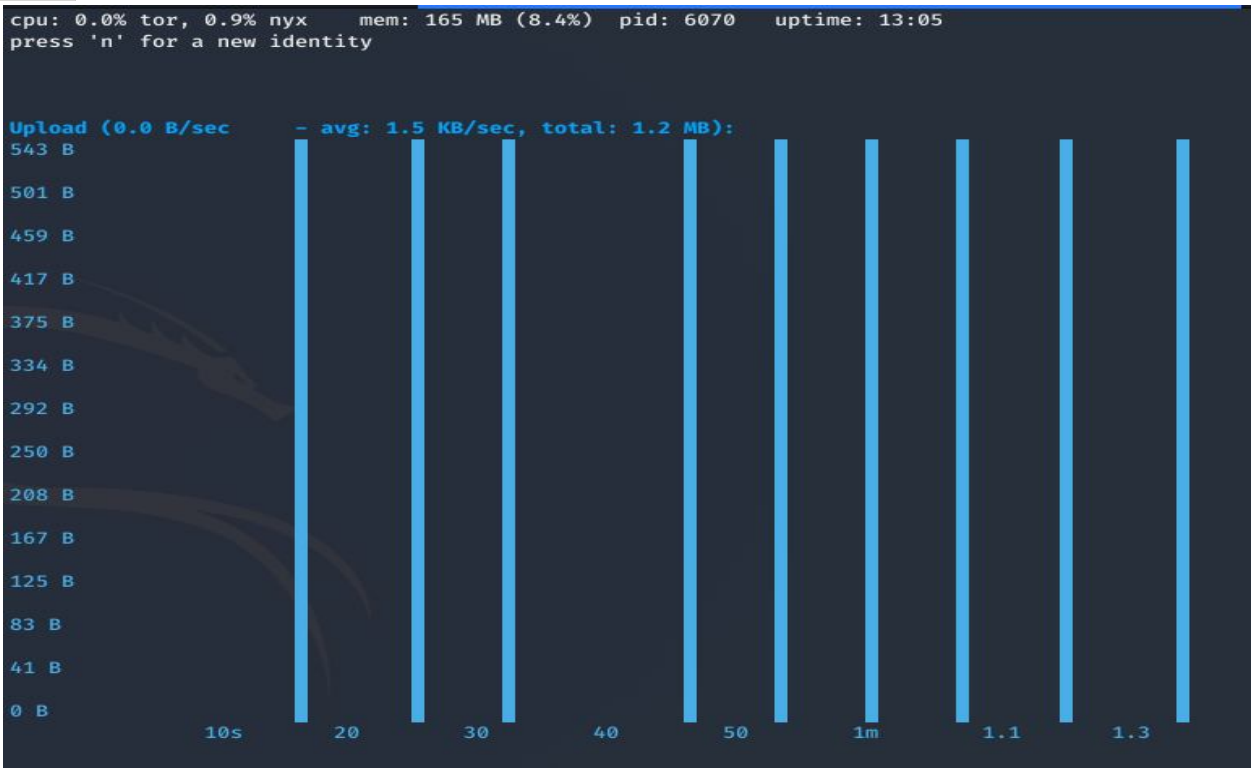


Fig. 3 Upload Speed Graph

Fig. 4 Download Speed Graph

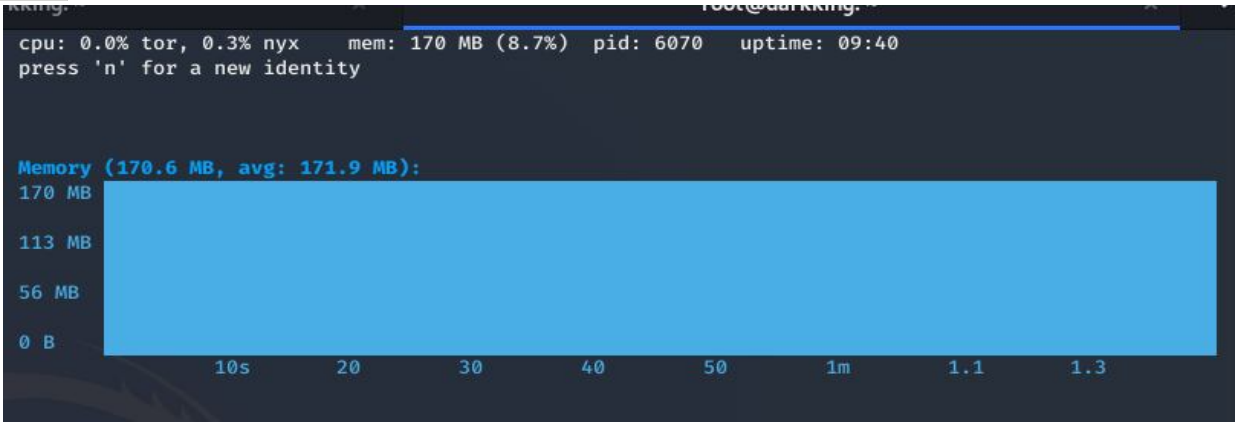


Fig. 5 Resource Speed Graph

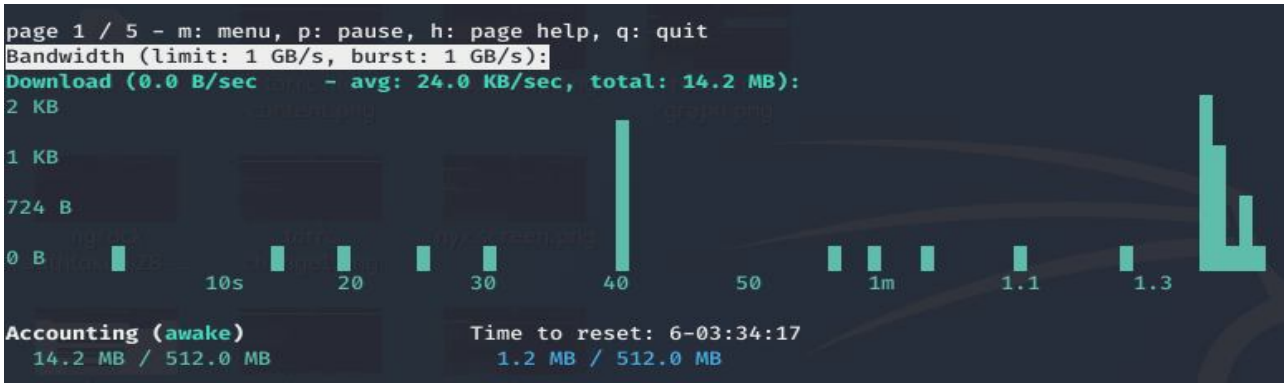


Fig. 6 Download Bandwidth Graph

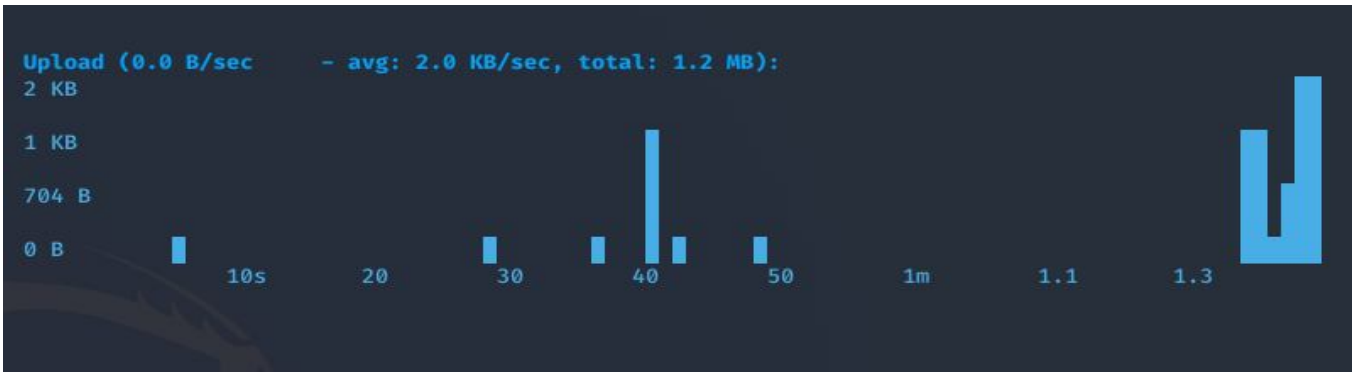


Fig. 7 Upload Bandwidth Graph

Fig. 8 Connection Graph

```
C:\Users\HP>netstat 0rn

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.0.104:17427    40.119.211.203:https   ESTABLISHED
  TCP    192.168.0.104:17469    ec2-34-243-213-235:8282  ESTABLISHED
  TCP    192.168.0.104:17751    sb-in-f188:5228        ESTABLISHED
  TCP    192.168.0.104:18918    104.27.188.10:http     TIME_WAIT
  TCP    192.168.0.104:18919    104.27.188.10:http     TIME_WAIT
  TCP    192.168.0.104:18920    104.27.188.10:http     TIME_WAIT
  TCP    192.168.0.104:18921    52.184.87.198:https    ESTABLISHED
  TCP    192.168.0.104:18923    shodan:https           ESTABLISHED
  TCP    192.168.0.104:18924    151.101.36.134:https   ESTABLISHED
  TCP    192.168.0.104:18925    shodan:https           ESTABLISHED
  TCP    192.168.0.104:18926    151.101.154.49:https   ESTABLISHED
  TCP    192.168.0.104:18927    map2:https             ESTABLISHED
  TCP    192.168.0.104:18928    151.101.0.134:https    ESTABLISHED
  TCP    192.168.0.104:18929    104.16.79.166:https    ESTABLISHED
  TCP    192.168.0.104:18930    shodan:https           ESTABLISHED
  TCP    192.168.0.104:18931    shodan:https           ESTABLISHED
  TCP    192.168.0.104:18933    114:https              ESTABLISHED
  TCP    192.168.0.104:18934    151.139.128.10:https   ESTABLISHED
  TCP    192.168.0.104:18935    ec2-34-234-61-170:https  ESTABLISHED
  TCP    192.168.0.104:18936    ec2-34-234-61-170:https  ESTABLISHED
  TCP    192.168.0.104:18938    240:https              ESTABLISHED
  TCP    192.168.0.104:18940    server-13-227-185-37:https  ESTABLISHED
```

Fig. 9 Active Routing Connection

The above all graph is a part of the Nyx tool which is be installed into Kali Linux OS by typing the following command into the terminal

sudo apt-get install nyx

It will automatically install all the dependencies and required resources then run the command

nyx

It will automatically start all the process, fig 2.3 and 2.4 shows the upload and download speed graph w.r.t time. Fig 5 is a resources graph which represents how many resources are connects to the middle relay, here researcher make a middle relay for analysis purpose. To make a middle relay first install the tor software by typing the following command in the terminal

sudo apt-get install tor

It will automatically install all the dependencies and required resources after that go open the torrc file by typing the following command into the terminal

nano /etc/tor/torrc

Uncomment the required lines [29],[30],[31],[32] and save it and then run the tor service then check the notices.log file if any error is there or for misconfiguration of tor then run the debug.log file by below command

tail –f /var/log/tor/notices.log

tail –f /var/log/tor/debug.log

Run the nyx and you will see the graphs fig. 3, 4, 5, 6, 7, and 8 it will give results in the form of graphs and give a better idea about tor services and how tor works it also lists the circuit details and directory details with the flags and other details.

V. FUTURE WORK

A. *Challenges*

Firewall error and internet issues in Tor relay and analysis issues due to protection by ISP. DirPort and ORPort is not reachable due to ISP blocking the Traffic. Available Payload not meet the requirements because as of now there are no payload available to satisfies the needs, the big reason is Metasploit payloads are people uses for exploiting now a days, and use readily available payload. Installation of tools is difficult because of lack of material and no proper indexing of available content. There are lot of challenges faced during the research like lack of person and time limitation according to available man strength.

The challenges faced during this research is dissolve by the researcher as a work is carried out in the next phase, as of now analyzing the middle relay and understanding the Tor relay and getting the complete idea about Tor network and understanding it completely.

VI. CONCLUSION

The research started in such a way that the researcher wants to get good in-depth knowledge about Tor, understanding the Dark Web and Deep Web, Criminal activities are done through the Tor and why the U.S. government is so concern and financially supporting its development. There is some assumption in the researcher's mind before starting the research is like Researchers want to check the possibility of the payload whether it is powerful enough to penetrate the normal network or not and also it is feasible to get the routing table or IP table of the router or not. If payload gets the successful attempt then how many routers can exploit. Second, is payload pingback routing table information i.e. a list of IP addresses to the researcher or not i.e. simply to check whether the payload does the work what it made for or not. If payload meets the desired output of what it made for then the researcher can modify it for tor in such a way that it can maintain persistent TCP connection, second, it pings the IP-address of the source (in our case relay). The third it's powerful enough to exploit the normal network or not and if it is, then the researcher can deploy against the Tor network and check the workability inside Tor.

This research paper gives a good idea about working of the Tor network, how the client/user connects to the Tor network and actual communication happen inside Tor which helps and guides readers to further analysis of Tor and future work. The researcher talks about how payload helpful in the entire research. This research is based on identifying relay location with the help of payload by binding it with the http/https request and send it to the Tor network and analyze the behavior or payload and also getting IP-address of a relay in a circuit. Here traffic analysis of a Tor plays a vital part to understand the Tor network in order to perform network attacks.

REFERENCES

[1] R. Dingledine, N. Mathewson, and P. Syverson "Tor: The Second-Generation Onion Router", 13th USENIX Security Symposium, San diego, CA, USA, August 9-13, 2004.

[2] L. Øverlier and P. Syverson. "Locating Hidden Servers". IEEE Symposium on security and Privacy, claremontresort-Oakland, California, USA, May 21-24, 2006.

[3] J. Victors, M. Li, and X. Fu "The Onion Name System: Tor-powered Decentralized DNS for Tor Onion Services". Proceeding on Privacy Enhancing Technologies symposium 2017(1), January 2017.

[4] P. Winter, A. Edmundson, L. M. Roberts, A. Dutkowska-Zuk, M. Chetty, and N. Feamster "How Do Tor Users Interact With Onion Services?" Proceedings of the 27th Usenix Security Symposium, Baltimore, MD, USA, August 15–17, 2018.

[5] S. Chakravarty, M. V. Barbera, G. Portokalidis, M. Polychronakis, and A. D. Keromytis "On the Effectiveness of Traffic Analysis Against Anonymity Networks Using Flow Records" Proceedings of the 15th Passive and Active Measurements Conference (PAM 2014), Los Angeles, CA, USA, March 10-11, 2014.

[6] R. Jansen, M. Juarez, R. Gálvez, T. Elahi, and C. Diaz "Inside Job: Applying Traffic Analysis to Measure Tor from Within" Proceedings of the 25th Symposium on Network and Distributed System Security (NDSS '18), San Diego, CA, USA, February 18-21, 2018.

[7] P. Mittal, A. Khurshid, J. Juen, M. Caesar, and N. Borisov "Stealthy Traffic Analysis of Low-Latency Anonymous Communication Using Throughput Fingerprinting" Proceedings of the 18th ACM conference on Computer and Communications Security, Chicago, Illinois, USA, October 17 - 21, 2011.

[8] Y. Gilad and A. Herzberg "Spying in the Dark: TCP and Tor Traffic Analysis" Proceedings of the 12th Privacy Enhancing Technologies Symposium (PETS 2012), Vigo, Spain, July 11–13, 2012.

[9] S. Chakravarty, G. Portokalidis, M. Polychronakis, and A. D. Keromytis "Detecting Traffic Snooping in Tor Using Decoys" Proceedings of the 14th International Conference on Recent Advances in Intrusion Detection, Menlo Park, CA, USA, September 20-21, 2011.

[10] S. J. Murdoch and G. Danezis "Low-Cost Traffic Analysis of Tor" Proceedings of the 2005 IEEE Symposium on Security and Privacy, The Claremont Resort, Oakland, California, USA , May 8-11, 2005.

[11] F. Rochet and O. Pereira "Dropping on the Edge: Flexibility and Traffic Confirmation in Onion Routing Protocols" Proceedings on 18th Privacy Enhancing Technologies Symposium (PETS 2018), Barcelona, Spain, July 24–27, 2018.

[12] P. Mittal, A. Khurshid, J. Juen, M. Caesar, and N. Borisov "OSINT Analysis of the TOR Foundation".

[13] R. Jansen, N. Hopper "Shadow: Running Tor in a Box for Accurate and Efficient Experimentation".

[14] N. Dutta and HKD Sarma, "A probability based stable routing for cognitive radio Adhoc networks", Wire. Net., (Springer), vol. 23(1), pp. 65-78, 2017.

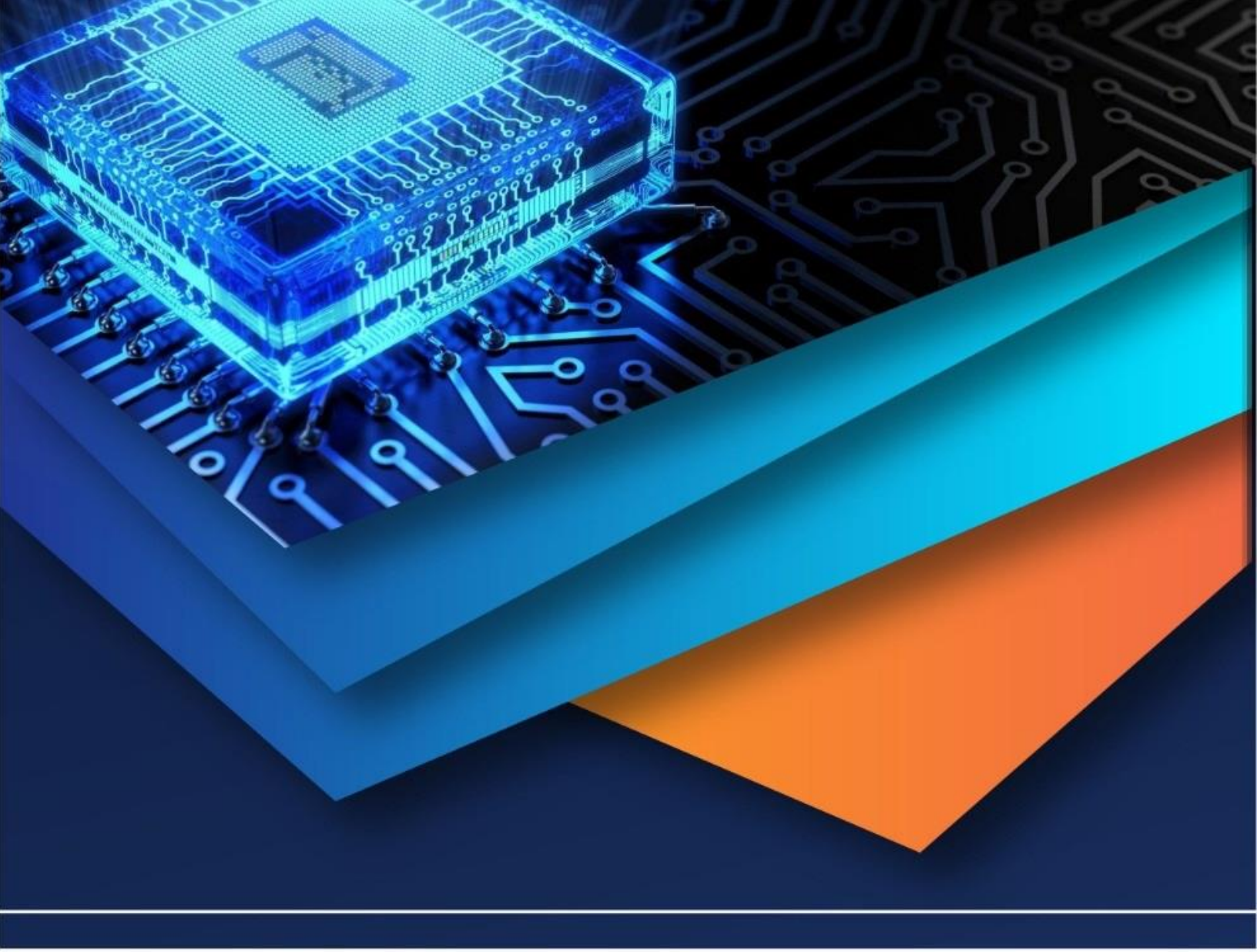
[15] N. Dutta and IS Misra,"Multilayer hierarchical model for mobility management in IPv6: a mathematical exploration", Wire. Pers. Comm.(Springer), vol.78 (2),pp.1413-1439, 2014.

[16] N. Dutta and IS Misra, "Mathematical modelling of HMIPv6 based network architecture in search of an optimal Performance", IEEE 15 th ADCOM, Guwahati, India, pp. 599-605, 2007.

[17] N. Dutta, HKD Sarma and Z. Polkowski, "Cluster based routing in cognitive radio Adhoc networks: reconnoitering SINR and ETT impact on clustering", Com. Com., (Elsevier), pp. 10-20, vol. 115, 2018.

[18] VMWare Workstation, accessed on 2019, https://www.vmware.com/

[19] Kali Linux, accessed on November 2019, https://www.kali.org/
[20] Wireshark, accessed on September 2019, https://www.wireshark.org/
[21] Research paper for Tor accessed on September 2019, https://www.freehaven.net/anonbib/
[22] Tor official website, accessed on September 2019, https://research.torproject.org/
[23] Tor official website, accessed on September 2019, https://skerritt.blog/how-does-tor-really-work/#overview-
[24] Tor official website, accessed on September 2019, https://2019.www.torproject.org/docs/documentation.html.en
[25] Tor Bridges websites, accessed on September 2019, https://2019.www.torproject.org/docs/bridges.html.en
[26] Guard node information, accessed on September 2019, https://support.torproject.org/tbb/tbb-2/
[27] list of Tor onion services, accessed on September 2019, https://en.wikipedia.org/wiki/List_of_Tor_onion_services
[28] list of onion sites, accessed on October 2019, https://www.gadgetgyani.com/top-best-onion-deep-web-sites/
[29] how to be a volunteer relay in tor network, accessed on October 2019, https://famicoman.com/2018/01/03/configuring-and-monitoring-a-tor-middle-relay/
[30] how to be a volunteer relay in tor network, accessed on October 2019, https://2019.www.torproject.org/docs/faq.html.en#torrc
[31] how to be a volunteer relay in tor network, accessed on October 2019, https://trac.torproject.org/projects/tor/wiki/TorRelayGuide
[32] how to be a volunteer relay in tor network, accessed on October 2019, https://2019.www.torproject.org/docs/tor-doc-unix.html.en
[33] routing table, accessed on, January 2020, http://www.fixedbyvonnie.com/2014/06/display-routing-table-windows-linux/#.XhVRdEczaM8
[34] EXIT NODE (Relay), accessed on February 2020, https://collector.torproject.org/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY