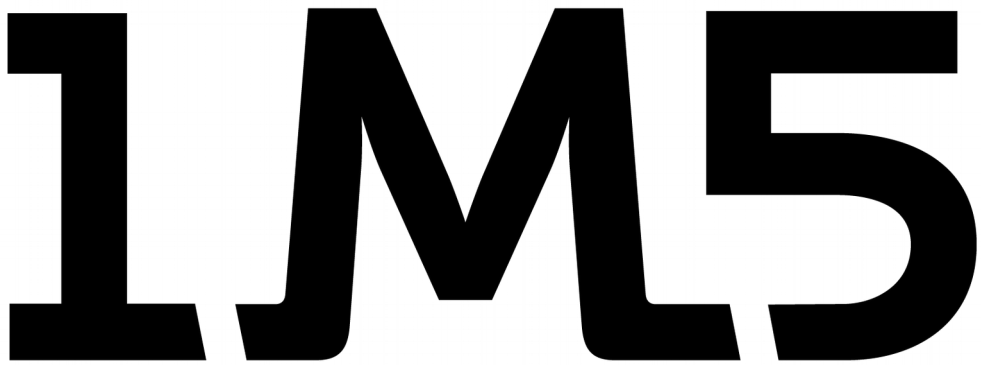


UNCENSORED COMMUNICATIONS

Invisible Matrix Services

Architecture Description
System v0.6.1
Document v9

Background

Invisible Matrix Services (1M5 using leet) is the first decentralized services platform with intelligent routing between anonymity networks to fight censorship. This is required as a base level for electronic communications to ensure freedom of speech, expression, association, and assembly using this medium.

Censorship resistance is accomplished by currently using Tor and I2P and in the future to include 1DN (a direct wireless ad-hoc network), Radio, and Satellite as well as other future anonymity networks. When a user's device gets blocked on one network, other networks are used to route around the block until another user's device can make the request. How is this accomplished?

Overview

By embedding[i] 1M5 into a decentralized application and using it for communications, 1M5 works to ensure those communications do not get blocked nor give up a user's identity to those they wish to not to share it with. It accomplishes this by escalating to additional anonymity networks to handle block attempts.

Scenario 1: Viewing a Clearnet Website

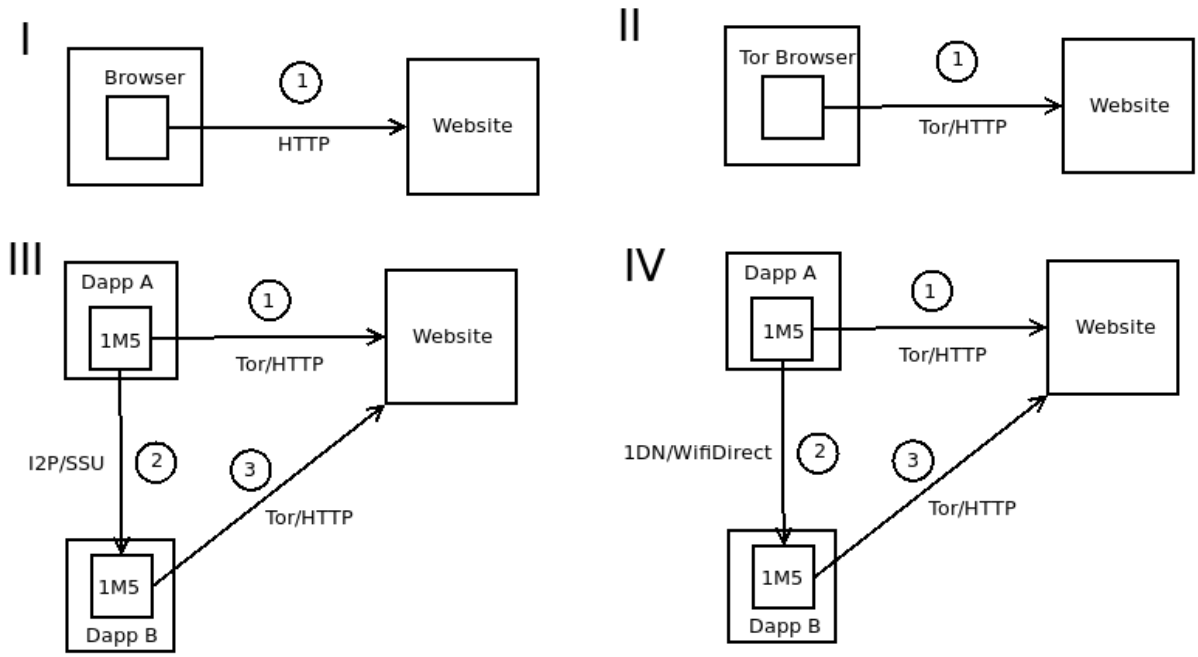
Typical scenario of a person attempting to view a clearnet web site, e.g. YouTube.

In section I, a browser is used to connect to a web site to view its content. This is normally blocked IP or domain name filtering by Internet Service Providers (ISP) by governments. People then look for alternative methods to get around the block.

In section II, they find Tor browser, download and install it, then attempt to view the website through Tor. This gets around the IP/Domain blocks so long as the exit nodes are not blocked. Considering that most exit nodes are in jurisdictions that have stronger support for freedom of speech, this is normally effective. But governments who are more astute, e.g. China, they hunt down the entrance nodes that are running Tor and begin black listing their IP addresses preventing access to the Tor network.

In section III, they discover 1M5, download and install the 1M5 Proxy, configuring the Tor browser to use it as a proxy, then point it to the url again. This time, it seeing that it is unable to access the Tor network so forwards the request to another 1M5 node that has access Tor using I2P. This other dapp node's 1M5 instance connects to the site desired, collects the response, and forwards it to the original requester. But what happens then if the government orders local cellular towers shutdown?

In section IV, they install 1DN or another direct wireless ad-hoc network into 1M5 and then make the request. Now 1M5 uses the ad-hoc network to route out until it again finds a 1M5 node with Tor access. If this fails to return a request in a specified time, the Radio component can be used and/or the Satellite component can.



Scenario 2: Person-to-Person Applications

Person-to-person applications are messengers, email, and voice.

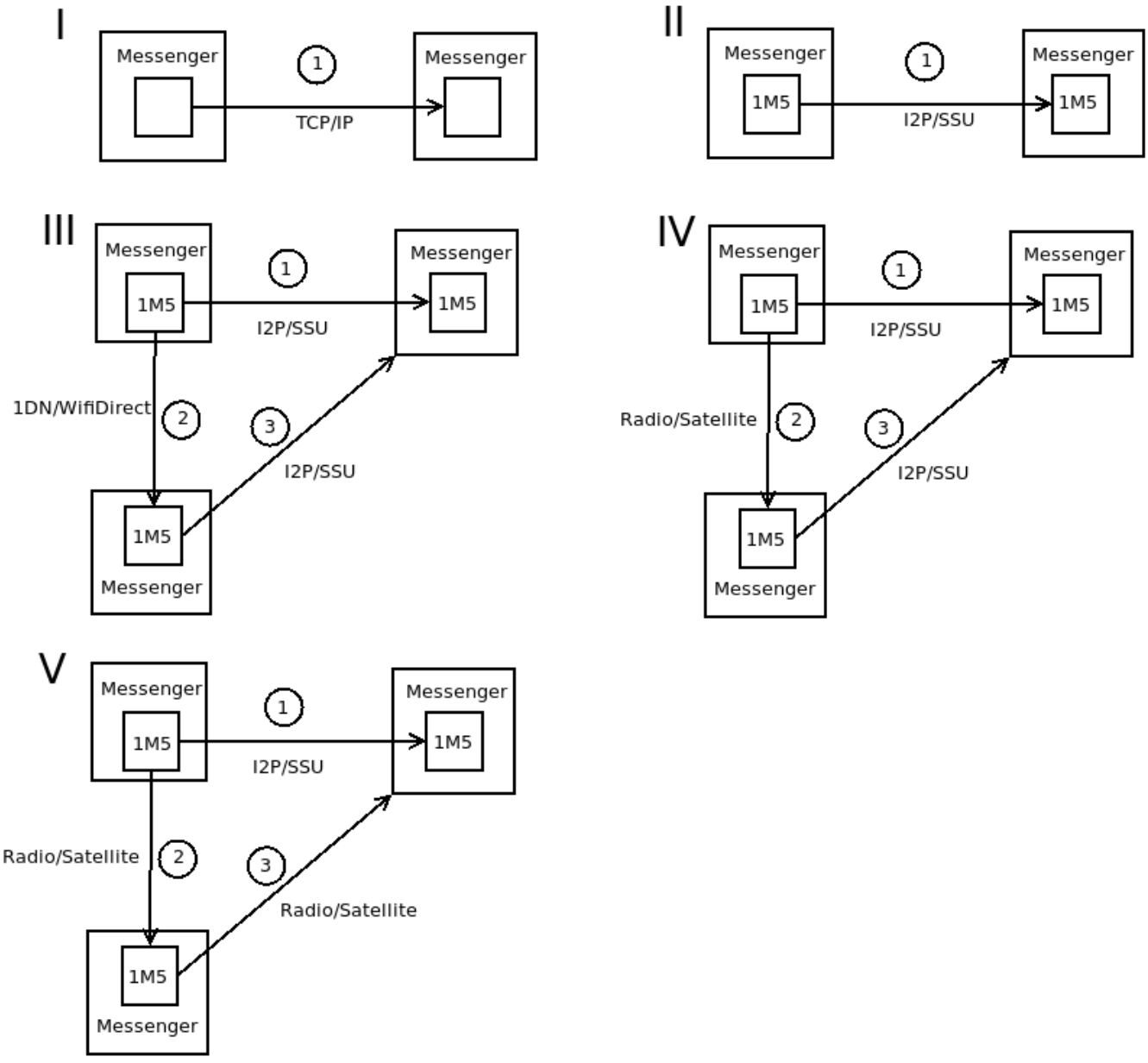
In section I, we're using a typical messenger using TCP/IP to communicate with a server to forward messages to other messengers. The server gets taken down or blocked preventing the communications.

In section II, a messenger with 1M5 embedded is used for messaging over I2P (SSU) preventing the ability to shutdown messaging by shutting down or blocking a server (no servers are used). At this point, the local cellular towers could be shut down preventing messages from getting out of that geographical area via cellular.

In section III, a WifiDirect based ad-hoc network is used in an attempt to get out to a 1M5 embedded client. If this works, it will continue communications with the other messengers. If not successful in a set time, we move onto section IV.

In section IV, the radio and/or satellite sensors are used to get a message to a 1M5 peer who has I2P access to make the communications. If this fails to happen, e.g. the internet is down globally…

In section V, it switches to purely radio and/or satellite for all communications.


I
Messenger
1
Messenger
TCP/IP
II
Messenger
1M5
1
Messenger
1M5
I2P/SSU
III
Messenger
1M5
1
Messenger
1M5
I2P/SSU
1DN/WifiDirect
2
3
I2P/SSU
1M5
Messenger
IV
Messenger
1M5
1
Messenger
1M5
I2P/SSU
Radio/Satellite
2
3
I2P/SSU
1M5
Messenger
V
Messenger
1M5
1
Messenger
1M5
I2P/SSU
Radio/Satellite
2
3
Radio/Satellite
1M5
Messenger

ManCon

The primary threats to freedom of speech/expression are governments but other entities commonly engage in it such as corporate based media. The 1M5 community works to determine the default level of maneuvering required to avoid censorship based on what claimed jurisdiction the end user is currently in. From there, the router will work to maintain uncensored communications for the applications using it. This maneuvering condition is called ManCon.

ManCon is similar to the United States Armed Force's DEFCON. It is an alert state signalling the maneuvering required to achieve freedom of expression. It can change at any time in response to new conditions arising. The base ManCon for a claimed jurisdiction is largely based on the Press Freedom Index.

- 5 = Good Situation
- 4 = Satisfactory Situation
- 3 = Noticeable Problems
- 2 = Difficult Situation
- 1 = Very Serious Situation

The following ManCons provide a description, indications, and availability.

ManCon 5

Low Security – Minimal threats to privacy and little to no control over nor monitoring of the internet.

Open/normal SSL based communications with no expected censorship or privacy intrusion attempts. Web: will use HTTPS. Failures will not attempt HTTP but will use other peers to assist.

- Tor for .onion addresses
- I2P for .i2p addresses
- I2P is used for peer-to-peer services such as messaging

ManCon 4

Medium Security - Normal censorship attempts by states on reading news with public web sites getting blocked and/or government shutdown of cloud CDN content. Respect for freedom of expression may be limited.

Normal censorship attempts by states on reading news (public web sites getting blocked, government shutdown of cloud cdn content). When an HTTPS clearnet site gets blocked that has an associated Tor hidden service, that Tor hidden service will be used. All other routing remains unchanged.

Web: will attempt to use Tor. If fails and an associated Tor hidden service is available, that hidden services will be used. If no Tor hidden service is associated with the site, other peers will be used to assist. Expect latencies of 500 milliseconds to 2 seconds.

ManCon 3

High Security - Tor nodes discovered with IPs blocked. Likely little respect for Freedom of Expression.

Tor hidden services that have been blocked or taken down but have an associated I2P eep site, that I2P eep site will be accessed. Default sensitivity in Envelope.

Web: will use an I2P peer that has access to Tor to make the request. Expect latencies of 1-4 seconds.

ManCon 2

Very-High Security - I2P EEP sites getting attacked/targeted. Actual threats and prison time for speaking out.

Use 1M5 mainly with I2P with high delays. Only able to access information directly via I2P using a decentralized content distribution network, e.g. Inkrypt.

- Web: will use an I2P peer with random delays that has access to Tor to make the request. Expect latencies of 2-3 minutes.
- P2P: direct comms with I2P but with random delays. Expect latencies of 2-90 seconds.

ManCon 1

Extreme Security - Internet access getting shutdown in areas. Strong censorship attempts with massive number of nodes blocked, deep packet inspections across internet on unencrypted payloads, and/or I2P timing/DDOS attacks. People getting murdered for speaking out. Absolutely no respect for freedom of expression by governments.

Use 1M5 with 1DN to route to peers with internet access. Wide-ranging latencies but strong privacy.

- Web: a 1DN peer will be used to access Tor. Expect latencies of 2-25 minutes when in large cities with many 1M5 nodes.
- P2P: 1DN peers will be used until a peer with I2P access can route the request.

1M5 Embedded Communication Technologies

Tor

Provides onion-routing, layered encryption, and bi-directional channels for IP anonymity. Best for accessing clearnet web sites/services such as IPFS and Ethereum. Embedded as a Sensor in 1M5 and used through the Tor Browser and Android Orbot for content consumption.

I2P – Invisible Internet Project

Provides garlic-routing, layered encryption, and uni-directional channels for IP anonymity. Best for communicating P2P with other I2P users. Embedded as a Sensor in 1M5 for low-latency high sensitivity content distribution.

Direct Wireless Ad-Hoc

A direct wireless mesh network for routing when there is no internet connectivity or for extremely sensitive fragments. Embedded in 1M5 for the Author Android DApp and Gateway.

1DN

A direct wireless mesh network for routing when there is no internet connectivity or for extremely sensitive fragments. Embedded in 1M5 for the Author Android DApp and Gateway.

Radio

A direct wireless ad-hoc network for routing when there is no internet connectivity or for extremely sensitive fragments. Embedded in 1M5 for the Author Android DApp and Gateway.

Satellite

A direct wireless mesh network for routing when there is no internet connectivity or for extremely sensitive fragments. Embedded in 1M5 for the Author Android DApp and Gateway.

Implementation Roadmap

0.1 Synaptic Celerity: Real-time Analytics as a service POC

Pay-as-you-go real-time analytics as a service POC on Amazon AWS using Lambda, Kinesis, DynamoDB.

Completed Winter 2014.

0.2 Synaptic Celerity: Real-time Analytics Prototype

Moved to a Jetty/Kafka/Storm/Cassandra stack for more control over the processing.

Completed Winter 2015.

Abandoned real-time analytics as a service as the big cloud providers were beginning to offer it.

0.3 Synaptic Celerity: Real-Time Decentralized Directed Acyclic Graph (DDAG) Processing POC

Embedded a rules engine (Drools) as Storm component to provide more easily customized logic to begin shaping the platform into a more artificial intelligence (AI) platform.

Completed Winter 2016.

0.4 Synaptic Celerity: Real-Time Decentralized Directed Acyclic Graph (DDAG) Processing Prototype

Began decentralizing the platform by using DHT (Decentralized Hash Tables) for routing.

Began building an Artificial Intelligence service by implementing how the brain is thought to work.

Completed Winter 2017.

0.5 1M5: New SOA/EDA Platform with I2P POC

Major rewrite to a new SOA/EDA based platform.

Added Censorship-Resistant Routing for focusing on new mission as 1M5.

Completed Winter 2018.

0.6 1M5: Major upgrades to components including addition of Tor Sensor

Added many upgrades including Tor and censorship-resistance routing.

Completed Winter 2019.

0.6.1 1M5: Fine tunings of current components

Mostly support for Inkrypt as primary community member.

Completed Spring 2019.

0.7 1M5: Full Support of 1M5 Proxy

This version is expected to fully flush out the platform for what's required to maximize censorship-resistance using Tor and I2P.

EST Winter 2020.

0.8 1M5: 1DN Prototype

This version is expected to implement a basic WiFi-Direct based ad-hoc direct wireless network.

Some work has already been accomplished but this version should prove it working in the field.

This is likely to require many more nodes for uptake, hence Purism and other adoption should greatly aid here.

EST Winter 2021.

0.9 1M5: Radio Prototype

This version is expected to implement a basic GNU Radio network to maximize long-distance connections in the worst-case scenarios.

EST Winter 2022.

1.0 1M5: Satellite Prototype

This version is expected to implement a basic Satellite network as a further option for long-distance communications.

The entire platform is expected to be stable at this point although minimally implemented.

Further improvements in the platform and each component is expected to begin greatly at this point with additional funding as the platform proves itself.

EST Winter 2023.

i Instructions on how to embed and integrate with 1M5 can be found in the developers paper (1m5-dev.pdf).