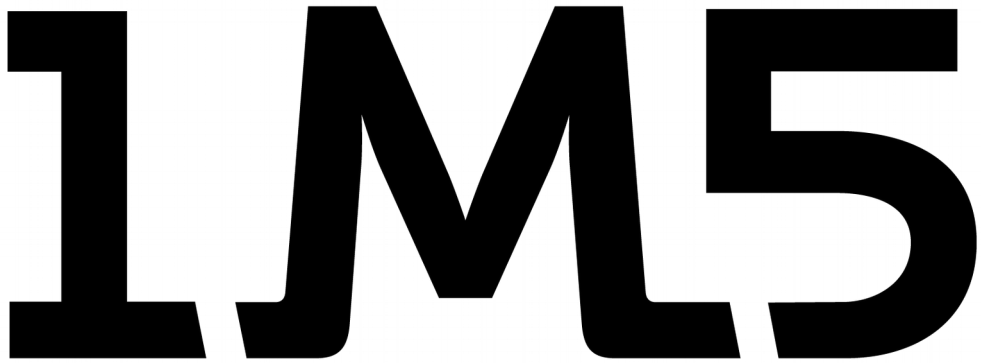


UNCENSORED COMMUNICATIONS

Invisible Matrix Services

Architecture Description
System v0.6.1
Document v6

Background

Invisible Matrix Service (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

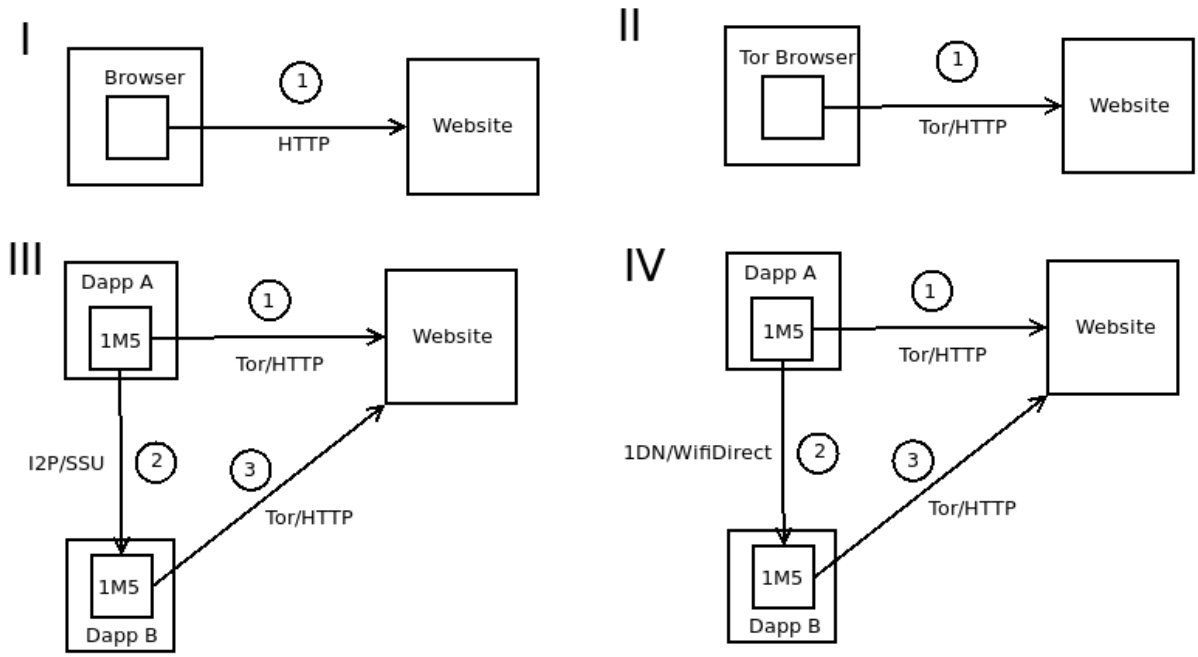
Typical scenario of a person attempting to view a clearnet web site, e.g. YouTube.

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.

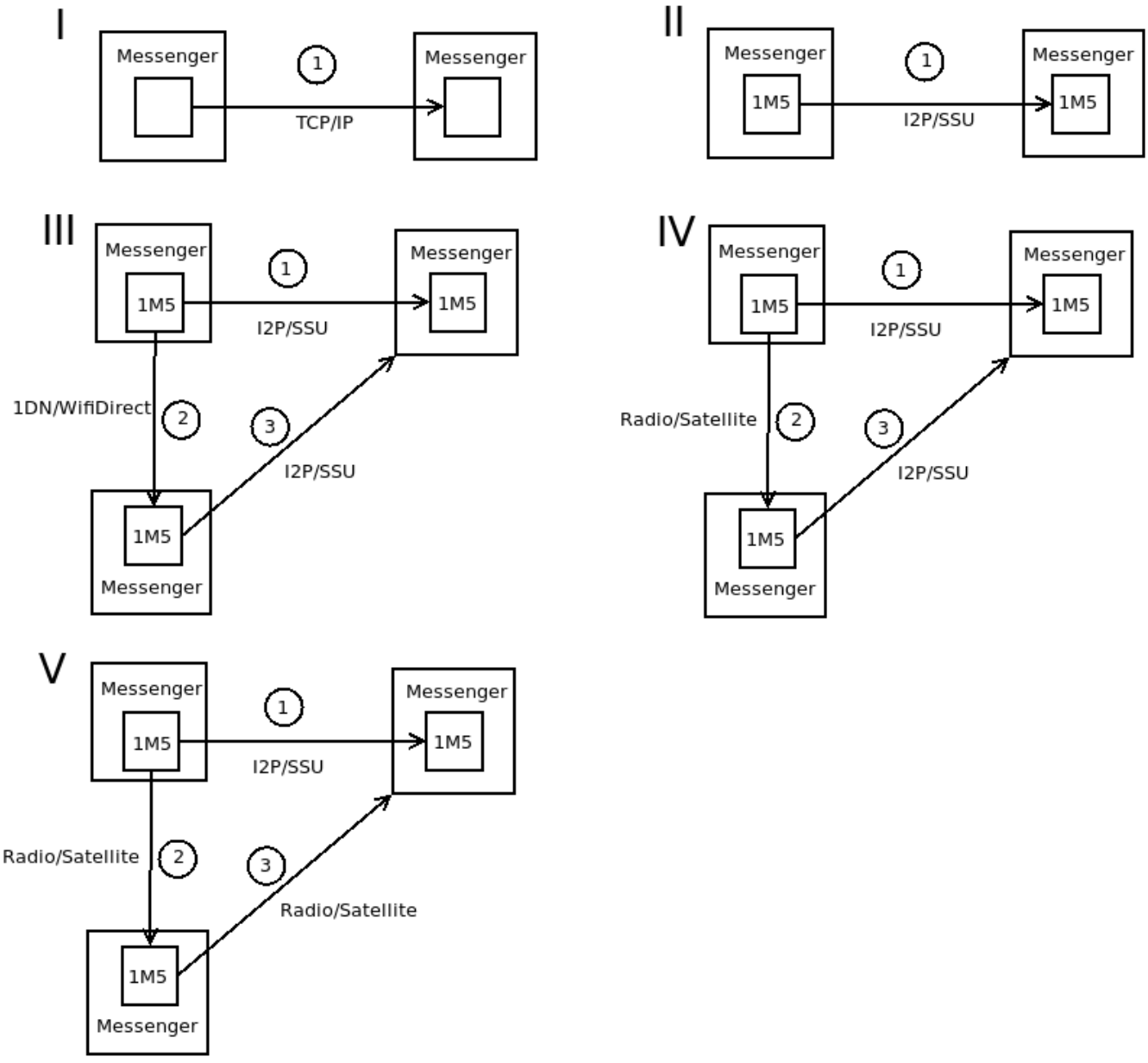
In section I, we're using a typical messenger using TCP/IP to communicate with a server to forward messages to other messengers. The server gets taken down or blocked preventing the communications.

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

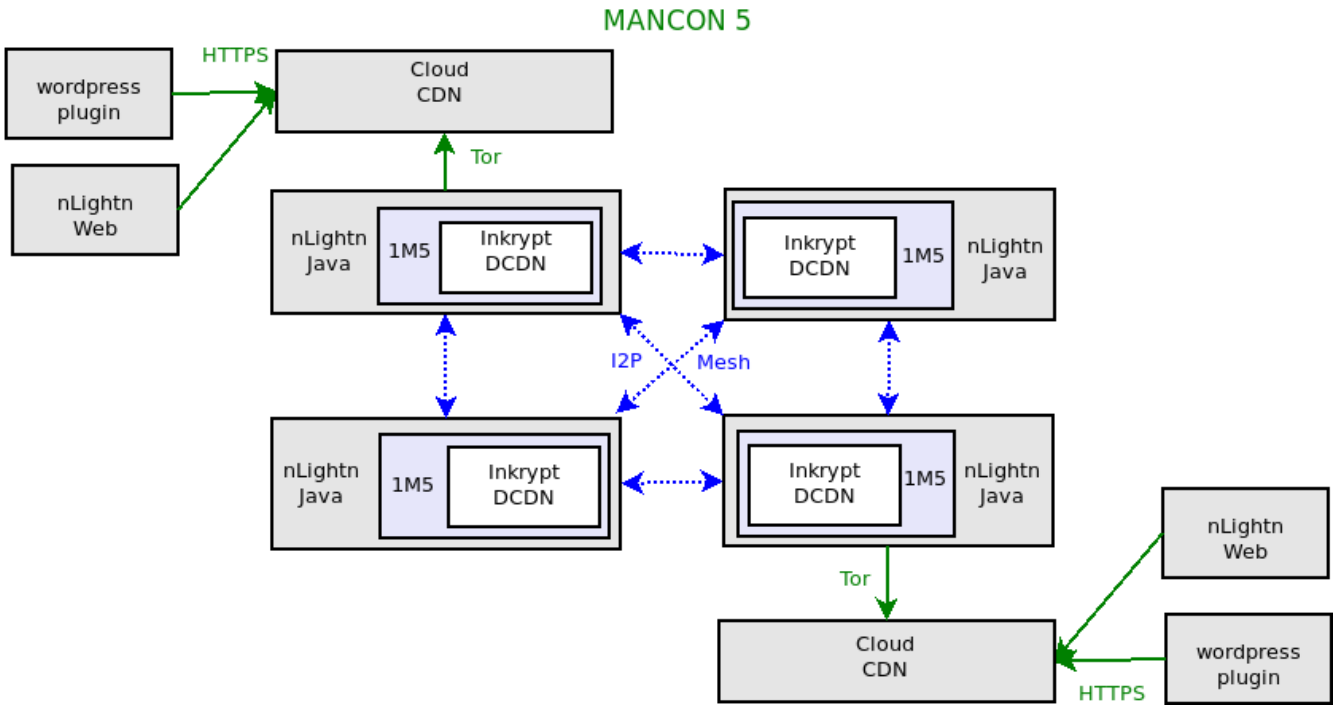
The following ManCons provide a description, indications, and Inkrypt DCDN availability.

ManCon 5

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

Content is published to the Inkrypt DCDN by content producers using nLightn Java over I2P/Mesh and to Cloud CDNs (e.g. AWS, Google, Azure) via Tor to maintain node privacy. Content can be consumed directly from the DCDN by nLightn Java over I2P and published content from Cloud CDNs by nLightn Web and WordPress plugin over HTTPS in the clear.

Provides low latency / limited privacy when consuming content from the Cloud CDNs and medium latency / medium privacy when consuming content over I2P using nLightn Java.

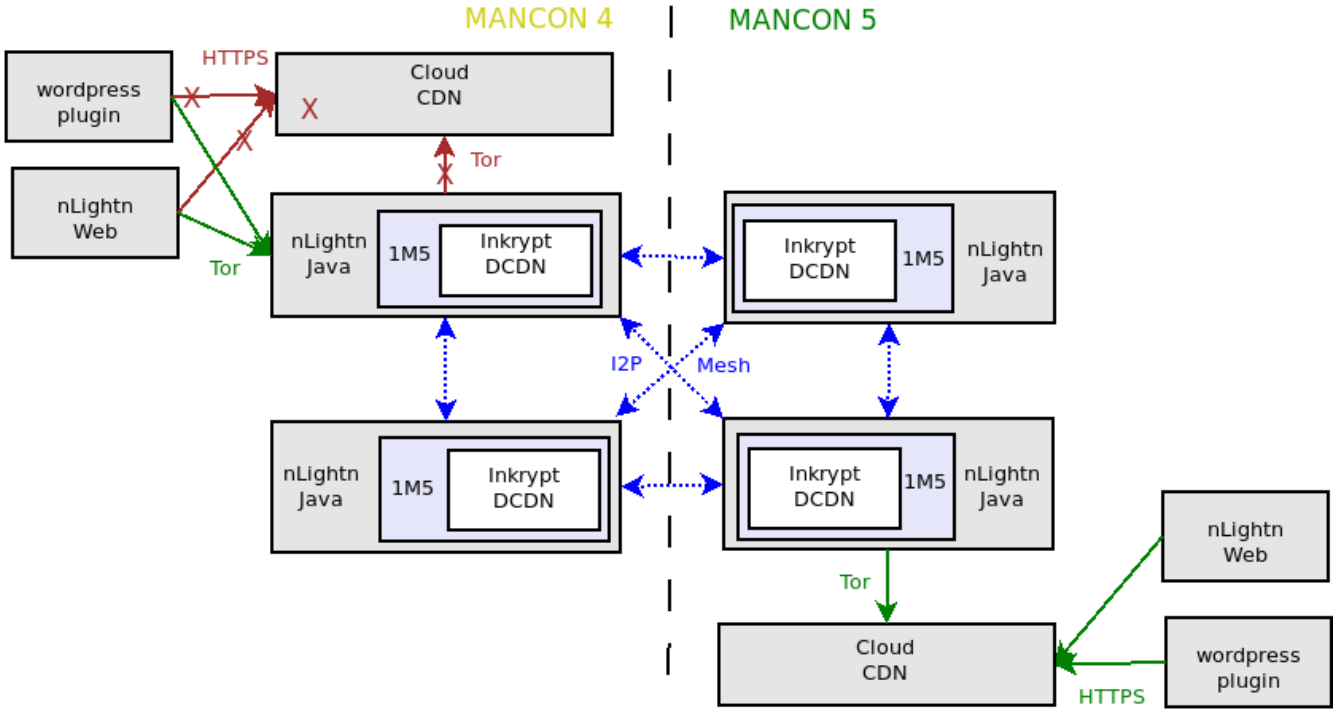


ManCon 4

Low 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.

WordPress Plugin and nLightn Web likely blocked from consuming content from Cloud CDNs over HTTPS and nLightn Java could be blocked from publishing to Cloud CDNs over Tor. Network monitoring may determine Tor is in use by your node or browser by seeing default Tor ports 443, 9001, and 9030 in use.

WordPress Plugin and nLightn Web requires Tor proxy or nLightn Web can use Tor Browser to connect to a number of nLightn Java based Tor Hidden Services exposing the Inkrypt DCDN.

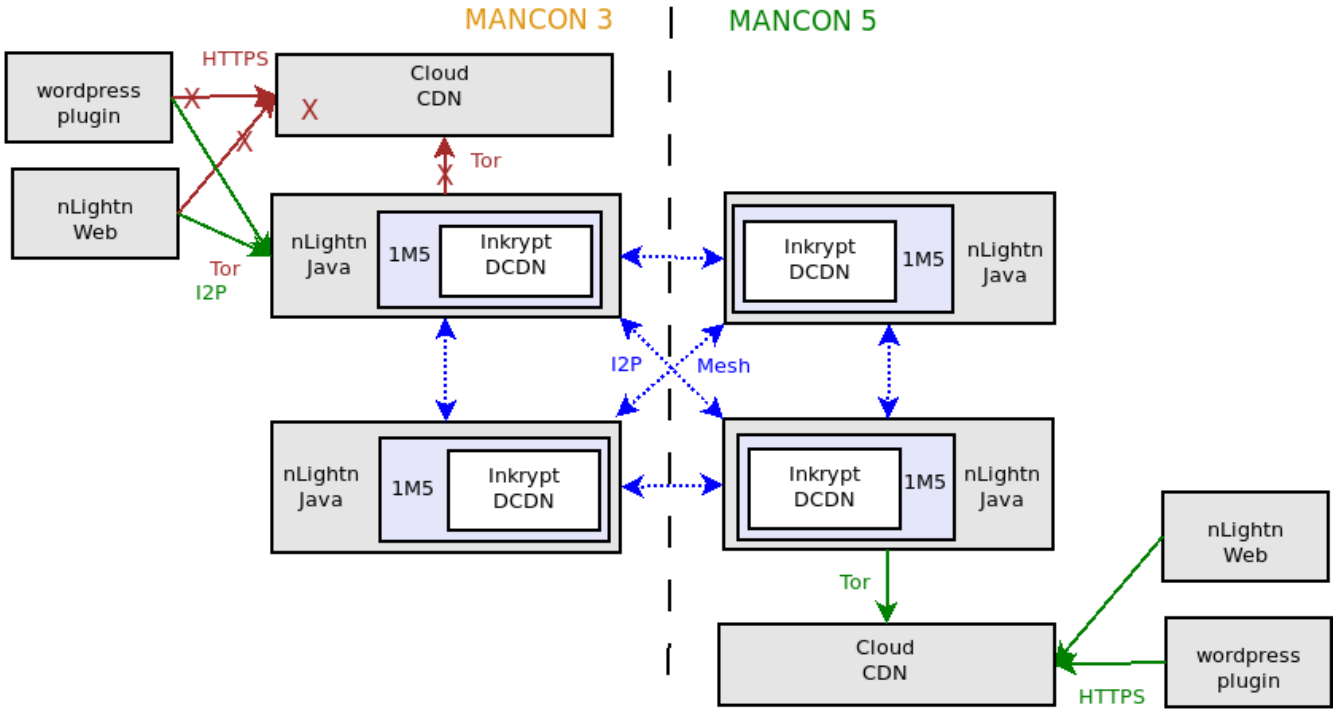


ManCon 3

Medium Security - Tor nodes discovered with IPs blocked. Likely no respect for Freedom of Expression.

Tor access to nLightn Java based Tor hidden services could be blocked by IP.

I2P EEP sites offered by nLightn Java nodes for WordPress plugin and nLightn Web components to consume content using .i2p URLs. Network monitoring can determine end user is likely using I2P due to default I2P port 4444 in use.

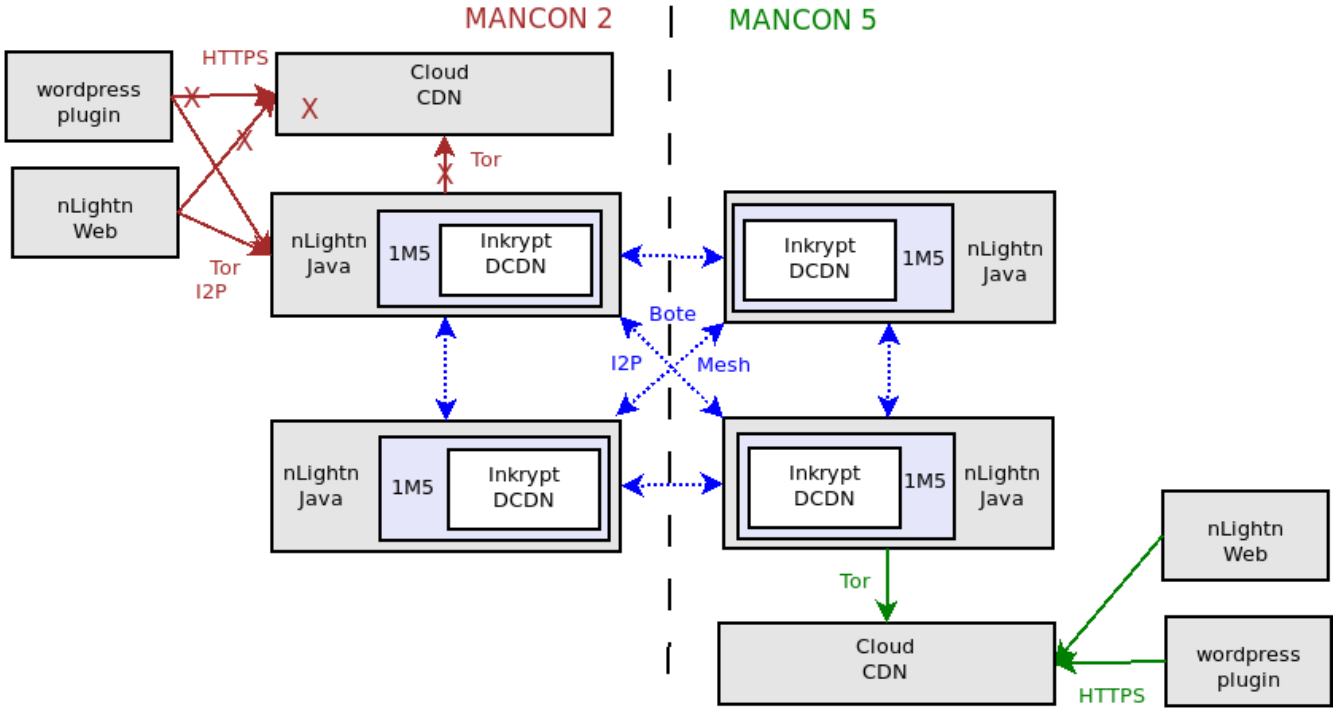


ManCon 2

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

Pure decentralized content consumption over I2P/I2P Bote is required. This may prevent use of WordPress Plugin and nLightn Web. Only nLightn Java can be assured of content consumption from Inkrypt DCDN.

I2P in nLightn Java uses random ports and all data is encrypted (deep packet inspection doesn't work on encrypted payloads) so it's extremely difficult to determine I2P is in use.

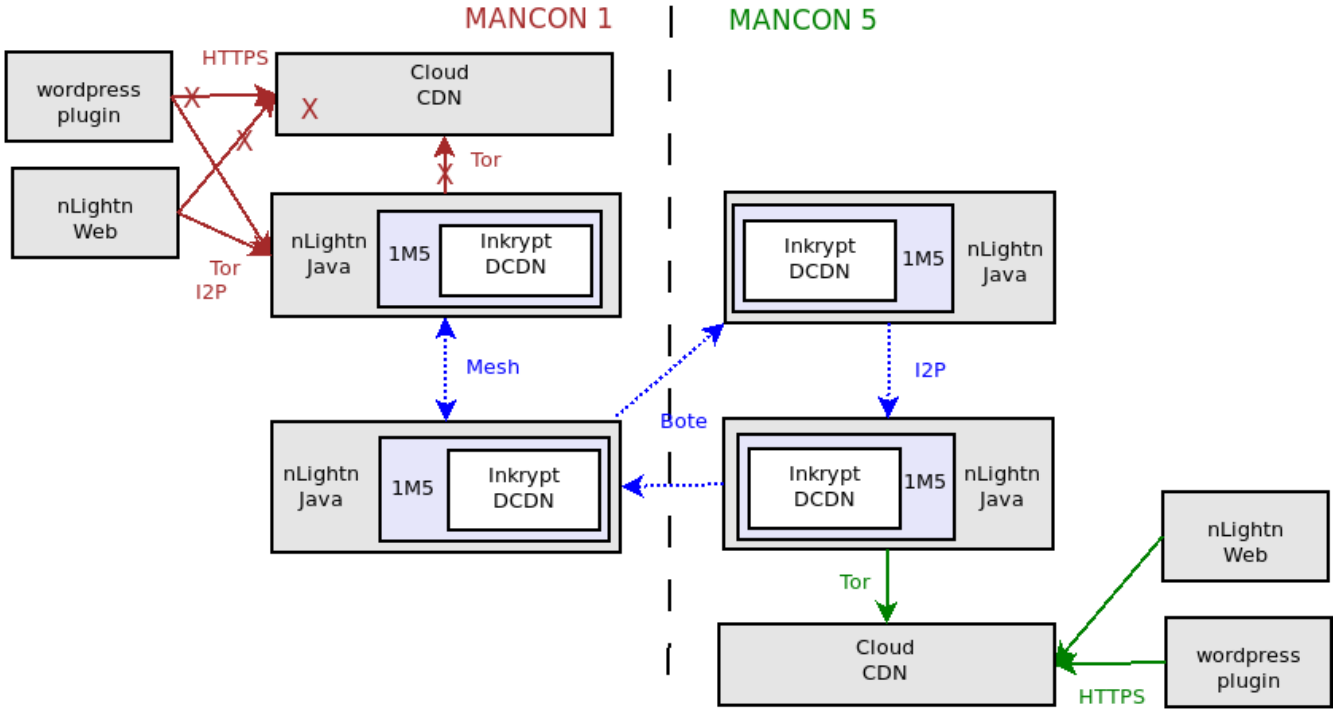


ManCon 1

Highest of 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.

1M5 Neo routing using Direct Wireless mesh and I2P Bote with high delays running on Purism Libre Mobile and Laptops.

In the example below, the nLightn Java dapp is isolated by local cell towers turned off. It discovers a nearby 1M5 node via Direct Mesh in an Android and sends a request for an article describing the censorship. The request makes it to an nLightn Android in a Mancon 5 area where it forwards the request to an nLightn Java node known for having the content. This node sends the content via Bote back towards the nLightn Java client via an nLightn Android client which in turn uses its Direct Mesh to return the content to the original requester.



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.

I2P Bote

Email DApp using I2P to provide relay delays to guard against network timing attacks. Embedded as a Sensor in 1M5 for for higher-latency very high sensitivity content distribution.

Direct Mesh

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 POC

Minimal functionality to prove out 1.0 platform idea with minimal private investor funding. Completed summer 2018.

Features

- Anonymous Article Postings
- Anonymous Article Consumption

Use Case

Author

1. Installs the Android DApp on their Android phone and it starts up.
2. Creates an alias with passphrase or logs in with current alias.
3. Creates a new blog fragment by providing a Blog name 'Syria 2018 Aleppo Feb 8', entering some text in the fragment space and pressing Send button.
4. Continues creating and send additional blog fragments with the same Blog name.

Consumer

1. Accesses the consumer java dapp.
2. Subscribes to author above.
3. Sees the blog with name 'Syria 2018 Aleppo Feb 8' after author submits above.
4. Selects the blog and it is viewed.

Applications Implementation

Applications include Android DApp and Native Java DApp.

Android DApp

- Provides a login screen with alias and passphrase.
- If alias is not present, creates and persists it.
- Home screen provides a blog name text box, meta-data text box, and a fragment text box to enter text into. Pressing the send button sends the text to the other Peer using I2P Bote and clears out the fragment text box.

Native Java DApp

- Provides a login screen with alias and passphrase.

- If alias is not present, creates and persists it.
- Can subscribe to author of canned blog
- Receives subscribed blogs
- Clicking a blog name brings up the blog with all fragments

Budget

- Front-End Engineer @ 4 Months
- Back-End Engineer @ 4 Months
- Blockchain Engineer @ x Months
- System Architect @ 4 Months

Timeline

3rd Qtr 2018

0.2-0.3 Token Generation & Test-net Bootstrapping

Additional features...including tokenization...

Features

- ...

Budget

- Front-End Engineer @ x Months
- Back-End Engineer @ x Months
- Blockchain Engineer @ x Months
- System Architect @ x Months

Timeline

4th Qtr 2018

0.4-0.5 Alpha Launch & API Development

Additional features...including APIs...

Features

- ...

Budget

- Front-End Engineer @ x Months
- Back-End Engineer @ x Months
- Blockchain Engineer @ x Months

- System Architect @ x Months

Timeline

2019

0.6-0.7 Governance Devolution & Beta Launch

...

Features

- ...

Budget

- Front-End Engineer @ x Months
- Back-End Engineer @ x Months
- Blockchain Engineer @ x Months
- System Architect @ x Months

Timeline

2020

0.8-1.0 GA – Nodal Optimization & Main-net Launch

Ensure very stable system with strong security auditing ready for general availability.

Features

- ...

Budget

- Front-End Engineer @ x Months
- Back-End Engineer @ x Months
- Blockchain Engineer @ x Months
- System Architect @ x Months

Timeline

2021

Security Resources

1. https://steemit.com/security/@camb/how-to-trace-a-source-s-ip-in-anonymous-dht-networks-a-simple-essay

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