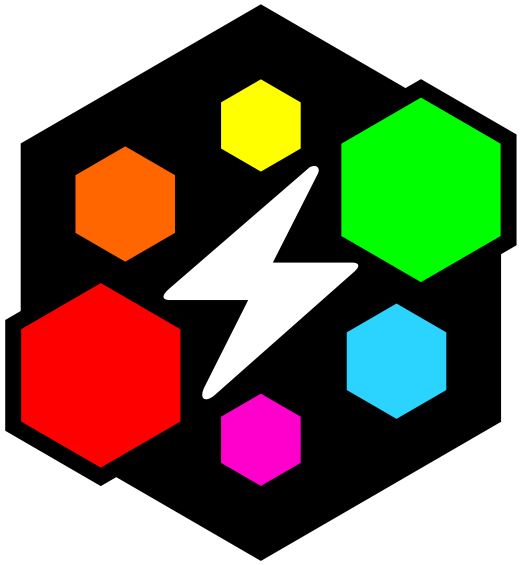


Indra Routing Protocol White Paper

Onion routed distributed virtual private network protocol with anonymised payments to create scaling incentives.

David Vennik September 2022

Abstract

The state of counter-surveillance technologies has remained largely unchanged in the 20 years since the inception of the Tor network.

The primary use case has always been obscuring the location information of users from clearnet sites, and the more it has been used for this purpose, the more hostile clearnet sites have become towards this network, due to its frequent use to launch attacks on web services.

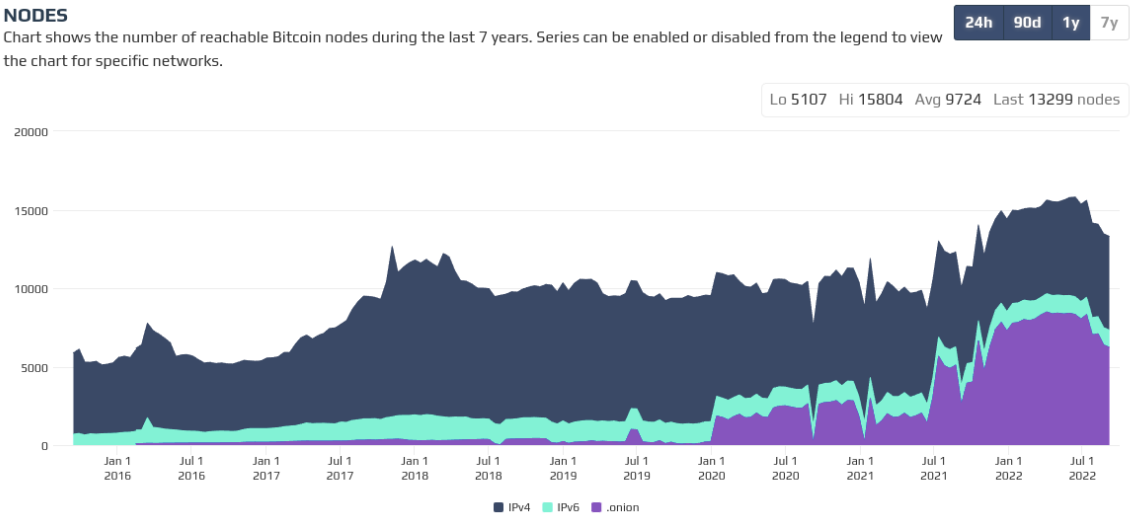
With the increasing amounts of value being transported in data packets on the Internet since the appearance of the Bitcoin network, the need for eliminating the risks of geographical correlation between payments and user locations continues to rise.

However, without any way for users to pay routers without creating an audit trail, the anonymising networks have not grown in nearly a decade, and thus well heeled attackers have largely been able to keep pace and pluck off high value targets, such as the Carnegie Mellon University - implicated in part of what led to the arrest of the Silk Road founder, Ross Ulbricht.

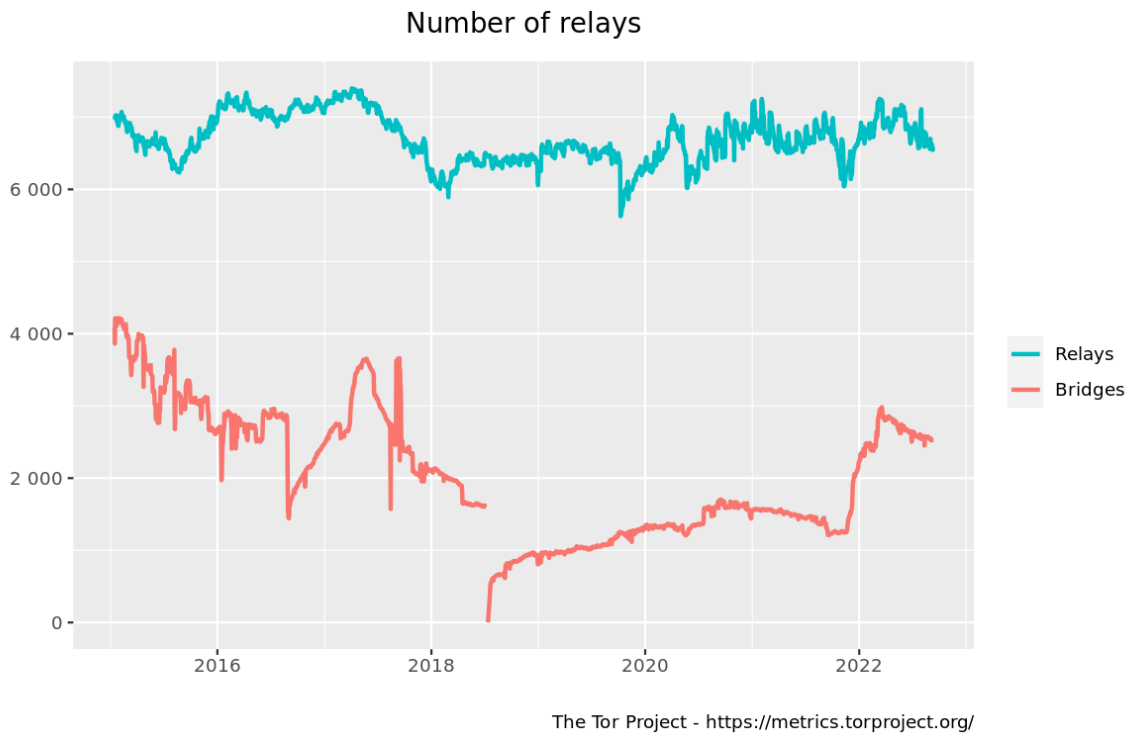
It is the central thesis of this paper to demonstrate how obfuscating correlation between payments and session usage can be achieved and create a marketplace in routing services which can economically increase to a size that is beyond the capabilities of a state sized actor to fund an attack, while also improving latency and stability of routed connections.

Tor Isn't Scaling, But Bitcoin Needs Onion Routing

For comparison, this is Bitcoin's node count:



Versus Tor in a comparable period:



It is not hard to see:

- Tor is not growing, it has flatlined.
- Bitcoin is growing.

Not only that, you can also see that onion routing is forming an increasingly large component of Bitcoin connectivity.

Goals of Indra Routing Protocol

Three key elements of the Tor protocol make it less than desirable in general.

1. Establishment of circuits is quite slow, taking a large number of steps to "telescope" into a circuit.
2. Once a circuit is running, when it fails, the failure is opaque to the client side, and there is no way to provide a latency guarantee or connection stability. It is unsuitable for interactive and long living connections.
3. There is no profit motive to drive expansion of router capacity.

Tor is a poor solution for a very limited subset of of the use cases that benefit from the security of route obfuscation. Indra aims to provide what Tor has definitely now failed to achieve for a large majority of internet users: location privacy.

Anonymised Session Purchase Protocol

The initial purchase of a routing session presents a chicken and egg situation. Without an existing circuit, how does a client node acquire tokens for sessions with onion routers to use for creating hops in an onion route?

For this, we borrow from Lightning Network protocol BOLT#4 which we cannot use by itself as it has no provision for returning an arbitrary package of data, nor the notion of an interacting midpoint in the loop, with the path going back to the sender.

As distinct from this `lightning-onion` protocol, we use ed25519 for signatures and curve25519 for the ECDH key exchange, and encrypt traffic with AES-GCM. Rolling over encryption ciphers is done partly via hash chains and can also be periodically triggered in return messages from circuit exit points.

Session Tokens

Session tokens are an arbitrary random value that must be present in the header of encrypted data and is hashed in a chain to provide a counter for the packet sequence within a session.

With these, routers check off remaining data in a client session, ensuring they deliver what was paid for and nothing more. They function as authentication as well as session accounting.

Exit Sessions and Charging

Packets that are intended to be delivered, as occurs at the exit hop of a circuit, to another service, or across a rendezvous point, can have different rates charged. These rates and the services they apply to are advertised as part of a router's status advertisement.

Such exit traffic is paid for via the session chains same as for relaying. Exit relays include a double charge because of the return path, one charge for the exit, one for the return that comes back from the exit.

Charges are part of the return payload so that clients confirm their remaining allocations. When a node fails, only its last acknowledged relays are charged for, or if the node goes offline, the client discovers this when they activate path hop acknowledgments.

Path Hop Acknowledgements

In order to ensure the session purchase protocol is properly executed, in each layer of the onion there is special acknowledgement onion messages carrying the payment receipt that confirms delivery, and route backwards to the buyer, who knows then that a hop has succeded.

In this way the buyer can expect 5 acknowledgements to be successful and then receive the session key from the 5th node in the circuit.

The acknowledgement onions are constructed so that nodes do not know what step they are, so each has space for 5 steps, which are masked using methods as described in BOLT#4.

If the 5 acknowledgements are not received within a reasonable time, the buyer then propagates forwards payment reversals up to the last acknowledged payment, reversing the payment and denying the misbehaving node where the route stopped.

Source Routing

As distinct from TOR, Indra uses source routing, thanks to the magic of the session tokens and ECDH, means that in the event of a route path failing, a new path can be generated with a changed set of intermediate routers when a timeout occurs.

Latency Guarantee and Path Timeout Diagnostics

For time sensitive interactive applications, these progress detecting onions be used at every step to ensure the moment one hop latency exceeds a prescribed threshold the source routing algorithm can then swap out a different node in the route and thus provide a strong latency guarantee.

Some applications are very time sensitive. Real-time interactive shared environments such as games can have very serious consequences (to the players) when their connection starts to increase in latency putting them at disadvantage against their opponents, and in general, a sluggishness of the interactivity.

Long lived sessions like SSH also can become tiresome when running over Tor when inevitably congestion or downtime hits a hop in the path. For applications where a few seconds stall do not disrupt the protocol, activating path timeout diagnostic onion acknowledgement packets enables the client to determine which hop needs to be replaced.

For additional security, a user can configure the return onions to return via random, multi hop paths, rather than reversing the forward path.

Circular Paths

One of the key inventions of Indra is the notion of circular paths. These are two hops out to the exit/destination point, and two hops backwards, on a different path, for the return.

By using this circular topology, the source can provide a return path that is not the same as the forward path, and when the path timeout diagnostics are not in play, there is no visible reverse path confirmation timing for large scale network traffic analysis.

That is to say, the packets appear to always only be going forward, and no correlation is easily made between, therefore, forward, or reverse paths, which is not the case with telescoped TOR protocol packets, and for most general purposes in Indra are avoided when traffic achieves the intended forward path without excessive latency.

The return paths also serve as a path to return a new cipher for an exit node, whose messages are carried with the return loop, as well as bandwidth accounting data, via provided ciphers for the return path payload.

Dancing Paths

As well as introducing a mechanism for monitoring the progress of packets through paths, it then becomes possible, due to the source routing strategy, for every single path to be different, aside from the exit point of the path.

Redundant/Fragmented Parallel Paths

In addition, a further feature for future work is the use of Shamir's Secret Shares, as well as Reed Solomon Forward Error Correction to provide a reduction in path length or higher guarantee of messages passing in one try via parallel paths. These paths require end points to collate the fragments and forward the combined packets to their destination. Such paths have a higher cost, in proportion with their redundancy, but enable strong retransmission avoidance.

Packet Sizes

All packets are 8 Kb in size. Acknowledgement onions increase overhead and reduce data that can be carried. Routers charge for the total payload. By making packets uniform, it is a simple matter of counting packets, and thus the hash-chain counters directly relate to total routed traffic volume.

Rendezvous

Rendezvous is an important type of route to consider in the discussion of routing. Rendezvous are points where circuits are established between nodes at the exit point (3rd) in a standard 5 hop Indra circuit.

Users wishing to receive inbound connections from the network can use these to obscure their location.

The client opens circuits to notify 6 different other routers, that a service with a given identity can be reached from it.

These nodes then advertise they are able to reach a given hidden service address. The servers will thus pay for half of the cost of traffic to them, in exchange for having their IP address concealed.

Liveness

Because of the circular path and the reverse path after the middle carrying return messages, communication must always be prompted by the client in order for ongoing return messages to occur.

Indra uses UDP, eliminating any session overhead, the path acknowledgements and return paths are already defined in the onion packets. TCP and QUIC can be carried across the circuits, as will often be the case for hidden services. Indra aware services can take advantage of the knowledge of the protocol and trigger features of the protocol such as return acknowledgements and the return hops to carry things like acknowledgements of packets received via their hash fingerprint.

There is no need for negotiating connections, data is simply forwarded around on the basis of pre-agreed contracts of service created by the purchase of data sessions, and authenticated by valid headers, which prove relation to the session root code.

This messaging strategy does require a constant request/reply pattern, but a node does not need to send a second request unless the response does not come back within an expected time window, or is expected to have some amount of delay, because the return path is already plotted, and the cipher provided to the exit hop in the circuit.

For some applications, this is fine, such as a terminal session, as while the user is not asking for anything, the listener does not either have to wait for anything. For this type of traffic there can be pings, which are short packets and do not need path diagnostics, so they are cheap for monitoring liveness.

In addition, nodes monitor the state of other nodes in the clear when gossiping status updates and advertisements, and if the (uncharged) traffic of asking for status updates from peers reveals a node is unresponsive this is a back channel that can be used to trigger a circuit path change to route around a dead router.

Additional Applications

Aside from obscuring the paths of traffic between users on the network, some additional potential uses emerge that solve other long standing problems.

Wireless Hotspots - In Band Access Payments

Because the wireless traffic can be bounded for this purpose, and does not represent a forward path to routing, Indra routers can provide chain and lightning data freely to mobile connected nodes for the purpose of sync and then establishing data sessions through the node with the wireless hotspot enabled.

Mobile nodes can run Neutrino SPV Bitcoin light nodes, as full node data requirements are impractical and network data are excessive for a device which can only really act as a client.

As such, we then create a potential use case for mobile devices to update their network state for free, with a limitation on how much the Bitcoin and LN node's provide to enable the spending of tokens to initiate a session, and by this, we thus enable operators to provide network access to mobile users while being paid for their traffic.

The requirements for one or several nodes syncing via compact filters to get up to date versus the total on-network routing are light and do not greatly impact network performance on the internet side.

Meshes and Wide Area Network Redundancy

Further, this opens up another potential use case, perhaps of lesser utility, but nevertheless notable, of where other routers in the vicinity of a router, also providing this network access, can negotiate connectivity, and serve to back up each other in the event their primary - and even secondary - routes go dark, there can be connectivity for the core network via connected peer hotspots.

Since all traffic going across Indra is charged for anyway, this allows maintaining of connectivity for nearby routers to maintain access to the IRP network, with a greater uptime guarantee than any of the local cabled and/or wireless network services in use at a given location.

This has extra relevance in the case of a sudden hostile turn of events, either government or natural disaster, keeping connections up as much as possible to enable people to find their way to safety.

Conclusion

The central goal of Indra is to create an overlay network that is adequate to completely replace base layer of the network while providing extra security. Primarily against large scale surveillance and well heeled attackers attempting to unmask target users, but also to provide universal inbound routing, wireless mobile network access.

Ultimately, to form the basis of a uniform in-band payment system for network routing that enables all node operators to make a slim margin of profit for running their infrastructure and making more efficient use of network infrastructure as a whole, by allowing use of traffic with direct compensation.

Just as TLS/SSL has come to be universal, it is the hope of the designers of Indra Routing Protocol to eventually become a universal routing protocol that protects users data, physical location, money and helps secure against network-enabled attacks in general. Hackers cannot perform a denial of service attack if they cannot afford the traffic.

End