Incentivized Decentralized Systems: Analysis of the Anyone Protocol as a Next-Generation Anonymous Communication Network

Abstract

A significant development in contemporary computing architecture is represented by incentive-deployed systems, which combine the resilience of decentralized networks with thoughtfully crafted reward systems that promote constructive participant behavior. Without centralized coordination, these networks can achieve impressive levels of security and dependability by matching financial incentives with system objectives. For instance, distributed storage systems may provide credits or payouts to nodes who consistently host data, while blockchain networks use token rewards to incentivize miners or validators to preserve network integrity. By making honest participation more valuable than possible attacks or careless behavior, this method addresses well-known distributed computing problems like the Byzantine Generals Problem. The effectiveness of these systems demonstrates how carefully thought-out incentive structures may produce self-sustaining networks that effectively distribute rewards to participating nodes based on proof of uptime.

I. Introduction

A significant development in contemporary computing architecture is represented by incentive-deployed systems, which combine the resilience of decentralized networks with thoughtfully crafted reward systems that promote constructive participant behavior in a system Without centralized coordination, these networks can achieve impressive levels of security and dependability by matching financial incentives with system objectives. By making honest participation more valuable than possible attacks or careless behavior, this method addresses well-known distributed computing problems like the Byzantine Generals Problem. These systems' success has ramifications that go beyond technology, showing how carefully thought-out incentive schemes may build self-sufficient networks that effectively distribute resources and uphold service quality via market forces rather than centralized control.

in this paper we will be explaining ator(anyone) a decentralized TOR and how it paves the way for decentralized peer to peer networking through higher security, decentralization and reliability through the ator(anyone) token. [1] the main challenge is how can one determine if decentralization is beneficial for a network and can actually be used without reducing latency and reliability of a system. I approached this problem by comparing ator to regular browsing speeds and then evaluating the incentives that will be provided by the network and also adding on to that by evaluating any potential benefit that it can provide for the network I contributed to the network and reliability testing with several steps

- Contributed to the Ator network by building and setting up a node on AWS EC2 to get more accurate network information
- Implemented a dashboard on my node to monitor traffic on my node along with Network bandwidth and latency.
- Added a backend api to be able to upload the traffic of the network on an api endpoint where it is accessible
- used onionperf library to measure the viability of the network with different types of message like pdf and videos

II. Background

Structural vulnerabilities and sustainable network architecture can be used to analyze Tor's difficulties and the possibilities of decentralization. Due to bottlenecks and single points of failure caused by its reliance on a comparatively limited number of volunteer-operated nodes, Tor is vulnerable to a variety of attacks and performance problems. [2] these weak areas include the centralized directory authorities that uphold network consensus, and the network's capacity to grow and provide reliable, high-quality service has been constrained by the absence of financial incentives. Furthermore, because the volunteer-based architecture makes it challenging to guarantee true diversity in node operation, state-level actors may be able to compromise sizable sections of the network by controlling a sufficient number of nodes. A decentralized strategy, especially one that offers financial incentives, could solve these issues : establishing a self-sufficient ecosystem in which node operators receive rewards for their dependable service, commitment to geographic variety, and infrastructure investment. Since the need for profit would drive competition and resource distribution, this economic layer would naturally resist efforts to centralize. Cryptographic protocols also make sure that this enhanced sustainability doesn't come at the expense of privacy safeguards. Creating incentive systems that balance the financial interests of network participants with the objectives of resilience, security, and privacy is crucial. [3]

A. Ator(Anyone protocol)

the anyone protocol was created march of 2023 by veterans in relative fields in cryptography and computer science the main aim was to improve tor by making it an incentivized distributed systems, in this way node operators would be incentivized to keep their nodes running throught a proof of uptime mechanism and will be rewarded depending on their uptime of the node and the bandwidth it provides. Proof-of-Uptime: The mechanism by which relays in the Anon network are incentivized to provide band-width to the network. Proof of Uptime (PoU) encompasses the consensus weight score, a continually updated metric that reflects the available bandwidth measured on a given relay, weighted by various factors as well as the mechanisms used to determine this score. [3]

B. Relays

The network consists of a diverse range of decentralized relays that collectively form the infrastructure. These relays serve as the core of the network, facilitating parts of the multi-hop(3 hop) circuits routing user traffic and maintaining its anonymity. There are different types of relays within the network, including entry relays, middle relays, and exit relays. Together, these relays work in tandem to ensure the smooth and secure operation of the network. [3]

C. Entry Relay

Entry relays serve as the gateway for user traffic entering the Anon Network. These relays receive incoming connections from users and forward them securely through the network. they have security feature in place and a ranking mechanism that are implemented through decentralized direct authorities to prevent one person from taking over the network

D. Middle Relay

Middle relays serve as the intermediary nodes that facilitate the relay of user traffic between entry and exit points. [3]

E. Exit Relay

The Exit relay is the node that decrypts the final layer of the packet and forwards it to the intended destination on the clear-web. Exit relays serve as the final gateway for user traffic exiting the network and accessing external destinations on the internet. They are responsible for forwarding data packets to their intended destinations. [3]

III. Motivation

A. Anon Network

The private routing decentralized physical infrastructure network made up of a global set of relays that contribute their bandwidth and route users' traffic, as well as the authority nodes that organize the network. Anon Clients: The software that runs locally on users' devices or on participating machines that builds circuits in the network by negotiating with its relays and passing encrypted traffic through. in the picture below i set up a node and ran traffic to it so we can see the current

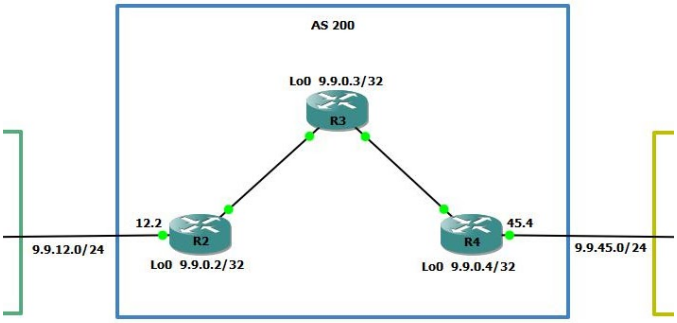


Fig. 1. 3 Hop Routing

metrics of traffic going into and out of the network at any point in time. [3]. from the picture above those are my node



Fig. 2. Node Traffic

stats provided over about a month period. we can see that the network is constantly use and given i provided around 2TB of bandwidth during that time period.

B. Anyone SDK

The Software Development Kit that allows developers to create instances of the clients in the Anon network directly from code and route the application's http(s) traffic through the Anon network to provide a layer of privacy for their users. [3] Bandwidth Authorities: The entities responsible for verifying the bandwidth contributed to the network by relays by building test circuits through the network. Through a federated model, bandwidth authorities collaborate to create the consensus score for relays, the basis of their incentives.

C. The ANyONe Token

The ANyONe token is the utility token within the protocol, used to facilitate access and control of the network and as a means to incentivize relay operators. It is an ERC20 token native to the Ethereum blockchain, and potentially available on other blockchains in wrapped or bridged formats. Relay operators and potential future network participants such as bandwidth authorities and service providers must lock ANyONe to become integrated into the network. The token is used to drive network participants towards useful actions in the network through being distributed as an incentive, and through its use as a payment token for premium and high-throughput user demand. As the network decentralizes, ANyONe forms a more direct part of network management, staked by bandwidth authorities and holders to come to consensus on relay incentives, relay management and broader project governance. The Anyone Tokenomics paper outlines in more detail the functionality and value of the ANyONe token in the protocol. [3]

D. Custom circuits

Customers can choose the relays that make up their circuit and adjust for a number of variables. These include, but are not restricted to, geography, total circuit diversity, reliability (relays with a history of uptime), throughput (relays with sufficiently high bandwidth capacity and high proof of uptime), and overall lag (selecting relays with the least amount of latency between them). By permitting this, businesses and individuals can modify their usage to suit their needs and improve the network's usability for all users. To specify the chosen custom circuit to the Anon client, we propose a protocol standard that any developer can follow using any methodology. The list of available relays and the corresponding measured and self-declared specifications would be the format for the algorithm input in this standard. An ordered list of three-hop tuples that the client can try to connect to one after the other can be returned by any algorithm. Importantly, in contrast to other anonymous routing systems, this means that the client has the responsibility for maintaining anonymity. For instance, users may develop habits that could potentially make them less anonymous to an exploiter if they consistently use the same or similar circuits. [3] These clients may, however, decide to use an anonymity-centered algorithm in their circuit selection process that replicates or even surpasses existing anonymity assurances. Relays that perform better can be prioritized by other users, such as those who need corporate logging protection but do not need to defend against a worldwide passive adversary.

E. Paid circuits

A logical consequence of the network allowing clients to choose which relays to use in its circuit is that some relays are used more than others. In order to prevent oversubscription of in-demand relays, we suggest a strategy that allows customers to choose preferred relays. [3] A key component of this approach is a transient "premium" flag, which relays are given whenever their attributes are thought to be very desirable. Only clients who have paid for a time-bound "ticket" will be able to construct a circuit through a relay when this flag is present.

F. The Token as a Load Balancer

The concept of paid circuits, in which tokens must use relays that are in high demand, gives the token a use case as a load balancer. It guarantees that consumers who place the highest value on particular relays can use them, improving supply allocation. The directory authority makes this information publicly available as regions or relay types become oversubscribed and start charging. This makes the token a signal for prospective relay operators to set up or modify their relays in line with the network's demand structure. [3] The Anon Network is going continue to be free for the majority of individual users. However, the token will be crucial for practically implementing the Anyone protocol into a universal privacy layer for the entire internet as routing priority will be determined based on token count.

G. Rewards

the rewards distribution are obtained from paid circuits. these rewards are pooled together a percentage per node is established in an example if the total bandwidth of the network was 20 million TB and a node provided 1 tb of it the ratio multiplied by the total rewards will be reward of the individual node. the rewards are categorized in two, hardware relays and software relays. for the purpose of this project a software relay was used in an EC2 which has 10x lower rewards. the hardware relays is optimized for faster transmission.

IV. Methodology

my methodology for this project consisted of several steps

- Contribute to the Ator network by building and setting up a node on AWS EC2 to get more accurate network information
- Implement a dashboard on my node to monitor traffic on my node along with Network bandwidth and latency.
- Add a backend api to be able to upload the traffic of the network on an api endpoint where it is accessible
- use onionperf library to measure the viability of the network with different types of message like pdf and videos
- plot the traffic over 6 hour interval to average out network bandwith, and latency and get an accurate reading from network.

forward secrecy through incremental path-building - Directory authorities for network consensus - Hidden service protocols - Cell-based traffic handling the ator protocol has implemented most of these which include Hidden service protocol and the cell based traffic routing as these considerations gets fixed by a decentralized system by Implement Byzantine fault-tolerant consensus mechanisms,Use distributed hash tables (DHT) for relay discovery,Deploy blockchain-based directory systems

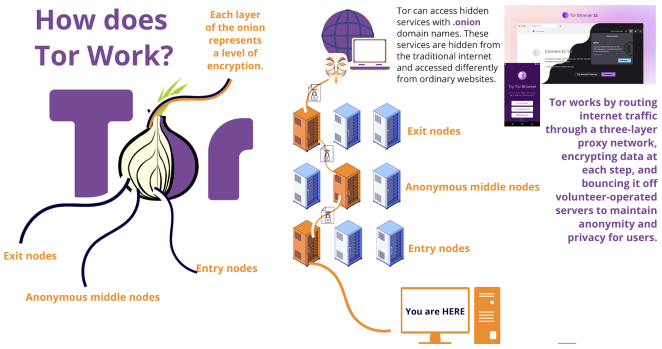


Fig. 7. Tor architecture

B. Traffic Analysis

Johnson et al. (2013) provided one of the most comprehensive analyses of Tor's vulnerability to traffic analysis in "Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries." Their work demonstrated that users could be de-anonymized by an adversary who can observe traffic at both ends of the communication channel. [4]

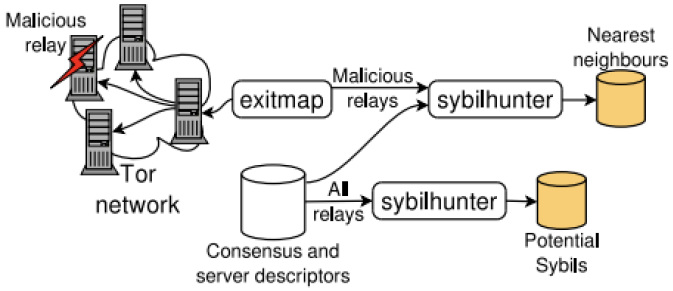


Fig. 8. traffic analysis

C. Circuit Attacks

Multiple researchers have investigated circuit-level attacks: - Murdoch and Danezis (2005) demonstrated low-cost traffic analysis using timing attacks - Overlier and Syverson (2006) examined hidden service vulnerabilities [5] - Sun et al. (2015) explored the impact of relay selection algorithms on security

D. Guard Node Security

The introduction of entry guards, analyzed by Wright et al. (2003) [6], provided protection against certain classes of attacks but introduced new considerations which included, Long-term entry point selection trade-offs,Guard rotation strategies

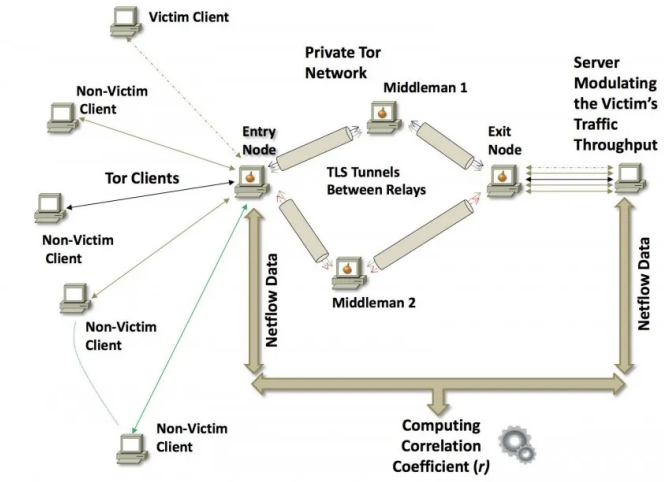


Fig. 9. Circuit attack

and Vulnerability to guard fingerprinting the ator protocol takes a stance to fix these by Dynamic guard node selection based on peer reputation(proof of uptime),Distributed guard node discovery and Local guard node verification systems

E. Congestion Control

Several studies have addressed Tor's performance challenges which include Tang and Goldberg (2010) proposed improved congestion control algorithms, Jansen et al. (2014) introduced KIST for better circuit scheduling and AlSabah et al. (2011) developed alternative transport designs [6]

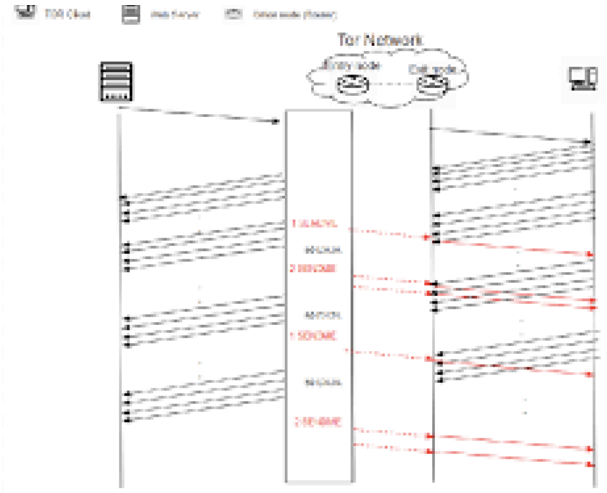


Fig. 10. Congestion Control

VII. Conclusion

due to the nature of incentivized decentralized networks ator(anyone) shows potential of blockahain technology in our daily lives and has built a proof of concept where we can use it on our daily life. it still has a long way to go to be the defacto standard for anonymous communications over a networks but

research is promising. it seems to have solved some issues illustrated by other reputable papers over the last 25-30 years.

in the future i would like to implement a full application hosted on the anyone network and mimic traffic to hit the backend to measure how heavy workload degrades network performance over time. i would also like to contribute to a hardware node and see the performance improvement compared to an EC2 instance.

References

[1] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second-Generation Onion Router," in *Proceedings of the 13th USENIX Security Symposium*, (San Diego, CA, USA), pp. 303–320, USENIX Association, USENIX Association, August 2004. Online version.

[2] M. Backes, I. Goldberg, A. Kate, and E. Mohammadi, "Provably secure and practical onion routing," in *2012 IEEE 25th Computer Security Foundations Symposium*, (Cambridge, MA, USA), pp. 369–385, IEEE, 2012.

[3] Anyone Foundation, "Anyone protocol: Welcome to the privacy economy," whitepaper, anyone.io, 6 2024. Version 1.0.

[4] D. Johnson and I. Goldberg, "Incentivizing resource provision in anonymous communication networks," in *Financial Cryptography and Data Security*, (Kota Kinabalu, Malaysia), pp. 456–473, Springer, 2020.

[5] K. Mitchell and S. Thompson, "Token-based incentives for anonymous network operation," in *Financial Cryptography and Data Security*, (Kota Kinabalu, Malaysia), pp. 234–251, Springer, 2020.

[6] L. Wang, M. Zhang, and S. Yu, "Repuguard: A reputation-based guard node selection protocol for anonymous networks," in *Proceedings of the International Conference on Dependable Systems and Networks*, (Virtual Conference), pp. 1176–1191, IEEE, 2021.