Dear EuroS&P reviewers,

We thank you for the time spent reading and evaluating our submission.

As requested by the conference guidelines, we present below the reviews we received after the submission of an earlier version of this work to the NDSS 2023 conference, and detail how we addressed the comments. Please note that we received only two reviews for NDSS.

Our comments are prefixed by Response: and highlighted in yellow. Key points made by the reviewers are highlighted in light blue.

Note that **TOPDISC** was used as a codename for **discv5**, the name of our system, in this NDSS submission.

A summary of the major changes is as follows:

- Major revamp of the paper presentation to improve clarity on our design objectives and the protocol itself.
- Experiments performed not only by simulation but also using an implementation of discv5 in the Go Ethereum client.
- Clarification of the fact that discv5 is the contribution of the paper, and is the upcoming service discovery mechanism in Ethereum, and not an extension of an already-existing service discovery protocol.

Best regards,
The authors of EuroS&P anonymous submission #48.

Review #148A

Overall Recommendation

2.

Leaning towards reject

Writing Quality

2.

Needs improvement

Reviewer Expertise

3.

Knowledgeable

Paper Summary

This paper presents TOPDISC, a practical, secure and efficient service discovery protocol. TOPDISC combines the efficiency of traditional DHT operations with security inherited from pseudo-random ad placement. In addition, TOPDISC only involves simple mathematical calculations, can protect against a wide range of malicious behaviors (e.g., eclipse attack), and can ensure equal load distribution and promotes diversity in the network. A prototype of

TOPDISC is developed and evaluated functionally, and it shows that TOPDISC can outperform other related approaches.

Strengths

1. A novel design to achieve a practical, secure and efficient service discovery protocol.

Weaknesses

1. Poor motivation: how does TOPDISC work? Why can TOPDISC outperform others? Why do the two challenges exist?

   Response: We rewrote the introduction and clarified our problem statement in sections 1-2. We thoroughly revised the description of the protocol in sections 3-6 to highlight why discv5 aimed at a tradeoff between security and performance, and why existing solutions were not satisfactory.

2. Incomplete experiments: additional experiments that are conducted on real world devices are required.

   Response: A major change in the EuroS&P submission is the addition of experiments using the actual Go Ethereum client. The NDSS submission only contained simulation results.

3. Missing but useful related work: how does Discv5 work? Why do authors claim that TOPDISC is fully integrated with the Discv5?

   Response: There was source of confusion on in the NDSS submission, where TOPDISC was presented as a contribution to discv5, when it actually is the discv5 protocol itself. We clarified this in the present submission.

4. Contributions are limited.

   Response: We politely disagree with this statement. Discv5 is planned to be the service discovery protocol in the future Ethereum platform, and the design answers practical, real-world challenges. It has the potential to impact significantly the security and scalability of one of the largest deployed decentralized systems.

Detailed Comments for Authors

Overall I think this is interesting work. I appreciate the design of TOPDISC that leverages pseudo-random and deterministic advertisement placement to achieve a practical, secure and efficient service discovery protocol. On the other hand I have a few major concerns with this work.

1. Authors indicate that TOPDISC is fully integrated with the Discv5. Although Discv5 is a work in progress currently, the specification, design, and algorithms of Discv5 have been

proposed in Discv5's repositories [1]. However, in this work, authors don't give a clear description of Discv5. I am not fully convinced that TOPDISC has the fundamental contributions and is integrated with the further development of Ethereum's Node Discovery Protocol design.

Response: We clarified this in the current submission. discv5 is the contribution of this paper and is planned for integration in the future version of Ethereum. The linked webpage is outdated and does not present the work we did to bring discv5 objectives to fruition.

2. Authors need to introduce how TOPDISC works in an overall view. Currently, I had to read this paper multiple times before I could understand the steps of TOPDISC. Besides, in the overall illustration, it will be more clear to understand how different roles (i.e., Registrar, Advertiser, and Searcher) communicate with each other. Due to such limitations, I am not convinced why the two challenges (i.e., IV-A and V-A) exist, and why it is significant to solve the two challenges.

   Response: We significantly modified the description of the system to improve clarity of the presentation and our motivation, compared to the previous NDSS submission.

3. Authors only leverage a P2P network simulator to demonstrate the performance of TOPDISC. Authors should also conduct the experiments with real world devices to demonstrate that TOPDISC can be applied in practice, and TOPDISC is more efficient than others.

   Response: As previously mentioned, we only presented simulation results in the NDSS submission. The current submission presents deployment results from the implementation of the protocol in Ethereum's main implementation, Go Ethereum..

4. Contributions are limited. According to the experiments, TOPDISC can significantly outperform the Discv4 in limited scenarios, e.g., the adversary has a single IP address for its Sybils when attacking the least popular topic.

   Response: We took this comment into account by considering more advanced Sybil attack scenarios in the experiments.

[1] https://github.com/ethereum/devp2p/blob/master/discv5/discv5.md

Ethics

3.

No ethic issues

Review #148B

Overall Recommendation

2.

Leaning towards reject

Writing Quality

3.

Adequate

Reviewer Expertise

3.

Knowledgeable

Paper Summary

In this paper, the authors proposed a new protocol named TOPDISC, enabling Ethereum clients to discover other peers (services) faster and safer. First, TOPDISC adopts a new admission control protocol that protects against various malicious behaviors, including DOS attacks and Sybil adversaries. Second, TOPDISC performs lookup operations up to three orders of magnitude. The experimental results demonstrate that TOPDISC enables miners to discover peers more efficiently than the existing protocols while achieving a similar security level.

Strengths

- Design and implement TOPDISC to accelerate the service discovery without scarifying the security.
- Evaluate the performance of TOPDISC in terms of efficiency, fairness, and security through simulation.

Weaknesses

- The motivation of this paper needs to be further strengthened.

  Response: As previously mentioned, we clarified our assumptions and objectives through a major revamp of the first sections of the paper.

- The novelty of TOPDISC is unclear.

  Response: We improved the related work section and positioned our work w.r.t. past work more clearly.

- Although the paper presents the details of the protocol, it does not explain the rationale behind most steps.

  Response: Compared to the NDSS submission, we rewrote for better clarity all the sections describing the protocol itself (Sections 3 to 6).

- TOPDISC should also be evaluated on a testbed, and the evaluation result on testnet should be reported.

Response: As mentioned in responses to the previous review, the current submission now contains the results of the evaluation of the discv5 implementation of Go Ethereum.

Detailed Comments for Authors

In this paper, the authors designed a new protocol called TOPDISC based on DISC protocol to discover application-specific peers in networks. Specifically, TOPDISC considers the efficiency (the speed of finding network peers), the fairness (the load balancing for handling querying specific peers), the security (the resilience in defending DoS/eclipse attack) to optimize DISC.

Response: There is no such thing as a DISC protocol, but probably the reviewer wanted to mean discv4, the actual discovery protocol in Ethereum. Discv5 is a complete new design for service discovery in Ethereum, and does not build upon the random walk approach of discv4.

The evaluation based on simulation shows that TOPDISC outperforms existing DHT-related network protocols. However, I have the following concerns.

- The motivation of this paper needs to be further strengthened. Please elaborate on why a service that allows Ethereum nodes to discover an application sub-network is needed. What kind of applications did the authors aim at? To make the blockchain secure, it would be good to involve all nodes into the computation. If the goal is to improve the efficiency, why not using the existing sharding approaches?

  Response: **(1)** We strengthened the point that Ethereum is not only the blockchain of the same name but an ecosystem, or platform supporting multiple applications, of which the mainnet is only one of them. We agree this is confusing to many, as Ethereum is usually used to mention the 'mainnet', i.e., the main blockchain of the ecosystem. We adopted the mention of "Ethereum platform" and "Ethereum ecosystem" in the current submission to help readers avoid the confusion, and included examples of applications. **(2)** We also point out that sharding is a technique for improving the performance of one blockchain system (mainnet, or another blockchain running as an application in the Ethereum ecosystem) using parallel processing, but is not a solution to allow efficient and safe service discovery in a decentralized system.

- The authors argued that DISCv4 "suffers from very poor scalability and performance, in particular for small subnetworks.". Please elaborate on the reason, especially for small subnetworks.

  Response: We clarified this with specific experiments and by giving numerical examples in section 2 (Background), showing that discv4 is very ineffective for small subnetworks, and impose a high load on the system when discovering these.

- The novelty of TOPDISC is unclear. It is unclear which design element was new compared to existing service discovery protocols designed for P2P networks. Moreover, since TOPDISC introduces some new entities e.g., ad and roles e.g., registrar, advertiser, please discuss its impact on Ethereum and existing applications running on top of Ethereum. Does it require any modifications to existing applications? The waiting time mechanism is not novel because similar techniques have been proposed for defending against DDoS attacks and adopted by Internet applications.

  Response: (1) discv5, as one of the components of the upcoming Ethereum platform, will indeed require updating the base platform code for nodes participating in the ecosystem. It will not require, however, modifications to the applications bootstrap code: Applications will solicit and receive a number of bootstrap peers from the specified topic, just as with discv4, but the response will be faster and will impose less load on the overall system. (2) We discuss additional references compared to the NDSS submissions to position our work compared to other work that used a 'announce-and-wait' mechanism for rate control.

- Although the paper presents the details of the protocol, it does not explain the rationale behind most steps. For example, why is the mechanism of service advertisements introduced? What kind of problems can be addressed by this mechanism? Is it the best solution to tackle the problems listed in the introduction? How to define services? What are the relationships between the topics and existing smart contract based applications?

  Response: (1) We reworked thoroughly the presentation of the protocol and of discv5 components in order to make it clearer and better motivated, as previously explained. (2) This comment results from confusion between the Ethereum platform and the mainnet blockchain. discv5 does not operate at the level of the mainnet blockchain and is thus oblivious to the use of smart contracts, or, in fact, any blockchain-specific construct.

- Why is the assumption of "no honest node is fully eclipsed by the malicious ones" needed? It seems that TOPDISC relies on Ethereum's mechanism to defend against eclipse attacks. In this case, what is the advantage of TOPDISC?

  Response: We clarified our assumptions regarding the construction of the underlying DHT regarding eclipse attacks in the routing table, and better motivated how the design of discv5 aimed at avoiding eclipse attacks at the level of the discovery protocol itself (i.e., when advertising topics and when looking up for topics).

- How to bootstrap Ethereum if TOPDISC is deployed?

  Response: Probably the reviewer means "mainnet" by "Ethereum", as in previous comments. Mainnet can start as any other application by having its forming peer discover each other with discv5. If the reviewer means, instead, how is the global DHT of the Ethereum platform bootstrapped, the answer is: The Ethereum foundation maintains

a number of trusted servers to allow nodes to join this global DHT. This is acceptable for the global DHT, but would not be an acceptable solution for individual applications as we detail in our introduction.

- Please explain why "This is likely to happen far before reaching registrars located near the topic hash, especially for popular top"?
- How to select \deltat_{window}? In Section VI, although the authors describe how to compute the scores, they did not explain why such a design is selected and why it is proper (or better than alternatives).

  Response: We clarified these points in the current submission.

- In TOPDISC, every registrar needs to maintain an ad cache. Since it uses the number of same topics in ad cache to compute the similarity of topics, attackers can use random topics and different IP to quickly fill the target registrar's ad cache. Note that TOPDISC uses waiting time to limit the ad cache flashing rate.
- There is no formal security analysis on TOPDISC to support the arguments in VII.C.

  Response: The present submission contains an extensive analysis (section 7) complemented with more details in the appendix.

- TOPDISC should also be evaluated on a testbed. For example, following many papers on new consensus protocols for blockchain, the authors could rent hundreds of machines from cloud platforms to construct a testbed for experiments. As the authors mentioned that the proposed protocol is under testnet evaluation, they should report the results.

  Response: As mentioned before, the present submission presents experimental results of the implementation of discv5 in Go Ethereum, running over a large-scale testbed.

- There is no evaluation on the efficiency of TOPDISC in defending DoS attacks.

Ethics

3. No ethic issues