

М. С. Карапетьянц¹

Метод оценки доступности информационных ресурсов в оверлейной сети на базе луковой маршрутизации

¹Национальный исследовательский ядерный университет «МИФИ»,
г. Москва, Российская Федерация
e-mail: mkarapetyants@mephi.ru

Аннотация. Оверлейные сети на базе луковой маршрутизации формируют распределенную инфраструктуру сетевых сервисов, не индексируемых поисковыми системами глобальной сети, мониторинг которой представляет практический интерес для специалистов в области информационной безопасности. Существующие инструменты применяют разрозненные методы проверки без формального разграничения уровней взаимодействия, что существенно снижает точность мониторинга и воспроизводимость результатов. Целью настоящей работы является систематизация и сравнительная оценка методов определения доступности информационных ресурсов оверлейной инфраструктуры для повышения эффективности инструментов разведки на основе открытых источников. В работе предложена пятиуровневая иерархическая модель, формализующая уровни проверки от публикации дескриптора в распределенной хэш-таблице до семантической верификации контента, и проведена экспериментальная оценка трех методов на выборке из 1000 узлов оверлейной инфраструктуры третьей версии протокола. Результаты показали, что методы существенно различаются по профилю ошибок и области применимости. Метод HTTP-зондирования обеспечил наилучшее общее качество классификации: точность 89,56%, F1-мера 0,910 при умеренной средней задержке 2213 мс и незначительной доле неопределенных ответов (1,3%). Метод проверки публикации дескриптора продемонстрировал почти идеальную полноту ($\text{recall}=0,989$), однако низкую прецизионность (0,689) вследствие сохранения устаревших дескрипторов в распределенной хеш-таблице (DHT, англ. Distributed Hash Table) после перехода ресурса в офлайн, что ограничивает его применимость задачами предварительной фильтрации. Метод проверки TCP-соединения показал наихудшие результаты (точность 58,80%, $F1=0,560$) в силу систематической ошибки, обусловленной нестандартным распределением прослушиваемых портов целевых ресурсов. Практическая значимость работы состоит в обоснованной иерархической стратегии комбинированного применения методов, позволяющей совместить скорость метода проверки публикации дескриптора с точностью HTTP-зондирования при минимизации числа запросов к целевой инфраструктуре. Направления дальнейших исследований включают разработку и верификацию метода проверки доступности точек введения, а также анализ временной динамики доступности ресурсов при многократном тестировании.

Ключевые слова: оверлейные сети, луковая маршрутизация, доступность ресурсов, сетевой мониторинг, инструменты OSINT

M. S. Karapetyants¹

A method for assessing the availability of information resources in an onion routing overlay network

¹National Research Nuclear University "MEPhI", Moscow, Russian Federation
e-mail: mkarapetyants@mephi.ru

Abstract. Onion-routing-based overlay networks form a distributed infrastructure of network services that are not indexed by search engines on the global Internet, and monitoring this infrastructure

is of practical interest to information security specialists. Existing tools rely on fragmented verification methods without a formal separation of interaction levels, which significantly reduces monitoring accuracy and the reproducibility of results. The aim of this study is to systematize and comparatively evaluate methods for determining the availability of information resources within overlay infrastructures in order to improve the effectiveness of open-source intelligence tools. The paper proposes a five-level hierarchical model formalizing verification stages ranging from descriptor publication in a distributed hash table to semantic content verification, and presents an experimental evaluation of three methods on a sample of 1,000 nodes of a version 3 overlay infrastructure protocol. The results show that the methods differ substantially in both error profile and scope of applicability. The HTTP probing method achieved the best overall classification performance, with an accuracy of 89.56%, an F1 score of 0.910, a moderate average latency of 2,213 ms, and a negligible proportion of indeterminate responses (1.3%). The descriptor publication verification method demonstrated near-perfect recall (0.989), but low precision (0.689) due to the persistence of stale descriptors in the distributed hash table (DHT, Distributed Hash Table) after a resource transitions offline, which limits its applicability to preliminary filtering tasks. The TCP connectivity verification method showed the weakest performance (accuracy 58.80%, F1 = 0.560) because of a systematic error caused by the non-standard distribution of listening ports across the target resources. The practical significance of the study lies in a justified hierarchical strategy for combining methods, making it possible to couple the speed of descriptor publication verification with the accuracy of HTTP probing while minimizing the number of requests sent to the target infrastructure. Future research directions include the development and validation of a method for checking the availability of introduction points, as well as the analysis of temporal availability dynamics through repeated testing.

Keywords: overlay networks, onion routing, resource availability, network monitoring, OSINT tools

Введение

Оверлейные сети на базе луковой маршрутизации реализуют децентрализованную модель сетевых сервисов, при которой адресация узлов инфраструктуры осуществляется через криптографически верифицированные псевдослучайные идентификаторы, а не через публичные IP-адреса [1]. Данная архитектура обеспечивает анонимность как для операторов сервисов, так и для их пользователей, что обуславливает широкий диапазон сценариев применения – от легитимных коммуникационных платформ до инфраструктуры противоправной деятельности [2–4].

Задача оценки доступности информационных ресурсов в подобных сетях принципиально отличается от аналогичной задачи в открытом сегменте интернета. Стандартные инструменты сетевого мониторинга такие как ICMP-зондирование, DNS-резолуция, публичное IP-сканирование неприменимы в силу архитектурных особенностей луковой маршрутизации [5]. Вместе с тем практическая потребность в систематическом мониторинге узлов оверлейной инфраструктуры велика. По данным измерительных исследований Owen и Savage [6], от 30% до 50% известных ресурсов недоступны в любой момент времени, а в работе Sanatinia, Park и Blass [7] показано, что медианное время существования ресурса составляет порядка 12 суток. При этом Boshmaf et al. [8] зафиксировали, что 47,8% узлов оверлейной инфраструктуры находятся в офлайн в любой произвольный момент наблюдения.

Анализ существующих работ выявляет принципиальный методологический пробел. Инструменты мониторинга OnionScan, Onionprobe, TorBot и другие – применяют разрозненные методы проверки доступности без формального разграничения проверяемых уровней стека взаимодействия. Loesing et al. [9] первыми декомпозировали задержки протокола по отдельным шагам, однако не формализовали понятие уровня доступности. Это приводит к несопоставимости результатов между исследованиями и к систематическим ошибкам классификации, механизм которых остается необъясненным при отсутствии единой иерархической модели.

Целью настоящей работы является систематизация и сравнительная оценка методов определения доступности информационных ресурсов оверлейной инфраструктуры для повышения эффективности инструментов разведки на основе открытых источников. Для достижения поставленной цели решались следующие задачи: формализация пятиуровневой иерархической модели оценки доступности; разработка и реализация трех независимых методов, соответствующих отдельным уровням модели; проведение сравнительного эксперимента на репрезентативной выборке; количественная оценка сравнительной эффективности методов.

Теоретическая значимость работы заключается в формализации иерархической модели уровней доступности применительно к оверлейным сетям – данная классификация в явном виде отсутствует в существующей литературе, несмотря на то что отдельные ее элементы имплицитно используются в ряде инструментальных реализаций. Практическая значимость определяется возможностью непосредственного применения предложенной иерархической стратегии в системах автоматизированного мониторинга и OSINT-инструментах, ориентированных на работу с ресурсами оверлейной инфраструктуры.

Методы и материалы

Предложенная иерархическая модель оценки доступности включает пять уровней, каждый из которых соответствует более глубокому слою протокольного стека взаимодействия с ресурсом.

Первый уровень. Публикация дескриптора проверяет факт наличия актуального дескриптора сервиса в распределенной хэш-таблице (DHT) сети. Наличие дескриптора свидетельствует о том, что оператор сервиса активно анонсирует свой ресурс в инфраструктуре. Ключевое ограничение данного уровня состоит в том, что дескриптор сохраняет валидность в течение нескольких часов после остановки сервиса, что порождает ложноположительные срабатывания [10–12].

Второй уровень. Доступность точек введения извлекает из дескриптора список relay-узлов, выполняющих функцию точек введения, и проверяет их актуальный статус в консенсусе сети. Дескриптор может существовать, однако все точки введения при этом могут быть уже исключены из активной инфраструктуры, что делает сервис фактически недостижимым.

Третий уровень. Транспортная доступность – попытка установить TCP-соединение с ресурсом через SOCKS5-прокси на указанных портах. Данный уровень

проверяет достижимость прикладного процесса, но принципиально зависит от корректного указания прослушиваемых портов.

Четвертый уровень. Прикладное зондирование направляет полноценный протокольный запрос (HTTP/HTTPS) и оценивает валидность полученного ответа. Это наиболее информативный и практически значимый уровень для задач мониторинга.

Пятый уровень. Семантическая верификация анализирует содержимое ответа на соответствие ожидаемому контенту. Данный уровень выходит за рамки задачи мониторинга доступности в узком смысле и относится к задачам краулинга и идентификации ресурсов.

Для экспериментальной проверки сформирована выборка из 1000 узлов оверлейной инфраструктуры третьей версии протокола. Выборка включает три категории: 121 эталонный ресурс с постоянно верифицированным онлайн-статусом, 535 ресурсов, обнаруженных посредством автоматизированного краулинга и находившихся в онлайн на момент сбора, и 344 ресурса с верифицированным офлайн-статусом. Фактическое соотношение статусов на момент прогона составило приблизительно 533 онлайн и 465 офлайн в силу естественной нестабильности ресурсов между периодами краулинга и тестирования – явление, хорошо известное из литературы [13].

Для оценки качества применялись стандартные метрики бинарной классификации: точность (accuracy), прецизионность (precision), полнота (recall) и F1-мера. Дополнительно фиксировались средняя, медианная задержка и 95-й перцентиль времени проверки, а также доля результатов с неопределенным статусом.

Результаты

В рамках экспериментального исследования проведена сравнительная оценка трех методов определения доступности информационных ресурсов оверлейной инфраструктуры. Результаты фиксировались с временными метками и детализированными кодами завершения, что обеспечило возможность сравнения как метрик качества классификации, так и показателей производительности. Сводные результаты представлены в табл. 1 и 2.

Метод HTTP-зондирования демонстрирует наилучшее соотношение показателей качества: точность 89,56%, F1-мера 0,910 при сравнительно умеренных задержках (среднее 2213 мс, медиана 1966 мс). Незначительное число ложноотрицательных срабатываний обусловлено таймаутами у части онлайн-ресурсов, а 95 ложноположительных результатов связаны преимущественно с ресурсами, доступными на уровне HTTP-ответа, но отдающими коды ошибок.

Таблица 1. Оценка методов на основе метрик качества классификации

Метод	Acc, %	Prec	Rec	F1	TP	TN	FP	FN	Unk, %	Ср. t, мс
Метод публикации дескриптора	75,85	0,689	1,000	0,816	533	224	241	0	0,20	1024
Метод ТСП-соединения	58,80	0,653	0,490	0,560	262	326	139	273	0,00	4286
Метод НТТР-зондирования	89,56	0,846	0,985	0,910	523	361	95	8	1,30	2213

Таблица 2. Оценка методов на основе метрик производительности и покрытия

Метод	count_total	count_known	median_t, мс	p95_t, мс	Интерпретация
Публикации дескриптора	1000	998	935	2486	Стабильный, быстрый
ТСП-соединения	1000	1000	3701	10012	Нет unknown, медленный
НТТР-зондирования	1000	987	1966	3918	Незначит. unknown, средний

Метод проверки публикации дескриптора обнаруживает парадоксальную картину: при почти идеальной полноте он демонстрирует низкую прецизионность. Это означает, что метод не пропускает ни одного онлайн-ресурса, однако признает доступными 241 ресурс, реально находящийся в офлайн. Механизм данного эффекта объясняется архитектурой DHT: дескриптор продолжает существовать в распределенном хранилище в течение нескольких часов после остановки сервиса, формируя устаревшие записи. Высокая скорость метода делает его привлекательным для предварительной фильтрации, но недостаточным для финальной верификации.

Метод проверки ТСП-соединения показал наихудшие результаты по всем ключевым метрикам: точность 58,80%, F1-мера 0,560, 273 ложноотрицательных срабатывания. Анализ деталей показывает, что значительная часть онлайн-ресурсов прослушивает нестандартные порты, что влечет систематическую ошибку при использовании портов по умолчанию. Дополнительно метод является самым медленным: среднее время 4286 мс, 95-й перцентиль 10012 мс – это объясняется накоплением задержек при ожидании таймаутов соединения.

Обсуждение

Установленный профиль ошибок метода проверки публикации дескриптора – высокая полнота при низкой прецизионности – находит прямое объяснение в архитектурных свойствах DHT. Buitrago et al. [10] показали, что дескриптор сохраняет валидность в хранилище в течение нескольких часов после остановки ресурса, а

доля запросов к DHT, приходящихся на несуществующие записи, достигает 80%. Зафиксированные $FP=241$ при $FN=0$ полностью согласуются с данной закономерностью, подтверждая, что метод первого уровня не способен различить активный ресурс и устаревший дескриптор, что ограничивает его применимость задачами предварительной фильтрации.

Результаты метода НТТР-зондирования соответствуют показателям, зафиксированным Loesing et al. [9] при тестировании аналогичных зондов - 85–92% в зависимости от конфигурации таймаутов. Незначительное число ложноотрицательных срабатываний объясняется таймаутами у перегруженных узлов, что Owen и Savage [6] также отмечают, как характерную особенность высоконагруженных ресурсов оверлейной инфраструктуры.

Низкие показатели метода ТСР-соединения согласуются с наблюдениями Buitrago et al. [10]. Значительная доля ресурсов прослушивает нестандартные порты, вследствие чего методы, ориентированные на порты 80 и 443, систематически занижают оценку доступности. Данная проблема устранима введением предварительного портового зондирования с расширенным набором типичных портов.

Зафиксированное изменение статуса $\sim 18\%$ ресурсов за период менее 24 часов согласуется с данными Owenson et al. [11] и указывает на необходимость многократного тестирования с временным интервалом как самостоятельного исследовательского направления.

На основании полученных результатов предлагается иерархическая стратегия комбинированного применения методов: метод публикации дескриптора используется как быстрый предварительный фильтр, а метод НТТР-зондирования как финальная верификация для ресурсов, прошедших первый шаг, и как резервный при статусе «неопределено» [14, 15]. Аналогичный каскадный подход предложен в работе Bergman [16], однако без количественного обоснования на реальной выборке настоящее исследование восполняет данный пробел.

Заключение

В настоящей работе предложена пятиуровневая иерархическая модель оценки доступности информационных ресурсов оверлейных сетей на базе луковой маршрутизации и проведена экспериментальная оценка трех методов, соответствующих первому, третьему и четвертому уровням модели, на выборке из 1000 узлов инфраструктуры третьей версии протокола.

Установлено, что методы принципиально различаются по профилю ошибок и области применимости: метод НТТР-зондирования обеспечивает наилучшее качество классификации и рекомендуется для финальной верификации; метод проверки публикации дескриптора применим исключительно как предварительный фильтр вследствие систематических ложноположительных срабатываний; метод ТСР-соединения требует доработки в части портового зондирования. На основании результатов обоснована иерархическая стратегия комбинированного применения методов, обеспечивающая баланс точности и скорости при минимизации нагрузки на целевую инфраструктуру.

Направления дальнейших исследований включают реализацию метода второго уровня иерархии - проверки доступности точек введения, - введение механизма портового зондирования для транспортного уровня, а также анализ временной динамики доступности ресурсов при многократном тестировании.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Appelbaum, J., & Muffett, A. (2015). RFC 7686: The “.onion” Special-Use Domain Name. Internet Engineering Task Force. URL:<https://datatracker.ietf.org/doc/html/rfc7686>
2. Pastor-Galindo J. et al. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends //IEEE access. – 2020. – Т. 8. – С. 10282-10304.
3. Barredo-Valenzuela A. R., Pastrana S., Suarez-Tangil G. Snorkeling in dark waters: A longitudinal surface exploration of unique Tor Hidden Services //IEEE Transactions on Information Forensics and Security. – 2025.
4. Winter P., Edmundson A., Roberts L. M., Dutkowska-Żuk A., Chetty M., & Feamster N. How do tor users interact with onion services? //27th USENIX Security Symposium (USENIX Security 18). – 2018. – С. 411-428.
5. Басыня Е. А., Хиценко В. Е., Рудковский А. А. Метод идентификации киберпреступников, использующих инструменты сетевого анализа информационных систем с применением технологий анонимизации //Доклады Томского государственного университета систем управления и радиоэлектроники. – 2019. – Т. 22. – №. 2. – С. 45-51.
6. Owen G., Savage N. Empirical analysis of tor hidden services //IET Information Security. – 2016. – Т. 10. – №. 3. – С. 113-118.
7. Sanatinia A., Park J., Blass E.-O., Mohaisen A., & Noubir G. A Privacy-preserving longevity study of Tor's hidden services //arXiv preprint arXiv:1909.03576. – 2019.
8. Boshmaf Y., Perera I., Kumarasinghe U., Liyanage S., Al Jawaheri H. Dizzy: large-scale crawling and analysis of onion services //Proceedings of the 18th International Conference on Availability, Reliability and Security. – 2023. – С. 1-11.
9. Learmonth I. R., Loesing K. Towards modernising data collection and archive for the Tor network //arXiv preprint arXiv:1812.08429. – 2018.
10. Biryukov A., Pustogarov I., Weinmann R. P. Trawling for tor hidden services: Detection, measurement, deanonymization //2013 IEEE Symposium on Security and Privacy. – IEEE, 2013. – С. 80-94.
11. Owenson G., Cortes S., Lewman A. The darknet's smaller than we thought: The life cycle of Tor Hidden Services //Digital Investigation. – 2018. – Т. 27. – С. 17-22.
12. Höller, T., & Mayrhofer, R. (2025). Evaluating Onion Address Collection Methods. In PETS 2025 / Free and Open Communications on the Internet (pp. 28–36). URL: <https://www.petsymposium.org/foci/2025/foci-2025-0009.pdf>
13. Buitrago López A., Pastor-Galindo J., Gómez Mármol F. Updated exploration of the Tor network: advertising, availability and protocols of onion services //Wireless Networks. – 2024. – Т. 30. – №. 9. – С. 7527-7541.
14. Huete Trujillo D. L., Ruiz-Martínez A. Tor hidden services: A systematic literature review //Journal of Cybersecurity and Privacy. – 2021. – Т. 1. – №. 3. – С. 496-518.
15. Оценка применимости инструментов анализа скрытых сервисов Tor // Интерэкспо Гео-Сибирь, 2025г. Т. 7, Вып. 2 Стр. 118-123
16. Bergman, J., & Popov, O. B. (2023). Exploring Dark Web Crawlers: A Systematic Literature Review of Dark Web Crawlers and Their Implementation. IEEE Access, 11, 35914–35933. URL: <https://su.diva-portal.org/smash/person.jsf?pid=authority-person:99686>

© М. С. Каранетьянц, 2026