UDC 621.391 DOI 10.36910/775.24153966.2023.76.18

V. Faychuk

Lviv Polytechnic National University

RESEARCHING ANONYMOUS ROUTING MODELS

Numerous solutions have been created for online anonymous communication. We do evaluations of security on several systems. We examine features such as Onion Routing, anonymous VPN services, probabilistic anonymity, and deterministic anonymity among different systems. There are also additional forms of anonymous communication that are discussed, including messaging, peer-to-peer communication, using the web, emailing, and using other Internet apps. We then go on to show several attack methods that aim to identify people who communicate anonymously. The objective of the research is to achieve an exact adjust between guaranteeing the adequacy and dependability of message delivery and ensuring customer anonymity. The NIAR model's non-interactive highlight makes it more valuable since it licenses secure communication without requiring nonstop client support. Communication privacy is threatened by an ever-growing volume of data generated by an ever-growing number of networked devices. Because of this, Anonymous Communication Systems (ACSs)—which offer the privacy qualities of anonymity, unsinkability, and observability—are recommended to conceal the relationship between transmitted communications and their senders and recipients. The objective of this essay is to evaluate the literature on Dining Cryptographers Networks (DCNs) in the subject of ACSs. Since the DCN-based techniques offer unconditional guarantees of observability, they are information-theoretically safe. Their computation and communication expense was considered high at the time, and scalability issues arose, which originally impeded their use for anonymous communications. By satisfying these targets, the research improves the state of encrypted communication systems and opens the door to a day when protecting client security will be a best need without sacrificing message delivery's significant dependability and efficiency.

Keywords: *Anonymous Routing, Onion Routers, NIAR Model, Privacy-preserving Communication, Network Security*

В. О. Файчук

ДОСЛІДЖЕННЯ МОДЕЛЕЙ АНОНІМНОЇ МАРШРУТИЗАЦІЇ

Створено багато рішень для анонімного спілкування в Інтернеті. Ми оцінюємо безпеку декількох систем. Ми розглядаємо такі функції, як Onion Routing, анонімні VPN-сервіси, імовірнісна анонімність та детермінована анонімність між різними системами. Також обговорюються додаткові форми анонімної комунікації, включаючи обмін повідомленнями, пірінгове спілкування, використання Інтернету, електронну пошту та інші інтернет-додатки. Далі ми покажемо кілька методів атак, спрямованих на ідентифікацію людей, які спілкуються анонімно. Метою дослідження є досягнення точного балансу між гарантуванням адекватності та надійності доставки повідомлень і забезпеченням анонімності користувачів. Неінтерактивність моделі NIAR робить її більш цінною, оскільки вона ліцензує безпечну комунікацію, не вимагаючи цілодобової підтримки клієнтів. Конфіденційність комунікації знаходиться під загрозою через постійно зростаючий обсяг даних, що генеруються постійно зростаючою кількістю мережевих пристроїв. Через це анонімні комунікаційні системи (ACS), які пропонують такі якості конфіденційності, як анонімність, непотоплюваність і спостережуваність, рекомендуються як спосіб приховати зв'язок між переданими повідомленнями та їхніми відправниками і одержувачами. Мета цього есе - оцінити літературу про мережі криптографів Dining Cryptographers Networks (DCN) в контексті АСУ. Оскільки методи, засновані на DCN, пропонують безумовні гарантії спостережуваності, вони є інформаційно-теоретично безпечними. Їх обчислювальні та комунікаційні витрати на той час вважалися високими, а також виникали проблеми з масштабуванням, що спочатку перешкоджало їх використанню для анонімних комунікацій. Задовольняючи ці цілі, дослідження покращує стан зашифрованих систем зв'язку і відкриває двері до того дня, коли захист безпеки клієнтів буде найкращою потребою без шкоди для значної надійності та ефективності доставки повідомлень.

Ключові слова: *Анонімна маршрутизація, цибулинні маршрутизатори, модель NIAR, конфіденційність зв'язку, мережева безпека*

Problem statement. In many circumstances, people may want strong communication privacy and anonymity when using the Internet. These are situations when individuals must report any knowledge they may have about illicit activity without worrying about reprisals or penalties. Additionally, those who reside in countries where authorities attempt to control what their citizens may say and do online require ways to get around censorship and other limitations on their right to free expression. Furthermore, individuals may desire the freedom to use the internet without third parties tracking their online activities and selling their data to other businesses.

Our goal in writing this study is to analyze open problems and the current state of the art in ACS. Specifically, we have been able to concentrate on any research project whose primary objective is to offer a solution for emerging trends in anonymous systems. Any researcher interested in beginning a study in this field should be aware of the most recent developments and the ACS's current research priorities.

Analysis of recent research and publications. It was suggested that (Lightweight Incentivized Routing for Anonymity) LIRA [1] use a crypto lottery at routers to overcome some of these restrictions. A customer can estimate and receive priority service with a configurable probability if he requests a prioritized

service. Clients can operate as routers and get token from a central bank in return for their bandwidth to receive priority service guarantees. After that, clients can buy "guaranteed winners" tickets to the lottery with those tokens to receive superior support at the routers. LIRA's primary flaw is the fact that disobedient clients can attempt to construct many circuits before receiving a prioritized one. If, in the absence of a "guaranteed winner" ticket, the likelihood of gaining the lottery to get a better service is 20%, for instance, clients will typically receive two prioritized networks out of every ten that they build. This will incentivize clients to keep creating networks to find winners, thereby wasting network resources. Reducing the likelihood of success creates problems with anonymity because the anonymity set might be shrunk by an adversary keeping an eye on a priority circuit. Nevertheless, because LIRA's bank only communicates with ORs rather than with all customers, LIRA handles the scalability concerns associated with BRAIDS.

By spreading the administration of incentives over several semi-trusted parties, like the official directory servers already in use by Tor, TEARS [1] aims to address the scalability issues. The semi-trusted servers communicate with routers via an openly auditable e-cash protocol, which is akin to Bitcoin, to deter misbehavior. In return for bandwidth, they use to transport anonymous traffic, servers provide routers anonymous currency known as Shallots. Priority Passes are router-specific tickets that may be traded for cash to receive network service that is prioritized. To boost the routers' anonymity, set, the trustworthy servers additionally give users Shallots. One problem facing TEARS is that, to do safe bandwidth measurements, it depends on a decentralized procedure, which is not present in the current version of Tor network. Although the Tor network presently uses bandwidth authority, how accurate their measures are in the face of different antagonistic situations is unclear.

According to Kuhn, Christiane, et al., the pairing-based onion routing (PB-OR) protocol, which makes use of a pairing-based non interactive important agreement process, should be used in place of the circuit creation strategy in TOR (the onion router). They employ an identity-based infrastructure to enable their approach to achieve unilateral anonymity, which is the ability of the client to authenticate a router without disclosing the client's identity. A reliable party called the private key generator (PKG) utilizes a master key that is only known to the PKG in conjunction with a router's well-known identification ID to create a secret key d for the router. Conversely, clients have the ability to independently construct an unlimited number of pseudonyms and the private keys associated with each one. Subsequently, the client presents a unique pseudonym to each router to maintain anonymity throughout the key agreement phase; routers utilize their personal keys d to finalize the key agreement. In comparison to Tor, the key agreements protocol greatly minimizes the communication-related cost of circuit building because it is non-interactive, enabling the establishment of a circuit in a single pass. Nevertheless, there is a single point of failure since the PKG may decode any communication that has been encrypted for clients. Additionally, routers must engage in expensive interactions with the PKG to regularly update their identification keys in order to preserve forward secrecy [2].

Based on the idea of onion routing, Tor is a low-latency anonymity network. Today, the network is made up of over 6000 Onion Routers (ORs), which are volunteer-operated routers. Every OR generates a router descriptor and submits it to directory authority with contact details about the router, including its Internet Protocol (IP) address, ports and public keys, and bandwidth capacity. These authorities create a document outlining the network consensus and forward it to directory servers with the descriptors. Before they can interact with their Internet destinations, Tor clients, also known as Onion Proxies (OPs), establish pathways, or circuits, via the network by downloading the consensus and descriptors from the directory servers. Depending on where they are in the circuit, the three ORs, or hops, that make up each circuit are called the entrance guard, middle, and exit ORs. TLS is utilized to offer hop-by-hop authenticity, data integrity, and secrecy when ORs in a circuit are connected via TCP connections. In Tor, data is sent in cells, which are fixed-sized units of 512 bytes [3].

Presentation of the main material. The contemporary information age's tremendous advancements in communication and pervasive computer capabilities, which are collecting ever-increasing amounts of data, are benefiting society greatly. This includes possibilities and revolutionary shifts brought about in a variety of spheres of everyday life, such as social contact, healthcare, transportation, and education. Many of the gathered data, meanwhile, may be delicate or contain personal data. As a result, there are significant privacy problems with their gathering and transmission. These could stop new technologies from being incorporated into daily life on a larger scale [4].

Furthermore, in many circumstances, people may want great communications anonymity and confidentiality on the Internet. These are situations when people must report any knowledge, they may have about illegal activity without worrying about retaliation or penalties. Additionally, those who reside in

countries where authorities attempt to restrict what their people may say and do online require ways to get around censorship and other limitations on their right to free expression. Furthermore, individuals may desire unrestricted access to the internet for personal purposes, free from third-party data collection on their online activities and subsequent sale of their personal data to other businesses [5]. To prevent situations like these and guarantee the security of messages carried across intermediate networks, end-to-end encryption is frequently utilized. After that, the communication may only be read by the designated recipient. Nevertheless, encryption only prevents other parties from accessing data that has been transferred. It is unable to conceal the fact that parties are conversing and exchanging messages [6, 7].

Because they handle the majority of network protocols, popular application-level switches including Virtual Private Networks (VPNs), proxies, mix-based solutions, and onion-based routings like The Onion Router (Tor) [8] have been extensively implemented in practice. However, they typically only provide a restricted level of anonymity protection, and traffic analysis attacks can still be launched by an observer tracing packets in order to violate anonymity assurance. Conversely, an adversary keeping tabs on users cannot discern between messages containing genuine content and random noise when using DCN-based Anonymous communication system (ACSs). These systems do, however, present some difficulties, such as handling interruptions and offering round (or slot) reservation strategies [9]. Furthermore, there was a lack of scalability and significant computation and communications overheads with the first DCN-based ACSs. Because of this, despite the fact that DCN has been around for about thirty years, they were seldom ever used in anonymous real-world communications until fixes were offered to increase their effectiveness and make them more practical [10].

In the framework of circuit-based routing developed onion routing-based approaches as an equivalent of Mix networks. In contrast to mixes, onion routing does not route each packet independently. Rather, the client selects a path then sends the initial message and labels the selected path to start a circuit using the network. Each onion router in a circuit is aware of the previous one and successor, while it is unaware of the other node in the network. Once the circuit is established, each message with a certain label is sent along this pre-planned path. Ultimately, the route can be closed with a message issued [11].

Onion routing-based ACSs offer a socket connection that is independent of application. As a result, several apps (such as web surfing, SSH, and instant messaging) may use them with ease [124]. Onion routing-based ACSs vary, nevertheless, in terms of how the onion router are set up, how encryption techniques are used, how tunnels are created, whether TCP or UDP is used at the transport layer, and whether or not the clients transmit traffic to additional clients. As a result, many ACSs using onion routing as their foundational technique have been put into use. The reduced latency connections provided by these systems have drawn millions of consumers. Based on the onion routing concept [12], Tor is a distributed-trust, low-latency, anonymous communication network that operates on circuits. Overlay networks, like Tor, are built as communication networks on top of other networks [60]. It is made up of a group of servers known as onion routers that are provided voluntarily and are used to construct circuits and send data. Another message-oriented system that provides anonymization services using a peer-to low-latency communication is the Invincible Internet Project (I2P). In actuality, I2P is an additional overlay network that was primarily created to allow for completely anonymous communication within the network between two participants [13].

Broadcasting or multicast-based communication is used by several ACSs. This sort of strategy can also include DCN-based techniques. Nonetheless, it is more appropriate to treat DCN-based ACSs as a primary distinct category because they are primarily developed on Chaum's protocols and offer sender anonymity as well. ACSs that are based on broadcasting or multicasting include Peer-to-Peer Personal Privacy Protocol (P5) [14], K-Anonymity [15], Multicasting Mixes for Efficient and Anonymous Communication (M2) [16], Mutual Anonymous Multicast (MAM) [10], and Broadcast Anonymous Routing (BAR) [17]. For example, P5 establishes a broadcast hierarchy whereby varying hierarchy levels offer varying degrees of anonymity at the expense of communication dependability and bandwidth [18]. In P5, a single up node transmits all messages intended for a specific recipient. As a result, neither the sender nor the recipient are aware of each other's identities or the host or address that the recipient is using.

Rabin presented the initial version of Oblivious Transfer (OT) in [19], which was utilized as a protocol for secret communication between two parties [70]. An OT protocol allows a sender to deliver a record of data to a recipient from a series of records, concealing the other records from the recipient and keeping the sender in the dark regarding which record is chosen. "Chosen one-out-of-two" OT, or OT2 1, is a somewhat more sophisticated type of OT in which the sender provides two private inputs (X1, X2), and the recipient can select to receive only one of them while remaining unaware of the other input. Similar to this, model developed the generalized version of OT under the title of all or nothing disclosure of secrets

(ANDOS). The sender has n private inputs in 1-out-of-n, or OT n 1, and the recipient can select one of them at will without knowing the other inputs or the sender's identity of which input is sent [20].

Similar to OT, Private Information Retrieval (PIR) protocols enable a client to obtain an item from a location inside the client's database without disclosing which record was obtained [21]. Although it can't adapt to shifts in the network structure. Samy, Islam, et al. implements anonymous communication with a respectable privacy guarantee using hybrids mix networks and PIR methods. In a system with numerous servers, Riposte [33] also makes use of PIR methods to allow anonymous message broadcasting [22]. Private Keyword-Based Push and Pull (P3) [23], and Private Information Retrieval for Everyone (XPIR) [24] are other PIR-based anonymous communication systems which let users to send and receive messages without anybody discovering they are part of a discussion by using a key-value store. These techniques show a significant client load, even though good database organization makes them easier to scale to a high number of users. Because of this, PIR approaches need a lot of processing power and bandwidth. They also often offer data anonymity, which means that although the destination is aware of the client, it is unaware of the records that are read or transmitted.

Recently, Shi and Wu offered a very different method to this problem: hiding connection patterns via cryptographic approaches. They specifically offer the Non-Interactive Anonymous Router (NIAR) paradigm, in which all data passes via a central router and a set of N receiving nodes want to receive data from a set of N sending nodes. According to their concept, anonymity is the incapacity to connect any sender to the matching receiver, even in cases where the network router and (up to $N - 2$) different (sender, receiver) pairings are vulnerable to an opponent that is both honest and inquisitive. The NIAR model as previously said has application in several real-world situations. Large messages to be transferred and/or non-ephemeral/indefinite communication channels are crucial components of any such application, as is the desire of several (sender, receiver) pairs to interact anonymously with one another through a central server [25].

Conclusion. We now live in an era of technology where we may speak, share information, connect social networks, amuse ourselves, and more through communications technologies. These conversations can be tracked and overheard to gather useful data about users, including personally identifying information, communication patterns, and other details that make it possible to create user profiles. Systems for anonymous communications have been proposed to protect our privacy.

In the last few years, ACS has built a significant research effort. We conducted this research, which spans a recent period and allows any research dedicated to this topic to know the state of the art to determine the state of the art in this field. Online anonymity is offered by several businesses and applications. The first point to note is that each program and/or service has a designated region where anonymity is offered. A service or software cannot be protected against every potential attack.

A greater level of security and anonymity may be provided by distributed anonymizing systems like TOR and I2P than by centralized services, where identity disclosure occurs at a single location. However, timing, intersection, and cooperative eavesdroppers might jeopardize anonymity.

References

1. Jansen R., Johnson A. On the Accuracy of Tor Bandwidth Estimation. *Passive and Active Measurement*. Cham, 2021. P. 481–498. URL: https://doi.org/10.1007/978-3-030-72582-2_28 (date of access: 18.12.2023).
2. Onion Routing with Replies / C. Kuhn et al. *Lecture Notes in Computer Science*. Cham, 2021. P. 573–604. URL: https://doi.org/10.1007/978-3-030-92075-3_20 (date of access: 18.12.2023).
3. CRYPTOGRU: Low Latency Privacy-Preserving Text Analysis With GRU / B. Feng et al. *Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing*, Online and Punta Cana, Dominican Republic. Stroudsburg, PA, USA, 2021. URL: https://doi.org/10.18653/v1/2021.emnlp-main.156 (date of access: 18.12.2023).
4. Bunn P., Kushilevitz E., Ostrovsky R. Anonymous Permutation Routing. *Theory of Cryptography*. Cham, 2023. P. 33–61. URL: https://doi.org/10.1007/978-3-031-48621-0_2 (date of access: 18.12.2023).
5. Chauhan M., Singh A. K., Komal. Survey of Onion Routing Approaches: Advantages, Limitations and Future Scopes. *Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI - 2019)*. Cham, 2020. P. 686–697. URL: https://doi.org/10.1007/978-3-030-43192-1_76 (date of access: 18.12.2023).
6. Ke Y., Zilin W., Zhanfei D., Xinzheng H., Chunfu J., Yuan H. Anonymous Query Mechanism Construction of Timed-Release Encryption. *Advanced Engineering Science/Gongcheng Kexue* Yu Jishu. 2022. vol. 54. URL: https://www.gkyj-aes-20963246.com/article/anonymous-query-mechanism-construction-of-timed-release-encryption (date of access: 18.12.2023).

7. Komlo C. H., Mathewson N., Goldberg I. Walking onions: Scaling anonymity networks while protecting users: *Proceeding of the 29th USENIX Security Symposium (USENIX Security 20)*. 2020. P. 1003-1020. URL: https://www.usenix.org/conference/usenixsecurity20/presentation/komlo (date of access: 18.12.2023).
8. Hiller J., Pennekamp J., Dahlmanns M., Henze M., Panchenko A., & Wehrle K. Tailoring onion routing to the internet of things: Security and privacy in untrusted environments. *2019 IEEE 27th International Conference on Network Protocols (ICNP)*. 2019. P. 1-12. doi: 10.1109/ICNP.2019.8888033
9. Deep Learning and Onion Routing-based Collaborative Intelligence Framework for Smart Homes underlying 6G Networks / N. K. Jadav et al. *IEEE Transactions on Network and Service Management*. 2022. P. 1. URL: https://doi.org/10.1109/tnsm.2022.3164715 (date of access: 18.12.2023).
10. A Survey on Anonymous Communication Systems with a Focus on Dining Cryptographers Networks / M. Shirali et al. *IEEE Access*. 2023. P. 1. URL: https://doi.org/10.1109/access.2023.3242870 (date of access: 18.12.2023).
11. Dimitriou T. Efficient, Coercion-free and Universally Verifiable Blockchain-based Voting. *Computer Networks*. 2020. Vol. 174. P. 107234. URL: https://doi.org/10.1016/j.comnet.2020.107234 (date of access: 18.12.2023).
12. Blockchain and Onion Routing-based Secure Message Exchange System for Edge-enabled IIoT / R. Gupta et al. *IEEE Transactions on Industrial Informatics*. 2022. P. 1–12. URL: https://doi.org/10.1109/tii.2022.3191444 (date of access: 18.12.2023).
13. Ghazi-Tehrani A. K. Mapping Real-World Use of the Onion Router. *Journal of Contemporary Criminal Justice*. 2023. P. 104398622311575. URL: https://doi.org/10.1177/10439862231157553 (date of access: 18.12.2023).
14. Design of peer-to-peer protocol with sensible and secure IoT communication for future internet architecture / V. Vijaya Kumar et al. *Microprocessors and Microsystems*. 2020. Vol. 78. P. 103216. URL: https://doi.org/10.1016/j.micpro.2020.103216 (date of access: 18.12.2023).
15. Arava K., Lingamgunta S. Adaptive k-Anonymity Approach for Privacy Preserving in Cloud. *Arabian Journal for Science and Engineering*. 2019. Vol. 45, no. 4. P. 2425–2432. URL: https://doi.org/10.1007/s13369-019-03999-0 (date of access: 18.12.2023).
16. GKMPAN: An Efficient Group Rekeying Scheme for Secure Multicast in Ad-Hoc Networks* / S. Zhu et al. *Journal of Computer Security*. 2006. Vol. 14, no. 4. P. 301–325. URL: https://doi.org/10.3233/jcs-2006-14401 (date of access: 18.12.2023).
17. Tian C., Zhao S., Cheng Z. AntCom: An effective and efficient anti-tracking system with dynamic and asymmetric communication channel. *Journal of Network and Computer Applications*. 2023. P. 103700. URL: https://doi.org/10.1016/j.jnca.2023.103700 (date of access: 18.12.2023).
18. Kotzanikolaou P., Chatzisofroniou G., Burmester M. Broadcast anonymous routing (BAR): scalable real-time anonymous communication. *International Journal of Information Security*. 2016. Vol. 16, no. 3. P. 313–326. URL: https://doi.org/10.1007/s10207-016-0318-0 (date of access: 18.12.2023).
19. A Survey of Oblivious Transfer Protocol / V. K. Yadav et al. *ACM Computing Surveys*. 2022. URL: https://doi.org/10.1145/3503045 (date of access: 18.12.2023).
20. Peer-Communication in Distance Education: Perspectives and Challenges / C. Papi et al. *Ubiquitous Learning: An International Journal*. 2019. Vol. 12, no. 1. P. 13–33. URL: https://doi.org/10.18848/1835-9795/cgp/v12i01/13-33 (date of access: 18.12.2023).
21. Vithana S., Banawan K., Ulukus S. Semantic Private Information Retrieval. *IEEE Transactions on Information Theory*. 2022. Vol. 68, no. 4. P. 2635–2652. URL: https://doi.org/10.1109/tit.2021.3136583 (date of access: 18.12.2023).
22. Asymmetric Leaky Private Information Retrieval / I. Samy et al. *IEEE Transactions on Information Theory*. 2021. Vol. 67, no. 8. P. 5352–5369. URL: https://doi.org/10.1109/tit.2021.3085363 (date of access: 18.12.2023).
23. Eskandarian S., Corrigan-Gibbs H., Zaharia M., & Boneh D. Express: Lowering the cost of metadata-hiding communication with cryptographic privacy. In *arXiv [cs.CR]*. 2019. http://arxiv.org/abs/1911.09215
24. Mozaffari H., Houmansadr, A. Heterogeneous Private Information Retrieval. Proceedings 2020 Network and Distributed System Security Symposium. 2020. https://www.ndss-symposium.org/wp-content/uploads/2020/02/24363-paper.pdf
25. Shi E., Wu K. Non-interactive anonymous router. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2021. P. 489-520.