Comunicação: Algoritmos de Resposta Aleatória como Mecanismo para a Desvinculação entre o Tráfego de Entrada e de Saída em Sistemas de Anonimato Baseados em Circuitos

Afonso Vilalonga, Kevin Gallagher, Alex Davidson, and Henrique Domingos

Universidade NOVA de Lisboa & NOVA LINCS
Portugal
j.vilalonga@campus.fct.unl.pt, {k.gallagher,a.davidson,hj}@fct.unl.pt

Resumo Sistemas de comunicação anónima são, atualmente, fundamentais para que utilizadores em qualquer parte do mundo possam manter o seu direito à liberdade de expressão e privacidade. No entanto, com os avanços científicos nas metodologias de análise de tráfego, é cada vez mais difícil garantir a desvinculação (i.e., *unlinkability*) entre o tráfego de entrada e saída em sistemas de anonimato baseados em circuitos, como o Tor, permitindo desanonimizar os seus utilizadores. Para endereçar este problema, defendemos a adaptação de algoritmos de resposta aleatória para sistemas de comunicação anónima baseados em circuitos. Estes permitem providenciar privacidade diferencial, garantido assim que o sistema que os utiliza mantém uma noção forte de privacidade aos seus utilizadores. Para tal, convertemos este tipo de algoritmos numa primitiva de encaminhamento de pacotes que, com base numa probabilidade predefinida, determina se um dado pacote é encaminhado para o próximo nó do circuito ou se, em vez do pacote verdadeiro, é enviado um pacote falso. Implementámos um protótipo inicial deste sistema por cima da rede Tor através do desenvolvimento de um *pluggable transport*. Por fim, apresentamos ainda uma avaliação preliminar da performance do protótipo desenvolvido.

Keywords: Sistemas de anonimato · Anonimato e privacidade em redes · Algoritmos de resposta aleatória · Privacidade diferencial.

1 Introdução e Contexto

O direito à privacidade e ao anonimato numa sociedade democrática é de extrema importância, permitindo que diferentes grupos de pessoas se sintam seguras e livres de se expressarem como desejam. No entanto, garantir a privacidade e o anonimato online é complexo, dada a natureza das próprias comunicações ao nível da rede, que colocam um identificador de recipiente e remetente em cada pacote enviado.

Para mitigar este problema e garantir a privacidade dos utilizadores da Internet, foram desenvolvidos sistemas de anonimato que desvinculam os utilizadores

dos destinos por estes acedidos, impedindo assim que observadores externos infiram simultaneamente o remetente e o destinatário de um dado fluxo de tráfego. Estes sistemas podem ser essencialmente classificados em três tipos: sistemas de baixa, média e alta latência. Os sistemas de alta latência [1,2,3] oferecem as garantias de anonimato mais fortes, mas, na prática, são inutilizáveis para tarefas comuns devido ao alto tempo de resposta e ao facto de terem como foco o envio de mensagens ao invés de operarem por conexões ou circuitos. No outro extremo existem os sistemas de baixa latência [4,5,6], sendo que estes oferecem o menor grau de anonimato aos seus utilizadores dada a sua vulnerabilidade a ataques de correlação de tráfego [7]. No entanto, são também os que oferecem menores tempos de resposta uma vez que operam através de conexões e, portanto, permitem o seu uso em tarefas do dia-a-dia, como navegar online. Os sistemas de média latência [8,9,10] tentam equilibrar as garantias de anonimato que oferecem e o tempo de resposta, garantindo um maior grau de anonimato que os sistemas de baixa latência (ainda que menor que os sistemas de alta latência), e um tempo de resposta menor que os sistemas de alta latência (ainda que maior que os sistemas de baixa latência). É, no entanto, importante salientar que tanto os sistemas de alta latência como os de média latência, tendem a providenciar garantias de anonimato aos seus utilizadores medidas através de metodologias baseadas em teoria da informação [11,12], exigindo características e restrições especificas ao tráfego e, portanto, não sendo, muitas vezes, compatíveis com sistemas de anonimato baseados em circuitos. Os sistemas de baixa latência tendem a utilizar avaliações experimentais para demonstrar as suas garantias de anonimato, que apesar de indicativas, não providenciam garantias fortes e formais de anonimato.

Nesta comunicação, adicionamos ao estado da arte a nossa contribuição, olhando para este problema pela lente da privacidade diferencial [13]. Propomos um algoritmo de encaminhamento de pacotes para descrever um possível sistema de anonimato baseado em circuitos que assegure a definição de privacidade diferencial. O sistema proposto tem por base a família de algoritmos de resposta aleatória, sendo estes um mecanismo inicialmente desenvolvido para obter informação estatística sobre comportamentos ilegais ou embaraçosos por meio de questionários feitos a entrevistados [14]. A noção de privacidade advém do conceito de negação plausível de qualquer resultado por parte do entrevistado quando este é questionado se tem uma dada propriedade P (algo embaraçoso ou ilegal), uma vez que tanto a resposta afirmativa como a negativa ocorrem com pelo menos uma dada probabilidade, independentemente do entrevistado a ter ou não [15]. Apresentamos uma versão preliminar do nosso sistema na secção 2, implementado sobre a forma de um *pluggable transport* e validamos a sua usabilidade com base em métricas de performance na secção 3. Por fim concluímos a comunicação na secção 4.

2 Modelo do Sistema

O sistema desenvolvido tem por base uma primitiva de encaminhamento de tráfego que usa algoritmos de resposta aleatória para decidir o que fazer com cada

pacote em cada intervalo de tempo *it*. Implementámos este sistema como um *pluggable transport* para a rede Tor. No entanto, este pode ser adaptado para qualquer outro sistema de anonimato baseado em circuitos existente ou novo. Tendencialmente, um *pluggable transport* pode ser dividido em dois componentes: um componente executado do lado do utilizador e um componente executado no nó de entrada da rede Tor, designado de *Bridge*. Ambos os componentes comunicam entre si através de um protocolo específico a cada *pluggable transport*, tendo este protocolo o intuito de alterar as características do tráfego Tor transmitido entre os dois componentes, de forma a que um observador externo não o identifique como tráfego Tor.

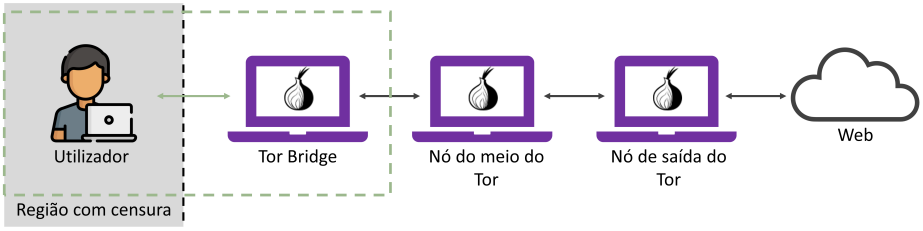

Figura 1: Modelo do sistema.

A Figura 1 apresenta uma visão de alto nível do sistema implementado. O quadrado tracejado a verde destaca o local de atuação do nosso *pluggable transport* na rede Tor. Quando um utilizador utiliza o *pluggable transport* desenvolvido para se conectar à rede Tor, todos os pacotes transmitidos entre o utilizador e a *Bridge* são processados pelo algoritmo de encaminhamento. O algoritmo é ativado a cada *it* unidades de tempo. Caso não exista nenhum pacote para enviar (i.e., pacote verdadeiro), um pacote falso é enviado. Caso existam pacotes a enviar, o algoritmo de resposta aleatória envia ou um pacote verdadeiro, ou um pacote falso, com probabilidades $\frac{e^{\epsilon}}{1+e^{\epsilon}}$ e $\frac{1}{1+e^{\epsilon}}$ [16], respetivamente (o valor de ϵ regula o grau de privacidade do nosso sistema). Tanto os pacotes falsos como os verdadeiros são moldados para terem o mesmo tamanho.

3 Avaliação do Sistema

Para avaliar a usabilidade do sistema, realizámos uma avaliação preliminar com base no tempo de *download* de um ficheiro (10 MB), semelhante aos testes de performance feitos para o Tor [17]. Os testes foram realizados através da rede Tor com o nosso *pluggable transport* configurado. Cada observação apresentada no gráfico corresponde a uma média de 5 repetições do mesmo teste. Foram testadas diferentes configurações do sistema, nomeadamente, valores de ϵ (grau de privacidade) e de intervalos temporais de execução do algoritmo (*it*) diferentes.

Os resultados são apresentados no gráfico 2. Avaliámos o sistema para intervalos de tempo *it* de 100 microssegundos (μs), 1 milissegundo (ms), 2 ms, e 5

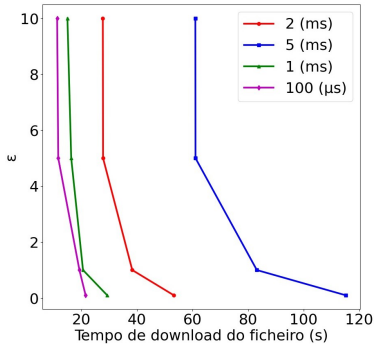

Figura 2: Tempos de *download* de um ficheiro (10 MB), variando ϵ e it.

ms, testando cada valor de it para diferentes ϵ (0,1, 1, 5 e 10). Para comparação, medimos também o tempo de *download* do ficheiro utilizando a rede Tor sem o nosso *pluggable transport* configurado, obtendo um valor de 9,14 segundos (s). Olhando para os extremos, o melhor tempo observado ($it = 100$ μs e $\epsilon = 10$) foi de 11,29 s, resultando assim num aumento de 2,15 s em relação à rede Tor sem o nosso *pluggable transport*. O pior tempo observado ($it = 5$ ms e $\epsilon = 0,1$) foi de 115,13 s, resultando num aumento de 105,99 s em relação à rede Tor sem o nosso *pluggable transport*. Podemos ainda concluir que intervalos de tempo it maiores resultam em tempos de *download* mais longos, dado que a frequência de envio de pacotes é menor. Por outro lado, valores de ϵ menores resultam num aumento do tempo de *download*, uma vez que quanto menor o ϵ maior a probabilidade de enviar um pacote falso.

4 Conclusão

Nesta comunicação, endereçámos preliminarmente a vulnerabilidade dos sistemas de baixa latência a ataques de correlação de tráfego e a impraticabilidade no uso dos sistemas de alta e média latência. Desenvolvemos um sistema baseado em algoritmos de resposta aleatória, implementado como um *pluggable transport* e realizámos uma avaliação preliminar da usabilidade do sistema. Como trabalho futuro, pretendemos analisar o grau de privacidade oferecido pelo sistema e estender a implementação para permitir que múltiplos nós de uma rede de anonimato possam utilizar esta lógica no encaminhamento dos pacotes. Realizaremos ainda uma análise experimental detalhada com foco na performance, escalabilidade e resistência a ataques de correlação e de análise de tráfego [18,19].

Agradecimentos

Este trabalho foi suportado pelo NOVA LINCS ref. UIDB/04516/2020 (`https://doi.org/10.54499/UIDB/04516/2020`) e ref. UIDP/04516/2020 (`https://doi.org/10.54499/UIDP/04516/2020`) com o apoio financeiro da FCT.IP.

Referências

1. Gulcu, C. & Tsudik, G. Mixing E-mail with Babel. *Proceedings Of Internet Society Symposium On Network And Distributed Systems Security*. pp. 2-16 (1996)
2. Danezis, G., Dingledine, R. & Mathewson, N. Mixminion: design of a type III anonymous remailer protocol. *2003 Symposium On Security And Privacy, 2003.*. pp. 2-15 (2003)
3. Moeller, U. Mixmaster Protocol Version 2. (Internet Engineering Task Force,2004,12), https://datatracker.ietf.org/doc/draft-sassaman-mixmaster/03/, Work in Progress
4. Dingledine, R., Mathewson, N. & Syverson, P. Tor: The Second-Generation Onion Router. *13th USENIX Security Symposium (USENIX Security 04)*. (2004,8), https://www.usenix.org/conference/13th-usenix-security-symposium/tor-second-generation-onion-router
5. Chen, C., Asoni, D., Barrera, D., Danezis, G. & Perrig, A. HORNET: High-speed Onion Routing at the Network Layer. *Proceedings Of The 22nd ACM SIGSAC Conference On Computer And Communications Security*. pp. 1441-1454 (2015), https://doi.org/10.1145/2810103.2813628
6. The I2P Project I2P: The Invisible Internet Project. , https://geti2p.net/en/, [accessed 11-July-2024]
7. Serjantov, A. & Sewell, P. Passive Attack Analysis for Connection-Based Anonymity Systems. *Computer Security – ESORICS 2003*. pp. 116-131 (2003)
8. Piotrowska, A., Hayes, J., Elahi, T., Meiser, S. & Danezis, G. The Loopix Anonymity System. *26th USENIX Security Symposium (USENIX Security 17)*. pp. 1199-1216 (2017,8), https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/piotrowska
9. Nunes, V., Brás, J., Carvalho, A., Barradas, D., Gallagher, K. & Santos, N. Enhancing the Unlinkability of Circuit-Based Anonymous Communications with k-Funnels. *Proc. ACM Netw.*. **1** (2023,11), https://doi.org/10.1145/3629140
10. Diaz, C., Halpin, H. & Kiayias, A. The Nym Network. (https://nymte.ch/nym-whitepaper.pdf,2021)
11. Serjantov, A. & Danezis, G. Towards an Information Theoretic Metric for Anonymity. *Privacy Enhancing Technologies*. pp. 41-53 (2003)
12. Díaz, C., Seys, S., Claessens, J. & Preneel, B. Towards Measuring Anonymity. *Privacy Enhancing Technologies*. pp. 54-68 (2003)
13. Dwork, C., McSherry, F., Nissim, K. & Smith, A. Calibrating Noise to Sensitivity in Private Data Analysis. *Theory Of Cryptography*. pp. 265-284 (2006)
14. Warner, S. Randomized Response: A Survey Technique for Eliminating Evasive Answer Bias. *Journal Of The American Statistical Association*. **60**, 63-69 (1965), http://www.jstor.org/stable/2283137
15. Dwork, C. & Roth, A. The Algorithmic Foundations of Differential Privacy. *Foundations And Trends® In Theoretical Computer Science*. **9**, 211-407 (2014), http://dx.doi.org/10.1561/0400000042
16. Holohan, N., Leith, D. & Mason, O. Optimal Differentially Private Mechanisms for Randomised Response. *IEEE Transactions On Information Forensics And Security*. **12**, 2726-2735 (2017)
17. Tor Project Tor Metrics. (https://metrics.torproject.org/torperf.html,2024), Accessed: 2024-07-11

18. Hayes, J. & Danezis, G. k-fingerprinting: A Robust Scalable Website Fingerprinting Technique. *25th USENIX Security Symposium (USENIX Security 16)*. pp. 1187-1203 (2016,8), https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/hayes
19. Sirinam, P., Imani, M., Juarez, M. & Wright, M. Deep Fingerprinting: Undermining Website Fingerprinting Defenses with Deep Learning. *Proceedings Of The 2018 ACM SIGSAC Conference On Computer And Communications Security*. pp. 1928-1943 (2018), https://doi.org/10.1145/3243734.3243768