The novel use of Bridge Relays to provide persistent Tor connections for mobile devices

Stephen Doswell*, Nauman Aslam*, David Kendall* and Graham Sexton*
*Faculty of Engineering and Environment
Northumbria University, Newcastle upon Tyne, United Kingdom NE1 8ST
Email (main author): stephen.doswell@northumbria.ac.uk

***Abstract*—The number of wireless mobile devices connecting to the Internet, is predicted to surpass static connections by 2014. A desire for privacy will provide additional challenges in the future, for anonymity networks such as Tor, in supporting this increasing mobile user base. In this paper, we assess the potential performance impact to a mobile user accessing Tor while roaming from different Internet connections. An experiment was undertaken to simulate a mobile user at various mobility speeds (e.g. walking) alongside a range of Tor circuit build times. The results show that the impact to the mobile user (and potentially the overall Tor network) was significant when roaming between networks, and as expected, increased with higher mobility speeds and longer circuit build times. We also reviewed previous related research and, as one potential solution, considered whether Bridge Relays could additionally be used to provide a persistent connection to the Tor network, for roaming mobile users. Performance is critical for low latency anonymity networks, such as Tor, and understanding the potential impact of this increasing mobile user base, to both the mobile user and overall Tor network, is becoming critical.**

I. Introduction

Tor is a "distributed overlay network designed to anonymize TCP-based applications like web browsing, secure shell and instant messaging" [1]. Tor uses the concept of 'onion routing' [2], based on Chaum's original 'Mix-Net' design [3].

In order to access anonymously the World Wide Web (WWW), for example, a Tor user first receives a list of available routers from one of the distributed Tor directory servers. The user initiates a path by sending a message to the first router (Entry Guard) and, using a Diffie-Hellman key exchange [4], a session key is generated between the user and Entry Guard. The circuit is then extended by undertaking the same process one Tor router ('hop') at a time, incrementally extending each time with the established session keys for the previous hop(s); a technique also known as 'telescoping'. Once three hops have been established, the circuit is complete and ready for use. The 'core' messages from the user e.g. HTTP GET requests, are encapsulated alongside an Internet Protocol (IP) header for each router, within individually encrypted layers creating the multi-layered Tor 'onion'. The onion is forwarded through the SOCKS proxy interface (localhost), and then relayed by one of the available circuits, as data-streams, via multiplexed TCP connections between the routers. The onion is then 'un-peeled' incrementally by the router at each hop, revealing the next layer until the core message is exposed at the final hop (i.e. Exit Router), where it is sent to and processed by the final destination.

The balance between maintaining anonymity and performance is critical for Tor [5]. Low latency anonymity networks, such as Tor, have to continually make design decisions based on maintaining this balance [6]. The number of 'hops' and router selection algorithms are key examples [7][8]. However, it is not only design choices which can affect this critical balance. Research has also shown that threats to reliability, such as a denial of service attack on Tor routers, can simply decrease anonymity through an overall reduction of available routers for circuit building by the user [9]. Additionally, poor performance can also impact user satisfaction and consequently may deter users and reduce the overall anonymity set (in a 'snow-ball' effect), where eventually the number of concurrent users probabilistically offer minimal or no anonymity [10].

The development of smartphone technology has increased Internet usage from mobile devices which, worldwide, is estimated to surpass desktop access by 2014 [11]. Onion routing was originally conceived at the time of persistent wired Internet connections. However, when a device is used within a truly mobile context such as 'roaming', it may access the Internet from a combination of networks and/or service providers (e.g. cellular, Wi-Fi hot-spots). For example, at an average walking speed of 1.2 m/s, a hand-off may occur approximately every couple of minutes, potentially obtaining a different external IP address each time [12], even with the same provider such as a Wi-Fi hot-spot service [13].

In 2010, Orbot was released, which enables access to the Tor network from Android devices [14], with over 500,000 installations so far recorded [15]. According to the Tor project, running Orbot without any form of optimization "...is handling the mobile network environment very well...", but it is admitted that, "...this observation of 'very well', is just based on user experience, and not any detailed study of what exactly is happening" [16]. However, due to the current design of Tor, when an Orbot user is roaming, the connection to the Tor network will break at each hand-off due to a change of the user's external IP address, and therefore all existing circuits will be lost and require rebuilding (see Figure 1).

A limited amount of research has so far examined using anonymity networks, such as Tor, from a mobile device [17] [18], and although an important starting point, these studies have not assessed mobility in terms of roaming and the potential impact on performance to both the user and the

978-1-4577-1348-4/13/$31.00 ©2013 IEEE

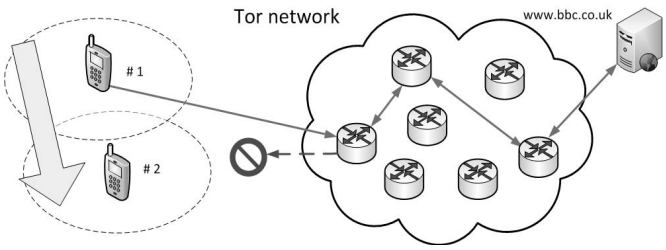

Fig. 1. A roaming mobile user breaking connection to the Tor network.

overall Tor network.

It is clear from the current use of Orbot that the Tor network can be successfully accessed from mobile devices. However, the results from our study provide an early assessment of the performance degradation that may occur when accessing Tor while roaming. The hypothesis that we considered is that an increase in the speed of a mobile user, or in the time taken to recover a user's connection to the Tor network, leads to an increase in download time and in data 'lost in flight'. Our results suggest that this is, indeed, the case and imply that the design of Tor may need some modification in order to support a growing mobile user base effectively.

II. Related Work

Two studies have previously examined the impact of mobility on anonymity networks, in both cases using Tor as a case study [17][18]. The researchers in [17] carried out an experiment to assess the performance of running Tor from a device connected to a cellular network ('standard' GPRS/GSM mobile phone). The experiment compared performance (timings for downloading files via the Tor network) from both wired and wireless Internet connections. As expected, performance from the faster wired connection was significantly higher and generally more consistent, than from the wireless connection. However, the experiment was based on the mobile device remaining stationary, and although the study provided an early indication of performance, more importantly it proved the feasibility of connecting to Tor from a mobile device, prior to the development of Orbot.

The researchers in [18] also assessed the impact of mobility on anonymity networks, such as Tor, but this time in the context of providing 'location privacy'. The research concluded, again prior to Orbot, that Tor "...does not support mobility...", suggesting that, "...adding mobility to a anonymity network means that location privacy is lost..."; when applying a relatively simple solution such as MobileIP. Three potential solutions were proposed in terms of supporting location privacy:

1) A MobileIP based approach, where a static 'home' Tor connection re-directs data-streams between the 'home' and 'care of' external IP addresses when the mobile device is roaming;
2) Changes made to the Tor network at the entry point (i.e. Entry Guard), to track a mobile user's change in external IP address, with supporting traffic management processes such as stop/resume control commands, to redirect data-streams as appropriate;
3) Changes at the exit point (i.e. Exit Router) from the Tor network; again providing the same stop/resume control commands based on the circuit identifier (i.e. CircuitID) between routers, rather than the user's external IP address.

In terms of findings, the researchers stated that the first solution, although providing effective mobility management, did not offer location privacy, as the 'care of' address is revealed. A further concern was the additional 'hops' required for maintaining the connection 'end-to-end', and whether this would significantly impact performance. The second solution again was deemed to afford mobility management, but concern was raised about location privacy, as the Entry Guard would have the ability to directly track the physical location of the mobile user. For the third and final proposed solution, the researchers suggested that it not only supported mobility but also maintained location privacy. As mobility is managed by the Exit Router, the mobile Tor user's location cannot be revealed by a 'care of' address or tracked by the Entry Guard.

The two previous studies were an important first step in understanding anonymity networks, such as Tor, in the context of mobility. However the impact on performance of mobility, especially while roaming, has not been examined, and with a potential increase in the mobile Tor user base, more research is required.

III. Method

At a high level, it is possible to estimate the potential impact to a roaming mobile user using Tor, based on two key variables: mobility speed and time to recover. For example, by applying an average speed against a set time-frame e.g. 1.2 metres per second (m/s) for 600 seconds (s), the total distance covered during the scenario would be 750 metres (m). The predicted number of hand-offs can then be simply derived by dividing the total distance covered by the mean range of the Wi-Fi networks. A 'time to recover' at each handoff, including the delay for re-establishing a connection to the physical network and rebuilding of Tor circuits, will generate the impact, as a percentage loss in overall availability. However, this approach will only calculate the interruption to service and not performance at an application level e.g. webpage downloads. Therefore, the potential impact of mobility with Tor was examined at a lower level, by undertaking an experiment, using a generic network simulator (OMNET++). A mobile device was simulated roaming across networks, at different mobility speeds while applying a range of Tor circuit build times, based on previous research findings [5][19]. The wireless access points were fixed at 75m apart and linear mobility used to ensure consistency of results for each run, to accurately compare the impact across different mobility speeds and range of recovery times. The key performance

TABLE I
KEY SIMULATION PARAMETERS

Parameter	Min	Range	Max
Speed	1.2 m/s	10 m/s	30 m/s
Circuit Build	0 s	to	30 s

metric was the average bit-rate (kbit/s) received by the mobile user, downloading an average sized web-page of 300KB [20], every 2 seconds over the time-frame of 600 seconds. The time-frame was chosen to reflect an existing design feature of Tor, where all closed and used circuits are refreshed approximately every 10 minutes. Based on previous work [21][22], artificial latency was also introduced, to try and reflect actual congestion on the Tor network, generating an overall time to complete of 11 seconds for each web-page request.

IV. RESULTS

The graph in Figure 2 shows the average bit-rate received over a time-frame of 600 seconds by mobile Tor user at rest (0 m/s), at average walking speed (1.2 m/s), at 'commute' speed (10 m/s), and finally at 'highway' speed (30 m/s), as used by researchers in [12]. The average bit-rate was also assessed for circuit build times, incremented at every second, between 0 (a theoretical baseline for not using Tor) and 30 seconds as the outer range of usability, with indicative markers of 3, 7, 15 to 20 seconds having been cited in previous research as timings for 'good', 'average' and 'slow' circuit rebuild times [6].

It is accepted that the introduction of mobility itself will inherently reduce performance, as the physical network hand-off will introduce an interruption in service of approximately one second. However, while using Tor, each break in the physical network connection will require the subsequent re-building of Tor circuits and this will increase substantially the impact on performance. At user mobility speeds above walking pace, i.e. commute and highway, the reduction in performance from the baseline was dramatic, at 85% and 97% respectively. Use of Tor is probably impractical in these circumstances. However, even at average walking speed, the impact to performance can still be significant, incurring a 66% reduction in average bit-rate at a 'good' circuit build time of 3 seconds, and approximately 77% for 'slow' circuit build times of 15 to 20 seconds. At 30 second circuit build times, the reduction was 91%, with impact similar to high mobility speeds.

In summary, the results show that, even at average walking speed with 'good' circuit build times, there is a significant reduction in the performance from Tor received by the mobile user. As per the hypothesis, an increase in user mobility speed and/or the time taken to recover the connection to the Tor network, significantly degrades performance to the mobile user. In some scenarios the impact is so substantial, that the use of Tor is considered impractical. As a final point, it was also observed that the break in connection by the mobile Tor user, generated on average a 3% to 4% of data left 'in-flight' within the simulated Tor network. This is also significant as

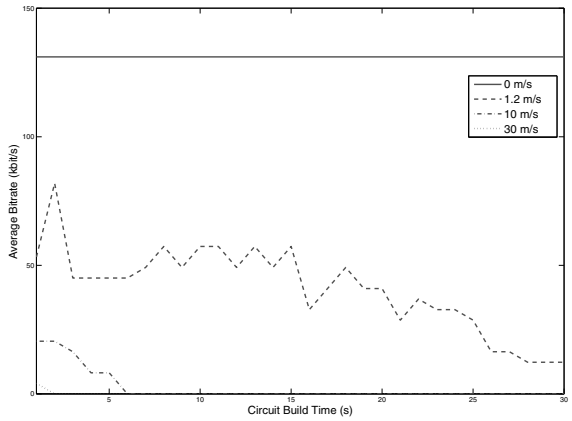

Fig. 2. Performance impact at different mobility speeds, with a range of Tor circuit build times. Please note the 0 m/s baseline is shown for illustrative purposes only, as in reality, no hand-offs and subsequent circuit builds should occur within the time-frame at 0 m/s.

'orphaned' data will create congestion at the Entry Guards, causing performance impact to the wider Tor network.

V. DISCUSSION

The results of our simulation support the hypothesis that an increase in user mobility speed, and/or the time taken to recover connection to the Tor network, will have a significant, detrimental effect on the performance received from Tor by a roaming mobile user.

This hypothesis is somewhat intuitive and it is appreciated that a more detailed analysis and improved experimental approach are desirable. First, the current lack of a tool that can support simulation both of a roaming mobile user and of the Tor network led to the final selection of a generic network simulator (OMNET++). However, OMNET++ was deemed suitable for this preliminary study, as the primary focus was to assess general performance impact at the 'outer edges' of the Tor network, rather than to emulate precisely the behaviour of Tor itself. Additionally, many of the simulation parameters remained static e.g. fixed network signal range, in order maintain a clear comparison across the key variables. However, it is clear that, in a real-world environment, mobile users do not walk constantly in straight lines at a fixed speed, nor do they receive data at a constant rate when their wireless signal strength is variable. These factors, amongst many, will affect the performance achieved. Finally, an inherent difficulty in carrying out an analysis of this type is that the actual effect on an individual Tor user will be a matter of speculation, unless the actual significance of 'lost' application data is known. Therefore, a 'good-put' metric often has to be accepted as a general assessment of impact. Even so, using this type of metric may not be suitable for all types of application. For example, an average bit rate may provide a suitable indication of performance in terms of light web-browsing, but may not be appropriate for Voice-over-IP (VoIP) where a high bit-rate may be irrelevant if there is a break in connection of 10 seconds

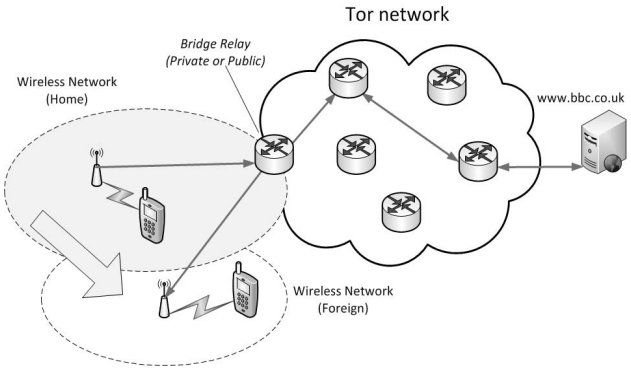

Fig. 3. The use of a Bridge Relay to provide a roaming mobile user a persistent connection to the Tor network.

every minute.

The accepted limitations of this preliminary study aside, the results have shown that the current design of Tor may not be best suited for mobile Tor users, especially when roaming, and suggests that attempting to provide 'persistence' into the design, for mobile Tor users, may require consideration.

Reflecting on the three solutions proposed in [18], it was stated that the second solution provided mobility management, but the researchers also raised a concern about location privacy, as the Entry Guard would be able to directly track the physical movements of the mobile Tor user. It was suggested by the researchers, that for the second solution to be viable, "the Tor entry node must be a trusted node. However, this is very unlikely to happen" [18]. But what if the entry point to the Tor network is explicitly trusted?

The proposal in Figure 3, builds upon this solution, where the entry point (Entry Guard) would provide persistence to the Tor network, for a roaming mobile user. However, in this new proposal, the entry point would be a 'trusted' Bridge Relay, either operated by the Tor user or an explicitly trusted third-party operator. After a break in, and subsequent re-establishment to a physical network connection, a command cell (i.e. resume) would be issued by the mobile user to their 'home' Bridge Relay. On receiving this resume command, the Bridge Relay would update the stored IP address for each of the existing circuit identifiers (i.e. CircuitID), and then resend the outstanding data-streams on to the user, alongside any new requests thereafter.

In order to consider further this potential solution, a number of key (and still open) questions need to be addressed: 1. Performance impact of using a Bridge Relay; 2. Impact on anonymity to the mobile Tor user; and 3. Impact on the wider Tor network.

The original aim of this study was to assess the potential performance impact of mobility on Tor. It became apparent from the early simulation results, that the provision of persistence to the Tor network, may be required to mitigate this impact. As a preliminary study, the proposed solution has yet to be fully evaluated from a performance perspective due to these open questions. However, the results shown in Figure 4 suggest that performance could fall at some point between that achieved by 'non-Tor / Mobile' and 'Tor / Static'. For example, as a Bridge Relay will be operating as the first hop within a circuit (i.e. replacing the Entry Guard), if it has a high available bandwidth, similar performance gains could be achieved as shown for using only a 2 hop circuit [8]. However, this may also be countered by the issues raised in [22], where congestion can be caused by an imbalance in available router bandwidth along a circuit, causing bottlenecks.

In terms of the potential impact on anonymity, as a starting point, it is worth considering the different types of Bridge Relay 'operation'. A 'Public' bridge is published through the bridge authority and the connection from the Bridge Relay into the Tor network (to the Middle router) will be shared. If a roaming mobile Tor user is also the operator of a Public Bridge, the user should appear no different to the rest of the Tor network. Based on the model previously used in [17], the anonymity achieved could be classified at some point between 'absolute privacy' and 'beyond suspicion'. However, if only two users were using the Bridge Relay at the same time and one is the operator, theoretically this should be classified lower, as 'probable innocence', but a defence of 'plausible denial-ability' may also be offered. The second example of operation is where the Bridge Relay is not published by the bridge authority, and therefore operates as a 'Private' bridge. A single Tor user using a high bandwidth and unshared Private Bridge, acting as the 'first hop' within the Tor network, may receive, although not necessarily, a gain in performance, as previously outlined. However, any potential performance gain, may be outweighed by the impact on anonymity, when using a Private bridge as the only Tor user. At best, this may only offer 'possible innocence', and at worst 'exposed' or 'provably exposed', depending on the attackers capabilities and duration of the traffic analysis [17]. A detailed assessment of the impact to anonymity, alongside the dynamic nature of the Bridge Relay usage, requires further work, and probably deserves a study in its own right.

Finally, what would happen if a significant subset of the current mobile Tor user base began operating a Bridge Relay as a home agent? This question has already been posed in [23], where it stated that "the current infrastructure can handle up to 10,000 bridges" but not a "massive 10-50 times increase in Public Bridges", the key issue being that there is currently only one bridge authority operated by the Tor network.

VI. Conclusions

It is apparent from the current use of Orbot, that the Tor network can be successfully accessed from mobile devices. However, based on the key findings from this preliminary study, there is some doubt as to whether Tor can support mobility effectively, for an increasing mobile user base.

The results show that the performance impact on a mobile Tor user is significant when roaming between different

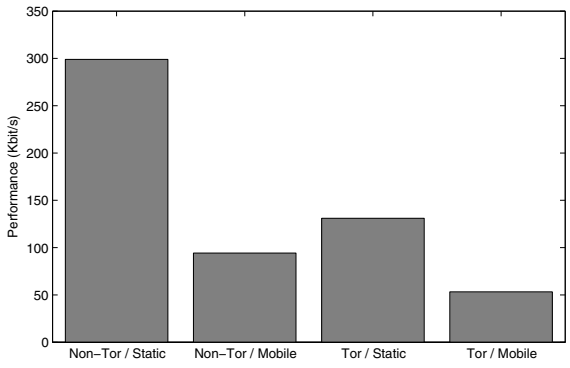

Fig. 4. A comparison of mean performance when downloading the web-page with / without Tor, in both a static and mobile context.

networks. In some scenarios, due to high mobility speeds and/or long circuit build times, impact was so significant that the use of Tor is no longer considered practical. In addition to any direct impact to the mobile user, data left 'in flight' from mobile users breaking connections, could also cause congestion and wider impact to the Tor network and subsequently other Tor users.

Tor, and other anonymity networks, may need to start reconsider their existing design, in order to support a larger mobile user base. A solution may require the provision of persistent connections to the anonymity network for mobile users, and an approach to mitigate the impact on performance of data lost 'in flight' when connections are broken. Clearly, any solution will be required to maintain the critical balance between anonymity and performance.

There are still a number of open questions concerning the proposed use of Bridge Relays to provide a persistent Tor connection for mobile devices, however it is hoped this preliminary study will generate further discussion and solutions for this research topic.

REFERENCES

[1] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," in *Proceedings of the 13th Usenix Security Symposium*, 2004.

[2] M. Reed, D. Goldschlag, and P. Syverson, "Anonymous connections and onion routing," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 482–494, May 1998.

[3] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, no. February, 1981.

[4] W. Diffie and M. Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on*, vol. 22, no. 6, pp. 644–654, 1976.

[5] R. Dingledine and S. J. Murdoch, "Performance improvements on Tor or, why Tor is slow and what we're going to do about it," The Tor Project, Tech. Rep. 2009-11-001, November 2009.

[6] R. Dingledine, "Tor Development Roadmap, 2008-2011," Tech. Rep., 2008.

[7] R. Snader and N. Borisov, "Improving Security and Performance in the Tor Network through Tunable Path Selection," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 5, pp. 728–741, Sep. 2011.

[8] K. Bauer, J. Juen, N. Borisov, D. Grunwald, D. Sicker, and D. McCoy, "On the optimal path length for Tor," *HotPets in conjunction with Tenth International Symposium on Privacy Enhancing Technologies (PETS 2010), Berlin, Germany*, 2010.

[9] N. Borisov, G. Danezis, P. Mittal, and P. Tabriz, "Denial of service or denial of security? How attacks on reliability can compromise anonymity," in *Proceedings of CCS 2007*, October 2007.

[10] C. Diaz, S. Seys, J. Claessens, and B. Preneel, "Towards measuring anonymity," *Designing Privacy Enhancing Technologies*, pp. 54–68, 2002.

[11] Microsoft, "The Growth of Mobile Marketing and Tagging," Website, 2013, https://tag.microsoft.com.

[12] B. Naeem, "Seamless Vertical Handover in WiFi and WiMAX Networks using RSS and Motion Detection: An Investigation." *akamaiuniversity.us*, vol. 12, no. 1, pp. 298–304, 2011.

[13] BT Group, "BT Wifi," Website, 2013, https://www.btwifi.co.uk/.

[14] The Guardian Project, "Orbot: Mobile Anonymity + Circumvention," Website, 2013, https://guardianproject.info/apps/orbot/.

[15] Google, "Orbot: Tor on Android," Website, 2013, https://play.google.com/store/apps/details?id=org.torproject.android.

[16] The Tor Project, "Tor," Website, 2013, https://www.torproject.org/.

[17] C. Andersson and A. Panchenko, "Practical anonymous communication on the mobile internet using Tor," *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops - SecureComm 2007*, pp. 39–48, 2007.

[18] R. Wiangsripanawan, W. Susilo, and R. Safavi-Naini, "Achieving mobility and anonymity in IP-based networks," in *Proceedings of the 6th international conference on Cryptology and network security*, ser. CANS'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 60–79.

[19] M. Perry, "Torflow: Tor network analysis," The Tor Project, Tech. Rep. 2009-08-003, August 2009. [Online]. Available: https://research.torproject.org/techreports/torflow-2009-08-07.pdf

[20] Ramachandran, S., "Web metrics: Size and number of resources." Website, 2012, https://code.google.com/speed/articles/web-metrics.html.

[21] R. Jansen, P. Syverson, and N. Hopper, "Throttling tor bandwidth parasites," *University of Minnesota-Computer Science and Engineering Technical Report 11*, vol. 19, 2011.

[22] M. AlSabah, K. Bauer, T. Elahi, and I. Goldberg, "The Path Less Travelled: Overcoming Tor Bottlenecks with Multipaths," 2011.

[23] K. Loesing, "What if the Tor network had 50,000 bridges," The Tor Project, Tech. Rep. 2012-03-001, March 2012. [Online]. Available: https://research.torproject.org/techreports/bridge-scaling-2012-03-09.pdf