continuously come from different IP addresses. On the other hand, a Meek user makes connections to addresses registered with the high level domain name used such as Google. Meek uses these addresses as long as the Meek user is still connected to the Tor network using the same domain. However, an FTE user makes multiple connections resulting in traffic looking like HTTP.

B. *Transferred data and the number of connections*

While analyzing the amount of data sent and received compared to the number of connections that the pluggable transport users make, we observed that the relationship between these two variables shows which type of pluggable transport is used by the user. For example, a non-Tor user establishes multiple connections to download a file when using BitTorrent. The number of connections is high and at the same time the amount of data transferred is relatively high, too. In contrast, when using the pluggable transport, especially for Flashproxy, the number of connections is high but the amount of data is low compared to BitTorrent.

C. *Duration*

When the Tor user configures the Tor browser to use one of the supported pluggable transports over his/her connection with the Tor network, the duration of the connection is relatively high compared to a non-Tor user who is browsing websites. Even though if the non-Tor user browses only one website for a long time, this time is much less than a Tor user who is browsing multiple websites. In this case, the duration of the browsing of multiple websites associated with the Tor user points to one connection. The connection duration in most pluggable transports distinguishes the Tor users even if the pluggable transport obfuscates the traffic to look like random strings or HTTP traffic.

VII. CONCLUSION

Tor pluggable transports with their different forms provide evasions or resistance to censorships. Obfsproxy is the framework used by these pluggable transports to obfuscate the user connection to the Tor network. This obfuscation mainly concentrates on hiding the contents that make the connections to the Tor network recognizable. Consequently, using deep packet inspection cannot detect them as Tor. Pluggable transports successfully obfuscated Tor traffic to look like random or different forms of traffic. At the same time, this success to hide the content is not for free. The obfuscation in the pluggable transports changes the content shape distinct from Tor and therefor creates a fingerprint for the obfuscated pluggable transports. The results in this work show that pluggable transports' flows have their own unique fingerprints which make them recognizable.

Future work will explore the usage of other Tor traffic traces as well as other data mining algorithms for studying the best practices for feature selection and training set formations.

ACKNOWLEDGMENT

This research is partially supported by the Natural Science and Engineering Research Council of Canada (NSERC) grant, and is conducted as part of the Dalhousie NIMS Lab at http://projects.cs.dal.ca/projectx/. The first author would like to thank the Ministry of Higher Education in Saudi Arabia for his scholarship.

REFERENCES

[1] Tor Bridges. [Online]. Available: https://www.torproject.org/docs/bridges.html.en

[2] Z. Ling, J. Luo, W. Yu, M. Yang, and X. Fu, "Extensive analysis and large-scale empirical evaluation of tor bridge discovery," in INFOCOM, 2012 Proceedings IEEE, 2012.

[3] Tor Pluggable Transports. [Online]. Available: https://www.torproject.org/docs/pluggable-transports.html.en

[4] E. Hjelmvik, and W. John, "Breaking and Improving Protocol Obfuscation". Department of Computer Science and Engineering, Chalmers University of Technology, Technical Report No. 2010-05, ISSN 1652-926X, 2010.

[5] G. La Mantia, D. Rossi, A. Finamore, M. Mellia, and M. Meo, " Stochastic Packet Inspection for TCP Traffic, " in 2010 IEEE International Conference on Communications. IEEE, May 2010, pp. 1-6.

[6] J. Barker, P. Hannay, and P. Szewczyk, "Using traffic analysis to identify the second generation onion Router," in the 9th IFIP International Conference on embedded and ubiquitous computing, Melbourne, AUS, 2011, pp.72-78.

[7] A. Houmansadr, C. Brubaker, and V. Shmatikov, "The parrot is dead: Observing unobservable network communications," in Proc. of IEEE S&P, 2013.

[8] T. Wilde. Great firewall Tor probing circa. [Online]. Available: https://gist.github.com/twilde/da3c7a9af01d74cd7de7

[9] P. Winter, and S. Lindskog, "How the great firewall of China is blocking Tor," in Proceedings of the 2nd USENIX Workshop on Free and Open Communications on the Internet , USENIX Association,2012.

[10] D. Fifield, N. Hardison, J. Ellithrope, E. Stark, R. Dingledine, D. Boneh, and P. Porras, "Evading Censorship with Browser-Based Proxies," In PETS, 2012.

[11] P. Winter, T. Pulls, and J. Fuss. "ScrambleSuit: A Polymorphic Network Protocol to Circumvent Censorship," In Workshop on Privacy in the Electronic Society, Berlin, Germany, 2013. ACM.

[12] K. Dyer, S. Coull, T. Ristenpart and T. Shrimpton, "Protocol Misidentication Made Easy with Format-Transforming Encryption," ACM SIGSAC Conference on Computer and Commu- nication Security, CCS'13, pp. 61-72, ACM, 2013.

[13] Obfsproxy. [Online]. Availabe: https://www.torproject.org/projects/obfsproxy.html.en

[14] Meek. [Online]. Available: https://trac.torproject.org/projects/tor/wiki/doc/meek

[15] Obfs3. [Online]. Available: https://gitweb.torproject.org/pluggable-transports/obfsproxy.git/tree/doc/obfs3/obfs3-protocol-spec.txt

[16] TRANALYZER2 [Online]. Available: http://tranalyzer.com/

[17] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. Witten,"The WEKA data mining software: an update," SIGKDD Explorations, vol. 11, no. 1, pp. 10-18, 20

[18] K. Shahbar, and A. N. Zincir-Heywood, "Benchmarking two techniques for Tor classification: Flow level and Circuit level classification,". in IEEE Symposium on Computational Intelligence in Cyber Security, 2014.