The Effect of Malicious Nodes on Tor Security

Maria Khan[*], Muhammad Saddique[*], Umar Pirzada[*], Muhammad Zohaib[*], Afzaal Ali[*], Bilal Wadud[*], Imran Ahmad[+]
[*]Cecos University of IT & Emerging Sciences, Peshawar, Pakistan, [+]UET Peshawar, Pakistan
Email: Icrg.csit@gmail.com

***Abstract*—Tor basically is designed as an overlay network for the Internet and its low latency anonymity environment is defending tens of thousands of users and protecting their privacy every day. The design had some deficiency on special nodes known as entry guards, the criteria needed to step in the anonymity network. This paper presents the effects of a number of malicious nodes on security and the compromised rate for Tor when considering all nodes as honest and introducing a very small malicious node of 100 Mbps/ 0.1 Gbps bandwidth, but relays nowadays are of much greater bandwidth and capacity. Second, if malicious nodes are more than one e.g., varied as (5 and 10) then the compromise rate diverges. In this paper, the compromise rate for high bandwidth malicious nodes and for more than one malicious node is experimented on the Tor network.**

Keywords—Tor; security; entry guard; malicious node, compromise rate

I. INTRODUCTION

Tor is an anonymous communication system and is designed as an overlay network on the Internet to anonymise the TCP (Transmission Control Protocol) streams. The mechanisms inside Tor are the basic principles of onion routers, which route Internet traffic on three relays or nodes known as entry, middle and exit in a communication network [1-2]. The users and network of Tor are growing day by day, Tor is approximately used in 76 countries with 6703 relays/nodes [3-4], to be anonymous and maintain online privacy for its users. Tor protocols and router selection criteria provide an open environment for users to select secure routers where data or information is kept confidential [5]. On the other hand, the high bandwidth properties advertised by the routers are an alarming scenario where an adversary has an upper hand to force or mitigate high risk. Malicious node is exchanged with non-malicious node, a client selects it and with no special privilege the adversaries leak user information and compromise the network. Router selection criteria in 2002; stated that relay or router selection is at random and uniform, to the extent that routers were un-compromisable. Nevertheless, in 2004, this parameter criterion for router selection was changed and preferences were on high bandwidth relays. Routers that provide specified threshold of higher bandwidth are to be selected more often than introduce the idea of Entry Guard relay. They are special helper nodes and maintained by OP in a guard list that guards for a period of 30-60 days, hence they fail to hold and repopulate to select in the guard list. Secondly, Tor Network was fading and failing in end-to-end user anonymity because of the threats and attacks such as (locating hidden services or traffic confirmation attack and predecessor attack); [4, 5]. Hence, the increase in the number of malicious nodes is at a risk of high compromised rate i.e., security is less for the Tor network. In this paper, the compromise rate of malicious bandwidth is higher than 0.1 Gbps is introduced and experiments on the number of malicious nodes exactly more than one e.g. varying the malicious node as 5 and 10 for the given advertised bandwidth (2.3 and 4.5 Gbps), that provide and identify a full proof view on the effect of security and compromise rate on Tor network.

The rest of the paper is organized as follows: in section 2, previous work is overviewed. In section 3, research questions are defined. In section 4, data and results of work are given. In section 5 experimentation on changing the number of nodes is provided; and in section 6, the paper concludes with future work.

II. RELATED WORK

Numerous works have been developed for the area of computer networks and anonymous communication [8-11]. Wright et al, [12-13], proposed an entry guard known as helper nodes to defend against the predecessor attack. He also proposed that in Tor network first relay of a path to be-fixed. Onion Routing network such as Tor, Overlier and Syverson [14], proposed entry guards for it. Bauer et al, [15], described that an attacker or adversary can replace a (non-malicious guard with a malicious guard) and risk abwide number of relays and destroy the network by launching Sybil attack through it. Borisov et al [16], describe a client that using a honest entry guard vs. a client using a malicious entry guards and the effect of the selective denial of service (DoS) attacks. Abbott et al, [17], described a browser-based attack on Tor where a malicious exit injects a signal generator to the user's traffic. A malicious entry guard is required to perform traffic analysis on its clients' circuits to identify if a circuit carries the injected signal. Adversaries that have limited sight on the network, Tor provides anonymity against these opponents. So the threshold setup by Tor authorities is control by the adversary they exchange non-malicious nodes with malicious nodes and target servers to get the guard and exit flag, this is usually done on identical circuit to compromise the user. To satisfy the open research questions proposed by Dingledine [18], regarding Tor entry guard and its design; Tariq et al, in his paper constructed a COGS framework and experimented it for the compromise rate to answer the specified research questions. He collected eight months data from (Apr, 2011 to Dec, 2011) Tor metrics website they took approx. 800 guards

but considered very small adversary i.e., 100 Mbps/0.1 Gbps to find out the compromise rate for Tor Network.

III. The Research Methodology

A. Problem Definition

The Tor network is developing and expanding day by day, for project success more volunteers are added and available in approx. 76 countries. Increase in network directly corresponds to increase in malicious node (adversary). The paper presents the idea of compromise rate for malicious bandwidth higher than 100 Mbps/0.1 Gbps which was previously proposed and experimented in COGS. Phenomenal experiments on the number of malicious nodes; i.e., considering the average advertised bandwidth of 2.3 Gbps for (5 and 10 nodes). Secondly, the present the fastest relay which advertises up to 4.5 Gbps bandwidth has fascinatingly proved the effects of security and compromise rate on Tor Network.

B. Significance of Work

The efforts and study on Tor nodes will impart provide the effect of malicious nodes and expound how high bandwidth relays risk the Tor anonymity by advertising a high bandwidth relay and introducing them in the network to deanonymize the users.

C. Proposed Work

Foremost in next section 4, the effect of high malicious node is greater than 100 Mbps or 0.1 Gbps and the overall compromise rate on the nodes or users of Tor network. Moving to section 5, finding the compromise rate by varying the number of malicious nodes at 2.5 and 4.5 Gbps bandwidth experimenting how it mitigates the Tor security.

IV. Data and Results

A. Data

The data of fig. 1 and fig. 2, is of eight months (from Sep, 2014 to Apr, 2015) for the advertised bandwidth and n-quickest relay collected from Tor metrics website [19-20], through these figures a direct view inside the network is available. The graphical data tables and graphs are generated to study the effect of different nodes and high bandwidth relays that reveal if there is more than one malicious node, what is the compromised rate that lowers the security of Tor network. As the graph confers, the advertised data of eight months:

TABLE I.
COMPROMISE RATE FOR NODES (0.1, 2.3, AND 4.5) W.R.T TO ADVERTISED BANDWIDTH

Month	Advertised B.W (Gbps)	*C.R for 0.1*	*C.R for 2.3*	*C.R for 4.5*
Sep	97	0.00103	0.02370	0.04639
Oct	100	0.00100	0.02300	0.04500
Nov	108	0.00092	0.02120	0.04160
Dec	107	0.00093	0.02140	0.04200
Jan	110	0.00090	0.02090	0.04090
Feb	120	0.00083	0.01910	0.03750
Mar	139	0.00071	0.01650	0.03237
Apr	122	0.00081	0.01880	0.03688

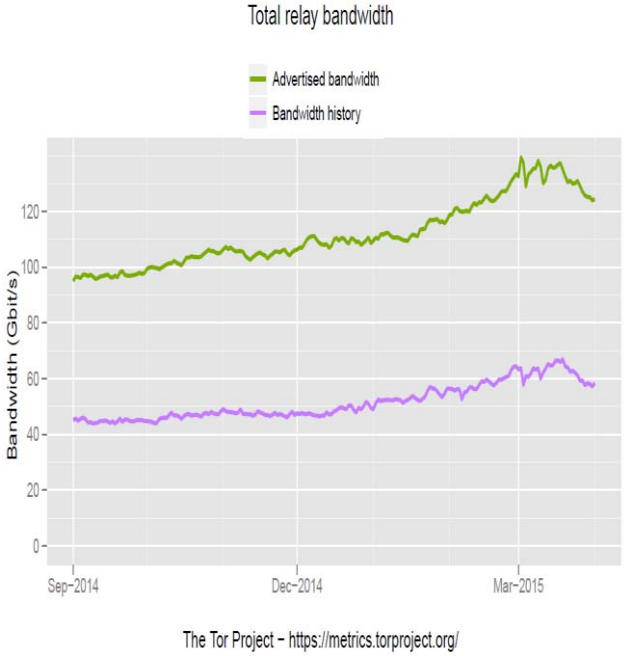

Fig. 1 The advertised bandwidth for the Tor relays.

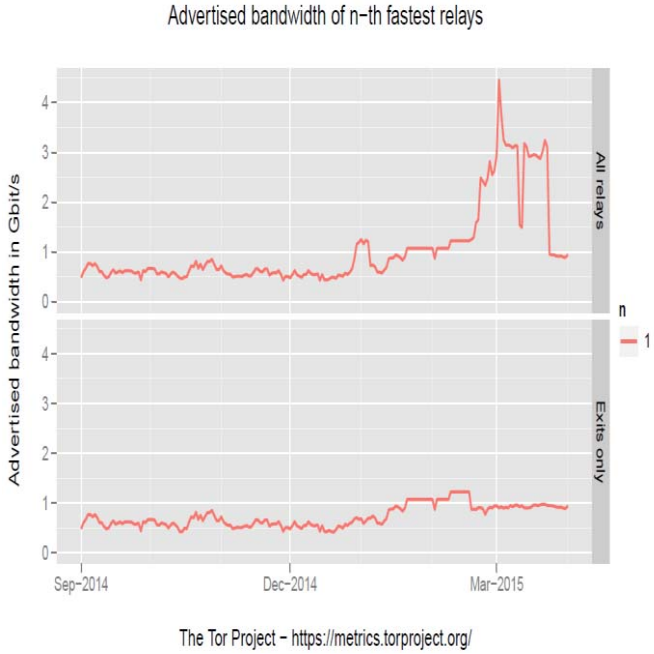

Fig. 2 The advertised fastest relay - i.e., 4.5 Gbps.

B. Results

Table 1 and fig. 3 suggest that the compromise rate for C.R 0.1, i.e. the malicious node bandwidth Tariq et al; paper [21], his experiments are tested on 0.1 Gbps criteria but as discussed above that is a very small adversary in percentage of advertise bandwidth and volunteer relays. C.R 2.3 Gbps is the malicious bandwidth, which is the average of 0.1 Gbps and 4.5

Gbps malicious B.W. As C.R 4.5 Gbps is the peak bandwidth of the relay, taken from Tor metrics website in figure 2. A great increase in compromise rate is produced when A.B.W is kept constant and varying the malicious nodes which results in an increase in the compromise rate. As for the compromise rate of malicious B.W, 0.1 Gbps there is a 1.961 times increase, when changing the malicious B.W to 2.3 Gbps there is 23.239 times increase in C.R, repeating the same process for 4.5 Gbps there is 45.591 times increase of compromise rate for the course of 8 months.

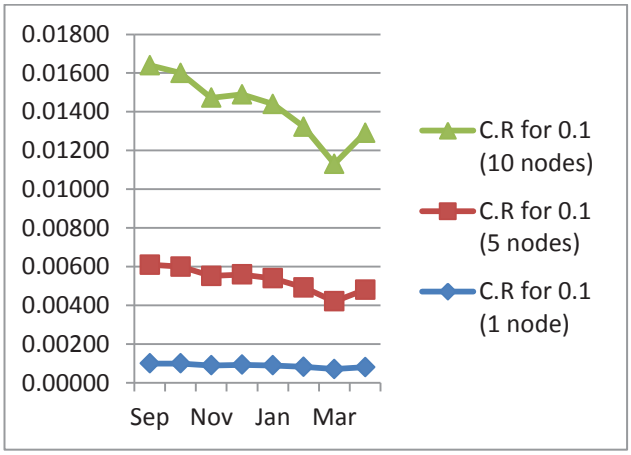

Fig. 3 Compromise rate for node 0.1 vs. compromise rate for nodes (2.3 and 4.5.

V. Experimentation on Changing Number of Nodes

Table 2 and fig. 4 show, the compromise rate from Sep. 2014 to Apr. 2015 here 0.1 Gbps of single malicious nodes are checked on (5 and 10 malicious nodes). The range is from 97 to 139 where for 5 nodes there is an increase of 5.1 times from 0.1 (1 node) of compromise rate and for 10 nodes there is an increase of 10.3 times from 0.1 (1 node) of compromise rate.

TABLE II.
INCREASING NUMBER OF NODES FOR 0.1 Gbps

Month	Advertise B.W (Gbps)	C.R for 0.1 (1 node)	C.R for 0.1 (5 nodes)	C.R for 0.1 (10 nodes)
Sep	97	0.00100	0.00510	0.01030
Oct	100	0.00100	0.00500	0.01000
Nov	108	0.00090	0.00462	0.00920
Dec	107	0.00093	0.00467	0.00930
Jan	110	0.00090	0.00450	0.00900
Feb	120	0.00083	0.00410	0.00830
Mar	139	0.00071	0.00350	0.00710
Apr	122	0.00081	0.00400	0.00810

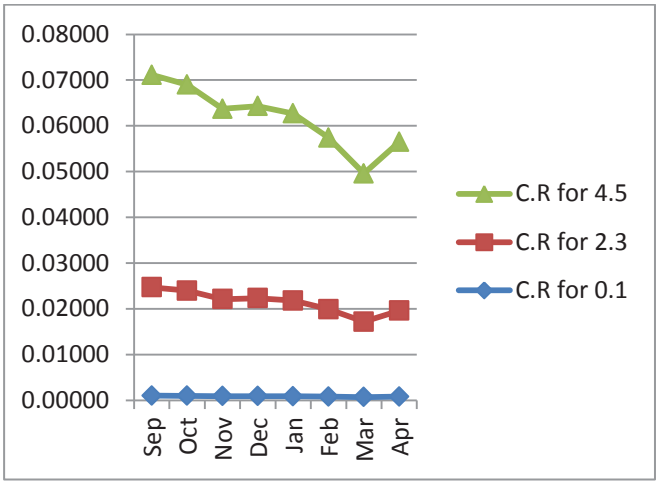

Fig. 4 output compromise rate for 0.1 Gbps on (1, 5, and 10) nodes.

Table 3 and fig. 5 give, the compromise rate from Sep. 2014 to Apr. 2015 here 2.3 Gbps of single malicious nodes are checked on (5 and 10 malicious nodes).The range is from 97 to 139 where for 5 nodes there is an increase of 4.97 times from 2.3 (1 node) of compromise rate and for 10 nodes there is an increase of 10.00 times from 2.3 (1 node) of the compromise rate.

TABLE III.
INCREASING NUMBER OF NODES FOR 2.3 Gbps

Month	Advertise B.W	C.R for 2.3 (1 node)	C.R for 2.3 (5 nodes)	C.R for 2.3 (10 nodes)
Sep	97	0.02370	0.11800	0.23710
Oct	100	0.02300	0.11500	0.23000
Nov	108	0.02120	0.10600	0.21290
Dec	107	0.02140	0.10700	0.21490
Jan	110	0.02090	0.10400	0.20900
Feb	120	0.01910	0.09500	0.19160
Mar	139	0.01650	0.08270	0.16540
Apr	122	0.01880	0.09400	0.18850

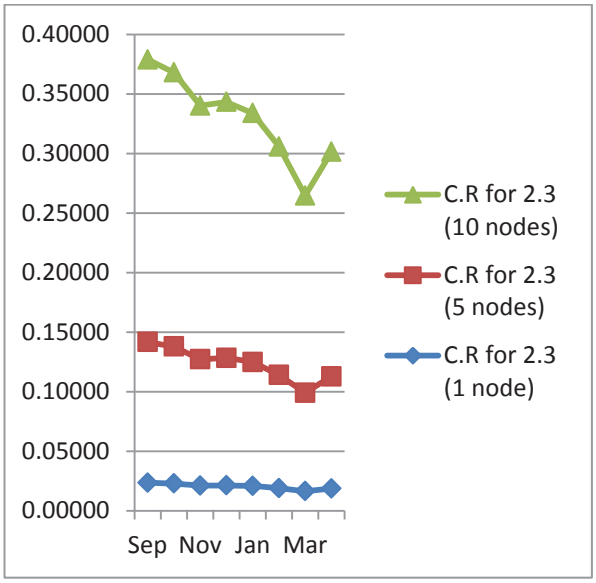

Fig. 5 Output compromise rate for 2.3 Gbps on (1, 5, and 10) nodes.

Table 4 and fig. 6 present, the compromise rate from Sep. 2014 to Apr. 2015, here 4.5 Gbps of single malicious nodes are checked on (5 and 10 malicious nodes). The range is from 97 to 139 where for 5 nodes there is an increase of 4.99 times from 4.5 (1 node) of compromise rate and for 10 nodes there is an increase of 10 times from 4.5 (1 node) of compromise rate. Finally, looking at 0.1 for 1 malicious node there is an increase in compromise rate of 5.1 times for 5 nodes (0.1 Gbps) and 10.3 times for 10 nodes (0.1 Gbps), 0.1 for 1 malicious node there is an increase in compromise rate of 23.7 times for 1 node (2.3 Gbps) and 46.39 times for 1 node (4.5 Gbps), then 0.1 for 1 malicious node there is an increase of 118 times for 5 nodes (2.3 Gbps) and 231.9 times for 5 node (4.5 Gbps), then 0.1 for 1 malicious node there is an increase of 237.1 times for 10 nodes (2.3 Gbps) and 463.9 times for 10 nodes (4.5 Gbps).

TABLE IV.
INCREASING NUMBER OF NODES FOR 4.5 Gbps

Month	Advertise B.W	C.R for 4.5 (1 node)	C.R for 4.5 (5 nodes)	C.R for 4.5 (10 nodes)
Sep	97	0.04639	0.23190	0.46390
Oct	100	0.04500	0.22500	0.45000
Nov	108	0.04160	0.20800	0.41660
Dec	107	0.04200	0.21000	0.42050
Jan	110	0.04090	0.20400	0.40900
Feb	120	0.03750	0.18700	0.37500
Mar	139	0.03237	0.16100	0.32370
Apr	122	0.03688	0.18400	0.36880

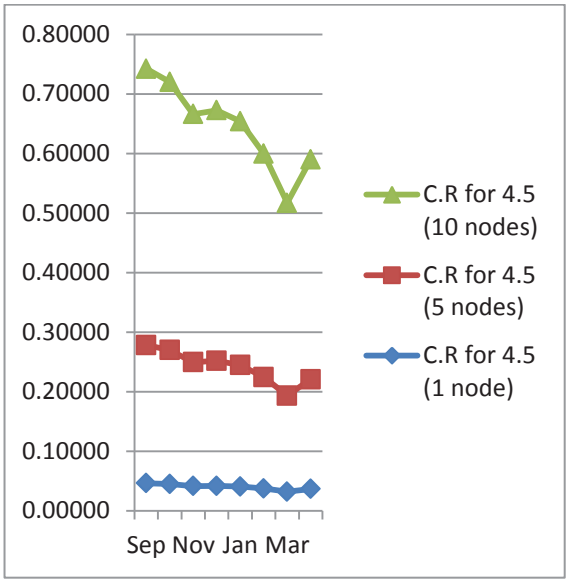

Fig. 6 Output compromise rate for 4.5 Gbps on (1, 5, and 10) nodes.

VI. Conclusions

In this paper, the compromise rate for Tor-an anonymous communication system is introduced as previously mentioned in COGS, they discussed a very small 100 Mbps/0.1 Gbps malicious node and experimented it for a single malicious node. Presently, Tor is used in approximately 75 countries to the extent that the number of malicious nodes has massively increased and advertised bandwidth of volunteer relays are offering a threshold up to 4.5 Gbps bandwidth. It clearly transforms and shows an increase of 463.9 times compromise rate as compared with the compromised rate in case of 0.1 Gbps bandwidth which identified that Tor needs some changes in its protocols and guard selection criteria. It's a threat to the network and the anonymity of the user gets compromised. The relay selection criteria, for user-level programs are updated to fair/balance the security and performance. Entry guard selection criteria and parameters are theoretically experimented; teams are assigned to inspect guard list to lower adversaries that compromise the network.

References

[1] T. Elahi, K. Bauer, M. Al Sabah, R. Dingledine and I. Goldberg, "Changing of the Guards: A Framework for Understanding and Improving Entry Guard Selection in Tor", in proceedings of the 2012 *ACM workshop* on Privacy in the electronic society, NY, USA 2012, pp. 43-54.

[2] R. Dingledine, N. Mathewson and P. Syverson, "Tor: the second-generation onion router", in Proceedings of the 13th conference on *USENIX Security Symposium* - Volume 13, USENIX Association, 2004, pp. 21–21.

[3] https://metrics.torproject.org/bubbles.html#country, retrieved on September 1, 2015.

[4] R. A. Haraty and B. Zantout, "The TOR Data Communication System", Journal of Communications and Networks. ISSN 1229-2370. Volume 16, pp. 415-420, August 2014.

[5] R. A. Haraty and B. Zantout, "The TOR Data Communication System – A Survey," Proceedings of the Sixth IEEE International Workshop on Performance Evaluation of Communications in Distributed Systems

and Web based Service Architectures (PEDISWESA'2014). Madeira, Portugal. June 2014.

[6] L. Overlier and P. Syverson, "Locating Hidden Servers", in Symposium on Security and Privacy (2006), IEEE, pp. 100–114.

[7] M. Wright, M. Adler, B. Levine and C. Shields, "The predecessor attack: An analysis of a threat to anonymous communications systems", in ACM Transactions on Information and System Security (TISSEC) 7, 4 (2004), pp. 489–522.

[8] R. A. Haraty and B. Zantout, "A Collaborative-based approach to Avoiding Traffic Analysis and Assuring Data Integrity in Anonymous Systems", Computers in Human Behavior Journal. 2014.

[9] B. Zantout and R. A. Haraty, "A Comparative Study between BitTorrent and NetCamo Data Communication Systems," International Journal of Computational Intelligence and Information Security. March 2010. Volume 1, Number 2, 2010.

[10] B. Zantout and R. A. Haraty, "I2P Data Communication System," Proceedings of the Tenth International Conference on Networks (ICN 2011). St. Maarten, The Netherlands Antilles. January 2011.

[11] Badieh Trabousli and Ramzi A. Haraty. *MANET with Q-Routing Protocol*. Proceedings of the Eleventh International Conference on Networks (ICN 2012). Reunion Island, France. February 2012.

[12] M. Wright, M. Adler, B. Levine and C. Shields, "Defending Anonymous Communications against Passive Logging Attacks", in Proceedings of the IEEE Symposium on Security and Privacy (2003), pp. 28–41.

[13] M. Wright, M. Adler, B. Levine and C. Shields, "The predecessor attack: An analysis of a threat to anonymous communications systems", in ACM Transactions on Information and System Security (TISSEC) 7, 4 (2004), pp. 489–522.

[14] L. Overlier and P. Syverson, "Locating Hidden Servers", in Symposium on Security and Privacy (2006), IEEE, pp. 100–114.

[15] K. Bauer, D. McCoy, D. Grunwald, T. Kohno and D. Sicker, "Low-Resource Routing Attacks against Tor", in Proceedings of the Workshop on Privacy in the Electronic Society on October 2007, pp. 11–20.

[16] N. Borisov, G. Danezis, P. Mittal and P. Tabriz, "Denial of service or denial of security?", in Proceedings of the 14th ACM conference on Computer and communications security New York, NY, USA, 2007, CCS '07, ACM, pp. 92–102.

[17] T. Abbott, K. Lai, M. Lieberman and E. Price, "Browser-based Attacks on Tor", in Proceedings of the 7th International Conference on Privacy Enhancing Technologies Berlin, Heidelberg, 2007, Springer-Verlag, pp. 184–199.

[18] https://blog.torproject.org/category/tags/entry-guards, Retrieved on September 17, 2015.

[19] https://metrics.torproject.org/advbwdist-relay.html, Retrieved on September 17, 2015.

[20] https://metrics.torproject.org/bandwidth.html, Retrieved on September 17, 2015.

[21] T. Elahi, K. Bauer, M. Al-Sabah, R. Dingledine and I. Goldberg, "Changing of the Guards: A Framework for Understanding and Improving Entry Guard Selection in Tor", in proceedings of the 2012 ACM workshop on Privacy in the electronic society, NY, USA 2012, pp. 43-54.