

Technology of Load Balancing in Anonymous Network Based on Proxy Nodes Cascade Platform

Tkachov Vitalii
Hunko Mykhailo
Bondarenko Maksym
Artyomov Serhii

Kharkiv National University of Radio Electronics, 14 Nauky Ave,
Kharkiv UA-61166, Ukraine,
tkachov@ieee.org,
hunko@ieee.org,
bondarenko@ieee.org

Abstract. The work is devoted to the development of a technology for balancing network traffic between proxy nodes in a cascade scheme. The technology developed involves substituting proxy nodes in case of restricted node overload. The technology improves the fault-tolerance indicator of anonymous network.

Keywords: anonymous network, proxy, traffic balancing, computer engineering.

I. INTRODUCTION

One of the ways to organize the protection of personal information on the Internet is to use anonymous networks [1]. There are a very large number of anonymous networking technologies. One of such technologies is to use a cascade of proxy servers [1, 2]. A classic example of the given technology is the hybrid anonymous Psiphon network. The specifics of its work is that it uses a unique web address, login and password to connect to a proxy server without making any changes to the browser settings. However, this procedure can only be performed by proxies since the proxy administrator has documented information about the user's activity. The user can connect to any point on such a network and, according to the network settings, must pass a certain number of proxy nodes, which anonymizes its traffic.

The problem that arises at the stage of organizing a traffic route is the overloading of individual nodes. This most frequently happens when such an anonymous network uses the existing overlay infrastructure with geo-location of the client by its IP address [3] (including the one dynamically reconfigured with high-mobility nodes [5]). The nodes go into denial of service status or the quality of access decreases significantly. Mirroring of requests to other nodes can reduce traffic anonymity.

Thus, there is an urgent task of developing a balancing technology for network traffic in an anonymous network based on the proxy nodes cascade platform by even distribution of requests.

II. PROBLEM SOLUTION AND RESULTS

The developing technology is based on the use of a restricted proxy class. These are the proxies, the properties of which depend on their use. Limited proxies have capabilities similar to the cascading mechanism of executing operations, the members of which do not trust each other. The essence of technology is that requests for overloaded (but functioning) proxy nodes are redirected into the depth of the anonymous network. The proxy nodes that are less loaded become restricted ones for the requests. This technology is fair for an

anonymous network where all proxy nodes are equivalent. Thus, when passing through the proxy node that follows after the first one, i.e. the intermediate proxy node, the standard restrictions are applied to the traffic. They are added by approving a new proxy node with the original key. This technology is also fair to anonymous networks that implement only the delegated proxies where cascading authorization uses only the certificates of the original proxy node. Since the intermediate proxy node is explicitly identified in the original proxy node, it also provides such function of the proxy node, allowing it to act as an intermediate node in order to execute the initial proxy node.

Experimental studies of the given technology were carried out on the basis of the "Reconfigured and Mobile Systems Laboratory" at the Department of Electronic Computers, NURE, and showed that the failure rate of the anonymous network on the platform of the proxy nodes cascade decreased by 15%.

III. CONCLUSIONS

The technology of load balancing in the anonymous network built on the platform of proxy cascades has been considered in the work. The balancing scheme is based on the mechanism of request forwarding between nodes. The results show that the strategy of using the restricted proxy nodes with up-to-date information on the node load gives the least delay in determining the node for receiving traffic from a user.

REFERENCES

- [1] Ткачов В.М. Дослідження надійності анонімної мережі на основі каскадної технології прокусування / В.М. Ткачов, Д.С. Мітін, В.С. Володка // *Дев'ята міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління»*. – Баку-Харків-Жиліна. – 11-12 квітня 2019 р. – С. 40.
- [2] Zhang Y., Li J., Chen X., & Li H. Anonymous attribute-based proxy re-encryption for access control in cloud computing. *Security and Communication Networks*, 9(14), pp. 2397-2411.
- [3] Tkachov V., Bondarenko M., Ulyanov O. and Reznichenko O. Overlay Network Infrastructure for Remote Control of Radio Astronomy Observatory, 2019 *IEEE International Conference on Advanced Trends in Information Theory (ATIT)*, Kyiv, Ukraine, 2019, pp. 161-165.
- [4] Churyumov G. Method for Ensuring Survivability of Flying Ad-hoc Network Based on Structural and Functional Reconfiguration / Genadiy Churyumov, Vitalii Tkachov, Volodymyr Tokariev, Vladyslav Diachenko // *Selected Papers of the XVIII International Scientific and Practical Conference "Information Technologies and Security" (ITS 2018)* / Kyiv, Ukraine, November 27, 2018. – Pp. 64-76.