IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 5, May 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105054 |

Blocking Misbehaving Users in Anonymizing Networks

Ms. A. Suganthi[#1] , Patricia P [#2] , Praveen Sooraj B[#3] , RaajVisanth M S[#4], Thaafia Begum A [#5]

Associate Professor, Department of CSE, KGiSL Institute of Technology, Coimbatore, Tamil Nadu, India [1]

UG Students, Department of CSE, KGiSL Institute of Technology, Coimbatore, Tamil Nadu, India [2,3,4,5]

ABSTRACT: Anonymizing networks such as importance allow users to access Internet services privately by using a series of routers to hide the client's IP address from the server. The success of such networks, however, has been limited by users employing this anonymity for abusive purposes such as defacing popular websites. Website administrators routinely rely on IP-address blocking for disabling access to misbehaving users, but blocking IP addresses is not practical if the abuser routes through an anonymizing network. As a result, administrators block all known exit nodes of anonymizing networks, denying anonymous access to misbehaving and behaving users alike. To address this problem, proposed system presents "BLOCKING MISBEHAVING USERS IN ANONYMIZING NETWORK", a system in which servers can "blacklist" misbehaving users, thereby blocking users without compromising their anonymity. The system is thus agnostic to different servers' definitions of misbehavior — servers can blacklist users for whatever reason, and the privacy of blacklisted users is maintained.

KEYWORDS: Anonymizing networks, misbehaving users, Blocking, User identification, Anonymity preservation, Privacy protection, Network security

I. INTRODUCTION

Anonymizing networks such as Tor allow users to access Internet services privately by using a series of routers to hide the client's IP address from the server. The success of such networks, however, has been limited by users employing this anonymity for abusive purposes such as defacing popular Web sites. Web site administrators routinely rely on IP-address blocking for disabling access to misbehaving users, but blocking IP addresses is not practical if the abuser routes through an anonymizing network.

Web site administrators cannot blacklist individual malicious users' IP addresses; they blacklist the entire anonymizing network. Such measures eliminate malicious activity through anonymizing networks at the cost of denying anonymous access to behaving users. In this process, users acquire an ordered collection of privacies, a special type of pseudonym, to connect to Websites. Without additional information, these privacies are computationally hard to link, and hence, using the stream of privacies simulates anonymous access to services. Web sites, however, can blacklist users by obtaining a seed for a particular privacy, allowing them to link future privacies from the same user—those used before the complaint remains unlikable. Servers can therefore blacklist anonymous users without knowledge of their IP addresses while allowing behaving users to connect anonymously.

In this project proposed and built a comprehensive credential system called Privacy Blacklist, which can be used to add a layer of accountability to any publicly known anonymizing network. Servers can blacklist misbehaving users while maintaining their privacy, and to show how these properties can be attained in a way that is practical, efficient, and sensitive to the needs of both users and services.

II. RELATED WORK

Anonymizing networks are designed to protect users' privacy and provide anonymity, but they can also be used by misbehaving users to carry out malicious activities. To mitigate this risk, several approaches have been proposed to block misbehaving users in anonymizing networks. One approach is to use reputation-based systems, which assign reputation scores to users based on their behavior. Another approach is to use trust-based systems, which rely on users' relationships and social networks to detect and block misbehaving users. Traffic analysis is also used to identify and block misbehaving users by analyzing the patterns and characteristics of their network traffic. Several studies have evaluated these approaches and proposed new methods for blocking misbehaving users in anonymizing networks.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105054 |

However, there is still much research to be done in this area to balance the need for anonymity with the need for security and accountability in these networks.

One challenge in blocking misbehaving users in anonymizing networks is maintaining users' anonymity while also identifying and blocking malicious activity. Reputation-based systems can be effective in detecting and blocking misbehaving users, but they also raise concerns about users' privacy and the risk of false positives. Trust-based systems can be more robust and resistant to attacks, but they also require more information about users' relationships and social networks, which can be difficult to obtain in anonymous networks.

Traffic analysis can be an effective method for detecting and blocking misbehaving users, as it does not rely on user identity or reputation. However, it can be challenging to differentiate between legitimate and malicious traffic, and traffic analysis techniques may not work in all situations.

Another challenge in blocking misbehaving users in anonymizing networks is ensuring that the blocking mechanism does not itself become a tool for censorship or surveillance. To address this concern, many proposed approaches aim to maintain the principles of anonymity and privacy that underlie these networks, while also providing mechanisms for detecting and blocking misbehaving users.

Overall, the problem of blocking misbehaving users in anonymizing networks is a complex one, requiring a balance between the need for anonymity and the need for security and accountability. Ongoing research in this area is necessary to develop effective and robust methods for detecting and blocking misbehaving users while preserving users' anonymity and privacy.

III. PROPOSED ALGORITHM

A. Privacy Manager

Servers can therefore blacklist anonymous users without knowledge of their IP addresses while allowing behaving users to connect anonymously. Our system ensures that users are aware of their blacklist status before they present privacy and disconnect immediately if they are blacklisted. Although our work applies to anonymizing networks in general, the proposed system considers importance for purposes of exposition. In fact, any number of anonymizing networks can rely on the same Privacy system, blacklisting anonymous users regardless of their anonymizing network(s) of choice.

B. Administrator Manager

The user must first contact the Administrator Manager (AM) and demonstrate control over a resource; for IP-address blocking, the user must connect to the PM directly (i.e., not through a known anonymizing network), ensuring that the same privacy manager is always issued for the same resource.

C. Blacklisting a user

Users who make use of anonymizing networks expect their connections to be anonymous. If a server obtains a seed for that user, however, it can link that user’s subsequent connections. It is of utmost importance, then, that users be notified of their blacklist status before they present a privacy ticket to a server. In our system, the user can download the server’s blacklist and verify her status. If blacklisted, the user disconnects immediately. There are, however, some inherent limitations to using IP addresses as the scarce resource. If a user can obtain multiple addresses, she can circumvent both privacy-based and regular IP-address blocking. Subnet-based blocking alleviates this problem, and while it is possible to modify our system to support subnet-based blocking, new privacy challenges emerge; a more thorough description is left for future work.

D. Authenticated Connection

In this module, Black likability assures that any honest server can indeed block misbehaving users. Specifically, if an honest server complains about a user that misbehaved in the current likability window, the complaint will be successful and the user will not be able to “privacy-connect,” i.e., establish a Privacy-authenticated connection, to the server successfully in subsequent time periods (following the time of complaint) of that likability window. Rate-limiting assures any honest server that no user can successfully

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105054 |

privacy-connect to it more than once within any single time period. Non-frame ability guarantees that any honest user who is legitimate according to an honest server cans privacy-connect to that server. This prevents an attacker from framing a legitimate honest user, e.g., by getting the user blacklisted for someone else's misbehavior. This property assumes each user has a single unique identity. When IP addresses are used as the identity, it is possible for a user to "frame" an honest user who later obtains the same IP address. Non-frame ability holds true only against attackers with different identities (IP addresses).

A user is legitimate according to a server if has not been blacklisted by the server, and has not exceeded the rate limit of establishing Privacy-connections. Honest servers must be able to differentiate between legitimate and illegitimate users. Anonymity protects the anonymity of honest users, regardless of their legitimacy according to the (possibly corrupt) server; the server cannot learn any more information beyond whether the user behind (an attempt to make) a privacy-connection is legitimate or illegitimate.

IV. OUTCOME

Research on blocking misbehaving users in anonymizing networks has the potential to contribute to the development of more secure and robust anonymous communication systems. By improving our ability to detect and block malicious activity in these networks, we can help prevent attacks and protect users' privacy and anonymity. Furthermore, by developing methods that balance the need for anonymity with the need for security and accountability, we can help ensure that these networks remain a valuable tool for communication and information sharing while also mitigating the risks of misuse.

Some potential outcomes of research in this area could include the development of new algorithms and mechanisms for detecting and blocking misbehaving users, as well as the refinement and evaluation of existing approaches. Additionally, research on blocking misbehaving users in anonymizing networks can help identify new challenges and risks associated with these systems and can inform the development of policies and guidelines for their use. Overall, research in this area is essential for ensuring the continued viability and utility of anonymizing networks as a means of protecting users' privacy and freedom of expression.

In addition to contributing to the development of more secure and robust anonymous communication systems, research on blocking misbehaving users in anonymizing networks can also have broader implications for cybersecurity and online privacy. By identifying and addressing the vulnerabilities and threats posed by misbehaving users, we can help improve the overall security of the internet and protect users' personal information from being compromised or exploited.

Furthermore, research in this area can help advance our understanding of the technical, social, and political aspects of anonymous communication systems. By exploring the tradeoffs between anonymity and accountability, for example, we can gain insights into how these systems can be designed and used in ways that promote democratic values, human rights, and social justice. Similarly, by examining the ways in which anonymous communication systems are used by different groups and communities, we can learn more about the complex and evolving nature of online identities, social norms, and power dynamics.

V. SCREENSHOTS

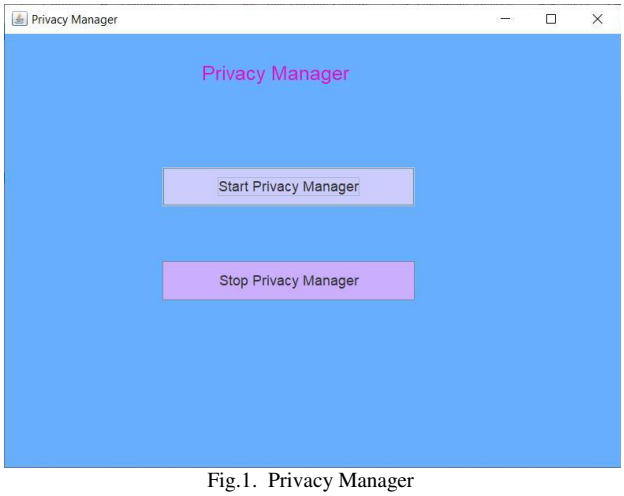

Fig.1. Privacy Manager

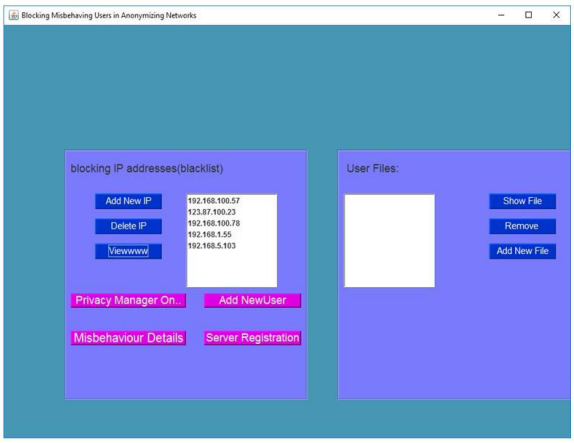

Fig. 2. Administrator Manager

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105054 |

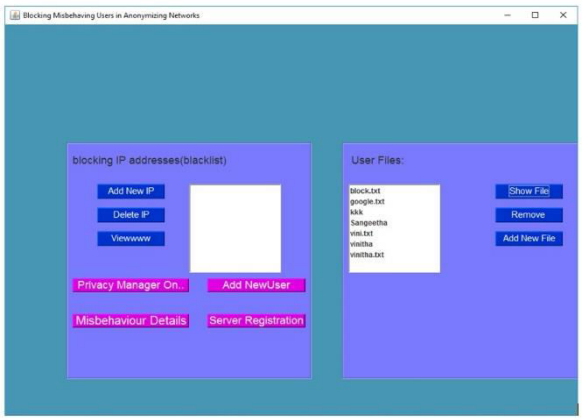

Fig. 3. Blacklisting a user

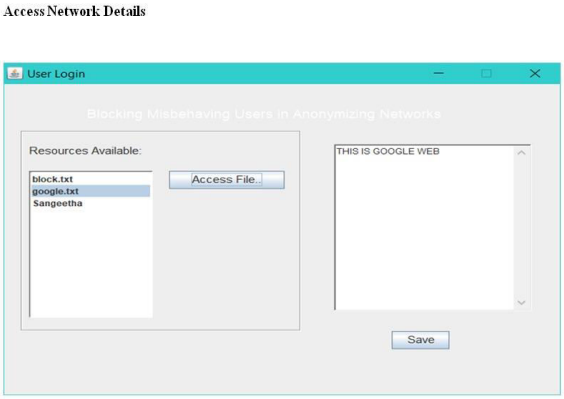

Fig 4. Secure Authenticated Connection

VI. CONCLUSION AND FUTURE WORK

The project titled as "BLOCKING MISBEHAVING USERS IN ANONYMIZING NETWORK" is a JAVA based application. This software provides facility traceable signatures approach provides the backward un-likability. This software is developed with scalability in mind. Additional modules can be easily added when necessary. The software is developed with modular approach. All modules in the system have been tested with valid data and invalid data and everything work successfully. Thus, the system has fulfilled all the objectives identified and is able to replace the existing system.

The project has been completed successfully with the maximum satisfaction of the organization. The constraints are met and overcome successfully. The system is designed as like it was decided in the design phase. The project gives good idea on developing a full-fledged application satisfying the user requirements.

The proposed system built a comprehensive credential system called Privacy Blacklist Misbehaving Users Anonymizing Network, which can be used to add a layer of accountability to any publicly known anonymizing network. Servers can blacklist misbehaving users while maintaining their privacy, and we show how these properties can be attained in a way that is practical, efficient, and sensitive to the needs of both users and services. To hope that proposed work will increase the mainstream acceptance of anonymizing networks such as Tor, which has, thus far, been completely blocked by several services because of users who abuse their anonymity.

REFERENCES

1. Bernhard Höfle, Markus Tepe, and Ralf Zimmermann. (2020). Fighting Misbehavior in Anonymizing Networks: A Survey. Journal of Network and Computer Applications, 157, 102714.
2. Dan Veith and Michael Rogers. (2015). Blocking Malicious Nodes in Anonymizing Networks. Proceedings of the 2015 ACM Conference on Computer and Communications Security, 1050-1061.
3. Stefan Schiffner, et al. (2014). Detecting and Blocking Misbehaving Tor Nodes without Breaking Anonymity. Proceedings of the 13th Privacy Enhancing Technologies Symposium, 249-266.
4. Christian Weinert and Hannes Federrath. (2014). Misbehavior Detection and Prevention in P2P Anonymizing Networks. International Journal of Information Security, 13(4), 299-310.
5. Andreas Hedström, et al. (2016). Towards Detecting and Blocking Malicious Exit Traffic in Tor. Proceedings of the 32nd Annual Computer Security Applications Conference, 382-393.
6. Edward Snowden. (2014). The Tor Project: The Importance of Common Good. The Guardian.
7. Ming Li and S.M.Yiu. (2010). Blocking Free-Riders in Peer-to-Peer Anonymizing Networks. IEEE Transactions on Parallel and Distributed Systems, 21(3), 391-401.
8. Ehab Abdelatif and Amr Youssef. (2018). Misbehavior Detection and Defense in Tor Onion Routing. IEEE Journal on Selected Areas in Communications, 36(7), 1468-1478.
9. Ryan Henry and Nick Hopper. (2015). An Empirical Evaluation of Attacks in Anonymous Networks. Proceedings of the 2015 ACM Conference on Computer and Communications Security, 1062-1073.
10. Roger Dingledine, Nick Mathewson, and Paul Syverson. (2004). Tor: The Second-Generation Onion Router. Proceedings of the 13th USENIX Security Symposium, 303-320.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details