

Nymble Blocking System for Countering Misbehaving Users over Anonymizing Networks

M. Vanaja

M.Tech.

Chaitanya Institute of Science and
Technology, Kakinada

M. Vamsi Krishna

Head, Deptt. of CSE,

Chaitanya Institute of Science and
Technology, Kakinada

Venkata Ramana

Asst.Prof., Deptt. of CSE,

Chaitanya Institute of Science and
Technology, Kakinada

Abstract – Anonymity networks such as TOR provide users with a means to communicate privately over the Internet. These networks help to solve the real and important problem of enabling users to communicate privately over the Internet. But some users misuse this service and they tried to deface popular websites like wikipedia. To counter such users, a system called Nymble is used. Nymble possesses the following properties: anonymous authentication, backward unlinkability, subjective blacklisting, fast authentication speeds, rate-limited anonymous connections, revocation auditability (where users can verify whether they have been blacklisted), and it also deals with the Sybil attack so as to make its implementation practical. This paper presents an overview of the anonymizing network- TOR and how it can be used with the Nymble system. The Nymble system only blocks dishonest users and allows anonymity to honest users.

Keywords — Anonymity, Blacklisting, Pseudonym, TOR.

I. INTRODUCTION

Anonymizing networks such as Tor[1][2] route traffic through independent nodes in separate administrative domains to hide a client's IP address. Unfortunately, some users have misused such networks—under the cover of anonymity, users have repeatedly defaced popular Web sites such as Wikipedia. Since 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.

To counter such malicious users and continuing anonymous access to behaving users, anonymizing networks such as Tor are combined with Nymble system. Nymble [3] is basically a system that intends to bind identity of an anonymous user to a pseudonym, generated from user's IP address, and simulates a service request with a ticket acquisition. This idea enables a server to complain about misbehavior of a user and blacklist his future tickets. Using this system honest users remain anonymous, a server can blacklist future connections of particular users. Moreover, all connections of a blacklisted user before the complaint remain anonymous and finally a user can check whether he is blacklisted or not at the beginning of a connection. Nymble can also counter sybil attack [4]. Nymble offers the following properties:

- **Anonymous blacklisting:** A server can block the IP address of a misbehaving user without knowing the identity of the user or his/her IP address.
- **Privacy:** Honest and misbehaving users both remain anonymous.

- **Backward anonymity:** The blacklisted user's previous activity remains anonymous/unlinkable, and is refused future connections.
- **Blacklist-status awareness:** A user can check whether he/she has been blocked before accessing services at the server.
- **Subjective judging:** Since misbehaving users are blocked without compromising their privacy, servers can provide their own definition of "misbehavior".

II. AN EXAMPLE ANONYMIZING NETWORK-TOR

TOR is the acronym for "The Onion Router". In an onion router system[5], network messages are multiply (triple) encrypted at the source and sent randomly through an IP network of routers (onion servers), where each router removes one layer of encryption — just as you can peel the layers off an onion. The Entry Point server is chosen from a smaller set of onion router servers called Entry Guards and then randomly chosen from this set. Each of the three servers, the one chosen randomly from the Entry Guard group and the other two chosen randomly from available onion router servers worldwide, then use their public key to remove one layer of encryption at a time. When the message arrives at its destination, the message is unencrypted but the receiver has no knowledge of where the message came from or what path it took to get there, only the last server to forward the data on. Not only is the receiver in the dark, but all of the intermediate nodes between the encryption source and the exit node also have no idea of the source, contents, or destination of the packets, making it impossible for anyone inside the onion network to be able to compromise the communication.

Fig.1 shows a schematic of how hidden services work. An installed hidden service advertises for clients by broadcasting its availability (1) using the hidden service protocol through random paths (virtual circuits) to servers and by storing its information and public key in the Tor Directory Server. Those servers accept the role of being an Introduction Point and store a public key for the hidden service (2). Because the path taken between the hidden service's server and the Introduction Points consists of random virtual circuits, there is no way for a client to be able to associate the two systems with one another or to learn the hidden server's IP address.

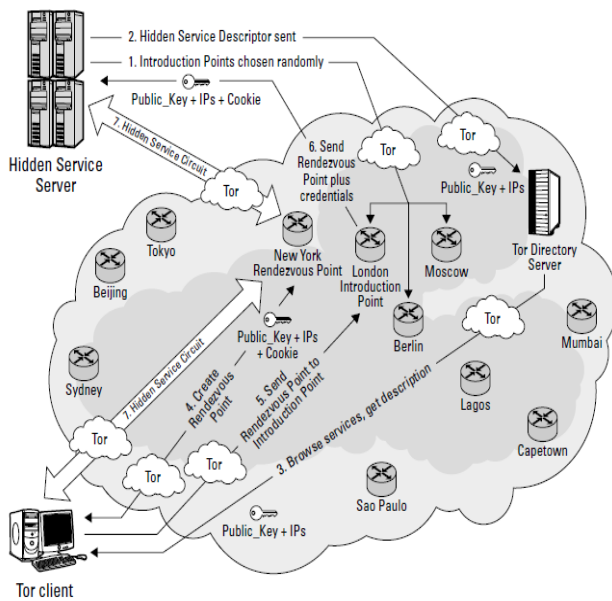


Fig.1. Hidden services on the TOR network

A Tor client learns about hidden services from the Tor Directory Server (3) and creates a Rendezvous Point. Then the Tor client communicates with one of the Introduction Point Servers (4). A Rendezvous Point contains both a public key and a cookie that are used to encrypt/decrypt information as well as supply information that allows the data to be forwarded from the hidden server to the Tor client. Once the Introduction Point transfers the Tor client's information to the Hidden Service Server, the virtual circuit shown as 7 with a large arrow is created. The system separates the Introduction Point from the Rendezvous Point, and by doing so ensures that the Tor client's information remains anonymous.

Unfortunately, some users have abused such networks to deface websites such as Wikipedia. Since servers are unable to block anonymous users, their normal response is to simply block the entire anonymizing network, denying anonymous access to honest and dishonest users alike. To counter only misbehaving users and allow honest users to use anonymizing networks like TOR, a system called Nymble is used.

III. BLOCKING MISBEHAVING USERS USING NYMBLE SYSTEM

Nymble is a credential system that can be used in conjunction with anonymizing networks such as Tor to selectively block anonymous users while maintaining their privacy. The purpose of the Nymble project is to allow for responsible, anonymous access online. It provides a mechanism for server administrators to block misbehaving users while allowing for honest users to stay anonymous; in fact even the blocked users remain anonymous. The name "Nymble" comes from a play on the word "pseudonym"[6][7] and "nimble". Instead of giving users a simple pseudonym, the Nymble system assigns users

"nymbles"; that is, a pseudonym with better anonymity properties.

Nymble is based on two administratively-separate "manager" servers, the Pseudonym Manager (PM) and the Nymble Manager (NM). The PM is responsible for pairing a user's IP address with a pseudonym deterministically generated based on the user's IP address. The NM pairs a user's pseudonym with the target server. As long as the two managers are not colluding, the user's connections remain anonymous to the PM, pseudonymous to the NM (note that the user does not communicate directly with the NM, and connects to the NM through Tor), and anonymous to servers that the user connects to.

A. Connecting to a server

Pseudonym Manager :

The user (in this case, Alice) must first demonstrate control over a resource, that is the Alice's IP-address. To do this Alice must first connect directly with the PM before receiving a pseudonym. The PM has knowledge of existing Tor routers, and thus can ensure that Alice is communicating with it directly. Note that the PM has no knowledge of the user's destination, similar to the entry node in Tor. The PM's sole responsibility is to map IP addresses to pseudonyms (Figure 2).

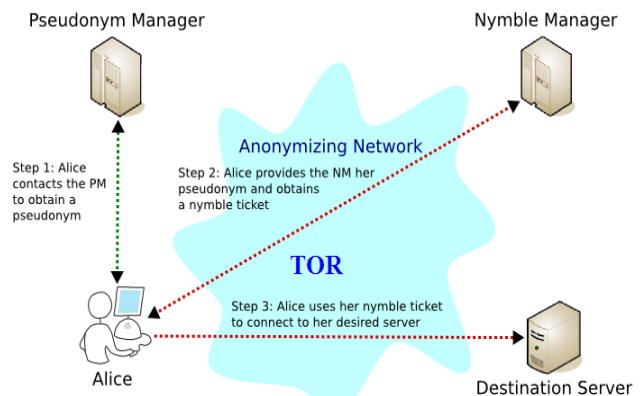


Fig.2. Connecting to a server

Nymble Manager:

Alice then connects to the NM through Tor presenting her pseudonym and her target server. The NM does not know the IP address of the user, but the pseudonym provided by the PM guarantees that some unique IP address maps to the pseudonym. She receives a set of nymble tickets as her credential for the target server. These nymble tickets are unlinkable, and therefore Alice can present these nymble tickets (once each) to gain anonymous access at the target server. The nymble ticket provides cryptographic protection as well as a trap door that can be accessed using a linking token

B. Blacklisting a user

Servers can present a user's nymble ticket to the NM as part of a complaint. The NM extracts a "linking token" from the nymble ticket that will allow the server to link future connections by the blacklisted user. The NM also issues servers with blacklists [8], which users can examine before performing any actions at the server. By checking servers' blacklists, blacklisted users are assured that their privacy is not compromised (Fig.3). We now

explain how nymble tickets are bound to certain "time periods" and "linkability windows."

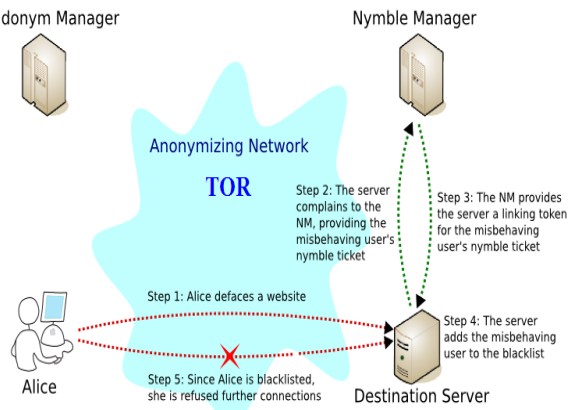


Fig.3. Blacklisting a user

Time in the nymble protocol is divided into linkability windows of some duration (default is 1 day). A linkability window (Fig.4) is then further divided into smaller time periods (default is 5 minutes). We illustrate the concepts in the diagram below; the linkability window is represented by the large, transparent rectangle while the time periods are labeled t_0, t_1, t_2 , etc.

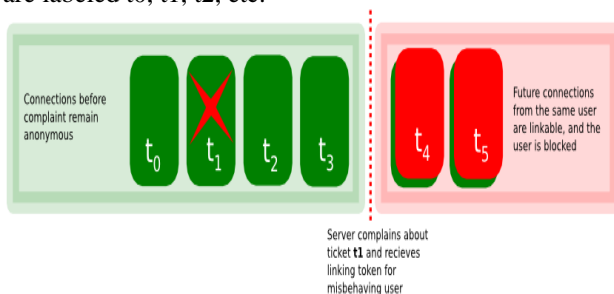


Fig.4. Linkability Window

A user's connections within a time period are tied to a single nymble ticket. If and when a user misbehaves, the server may not realize it for some amount of time and may not report it until a later time period. However, after receiving a linking token the server is able to block all future connections until the next linkability window. This is done for two reasons:

- **Dynamism:** IP-addresses can be reassigned to different, well-behaved users making it undesirable to permanently blacklist IP-addresses.
- **Forgiveness:** It ensures that bad behavior is forgiven after a certain amount of time.

IV. CONCLUSION

Nymble is a system that allows websites to selectively blacklist users of anonymizing networks such as Tor without knowing the user's IP-address. Users not on the blacklist enjoy anonymity while blacklisted users are not allowed future connections for a duration of time while their previous connections remain unlinkable. Since Nymble allows websites to blacklist anonymous users of their choice, and since users are notified of their blacklist

status, Nymble gives websites the power to define their own definition of "misbehavior".

REFERENCES

- [1] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second- Generation Onion Router," Proc. Usenix Security Symp., pp. 303- 320, Aug. 2004.
- [2] <http://www.torproject.org.in/>
- [3] Patrick P. Tsang, Apu Kapadia, Cory Cornelius, and Sean W. Smith. Nymble: Blocking misbehaving users in anonymizing networks. *IEEE Transactions on Dependable and Secure Computing*, 99(1), 2011.
- [4] J.R. Douceur, "The Sybil Attack," Proc. Int'l Workshop on Peer-to- Peer Systems (IPTPS), Springer, pp. 251-260, 2002.
- [5] J. Feigenbaum, A. Johnson, and P.F. Syverson, "A Model of Onion Routing with Provable Anonymity," Proc. Conf. Financial Cryptography, Springer, pp. 57-71, 2007.
- [6] A. Lysyanskaya, R.L. Rivest, A. Sahai, and S. Wolf, "Pseudonym Systems," Proc. Conf. Selected Areas in Cryptography, Springer, pp. 184-199, 1999.
- [7] D. Chaum, "Showing Credentials without Identification Transferring Signatures between Unconditionally Unlinkable Pseudonyms," Proc. Int'l Conf. Cryptology (AUSCRYPT), Springer, pp. 246-264, 1990.
- [8] Patrick P. Tsang, Man Ho Au, Apu Kapadia, and Sean W. Smith. Blacklistable anonymous credentials: blocking misbehaving users without ttps. In *CCS '07: Proceedings of the 14th ACM conference on Computer and communications security*, pages 72-81, New York, NY, USA, 2007. ACM.