Anonymous IP-Services via Overlay Routing

Olaf Landsiedel, Simon Rieche, Heiko Niedermayer, Klaus Wehrle, Georg Carle
Wilhelm-Schickard-Institute for Computer Science
University of Tübingen, Germany
firstname.lastname@uni-tuebingen.de

***Abstract*— Although research provides anonymous Internet communication schemes, anonymous IP-services received only limited attention. In this paper we present SARA (Anonymous Overlay Routing Providing Sender And Receiver Anonymity), which enables sender, receiver and relationship anonymity using layered encryption and distributed traffic mixes, similar to a Chaumian Mix. Via IP-datagram service and address virtualization it is fully transparent to applications. Organized as structured Peer-To-Peer system, SARA is highly scalable and fault tolerant.**

In SARA each communication partner randomly selects a number of nodes from the overlay and concatenates them to an anonymous communication path. The sender selects the head of the path, the receiver builds the tail and publishes this information in the overlay network using an anonymous ID. Via this ID the sender retrieves the tail nodes of the path and concatenates both path section. Layered encryption hides the identities of the sender, receiver and the intermediate nodes.

I. Introduction

For anonymous Internet communication, we envision that arbitrary hosts can communicate without revealing their identities, their relation and that nobody can eavesdrop the communication. Furthermore, we identify the need for a scalable, fault tolerant and transparent approach for all kinds of application types, e.g. web browsing, file transfer, secure shell, instant messaging and others.

In this paper we present SARA (Anonymous Overlay Routing Providing **S**ender **A**nd **R**eceiver **A**nonymity), an anonymous overlay routing scheme, which enables sender, receiver and relationship anonymity, enabling anonymous Internet services. Its Peer-To-Peer overlay routing scheme provides high scalability and fault tolerance, and a virtual network interface with address virtualization enables transparent and anonymous IP-service.

II. SARA's Architecture

Analog to the Chaumian Mix the sender sets up a path to the receiver through a number of randomly selected nodes, e.g. mixes. Each of the mixes forwards the data to its successor and so hides the sender's identity and the relationship of sender and receiver. Additionally, to ensure receiver anonymity in SARA, sender and receiver each select half of the nodes in the communication path: The sender as the head and the receiver as the tail of the path. The receiver publishes its tail section in the overlay using an anonymous ID. Via this ID the sender retrieves the tail from the overlay and concatenates head and tail sections to build an anonymous communication path.

Next to the anonymous path, layered encryption prevents that content, relationship, and path information can be revealed by malicious nodes and eavesdroppers. As SARA ensures near real-time performance, it cannot protect against a global eavesdropper.

III. Implementation Overview

Networking applications need access to TCP and UDP sockets and an underlying IP protocol with IP address. As many application protocols, like `ftp` and `H.323`, tend to communicate their address and identity in the message payload, address virtualization is crucial for anonymous Internet services. Thus, we use a virtual network interface with own protocol stack assigned a private IP address, for example `10.x.y.z` (see Fig. 1). This virtual IP address is derived from the node's anonymous ID using a hash.

To communicate the virtual network interface maps the virtual IP address and the anonymous ID; next the control application computes an anonymous path as described in section II.

IV. Evaluation

Obviously the routing via an anonymous path increases transmission latency. However, this is an inherited property of all anonymous routing approaches. Furthermore, SARA's design imposes low latency and overhead compared to a corresponding non-anonymous overlay routing scheme. As the proposed routing scheme of SARA is similar to onion routing, we identify similar threats. However, the limited space prevents a deeper discussion.

V. Conclusion

In this paper we present SARA, a novel approach to anonymous Internet communication. It does not only provide sender and relationship anonymity, but also enables receiver anonymity and is scalable and fault tolerant due to the underlying structured P2P-network. Furthermore, SARA's transparent architecture and address virtualization allow to provide network services ranging from web-servers to instant messaging and secure shell login without changes to the applications or communication protocols.

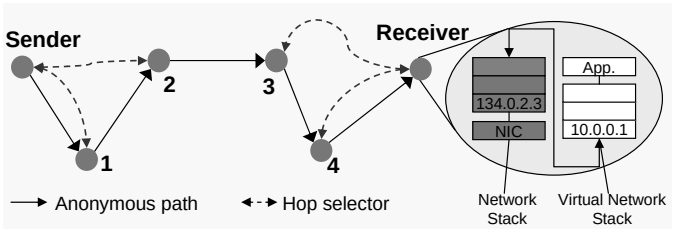

Fig. 1. Sender and receiver independently select a number of hops in the anonymous communication path. And a virtual network interface enables transparent application support.