УДК 004.72

студентка О.И. Авчинникова
ГВУЗ «Национальный горный университет»

АНОНИМНАЯ СЕТЬ INVISIBLE INTERNET PROGECT

Рассмотрены структурные особенности анонимной сети I2P и алгоритм передачи сообщений. Указаны возможные атаки и средства, снижающие их эффективность.

Анонимная сеть Invisible Internet Progect (I2P) представляет собой динамическую, децентрализованную, одноранговую сеть, заведомо адаптированную к условию, что любой из узлов сети враждебно настроен и может быть заинтересован в краже информации.

Проект I2P предоставляет пользователям возможность внутри сети создавать и просматривать сайты, обмениваться сообщениями, вести блоги, передавать файлы и выполнять многие другие действия, ставшие привычными при использовании обычной Интернет сети, в тоже время, обеспечивая высокий уровень анонимности и конфиденциальности в рамках сети.

Данная сеть разработана так, что пользователи могут обмениваться сообщениями и при этом не быть идентифицированы ни друг другом, ни третьими лицами. Принадлежность пользователя к сети не является секретом. Скрытой является информация о том, что делает пользователь и делает ли он что-либо вообще. Каждый маршрутизатор обладает уникальным криптографическим идентификатором, единственным образом, определяющим его в сети. Помимо маршрутизатора на рабочей станции пользователя могут быть активны и другие приложения («пункты назначения»), обладающие своими собственными идентификаторами, отличными от идентификатора маршрутизатора [1]. Эти приложения могут подключаться к маршрутизатору и использовать имеющиеся туннели для отправки и получения сообщений через сеть. В сети I2P для предоставления узлам сетевых метаданных организована внутренняя распределенная база данных (NetDB), основанная на модифицированном алгоритме DHT Kademlia.

Для передачи информации предусмотрены два вида туннелей: «исходящие» – туннели, отправляющие сообщения от создателя туннеля, и

«входящие» – приносящие сообщения создателю туннеля. Туннели представлены рядом маршрутизаторов, который изменяется каждые 10 минут, по предварительно выбранному пользователем алгоритму.

Если Алиса хочет послать Бобу сообщение, она первым делом делает поиск по NetDB, чтобы найти нынешние характеристики его входного туннеля. Далее она отправляет сообщение, по одному из своих исходящих туннелей на один из входящих туннелей Боба. Если Алиса хочет получить ответ на свое сообщение, она передает свою контактную информацию как часть сообщения, иначе Боб будет вынужден обращаться к NetDB, чтобы получить данные о действующем входящем туннеле Алисы. Каждая сторона строит два тоннеля, для исходящего и для входящего трафика. Таким образом, для передачи одного сообщения и получения ответа необходимы четыре туннеля (Рис. 1).

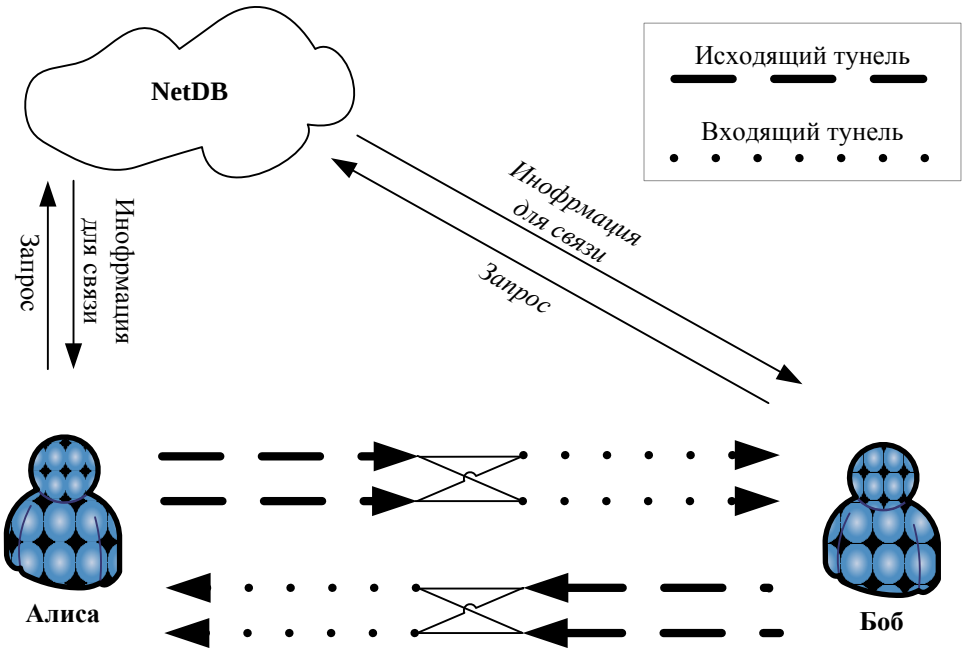

Рис. 1. Передача сообщений

Для защиты информацию в сообщении, адресата и, возможно, обратного адреса отправителя используется «чесночная» маршрутизация. При шифровании в «чеснок» собирается множество «зубчиков» – зашифрованных сообщений, каждое с инструкциями по доставке, сообщения могут принадлежать как данному узлу, так и быть транзитными [2]. Далее они

передаются следующим, указанным в инструкциях маршрутизаторам. При поступлении сообщения на очередной маршрутизатор с него снимается соответствующий слой шифрования, и маршрутизатор получает адрес следующего узла (адрес получателя), которому он должен передать сообщение.

I2P это микс-сеть с малым временем отклика, что делает ее уязвимой для атак типа тайминг-анализ, атака пересечением. Уровень безопасности данной анонимной сети прямо пропорционален количеству участников сети, поскольку клиенты сети одновременно являются и маршрутизаторами трафика. Снизить эффективность атак позволяет реализация двух типов туннелей, в результате чего возможность передачи исходящих сообщений и ответов на них одним и тем же путем маловероятна. Применяемая для шифрования данных «чесночная маршрутизация» помогает смешать трафик и ввести в замешательство атакующего, пытающегося сопоставить размер и время передачи сообщений [3].

Реализация высоких требований анонимности чаще всего производится за счет увеличения времени отклика, снижения скорости передачи данных, увеличения объемов побочного сетевого трафика и, как результат, за счет снижения производительности. Поскольку службы, функционирующие в I2P, требуют высокой скорости коммуникаций, то реализация больших временных задержек, таких как в сетях Mixmaster и Mixminion, не допустима.

Перечень литературы:

1. Tech intro. https://www.i2p2.de/techintro.html
2. Garlic Routing and “Garlic” Terminologi.
3. https://www.i2p2.de/how_garlicrouting.html
4. Adrian Crenshaw. Darknets and hidden servers: Identifying the true IP/network identity of I2P service hosts. http://www.irongeek.com/i.php?page=security/darknets-i2p-identifying-hidden-servers.