УДК 517.9

Развитие методов анонимности

О.В. Трушина

Московский физико-технический институт (государственный университет)

С развитием информационных технологий все большее значение приобретает задача обеспечения анонимности. В случае распределенных сетей часто достаточно защитить информацию о том, кто кому передает сообщение. Этот уровень защиты гарантирует, что злоумышленник не может прослеживать сообщения. Это значит, что последовательно прослушивая сообщения, передающиеся по смежным соединениям сети, злоумышленник не может установить между ними связи.

Необходимым условием для анонимности является обеспечение *битовой несвязности*. Битовая несвязность гарантирует, что сообщения поступающие в узел и выходящие из него «выглядят» по-разному.

Исследования в области анонимности были начаты работой [1], в которой предложен метод Mix-net. В дальнейшем этот метод развился в один из самый широко известных методов – Onion Routing [2]. Битовая несвязность в Mix-net достигается посредством шифрования на каждом шаге передачи. Отправитель формирует сообщение вида, получившего в дальнейшем название «луковица» $E_{k_1}\left(E_{k_2}\left(\ldots E_{k_n}\left(M, I_B\right)\ldots, I_3\right), I_2\right)$, где $k_i, I_i, i=1,2,\ldots n$ соответственно открытые ключи и идентификаторы узлов, через которые будет передаваться сообщение M, I_B –идентификатор получателя. Узел принимает зашифрованные сообщения от разных отправителей пока их количество не достигнет некоторого n, затем расшифровывает их и отправляет следующему узлу в лексикографическом или произвольном порядке. В отличие от Mix-net, где отправитель для каждого передаваемого сообщения, для каждого mix должен выполнять операцию асимметричного шифрования, в Onion Routing асимметричное шифрование используется только при установлении соединения для передачи симметричного секретного ключа. Для передачи данных отправитель также формирует «луковицу», но с использованием симметричного шифрования. На идее Onion Routing основана одна из наиболее известных и широко используемых систем анонимности Tor [3].

Можно выделить еще один класс методов анонимности, которые используют случайную маршрутизацию [4,5]. Битовая несвязность по-прежнему достигается с помощью шифрования. Все пользователи сети образуют группу, называемую толпой, которая централизованно управляется узлом под названием блендер. Оправляя сообщение, источник передает его

произвольно выбранному члену толпы, предварительно зашифровав его на соответствующем секретном ключе. Получивший сообщение узел расшифровывает его и с некоторой вероятностью p отправляет следующему произвольному члену толпы или с вероятностью $1-p$ нужному узлу, зашифровав на соответствующем секретном ключе.

Все рассмотренные выше методы реализуют криптографический подход к обеспечению битовой несвязности, главный инструмент которого – шифрование. В работе [6] предложен информационно-теоретический подход к обеспечению битовой несвязности. Он основан на кодировании смежными классами. Исходное сообщение кодируется в случайный элемент определенного смежного класса. С помощью добавления случайного кодового слова передающие узлы преобразуют входное сообщение в другой элемент того же смежного класса так, что выходное и входное сообщения узла статистически независимы.

В настоящей работе представлен аналитический обзор работ, посвященных методам анонимности. Большинство методов реализуют криптографический подход. Но информационно-теоретический подход активно исследуется. Это связано с двумя его преимуществами. Современная криптография основана на том, что злоумышленник вычислительно ограничен. Информациооно-теоретический подход не накладывает вычислительных ограничений на злоумышленника, следовательно, обещает долгосрочную защиту и отсылает к понятию постквантовой защиты информации. Второе преимущество состоит в отсутствии задач распеределения ключей и управления ими, которые могут быть довольно сложными, а следовательно, энергозатратными, что существенно для систем связи с маломощными портативными устройствами.

Литература

1. *Chaum D.,* Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. - CACM - 1981. - V. 24, N. 2. - P. 84-88.

2. *Goldschlag D.M., Reed M.G., Syverson P.F.,* Hiding routing information. - Proceedings of the First International Workshop on Information Hiding. - 1996. - P. 137-150.

3. www.torproject.org

4. *Reiter M.K., Rubin A.D,* Crowds: Anonymity for Web Transactions. - ACM Transactions on Information and System Security. - 1998. - V. 1, N. 1.- P. 66–92.

5. *Levine B.N., Shields C.,* Hordes: A Muplicast Based Protocol for Anonymity. - Journal of Computer Security. - 2002. - V. 10, N. 3. - P. 213-240.

6. О. В. Трушина, Э. М. Габидулин, Новый метод обеспечения анонимности и секретности в сетевом кодировании. - *Пробл. передачи информ.* - 2015. - P. 82-89