ИСПОЛЬЗОВАНИЕ ПОЛЕЙ ЗАГОЛОВКА IP-ПАКЕТА ДЛЯ МЕТОДОВ СЕТЕВОЙ СТЕГАНОГРАФИИ

А.Н. Николайчук

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Сетевая модель TCP/IP описывает процесс передачи информации между двумя устройствами сети. Согласно этой модели, символьное сообщение отправителя преобразуется к бинарной последовательности, отправляется, а также дополняется некоторой служебной информацией, которая необходима, например, для того, чтобы обратно преобразовать бинарную последовательность получателя к исходному символьному сообщению.

В зависимости от типа данных (видео, картинка), служебная информация будет формироваться по-своему, в соответствии с некоторыми правилами, которые принято называть протоколами. Но использовать разные способы передачи данных для разных типов было бы неэффективно, поэтому операцию преобразования сообщения разбили на несколько уровней (прикладной, транспортный, сетевой, канальный), чтобы вне зависимости от типа входных данных сформированная бинарная последовательность имела одинаковую структуру. Название стека (набора) протоколов TCP/IP, на котором базируется Интернет происходит из двух важнейших протоколов семейства – Transmission Control Protocol (TCP) и Internet Protocol (IP), которые были разработаны первыми.

Протокол IP объединяет сегменты (данные транспортного уровня) в единую сеть, обеспечивая доставку пакетов (данные сетевого уровня) между любыми узлами сети через произвольное число промежуточных. IP не гарантирует надежной доставки пакета до адресата. Гарантию безошибочной доставки пакетов дают некоторые протоколы более высокого уровня. Возможно также возникновение ситуации, когда размер пакета превысит возможности узла системы связи. Для таких случаев протокол предусматривает возможность дробления пакета на уровне IP в процессе доставки (фрагментация). В известных методах сетевой стеганографии используются следующие поля заголовка пакета протокола IP: Type of Service, Identification, Flags, Fragment Offset, Options, Padding [1–3]. Использование именно этих полей для задач стеганографии обусловлено тем, что они, при некоторых условиях, позволяют разместить дополнительную информацию в пакете, так как существуют ситуации, при которых данные поля не используются. Однако такие методы характеризуются низкой пропускной способностью [4].

Список литературы

1. Zander, S. A Servey of convert channels and countermeasures in computer network protocol / S. Zander, G. Armitage, P. Branch // IEEE Communications Surveys & Tutorials – 2007. – Vol. 9. – № 3. – P. 44–57.

2. Handel, T. Hiding data in the OSI network model / T. Handel, M. Sandford // Proceedings of the First International Workshop on Information Hiding. – 1996. – P. 23–38.

3. Jankowski, B. PadSteg: Introducing inter-Protocol Steganography / B. Jankowski, W. Mazurczyk, K. Szczypiorski // Telecommunication Sys-tems. – 2011. – Vol. 52. – No. 2. – P. 1101–1111.

4. Применения сетевой стеганографии для скрытия данных, передаваемых по каналам связи / О.Ю. Пескова, Ю. Г. Халабурда // Известия ЮФУ. Технические науки. – 2012.