УДК 004.056.5

# Организация скрытых каналов на основе стека протоколов TCP/IP

С.С. Угрюмов

Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации (ФГУП ВНИИПВТИ)

Московский физико-технический институт (государственный университет)

Организация защиты информационных потоков от несанкционированного доступа является одной из ключевых задач, входящих в комплекс мер по обеспечению безопасности информации. Помимо стандартных методов защиты конфиденциальной информации, в частности, криптографических, которые скрывают содержимое передаваемых сообщений, существуют методы, которые скрывают сам факт передачи информации – стеганографические. Цель данной работы – проанализировать современные способы организации скрытых каналов [1] с помощью стеганографических методов на основе алгоритмов, используемых в технологиях стека протоколов TCP/IP. Также в данной работе автором предложен способ организации скрытого канала на основе уровня нагрузки линии при использовании технологии TCP Tahoe.

В рамках обзора существующих методов из четырех типов скрытых каналов [2]: Storage-based, Timing-based, Frequency-based, Protocol-based рассмотрены только Storage-based и Timing-based каналы. Особое внимание, как наиболее изученным и менее сложным в реализации, уделяется Storage-based каналам. Помимо этого рассмотрены методы детектирования скрытых каналов.

В настоящее время наиболее инновационными техниками организации Storage-based каналов являются CLACK [3] и RSTEG [4], использующие для скрытой передачи информации ACK-пакеты в рамках работы протокола TCP [5]. Особенностью RSTEG является идея имитации получателем потери фрагментов, использующаяся для принудительной посылки ACK-пакетов. В данной работе предпринята попытка развить эту идею, а именно, применить ее для имитации потери фрагментов вследствие перегрузки линии в рамках технологии TCP Tahoe [6].

Предлагается следующий метод. Технология TCP Tahoe предполагает, что успешная передача блока данных при некотором размере окна подтверждает неполную загруженность линии, вследствие чего размер окна для последующей передачи увеличивается (экспоненциально или линейно). Потеря же данных говорит о перегрузке линии, вследствие чего размер окна уменьшается до некоторого небольшого стартового значения и экспоненциальный/линейный рост размера окна начинается заново. В результате этого возникает явление TCP sawtooth [7] (рис.1). Имитация потери пакетов позволяет модулировать по некоторому закону уровень «пиков» нагрузки, что может использоваться для скрытой передачи данных.

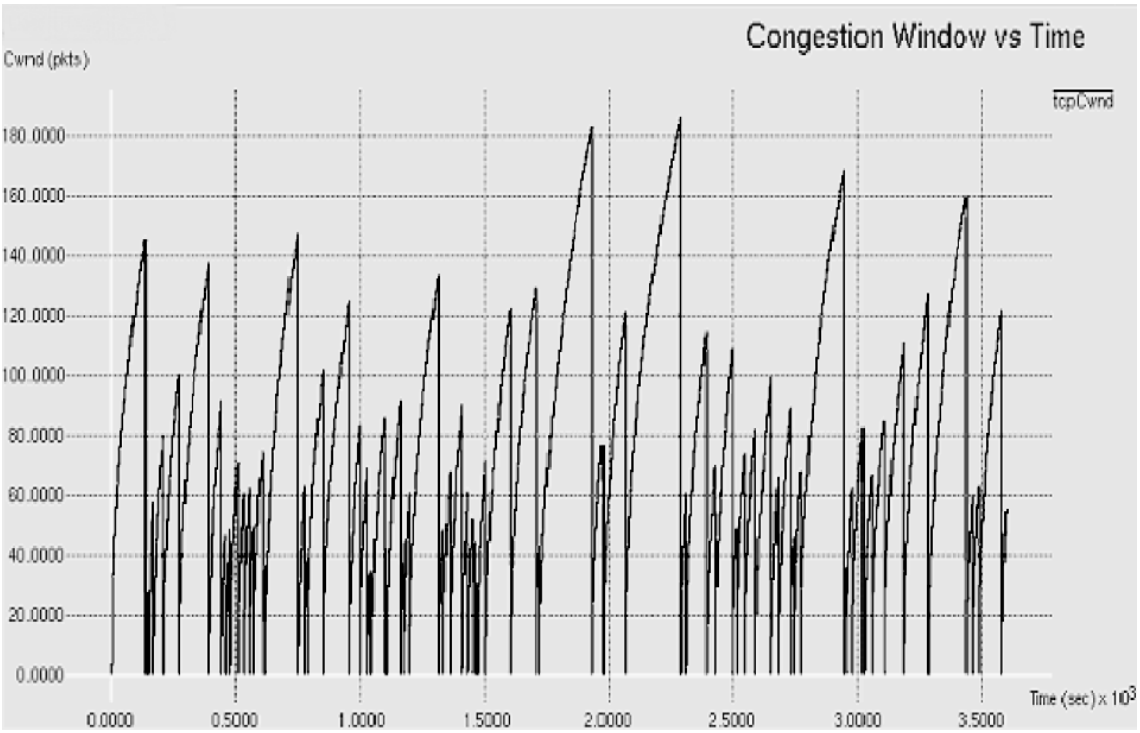


рис 1. TCP sawtooth [7]

В заключение работы рассматриваются способы использования данного алгоритма в случае наличия потерь фрагментов вследствие реальной перегрузки линии, единичных потерь вследствие помех и т.п.

Литература


1. *C. H. Rowland,* Covert channels in the TCP/IP protocol suite. - FirstMonday, Peer Reviewed Journal on the Internet. - 1997. - Tech. Rep. 5
2. *Manisha V. Changule, Sachin P. Patil,* Covert Channel Using TCP/IP Protocol Suite. - International Journal of Emerging Technology and Advanced Engineering. - 2014. - Volume 4. - Issue 9
3. *Xiapu Luo Chan, E.W.W. Chang, R.K.C,* CLACK: A Network Covert Channel Based on Partial Acknowledgment Encoding. - ICC '09. IEEE International Conference on Communications. – 2009. – pp. 1-5
4. *Mazurczyk W., Smolarczyk S., Szczypiorski K.,* Retransmission steganography and its detection. - Soft Computing. – 2011. - Volume 15. - pp 505-515
5. *Prof. RajeswariGoudar, SujataEdekar,* Ephemeral Feature Presentation of Covert Channels in Network Protocols. - International Journal of Scientific and Research Publications. – 2013. - Volume 3. - Issue 6
6. *V. Jacobson,* Congestion avoidance and control. - Proc. ACM SIGCOMM '88. – 1988. - pp. 314-329
7. *Mehdi Hussain, M. Hussain,* A High Bandwidth Covert Channel in Network Protocol. - International Journal of Advanced Science and Technology. – 2011. - Volume 30 - p. 1