P.V. Yegorov

The Technical Issues of Traffic Analysis

Keywords: traffic analysis, traffic classification, payload.

The main problem in the analysis of Internet traffic associated with a large number of network applications, complex patterns of communication and a significant amount of information. The definition of the category of traffic using the analysis of the number of port is irrelevant for P2P applications, streaming data and many other types of network applications. The article describes some of technical issues related to the analysis of Internet traffic.

П.В. Егоров

ТЕХНИЧЕСКИЕ ОСОБЕННОСТИ АНАЛИЗА ТРАФИКА

С развитием сетей передачи данных анализ сетевого трафика становится всё более актуальной задачей. Он используется не только для проектирования планов развития сети, но и обнаружения проблем в сети, построения систем мониторинга, отчетности и предотвращения вторжений.

Одной из основных операций, связанной с анализом сетевого трафика, является определение различных типов приложений, которые используют те или иные ресурсы сети. Подобная информация востребована сетевыми администраторами, так как управление сетью и её развитие и проектирование возможно только в том случае, когда имеются сведения о типах трафика, используемых в сети. Эти сведения дают возможность предугадать рост нагрузки с целью проведения своевременной модернизации. Кроме того, такой анализ дает возможность обнаружить возможные факты нецелевого использования сетевых ресурсов.

При анализе трафика наиболее значимы две проблемы. Первая связана с тем, как справиться с большими объемами трафика, получаемых в режиме реального времени. [1] Вторая проблема заключается в анализе сложных структур данных, генерируемых различными сетевыми приложениями [2].

Основные технические особенности анализа сетевого трафика:

– многие сетевые приложения используют проприетарные протоколы, не имеющие четкой и публичной спецификации;

– отдельные сетевые приложения используют нестандартные номера портов;

– значительное количество портов, используемых сетевыми приложениями, не входит в список IANA [3];

– активное использование мер для сокрытия трафика и его шифрование.

Эти особенности делают анализ трафика сложным процессом. В докладе описаны примеры указанных особенностей и предложены меры по решению описанных проблем. С целью создания алгоритма идентификации трафика сетевых приложений, описывается фреймворк на языке программирования Python для проведения процедуры анализа трафика. Также в докладе изложены принципы получения исходные данных и основные блоки алгоритма.

СПИСОК ЛИТЕРАТУРЫ:

1. Rosen E., Viswanathan A. and Callon R. Multiprotocol Label Switching Architecture, RFC3031, IETF, Jan. 2001.
2. Sen Subhabrata and Wang Jia. Analyzing Peer-to-Peer Traffic across Large Networks, Proc. of the second ACM SIGCOMM Workshop on Internet Measurement Workshop, Nov. 2002.
3. IANA, http://www.iana.org/assignments/port-numbers.

REFERENCES:

1. Rosen E., Viswanathan A. and Callon R. Multiprotocol Label Switching Architecture, RFC3031, IETF, Jan. 2001.
2. Sen Subhabrata and Wang Jia. Analyzing Peer-to-Peer Traffic across Large Networks, Proc. of the second ACM SIGCOMM Workshop on Internet Measurement Workshop, Nov. 2002.
3. IANA, http://www.iana.org/assignments/port-numbers.