欢迎搭乘Hyperscan号极速列车~

原创 DPDK开源社区 2016-12-15

作者 王翔

Hyperscan是一款来自于Intel的高性能的正则表达式匹配库。它是基于X86平台以PCRE为原型而开发的，并以BSD许可开源在https://01.org/hyperscan。在支持PCRE的大部分语法的前提下，Hyperscan增加了特定的语法和工作模式来保证其在真实网络场景下的实用性。与此同时，大量高效算法及IntelSIMD*指令的使用实现了Hyperscan的高性能匹配。Hyperscan适用于部署在诸如DPI/IPS/IDS/FW等场景中,目前已经在全球多个客户网络安全方案中得到实际的应用。此外，Hyperscan还支持和开源IDS/IPS产品Snort(https://www.snort.org)和Suricata (https://suricata-ids.org)集成，使其应用更加广泛。

原理

Hyperscan以自动机理论为基础，其工作流程主要分成两个部分：编译期(compiletime)和运行期(run-time)。

编译期

Hyperscan 自带C++编写的正则表达式编译器。如图1所示，它将正则表达式作为输入，针对不同的IA平台，用户定义的模式及特殊语法，经过复杂的图分析及优化过程，生成对应的数据库。另外，生成的

数据库可以被序列化后保存在内存中，以供运行期提取使用。

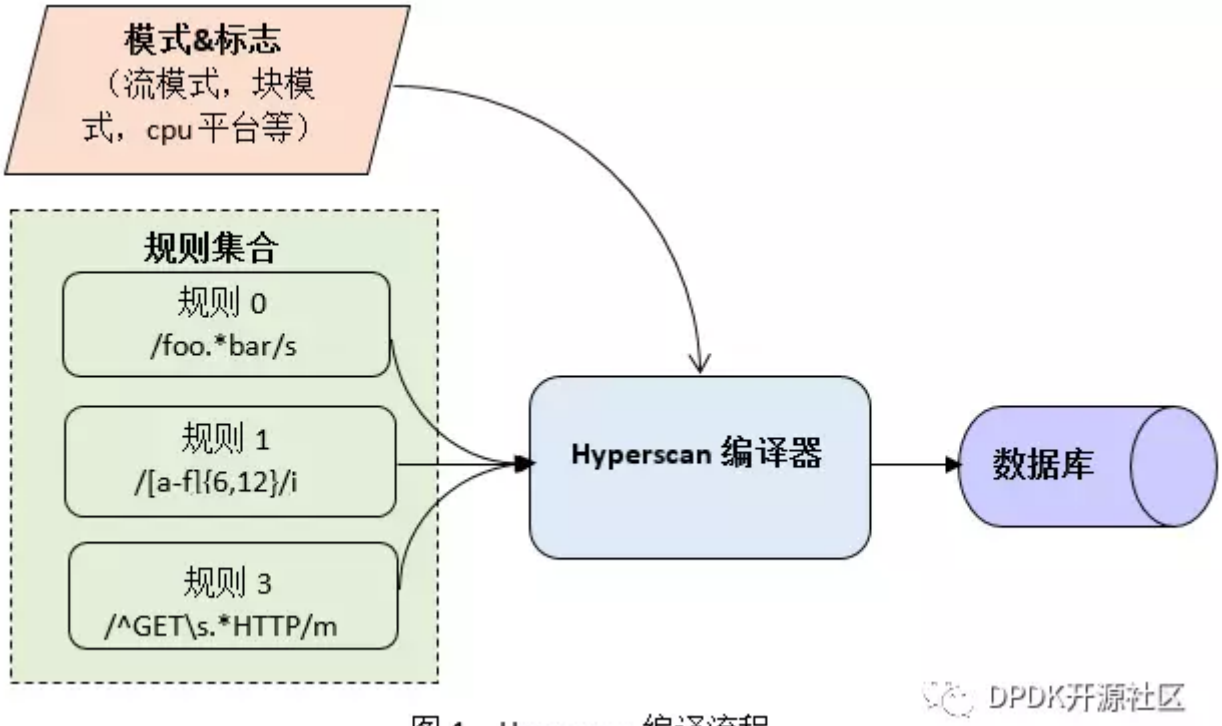

图 1：Hyperscan 编译流程

运行期

Hyperscan的运行期是通过C语言来开发的。图2展示了Hyperscan在运行期的主要流程。用户需要预先分配一段内存来存储临时匹配状态信息，之后利用编译生成的数据库调用Hyperscan内部的匹配引擎(NFA, DFA等)来对输入进行模式匹配。Hyperscan在引擎中使用Intel处理器所具有的SIMD指令进行加速。同时，用户可以通过回调函数来自定义匹配发生后采取的行为。由于生成的数据库是只读的，用户可以在多个CPU核或多线程场景下共享数据库来提升匹配扩展性。

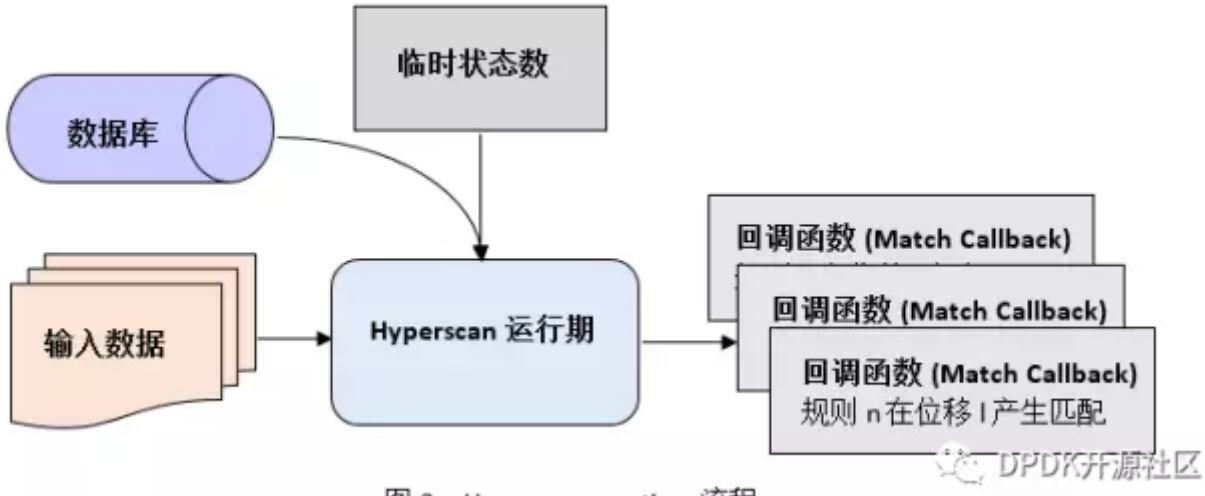

图 2：Hyperscan run-time 流程

特点

功能多样

作为纯软件产品，Hyperscan支持Intel处理器多平台的交叉编译，且对操作系统无特殊限定，同时支持虚拟机和容器场景。Hyperscan 实现了对 PCRE 语法的基本涵盖，对复杂的表达式例如”.*”和”[^>]*”不会有任何支持问题。在此基础上，Hyperscan增加了不同的匹配模式(流模式和块

模式)来满足不同的使用场景。通过指定参数，Hyperscan能找到匹配的数据在输入流中的起始和结束位置。更多功能信息请参考http://01org.github.io/hyperscan/dev-reference/。

大规模匹配

根据规则复杂度的不同，Hyperscan能支持几万到几十万的规则的匹配。与传统正则匹配引擎不同，Hyperscan支持多规则的同步匹配。在用户为每条规则指定独有的编号后，Hypercan可以将所有规则编译成一个数据库并在匹配过程中输出所有当前匹配到的规则信息。

流模式 (streaming mode)

Hyperscan主要分为两种模式：块模式 (blockmode)和流模式 (streaming mode). 其中块模式为状态正则匹配引擎具有的模式，即对一段现成的完整数据进行匹配，匹配结束即返回结果。流模式是Hyperscan为网络场景下跨报文匹配设计的特殊匹配模式。在真实网络场景下，数据是分散在多报文中。若有数据在尚未到达的报文中时，传统匹配模式将无法适用。在流模式下，Hyperscan可以保存当前数据匹配的状态，并以其作为接收到新数据时的初始匹配状态。如图3所示，不管数据”xxxxabcxxxxxxxxdefx”以怎样的形式被分散在以时间顺序到达的报块中，流模式保证了最后匹配结果的一致性。另外，Hyperscan对保存的匹配状态进行了压缩以减少流模式对内存的占用。Hyperscan流模式解决了数据完整性问题，极大地简化用户网络流处理的过程。

图3：网络数据以时间顺序被分散在不同数据单元中

高性能及高扩展性

Hyperscan以IntelSSSE3指令作为最低要求，使用了大量SIMD指令对匹配性能进行加速。我们基于防火墙厂商的真实规则，在Intel(R) Xeon(R) CPUE5-2699 v3 @ 2.30GHz对IPS真实网络流量进行测试。以下数据是Hyperscan的单独匹配性能(Gbps)：

模式	规则	规则数目	1C	2C	4C	18C	36C	36C 2 T/C
streaming	to_client_1	**69**	23.9	51.3	94.0	350.7	709.2	720.0
streaming	to_client_2	**142**	21.0	40.7	79.4	275.6	562.6	577.5
streaming	to_server_1	**43**	10.8	20.6	40.4	140.1	276.4	285.3
streaming	to_server_2	**235**	6.0	11.1	22.6	75.3	155.1	147.5
block	to_server_uri_1	**13110**	3.6	5.7	11.2	45.0	90.6	102.4
block	to_server_uri_2	**8801**	4.4	8.8	17.2	73.1	142.6	149.4

可以看到，Hyperscan在不同规则集下，单核性能可实现3.6Gbps~23.9Gbps。而且Hyperscan具有良好的扩展性，随着使用核数的增加，匹配性能基本处于线性增长的趋势。在网络场景中，同一规则库往往需要匹配多条网络流。Hypercan的高扩展性为此提供了有力的支持。

Hyperscan与DPDK的整合方案

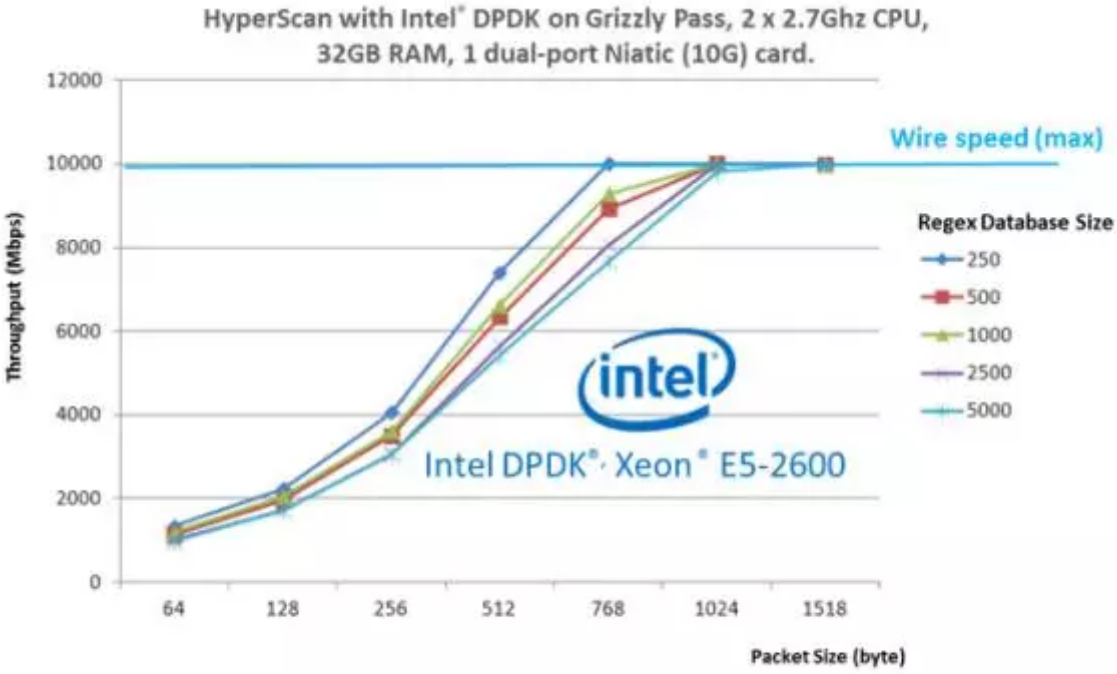

图 4：Hyperscan 与 DPDK 整合方案性能

DPDK (http://dpdk.org)作为高速网络报文处理转发套件，在业界得到了极为广泛的应用。Hyperscan能与DPDK整合成为一套高性能的DPI解决方案。图4展示了Hyperscan与DPDK整合后的性能数据。我们在测试中使用了真实的规则库并以http流量作为输入。Hyperscan与DPDK的结合实现了较高的性能，且随着包大小的增长，性能可以到达物理的极限值。

总结

Hyperscan是一款基于Intel架构的成熟的正则表达式匹配库。它具有同时匹配大规模规则的强大能力，并展现了出色的匹配性能与扩展性。同时，它针对网络报文处理设计了独有的匹配模式。并且Hyperscan与DPDK的整合为DPI/IDS/IPS等产品提供了成熟高效的整套方案。

SIMD*：SIMD单指令流多数据流(SingleInstruction Multiple Data,SIMD)是一种采用一个控制器来控制多个处理器，同时对一组数据（又称“数据向量”）中的每一个分别执行相同的操作从而实现空间上的并行性的技术。

作者简介：王翔，英特尔软件工程师，负责Hyperscan研发。主要研究领域包括正则表达式匹配，深度报文检测等。

❀ 感谢张磊的建议和修改 ❀

DPDK开源社区

干货满满，不容错过

阅读原文 投诉