(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115314269 A
(43)申请公布日 2022.11.08

(21)申请号 202210905306.6

(22)申请日 2022.07.29

(71)申请人 北京国领科技有限公司
地址 100094 北京市海淀区丰慧中路7号新材料创业大厦A座313号

(72)发明人 张建国 付晓峰

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/1036(2022.01)

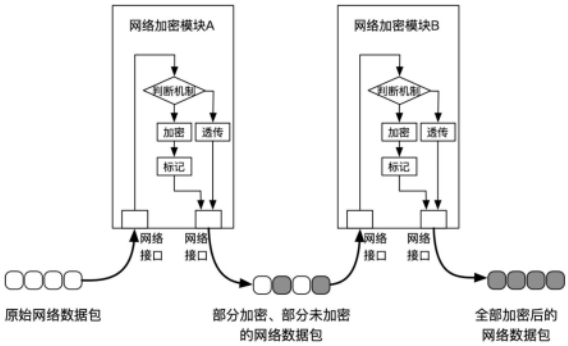
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种串行任务分工实现高性能网络加密的方法

(57)摘要

本发明公开了一种串行任务分工实现高性能网络加密的方法。单个网络加密模块因密码运算性能有限，无法满足高并发、大带宽等高性能要求，在大量应用场景中，需要使用负载均衡系统将大量数据分发到多个并行的网络加密模块中进行处理。本方法采用一种串行任务分工机制，让网络数据流量依次串行进入多个网络加密模块，通过一定的判断机制和标记方法让多个网络加密模块共同分担和完成所有网络流量的加密任务。本方法无需传统负载均衡系统即可实现将大量网络数据包均衡的分配到多个网络加密模块中，让网络加密系统拓扑更加精简、易部署，能够解决多种无法部署负载均衡的场景下高性能网络加密瓶颈的问题。



CN 115314269 A

1.一种串行任务分工实现高性能网络加密的方法,其特征在于:所述方法至少包含2个网络加密模块,每个网络加密模块至少包含2个网络接口,网络加密模块中还包含数据包判断机制、加密功能、透传功能,以及标记功能;多个网络加密模块之间使用网线串行连接;网络数据能够从串行的多个网络加密模块中的第一个网络加密模块的网络接口中传入,依次穿过所有网络加密模块,从最后一个网络加密模块的网络接口中传出;

所述网络加密模块能够使用所述判断机制,对从网路接口中传入的数据包进行条件判断;判断的依据包括下列的一种或多种:该数据包是否包含已加密标识、当前所述网络加密模块性能是否达到阈值、数据包某种特征是否符合过滤规则;符合条件的数据包使用所述加密功能进行处理,然后对加密后的数据包使用所述标记功能进行标记(防止后续所述网络加密模块再次对该数据进行加密)再发送出去;不符合条件的数据包使用所述透传功能直接发送出去;

通过设定合理的所述判断机制,多个所述网络加密模块能够协同分工,共同完成所有网络数据包的加密任务。

2.根据权利要求1所述的串行任务分工实现高性能网络加密的方法,其特征在于串行执行任务分工的最后一个所述网络加密模块,采用不同的所述判断机制,对所有尚未加密的数据包进行加密,防止未加密数据包透传出去的情况发生。

3.根据权利要求1所述的串行任务分工实现高性能网络加密的方法,其特征在于多个所述网络加密模块串行任务分工完成:解密、数字签名、数字签名验证、哈希运算、数据压缩、数据编解码功能中的一个或多个,原理和流程与加密操作类似。

4.根据权利要求1所述的串行任务分工实现高性能网络加密的方法,其特征在于方法不仅适用于网络接口和协议,还包括串行接口和协议、PCI-E 接口和协议等。

一种串行任务分工实现高性能网络加密的方法

技术领域

[0001] 本发明涉及一种计算机网络通讯传输加密系统和技术,以及涉及多任务负载均衡处理技术。

背景技术

[0002] 在网络数据加密应用场景中(例如 VPN 加密网关、链路加密机、透明加密网卡等应用场景),单个网络加密模块因密码运算性能有限,无法满足高并发、大带宽等高性能要求。在大部分情况中,需要使用负载均衡系统将大量数据分发到多个并行的网络加密模块中进行处理(参见附图:图1)。

[0003] 使用负载均衡系统也存在缺点:需要在网络系统中添加一个专用的负载均衡系统(以及多数情况下需要配套增加交换机),增加较大成本;另外会让网络拓扑结构变得复杂,故障点也会增加;在使用纯透明链路层加密机场景中,链路加密机本身可能没有 IP 地址和 MAC 地址,此时负载均衡器可能难以将数据包根据加密机的地址特征进行分发。

发明内容

[0004] 针对现有负载均衡系统在网络加密场景下表现出来的不足,本发明提供了一种串行任务分工机制,让网络数据流量依次串行进入多个网络加密模块,通过一定的判断机制和标记方法让多个网络加密模块共同分担和完成所有网络流量的加密任务。本方法无需传统负载均衡系统即可实现将大量网络数据包均衡的分配到多个网络加密模块中,让网络加密系统更加精简、易部署;同时也能支持纯透明链路加密模块的多节点高性能协同工作,解决多种无法部署负载均衡的场景下高性能网络加密瓶颈的问题。

[0005] 为实现上述目的,本发明提供如下技术方案:

一种串行任务分工实现高性能网络加密的方法,其特征在于,所述方法至少包含2个网络加密模块,每个网络加密模块至少包含2个网络接口,网络加密模块中还包含数据包判断机制、加密功能、透传功能,以及标记功能;多个网络加密模块之间使用网线串行连接;网络数据能够从串行的多个网络加密模块中的第一个网络加密模块的网络接口中传入,依次穿过所有网络加密模块,从最后一个网络加密模块的网络接口中传出;

所述网络加密模块能够使用预置的所述判断机制,对从网路接口中传入的数据包特征进行条件判断;判断的依据包括下列的一种或多种:该数据包是否包含已加密标识、当前所述网络加密模块性能是否达到阈值、根据数据包某种特征进行过滤匹配;符合条件的数据包使用所述加密功能进行处理,然后对加密后的数据包使用所述标记功能进行标记(防止后续所述网络加密模块再次对该数据进行加密)再发送出去;不符合条件的数据包使用所述透传功能直接发送出去;

通过设定合理的所述判断机制,多个所述网络加密模块能够协同分工,共同完成所有网络数据包的加密任务。由于加密功能所耗用的系统资源和时间,远远大于透传功能所消耗的系统资源和时间,因此本方法实现了一种类似流水线的分时分工处理机制,达到

整体提升网络加密性能的目的。

[0006] 根据一个优选的实施方式，所述的串行任务分工实现高性能网络加密的方法，其特征在于，串行执行任务分工的最后一个所述网络加密模块，采用较其他所述网络加密模块不同的所述判断机制，对所有尚未加密的数据包进行加密，防止未加密数据包透传出去的情况发生。

[0007] 根据一个优选的实施方式，所述的串行任务分工实现高性能网络加密的方法，其特征在于，多个所述网络加密模块串行任务分工完成：解密、数字签名、数字签名验证、哈希运算、数据压缩、数据编解码功能中的一个或多个，原理和流程与加密操作类似。

[0008] 根据一个优选的实施方式，所述的串行任务分工实现高性能网络加密的方法，其特征在于，不仅适用于网络接口和协议，还包括串行接口和协议、PCI-E 接口和协议等。

[0009] 综上所述，本发明与现有技术相比具有以下有益效果：

(1).无需添加专用的负载均衡系统，增加直接成本和间接成本；

(2).简化网络拓扑结构，更易组网；

(3).多个网络加密模块可以在物理或逻辑上快速整合，对外表现为一个整体形态，更易推广、销售和部署

(4).针对不具备 IP 地址和 MAC 地址的透明链路加密机来讲，大部分负载均衡器无法实现并行任务分工；本发明可满足要求

(5).对于零部件类型的网络加密模块，如：PCI-E 接口的网络加密卡来讲，额外添加传统负载均衡系统会让产品整机显得非常复杂；本发明可支持在多个PCI-E 接口的网络加密卡之间实现串行任务分工，使得整机网路加密性能数倍增强。

附图说明

[0010] 图1为传统网络加密场景使用负载均衡系统的示意图。

[0011] 图2为本发明串行任务分工实现高性能网络加密的方法的示意图。

具体实施方式

[0012] 下面结合附图和具体实施例对本发明的技术方案做进一步的说明。

[0013] 一种串行任务分工实现高性能网络加密的方法，其特征在于，所述方法至少包含2个网络加密模块，每个网络加密模块至少包含2个网络接口，网络加密模块中还包含数据包判断机制、加密功能、透传功能，以及标记功能；多个网络加密模块之间使用网线串行连接；网络数据能够从串行的多个网络加密模块中的第一个网络加密模块的网络接口中传入，依次穿过所有网络加密模块，从最后一个网络加密模块的网络接口中传出；

所述网络加密模块能够使用预置的所述判断机制，对从网路接口中传入的数据包特征进行条件判断；判断的依据包括下列的一种或多种：该数据包是否包含已加密标识、当前所述网络加密模块性能是否达到阈值、根据数据包某种特征进行过滤匹配；符合条件的数据包使用所述加密功能进行处理，然后对加密后的数据包使用所述标记功能进行标记(防止后续所述网络加密模块再次对该数据进行加密)再发送出去；不符合条件的数据包使用所述透传功能直接发送出去；

通过设定合理的所述判断机制，多个所述网络加密模块能够协同分工，共同完成

所有网络数据包的加密任务。

[0014] 实施例1：

参见图2所示，系统包含网络加密模块A 和网络加密模块 B，每个网络加密模块分别包含2个网络接口，每隔网络加密模块中还包含数据包判断机制、加密功能、透传功能，以及标记功能；A 和 B之间使用网线串行连接；网络数据能够从A的网络接口中传入，处理后在另外一个网络接口传出，再传入B 的网络接口，处理后在另外一个网络接口传出；

网络加密模块A使用预置的所述判断机制，对从网路接口中传入的数据包特征进行条件判断；判断的依据为：该数据包是否存在已加密标识、网络加密模块 A性能是否达到阈值；符合条件的数据包（不存在已加密标识，且本模块性能未达到阈值）使用加密功能进行处理，然后对加密后的数据包使用所述标记功能进行标记（防止后续所述网络加密模块再次对该数据进行加密）再发送出去；不符合条件的数据包（已经加密过了，或本模块当前性能达到阈值）使用所述透传功能直接发送出去；

从网络加密模块A 中传出的数据包中，部分经过了加密并打上了标记，部分尚未加密；这些数据包继续传递到网络加密模块 B 中。网络加密模块B 会使用类似的判断机制，对符合条件的数据包进行加密并打上标识，最后所有数据包都将从B 的网络接口中传出来。

[0015] 至此，网络加密模块A 和 B 协同完成了网络数据包的加密处理，分时分工提升了整个网络加密的效率。

[0016] 实施例2：

与实施例1相似，区别是：网络数据包从网络加密模块A 中传出并再传入网络加密模块 B 时，网络加密模块B 会使用不同的判断机制，对所有尚未加密的数据包进行加密并打上标识，最后所有数据包都将从B 的网络接口中传出来。

[0017] 至此，网络加密模块A 和 B 协同完成了所有网络数据包的加密处理，分时分工提升了整个网络加密的效率：

需要注意的是，上述具体实施方式是示例性的，本领域技术人员可以在本发明公开内容的启发下想出各种解决方案，以及对本发明的各项权利进行非实质性改变，特别是参考本方法完成不同类型的数据运算，或使用其他更多所述判断机制，以及使用不同的传输协议；而这些解决方案和改变也都属于本发明的公开范围并落入本发明的保护范围之内。本领域技术人员应该明白，本发明说明书及其附图均为说明性而并非构成对权利要求的限制。本发明的保护范围由权利要求及其等同物限定。

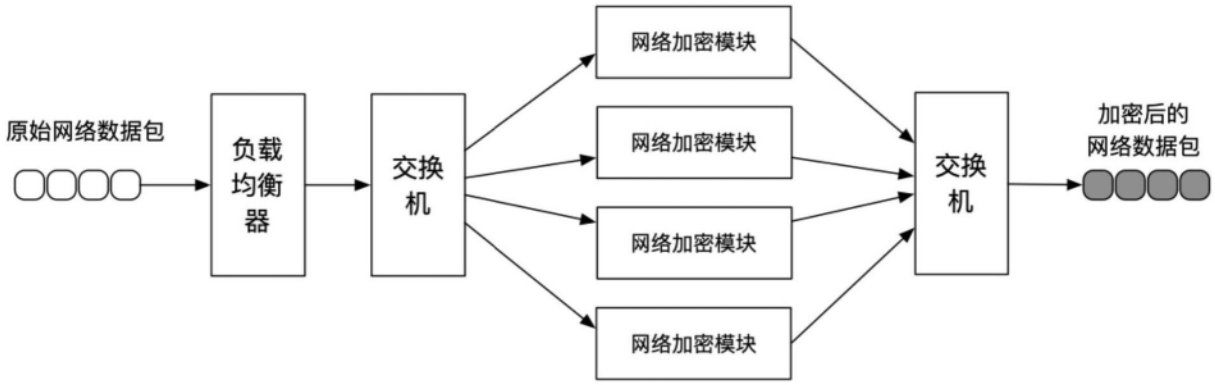

原始网络数据包
负载均衡器
交换机
网络加密模块
网络加密模块
网络加密模块
网络加密模块
交换机
加密后的网络数据包

图1

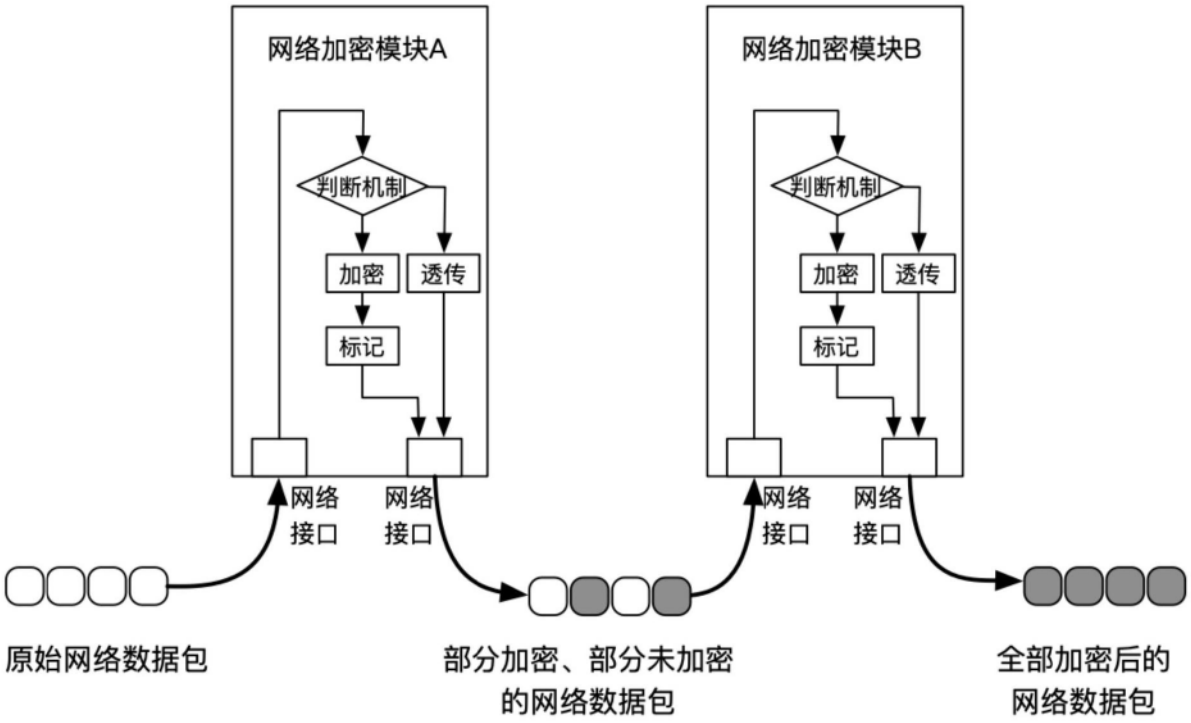

网络加密模块A
判断机制
加密
透传
标记
网络接口
网络接口
网络加密模块B
判断机制
加密
透传
标记
网络接口
网络接口
原始网络数据包
部分加密、部分未加密的网络数据包
全部加密后的网络数据包

图2