(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 110535861 B
(45)授权公告日 2022.01.25

(21)申请号 201910812854.2
(22)申请日 2019.08.30
(65)同一申请的已公布的文献号
申请公布号 CN 110535861 A
(43)申请公布日 2019.12.03
(73)专利权人 杭州迪普信息技术有限公司
地址 310051 浙江省杭州市滨江区西兴街道通和路68号中财大厦11楼A区05室
(72)发明人 米岩 王喆
(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 陈蕾
(51)Int.Cl.
H04L 9/40(2022.01)

(56)对比文件
CN 109889550 A,2019.06.14
CN 107634971 A,2018.01.26
CN 105991632 A,2016.10.05
CN 105791248 A,2016.07.20
CN 102291441 A,2011.12.21
CN 107547507 A,2018.01.05
CN 108768942 A,2018.11.06
CN 101369973 A,2009.02.18
US 10284594 B2,2019.05.07
CN 110071939 A,2019.07.30
WO 2009003851 A2,2009.01.08
US 7426634 B2,2008.09.16
CN 105262691 A,2016.01.20
CN 101170402 A,2008.04.30
CN 107959690 A,2018.04.24
US 10116693 B1,2018.10.30

审查员 徐思毅

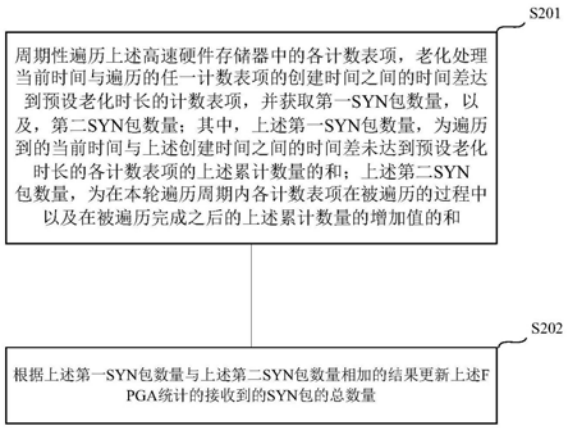
权利要求书3页 说明书15页 附图2页

(54)发明名称

一种识别SYN攻击行为中统计SYN包数量的方法及装置

(57)摘要

本申请提供一种识别SYN攻击行为中统计SYN包数量的方法，应用于网络设备，所述网络设备包括用于统计接收到的SYN包的总数量的FPGA；以及，与所述FPGA连接的高速硬件存储器；该方法包括：周期性遍历所述高速硬件存储器中的各计数表项，老化处理当前时间与遍历的任一计数表项的创建时间之间的时间差达到预设老化时长的计数表项，并获取第一SYN包数量，以及，第二SYN包数量；根据所述第一SYN包数量与所述第二SYN包数量相加的结果更新所述FPGA统计的接收到的SYN包的总数量。



CN 110535861 B

1.一种识别SYN攻击行为中统计SYN包数量的方法,应用于网络设备,其特征在于,所述网络设备包括用于统计接收到的SYN包的总数量的FPGA;以及,与所述FPGA连接的高速硬件存储器;其中,所述高速硬件存储器存储了与接收到的SYN包的源IP对应的若干计数表项;所述计数表项包括表项创建时间、源IP和接收到的与所述源IP对应的SYN包的累计数量;所述方法包括:

周期性遍历所述高速硬件存储器中的各计数表项,老化处理当前时间与遍历的任一计数表项的创建时间之间的时间差达到预设老化时长的计数表项,并获取第一SYN包数量,以及,第二SYN包数量;其中,所述第一SYN包数量,为遍历到的当前时间与所述创建时间之间的时间差未达到预设老化时长的各计数表项的所述累计数量的和;所述第二SYN包数量,为在本轮遍历周期内各计数表项在被遍历的过程中以及在被遍历完成之后的所述累计数量的增加值的和;

根据所述第一SYN包数量与所述第二SYN包数量相加的结果更新所述FPGA统计的接收到的SYN包的总数量。

2.根据权利要求1所述的方法,其特征在于,所述获取第一SYN包数量,包括:

确定当前时间与遍历的计数表项的创建时间之间的时间差是否达到预设老化时长;

如果当前时间与遍历的任一计数表项的创建时间未达到预设老化时长,则记录该计数表项中的所述累计数量;以及,对记录的各计数表项的所述累计数量进行累加,得到所述第一SYN包数量。

3.根据权利要求1所述的方法,其特征在于,所述高速硬件存储器预先被划分为若干个与计数表项一一对应的存储地址单元;所述网络设备中预设了第一纠错计数器;所述获取第二SYN包数量包括:

确定在本轮遍历周期内待写入所述高速硬件存储器的SYN包的源IP对应的目标计数表项的存储地址,是否小于等于当前正在遍历的计数表项的存储地址;如果是,更新所述目标计数表项的累计数量,并将预设的第一纠错计数器的计数结果加一;所述本轮遍历周期,为从所述FPGA向所述高速硬件存储器发送第一个存储地址读命令的时刻开始至所述FPGA接收到所述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束;

在本轮遍历周期结束后,读取所述第一纠错计数器的计数结果,得到所述第二SYN包数量。

4.根据权利要求1所述的方法,其特征在于,所述高速硬件存储器预先被划分为若干个与计数表项一一对应的存储地址单元;所述网络设备中预设了第二纠错计数器;所述获取第二SYN包数量包括:

确定与在本轮遍历周期内待写入所述高速硬件存储器的SYN包的源IP对应的目标计数表项的存储地址,是否小于当前正在遍历的计数表项的下一计数表项的存储地址;如果是,更新所述目标计数表项的累计数量,并将预设的第二纠错计数器的计数结果加一;所述本轮遍历周期,为从所述FPGA向所述高速硬件存储器发送第一个存储地址读命令的时刻开始至所述FPGA接收到所述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束;

在本轮遍历结束后,读取所述第二纠错计数器的计数结果,得到所述第二SYN包数量。

5.根据权利要求4所述的方法,其特征在于,所述网络设备中还预设了第三纠错计数器;所述方法还包括:

在本轮遍历周期内遍历最后一个存储地址单元的过程中，每当所述高速硬件存储器被写入一个SYN包时，将预设的第三纠错计数器的计数结果加一；

将所述第二纠错计数器与所述第三纠错计数器的计数结果相加，得到所述第二SYN包数量。

6.根据权利要求5所述的方法，其特征在于，所述在本轮遍历周期内遍历最后一个存储地址单元的过程包括：

从所述FPGA向所述高速硬件存储器发送最后一个存储地址的读命令的时刻开始至所述FPGA接收到所述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束。

7.一种识别SYN攻击行为中统计SYN包数量的装置，应用于网络设备，其特征在于，所述网络设备包括用于统计接收到的SYN包的总数量的FPGA；以及，与所述FPGA连接的高速硬件存储器；其中，所述高速硬件存储器存储了与接收到的SYN包的源IP对应的若干计数表项；所述计数表项包括表项创建时间、源IP和接收到的与所述源IP对应的SYN包的累计数量；所述装置包括：

周期性遍历模块，周期性遍历所述高速硬件存储器中的各计数表项，老化处理当前时间与遍历的任一计数表项的创建时间之间的时间差达到预设老化时长的计数表项，并获取第一SYN包数量，以及，第二SYN包数量；其中，所述第一SYN包数量，为遍历到的当前时间与所述创建时间之间的时间差未达到预设老化时长的各计数表项的所述累计数量的和；所述第二SYN包数量，为在本轮遍历周期内各计数表项在被遍历的过程中以及在被遍历完成之后的所述累计数量的增加值的和；

更新SYN包总数量模块，根据所述第一SYN包数量与所述第二SYN包数量相加的结果更新所述FPGA统计的接收到的SYN包的总数量。

8.根据权利要求7所述的装置，其特征在于，所述周期性遍历模块，还包括：

获取第一SYN包数量模块，确定当前时间与遍历的计数表项的创建时间之间的时间差是否达到预设老化时长；

如果当前时间与遍历的任一计数表项的创建时间未达到预设老化时长，则记录该计数表项中的所述累计数量；以及，对记录的各计数表项的所述累计数量进行累加，得到所述第一SYN包数量。

9.根据权利要求7所述的装置，其特征在于，所述高速硬件存储器预先被划分为若干个与计数表项一一对应的存储地址单元；所述网络设备中预设了第一纠错计数器；所述周期性遍历模块，还包括：

获取第二SYN包数量模块，确定在本轮遍历周期内待写入所述高速硬件存储器的SYN包的源IP对应的目标计数表项的存储地址，是否小于等于当前正在遍历的计数表项的存储地址；如果是，更新所述目标计数表项的累计数量，并将预设的第一纠错计数器的计数结果加一；所述本轮遍历周期，为从所述FPGA向所述高速硬件存储器发送第一个存储地址读命令的时刻开始至所述FPGA接收到所述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束；

在本轮遍历周期结束后，读取所述第一纠错计数器的计数结果，得到所述第二SYN包数量。

10.根据权利要求7所述的装置，其特征在于，所述高速硬件存储器预先被划分为若干

个与计数表项一一对应的存储地址单元;所述网络设备中预设了第二纠错计数器;所述周期性遍历模块,还包括:

获取第二SYN包数量模块,确定与在本轮遍历周期内待写入所述高速硬件存储器的SYN包的源IP对应的目标计数表项的存储地址,是否小于当前正在遍历的计数表项的下一计数表项的存储地址;如果是,更新所述目标计数表项的累计数量,并将预设的第二纠错计数器的计数结果加一;所述本轮遍历周期,为从所述FPGA向所述高速硬件存储器发送第一个存储地址读命令的时刻开始至所述FPGA接收到所述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束;

在本轮遍历结束后,读取所述第二纠错计数器的计数结果,得到所述第二SYN包数量。

11.根据权利要求10所述的装置,其特征在于,所述网络设备中还预设了第三纠错计数器;所述周期性遍历模块,还包括:

获取遍历过程漏计的SYN包数量模块,在本轮遍历周期内遍历最后一个存储地址单元的过程中,每当所述高速硬件存储器被写入一个SYN包时,将预设的第三纠错计数器的计数结果加一;

将所述第二纠错计数器与所述第三纠错计数器的计数结果相加,得到所述第二SYN包数量。

12.根据权利要求11所述的装置,其特征在于,所述在本轮遍历周期内遍历最后一个存储地址单元的过程包括:

从所述FPGA向所述高速硬件存储器发送最后一个存储地址的读命令的时刻开始至所述FPGA接收到所述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束。

一种识别SYN攻击行为中统计SYN包数量的方法及装置

技术领域

[0001] 本申请涉及计算机技术领域，尤其涉及一种识别SYN攻击行为中统计SYN包数量的方法及装置。

背景技术

[0002] 当今通信领域中，客户端与服务端间通常使用TCP协议(面向连接的、可靠的、基于字节流的传输层通信协议)进行数据交互。客户端与服务端建立TCP连接时会进行三次握手，首先，客户端发送SYN包至服务端，完成客户端与服务端的第一次握手；服务端响应于上述SYN包，向上述客户端返回SYN包和ACK包，完成客户端与服务端的第二次握手；上述服务端在完成向上述客户端返回SYN包和ACK包后将一直处于等待状态，直至接收到上述客户端发送的ACK包，完成客户端与服务端的第三次握手。当客户端与服务端完成上述三次握手后，可以相互传输数据。

[0003] 现实中，许多黑客在短时期内伪造大量不存在的IP，并将上述IP封装至客户端向服务端发送的SYN包中。当服务端接收到客户端发送的上述SYN包后，将向客户端返回SYN包和ACK包(第二次握手)，并等待客户端之后发送的ACK包，但是，由于上述SYN包中的源IP是不存在的，因此，服务端发出SYN包和ACK包后将不会得到任何客户端响应，从而导致服务端一种处于等待状态，不能正常工作，引起网络堵塞和服务端系统瘫痪(以下简称SYN攻击)。

[0004] 目前，为了防止服务端遭受SYN攻击，服务端通常将连接能够识别SYN攻击的网络设备。如果上述网络设备确定自身当前正在遭受到SYN攻击时，则停止向与自身连接的服务端转发客户端发送的SYN包，以使服务端避免遭受SYN攻击。

[0005] 实际应用中，为了识别SYN攻击行为，上述网络设备通常判断在一段间隔时长(例如，周期性启动老化机制的时间间隔)内经过该网络设备的SYN包的数量是否达到预设阈值，并当上述网络设备确定在一段间隔时长内经过该网络设备的SYN包的数量突破预设阈值时，确定自身正在遭受SYN攻击。

[0006] 由上可见，在上述网络设备中，需要一种记录SYN包数量的方法，以使网络设备能够识别服务端是否遭受SYN攻击。

发明内容

[0007] 有鉴于此，本申请提供一种识别SYN攻击行为中统计SYN包数量的方法，应用于网络设备，上述网络设备包括用于统计接收到的SYN包的总数量的FPGA；以及，与上述FPGA连接的高速硬件存储器；其中，上述高速硬件存储器存储了与接收到的SYN包的源IP对应的若干计数表项；上述计数表项包括表项创建时间、源IP和接收到的与上述源IP对应的SYN包的累计数量；上述方法包括：

[0008] 周期性遍历上述高速硬件存储器中的各计数表项，老化处理当前时间与遍历的任一计数表项的创建时间之间的时间差达到预设老化时长的计数表项，并获取第一SYN包数量，以及，第二SYN包数量；其中，上述第一SYN包数量，为遍历到的当前时间与上述创建时间

之间的时间差未达到预设老化时长的各计数表项的上述累计数量的和;上述第二SYN包数量,为在本轮遍历周期内各计数表项在被遍历的过程中以及在被遍历完成之后的上述累计数量的增加值的和;

[0009] 根据上述第一SYN包数量与上述第二SYN包数量相加的结果更新上述FPGA统计的接收到的SYN包的总数量。

[0010] 在示出的一实施例中,上述获取第一SYN包数量,包括:

[0011] 确定当前时间与遍历的计数表项的创建时间之间的时间差是否达到预设老化时长;

[0012] 如果当前时间与遍历的任一计数表项的创建时间未达到预设老化时长,则记录该计数表项中的上述累计数量;以及,对记录的各计数表项的上述累计数量进行累加,得到上述第一SYN包数量。

[0013] 在示出的一实施例中,上述高速硬件存储器预先被划分为若干个与计数表项一一对应的存储地址单元;上述网络设备中预设了第一纠错计数器;上述获取第二SYN包数量包括:

[0014] 确定在本轮遍历周期内待写入上述高速硬件存储器的SYN包的源IP对应的目标计数表项的存储地址,是否小于等于当前正在遍历的计数表项的存储地址;如果是,更新上述目标计数表项的累计数量,并将预设的第一纠错计数器的计数结果加一;上述本轮遍历周期,为从上述FPGA向上述高速硬件存储器发送第一个存储地址读命令的时刻开始至上述FPGA接收到上述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束;

[0015] 在本轮遍历周期结束后,读取上述第一纠错计数器的计数结果,得到上述第二SYN包数量。

[0016] 在示出的一实施例中,上述高速硬件存储器预先被划分为若干个与计数表项一一对应的存储地址单元;上述网络设备中预设了第二纠错计数器;上述获取第二SYN包数量包括:

[0017] 确定与在本轮遍历周期内待写入上述高速硬件存储器的SYN包的源IP对应的目标计数表项的存储地址,是否小于当前正在遍历的计数表项的下一计数表项的存储地址;如果是,更新上述目标计数表项的累计数量,并将预设的第二纠错计数器的计数结果加一;上述本轮遍历周期,为从上述FPGA向上述高速硬件存储器发送第一个存储地址读命令的时刻开始至上述FPGA接收到上述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束;

[0018] 在本轮遍历结束后,读取上述第二纠错计数器的计数结果,得到上述第二SYN包数量。

[0019] 在示出的一实施例中,上述网络设备中还预设了第三纠错计数器;上述方法还包括:

[0020] 在本轮遍历周期内遍历最后一个存储地址单元的过程中,每当上述高速硬件存储器被写入一个SYN包时,将预设的第三纠错计数器的计数结果加一;上述在本轮遍历周期内遍历最后一个存储地址单元的过程中,为从上述FPGA向上述高速硬件存储器发送最后一个存储地址的读命令的时刻开始至上述FPGA接收到上述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束;

[0021] 将上述第二纠错计数器与上述第三纠错计数器的计数结果相加，得到上述第二SYN包数量。

[0022] 在示出的一实施例中，上述在本轮遍历周期内遍历最后一个存储地址单元的过程包括：

[0023] 从上述FPGA向上述高速硬件存储器发送最后一个存储地址的读命令的时刻开始至上述FPGA接收到上述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束。

[0024] 本申请还提供一种识别SYN攻击行为中统计SYN包数量的装置，应用于网络设备，上述网络设备包括用于统计接收到的SYN包的总数量的FPGA；以及，与上述FPGA连接的高速硬件存储器；其中，上述高速硬件存储器存储了与接收到的SYN包的源IP对应的若干计数表项；上述计数表项包括表项创建时间、源IP和接收到的与上述源IP对应的SYN包的累计数量；上述装置包括：

[0025] 周期性遍历模块，周期性遍历上述高速硬件存储器中的各计数表项，老化处理当前时间与遍历的任一计数表项的创建时间之间的时间差达到预设老化时长的计数表项，并获取第一SYN包数量，以及，第二SYN包数量；其中，上述第一SYN包数量，为遍历到的当前时间与上述创建时间之间的时间差未达到预设老化时长的各计数表项的上述累计数量的和；上述第二SYN包数量，为在本轮遍历周期内各计数表项在被遍历的过程中以及在被遍历完成之后的上述累计数量的增加值的和；

[0026] 更新SYN包总数量模块，根据上述第一SYN包数量与上述第二SYN包数量相加的结果更新上述FPGA统计的接收到的SYN包的总数量。

[0027] 在示出的一实施例中，上述周期性遍历模块，还包括：

[0028] 获取第一SYN包数量模块，确定当前时间与遍历的计数表项的创建时间之间的时间差是否达到预设老化时长；

[0029] 如果当前时间与遍历的任一计数表项的创建时间未达到预设老化时长，则记录该计数表项中的上述累计数量；以及，对记录的各计数表项的上述累计数量进行累加，得到上述第一SYN包数量。

[0030] 在示出的一实施例中，上述高速硬件存储器预先被划分为若干个与计数表项一一对应的存储地址单元；上述网络设备中预设了第一纠错计数器；上述周期性遍历模块，还包括：

[0031] 获取第二SYN包数量模块，确定在本轮遍历周期内待写入上述高速硬件存储器的SYN包的源IP对应的目标计数表项的存储地址，是否小于等于当前正在遍历的计数表项的存储地址；如果是，更新上述目标计数表项的累计数量，并将预设的第一纠错计数器的计数结果加一；上述本轮遍历周期，为从上述FPGA向上述高速硬件存储器发送第一个存储地址读命令的时刻开始至上述FPGA接收到上述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束；

[0032] 在本轮遍历周期结束后，读取上述第一纠错计数器的计数结果，得到上述第二SYN包数量。

[0033] 在示出的一实施例中，上述高速硬件存储器预先被划分为若干个与计数表项一一对应的存储地址单元；上述网络设备中预设了第二纠错计数器；上述周期性遍历模块，还包括：

[0034] 获取第二SYN包数量模块，确定与在本轮遍历周期内待写入上述高速硬件存储器的SYN包的源IP对应的目标计数表项的存储地址，是否小于当前正在遍历的计数表项的下一计数表项的存储地址；如果是，更新上述目标计数表项的累计数量，并将预设的第二纠错计数器的计数结果加一；上述本轮遍历周期，为从上述FPGA向上述高速硬件存储器发送第一个存储地址读命令的时刻开始至上述FPGA接收到上述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束；

[0035] 在本轮遍历结束后，读取上述第二纠错计数器的计数结果，得到上述第二SYN包数量。

[0036] 在示出的一实施例中，上述网络设备中还预设了第三纠错计数器；上述周期性遍历模块，还包括：

[0037] 获取遍历过程漏计的SYN包数量模块，在本轮遍历周期内遍历最后一个存储地址单元的过程中，每当上述高速硬件存储器被写入一个SYN包时，将预设的第三纠错计数器的计数结果加一；上述在本轮遍历周期内遍历最后一个存储地址单元的过程中，为从上述FPGA向上述高速硬件存储器发送最后一个存储地址的读命令的时刻开始至上述FPGA接收到上述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束；

[0038] 将上述第二纠错计数器与上述第三纠错计数器的计数结果相加，得到上述第二SYN包数量。

[0039] 在示出的一实施例中，上述在本轮遍历周期内遍历最后一个存储地址单元的过程包括：

[0040] 从上述FPGA向上述高速硬件存储器发送最后一个存储地址的读命令的时刻开始至上述FPGA接收到上述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束。

[0041] 由上述记载的技术方案可知，一方面，由于上述网络设备包括用于统计接收到的SYN包的总数量的FPGA；以及，与上述FPGA连接的高速硬件存储器；其中，上述高速硬件存储器存储了与接收到的SYN包的源IP对应的若干计数表项；上述计数表项包括表项创建时间、源IP和接收到的与上述源IP对应的SYN包的累计数量，因此，当上述网络设备监听到在一段间隔时长内上述FPGA统计的接收到的SYN包的总数量突破预设阈值时，则可以确认自身正在遭受SYN攻击，并且，上述网络设备可以在确定自身遭受到SYN攻击后，将统计的上述累计数量的增长速率大于预设值的计数表项对应的源IP确定为SYN攻击包的源IP。

[0042] 另一方面，由于网络设备周期性遍历上述高速硬件存储器中的各计数表项，老化处理当前时间与遍历的任一计数表项的创建时间之间的时间差达到预设老化时长的计数表项，并且将遍历到的当前时间与上述创建时间之间的时间差未达到预设老化时长的各计数表项的上述累计数量的和，以及，在本轮遍历周期内各计数表项在被遍历的过程中以及在被遍历完成之后的上述累计数量的增加值的和相加的结果更新为上述FPGA统计的接收到的SYN包的总数量，因此，使得上述FPGA统计的接收到的SYN包的总数量可以与上述各计数表项的计数结果的和保持同步增减，不会一直累加，从而避免了上述网络设备由于上述FPGA统计的接收到的SYN包的总数量一直累加直至突破预设阈值而导致的误以为自身正在遭受SYN攻击的误判。

附图说明

[0043] 图1为本说明书示出的一种网络设备的结构图；

[0044] 图2为本申请提出的一种识别SYN攻击行为中统计SYN包数量的方法的流程图；

[0045] 图3为本说明书示出的一种识别SYN攻击行为中统计SYN包数量的装置的结构图。

具体实施方式

[0046] 下面将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的设备和方法的例子。

[0047] 在本申请使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“上述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。还应当理解，本文中所使用的词语“如果”，取决于语境，可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0048] 在实际应用中，为了使网络设备可以识别SYN攻击行为，网络设备中通常将设置统计接收到的SYN包总数量的计数器(以下简称总计数器)，并建立周期性清除上述总计数器上的计数的老化机制。在上述情形下，如果该网络设备确定在一段间隔时长(例如，周期性启动老化机制的时间间隔)内该总计数器记录的SYN包总数量突破预设阈值，则该网络设备确认自身正在遭受SYN攻击。

[0049] 而为了获取SYN攻击包的源IP，网络设备中通常还设置了若干个统计与接收到的SYN包的源IP对应的SYN包的累计数量的计数表项，上述计数表项包括表项创建时间、源IP和接收到的与上述源IP对应的SYN包的累计数量。当上述网络设备确定自身正在遭受SYN攻击时，可以根据各计数表项的计数结果的变化情况来确定SYN攻击包的源IP。例如，网络设备可以将统计的上述累计数量增长速率大于预设值的计数表项对应的源IP确定为SYN攻击包的源IP。

[0050] 在实际应用中，为了保证总计数器中的计数结果不会一直累加，而是与各计数表项上的计数结果的和保持同步增减，且上述网络设备在未遭受SYN攻击时，该计数结果不会突破预设阈值的动态平衡状态，上述网络设备中将建立另一种老化机制。上述老化机制可以是，上述网络设备通常周期性遍历各计数表项，并在遍历周期内判断当前时间与各计数表项创建时间之间的时间差是否达到老化时长(该老化时长可以在网络设备中预先设置)。当上述网络设备在上述遍历周期内确定当前时间与各计数表项创建时间之间的时间差达到上述老化时长的计数表项时，则将上述总计数器中的计数结果减去该计数表项上的计数结果，并将该计数表项上的计数结果清零，以此来保证总计数器中的计数结果不会一直累加，而是与各计数表项上的计数结果的和保持同步增减以处于上述动态平衡状态，从而使上述网络设备在未遭受SYN攻击时，上述总计数器中的计数不会突破预设阈值。

[0051] 在此，需要说明的是，上述总计数器设置的位置可以是网络设备的CPU、FPGA或其他位置；上述计数表项设置的位置可以是网络设备的CPU、FPGA或高速硬件存储器中。

[0052] 以下，结合具体场景进行说明。

[0053] 请参见图1,图1为本说明书示出的一种网络设备的结构图。

[0054] 如图1所示,网络设备采用CPU(Central Processing Uint,中央处理器)与FPGA(Field-Programmable Gate Array,现场可编程门阵列)的异构架构,上述FPGA与高速硬件存储器通信连接。

[0055] 上述FPGA,可以处理上述网络设备接收到的SYN包。当上述网络设备接收到SYN包时,上述FPGA可以更新自身统计的额该网络设备接收到的SYN包的总数量。例如,上述FPGA中可以设置总计数器,用于统计接收到的SYN包的总数量。上述FPGA还可以获取上述接收到的SYN包的源IP,并在获取到上述源IP后与上述高速硬件存储器进行通信以使上述高速硬件存储器将上述FPGA接收的SYN包存储起来。

[0056] 上述高速硬件存储器,可以存储与接收到的SYN包的源IP对应的若干计数表项;上述计数表项包括表项创建时间、源IP和接收到的与上述源IP对应的SYN包的累计数量(以下简称计数结果)。

[0057] 例如,上述高速硬件存储器预先被划分为若干个与计数表项一一对应的存储地址单元,上述存储地址单元可以存储上述计数表项。在上述情况下,当上述FPGA接收到SYN包时,上述FPGA可以获取该SYN包的源IP,并通过该源IP进一步判断该SYN包是否为首次进入网络设备的SYN包,如果该SYN包为首次进入网络设备的SYN包,则上述FPGA可以向上述高速硬件存储器发送在未存储计数表项的存储地址单元上创建计数表项的命令,并将上述新创建的计数表项上的计数结果更新为一;如果该SYN包不是首次进入网络设备的SYN包,则上述FPGA可以获取与该SYN包的源IP对应的计数表项的计数结果,并将该计数加一后重新写入该计数表项。

[0058] 上述网络设备,可以预先设置预设阈值。如果上述网络设备在一段间隔时长(例如,周期性启动老化机制的时间间隔)内监听到上述FPGA统计的该网络设备接收到的SYN包的总数量突破上述预设阈值时,则确定自身正在遭受SYN攻击。例如,上述网络设备的CPU或FPGA可以监听FPGA中的总计数器的计数结果在一段间隔时长内是否突破上述预设阈值,并在监听到该总计数器的计数结果在一段间隔时长内突破上述预设阈值时,确定上述网络设备正在遭受SYN攻击。

[0059] 上述网络设备可以存在老化机制。例如,上述网络设备周期性遍历上述高速硬件存储器所有的存储地址单元,并在遍历周期内判断当前时间与各计数表项创建时间之间的时间差是否达到老化时长(该老化时长可以在网络设备中预先设置)。当上述网络设备在上述遍历周期内确定当前时间与各计数表项创建时间之间的时间差达到上述老化时长的计数表项时,则将上述FPGA中的总计数器中的计数结果减去该计数表项上的计数结果,并将该计数表项上的计数结果清零,以此来保证总计数器中的计数结果不会一直累加,而是与各计数表项上的计数结果的和保持同步增减以处于上述动态平衡状态,以使上述网络设备在未遭受SYN攻击时,上述总计数器中的计数不会突破预设阈值。

[0060] 由于上述网络设备可以监听该网络设备在一段间隔时长(例如,周期性启动老化机制的时间间隔)内接收的SYN包的总数量是否突破上述预设阈值,并在监听到上述总网络设备在一段间隔时长内接收的SYN包的总数量突破上述预设阈值后,确定上述网络设备正在遭受SYN攻击,并且,上述网络设备可以在确定自身遭受到SYN攻击后,可以将上述高速硬件存储器中统计的上述累计数量增长速率大于预设值的计数表项对应的源IP确定为SYN攻

击包的源IP;因此,上述网络设备可以识别SYN攻击行为,并获取上述SYN攻击包的源IP。

[0061] 当然,该网络设备在获取上述SYN攻击包的源IP后,可以将该源IP作为加入过滤黑名单,以使网络设备可以过滤掉包含该源IP的SYN包,从而有效防止服务端遭受SYN攻击。

[0062] 而实际应用中,当流经上述网络设备的SYN包数量过大时,上述FPGA仍然可以准确记录流经上述网络设备的SYN包的数量;但是,当上述FPGA在将接收到的SYN包写入上述高速硬件存储器时,将可能由于上述高速硬件存储器处理速度较慢,使上述FPGA向上述高速硬件存储器发送的待写入的SYN包不能完全存储至上述高速硬件存储器中,而造成的SYN包漏计。

[0063] 在上述情况下,上述FPGA统计的网络设备接收到的SYN包的总数量与上述高速硬件存储器中各计数表项的计数结果的和之间的差值将越来越大;上述FPGA统计的网络设备接收到的SYN包的总数量将不会与上述各计数表项的计数结果的和保持同步增减,因此,上述FPGA统计的网络设备接收到的SYN包的总数量将一直累加;从而导致,在网络设备正常工作时,FPGA统计的网络设备接收到的SYN包的总数量的计数结果有可能由于不断累加而突破预设阈值,造成网络设备误以为自身正在遭受SYN攻击的误判。

[0064] 基于此,本申请提出一种识别SYN攻击行为中统计SYN包数量的方法,应用于网络设备。

[0065] 上述网络设备采用CPU(Central Processing Uint,中央处理器)与FPGA(Field-Programmable Gate Array,现场可编程门阵列)的异构架构,上述FPGA与高速硬件存储器通信连接。

[0066] 该方法通过周期性地获取上述高速硬件存储器中存储的SYN包数量,并根据获取到的SYN包数量,更新上述FPGA中统计的接收到的SYN包的总数量,以保证上述FPGA中统计的接收到的SYN包的总数量与上述高速硬件存储器中的存储的SYN包数量保持一致。

[0067] 请参见图2,图2为本申请提出的一种识别SYN攻击行为中统计SYN包数量的方法的流程图。应用于网络设备,上述网络设备包括用于统计接收到的SYN包的总数量的FPGA;以及,与上述FPGA连接的高速硬件存储器;其中,上述高速硬件存储器存储了与接收到的SYN包的源IP对应的若干计数表项;上述计数表项包括表项创建时间、源IP和接收到的与上述源IP对应的SYN包的累计数量;

[0068] S201,周期性遍历上述高速硬件存储器中的各计数表项,老化处理当前时间与遍历的任一计数表项的创建时间之间的时间差达到预设老化时长的计数表项,并获取第一SYN包数量,以及,第二SYN包数量;其中,上述第一SYN包数量,为遍历到的当前时间与上述创建时间之间的时间差未达到预设老化时长的各计数表项的上述累计数量的和;上述第二SYN包数量,为在本轮遍历周期内各计数表项在被遍历的过程中以及在被遍历完成之后的上述累计数量的增加值的和;

[0069] S202,根据上述第一SYN包数量与上述第二SYN包数量相加的结果更新上述FPGA统计的接收到的SYN包的总数量。

[0070] 需要说明的是,上述S201与S202的步骤可以由网络设备的CPU、FPGA或者其他控制器件单独完成、也可以由网络设备中的各控制器件(CPU、FPGA等控制器件)配合完成,在此不作限定。

[0071] 由上述记载的技术方案可知,一方面,由于上述网络设备包括用于统计接收到的

SYN包的总数量的FPGA;以及,与上述FPGA连接的高速硬件存储器;其中,上述高速硬件存储器存储了与接收到的SYN包的源IP对应的若干计数表项;上述计数表项包括表项创建时间、源IP和接收到的与上述源IP对应的SYN包的累计数量,因此,当上述网络设备监听到在一段间隔时长内上述FPGA统计的接收到的SYN包的总数量突破预设阈值时,则可以确认自身正在遭受SYN攻击,并且,上述网络设备可以在确定自身遭受到SYN攻击后,将统计的上述累计数量的增长速率大于预设值的计数表项对应的源IP确定为SYN攻击包的源IP。

[0072] 另一方面,由于网络设备周期性遍历上述高速硬件存储器中的各计数表项,老化处理当前时间与遍历的任一计数表项的创建时间之间的时间差达到预设老化时长的计数表项,并且将遍历到的当前时间与上述创建时间之间的时间差未达到预设老化时长的各计数表项的上述累计数量的和,以及,在本轮遍历周期内各计数表项在被遍历的过程中以及在被遍历完成之后的上述累计数量的增加值的和相加的结果更新为上述FPGA统计的接收到的SYN包的总数量,因此,使得上述FPGA统计的接收到的SYN包的总数量可以与上述各计数表项的计数结果的和保持同步增减,不会一直累加,从而避免了上述网络设备由于上述FPGA统计的接收到的SYN包的总数量一直累加直至突破预设阈值而导致的误以为自身正在遭受SYN攻击的误判。

[0073] 以下结合具体的实施例对本申请记载的技术方案进行说明。

[0074] 在本申请示出的一实施例中,网络设备的结构图如图1所示,上述网络设备采用CPU(Central Processing Uint,中央处理器)与FPGA(Field-Programmable Gate Array,现场可编程门阵列)的异构架构,上述FPGA与高速硬件存储器通信连接。

[0075] 上述FPGA,可以处理上述网络设备接收到的SYN包。当上述网络设备接收到SYN包时,上述FPGA可以更新自身统计的额该网络设备接收到的SYN包的总数量,并与上述高速硬件存储器进行通信以使上述高速硬件存储器将上述FPGA接收的SYN包存储起来。

[0076] 例如,上述FPGA中可以设置总计数器,用于统计接收到的SYN包总数量。上述FPGA还可以获取上述接收到的SYN包的源IP,并在获取到上述源IP后与上述高速硬件存储器进行通信以使上述高速硬件存储器将上述FPGA接收的SYN包存储起来。

[0077] 上述高速硬件存储器,可以存储与接收到的SYN包的源IP对应的若干计数表项;上述计数表项包括表项创建时间、源IP和接收到的与上述源IP对应的SYN包的累计数量(以下简称计数表项的计数结果)。

[0078] 例如,上述高速硬件存储器预先被划分为若干个与计数表项一一对应的存储地址单元,上述存储地址单元可以存储上述计数表项。在上述情况下,当上述FPGA接收到SYN包时,可以获取该SYN包的源IP,并通过该源IP进一步判断该SYN包是否为首次进入网络设备的SYN包,如果该SYN包为首次进入网络设备的SYN包,则上述FPGA可以向上述高速硬件存储器发送在未存储计数表项的存储地址单元上创建计数表项的命令,并将上述新创建的计数表项上的计数结果更新为一;如果该SYN包不是首次进入网络设备的SYN包,则上述FPGA可以获取与该SYN包的源IP对应的计数表项的计数结果,并将该计数加一后重新写入该计数表项。

[0079] 上述网络设备,可以预先设置预设阈值。如果上述网络设备在一段间隔时长(例如,周期性启动老化机制的时间间隔)内监听到上述FPGA统计的该网络设备接收到的SYN包的总数量突破上述预设阈值时,则确定自身正在遭受SYN攻击。

[0080] 例如，上述网络设备的CPU或FPGA可以监听FPGA中的总计数器的计数结果在一段间隔时长内是否突破上述预设阈值，并在监听到该总计数器的计数结果在一段间隔时长内突破上述预设阈值时，确定上述网络设备正在遭受SYN攻击。需要说明的是，上述预设阈值可以是管理人员自行设定，也可以是网络设备根据现场运行环境自行生成，在此不作限定。

[0081] 上述网络设备可以存在老化机制，上述高速硬件存储器中的计数表项可以被老化。

[0082] 例如，上述CPU或FPGA周期性遍历上述高速硬件存储器中的各计数表项时，判断当前时间与各计数表项创建时间之间的时间差是否达到老化时长(该老化时长可以在网络设备中预先设置)。当上述网络设备在上述遍历周期内确定当前时间与各计数表项创建时间之间的时间差达到上述老化时长的计数表项时，则将该计数表项上的计数结果清零。

[0083] 以下具体说明本申请记载的执行步骤。需要说明的是，以下步骤可以由网络设备的CPU、FPGA或者其他控制器件单独完成、也可以由网络设备中的各控制器件(CPU、FPGA等控制器件)配合完成，在此不作限定。以下以FPGA作为执行主体进行说明，其他执行主体的执行步骤可以参照FPGA作为执行主体的执行步骤。

[0084] S301，周期性遍历上述高速硬件存储器中的各计数表项；S302，老化处理当前时间与遍历的任一计数表项的创建时间之间的时间差达到预设老化时长的计数表项；S303，获取第一SYN包数量；S304，获取第二SYN包数量；S305，根据上述第一SYN包数量与上述第二SYN包数量相加的结果更新上述FPGA统计的接收到的SYN包的总数量。其中，需要说明的是，上述第一SYN包数量，为遍历到的当前时间与上述创建时间之间的时间差未达到预设老化时长的各计数表项的上述累计数量的和；上述第二SYN包数量，为在本轮遍历周期内各计数表项在被遍历的过程中以及在被遍历完成之后的上述累计数量的增加值的和。并且，上述S302-S304步骤是嵌套在执行S301的过程中执行的，在此仅是为了方便分别对各步骤进行详细说明。

[0085] 在S301中，上述FPGA可以预先设置周期性启动遍历地址的时间间隔时长。

[0086] 例如，上述时间间隔时长为5s。上述FPGA可以在完成上一次遍历上述高速硬件存储器中的各计数表项后经过5s后再次启动遍历。

[0087] 在S302中，上述FPGA周期性遍历上述高速硬件存储器中的各计数表项时，可以确定当前时间与该计数表项的创建时间之间的时间差是否达到预设老化时长；如果当前时间与该计数表项的创建时间之间的时间差达到预设老化时长，则对该技术表项进行老化处理；

[0088] 例如，上述预设老化时长为2min。上述FPGA中设置了统计第一SYN包数量的计数器。在某一轮遍历周期内，上述FPGA在遍历到某一计数表项(创建时间为7:58)时，确定当前时间(8:00)与该表项的创建时间(7:58)之间的时间差已达到上述预设老化时长(2min)，则对该计数表项进行老化处理，将该计数表项的计数结果清零。

[0089] 在S303中，上述FPGA周期性遍历上述高速硬件存储器中的各计数表项时，可以确定当前时间与该计数表项的创建时间之间的时间差是否达到预设老化时长；如果当前时间与该计数表项的创建时间之间的时间差未达到预设老化时长，则记录该计数表项中的上述累计数量；以及，对记录的各计数表项的上述累计数量进行累加，得到上述第一SYN包数量。

[0090] 例如，上述预设老化时长为2min。上述FPGA中设置了统计第一SYN包数量的计数

器。在某一轮遍历周期内，当上述FPGA在遍历到某一计数表项(创建时间为8:59)时，确定当前时间(9:00)与该表项的创建时间(8:59)之间的时间差未达到上述预设老化时长(2min)，则将该计数表项中的计数结果与当前上述统计第一SYN包数量的计数器中的计数结果累加后记录入该统计第一SYN包数量的计数器。当完成本轮遍历后，查询上述统计第一SYN包数量的计数器的计数结果，并将该结果作为上述第一SYN包数量。

[0091] 在S304中，上述FPGA可以将在上述遍历周期内各计数表项在被遍历的过程中以及在被遍历完成之后的上述累计数量的增加值的和作为上述第二SYN包数量。

[0092] 在一实施例中，上述高速硬件存储器可以预先被划分为若干个与计数表项一一对应的存储地址单元。上述FPGA周期性遍历上述高速硬件存储器中所有的存储地址单元上的计数表项。上述网络设备中预设了第一纠错计数器(例如，在FPGA中预设了第一纠错计数器)。

[0093] 上述FPGA确定在本轮遍历周期内待写入上述高速硬件存储器的SYN包的源IP对应的目标计数表项的存储地址，是否小于等于当前正在遍历的计数表项的存储地址；如果是，更新上述目标计数表项的累计数量，并将预设的第一纠错计数器的计数结果加一；在本轮遍历周期结束后，读取上述第一纠错计数器的计数结果，得到上述第二SYN包数量。需要说明的是，上述本轮遍历周期，为从上述FPGA向上述高速硬件存储器发送第一个存储地址读命令的时刻开始至上述FPGA接收到上述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束。

[0094] 例如，上述高速硬件存储器中的存储地址的编号为从1至N。当上述FPGA正在遍历编号为10的存储地址时(可以是在上述FPGA向上述高速硬件存储器发送编号为10的存储地址读命令的时刻与上述FPGA接收到上述高速硬件存储器发送编号为10的存储地址回读结果的时刻中间的任一时刻)，如果上述高速硬件存储器待写入的SYN包的源IP对应的目标计数表项的存储地址的编号为10以下中的任一，上述FPGA将上述目标计数表项的存储地址的编号(例如，8)与当前正在遍历的计数表项的存储地址的编号(10)比较，确定上述目标计数表项的存储地址的编号小于当前正在遍历的计数表项的存储地址的编号，则会更新上述目标计数表项的累计数量，并将预设的第一纠错计数器的计数结果加一。在本轮遍历周期结束后，读取上述第一纠错计数器的计数结果，得到上述第二SYN包数量。

[0095] 在另一实施例中，上述高速硬件存储器可以预先被划分为若干个与计数表项一一对应的存储地址单元。上述FPGA周期性遍历上述高速硬件存储器中所有的存储地址单元上的计数表项。上述网络设备中预设了第二纠错计数器(例如，在FPGA中预设了第二纠错计数器)。

[0096] 上述FPGA确定与在本轮遍历周期内待写入上述高速硬件存储器的SYN包的源IP对应的目标计数表项的存储地址，是否小于当前正在遍历的计数表项的下一计数表项的存储地址；如果是，更新上述目标计数表项的累计数量，并将预设的第二纠错计数器的计数结果加一；在本轮遍历结束后，读取上述第二纠错计数器的计数结果，得到上述第二SYN包数量。需要说明的是，上述本轮遍历周期，为从上述FPGA向上述高速硬件存储器发送第一个存储地址读命令的时刻开始至上述FPGA接收到上述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束。

[0097] 例如，上述高速硬件存储器中的存储地址的编号为从1至N。当上述FPGA正在遍历

编号为10的存储地址时(可以是在上述FPGA向上述高速硬件存储器发送编号为10的存储地址读命令的时刻与上述FPGA接收到上述高速硬件存储器发送编号为10的存储地址回读结果的时刻中间的任一时刻),如果上述高速硬件存储器待写入的SYN包的源IP对应的目标计数表项的存储地址的编号为10以下中的任一,上述FPGA将上述目标计数表项的存储地址的编号(例如,10)与正在遍历的计数表项的下一计数表项的存储地址的编号(11)比较,确定上述目标计数表项的存储地址的编号小于正在遍历的计数表项的下一计数表项的存储地址的编号,则会更新上述目标计数表项的累计数量,并将预设的第二纠错计数器的计数结果加一。在本轮遍历周期结束后,读取上述第二纠错计数器的计数结果,得到上述第二SYN包数量。

[0098] 而在实际应用中,假设当前正在遍历最后一个存储地址单元(编号为N)上的计数表项,上述当前正在遍历的计数表项的下一计数表项的存储地址的编号将为1。由于在遍历最后一个存储地址单元时,上述高速硬件待写入的SYN包的源IP对应的目标计数表项的存储地址的编号肯定大于等于1,因此,在上述遍历最后一个存储地址单元时,上述高速硬件存储器新增加的SYN包的数量将会被漏计。

[0099] 为了计数准确,在一实施例中,上述网络设备中还预设了第三纠错计数器(例如,在FPGA中预设了第三纠错计数器)。

[0100] 在本轮遍历周期内遍历最后一个存储地址单元的过程中,每当上述高速硬件存储器被写入一个SYN包时,将预设的第三纠错计数器的计数结果加一;上述在本轮遍历周期内遍历最后一个存储地址单元的过程中,为从上述FPGA向上述高速硬件存储器发送最后一个存储地址的读命令的时刻开始至上述FPGA接收到上述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束;将上述第二纠错计数器与上述第三纠错计数器的计数结果相加,得到上述第二SYN包数量。

[0101] 需要说明的是,上述在本轮遍历周期内遍历最后一个存储地址单元的过程包括从上述FPGA向上述高速硬件存储器发送最后一个存储地址的读命令的时刻开始至上述FPGA接收到上述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束。

[0102] 在S305中,在完成一轮遍历周期后,上述FPGA可以将获取的上述第一SYN包数量与获取的上述第二SYN包数量相加的结果更新为上述FPGA统计的接收到的SYN包的总数量。

[0103] 例如,上述FPGA中设置了总计数器,用于统计网络设备接收到的SYN包的总数量。上述FPGA可以将获取的上述第一SYN包数量与获取的上述第二SYN包数量相加的结果更新为上述总计数器中的计数结果。在本实施例中,由于上述总计数器中的计数结果被更新为上述第一SYN包数量与获取的上述第二SYN包数量相加的结果,因此,上述总计数器的结果不会一直累计,从而避免了当上述网络设备接收大量SYN报文时,总计数器中的计数有可能达到该总计数器能够记录的最大值而造成从零开始重新记录,导致计数结果混乱。

[0104] 由上述记载的技术方案可知,一方面,由于上述网络设备包括用于统计接收到的SYN包的总数量的FPGA;以及,与上述FPGA连接的高速硬件存储器;其中,上述高速硬件存储器存储了与接收到的SYN包的源IP对应的若干计数表项;上述计数表项包括表项创建时间、源IP和接收到的与上述源IP对应的SYN包的累计数量,因此,当上述网络设备监听到在一段间隔时长内上述FPGA统计的接收到的SYN包的总数量突破预设阈值时,则可以确认自身正在遭受SYN攻击,并且,上述网络设备可以在确定自身遭受到SYN攻击后,将统计的上述累计

数量的增长速率大于预设值的计数表项对应的源IP确定为SYN攻击包的源IP。

[0105] 另一方面，由于网络设备周期性遍历上述高速硬件存储器中的各计数表项，老化处理当前时间与遍历的任一计数表项的创建时间之间的时间差达到预设老化时长的计数表项，并且将遍历到的当前时间与上述创建时间之间的时间差未达到预设老化时长的各计数表项的上述累计数量的和，以及，在本轮遍历周期内各计数表项在被遍历的过程中以及在被遍历完成之后的上述累计数量的增加值的和相加的结果更新为上述FPGA统计的接收到的SYN包的总数量，因此，使得上述FPGA统计的接收到的SYN包的总数量可以与上述各计数表项的计数结果的和保持同步增减，不会一直累加，从而避免了上述网络设备由于上述FPGA统计的接收到的SYN包的总数量一直累加直至突破预设阈值而导致的误以为自身正在遭受SYN攻击的误判。

[0106] 相应于上面的方法实施例，本申请还提供一种识别SYN攻击行为中统计SYN包数量的装置，应用于网络设备。

[0107] 上述网络设备包括用于统计接收到的SYN包的总数量的FPGA；以及，与上述FPGA连接的高速硬件存储器；其中，上述高速硬件存储器存储了与接收到的SYN包的源IP对应的若干计数表项；上述计数表项包括表项创建时间、源IP和接收到的与上述源IP对应的SYN包的累计数量。

[0108] 请参照图3，图3为本说明书示出的一种识别SYN攻击行为中统计SYN包数量的装置的结构图。

[0109] 如图3所示，上述装置300包括：

[0110] 周期性遍历模块310，周期性遍历上述高速硬件存储器中的各计数表项，老化处理当前时间与遍历的任一计数表项的创建时间之间的时间差达到预设老化时长的计数表项，并获取第一SYN包数量，以及，第二SYN包数量；其中，上述第一SYN包数量，为遍历到的当前时间与上述创建时间之间的时间差未达到预设老化时长的各计数表项的上述累计数量的和；上述第二SYN包数量，为在本轮遍历周期内各计数表项在被遍历的过程中以及在被遍历完成之后的上述累计数量的增加值的和；

[0111] 更新SYN包总数量模块320，根据上述第一SYN包数量与上述第二SYN包数量相加的结果更新上述FPGA统计的接收到的SYN包的总数量。

[0112] 在示出的一实施例中，上述周期性遍历模块310，还包括：

[0113] 获取第一SYN包数量模块，确定当前时间与遍历的计数表项的创建时间之间的时间差是否达到预设老化时长；

[0114] 如果当前时间与遍历的任一计数表项的创建时间未达到预设老化时长，则记录该计数表项中的上述累计数量；以及，对记录的各计数表项的上述累计数量进行累加，得到上述第一SYN包数量。

[0115] 在示出的一实施例中，上述高速硬件存储器预先被划分为若干个与计数表项一一对应的存储地址单元；上述网络设备中预设了第一纠错计数器；上述周期性遍历模块310，还包括：

[0116] 获取第二SYN包数量模块，确定在本轮遍历周期内待写入上述高速硬件存储器的SYN包的源IP对应的目标计数表项的存储地址，是否小于等于当前正在遍历的计数表项的存储地址；如果是，更新上述目标计数表项的累计数量，并将预设的第一纠错计数器的计数

结果加一;上述本轮遍历周期,为从上述FPGA向上述高速硬件存储器发送第一个存储地址读命令的时刻开始至上述FPGA接收到上述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束;

[0117] 在本轮遍历周期结束后,读取上述第一纠错计数器的计数结果,得到上述第二SYN包数量。

[0118] 在示出的一实施例中,上述高速硬件存储器预先被划分为若干个与计数表项一一对应的存储地址单元;上述网络设备中预设了第二纠错计数器;上述周期性遍历模块310,还包括:

[0119] 获取第二SYN包数量模块,确定与在本轮遍历周期内待写入上述高速硬件存储器的SYN包的源IP对应的目标计数表项的存储地址,是否小于当前正在遍历的计数表项的下一计数表项的存储地址;如果是,更新上述目标计数表项的累计数量,并将预设的第二纠错计数器的计数结果加一;上述本轮遍历周期,为从上述FPGA向上述高速硬件存储器发送第一个存储地址读命令的时刻开始至上述FPGA接收到上述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束;

[0120] 在本轮遍历结束后,读取上述第二纠错计数器的计数结果,得到上述第二SYN包数量。

[0121] 在示出的一实施例中,上述网络设备中还预设了第三纠错计数器;上述周期性遍历模块310,还包括:

[0122] 获取遍历过程漏计的SYN包数量模块,在本轮遍历周期内遍历最后一个存储地址单元的过程中,每当上述高速硬件存储器被写入一个SYN包时,将预设的第三纠错计数器的计数结果加一;上述在本轮遍历周期内遍历最后一个存储地址单元的过程中,为从上述FPGA向上述高速硬件存储器发送最后一个存储地址的读命令的时刻开始至上述FPGA接收到上述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束;

[0123] 将上述第二纠错计数器与上述第三纠错计数器的计数结果相加,得到上述第二SYN包数量。

[0124] 在示出的一实施例中,上述在本轮遍历周期内遍历最后一个存储地址单元的过程包括:

[0125] 从上述FPGA向上述高速硬件存储器发送最后一个存储地址的读命令的时刻开始至上述FPGA接收到上述高速硬件存储器发送的最后一个存储地址回读结果的时刻结束。

[0126] 对于装置实施例而言,由于其基本对应于方法实施例,所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的,其中上述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本申请方案的目的。本领域普通技术人员在不付出创造性劳动的情况下,即可以理解并实施。

[0127] 本说明书中描述的主题及功能操作的实施例可以在以下中实现:数字电子电路、有形体现的计算机软件或固件、包括本说明书中公开的结构及其结构性等同物的计算机硬件、或者它们中的一个或多个的组合。本说明书中描述的主题的实施例可以实现为一个或多个计算机程序,即编码在有形非暂时性程序载体上以被数据处理装置执行或控制数据处

理装置的操作的计算机程序指令中的一个或多个模块。可替代地或附加地，程序指令可以被编码在人工生成的传播信号上，例如机器生成的电、光或电磁信号，该信号被生成以将信息编码并传输到合适的接收机装置以由数据处理装置执行。计算机存储介质可以是机器可读存储设备、机器可读存储基板、随机或串行存取存储器设备、或它们中的一个或多个的组合。

[0128] 本说明书中描述的处理及逻辑流程可以由执行一个或多个计算机程序的一个或多个可编程计算机执行，以通过根据输入数据进行操作并生成输出来执行相应的功能。上述处理及逻辑流程还可以由专用逻辑电路—例如FPGA(现场可编程门阵列)或ASIC(专用集成电路)来执行，并且装置也可以实现为专用逻辑电路。

[0129] 适合用于执行计算机程序的计算机包括，例如通用和/或专用微处理器，或任何其他类型的中央处理单元。通常，中央处理单元将从只读存储器和/或随机存取存储器接收指令和数据。计算机的基本组件包括用于实施或执行指令的中央处理单元以及用于存储指令和数据的一个或多个存储器设备。通常，计算机还将包括用于存储数据的一个或多个大容量存储设备，例如磁盘、磁光盘或光盘等，或者计算机将可操作地与此大容量存储设备耦接以从其接收数据或向其传送数据，抑或两种情况兼而有之。然而，计算机不是必须具有这样的设备。此外，计算机可以嵌入在另一设备中，例如移动电话、个人数字助理(PDA)、移动音频或视频播放器、游戏操纵台、全球定位系统(GPS)接收机、或例如通用串行总线(USB)闪存驱动器的便携式存储设备，仅举几例。

[0130] 适合于存储计算机程序指令和数据的计算机可读介质包括所有形式的非易失性存储器、媒介和存储器设备，例如包括半导体存储器设备(例如EPROM、EEPROM和闪存设备)、磁盘(例如内部硬盘或可移动盘)、磁光盘以及CD ROM和DVD-ROM盘。处理器和存储器可由专用逻辑电路补充或并入专用逻辑电路中。

[0131] 虽然本说明书包含许多具体实施细节，但是这些不应被解释为限制任何发明的范围或所要求保护的范围，而是主要用于描述特定发明的具体实施例的特征。本说明书内在多个实施例中描述的某些特征也可以在单个实施例中被组合实施。另一方面，在单个实施例中描述的各种特征也可以在多个实施例中分开实施或以任何合适的子组合来实施。此外，虽然特征可以如上上述在某些组合中起作用并且甚至最初如此要求保护，但是来自所要求保护的组合中的一个或多个特征在一些情况下可以从该组合中去除，并且所要求保护的组合可以指向子组合或子组合的变型。

[0132] 类似地，虽然在附图中以特定顺序描绘了操作，但是这不应被理解为要求这些操作以所示的特定顺序执行或顺次执行、或者要求所有例示的操作被执行，以实现期望的结果。在某些情况下，多任务和并行处理可能是有利的。此外，上述实施例中的各种系统模块和组件的分离不应被理解为在所有实施例中均需要这样的分离，并且应当理解，所描述的程序组件和系统通常可以一起集成在单个软件产品中，或者封装成多个软件产品。

[0133] 由此，主题的特定实施例已被描述。其他实施例在所附权利要求书的范围以内。在某些情况下，权利要求书中记载的动作可以以不同的顺序执行并且仍实现期望的结果。此外，附图中描绘的处理并非必需所示的特定顺序或顺次顺序，以实现期望的结果。在某些实现中，多任务和并行处理可能是有利的。

[0134] 以上上述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精

神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

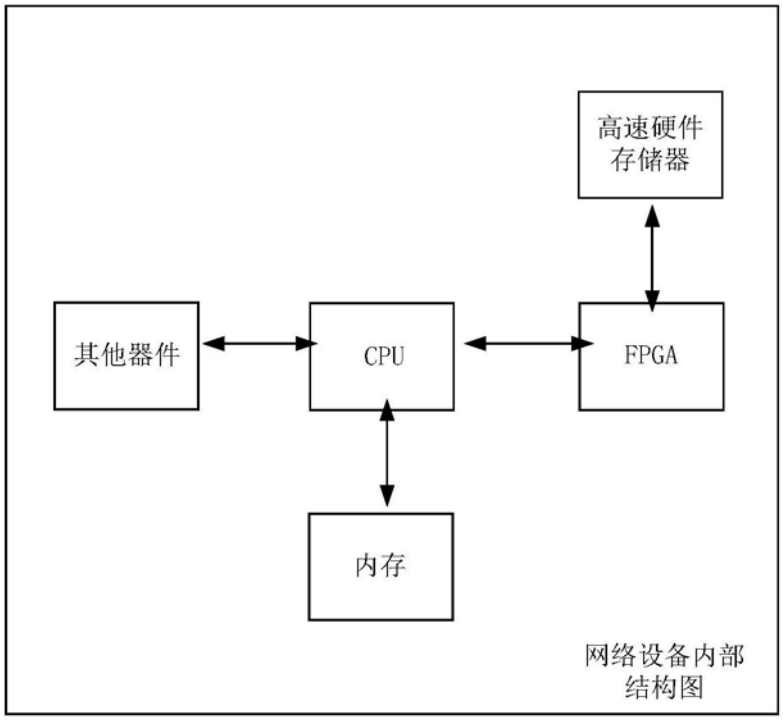

高速硬件
存储器
其他器件
CPU
FPGA
内存
网络设备内部
结构图

图1

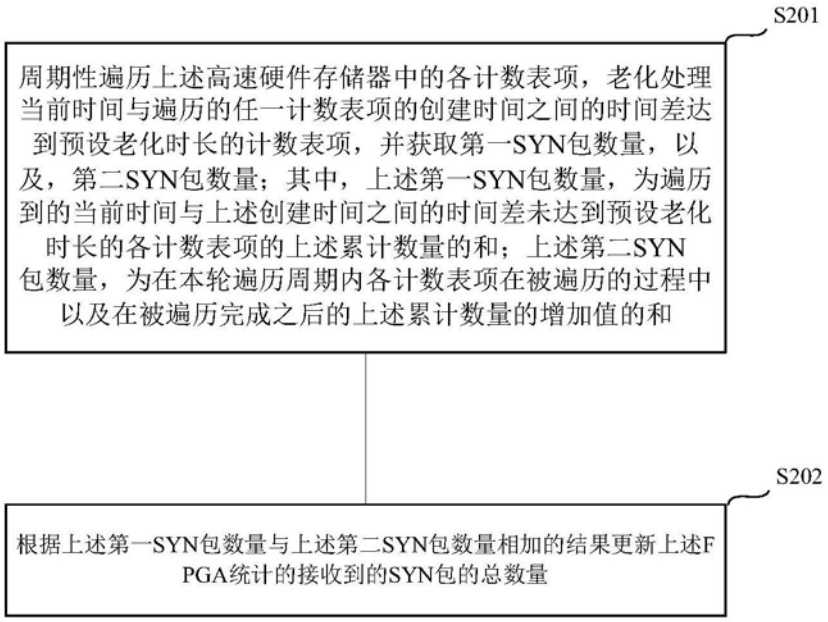

S201
周期性遍历上述高速硬件存储器中的各计数表项，老化处理当前时间与遍历的任一计数表项的创建时间之间的时间差达到预设老化时长的计数表项，并获取第一SYN包数量，以及，第二SYN包数量；其中，上述第一SYN包数量，为遍历到的当前时间与上述创建时间之间的时间差未达到预设老化时长的各计数表项的上述累计数量的和；上述第二SYN包数量，为在本轮遍历周期内各计数表项在被遍历的过程中以及在被遍历完成之后的上述累计数量的增加值的和
S202
根据上述第一SYN包数量与上述第二SYN包数量相加的结果更新上述FPGA统计的接收到的SYN包的总数量

图2

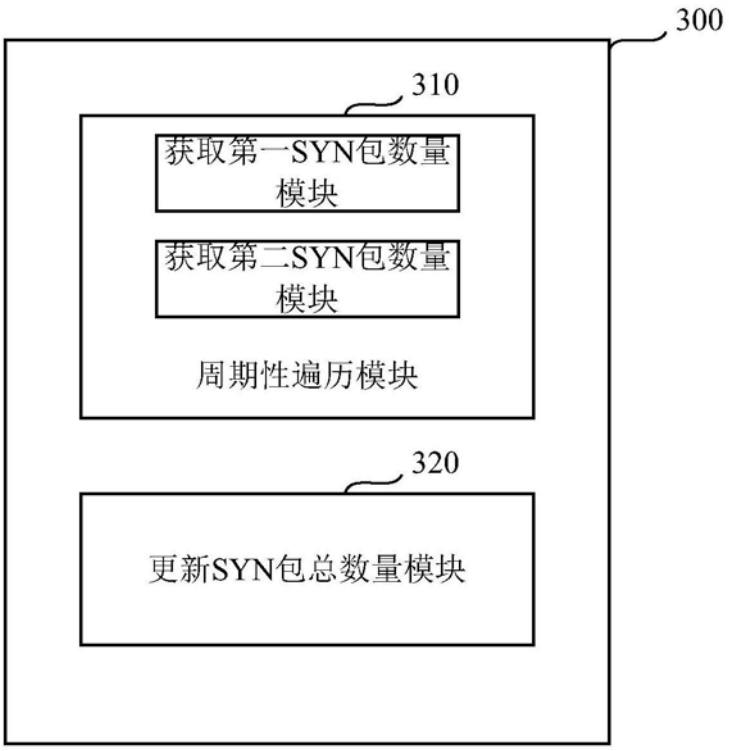

300
310
获取第一SYN包数量模块
获取第二SYN包数量模块
周期性遍历模块
320
更新SYN包总数量模块

图3