



(21) 申请号 202411545697.0

(22) 申请日 2024.11.01

(65) 同一申请的已公布的文献号

申请公布号 CN 119052000 A

(43) 申请公布日 2024.11.29

(73) 专利权人 湖南密码工程研究中心有限公司

地址 410205 湖南省长沙市高新开发区麓

云路100号兴工科技园10栋402

(72) 发明人 石理智 胡超 李京泽 周炳佳

黄名超

(74) 专利代理机构 长沙市岳麓慧专利代理事务

所(普通合伙) 43270

专利代理师 王中华

(51) Int. Cl.

H04L 9/40 (2022.01)

(56) 对比文件

CN 101572700 A, 2009.11.04

CN 108540287 A, 2018.09.14

审查员 张伟

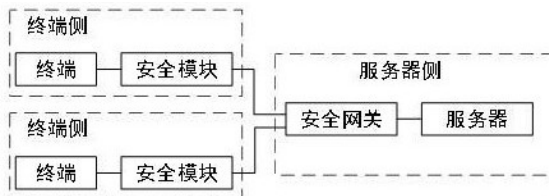
权利要求书2页 说明书5页 附图1页

(54) 发明名称

基于计数器模式高速数据安全传输的实现方法

(57) 摘要

本发明公开一种基于计数器模式高速数据安全传输的实现方法,包括:安全模块与安全网关建立双向认证连接,安全模块向安全网关发起主密钥请求,同时将IP地址发送给安全网关;安全网关将主密钥分发到安全模块;安全模块和安全网关基于主密钥,采用计数器模式分别计算出随机数后存储到上行会话密钥队列和下行会话密钥队列;终端访问服务器时,安全模块从上行会话密钥队列中提取会话密钥,对上行数据进行加密隐私保护;安全网关依据IP地址检索到对应的主密钥,依据主密钥从对应的上行会话密钥队列中提取会话密钥,对上行数据进行解密,将解密的明文数据转发到服务器;本发明可保障数据高速传输可信和安全,提升吞吐量并降低数据延时,部署简单。



1. 一种基于计数器模式高速数据安全传输的实现方法,其特征在于,包括:

安全模块与安全网关建立双向认证连接,其中,所述安全模块部署于终端侧,所述安全网关部署于服务器侧;

安全模块向安全网关发起主密钥请求,同时将IP地址发送给安全网关;

安全网关接收到主密钥请求后,将主密钥分发到安全模块;

安全模块接收安全网关分发的主密钥;

安全模块和安全网关基于所述主密钥,采用计数器模式分别计算出随机数后存储到上行会话密钥队列和下行会话密钥队列;

终端访问服务器时,安全模块从上行会话密钥队列中提取会话密钥,对上行数据进行加密隐私保护;

安全网关依据所述IP地址检索到对应的主密钥,依据主密钥从对应的上行会话密钥队列中提取会话密钥,对上行数据进行解密,将解密的明文数据转发到服务器;

安全模块接收安全网关分发的主密钥之后,所述方法还包括:安全模块对主密钥采用固定字符串加密得到密文数据,将密文数据发送到安全网关;安全网关接收到安全模块发送的密文数据后,选用分配给此安全模块的主密钥对密文数据进行解密;将解密后的数据与所述固定字符串进行比较;如果解密后的数据与所述固定字符串数据一致,则分发的主密钥有效,安全网关更新主密钥映射表;同时通知安全模块更新受保护网络表;如果解密后的数据与所述固定字符串数据不一致,则分发的主密钥无效,发送数据包要求安全模块重新申请主密钥;

安全模块和安全网关基于所述主密钥,采用计数器模式分别计算出随机数后存储到上行会话密钥队列和下行会话密钥队列,包括:验证主密钥有效后,安全模块与安全网关分别依据主密钥,采用计数器的方式计算随机数分别存储到上行会话密钥队列和下行会话密钥队列中,并监测上行会话密钥队列和下行会话密钥队列保持队列始终满载状态,同时将用户空间的上行会话密钥队列和下行会话密钥队列内存映射到内核空间;

终端访问服务器时,安全模块从上行会话密钥队列中提取会话密钥,对上行数据进行加密隐私保护,包括:安全模块在NF_IP_PRE_ROUTING上注册HOOK函数,截取上行数据,计算payload数据长度是否大于0;如果payload数据长度等于0,则表示没有数据需要进行加密,直接提交协议栈进行协议处理;如果payload数据长度大于0,则表示有数据需要进行加密,获取五元组,所述五元组包括源地址、目的地址、源端口、目的端口、协议;根据五元组计算HASH值,通过HASH值检索会话表;如果匹配会话表,则使用此会话表中对应的会话密钥,对数据进行分段异或加密,重新计算并更新IP校验和;将加密后的数据提交协议栈进行协议处理,并更新会话表中此会话超时时间;如果不匹配会话表,则依据源地址检索受保护网络表;不匹配受保护网络表则提交协议栈进行协议处理,匹配受保护网络表则从受保护网络表中获取相应的主密钥,依据主密钥从相对应的上行会话密钥队列中提取会话密钥与16字节计数器的值,依据会话密钥对数据进行分段异或加密,将16字节计数器的值附加在加密数据段末尾,重新计算并更新payload长度,重新计算并更新IP报文长度,重新计算并更新IP校验和;将加密后的数据提交协议栈进行协议处理,将五元组的HASH值与会话密钥存储到会话表,并设定此会话超时时间。

2. 如权利要求1所述的基于计数器模式高速数据安全传输的实现方法,其特征在于,安

全网关接收到主密钥请求后,将主密钥分发到安全模块,包括:

安全网关接收到安全模块发起的主密钥请求后,依据安全模块的IP地址,查询主密钥映射表;如果网络地址与主密钥映射表相匹配,将对应的主密钥分发到安全模块;如果网络地址与主密钥映射表不匹配,获取16字节随机数作为主密钥分发到安全模块。

3.如权利要求1所述的基于计数器模式高速数据安全传输的实现方法,其特征在于,安全网关依据所述IP地址检索到对应的主密钥,依据主密钥从对应的上行会话密钥队列中提取会话密钥,对上行数据进行解密,包括:

安全网关在NF_IP_PRE_ROUTING上注册HOOK函数,截取上行数据,计算payload数据长度是否大于0;

如果payload数据长度等于0,则表示没有数据需要进行解密,直接提交协议栈进行协议处理;

如果payload数据长度大于0,则表示有数据需要进行解密,获取五元组,根据五元组计算HASH值,通过HASH值检索会话表;如果匹配会话表,则使用此会话表中对应的会话密钥,对数据进行分段异或解密,重新计算并更新IP校验和,将解密后的数据提交协议栈进行协议处理,并更新会话表中此会话超时时间;

如果不匹配会话表,则依据源地址检索主密钥映射表,不匹配主密钥映射表则提交协议栈进行协议处理,匹配则从主密钥映射表中获取相应的主密钥,取payload数据段末尾16字节作为计数器的值,依据主密钥从相对应的上行会话密钥队列中提取计数器的值对应的会话密钥,依据会话密钥对数据进行分段异或解密,去除末尾16字节计数器的值,并更新payload,重新计算并更新payload长度,重新计算并更新IP报文长度,重新计算并更新IP校验和,将解密后的数据提交协议栈进行协议处理,将五元组的HASH值与会话密钥存储到会话表,并设定此会话超时时间。

4.如权利要求3所述的基于计数器模式高速数据安全传输的实现方法,其特征在于,所述方法还包括:

如果会话超时,从会话表中删除此会话,再次传输的数据获取新一轮的会话密钥对数据进行异或加密解密。

基于计数器模式高速数据安全传输的实现方法

技术领域

[0001] 本发明涉及网络安全技术领域,尤其涉及一种基于计数器模式高速数据安全传输的实现方法。

背景技术

[0002] 随着信息化系统建设的推广,大规模数据泄密事件频频发生,密码技术作为网络安全的核心和基础,成为各方关注的焦点。目前,业内关键信息基础设施中物联网终端设备基本没有任何保护措施,尤其是数据隐私保护。如何在网络攻击事件频繁发生的复杂网络环境中,不改变原有网络拓扑结构的前提,保障数据高速传输可信和安全、提升吞吐量、降低数据延时,同时部署简单易用,是业内急需解决的问题。

[0003] 现在技术通常采用双侧布署VPN的方案。在布署VPN的方案中,将云端服务器与终端设备隐藏起来,对其自身进行了保护,同时双侧的VPN建立隧道,数据通过VPN隧道对传输数据进行了保护。但是VPN服务器在应对大量的设备接入时将存在瓶颈,通过设备的堆叠将增加客户成本,同时数据经过多次修改传输路径,降低了网络传输效率,增大了数据延时,导致反向控制指令可能无法及时到达终端设备,进而造成无法预计的后果。

发明内容

[0004] 本发明提供一种基于计数器模式高速数据安全传输的实现方法,保障数据高速传输可信和安全,提升吞吐量并降低数据延时,部署简单。

[0005] 本发明提供一种基于计数器模式高速数据安全传输的实现方法,包括:

[0006] 安全模块与安全网关建立双向认证连接,其中,所述安全模块部署于终端侧,所述安全网关部署于服务器侧;

[0007] 安全模块向安全网关发起主密钥请求,同时将IP地址发送给安全网关;

[0008] 安全网关接收到主密钥请求后,将主密钥分发到安全模块;

[0009] 安全模块接收安全网关分发的主密钥;

[0010] 安全模块和安全网关基于所述主密钥,采用计数器模式分别计算出随机数后存储到上行会话密钥队列和下行会话密钥队列;

[0011] 终端访问服务器时,安全模块从上行会话密钥队列中提取会话密钥,对上行数据进行加密隐私保护;

[0012] 安全网关依据所述IP地址检索到对应的主密钥,依据主密钥从对应的上行会话密钥队列中提取会话密钥,对上行数据进行解密,将解密的明文数据转发到服务器。

[0013] 进一步地,安全网关接收到主密钥请求后,将主密钥分发到安全模块,包括:

[0014] 安全网关接收到安全模块发起的主密钥请求后,依据安全模块的IP地址,查询主密钥映射表;如果网络地址与主密钥映射表相匹配,将对应的主密钥分发到安全模块;如果网络地址与主密钥映射表不匹配,获取16字节随机数作为主密钥分发到安全模块。

[0015] 进一步地,安全模块接收安全网关分发的主密钥之后,所述方法还包括:

[0016] 安全模块对主密钥采用固定字符串加密得到密文数据,将密文数据发送到安全网关;

[0017] 安全网关接收到安全模块发送的密文数据后,选用分配给此安全模块的主密钥对密文数据进行解密;将解密后的数据与所述固定字符串进行比较;如果解密后的数据与所述固定字符串数据一致,则分发的主密钥有效,安全网关更新主密钥映射表;同时通知安全模块更新受保护网络表;如果解密后的数据与所述固定字符串数据不一致,则分发的主密钥无效,发送数据包要求安全模块重新申请主密钥。

[0018] 进一步地,安全模块和安全网关基于所述主密钥,采用计数器模式分别计算出随机数后存储到上行会话密钥队列和下行会话密钥队列,包括:

[0019] 验证主密钥有效后,安全模块与安全网关分别依据主密钥,采用计数器的方式计算随机数分别存储到上行会话密钥队列和下行会话密钥队列中,并监测上行会话密钥队列和下行会话密钥队列保持队列始终满载状态,同时将用户空间的上行会话密钥队列和下行会话密钥队列内存映射到内核空间。

[0020] 进一步地,终端访问服务器时,安全模块从上行会话密钥队列中提取会话密钥,对上行数据进行加密隐私保护,包括:

[0021] 安全模块在NF_IP_PRE_ROUTING上注册HOOK函数,截取上行数据,计算payload数据长度是否大于0;

[0022] 如果payload数据长度等于0,则表示没有数据需要进行加密,直接提交协议栈进行协议处理;

[0023] 如果payload数据长度大于0,则表示有数据需要进行加密,获取五元祖,所述五元祖包括源地址、目的地址、源端口、目的端口、协议;根据五元祖计算HASH值,通过HASH值检索会话表;如果匹配会话表,则使用此会话表中对应的会话密钥,对数据进行分段异或加密,重新计算并更新IP校验和;将加密后的数据提交协议栈进行协议处理,并更新会话表中此会话超时时间;

[0024] 如果不匹配会话表,则依据源地址检索受保护网络表;不匹配受保护网络表则提交协议栈进行协议处理,匹配受保护网络表则从受保护网络表中获取相应的主密钥,依据主密钥从相对应的上行会话密钥队列中提取会话密钥与16字节计数器的值,依据会话密钥对数据进行分段异或加密,将16字节计数器的值附加在加密数据段末尾,重新计算并更新payload长度,重新计算并更新IP报文长度,重新计算并更新IP校验和;将加密后的数据提交协议栈进行协议处理,将五元祖的HASH值与会话密钥存储到会话表,并设定此会话超时时间。

[0025] 进一步地,安全网关依据所述IP地址检索到对应的主密钥,依据主密钥从对应的上行会话密钥队列中提取会话密钥,对上行数据进行解密,包括:

[0026] 安全网关在NF_IP_PRE_ROUTING上注册HOOK函数,截取上行数据,计算payload数据长度是否大于0;

[0027] 如果payload数据长度等于0,则表示没有数据需要进行解密,直接提交协议栈进行协议处理;

[0028] 如果payload数据长度大于0,则表示有数据需要进行解密,获取五元祖,根据五元祖计算HASH值,通过HASH值检索会话表;如果匹配会话表,则使用此会话表中对应的会话密

钥,对数据进行分段异或解密,重新计算并更新IP校验和,将解密后的数据提交协议栈进行协议处理,并更新会话表中此会话超时时间;

[0029] 如果不匹配会话表,则依据源地址检索主密钥映射表,不匹配主密钥映射表则提交协议栈进行协议处理,匹配则从主密钥映射表中获取相应的主密钥,取payload数据段末尾16字节作为计数器的值,依据主密钥从相对应的上行会话密钥队列中提取计数器的值对应的会话密钥,依据会话密钥对数据进行分段异或解密,去除末尾16字节计数器的值,并更新payload,重新计算并更新payload长度,重新计算并更新IP报文长度,重新计算并更新IP校验和,将解密后的数据提交协议栈进行协议处理,将五元组的HASH值与会话密钥存储到会话表,并设定此会话超时时间。

[0030] 进一步地,所述方法还包括:

[0031] 如果会话超时,从会话表中删除此会话,再次传输的数据获取新一轮的会话密钥对数据进行异或加密解密。

[0032] 本发明具有以下有益效果:本发明的一种基于计数器模式高速数据安全传输的实现方法,基于计数器模式,进行预计算,提升数据加密解密效率。采用一会话一密钥的方式,会话表中的会话超时将销毁会话密钥,新一轮的会话将重新提取会话密钥,抵御重放攻击,同时提升了密钥的安全强度。

附图说明

[0033] 为了更清楚地说明本发明的技术方案,下面将对实施例中所需要使用的附图作简单地介绍,显而易见地,对于本领域普通技术人员而言,在不付出创造性劳动性的前提下,还可以根据这些附图获得其他的附图。

[0034] 图1为本发明提供的一种基于计数器模式高速数据安全传输的实现方法的网络部署图;

[0035] 图2为本发明提供的一种基于计数器模式高速数据安全传输的实现方法的流程图。

具体实施方式

[0036] 为使本发明的目的、技术方案和优点更加清楚,下面将结合本发明具体实施例及相应的附图对本发明技术方案进行清楚、完整地描述。显然,所描述的实施例仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。以下结合附图,详细说明本发明各实施例提供的技术方案。

[0037] 请参阅图1和图2,本发明实施例提供一种基于计数器模式高速数据安全传输的实现方法,包括:

[0038] S101,安全模块与安全网关建立双向认证连接,其中,所述安全模块部署于终端侧,所述安全网关部署于服务器侧。

[0039] 图1为基于计数器模式高速数据安全传输的实现方法的网络部署图,可以将此方法透明模式接入到现有网络中,无需改变原有网络拓扑,在终端侧部署安全模块,在服务器侧部署安全网关。通过安全模块与安全网关之间的双向认证连接,确保了通信双方的身份

真实性,有效防止了中间人攻击和数据篡改,保障了数据传输过程中的机密性和完整性。该方案的透明接入特性使得其易于部署和维护。无需对现有网络架构进行大规模调整,减少了实施成本和风险,同时也降低了后续运维的复杂度。

[0040] S102,安全模块向安全网关发起主密钥请求,同时将IP地址发送给安全网关。

[0041] S103,安全网关接收到主密钥请求后,将主密钥分发到安全模块。

[0042] 具体地,安全网关接收到安全模块发起的主密钥请求后,依据安全模块的IP地址,查询主密钥映射表;如果网络地址与主密钥映射表相匹配,将对应的主密钥分发到安全模块;如果网络地址与主密钥映射表不匹配,获取16字节随机数作为主密钥分发到安全模块。

[0043] S104,安全模块接收安全网关分发的主密钥。

[0044] 具体地,安全模块对主密钥采用固定字符串加密得到密文数据,将密文数据发送到安全网关;安全网关接收到安全模块发送的密文数据后,选用分配给此安全模块的主密钥对密文数据进行解密;将解密后的数据与所述固定字符串进行比较;如果解密后的数据与所述固定字符串数据一致,则分发的主密钥有效,安全网关更新主密钥映射表;同时通知安全模块更新受保护网络表;如果解密后的数据与所述固定字符串数据不一致,则分发的主密钥无效,发送数据包要求安全模块重新申请主密钥。

[0045] S105,安全模块和安全网关基于所述主密钥,采用计数器模式分别计算出随机数后存储到上行会话密钥队列和下行会话密钥队列。

[0046] 具体地,验证主密钥有效后,安全模块与安全网关分别依据主密钥,采用计数器的方式计算随机数分别存储到上行会话密钥队列和下行会话密钥队列中,并监测上行会话密钥队列和下行会话密钥队列保持队列始终满载状态,同时将用户空间的上行会话密钥队列和下行会话密钥队列内存映射到内核空间;主密钥更新时,重新依据主密钥,采用计数器的方式计算随机数分别存储到上行会话密钥队列和下行会话密钥队列中。

[0047] S106,终端访问服务器时,安全模块从上行会话密钥队列中提取会话密钥,对上行数据进行加密隐私保护。

[0048] 具体地,安全模块在NF_IP_PRE_ROUTING上注册HOOK函数,截取上行数据,计算payload数据长度是否大于0;

[0049] 如果payload数据长度等于0,则表示没有数据需要进行加密,直接提交协议栈进行协议处理;

[0050] 如果payload数据长度大于0,则表示有数据需要进行加密,获取五元祖,所述五元祖包括源地址、目的地址、源端口、目的端口、协议;根据五元祖计算HASH值,通过HASH值检索会话表;如果匹配会话表,则使用此会话表中对应的会话密钥,对数据进行分段异或加密,重新计算并更新IP校验和,如果是TCP协议数据还需要重新计算并更新TCP校验和;将加密后的数据提交协议栈进行协议处理,并更新会话表中此会话超时时间;

[0051] 如果不匹配会话表,则依据源地址检索受保护网络表;不匹配受保护网络表则提交协议栈进行协议处理,匹配受保护网络表则从受保护网络表中获取相应的主密钥,依据主密钥从相对应的上行会话密钥队列中提取会话密钥与16字节计数器的值,依据会话密钥对数据进行分段异或加密,将16字节计数器的值附加在加密数据段末尾,重新计算并更新payload长度,重新计算并更新IP报文长度,重新计算并更新IP校验和,如果是TCP协议数据还需要重新计算并更新TCP校验和;将加密后的数据提交协议栈进行协议处理,将五元祖的

HASH值与会话密钥存储到会话表,并设定此会话超时时间。

[0052] S107,安全网关依据所述IP地址检索到对应的主密钥,依据主密钥从对应的上行会话密钥队列中提取会话密钥,对上行数据进行解密,将解密的明文数据转发到服务器。

[0053] 具体地,安全网关在NF_IP_PRE_ROUTING上注册HOOK函数,截取上行数据,计算payload数据长度是否大于0;

[0054] 如果payload数据长度等于0,则表示没有数据需要进行解密,直接提交协议栈进行协议处理;

[0055] 如果payload数据长度大于0,则表示有数据需要进行解密,获取五元祖,根据五元祖计算HASH值,通过HASH值检索会话表;如果匹配会话表,则使用此会话表中对应的会话密钥,对数据进行分段异或解密,重新计算并更新IP校验和,如果是TCP协议数据还需要重新计算并更新TCP校验和,将解密后的数据提交协议栈进行协议处理,并更新会话表中此会话超时时间;

[0056] 如果不匹配会话表,则依据源地址检索主密钥映射表,不匹配主密钥映射表则提交协议栈进行协议处理,匹配则从主密钥映射表中获取相应的主密钥,取payload数据段末尾16字节作为计数器的值,依据主密钥从相对应的上行会话密钥队列中提取计数器的值对应的会话密钥,依据会话密钥对数据进行分段异或解密,去除末尾16字节计数器的值,并更新payload,重新计算并更新payload长度,重新计算并更新IP报文长度,重新计算并更新IP校验和,如果是TCP协议数据还需要重新计算并更新TCP校验和,将解密后的数据提交协议栈进行协议处理,将五元祖的HASH值与会话密钥存储到会话表,并设定此会话超时时间。

[0057] 反向数据流与S106,S107同理。如果会话超时,从会话表中删除此会话,再次传输的数据获取新一轮的会话密钥对数据进行异或加密解密。一会话一密钥,抵御重放攻击,同时提升了密钥的安全强度。

[0058] 由以上实施例可知,本发明通过透明模式接入,无需更改现有网络拓扑,可实现即插即用。本发明建立会话表,完成数据快速转发,提升数据转发效率。本发明基于计数器模式,进行预计算,提升数据加密解密效率,降低实时数据延迟。本发明采用一会话一密钥的方式,抵御重放攻击,同时提升了密钥的安全强度。

[0059] 以上所述的本发明实施方式并不构成对本发明保护范围的限定。

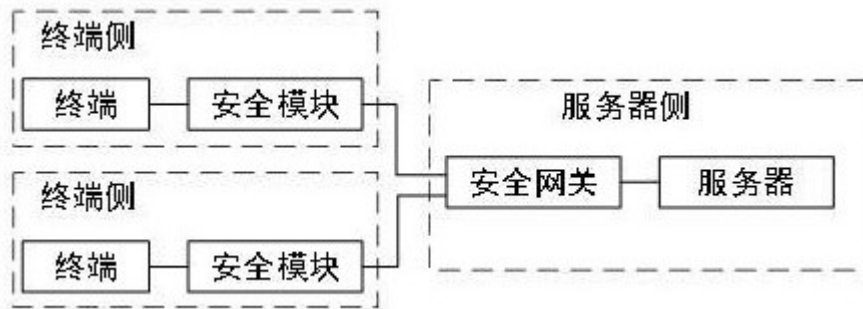


图 1

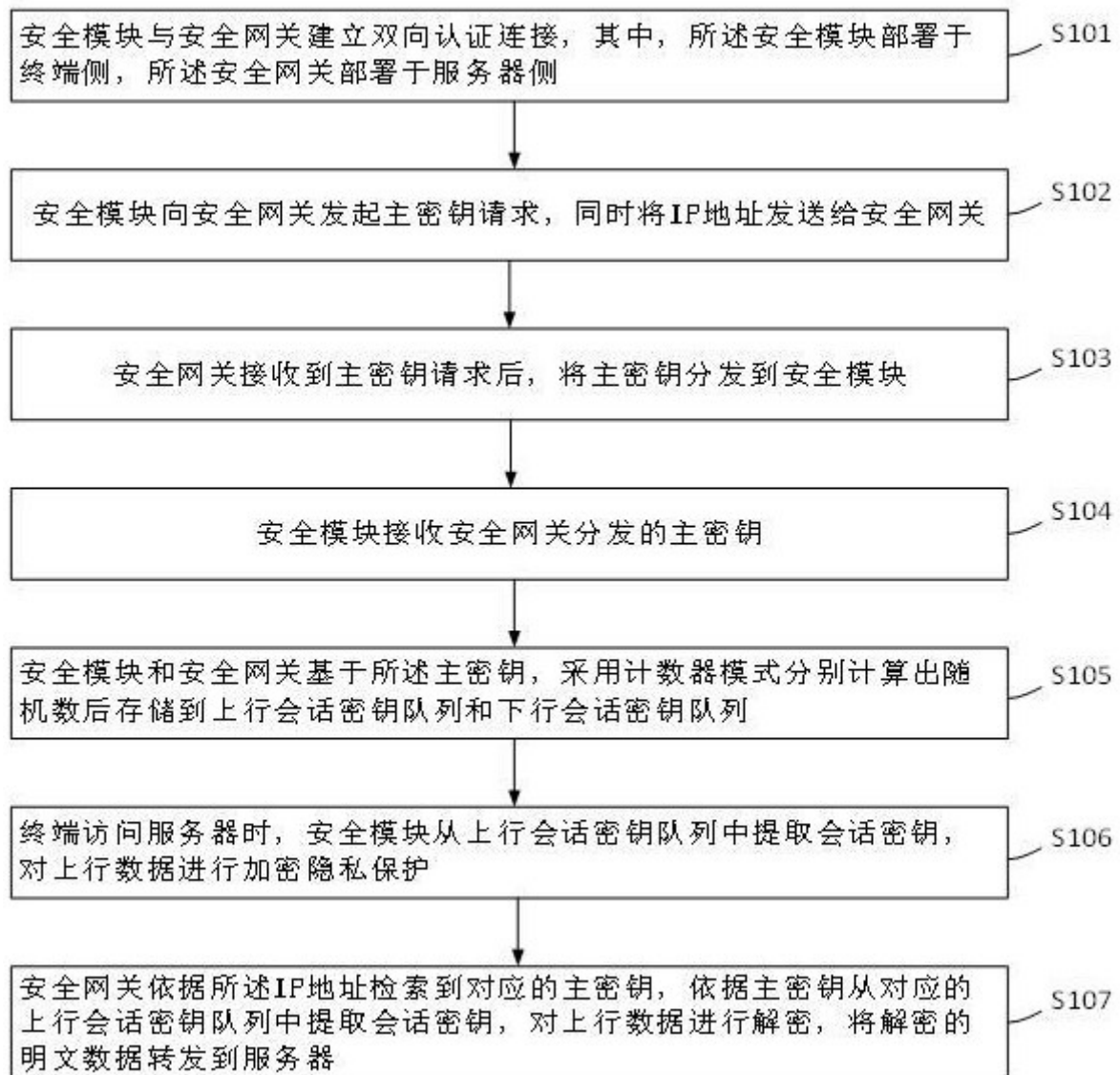


图 2