(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115834026 A
(43)申请公布日 2023.03.21

(21)申请号 202211512189.3

(22)申请日 2022.11.29

(71)申请人 中京天裕科技(北京)有限公司
地址 100085 北京市海淀区上地东路1号院3号楼六层608
申请人 中京天裕科技(杭州)有限公司

(72)发明人 晏培 张军 王彦丰

(74)专利代理机构 杭州君度专利代理事务所(特殊普通合伙) 33240
专利代理师 邬赵丹

(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)

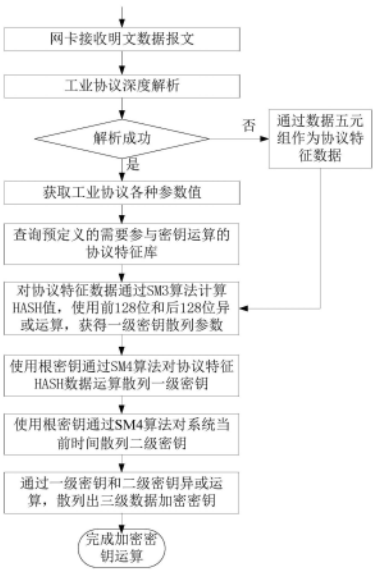
权利要求书1页 说明书4页 附图5页

(54)发明名称

一种基于工业协议的安全加密方法

(57)摘要

本发明涉及一种基于工业协议的安全加密方法。本发明使用根密钥对HASH值进行国密SM4加密运算,散列出三级数据加密密钥。使用SM4算法和散列的三级加密密钥对数据加密,将协议特征HASH数据和加密数据重新封装数据包;重新计算数据包的校验和,发送加密后的数据包。使用根密钥对HASH值进行国密SM4加密运算,散列出三级数据解密密钥。使用数据解密密钥通过SM4国密算法对数据包内容进行解密,重新封装数据包内容,去除协调特征HASH字段,还原明文数据包。本发明解决在工业环境中数据的安全加密问题,通过工业协调的特征参数和时间参数参与密钥散列,实现加密数据一包一密;完全透明方式部署,无需对现有拓扑结构做任何修改。



CN 115834026 A

1.一种基于工业协议的安全加密方法,其特征在于:包括加密密钥运算、数据加密封装、解密密钥运算和数据解密验证;

加密密钥运算具体步骤如下:

网卡接收明文数据包,工业协议深度解析模块对数据包进行深度解析;查询需要参与密钥运算的预定义的协议特征库,预定义的协议特征库为深度解析结果的任意几个字段,并对数据包中的协议特征通过国密SM3算法计算256位的HASH值,然后前128位于后128位进行异或运算,最终的到128位的协议特征HASH值;

获取系统当前时间,读取根密钥;

使用根密钥对计算的128位HASH值进行国密SM4加密运算,散列出一级密钥;使用根密钥对当前时间进行SM4运算,散列出二级密钥;一级密钥与二级密钥异或运算,散列出三级数据加密密钥;

数据加密封装过程如下:

接收明文数据包,获取数据包载荷数据;对需要加密的数据使用PKCS7Padding方式填充对齐,使用SM4算法和散列的三级加密密钥对数据加密;将协议特征HASH数据和加密数据重新封装数据包;重新计算数据包的校验和,包括IP头校验和和TCP/UDP头校验和;发送加密后的数据包;

数据解密密钥运算具体步骤如下:

网卡接收密文数据包,获取数据包载荷数据,其中前128位为协议特征HASH值,后面的为加密数据;

获取系统当前时间,读取根密钥;

使用根密钥对前128位为协议特征HASH值进行国密SM4加密运算,散列出一级密钥;使用根密钥对当前时间进行SM4运算,散列出二级密钥;一级密钥与二级密钥异或运算,散列出三级数据解密密钥;

数据解密过程如下:

网卡接收密文数据包,使用数据解密密钥通过SM4国密算法对数据包内容进行解密;

工业协议深度解析模块对解密后的数据包进行深度解析,查询需要参与密钥运算的预定义协议特征库,预定义的协议特征库为深度解析结果的任意几个字段,并对数据包中的协议特征库通过国密SM3算法计算256位的HASH值,然后前128位于后128位进行异或运算,最终的到128位的协议特征HASH值;

对得到的协议特征HASH值与收到的数据包载荷头部的HASH值对比,对比一致表示数据正确,否则数据可能被篡改,直接丢弃;重新封装数据包内容,去除协调特征HASH字段,还原明文数据包;转发数据包。

2.如权利要求1所述的基于工业协议的安全加密方法,其特征在于:所述的工业协议深度解析模块对数据包进行深度解析,包括modbus协议的寄存器种类、功能码、访问类型、PLC地址、寄存器地址。

一种基于工业协议的安全加密方法

技术领域

[0001] 本发明属于数据加密技术领域,涉及一种基于工业协议的安全加密方法。

背景技术

[0002] 当前市场加密产品还是以虚拟专用网(VPN)为主,VPN相关技术及产品目前市场已经非常成熟,目前使用比较多的VPN产品主要以IPSec VPN和SSLVPN为主,IP安全协议(IPSec)通过Internet密钥交换协议(IKE协议)进行秘钥协商后生成一个数据加密秘钥,并用这个秘钥对传输的数据进行封装和加密,SSL一般用在移动办公人员,另外一般还需要安装客户端软件或客户端插件。

[0003] 当前标准的VPN技术及产品也存在一定的不足和缺陷,一些漏洞和缺陷也经常被黑客所利用,比如IPSec VPN产品由于采用了DH交换,存在无法抵抗“中间人”攻击的漏洞,秘钥协商过程会泄漏协商者的身份,加密算法也都以国际算法为主,算法都比较公开。另外,IKE协商使用预共享密钥的身份认证方式,存在安全性低、技术落后、不符合我国相关密码政策等问题,随着信息化与工业化深度快速融合,众多国家关键基础设施在工业业务领域面临安全考验,该发明装置基于工业协议特征动态生成加密密钥,保证数据传输的安全,为工业业务场景提供更具适应性和更为安全性的全方位的数据安全加密解决方案。

[0004] 由于当前VPN产品存在如上问题,另外传统VPN配置复杂繁琐,工业环境需要互联的节点多,带宽小,传统VPN需要改变现有的网络拓扑结构,密钥协商也会增加额外的带宽开销,所以通过传统VPN产品根本无法在工业环境部署。

[0005] 因此设计了一种基于工业协议的安全加密方法,通过透明方式部署,无需对现有网络拓扑做任何修改,加密密钥基于工业协议特征动态生成,该装置可以对工业协议进行内容深度解析,客户可以自定义参与密钥运算的工业协调特征属性,加密密钥基于一个出厂预置的根密钥+工业协调特征+时间参数,通过根密钥和国密算法散列生成,保证密钥能实时更新,同时无需额外的密钥协商数据,减少网络带宽开销,根密钥预置,保证了密钥的绝对安全。

发明内容

[0006] 本发明的目的就是提供一种基于工业协议的安全加密方法,包括加密密钥运算、数据加密封装、解密密钥运算和数据解密。

[0007] 加密密钥运算具体步骤如下:

[0008] 网卡接收明文数据包,工业协议深度解析模块对数据包进行深度解析,比如modbus协议的寄存器种类、功能码、访问类型、PLC地址、寄存器地址。

[0009] 查询预定义的协议特征库,也就是需要参与密钥运算的内容,预定义的协议特征库可以为深度解析结果的任意几个字段,并对数据包中的协议特征数据通过国密SM3算法计算256位的HASH值(哈希值),然后前128位于后128位进行异或运算,最终的到128位的协议特征HASH值。

[0010] 获取系统当前时间，读取根密钥。

[0011] 使用根密钥对计算的128位HASH值进行国密SM4加密运算，散列出一级密钥；使用根密钥对当前时间进行SM4运算，散列出二级密钥；一级密钥与二级密钥异或运算，散列出三级数据加密密钥。

[0012] 数据加密封装过程如下：

[0013] 接收明文数据包，获取数据包载荷数据。

[0014] 对需要加密的数据使用PKCS7Padding方式填充对齐，因为使用SM4算法，所以加密数据长度必须是SM4算法密钥长度的整数倍。

[0015] 使用SM4算法和散列的三级加密密钥对数据加密，将协议特征HASH数据和加密数据重新封装数据包；重新计算数据包的校验和，包括IP头校验和和TCP/UDP头校验和；发送加密后的数据包。

[0016] 解密密钥运算具体步骤如下：

[0017] 网卡接收密文数据包，获取数据包载荷数据，其中前128位为协议特征HASH值，后面的为加密数据。

[0018] 获取系统当前时间，读取根密钥。

[0019] 使用根密钥对前128位协议特征HASH值进行国密SM4加密运算，散列出一级密钥；使用根密钥对当前时间进行SM4运算，散列出二级密钥；一级密钥与二级密钥异或运算，散列出三级数据解密密钥。

[0020] 数据解密过程如下：

[0021] 网卡接收密文数据包，使用数据解密密钥通过SM4国密算法对数据包内容进行解密。

[0022] 工业协议深度解析模块对解密后的数据包进行深度解析，比如modbus协议的寄存器种类、功能码、访问类型、PLC地址、寄存器地址等。

[0023] 查询预定义的协议特征库，也就是需要参与密钥运算的内容，预定义的协议特征库为深度解析结果的任意几个字段，并对数据包中的协议特征数据通过国密SM3算法计算256位的HASH值，然后前128位于后128位进行异或运算，最终的到128位的协议特征HASH值。

[0024] 对得到的协议特征HASH值与收到的数据包载荷头部的HASH值对比，对比一致表示数据正确，否则数据可能被篡改，直接丢弃。

[0025] 重新封装数据包内容，去除协调特征HASH字段，还原明文数据包；转发数据包。

[0026] 工业网络环境具有数据节点多，网络结构复杂，带宽比较低的特点，业网络环境部署传统加密产品对网络改动很大，不容易部署，增加带宽开销，还容易受到网络攻击，对业务会带来很多不稳定因素。本发明将根密钥固化在设备内部，外部无法获取，通过协议特征和时间参数散列三级密钥体系完成对数据的加密，解决在工业环境中数据的安全加密问题；通过工业协调的特征参数和时间参数参与密钥散列，实现加密数据一包一密；采用SM3国密算法，保证数据的完整性和正确性；完全透明方式部署，无需对现有拓扑结构做任何修改。

附图说明

[0027] 图1为加密密钥运算流程；

[0028] 图2为数据加密封装流程；

[0029] 图3为解密密钥运算流程图；

[0030] 图4为数据解密验证流程；

[0031] 图5为加密前后数据包内容示意图。

具体实施方式

[0032] 一种基于工业协议的安全加密方法，包括加密密钥运算、数据加密封装、解密密钥运算和数据解密：

[0033] 如图1所示，加密密钥运算具体包括如下步骤：

[0034] 网卡接收明文数据报文；

[0035] 将明文报文送往工业协议深度解析模块解析，如果解析成功，则查询预定义的需要参与密钥运算的协议特征库(由用户提前定义需要参与密钥运算的数据)，如果不是工业协议数据或深度解析失败，则通过数据五元组(数据的源地址、目的地址、源端口、目的端口、协议)作为协议特征数据；

[0036] 对协议特征数据通过SM3算法计算HASH值，输出256位的HASH数据，然后使用前128位和后128位异或运算，获得协议特征HASH数据，并作为一级密钥散列参数；

[0037] 使用根密钥通过SM4算法对协议特征HASH数据运算散列一级密钥；

[0038] 使用根密钥通过SM4算法对系统当前时间散列二级密钥；

[0039] 通过一级密钥和二级密钥异或运算，散列出三级数据加密密钥；

[0040] 如图2所示，数据加密封装过程具体为：

[0041] 接收明文数据包；

[0042] 获取数据包载荷数据；

[0043] 对需要加密的数据使用PKCS7Padding方式填充对齐，因为使用SM4算法，所以加密数据长度必须是SM4算法密钥长度的整数倍；

[0044] PKCS7Padding方式具体为：数据加密前需要对数据进行按照密钥长度的整数被对齐，假设数据长度需要填充n(n>0)个字节才对齐，那么填充n个字节，每个字节都是n；如果数据本身就已经对齐了，则填充一块长度为块大小的数据，每个字节都是块大小。

[0045] 使用SM4算法和散列的三级加密密钥对数据加密；

[0046] 将协议特征HASH数据和加密数据重新封装数据包；

[0047] 重新计算数据包的校验和，包括IP头校验和和TCP/UDP头校验和；

[0048] 发送加密后的数据包；

[0049] 如图3所示，解密密钥运算过程具体为：

[0050] 网卡接收加密数据报文；

[0051] 获取载荷数据前128位数据，获得协议特征HASH数据，该段数据为明文的工业协议特征数据的HASH值，通过该段数据散列解密密钥；

[0052] 使用根密钥通过SM4算法对协议特征HASH数据运算散列一级密钥；

[0053] 使用根密钥通过SM4算法对系统当前时间散列二级密钥；

[0054] 通过一级密钥和二级密钥异或运算，散列出三级数据解密密钥；

[0055] 如图4所示，数据解密具体包括如下步骤：

[0056] 接收加密数据包；

[0057] 提取数据包载荷数据前128位协议特征HASH数据；

[0058] 通过协议HASH数据和系统时间散列解密密钥；

[0059] 解密加密载荷数据；

[0060] 对解密后的数据进行工业协议深度解析；

[0061] 工业协议解析成功，则查询预定义的需要参与密钥运算的协议特征库，然后对协议特征数据通过SM3算法计算HASH值，使用前128位和后128位异或运算，获得解密后的协议特征HASH数据；工业协议解析失败，则使用五元组数据作为工业协议特征数据；

[0062] 解密后的HASH数据与接收到的载荷数据中的HASH或五元组HASH对比，对比成功，表示数据正常；对比失败表示数据被篡改或解密错误，直接丢弃；

[0063] 重新封装明文数据报文，并重新计算报文的校验和，包括IP头和TCP或UDP头的校验和；

[0064] 发送解密后的数据包；

[0065] 如图5所示，载荷数据为实际工业协议数据，为TCP或UDP头后面的数据，本发明数据加密不修改IP头和TCP/UDP头数据，所以无需修改现有拓扑结构，直接透明串联接入即可。

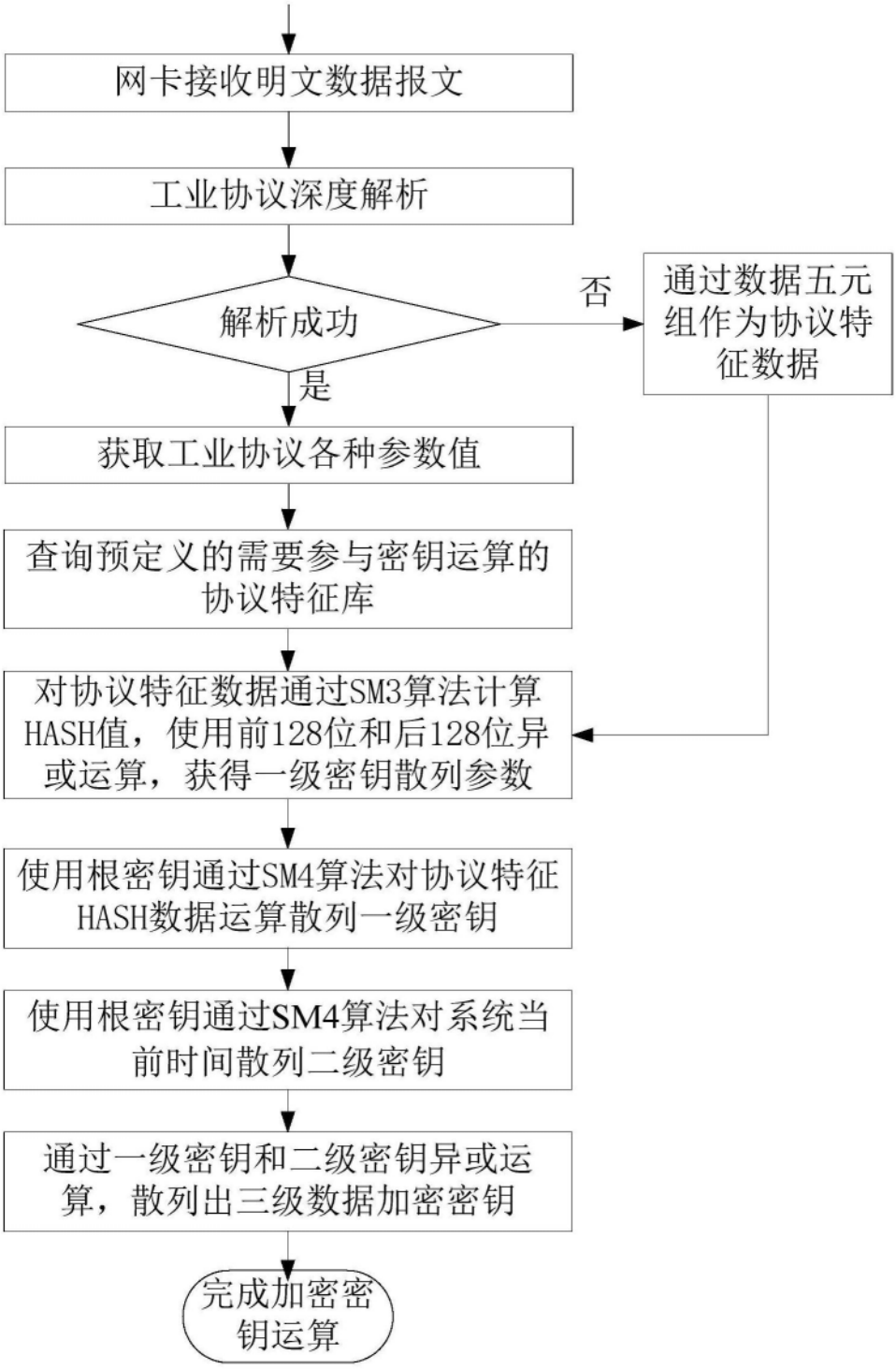

网卡接收明文数据报文
工业协议深度解析
解析成功
否
通过数据五元组作为协议特征数据
是
获取工业协议各种参数值
查询预定义的需要参与密钥运算的协议特征库
对协议特征数据通过SM3算法计算HASH值，使用前128位和后128位异或运算，获得一级密钥散列参数
使用根密钥通过SM4算法对协议特征HASH数据运算散列一级密钥
使用根密钥通过SM4算法对系统当前时间散列二级密钥
通过一级密钥和二级密钥异或运算，散列出三级数据加密密钥
完成加密密钥运算

图1


接收明文数据包
获取数据包载荷数据
计算需要加密数据的长度
对需要加密的数据使用PKCS7Padding方式填充对齐
使用SM4算法和散列的三级加密密钥对数据加密
将协议特征HASH数据和加密数据重新封装数据包
重新计算数据包的校验和
发送加密数据包

图2

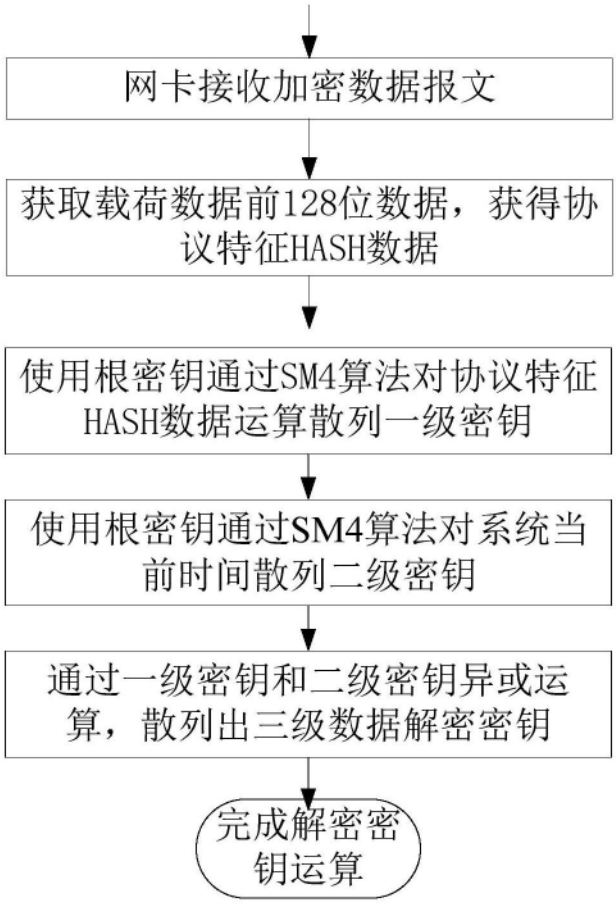

网卡接收加密数据报文
获取载荷数据前128位数据，获得协议特征HASH数据
使用根密钥通过SM4算法对协议特征HASH数据运算散列一级密钥
使用根密钥通过SM4算法对系统当前时间散列二级密钥
通过一级密钥和二级密钥异或运算，散列出三级数据解密密钥
完成解密密钥运算

图3

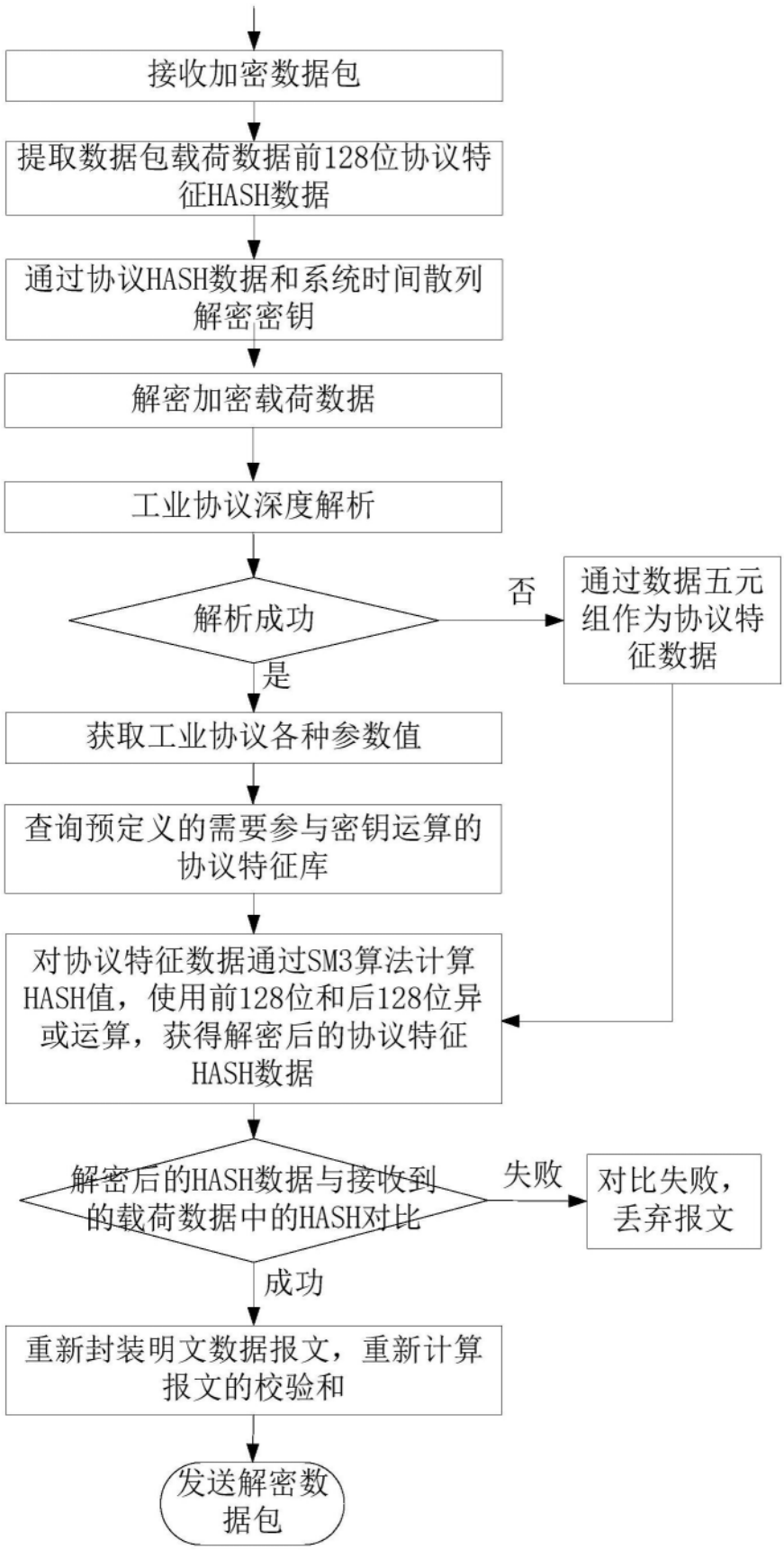

接收加密数据包
提取数据包载荷数据前128位协议特征HASH数据
通过协议HASH数据和系统时间散列解密密钥
解密加密载荷数据
工业协议深度解析
解析成功
否
通过数据五元组作为协议特征数据
是
获取工业协议各种参数值
查询预定义的需要参与密钥运算的协议特征库
对协议特征数据通过SM3算法计算HASH值，使用前128位和后128位异或运算，获得解密后的协议特征HASH数据
解密后的HASH数据与接收到的载荷数据中的HASH对比
失败
对比失败，丢弃报文
成功
重新封装明文数据报文，重新计算报文的校验和
发送解密数据包

图4

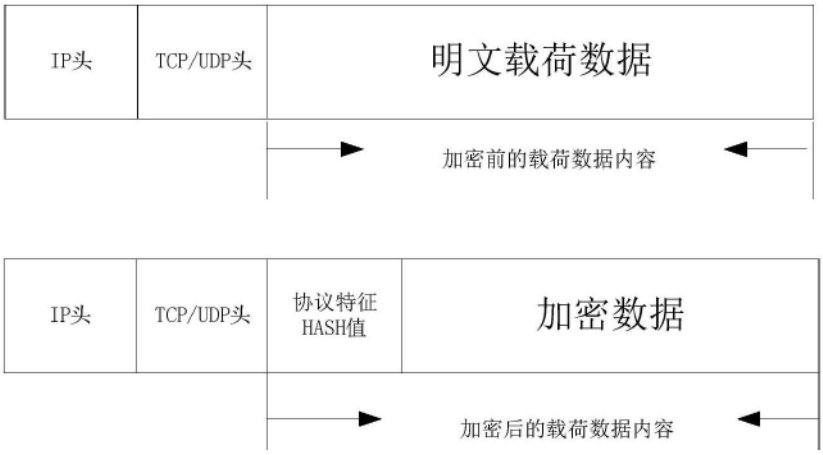

IP头
TCP/UDP头
明文载荷数据
加密前的载荷数据内容
IP头
TCP/UDP头
协议特征
HASH值
加密数据
加密后的载荷数据内容

图5