

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2015 年 10 月 8 日 (08.10.2015)



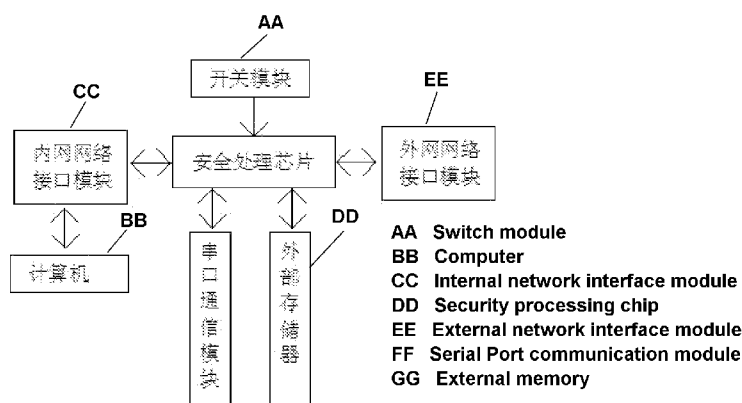
(10) 国际公布号
WO 2015/149669 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2015/075441
- (22) 国际申请日: 2015 年 3 月 31 日 (31.03.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201410133919.8 2014 年 4 月 3 日 (03.04.2014) CN
- (71) 申请人: 国家电网公司 (STATE GRID CORPORATION OF CHINA) [CN/CN]; 中国北京市西城区西长安街 86 号, Beijing 100031 (CN)。 国网河南省电力公司电力科学研究院 (STATE GRID HENAN ELECTRIC POWER CORPORATION ELECTRIC POWER SCIENCE RESEARCH INSTITUTE) [CN/CN]; 中国河南省郑州市二七区嵩山南路 85 号, Henan 450052 (CN)。
- (72) 发明人: 吕卓 (LV, Zhuo); 中国河南省郑州二七区嵩山南路 85 号, Henan 450052 (CN)。 张威 (ZHANG, Wei); 中国河南省郑州二七区嵩山南路 85 号, Henan 450052 (CN)。 莫坚松 (MO, Jiansong); 中国河南省郑州二七区嵩山南路 85 号, Henan 450052 (CN)。 张之刚 (ZHANG, Zhigang); 中国河南省郑州市二七区嵩山南路 85 号, Henan 450052 (CN)。
- (74) 代理人: 郑州联科专利事务所 (普通合伙) (ZHENGZHOU LIANKE PATENT AGENCY(COMMON PARTNERSHIP)); 中国河南省郑州市金水区红专路 58 号, Henan 450002 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ,

[见续页]

(54) Title: TRUSTED NETWORK ATTACK FILTERING DEVICE AND NETWORK ATTACK FILTERING METHOD

(54) 发明名称: 一种可信的网络攻击过滤装置及网络攻击过滤方法



【图号】 图 1 /FIG. 1

(57) Abstract: Disclosed are a trusted network attack filtering device and a network attack filtering method, comprising a network interface module and a security control module; the network interface module is used to receive and transmit an IP data packet; the security control module is used to identify the received IP data packet transmitted by a protected computer, and to parse and judge the received IP data packet transmitted by an external communication network. The present invention utilizes summary calculation to determine whether an IP data packet has been tampered with or forged, precisely differentiate between authorized and unauthorized data packets, and filter attacks from outside the system; in addition, the present invention can defend against replay attacks initiated by attackers by comparing sent serial numbers and received serial numbers, thus efficiently protecting network devices.

(57) 摘要:

[见续页]



WO 2015/149669 A1



BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

本发明公开了一种可信的网络攻击过滤装置及网络攻击过滤方法，包括网络接口模块和安全控制模块；网络接口模块用于完成 IP 数据包的收发；安全控制模块用于对所接收的被保护的计算机发送的 IP 数据包进行标识以及对所接收的外部通讯网络发送的 IP 数据包进行解析判别。本发明利用摘要运算判断 IP 数据包是否被篡改和伪造，精确区分合法与非法的数据包，过滤来自系统外部的攻击；同时，本发明利用比较发送序列号和接收序列号大小，能够抵御攻击者发出的重放攻击，有效地实现网络设备保护。

说明书

发明名称：一种可信的网络攻击过滤装置及网络攻击过滤方法

- [1] 技术领域
- [2] 本发明涉及网络安全防御领域，尤其涉及一种能够精确标识网络IP数据包并在标识的基础上精确过滤非法IP数据包的网络攻击过滤装置及网络攻击过滤方法。
- [3] 背景技术
- [4] 网络通信的发展大大推动了整个社会的发展，各个行业均不同程度地采用网络进行信息通信。但是，当前基于IP的网络通信在设计之初并没有充分考虑安全因素，因此网络设备经常受到来自网络的攻击，这些攻击造成了很大危害。因此，为提高网络安全性，防火墙、入侵检测、加密VPN等设备相继推出，在一定程度上提高了网络安全性。
- [5] 目前，主流的网络安全防御设备有防火墙、入侵检测和加密VPN等，每种设备均能起到一定的安全作用，但也存在弊端。
- [6] 防火墙主要基于IP数据包过滤技术来抵御网络攻击，当网络IP数据包到达防火墙时，防火墙根据预先设定的过滤规则检查IP数据包，放行允许的IP数据包，丢弃禁止的IP数据包。基于上述原理，防火墙能够抵御很多攻击，但是攻击者能够通过构造合乎过滤规则的IP数据包来欺骗并绕过防火墙或直接攻击防火墙。
- [7] 入侵检测主要基于特征检测和异常检测来确定攻击，本质上是基于网络IP数据包的活动规律来分析、综合、提取某种网络行为模式或规律，然后根据该行为模式或规律来判断IP数据包是否具有入侵性。但上述两种方式在原理上存在将正常IP数据包判断为入侵IP数据包或者入侵IP数据包当做合法IP数据包的可能，入侵检测很难做出精准的检测。
- [8] 加密VPN通过在网络通信双方建立加密的安全通道来进行通信，由于采用了密码学原理，因此可以做到对IP数据包的精确辨别，区分攻击包与合法包。但是设备本身的实现较为复杂，导致设备程序自身的正确性与安全性在原理上不能保证，存在设备本身被攻破的可能，同时在实际应用中，对数据进行加密会降低网络的数据吞吐率，且很多应用没有加密需求，增加了部署成本。

- [9] 从上述设备的分析可以看出，因为IP网络协议设计之初没有充分考虑安全因素，网络IP数据包自身没有可信的标识，容易发生通过伪造或篡改IP数据包以躲过网络安全防御装置，进而达到攻击目的的现象；同时，当前成本较高的VPN设备的复杂性导致的自身安全性问题降低了其安全防御级别，因此需要一种部署成本低、自身高度安全的网络防御设备，通过精确判别IP数据包的来源，区分合法IP数据包与攻击包，实现网络设备的有效保护。
- [10] 发明内容
- [11] 本发明的目的是提供一种可信的网络攻击过滤装置及网络攻击过滤方法，能够精确标识网络IP数据包，并在标识的基础上精确过滤非法IP数据包，实现网络设备的有效保护。
- [12] 本发明采用下述技术方案：
- [13] 一种可信的网络攻击过滤装置，包括网络接口模块和安全控制模块；
- [14] 所述的网络接口模块用于完成IP数据包的收发，网络接口模块包括外网网络接口模块和内网网络接口模块；外网网络接口模块连接安全控制模块和外部通信网络，用于接收外部通讯网络所发送的IP数据包并传送给安全控制模块，以及接收安全控制模块所发送的IP数据包并通过外部通信网络进行发送；内网网络接口模块连接内网中被保护的计算机和安全控制模块，用于接收安全控制模块所发送的IP数据包并传送给内网中被保护的计算机，以及接收内网中被保护的计算机所发送的IP数据包并传送给安全控制模块；
- [15] 所述的安全控制模块用于对所接收的被保护的计算机发送的IP数据包进行标识以及对所接收的外部通讯网络发送的IP数据包进行解析判别；安全控制模块内存储有与相应目的地址和来源地址对应的密钥、发送序列号及接收序列号，当安全控制模块接收到内网中被保护的计算机所发送的IP数据包时，安全控制模块读取该IP数据包并提取IP数据包目的地址，根据目的地址获取对应的密钥和发送序列号，将发送序列号置于IP数据包尾部，利用密钥对IP数据包和发送序列号进行摘要运算，将摘要运算结果附于发送序列号之后，并根据当前长度调整IP首部信息中的长度指示信息，然后将添加标识后的IP数据包通过外网网络接口模块发送至外部通讯网络；当安全控制模块接收到外部通讯网络所发送的IP数据包时，安

全控制模块读取该IP数据包并提取IP数据包来源地址，根据IP数据包来源地址获取对应的密钥和接收序列号，安全控制模块利用密钥对IP数据包中被保护的内容和发送序列号进行摘要运算，并将运算结果与IP数据包中自带的摘要运算结果进行比较，如果结果比较不一致则认为IP数据包被篡改和伪造，将此IP数据包丢弃；如果结果比较一致则判断IP数据包没有被篡改和伪造，继续比较从IP数据包中读取的发送序列号和接收序列号的大小，若发送序列号大于接收序列号则认为IP数据包合法，安全控制模块接收该IP数据包并将此IP数据包发送至内网中被保护的计算机；如果发送序列号小于等于接收序列号则认为IP数据包非法，将此IP数据包丢弃。

[16] 所述的安全控制模块包括安全处理芯片和与安全处理芯片连接的外部存储器。

[17] 所述的安全处理芯片还连接有开关模块和串口通信模块，开关模块的信号输出端连接安全处理芯片的信号输入端，开关模块用于向安全处理芯片输入高电平或低电平信号，安全处理芯片根据接收到开关模块发送的不同信号分别进入IP数据包标识和解析判别工作模式或配置程序运行模式，配置程序运行模式下安全处理芯片仅通过串口通信模块与外界进行通信。

[18] 所述的网络接口模块采用支持IEEE802.3的以太网规范的接口芯片。

[19] 所述的开关模块采用电路开关。

[20] 所述的串口通信模块采用支持RS232标准的异步串行通信接口芯片。

[21] 一种利用如权利要求1所述的可行的网络攻击过滤装置实现的网络攻击过滤方法，包括以下步骤：

[22] A：将每一台内网中被保护的计算机与外部通信网络之间连接一个网络攻击过滤装置，

当某一个网络攻击过滤装置中的安全控制模块接收到IP数据包时判断IP数据包来源，如果接收到的IP数据包来源为与此网络攻击过滤装置连接的计算机时，进入步骤B；如果接收到的IP数据包来源为另一个网络攻击过滤装置时，进入步骤F；

[23] B：安全控制模块读取该IP数据包并提取IP数据包目的地址，然后进入步骤C；

[24] C：安全控制模块根据IP数据包目的地址获取对应的密钥和发送序列号，然后

进入步骤D;

- [25] D: 安全控制模块将发送序列号置于IP数据包尾部, 利用密钥对IP数据包和发送序列号进行摘要运算, 将摘要运算结果附于发送序列号之后, 并根据当前长度调整IP首部信息中的长度指示信息, 然后进入步骤E;
- [26] E: 安全控制模块将标识后的IP数据包通过外网网络接口模块发送至外部通讯网络, 完成IP数据包标识操作, 然后返回步骤A;
- [27] F: 安全控制模块读取该IP数据包并提取IP数据包来源地址, 然后进入步骤G;
- [28] G: 安全控制模块根据IP数据包来源地址获取对应的密钥和接收序列号, 然后进入步骤H;
- [29] H: 安全控制模块利用密钥对IP数据包中被保护的内容和发送序列号进行摘要运算, 并将运算结果与IP数据包中自带的摘要运算结果进行比较, 如果结果比较一致则判断IP数据包没有被篡改和伪造, 然后进入步骤I; 如果结果比较不一致则认为IP数据包被篡改和伪造, 将此IP数据包丢弃, 然后返回步骤A;
- [30] I: 安全控制模块读取IP数据包中的发送序列号和接收序列号, 并比较发送序列号和接收序列号大小, 如果发送序列号大于接收序列号, 则认为IP数据包合法, 接收该IP数据包并将此IP数据包发送至内网中被保护的计算机; 如果发送序列号小于等于接收序列号, 则认为IP数据包非法, 将此IP数据包丢弃, 然后返回步骤A。
- [31] 本发明在内网中被保护的计算机向外发送的IP数据包时, 利用密钥对IP数据包和发送序列号进行摘要运算, 将摘要运算结果和发送序列号作为标识附于IP数据包后部, 然后将包含标识的IP数据包通过外网网络接口模块发送至外部通讯网络; 在接收外部通讯网络所发送的IP数据包时, 安全控制模块根据来源地址获取对应的密钥对IP数据包中被保护的内容和发送序列号进行摘要运算, 并将运算结果与IP数据包中自带的摘要运算结果进行比较判断IP数据包是否被篡改和伪造, 精确区分合法与非法的数据包, 过滤来自系统外部的攻击; 同时, 本发明利用安全控制模块读取并比较IP数据包中的发送序列号和接收序列号大小, 能够抵御攻击者发出的重放攻击, 有效地实现网络设备保护。进一步的, 本发明利用硬件开关隔离安全处理芯片两种运行逻辑, 安全处理芯片执行配置程序不通过网络

进行，只能通过串口通信模块进行，能够有效阻止通过网络接口模块发起的针对安全处理芯片本身的攻击，安全性大为提高。

[32] 附图说明

[33] 图1为本发明所述可信的网络攻击过滤装置的原理框图；

[34] 图2为本发明所述网络攻击过滤方法的流程示意图；

[35] 图3为IP数据包标识原理示意图；

[36] 图4为两台计算机分别通过网络攻击过滤装置进行数据通信的原理框图。

[37] 具体实施方式

[38] 如图1所示，本发明包括网络接口模块和安全控制模块，网络接口模块用于完成IP数据包的收发，安全控制模块用于对所接收的被保护的计算机发送的IP数据包进行标识以及对所接收的外部通讯网络发送的IP数据包进行解析判别。

[39] 所述的网络接口模块包括外网网络接口模块和内网网络接口模块，外网网络接口模块连接安全控制模块和外部通信网络，用于接收外部通讯网络所发送的IP数据包并传送给安全控制模块，以及接收安全控制模块所发送的IP数据包并通过外部通信网络进行发送；内网网络接口模块连接内网中被保护的计算机和安全控制模块，用于接收安全控制模块所发送的IP数据包并传送给内网中被保护的计算机，以及接收内网中被保护的计算机所发送的IP数据包并传送给安全控制模块。

[40] 安全控制模块包括安全处理芯片和与安全处理芯片连接的外部存储器，安全芯片具有ROM、EFLASH、RAM存储单元，安全芯片内部存储单元内存储有与相应目的地址和来源地址对应的密钥、发送序列号及接收序列号，当安全控制模块接收到内网中被保护的计算机所发送的IP数据包时，安全控制模块读取该IP数据包并提取IP数据包目的地址，根据目的地址获取对应的密钥和发送序列号，将发送序列号置于IP数据包尾部，利用密钥对IP数据包和发送序列号进行摘要运算，将摘要运算结果附于发送序列号之后，并根据当前长度调整IP首部信息中的长度指示信息，然后将添加标识后的IP数据包通过外网网络接口模块发送至外部通讯网络。IP数据包标识原理示意图如图3所示。当安全控制模块接收到外部通讯网络所发送的IP数据包时，安全控制模块读取该IP数据包并提取IP数据包来源地址，根据IP数据包来源地址获取对应的密钥和接收序列号，安全控制模块利用密

钥对IP数据包中被保护的内容和发送序列号进行摘要运算，并将运算结果与IP数据包中自带的摘要运算结果进行比较，如果结果比较不一致则认为IP数据包被篡改和伪造，将此IP数据包丢弃；如果结果比较一致则判断IP数据包没有被篡改和伪造，继续比较从IP数据包中读取的发送序列号和接收序列号的大小，若发送序列号大于接收序列号则认为IP数据包合法，安全控制模块接收该IP数据包并将此IP数据包发送至内网中被保护的计算机；如果发送序列号小于等于接收序列号则认为IP数据包非法，将此IP数据包丢弃。

- [41] 安全处理芯片所连接的外部存储器内存储有安全处理芯片配置程序，安全处理芯片还连接有开关模块和串口通信模块，开关模块的信号输出端连接安全处理芯片的信号输入端，开关模块用于向安全处理芯片输入高电平或低电平信号，安全处理芯片根据接收到开关模块发送的不同信号分别进入IP数据包接收处理工作模式或配置程序运行模式，配置程序运行模式下安全处理芯片仅通过串口通信模块与外界进行通信。当安全处理芯片执行IP数据包接收处理工作模式时，安全处理芯片从内部启动，即安全处理芯片从内部存储单元中读取程序并执行，安全处理芯片不能访问外部存储器，能够保证不会篡改外部存储中的程序，进而保证了配置程序的安全。当安全处理芯片执行配置程序运行模式时，安全处理芯片从外部存储器中读取配置程序并执行，配置程序在用户的计算机中运行，用户计算机通过串口通信模块与安全处理芯片进行通信，此时安全处理芯片中运行配置程序，与用户的计算机形成C/S的工作模式。本发明利用硬件开关隔离安全处理芯片两种运行逻辑，安全处理芯片执行配置程序不通过网络进行，能够有效阻止通过网络接口模块发起的针对安全处理芯片本身的攻击，不论安全处理芯片的配置程序有无漏洞，攻击者均不能修改安全处理芯片的配置程序，安全性大为提高。

- [42] 本实施例中，网络接口模块采用支持IEEE802.3等以太网规范的接口芯片，称为网卡芯片，能够支持以太网数据包的收发。为提高整体安全性，网卡芯片选择国产芯片。安全处理芯片，指具有安全功能的控制芯片，安全功能指能够进行密码运算且自身具有较强的防多种攻击措施，密码运算可采用摘要运算，自身具有的防攻击措施包括芯片具有的多层特殊版图设计、电压检测、存储区加

密保护、光照检测、MPU（内存保护单元）等防范物理攻击、软件攻击的保护措施。开关模块可采用电路开关，电路开关的开合可以向安全处理芯片发出低电平、高电平两种不同的控制信号。串口通信模块可采用支持RS232标准的异步串行通信接口芯片，通信时需要专用的串口电缆分别连接该异步串行通信接口芯片与用户配置用计算机上的异步串行通信接口芯片（一般称为COM口）。外部存储器可采用FLASH芯片，FLASH芯片为通用的一种存储芯片，在掉电情况下保存数据，可以通过FLASH芯片的外部接口对FLASH芯片进行读、写、擦除等操作。

[43] 如图2所示，本发明所述的网络攻击过滤方法，包括以下步骤：

[44] A：将每一台内网中被保护的计算机与外部通信网络之间连接一个网络攻击过滤装置，

当某一个网络攻击过滤装置中的安全控制模块接收到IP数据包时判断IP数据包来源，如果接收到的IP数据包来源为与此网络攻击过滤装置连接的计算机时，进入步骤B；如果接收到的IP数据包来源为另一个网络攻击过滤装置时，进入步骤F；

[45] B：安全控制模块读取该IP数据包并提取IP数据包目的地址，然后进入步骤C；

[46] C：安全控制模块根据IP数据包目的地址获取对应的密钥和发送序列号，然后进入步骤D；

[47] D：安全控制模块将发送序列号置于IP数据包尾部，利用密钥对IP数据包和发送序列号进行摘要运算，将摘要运算结果附于发送序列号之后，并根据当前长度调整IP首部信息中的长度指示信息，然后进入步骤E；

[48] E：安全控制模块将标识后的IP数据包通过外网网络接口模块发送至外部通讯网络，完成IP数据包标识操作，然后返回步骤A；

[49] F：安全控制模块读取该IP数据包并提取IP数据包来源地址，然后进入步骤G；

[50] G：安全控制模块根据IP数据包来源地址获取对应的密钥和接收序列号，然后进入步骤H；

[51] H：安全控制模块利用密钥对IP数据包中被保护的内容和发送序列号进行摘要运算，并将运算结果与IP数据包中自带的摘要运算结果进行比较，如果结果比较

一致则判断IP数据包没有被篡改和伪造，然后进入步骤I；如果结果比较不一致则认为IP数据包被篡改和伪造，将此IP数据包丢弃，然后返回步骤A；

[52] I: 安全控制模块读取IP数据包中的发送序列号和接收序列号，并比较发送序列号和接收序列号大小，如果发送序列号大于接收序列号，则认为IP数据包合法，接收该IP数据包并将此IP数据包发送至内网中被保护的计算机；如果发送序列号小于等于接收序列号，则认为IP数据包非法，将此IP数据包丢弃，然后返回步骤A。

[53] 本发明中的IP数据包由首部和数据两部分组成，首部中包含的来源地址和目的地址均为IP协议地址。本发明中的摘要运算为密码学中的基础算法之一，也称为哈希（Hash）算法或散列算法。

[54] 以下结合具体实施例，进一步说明本发明所述的网络攻击过滤方法。本实施例中，如图4所示，第一计算机通过第一网络攻击过滤装置与外部通信网络连接，第二计算机通过第二网络攻击过滤装置与外部通信网络连接。

[55] 当第一计算机需要向第二计算机发送IP数据包时，第一计算机首先向第一网络攻击过滤装置发送IP数据包，第一网络攻击过滤装置的安全控制模块读取该IP数据包并提取IP数据包目的地址，即第二计算机的地址，然后安全控制模块根据IP数据包目的地址获取对应的密钥和发送序列号，将发送序列号置于IP数据包尾部，利用密钥对IP数据包和发送序列号进行摘要运算，将摘要运算结果附于发送序列号之后，并根据当前长度调整IP首部信息中的长度指示信息，最后第一网络攻击过滤装置的安全控制模块将标识后的IP数据包通过外网网络接口模块利用外部通讯网络发送至第二计算机，完成IP数据包标识操作；

[56] 当第一计算机发送的IP数据包到达第二网络攻击过滤装置时，第二网络攻击过滤装置外网网络接口模块接收此IP数据包并此IP数据包发送至第二网络攻击过滤装置的安全控制模块，第二网络攻击过滤装置的安全控制模块读取该IP数据包并提取IP数据包来源地址，根据IP数据包来源地址获取对应的密钥和接收序列号，然后第二网络攻击过滤装置的安全控制模块利用密钥对IP数据包中被保护的内容和发送序列号进行摘要运算，并将运算结果与IP数据包中自带的摘要运算结果进行比较，如果结果比较不一致则认为IP数据包被篡改和伪造，将此IP数据包丢弃

；如果结果比较一致则判断IP数据包没有被篡改和伪造，第二网络攻击过滤装置的安全控制模块读取IP数据包中的发送序列号和接收序列号，并比较发送序列号和接收序列号大小，如果发送序列号大于接收序列号，则认为IP数据包合法，第二网络攻击过滤装置的安全控制模块接收该IP数据包并将此IP数据包发送至第二计算机；如果发送序列号小于等于接收序列号，则认为IP数据包非法，第二网络攻击过滤装置的安全控制模块将此IP数据包丢弃。

- [57] 本发明通过在IP数据包中增加摘要信息和序列号信息，摘要信息的计算建立在密钥与密码算法基础之上，在理论上能够确保通过摘要判断数据包的篡改和伪造；序列号信息的判断能够抵御攻击者发出的重放攻击。本发明通过上述机制能够精确区分合法与非法的数据包，过滤来自系统外部的攻击。本发明没有采用当前复杂的网络密码安全协议，功能简单，方便实现，具体实现可以通过形式化方法验证，确保实现本身的正确与安全。本发明还利用硬件开关隔离安全处理芯片两种运行逻辑，安全处理芯片执行配置程序不通过网络进行，只能通过串口通信模块进行，能够有效阻止通过网络接口模块发起的针对安全处理芯片本身的攻击，安全性大为提高。

权利要求书

[权利要求 1]

一种可信的网络攻击过滤装置，其特征在于：包括网络接口模块和安全控制模块；

所述的网络接口模块用于完成IP数据包的收发，网络接口模块包括外网网络接口模块和内网网络接口模块；外网网络接口模块连接安全控制模块和外部通信网络，用于接收外部通讯网络所发送的IP数据包并传送给安全控制模块，以及接收安全控制模块所发送的IP数据包并通过外部通信网络进行发送；内网网络接口模块连接内网中被保护的计算机和安全控制模块，用于接收安全控制模块所发送的IP数据包并传送给内网中被保护的计算机，以及接收内网中被保护的计算机所发送的IP数据包并传送给安全控制模块；

所述的安全控制模块用于对所接收的被保护的计算机发送的IP数据包进行标识以及对所接收的外部通讯网络发送的IP数据包进行解析判别；安全控制模块内存储有与相应目的地址和来源地址对应的密钥、发送序列号及接收序列号，当安全控制模块接收到内网中被保护的计算机所发送的IP数据包时，安全控制模块读取该IP数据包并提取IP数据包目的地址，根据目的地址获取对应的密钥和发送序列号，将发送序列号置于IP数据包尾部，利用密钥对IP数据包和发送序列号进行摘要运算，将摘要运算结果附于发送序列号之后，并根据当前长度调整IP首部信息中的长度指示信息，然后将添加标识后的IP数据包通过外网网络接口模块发送至外部通讯网络；当安全控制模块接收到外部通讯网络所发送的IP数据包时，安全控制模块读取该IP数据包并提取IP数据包来源地址，根据IP数据包来源地址获取对应的密钥和接收序列号，安全控制模块利用密钥对IP数据包中被保护的内容和发送序列号进行摘要运算，并将运算结果与IP数据包中自带的摘要运算结果进行比较，如果结果比较不一致则认为IP数据包被篡改和伪造，将此IP数据包丢

弃；如果结果比较一致则判断IP数据包没有被篡改和伪造，继续比较从IP数据包中读取的发送序列号和接收序列号的大小，若发送序列号大于接收序列号则认为IP数据包合法，安全控制模块接收该IP数据包并将此IP数据包发送至内网中被保护的计算机；如果发送序列号小于等于接收序列号则认为IP数据包非法，将此IP数据包丢弃。

[权利要求 2] 根据权利要求1所述的可信的网络攻击过滤装置，其特征在于：所述的安全控制模块包括安全处理芯片和与安全处理芯片连接的外部存储器。

[权利要求 3] 根据权利要求2所述的可信的网络攻击过滤装置，其特征在于：所述的安全处理芯片还连接有开关模块和串口通信模块，开关模块的信号输出端连接安全处理芯片的信号输入端，开关模块用于向安全处理芯片输入高电平或低电平信号，安全处理芯片根据接收到开关模块发送的不同信号分别进入IP数据包标识和解析判别工作模式或配置程序运行模式，配置程序运行模式下安全处理芯片仅通过串口通信模块与外界进行通信。

[权利要求 4] 根据权利要求3所述的可信的网络攻击过滤装置，其特征在于：所述的网络接口模块采用支持IEEE802.3的以太网规范的接口芯片。

[权利要求 5] 根据权利要求4所述的可信的网络攻击过滤装置，其特征在于：所述的开关模块采用电路开关。

[权利要求 6] 根据权利要求5所述的可信的网络攻击过滤装置，其特征在于：所述的串口通信模块采用支持RS232标准的异步串行通信接口芯片。

[权利要求 7] 一种利用如权利要求1所述的可信的网络攻击过滤装置实现的网络攻击过滤方法，其特征在于，包括以下步骤：

A：将每一台内网中被保护的计算机与外部通信网络之间连接一个网络攻击过滤装置，当某一个网络攻击过滤装置中的安全控制模块接收到IP数据包时判断IP数据包来源，如果接收到的IP数据包来源为与此网络攻击过滤装置连接的计算机时，进入步骤B；如果接

收到的IP数据包来源为另一个网络攻击过滤装置时，进入步骤F；

B：安全控制模块读取该IP数据包并提取IP数据包目的地址，然后进入步骤C；

C：安全控制模块根据IP数据包目的地址获取对应的密钥和发送序列号，然后进入步骤D；

D：安全控制模块将发送序列号置于IP数据包尾部，利用密钥对IP数据包和发送序列号进行摘要运算，将摘要运算结果附于发送序列号之后，并根据当前长度调整IP首部信息中的长度指示信息，然后进入步骤E；

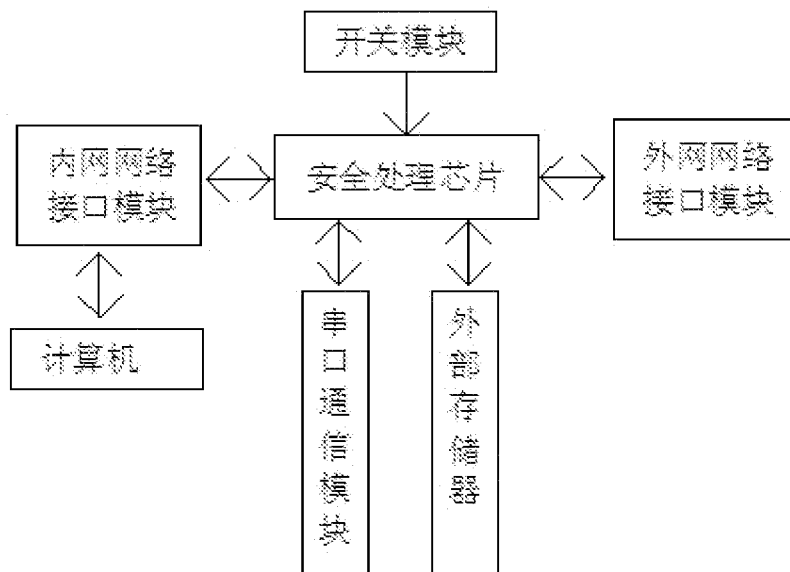
E：安全控制模块将标识后的IP数据包通过外网网络接口模块发送至外部通讯网络，完成IP数据包标识操作，然后返回步骤A；

F：安全控制模块读取该IP数据包并提取IP数据包来源地址，然后进入步骤G；

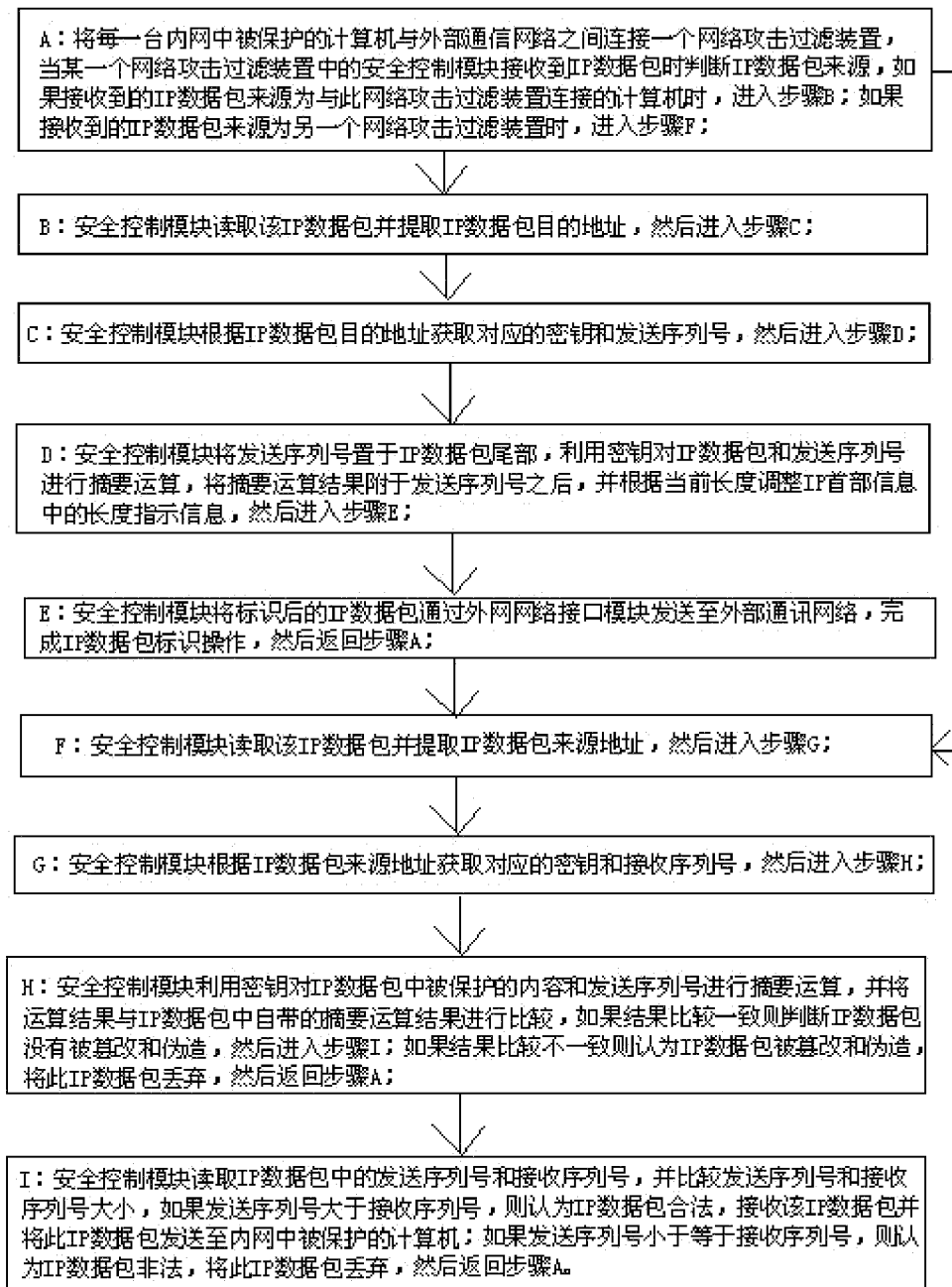
G：安全控制模块根据IP数据包来源地址获取对应的密钥和接收序列号，然后进入步骤H；

H：安全控制模块利用密钥对IP数据包中被保护的内容和发送序列号进行摘要运算，并将运算结果与IP数据包中自带的摘要运算结果进行比较，如果结果比较一致则判断IP数据包没有被篡改和伪造，然后进入步骤I；如果结果比较不一致则认为IP数据包被篡改和伪造，将此IP数据包丢弃，然后返回步骤A；

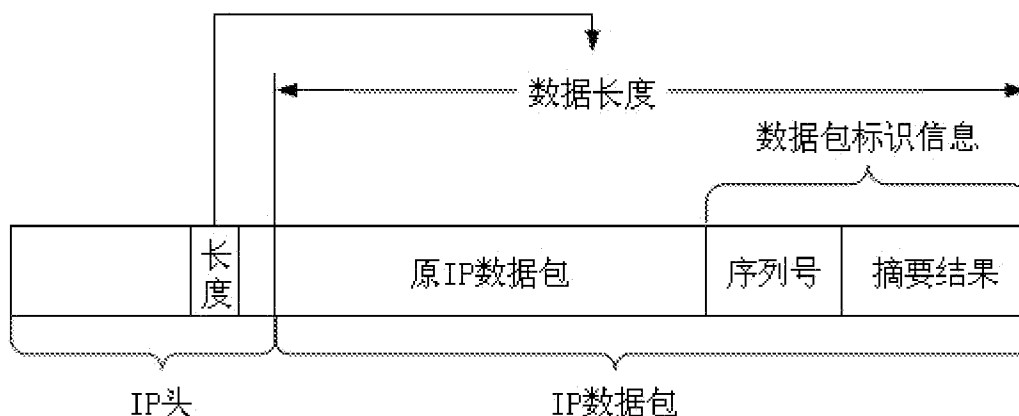
I：安全控制模块读取IP数据包中的发送序列号和接收序列号，并比较发送序列号和接收序列号大小，如果发送序列号大于接收序列号，则认为IP数据包合法，接收该IP数据包并将此IP数据包发送至内网中被保护的计算机；如果发送序列号小于等于接收序列号，则认为IP数据包非法，将此IP数据包丢弃，然后返回步骤A。



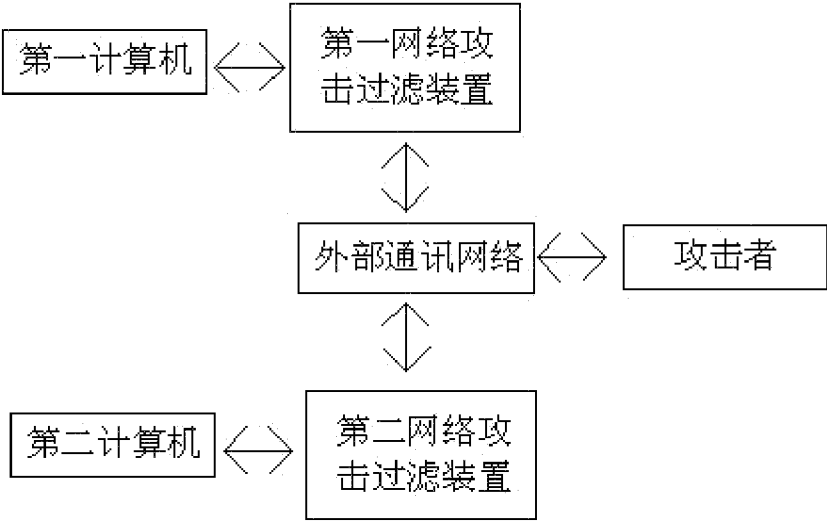
【图号】 图 1



【图号】 图 2



【图号】 图 3



【图号】 图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/075441

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS, CNKI, CNTXT, VEN: sequence number; IP, data, packet, abstract, summary, digest, calculation, computation, compare, sequence, number

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 103905452 A (STATE GRID CORPORATION OF CHINA et al.), 02 July 2014 (02.07.2014), claims 1-7	1-7
A	CN 102065067 A (H3C TECHNOLOGIES CO., LIMITED), 18 May 2011 (18.05.2011), the whole document	1-7
A	CN 103118363 A (CHINA TELECOM CORPORATION LIMITED), 22 May 2013 (22.05.2013), the whole document	1-7
A	US 2004047308 A1 (KAVANAGH, A. et al.), 11 March 2004 (11.03.2004), the whole document	1-7

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 15 June 2015 (15.06.2015)	Date of mailing of the international search report 01 July 2015 (01.07.2015)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer MAO, Yunnan Telephone No.: (86-10) 62089144

International application No.
PCT/CN2015/075441

Form PCT/ISA/210 (patent family annex) (July 2009)

A. 主题的分类 H04L 29/06 (2006.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类		
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) H04L; H04W 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNABS, CNKI, CNTXT, VEN; IP, 数据包, 分组, 摘要, 运算, 计算, 比较, 序列号; IP, data, packet, abstract, summary, digest, calculation, computation, compare, sequence, number		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 103905452 A (国家电网公司等) 2014年 7月 2日 (2014 - 07 - 02) 权利要求1-7	1-7
A	CN 102065067 A (杭州华三通信技术有限公司) 2011年 5月 18日 (2011 - 05 - 18) 全文	1-7
A	CN 103118363 A (中国电信股份有限公司) 2013年 5月 22日 (2013 - 05 - 22) 全文	1-7
A	US 2004047308 A1 (KAVANAGH, A. ET AL.) 2004年 3月 11日 (2004 - 03 - 11) 全文	1-7
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期 2015年 6月 15日		国际检索报告邮寄日期 2015年 7月 1日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局 (ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国 传真号 (86-10)62019451		授权官员 毛韵楠 电话号码 (86-10)62089144

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/075441

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	103905452	A	2014年 7月 2日	无	
CN	102065067	A	2011年 5月 18日	CN 102065067	B 2014年 6月 25日
CN	103118363	A	2013年 5月 22日	无	
US	2004047308	A1	2004年 3月 11日	无	