(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 105592054 B
(45)授权公告日 2018.11.27

(21)申请号 201510586231.X

(22)申请日 2015.09.15

(65)同一申请的已公布的文献号
申请公布号 CN 105592054 A

(43)申请公布日 2016.05.18

(73)专利权人 新华三技术有限公司
地址 310052 浙江省杭州市滨江区长河路466号

(72)发明人 晁军显

(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 林祥

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 103856489 A,2014.06.11,
Network Working Group.Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication.《IETF》.2003,
Network Working Group.IS-IS Cryptographic Authentication.《IETF》.2008,
Network Working Group.IS-IS Generic Cryptographic Authentication.《IETF》.2009,

审查员 来文燕

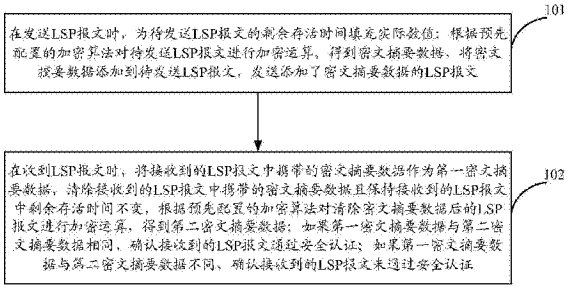
权利要求书2页 说明书8页 附图3页

(54)发明名称

一种LSP报文的处理方法和装置

(57)摘要

本发明提供一种LSP报文的处理方法和装置，该方法包括：在发送LSP报文时，为LSP报文的剩余存活时间填充实际数值；对LSP报文进行加密运算，得到密文摘要数据，将密文摘要数据添加到LSP报文，发送LSP报文；在收到LSP报文时，将LSP报文中携带的密文摘要数据作为第一密文摘要数据，清除LSP报文中携带的密文摘要数据，对LSP报文进行加密运算，得到第二密文摘要数据；如果第一密文摘要数据与第二密文摘要数据相同，确认LSP报文通过安全认证；如果第一密文摘要数据与第二密文摘要数据不同，确认LSP报文未通过安全认证。通过本发明的技术方案，可以获知LSP报文是否通过安全认证，在未通过安全认证时丢弃LSP报文，保证LSP报文传输的安全。



CN 105592054 B

1.一种链路状态协议LSP报文的处理方法，其特征在于，所述方法包括：

在发送LSP报文时，为待发送LSP报文的剩余存活时间填充实际数值；根据预先配置的加密算法对待发送LSP报文进行加密运算，得到密文摘要数据，将密文摘要数据添加到待发送LSP报文，发送添加了密文摘要数据的LSP报文；

在收到LSP报文时，将接收到的LSP报文中携带的密文摘要数据作为第一密文摘要数据，清除接收到的LSP报文中携带的密文摘要数据且保持接收到的LSP报文中剩余存活时间不变，根据预先配置的加密算法对清除密文摘要数据后的LSP报文进行加密运算，得到第二密文摘要数据；如果第一密文摘要数据与第二密文摘要数据相同，确认接收到的LSP报文通过安全认证；如果第一密文摘要数据与第二密文摘要数据不同，确认接收到的LSP报文未通过安全认证。

2.根据权利要求1所述的方法，其特征在于，所述方法进一步包括：

在根据预先配置的加密算法对待发送LSP报文进行加密运算，得到密文摘要数据之前，将待发送LSP报文的校验和字段修改为预设数值；

在将密文摘要数据添加到待发送LSP报文之后，且在发送添加了密文摘要数据的LSP报文之前，获得待发送LSP报文的校验和的实际数值，并将待发送LSP报文的校验和字段由预设数值修改为校验和的实际数值。

3.根据权利要求2所述的方法，其特征在于，在根据预先配置的加密算法对清除密文摘要数据后的LSP报文进行加密运算之前，所述方法进一步包括：

将清除密文摘要数据后的LSP报文的校验和字段修改为预设数值。

4.根据权利要求1所述的方法，其特征在于，待发送LSP报文中包括用于承载密文摘要数据的认证信息类型长度值TLV，在收到LSP报文之后，还包括：

当接收到的LSP报文具体为LSP清除报文时，则拒绝检查接收到的LSP清除报文中是否携带所述认证信息TLV之外的其它TLV；其中，所述LSP清除报文为剩余存活时间为0的LSP报文。

5.根据权利要求1所述的方法，其特征在于，所述方法进一步包括：

在根据预先配置的加密算法对待发送LSP报文进行加密运算，得到密文摘要数据之前，为待发送LSP报文设置第一标识；

在收到LSP报文时，如果发现接收到的LSP报文被设置了第一标识，则执行将接收到的LSP报文中携带的密文摘要数据作为第一密文摘要数据的过程。

6.一种链路状态协议LSP报文的处理装置，其特征在于，具体包括：

第一处理模块，用于在发送LSP报文时，为待发送LSP报文的剩余存活时间填充实际数值；根据预先配置的加密算法对待发送LSP报文进行加密运算，得到密文摘要数据，将密文摘要数据添加到待发送LSP报文，发送添加了密文摘要数据的LSP报文；

第二处理模块，用于在收到LSP报文时，将接收到的LSP报文中携带的密文摘要数据作为第一密文摘要数据，清除接收到的LSP报文中携带的密文摘要数据且保持接收到的LSP报文中剩余存活时间不变，根据预先配置的加密算法对清除密文摘要数据后的LSP报文进行加密运算，得到第二密文摘要数据；如果第一密文摘要数据与第二密文摘要数据相同，则确认接收到的LSP报文通过安全认证；如果第一密文摘要数据与第二密文摘要数据不同，则确认接收到的LSP报文未通过安全认证。

7.根据权利要求6所述的装置，其特征在于，

所述第一处理模块，还用于在根据预先配置的加密算法对待发送LSP报文进行加密运算，得到密文摘要数据之前，将待发送LSP报文的校验和字段修改为预设数值；在将密文摘要数据添加到待发送LSP报文之后，且在发送添加了密文摘要数据的LSP报文之前，获得待发送LSP报文的校验和的实际数值，并将待发送LSP报文的校验和字段由预设数值修改为校验和的实际数值。

8.根据权利要求7所述的装置，其特征在于，

所述第二处理模块，还用于在根据预先配置的加密算法对清除密文摘要数据后的LSP报文进行加密运算之前，将清除密文摘要数据后的LSP报文的校验和字段修改为预设数值。

9.根据权利要求6所述的装置，其特征在于，待发送LSP报文中包括用于承载密文摘要数据的认证信息类型长度值TLV；

所述第二处理模块，还用于在收到LSP报文之后，当接收到的LSP报文具体为LSP清除报文时，则拒绝检查接收到的LSP清除报文中是否携带所述认证信息TLV之外的其它TLV；其中，所述LSP清除报文为剩余存活时间为0的LSP报文。

10.根据权利要求6所述的装置，其特征在于，

所述第一处理模块，还用于在根据预先配置的加密算法对待发送LSP报文进行加密运算，得到密文摘要数据之前，为待发送LSP报文设置第一标识；

所述第二处理模块，还用于在收到LSP报文时，如果发现接收到的LSP报文被设置了第一标识，则执行将接收到的LSP报文中携带的密文摘要数据作为第一密文摘要数据的过程。

一种LSP报文的处理方法和装置

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种LSP报文的处理方法和装置。

背景技术

[0002] 随着网络需求的日益增长，网络设备的安全性、可靠性越来越得到关注。IS-IS(Intermediate System-to-Intermediate System，中间系统到中间系统)协议作为一种内部网关的动态路由协议，由于IS-IS协议的配置维护简单、可扩展性良好、可以支持大型网络，使得IS-IS协议得到广泛应用。在此背景下，IS-IS协议本身的安全性就显得尤为重要。为此，IETF(Internet Engineering Task Force，国际互联网工程任务组)通过RFC3567(Request For Comments 3567，请求注解3567)、RFC5304等标准，来加强IS-IS协议的安全性。

[0003] 其中，在网络设备之间使用IS-IS协议进行通信时，网络设备之间交互的报文包括IIH(IS-IS Hello，IS-IS的Hello报文)、LSPDU(Link State Protocol Data Unit，链路状态协议数据单元，简称LSP)、CSNP(Complete Sequence Numbers Protocol Data Unit，完全序列号协议数据单元)、PSNP(Partial Sequence Numbers Protocol Data Unit，部分序列号协议数据单元)等。

[0004] LSP报文是网络设备之间交互最多的一种报文，用于传递链路状态信息，因此，需要保证LSP报文在网络设备之间传输时的安全性。

发明内容

[0005] 本发明提供一种链路状态协议LSP报文的处理方法，所述方法包括：

[0006] 在发送LSP报文时，为待发送LSP报文的剩余存活时间填充实际数值；根据预先配置的加密算法对待发送LSP报文进行加密运算，得到密文摘要数据，将密文摘要数据添加到待发送LSP报文，发送添加了密文摘要数据的LSP报文；

[0007] 在收到LSP报文时，将接收到的LSP报文中携带的密文摘要数据作为第一密文摘要数据，清除接收到的LSP报文中携带的密文摘要数据且保持接收到的LSP报文中剩余存活时间不变，根据预先配置的加密算法对清除密文摘要数据后的LSP报文进行加密运算，得到第二密文摘要数据；如果第一密文摘要数据与第二密文摘要数据相同，确认接收到的LSP报文通过安全认证；如果第一密文摘要数据与第二密文摘要数据不同，确认接收到的LSP报文未通过安全认证。

[0008] 本发明提供一种链路状态协议LSP报文的处理装置，具体包括：

[0009] 第一处理模块，用于在发送LSP报文时，为待发送LSP报文的剩余存活时间填充实际数值；根据预先配置的加密算法对待发送LSP报文进行加密运算，得到密文摘要数据，将密文摘要数据添加到待发送LSP报文，发送添加了密文摘要数据的LSP报文；

[0010] 第二处理模块，用于在收到LSP报文时，将接收到的LSP报文中携带的密文摘要数据作为第一密文摘要数据，清除接收到的LSP报文中携带的密文摘要数据且保持接收到的

LSP报文中剩余存活时间不变，根据预先配置的加密算法对清除密文摘要数据后的LSP报文进行加密运算，得到第二密文摘要数据；如果第一密文摘要数据与第二密文摘要数据相同，则确认接收到的LSP报文通过安全认证；如果第一密文摘要数据与第二密文摘要数据不同，则确认接收到的LSP报文未通过安全认证。

[0011] 基于上述技术方案，本发明实施例中，通过比较LSP报文中携带的密文摘要数据与自身计算得到的密文摘要数据是否相同，以获知LSP报文是否通过安全认证，从而在未通过安全认证时丢弃LSP报文。上述方式可以保证LSP报文在网络设备之间传输时的安全性。而且，对LSP报文进行加密运算时，LSP报文的剩余存活时间为实际数值，即当攻击者对LSP报文的剩余存活时间进行修改，从而进行攻击时，可以检测到攻击行为的存在。

附图说明

[0012] 图1是本发明一种实施方式中的LSP报文的处理方法的流程图；

[0013] 图2是本发明另一种实施方式中的LSP报文的处理方法的流程图；

[0014] 图3是本发明一种实施方式中的网络设备的硬件结构图；

[0015] 图4是本发明一种实施方式中的LSP报文的处理装置的结构图。

具体实施方式

[0016] 本发明实施例中提出一种LSP报文的处理方法，如图1所示，该LSP报文的处理方法具体可以包括以下步骤：

[0017] 步骤101，在发送LSP报文时，为待发送LSP报文的剩余存活时间填充实际数值；根据预先配置的加密算法对待发送LSP报文进行加密运算，得到密文摘要数据，将密文摘要数据添加到待发送LSP报文，发送添加了密文摘要数据的LSP报文。

[0018] 步骤102，在收到LSP报文时，将接收到的LSP报文中携带的密文摘要数据作为第一密文摘要数据，清除接收到的LSP报文中携带的密文摘要数据且保持接收到的LSP报文中剩余存活时间不变，根据预先配置的加密算法对清除密文摘要数据后的LSP报文进行加密运算，得到第二密文摘要数据；如果第一密文摘要数据与第二密文摘要数据相同，确认接收到的LSP报文通过安全认证；如果第一密文摘要数据与第二密文摘要数据不同，确认接收到的LSP报文未通过安全认证。

[0019] 本发明实施例中，在根据预先配置的加密算法对待发送LSP报文进行加密运算，得到密文摘要数据之前，将待发送LSP报文的校验和字段修改为预设数值。在将密文摘要数据添加到待发送LSP报文之后，且在发送添加了密文摘要数据的LSP报文之前，获得待发送LSP报文的校验和的实际数值，并将待发送LSP报文的校验和字段由预设数值修改为校验和的实际数值。进一步的，在根据预先配置的加密算法对清除密文摘要数据后的LSP报文进行加密运算之前，将清除密文摘要数据后的LSP报文的校验和字段修改为预设数值。

[0020] 本发明实施例中，待发送LSP报文中包括用于承载密文摘要数据的认证信息TLV，在收到LSP报文后，当接收到的LSP报文具体为LSP清除报文时，拒绝检查接收到的LSP清除报文中是否携带认证信息TLV之外的其它TLV。

[0021] 本发明实施例中，在根据预先配置的加密算法对待发送LSP报文进行加密运算，得到密文摘要数据之前，则为待发送LSP报文设置第一标识；

[0022] 在收到LSP报文时，如果发现接收到的LSP报文被设置了第一标识，则执行将接收到的LSP报文中携带的密文摘要数据作为第一密文摘要数据的过程。

[0023] 基于上述技术方案，本发明实施例中，通过比较LSP报文中携带的密文摘要数据与自身计算得到的密文摘要数据是否相同，以获知LSP报文是否通过安全认证，从而在未通过安全认证时丢弃LSP报文。上述方式可以保证LSP报文在网络设备之间传输时的安全性。而且，对LSP报文进行加密运算时，LSP报文的剩余存活时间为实际数值，即当攻击者对LSP报文的剩余存活时间进行修改，从而进行攻击时，可以检测到攻击行为的存在。

[0024] 以下结合具体的应用场景对本发明实施例的技术方案进行说明。

[0025] 本发明实施例中提出一种LSP报文的处理方法，该方法应用于包括发送端设备和接收端设备的系统中，发送端设备和接收端设备均为配置IS-IS协议的网络设备。如图2所示，该LSP报文的处理方法具体可以包括以下步骤：

[0026] 步骤201，发送端设备获得LSP报文，为该LSP报文的剩余存活时间填充实际数值。其中，LSP报文的剩余存活时间表示此LSP报文所剩的生存时间，单位为秒。例如，当剩余存活时间为100秒时，表示此LSP报文所剩的生存时间为100秒，当剩余存活时间为0秒时，表示此LSP报文需要被清除。

[0027] 其中，发送端设备获得LSP报文的过程，具体包括但不限于：发送端设备接收来自其它网络设备的LSP报文，或者发送端设备自身生成LSP报文。

[0028] 步骤202，发送端设备根据预先配置的加密算法对LSP报文进行加密运算，得到密文摘要数据，并将该密文摘要数据添加到LSP报文中。

[0029] 步骤203，发送端设备将添加密文摘要数据的LSP报文发送给接收端设备。

[0030] 步骤204，接收端设备接收LSP报文，该LSP报文的剩余存活时间为实际数值。其中，LSP报文的剩余存活时间表示此LSP报文所剩的生存时间。

[0031] 步骤205，接收端设备将LSP报文中携带的密文摘要数据作为第一密文摘要数据，清除LSP报文中携带的密文摘要数据且保持接收到的LSP报文中剩余存活时间不变，并根据预先配置的加密算法对清除密文摘要数据后的LSP报文进行加密运算，得到第二密文摘要数据。

[0032] 步骤206，接收端设备比较第一密文摘要数据与第二密文摘要数据。如果第一密文摘要数据与第二密文摘要数据相同，则接收端设备执行步骤207；如果第一密文摘要数据与第二密文摘要数据不同，则接收端设备执行步骤208。

[0033] 步骤207，接收端设备确认LSP报文通过安全认证。

[0034] 步骤208，接收端设备确认LSP报文未通过安全认证。

[0035] 基于上述技术方案，本发明实施例中，接收端设备通过比较LSP报文中携带的密文摘要数据与自身计算得到的密文摘要数据是否相同，以获知LSP报文是否通过安全认证，从而在未通过安全认证时丢弃LSP报文。上述方式可以保证LSP报文在网络设备之间传输时的安全性。而且，对LSP报文进行加密运算时，LSP报文的剩余存活时间为实际数值，即当攻击者对LSP报文的剩余存活时间进行修改，从而进行攻击时，可以检测到攻击行为的存在。

[0036] 在LSP报文中，可以包括但不限于如下字段：1、PDU(Protocol Data Unit，协议数据单元)Length(长度)字段，表示整个LSP报文的长度，占2个字节。2、Remaining Lifetime(剩余存活时间)字段，占2个字节，表示此LSP报文所剩的生存时间，单位为秒，当剩余存活

时间为0时，LSP报文将被从链路状态数据库中清除。3、LSP标识字段，占系统标识长度+2个字节，用来标识不同的LSP报文和生成LSP报文的网络设备，其包括三部分：Source ID(源ID，也即系统标识)、PseudonodeID(伪节点标识)、LSP Number(LSP序列号，即LSP报文的分片号)。4、Sequence Number(序列号)字段，占4个字节，标识每个LSP报文的序列号。5、Checksum(校验和)字段，占2个字节，用于使接收端设备校验传送的LSP报文的完整性和正确性。6、P(Partition，分区)字段，占1位，表示区域划分或者分段区域的修复位。7、ATT(Attached，区域关联)字段，占4位，表示产生此LSP报文的网络设备与多个区域相连。8、OL(Overload，过载)字段，占1位，置1时表示本网络设备因内存不足而导致链路状态数据库不完整。9、IS Type(网络设备类型)字段，占2位，用来指明生成此LSP报文的网络设备的类型。

[0037] 在此LSP报文中，还包括扩展字段，在该扩展字段中可以承载各种类型的TLV(Type Length Value，类型长度值)，如用于携带路由信息的TLV，用于携带IP前缀信息的TLV，用于携带协议支持信息的TLV，用于携带区域信息的TLV等。在此基础上，可以在此LSP报文中添加用于承载密文摘要数据的TLV，该用于承载密文摘要数据的TLV可以称为认证信息TLV。

[0038] 在发送端设备获得LSP报文之后，在发送端设备根据预先配置的加密算法对LSP报文进行加密运算，得到密文摘要数据之前，由于发送端设备还没有获得密文摘要数据，因此，将认证信息TLV中承载的密文摘要数据设置为预设数值(如0)。在根据预先配置的加密算法对LSP报文进行加密运算时，该LSP报文中携带的认证信息TLV中承载的密文摘要数据为预设数值。在发送端设备根据预先配置的加密算法对LSP报文进行加密运算，得到密文摘要数据之后，发送端设备将该密文摘要数据添加到LSP报文的认证信息TLV中，即将认证信息TLV中携带的预设数值修改为该密文摘要数据。

[0039] 接收端设备在接收到LSP报文之后，会清除LSP报文中携带的密文摘要数据，如将LSP报文的认证信息TLV中承载的密文摘要数据设置为预设数值(如0)。在根据预先配置的加密算法对LSP报文进行加密运算时，该LSP报文中携带的认证信息TLV中承载的密文摘要数据为预设数值。

[0040] 本发明实施例中，发送端设备上预先配置的加密算法与接收端设备上预先配置的加密算法相同，如均为MD5(Message Digest Algorithm，消息摘要算法第五版)加密算法，且在发送端设备和接收端设备上配置相同的密钥。

[0041] 由于发送端设备上预先配置的加密算法与接收端设备上预先配置的加密算法相同，因此，如果接收端设备当前得到的密文摘要数据与LSP报文中携带的密文摘要数据相同，则说明LSP报文中的内容没有被修改，LSP报文通过安全认证，可以基于LSP报文进行后续处理。如果接收端设备当前得到的密文摘要数据与LSP报文中携带的密文摘要数据不同，则说明LSP报文中的内容被修改，LSP报文未通过安全认证，可以直接丢弃该LSP报文。

[0042] 其中，认证信息TLV中承载的密文摘要数据可以为16字节的密文摘要数据，上述认证信息TLV中承载的预设数值可以为16字节的全0。

[0043] 目前在RFC3567、RFC5304等标准中，在发送端设备根据预先配置的加密算法对LSP报文进行加密运算之前，发送端设备将LSP报文的剩余存活时间字段由实际数值(如100秒)修改为预设数值(如0)。在发送端设备将密文摘要数据添加到LSP报文之后，在将修改后的LSP报文发送给接收端设备之前，发送端设备将LSP报文的剩余存活时间字段由预设数值(如0)修改为实际数值(如100秒)。进一步的，在接收端设备根据预先配置的加密算法对修

改后的LSP报文进行加密运算之前，接收端设备将LSP报文的剩余存活时间字段由实际数值(如100秒)修改为预设数值(如0)。基于上述处理，可以保证发送端设备进行加密运算时使用的剩余存活时间、与接收端设备进行加密运算时使用的剩余存活时间相同，二者均为预设数值(如0)。

[0044] 但是，申请人发现上述标准存在技术缺陷，并会导致存在以下问题：攻击者在截获LSP报文后，不需要获知发送端设备/接收端设备使用的加密算法，也不需要对LSP报文中的密文摘要数据进行修改，可以直接修改LSP报文中的剩余存活时间，如将剩余存活时间由100秒修改为1秒或0秒等。接收端设备接收到LSP报文后，在根据加密算法对LSP报文进行加密运算之前，会将LSP报文的剩余存活时间字段由1秒或0秒修改为预设数值0，即进行加密运算时不考虑剩余存活时间字段的数值，因此，LSP报文会通过安全认证，但实际上，该LSP报文的剩余存活时间已经被攻击者篡改。

[0045] 假设攻击者修改后的剩余存活时间为0秒，则接收端设备认为该LSP报文是LSP清除报文，即该LSP后续不再产生，需要撤销，接收端设备会删除对应的拓扑信息，并会撤销路由。而实际上，剩余存活时间为100秒，接收端设备不应该执行上述操作。上述过程会导致路由撤销，网络震荡。

[0046] 假设攻击者修改后的剩余存活时间为趋近于0秒的数值，如1秒或者2秒等，则接收端设备在接收到LSP报文之后，该LSP报文对应的老化定时器很快就会超时(如1秒或者2秒后会超时)，此时，接收端设备同样会删除对应的拓扑信息，并会撤销路由。而实际上，剩余存活时间为100秒，接收端设备不应该执行上述操作。上述过程会导致路由撤销，网络震荡。

[0047] 针对上述发现，本发明实施例中，在发送端设备根据预先配置的加密算法对LSP报文进行加密运算之前，发送端设备不会将LSP报文的剩余存活时间字段由实际数值(如100秒)修改为预设数值(如0)，即发送端设备进行加密运算时使用的剩余存活时间为实际数值(如100秒)。在接收端设备根据预先配置的加密算法对修改后的LSP报文进行加密运算之前，接收端设备也不会将LSP报文的剩余存活时间字段由实际数值(如100秒)修改为预设数值(如0)，保持LSP报文中剩余存活时间不变，即接收端设备进行加密运算时使用的剩余存活时间为实际数值(如100秒)。基于上述处理，如果攻击者修改LSP报文中的剩余存活时间，如将剩余存活时间由100秒修改为1秒或0秒，则接收端设备将确认出LSP报文未通过安全认证，并丢弃该LSP报文，从而避免路由撤销，网络震荡等问题，并解决LSP报文的剩余存活时间的安全漏洞问题。

[0048] 本发明实施例中，在发送端设备根据预先配置的加密算法对LSP报文进行加密运算之前，发送端设备还可以将LSP报文的校验和字段由实际数值修改为预设数值(如0)。在发送端设备将密文摘要数据添加到LSP报文之后，在将修改后的LSP报文发送给接收端设备之前，发送端设备还可以获得LSP报文的校验和的实际数值，并将LSP报文的校验和字段修改为实际数值。进一步的，在接收端设备根据预先配置的加密算法对修改后的LSP报文进行加密运算之前，接收端设备还可以将LSP报文的校验和字段修改为预设数值。基于上述处理，可以保证发送端设备进行加密运算时使用的校验和、与接收端设备进行加密运算时使用的校验和相同，二者均为预设数值(如0)。

[0049] 其中，在发送端设备获得LSP报文的校验和的实际数值的过程中，发送端设备是对整个LSP报文(包含填充的密文摘要数据)计算校验和。同理，接收端设备也是对自身收到的

整个LSP报文(包含填充的密文摘要数据)计算校验和。基于此,攻击者在截获LSP报文后,如果直接修改LSP报文的校验和,而不修改LSP报文的其它内容,则接收端设备在接收到LSP报文后,虽然基于密文摘要数据无法确定出LSP报文已经被攻击者篡改,但是由于接收端设备对自身收到的整个LSP报文(包含填充的密文摘要数据)计算校验和的结果,与LSP报文中携带的校验和(攻击者修改后的校验和)不同,因此接收端设备会认为该LSP报文已经被攻击者篡改,并直接丢弃该LSP报文。

[0050] 目前在RFC3567、RFC5304等标准中,针对LSP清除报文(即剩余存活时间为0的LSP报文),发送端设备禁止在LSP清除报文中携带认证信息TLV之外的其它TLV,如用于携带路由信息的TLV,用于携带IP前缀信息的TLV,用于携带协议支持信息的TLV,用于携带区域信息的TLV等。接收端设备在接收到LSP清除报文后,需要检查LSP清除报文中是否携带认证信息TLV之外的其它TLV。但是,申请人发现上述标准存在技术缺陷,并会导致存在以下问题:增加接收端设备处理的复杂度,而且LSP清除报文无法携带认证信息TLV之外的其它TLV,浪费了LSP清除报文的资源。

[0051] 基于上述发现,本发明实施例中,针对LSP清除报文(即剩余存活时间为0的LSP报文),不对发送端设备发送的LSP清除报文进行限制,即不禁止发送端设备在LSP清除报文中携带认证信息TLV(用于承载密文摘要数据的TLV)之外的其它TLV。而且,接收端设备在接收到LSP清除报文后,也不需要检查LSP清除报文中是否携带认证信息TLV之外的其它TLV。

[0052] 基于上述过程,可以简化接收端设备处理的过程,而且LSP清除报文中可以携带认证信息TLV之外的其它TLV,充分利用了LSP清除报文的资源。

[0053] 为了与目前的RFC3567、RFC5304等标准进行兼容,可以基于用户配置来使能本发明实施例的技术方案或者去使能本发明实施例的技术方案。

[0054] 在一种具体实现中,如果在发送端设备和接收端设备上配置使能本发明实施例的技术方案,则发送端设备执行上述步骤101-步骤103,并在向接收端设备发送LSP报文时,为LSP报文设置第一标识,如将LSP报文的Reserved(预留)字段的首位设置为第一标识(如1),为LSP报文设置的第一标识表示LSP报文采用本发明技术方案。具体的,发送端设备在根据预先配置的加密算法对LSP报文进行加密运算之前,将LSP报文的Reserved字段的首位设置为第一标识。接收端设备在接收到LSP报文后,如果发现LSP报文被设置了第一标识,如LSP报文的Reserved字段的首位为第一标识(如1),则执行上述步骤104-步骤108,即执行将LSP报文中携带的密文摘要数据作为第一密文摘要数据,清除LSP报文中携带的密文摘要数据,并根据预先配置的加密算法对清除密文摘要数据后的LSP报文进行加密运算,得到第二密文摘要数据等过程。此外,发送端设备在向接收端设备发送LSP清除报文时,将LSP清除报文的Reserved字段的首位设置为第一标识(如1)。接收端设备在接收到LSP清除报文后,如果发现LSP清除报文的Reserved字段的首位为第一标识(如1),则不需要检查LSP清除报文中是否携带认证信息TLV之外的其它TLV。

[0055] 如果在发送端设备和接收端设备上配置去使能本发明实施例的技术方案,则发送端设备按照现有流程向接收端设备发送LSP报文,且在向接收端设备发送LSP报文时,将LSP报文的Reserved字段的首位设置为第二标识(如0),为LSP报文的Reserved字段的首位设置的第二标识表示LSP报文采用现有流程。接收端设备在接收到LSP报文后,如果发现LSP报文的Reserved字段的首位为第二标识(如0),则执行现有流程进行处理。此外,发送端设备在

向接收端设备发送LSP清除报文时，将LSP清除报文的Reserved字段的首位设置为第二标识(如0)。接收端设备在接收到LSP清除报文后，如果发现LSP清除报文的Reserved字段的首位为第二标识(如0)，则需要检查LSP清除报文中是否携带认证信息TLV之外的其它TLV。

[0056] 基于与上述方法同样的发明构思，本发明实施例中还提供了一种LSP报文的处理装置，该LSP报文的处理装置应用在网络设备上。其中，该LSP报文的处理装置可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为一个逻辑意义上的装置，是通过其所在的网络设备的处理器，将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，如图3所示，为本发明提出的LSP报文的处理装置所在的网络设备的一种硬件结构图，除了图3所示的处理器、网络接口、内存以及非易失性存储器外，网络设备还可以包括其他硬件，如负责处理报文的转发芯片等；从硬件结构上来讲，该网络设备还可能是分布式设备，可能包括多个接口卡，以便在硬件层面进行报文处理的扩展。

[0057] 如图4所示，为本发明提出的LSP报文的处理装置的结构图，所述LSP报文的处理装置具体包括：

[0058] 第一处理模块11，用于在发送LSP报文时，为待发送LSP报文的剩余存活时间填充实际数值；根据预先配置的加密算法对待发送LSP报文进行加密运算，得到密文摘要数据，将密文摘要数据添加到待发送LSP报文，发送添加了密文摘要数据的LSP报文；第二处理模块12，用于在收到LSP报文时，将接收到的LSP报文中携带的密文摘要数据作为第一密文摘要数据，清除接收到的LSP报文中携带的密文摘要数据且保持接收到的LSP报文中剩余存活时间不变，根据预先配置的加密算法对清除密文摘要数据后的LSP报文进行加密运算，得到第二密文摘要数据；如果第一密文摘要数据与第二密文摘要数据相同，则确认接收到的LSP报文通过安全认证；如果第一密文摘要数据与第二密文摘要数据不同，则确认接收到的LSP报文未通过安全认证。

[0059] 所述第一处理模块11，还用于在根据预先配置的加密算法对待发送LSP报文进行加密运算，得到密文摘要数据之前，将待发送LSP报文的校验和字段修改为预设数值；在将密文摘要数据添加到待发送LSP报文之后，且在发送添加了密文摘要数据的LSP报文之前，获得待发送LSP报文的校验和的实际数值，并将待发送LSP报文的校验和字段由预设数值修改为校验和的实际数值。

[0060] 所述第二处理模块12，还用于在根据预先配置的加密算法对清除密文摘要数据后的LSP报文进行加密运算之前，将清除密文摘要数据后的LSP报文的校验和字段修改为预设数值。

[0061] 待发送LSP报文中包括用于承载密文摘要数据的认证信息类型长度值TLV；所述第二处理模块12，还用于在收到LSP报文之后，当接收到的LSP报文具体为LSP清除报文时，则拒绝检查接收到的LSP清除报文中是否携带所述认证信息TLV之外的其它TLV。

[0062] 所述第一处理模块11，还用于在根据预先配置的加密算法对待发送LSP报文进行加密运算，得到密文摘要数据之前，为待发送LSP报文设置第一标识；所述第二处理模块12，还用于在收到LSP报文时，如果发现接收到的LSP报文被设置了第一标识，则执行将接收到的LSP报文中携带的密文摘要数据作为第一密文摘要数据的过程。

[0063] 其中，本发明装置的各个模块可以集成于一体，也可以分离部署。上述模块可以合

并为一个模块，也可以进一步拆分成多个子模块。

[0064] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本发明各个实施例所述的方法。本领域技术人员可以理解附图只是一个优选实施例的示意图，附图中的模块或流程并不一定是实施本发明所必须的。

[0065] 本领域技术人员可以理解实施例中的装置中的模块可以按照实施例描述进行分布于实施例的装置中，也可以进行相应变化位于不同于本实施例的一个或多个装置中。上述实施例的模块可以合并为一个模块，也可进一步拆分成多个子模块。上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0066] 以上公开的仅为本发明的几个具体实施例，但是，本发明并非局限于此，任何本领域的技术人员能思之的变化都应落入本发明的保护范围。

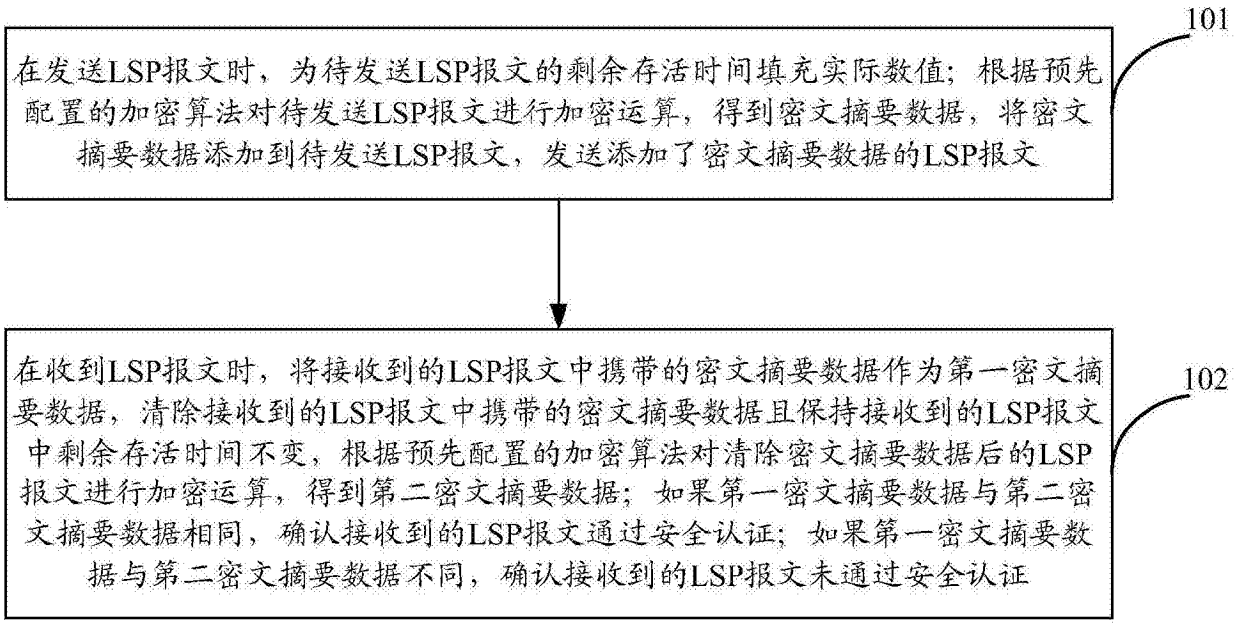

101
在发送LSP报文时，为待发送LSP报文的剩余存活时间填充实际数值；根据预先配置的加密算法对待发送LSP报文进行加密运算，得到密文摘要数据，将密文摘要数据添加到待发送LSP报文，发送添加了密文摘要数据的LSP报文
102
在收到LSP报文时，将接收到的LSP报文中携带的密文摘要数据作为第一密文摘要数据，清除接收到的LSP报文中携带的密文摘要数据且保持接收到的LSP报文中剩余存活时间不变，根据预先配置的加密算法对清除密文摘要数据后的LSP报文进行加密运算，得到第二密文摘要数据；如果第一密文摘要数据与第二密文摘要数据相同，确认接收到的LSP报文通过安全认证；如果第一密文摘要数据与第二密文摘要数据不同，确认接收到的LSP报文未通过安全认证

图1

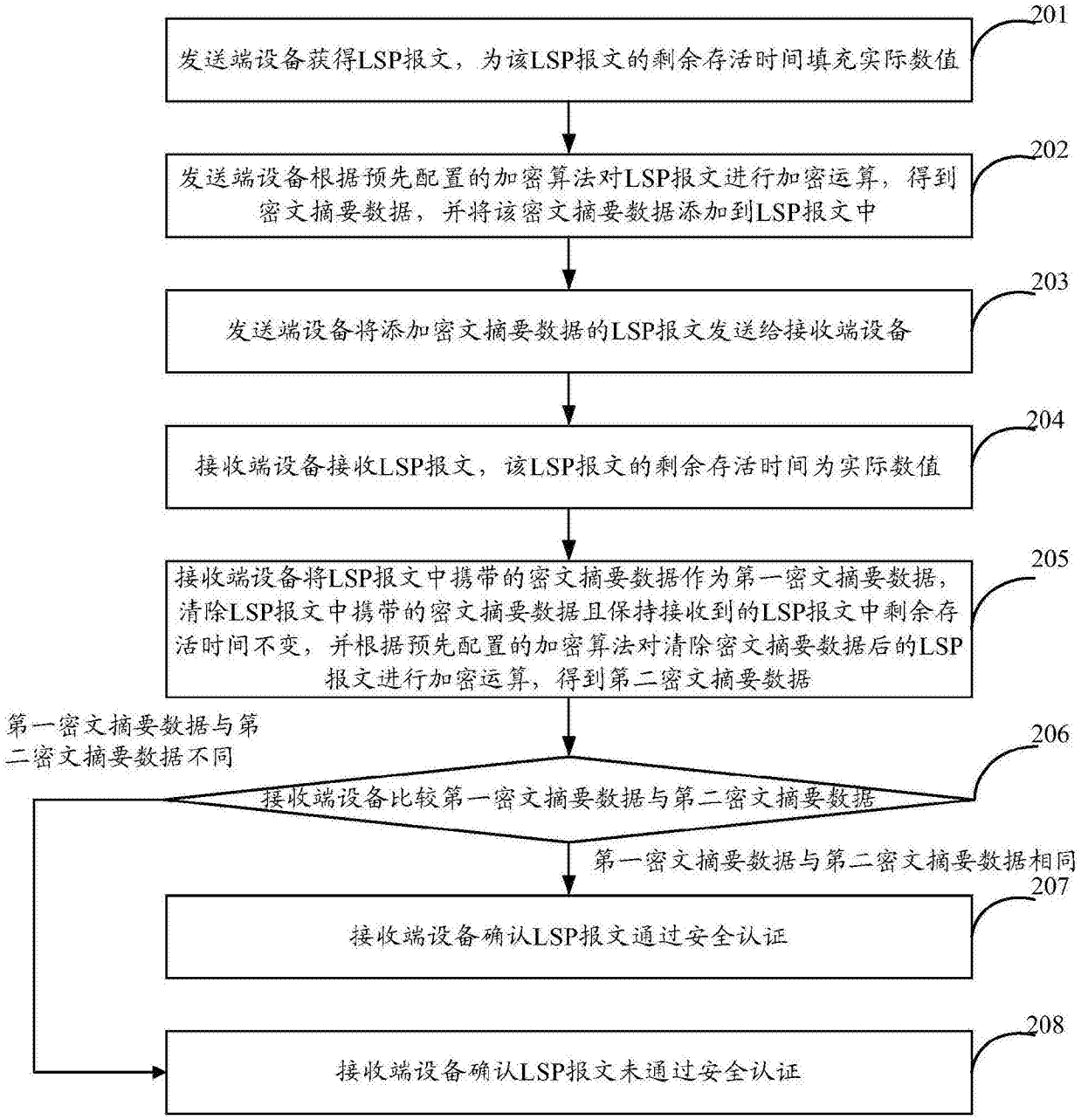

201
发送端设备获得LSP报文，为该LSP报文的剩余存活时间填充实际数值
202
发送端设备根据预先配置的加密算法对LSP报文进行加密运算，得到密文摘要数据，并将该密文摘要数据添加到LSP报文中
203
发送端设备将添加密文摘要数据的LSP报文发送给接收端设备
204
接收端设备接收LSP报文，该LSP报文的剩余存活时间为实际数值
205
接收端设备将LSP报文中携带的密文摘要数据作为第一密文摘要数据，清除LSP报文中携带的密文摘要数据且保持接收到的LSP报文中剩余存活时间不变，并根据预先配置的加密算法对清除密文摘要数据后的LSP报文进行加密运算，得到第二密文摘要数据
206
接收端设备比较第一密文摘要数据与第二密文摘要数据
第一密文摘要数据与第二密文摘要数据不同
第一密文摘要数据与第二密文摘要数据相同
207
接收端设备确认LSP报文通过安全认证
208
接收端设备确认LSP报文未通过安全认证

图2

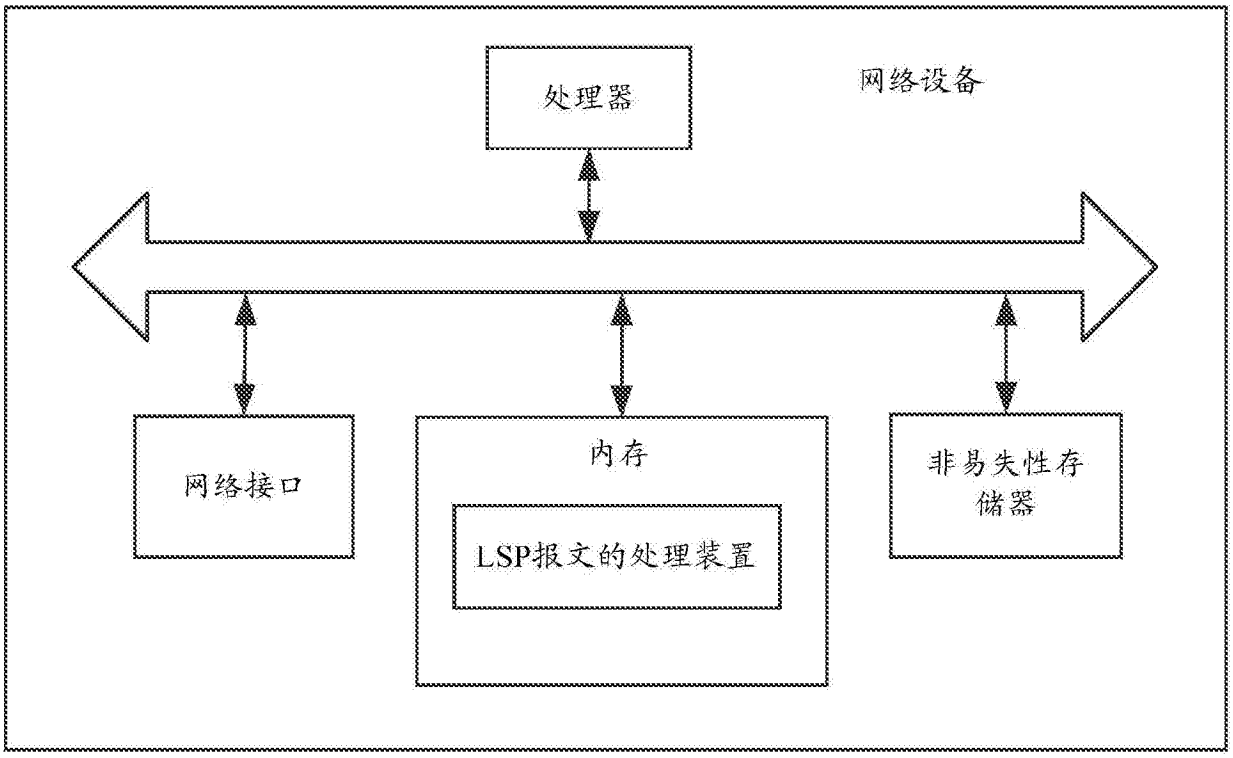

处理器
网络设备
网络接口
内存
LSP报文的处理装置
非易失性存储器

图3

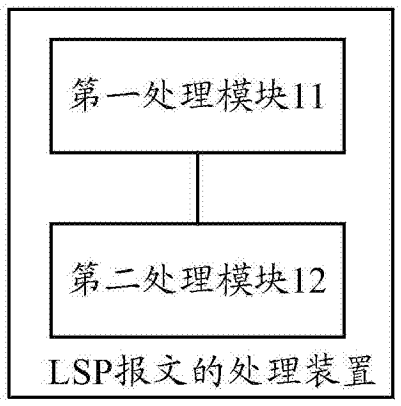

第一处理模块11
第二处理模块12
LSP报文的处理装置

图4