



(12) 发明专利申请

(10) 申请公布号 CN 102857521 A

(43) 申请公布日 2013. 01. 02

(21) 申请号 201210384384. 2

(22) 申请日 2012. 10. 12

(71) 申请人 盛科网络(苏州)有限公司

地址 215021 江苏省苏州市工业园区星汉街
5号(腾飞工业坊)B幢4楼13/16单元

(72) 发明人 刘敬一

(74) 专利代理机构 苏州慧通知识产权代理事务
所(普通合伙) 32239

代理人 安纪平

(51) Int. Cl.

H04L 29/06(2006. 01)

H04L 9/32(2006. 01)

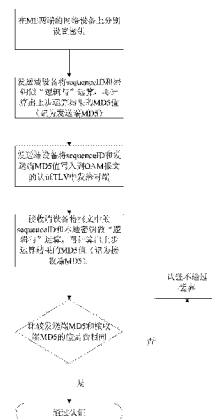
权利要求书 1 页 说明书 5 页 附图 2 页

(54) 发明名称

设置 OAM 安全认证的方法及装置

(57) 摘要

本发明揭示了一种设置 OAM 安全认证的方法及装置,其包括预先在 ME 两端的网络设备上设置密钥,在一端的网络设备发送 OAM 报文时,在发送的 OAM 报文中增加一个身份验证 TLV 字段,所述字段包括发送端 MD5 值,该发送端 MD5 值由 sequenceID 字段和所述密钥逻辑运算组成;ME 另一端的网络设备在收到所述 OAM 报文时,将所述报文中的 sequenceID 字段和本地预设的密钥进行相应的逻辑运算,得到接收端 MD5 值;并将两 MD5 值相比较,相同的 OAM 报文则通过认证,不同则将报文丢弃,如此,保证了 OAM 的通信安全,使得运行 CFM 协议的设备不易受到来自互联网的恶意攻击。



1. 一种设置 OAM 安全认证的方法,其特征在于包括:

预先在 ME 两端的网络设备上分别设置密钥,在一端的网络设备发送的 OAM 报文中设置身份认证 TLV 字段,所述身份认证 TLV 字段包括 sequenceID 字段和发送端 MD5 值,所述发送端 MD5 值是由所述 sequenceID 字段和所述密钥逻辑运算而成;

ME 另一端的网络设备在接收到所述 OAM 报文时,将所述报文中的 sequenceID 字段和本地预设的密钥进行相应的逻辑运算,得到接收端 MD5 值;以及

比较所述发送端 MD5 值和接收端 MD5 值,并将两者相同的 OAM 报文通过 OAM 认证。

2. 根据权利要求 1 所述的方法,其特征在于:在同一维护实体组中的所有合法设备上,所述密钥相同。

3. 根据权利要求 1 所述的方法,其特征在于:所述身份认证 TLV 字段的长度为 sequenceID 和 MD5 值的长度之和。

4. 根据权利要求 1 所述的方法,其特征在于:所述密钥不在网络上传输。

5. 根据权利要求 1 所述的方法,其特征在于:所述发送端 MD5 值和接收端 MD5 值均由 sequenceID 字段和对应设备的密钥逻辑与的结果作 MD5 运算产生。

6. 根据权利要求 1 所述的方法,其特征在于:对发送端 MD5 值不同于接收端 MD5 值的报文不通过认证,并将该报文丢弃。

7. 根据权利要求 1 所述的方法,其特征在于:所述身份认证 TLV 的字段位置位于紧邻終了 TLV 字段之前。

8. 一种设置 OAM 安全认证的装置,其特征在于包括:

密钥设置模块,用于预先在 ME 两端的网络设备上分别设置密钥;

OAM 报文发送模块,用于在报文发送端的网络设备发送的 OAM 报文中设置身份认证 TLV 字段,所述身份认证 TLV 字段包括 sequenceID 字段和发送端 MD5 值,所述发送端 MD5 值是由所述 sequenceID 字段和所述密钥逻辑运算而成;

OAM 报文接收模块,用于 ME 另一端的网络设备在接收到所述 OAM 报文时,将所述报文中的 sequenceID 字段和本地预设的密钥进行相应的逻辑运算,得到接收端 MD5 值;以及

MD5 值比较模块,用于比较所述发送端 MD5 值和接收端 MD5 值,并将两者相同的 OAM 报文通过 OAM 认证。

9. 根据权利要求 8 所述的方法,其特征在于:在同一维护实体组中的所有合法设备上,所述密钥相同。

10. 根据权利要求 8 所述的方法,其特征在于:所述身份认证 TLV 的字段位置位于紧邻終了 TLV 字段之前。

设置 OAM 安全认证的方法及装置

技术领域

[0001] 本发明涉及计算机通信技术领域,尤其涉及计算机网络通信技术的 CFM 协议中设置 OAM 安全认证的方法及装置。

背景技术

[0002] 根据运营商网络运营的实际需要,通常将网络的管理工作划分为 3 大类:操作(Operation)、管理(Administration)、维护(Maintenance),简称 OAM(Operation Administration and Maintenance)。操作主要完成日常网络和业务进行的分析、预测、规划和配置工作;维护主要是对网络及其业务的测试和故障管理等进行的日常操作活动。

[0003] 基于 Y. 1731 的 CFM(Continuity Fault Management,连接故障管理),目前已经被广泛应用于运营商网络。按照 CFM 的功能区分,可以分为两类:一类为用于差错管理的 OAM 功能,用来检测、验证、定位和通告网络中不同的故障情况。包括连续性检查、环回、链路跟踪、告警指示、远端故障指示、锁定信号、测试信号、自动保护转换和维护通信通道。另一类为用于性能监测的 OAM 功能,可以用来测量不同的性能参数,目前主要是针对点对点测量。包括帧丢失的测量、帧时延的测量和通量测量。

[0004] OAM PDU(Protocol Data Unit,协议数据单元)类型的信息单元和格式,满足了上述两类 OAM 功能的要求,而 OAM PDU 存在一种共同的格式,如下:

[0005]

	1								2								3								4							
	8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1
1	MEL			版本(0)					OpCode								标记								TLV偏置值							
5																																
:																																
:																																
最后	终止TLV																															

[0006] 上述格式中,OpCode 是一个字节的字段,其包含了一个表示 OAM PDU 类型的 OpCode,OpCode 用于识别 OAM PDU 中其余部分的内容。这一信息字段的数值如下表所示:

[0007]

OpCode 值	OAM PDU 类型
与 IEEE 802.1 共同的	
1	CCM
3	LEM
2	LEB
5	LTM
4	LTR
0, 6-31, 64-255	保留(注 1)
Y.1731 独有的	
33	AIS
35	LCK
37	TST
39	APS
41	MCC
43	LMM
42	LMR
45	IDM
47	DDM
46	DMR
49	EXM
48	EXR
51	VSM
50	VSR
32, 34, 36, 38, 44, 52-63	保留(注 2)
注 1-保留由 IEEE802.1 定义	
注 2-保留供 ITU-T 将来的标准化	

[0008] 然而 Y.1731 协议本身并没有考虑到安全性。且在真实的运营商网络中,缺乏安全性的协议很容易成为被网络攻击的对象。考虑到 OAM 在整个运营商网络中的重要地位,急需解决如何识别收到的 OAM 报文是否真实可靠这个问题。

发明内容

[0009] 本发明的目的在于克服现有技术的缺陷,提供一种设置 OAM 安全认证的方法,其在 ME (Maintenance Entity, 维护实体) 的两端分别对报文进行安全认证,尽可能地屏蔽恶意报文的冲击,以确保 CFM 协议的通信安全。

[0010] 为实现上述目的,本发明提出如下技术方案:一种设置 OAM 安全认证的方法,包括:

[0011] 预先在 ME 两端的网络设备上分别设置密钥,在一端的网络设备发送的 OAM 报文中设置身份认证 TLV 字段,所述身份认证 TLV 字段包括 sequenceID 字段和发送端 MD5 值,所述发送端 MD5 值是由所述 sequenceID 字段和所述密钥逻辑运算而成;

[0012] ME 另一端的网络设备在接收到所述 OAM 报文时,将所述报文中的 sequenceID 字段和本地预设的密钥进行相应的逻辑运算,得到接收端 MD5 值;以及

[0013] 比较所述发送端 MD5 值和接收端 MD5 值,并将两者相同的 OAM 报文通过 OAM 认证。

- [0014] 在同一维护实体组中的所有合法设备上,所述密钥相同。
- [0015] 所述身份认证 TLV 字段的长度为 sequenceID 和 MD5 值的长度之和。
- [0016] 所述密钥不在网络上传输。
- [0017] 所述发送端 MD5 值和接收端 MD5 值均由 sequenceID 字段和对应设备的密钥逻辑与的结果作 MD5 运算产生。
- [0018] 对发送端 MD5 值不同于接收端 MD5 值的报文不通过认证,并将该报文丢弃。
- [0019] 所述身份认证 TLV 的字段位置位于紧邻终了 TLV 字段之前。
- [0020] 本发明还提出一种设置 OAM 安全认证的装置,其包括:
- [0021] 密钥设置模块,用于预先在 ME 两端的网络设备上分别设置密钥;
- [0022] OAM 报文发送模块,用于在报文发送端的网络设备发送的 OAM 报文中设置身份认证 TLV 字段,所述身份认证 TLV 字段包括 sequenceID 字段和发送端 MD5 值,所述发送端 MD5 值是由所述 sequenceID 字段和所述密钥逻辑运算而成;
- [0023] OAM 报文接收模块,用于 ME 另一端的网络设备在接收到所述 OAM 报文时,将所述报文中的 sequenceID 字段和本地预设的密钥进行相应的逻辑运算,得到接收端 MD5 值;以及
- [0024] MD5 值比较模块,用于比较所述发送端 MD5 值和接收端 MD5 值,并将两者相同的 OAM 报文通过 OAM 认证。
- [0025] 在同一维护实体组中的所有合法设备上,所述密钥相同。
- [0026] 所述身份认证 TLV 的字段位置位于紧邻终了 TLV 字段之前。
- [0027] 与现有技术相比,本发明通过在 OAM 报文中引入身份认证机制,保证了 OAM 的通信安全,使得运行 CFM 协议的设备不易受到来自互联网的恶意攻击影响,进而提高了运营商网络的稳定性。

附图说明

- [0028] 图 1 是本发明中设置 OAM 安全认证的方法的流程图;
- [0029] 图 2 是本发明中的 OAM PDU 报文的组成示意图;
- [0030] 图 3 是本发明中设置 OAM 安全认证的装置的框架图。

具体实施方式

- [0031] 下面将结合本发明的附图,对本发明实施例的技术方案进行清楚、完整的描述。
- [0032] 如图 1 所示,本发明提出的设置 OAM 安全认证的方法,其预先为 ME 两端的网络设备定义一个密钥,此密钥不会在网络中传输,而是保存在设备内部。在 ME 一端的网络设备发送的 OAM 报文中设置一个身份认证 TLV (Type Length Value, 类型长度数值) 的字段,该身份认证 TLV 字段包括一个 MD5 (Message-Digest Algorithm 5, 信息摘要算法第五版) 值以及 sequenceID, 该 MD5 值为发送端的 MD5 值,其由 OAM 报文中的 sequenceID 和密钥进行“逻辑与”运算而得出的结果。
- [0033] ME 另一端的网络设备在接收到 OAM 报文时,将 OAM 报文中的 sequenceID 与本地密钥进行“逻辑与”运算得到接收端 MD5 值,通过将此接收端 MD5 值与收到的 OAM 报文中的发送端 MD5 值进行比较,将两者相等的 OAM 报文认证通过,否则认证失败,丢弃该报文。
- [0034] 所述身份认证 TLV 的报文格式如表一所示:

端的网络设备上分别设置密钥,所述 OAM 报文发送模块用于在一端的网络设备发送的 OAM 报文中设置身份认证 TLV 字段,所述身份认证 TLV 字段包括 sequenceID 字段和发送端 MD5 值,所述发送端 MD5 值是由所述 sequenceID 字段和所述密钥逻辑运算而成。

[0045] 所述 OAM 报文接收模块用于 ME 另一端的网络设备在接收到所述 OAM 报文时,将所述报文中的 sequenceID 字段和本地预设的密钥进行相应的逻辑运算,得到接收端 MD5 值;

[0046] 所述 MD5 值比较模块用于比较所述发送端 MD5 值和接收端 MD5 值,并将两者相同的 OAM 报文通过 OAM 认证。

[0047] 本发明在实际使用中,由于在 OAM 报文中引入了身份认证 TLV,使得原来的 OAM 报文的长度得以增加,在应用本发明时,要保证包含认证 TLV 的 OAM 报文长度不能超过链路上的最小 MTU(MaximumTransmission Unit,最大传输单元)。同时,由于目前大多数网络设备的 MD5 运算是基于软件的,而 OAM 中 CCM 的最短间隔很短,因此,本发明不推荐对 CCM 报文添加认证 TLV 字段。

[0048] 本发明的技术内容及技术特征已揭示如上,然而熟悉本领域的技术人员仍可能基于本发明的教示及揭示而作种种不背离本发明精神的替换及修饰,因此,本发明保护范围应不限于实施例所揭示的内容,而应包括各种不背离本发明的替换及修饰,并为本专利申请权利要求所涵盖。

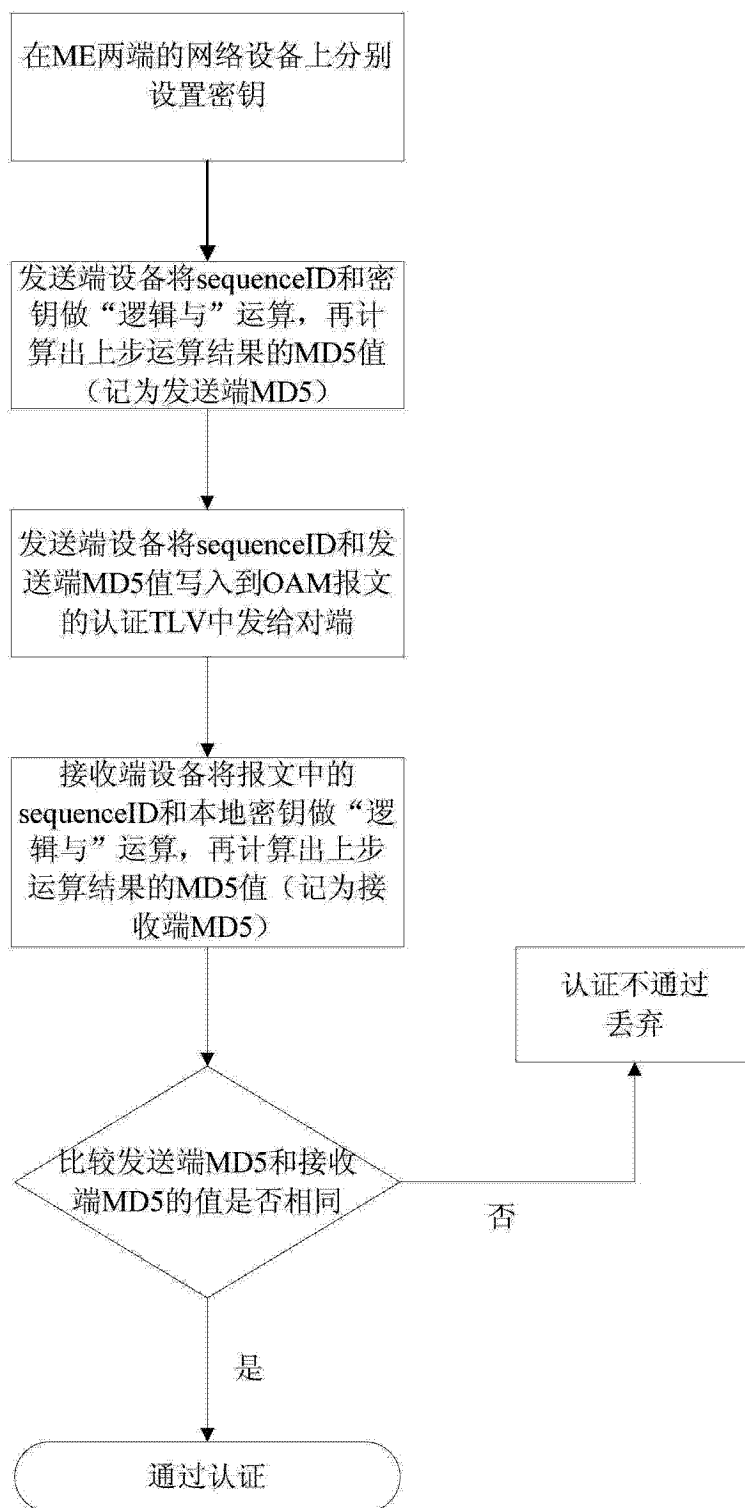


图 1

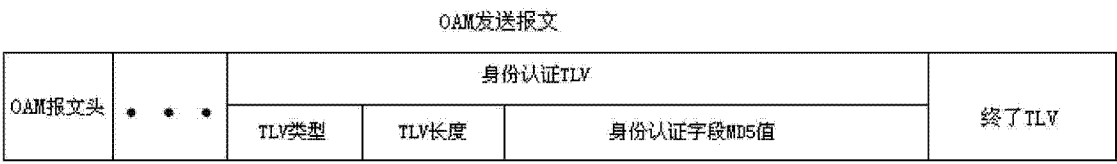


图 2

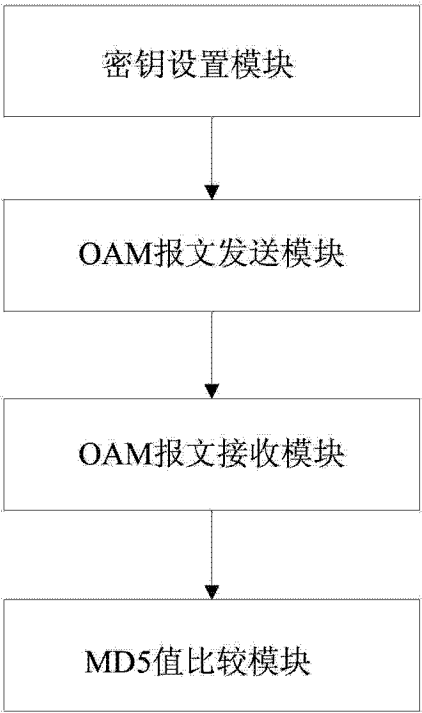


图 3