(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 111585965 B
(45)授权公告日 2021.05.14

(21)申请号 202010277208.3
(22)申请日 2020.04.10
(65)同一申请的已公布的文献号
申请公布号 CN 111585965 A
(43)申请公布日 2020.08.25
(73)专利权人 华南理工大学
地址 510640 广东省广州市天河区五山路381号
(72)发明人 陆以勤 毛中书 程喆 覃健诚 金冬子
(74)专利代理机构 广州市华学知识产权代理有限公司 44245
代理人 詹丽红
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/26(2006.01)
H04L 12/823(2013.01)

(56)对比文件
CN 105933184 A,2016.09.07
CN 103491076 A,2014.01.01
CN 108833430 A,2018.11.16
CN 109347889 A,2019.02.15
KR 20200031799 A,2020.03.25
WO 2019035634 A1,2019.02.21
CN 108632267 A,2018.10.09
Alharbi etal;.The (in) security of topology discovery in software defined networks.《IEEE》.2015,第502-505页.
赵汉佳.SDN控制平面安全防御研究.《中国优秀硕士学位论文全文数据库信息科技辑(月刊)》.2018,第I139-4页.
Nguyen etal;.Analysis of link discovery service attacks in SDN controller.《IEEE》.2017,第259-261页.

审查员 魏慧慧

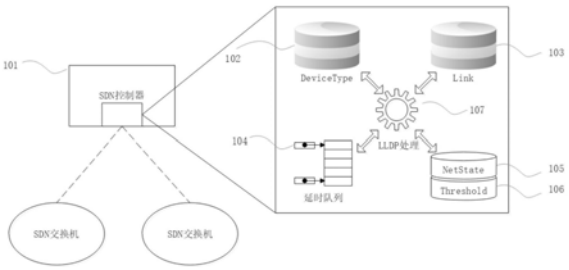
权利要求书3页 说明书8页 附图2页

(54)发明名称

一种防御软件定义网络中LLDP中继攻击的方法

(57)摘要

本发明公开了一种防御软件定义网络中LLDP中继攻击的方法,该方法包括以下步骤:记录每个端口和其连接的设备类型以及链路信息;记录LLDP帧延时并根据延时计算出当前的网络拥塞状态以及延时阈值;判断网络中新增链路的两个端口的设备类型是否都是HOST-REMOVED,如果是则认为满足LLDP中继攻击条件,需要进一步判断,如果不是则认为不满足LLDP中继攻击条件,将该LLDP判定为正常;若满足LLDP中继攻击的条件,此时结合网络拥塞状态判断该LLDP延时是否大于延时阈值,若大于延时阈值则判定为攻击并丢弃当前LLDP帧。该发明用以防御攻击者使用两台主机进行LLDP中继攻击,提高SDN控制器的安全性。



CN 111585965 B

1.一种防御软件定义网络中LLDP中继攻击的方法,其特征在于,所述方法包括下列步骤:

S1、在SDN控制器中记录每个端口和其连接的设备类型,记录链路信息;其中,在SDN控制器中维护一张DeviceType表,以记录每个端口和其接连的设备类型;其中,所述DeviceType表由PortID和Device组成,PortID使用数据路径DPID和端口号Port唯一标识网络中交换机的端口,Device表示该端口连接的设备类型;

S2、在SDN控制器中记录LLDP帧延时,并根据延时计算出当前的网络拥塞状态以及延时阈值;所述步骤S2过程如下:

在SDN控制器中设置大小为50的延时队列,用以记录最新的50个LLDP帧的延时时间;

在SDN控制器中设置初始值为0的Entropy_before、Entropy_current、NetState、Threshold,分别表示上一组延时队列的信息熵、当前延时队列的信息熵、当前网络的拥塞状态、延时阈值;

每当延时队列满时,首先将Entropy_current赋值给Entropy_before,接着统计当前延时队列中每个延时值出现的概率P_i,若延时值重复则只统计一次,因此i=1,2,……,m,0<m≤50,其中$P_i=N_i/50$,N_i为第i个延时在当前延时队列中出现的次数,再根据P_i计算出延时队列的信息熵H,其中$H = -\sum_{i=1}^{n} P_i \log_2 P_i$,$P_i$为第i个延时在当前延时队列中出现的概率,n为延时队列大小,最后将H值赋值给Entropy_current;

当Entropy_current更新后,比较Entropy_before与Entropy_current的大小,若出现熵增,即Entropy_before<Entropy_current则NetState值+1,若没有出现熵增,即Entropy_before≥Entropy_current则NetState值-1;

当NetState更新后,若此时Entropy_before≥Entropy_current且NetState≤0,则计算当前延时队列的平均值,并将该值乘以3后赋值给延时阈值Threshold,否则不更新延时阈值Threshold;

S3、判断网络中新增链路的两个端口的设备类型是否都是HOST-REMOVED,其中,HOST-REMOVED为Device字段的类型取值中的一种,当取值为HOST-REMOVED时代表上一次连接的设备为主机,如果不是则认为不满足LLDP中继攻击条件,将该LLDP帧判定为正常,如果是则认为该链路满足LLDP中继攻击条件,转入下一步骤对该LLDP帧进一步判断;

S4、若满足LLDP中继攻击的条件,此时结合网络拥塞状态判断该LLDP帧延时是否大于延时阈值,若大于延时阈值则判定为攻击并丢弃当前LLDP帧。

2.根据权利要求1所述的一种防御软件定义网络中LLDP中继攻击的方法,其特征在于,所述步骤S1过程如下:

在SDN控制器中维护一张DeviceType表,以记录每个端口和其接连的设备类型;其中,所述DeviceType表由PortID和Device组成,PortID使用数据路径DPID和端口号Port唯一标识网络中交换机的端口,Device表示该端口连接的设备类型,该Device字段的值共有四种类型:HOST、SWITCH、HOST-REMOVED、SWITCH-REMOVED,分别表示相应端口当前所连的设备为主机、交换机、空、空,HOST-REMOVED代表上一次连接的设备为主机;SWITCH-REMOVED代表上一次连接的设备为交换机;

在SDN控制器中维护一张Link表,以记录链路信息;其中,所述Link表由SrcPort和

DestPort组成,SrcPort使用DPID和Port标识链路的源端口,DestPort使用DPID和Port标识链路的目的端口;

当SDN控制器收到代表某个端口关闭的Port_down消息时,需要同时更新DeviceType表和Link表,当该端口存在于DeviceType表中时,若相应的Device字段为HOST则修改为HOST-REMOVED,若该字段为SWITCH则修改为SWITCH-REMOVED,当该端口存在于Link表中时,则需要删除SrcPort等于该端口的所有记录以及DestPort等于该端口的所有记录。

3.根据权利要求1所述的一种防御软件定义网络中LLDP中继攻击的方法,其特征在于,所述LLDP帧延时的计算方法如下:

修改SDN控制器生成的LLDP帧,在LLDP帧中的Optional TLV字段添加发送时间戳TLV,其值为每个LLDP帧的发送时间,当SDN控制器收到LLDP帧时,用当前收到的时间减去发送时间得到每个LLDP帧的传输延时。

4.根据权利要求2所述的一种防御软件定义网络中LLDP中继攻击的方法,其特征在于,所述步骤S3过程如下:

当SDN控制器收到一个Packet_in消息时,首先检查该Packet_in消息封装的消息类型,若封装的不是LLDP帧则根据Packet_in消息解析出交换机的接收端口Port,此时在DeviceType表中查找LLDP帧记录,若在DeviceType表中未查找到相应的记录则根据Port创建该记录,并将相应的Device字段设为HOST,若在DeviceType表中找到相应的记录,则无需更新DeviceType表;

若Packet_in消息封装的是LLDP帧时,则从Packet_in消息中取出链路信息,即链路源端口SrcPort和目的端口DestPort,然后判断该链路信息是否已存在于Link表中,若存在则代表该链路不是新增链路,此时计算得到该LLDP帧的延时值,并将该延时值交付延时队列,若该链路信息在Link表中不存在,那么判定该链路是一条新增链路,继续判断链路源端口SrcPort和目的端口DestPort在DeviceType表中的记录;

若链路源端口SrcPort和目的端口DestPort在DeviceType表中都有记录,且相应的Device字段都为HOST,那么直接丢弃该包并发出警报:“该链路是通过LLDP中继攻击伪造的”;若链路源端口SrcPort和目的端口DestPort在DeviceType表中都有记录,且都是HOST-REMOVED,此时该新增链路满足了LLDP中继攻击发起的条件,需要结合网络拥塞状态判断该LLDP延时是否正常;

若链路源端口SrcPort和目的端口DestPort不满足上述的两种情况,此时判断该链路不是LLDP中继攻击伪造的,使用该LLDP帧的延时更新延时队列,在Link表中添加源端口为SrcPort、目的端口为DestPort的链路,将DeviceType表中PortID分别为SrcPort和DestPort的两条记录的Device字段值设为SWITCH,即SrcPort和DestPort两个端口所连的设备为交换机,若在DeviceType表中没有相关记录则创建相应的记录,并将Device字段值设为SWITCH。

5.根据权利要求2所述的一种防御软件定义网络中LLDP中继攻击的方法,其特征在于,所述步骤S4过程如下:

首先检查NetState值,若该值大于0则丢弃当前的LLDP帧并发出警报:当前网络拥塞,不允许添加满足LLDP攻击条件的链路;

若NetState值小于等于0,比较当前LLDP帧的延时与延时阈值Threshold,若当前LLDP

帧延时大于延时阈值Threshold则丢弃当前LLDP帧,并发出警报:“该链路是通过LLDP中继攻击伪造的”;若当前LLDP帧延时小于等于延时阈值Threshold,则该新增链路一定为真,使用该LLDP帧的延时更新延时队列,在Link表中添加源端口为SrcPort、目的端口为DestPort的链路,同时将DeviceType表中PortID分别为SrcPort和DestPort的两条记录的Device字段值设为SWITCH,即SrcPort和DestPort两个端口所连的设备为交换机。

一种防御软件定义网络中LLDP中继攻击的方法

技术领域

[0001] 本发明涉及计算机网络技术领域，特别是软件定义网络(Software Defined Network，SDN)新式网络技术领域，具体涉及一种防御软件定义网络中LLDP中继攻击的方法。

背景技术

[0002] 软件定义网络(SDN)是一种新型的网络范式，它赋予控制器及其应用以全局的网络可视性和灵活的网络可编程性，实现了网络协议和应用的创新。SDN的核心优势之一就是SDN控制器提供了许多SDN应用所依赖的整个网络可视性。

[0003] SDN控制器使用链路层发现协议(Link Layer Discovery Protocol，LLDP)发现所有交换机之间的链路，当交换机的端口开启时，交换机会首先发送该端口的Port_up消息至控制器，控制器收到Port_up消息后为该端口生成LLDP并将生成的LLDP通过交换机相应的端口发送出去，若控制器从另外一台交换机收到了该LLDP，那么控制器就会认为这两台交换机之间存在一条链路。

[0004] 由上述过程可以看出，即使是主机也可以收到控制器所发的LLDP，因此攻击者可以通过两台主机中继各自收到LLDP在网络中伪造一条虚假链路。

[0005] 目前防御LLDP中继攻击的方法有：1、一种软件定义网络的拓扑保护方法；2、一种拓扑污染攻击防御方法和系统；3、TopoGuard+。简单介绍如下：

[0006] 现有技术一：一种软件定义网络的拓扑保护方法

[0007] 原理：初始化并维护每一个存活交换机端口的端口信息；根据收集到的Packet-in消息，进行主机状态检测，然后根据主机状态检测结果及所维护的端口信息对LLDP报文进行分类；针对不同类型的LLDP报文，采用相应的攻击检测方法进行攻击检测；若检测到攻击报文，则将攻击报文的报文规则实时记录在控制器的过滤规则中，从而通过报文规则过滤的方式实现攻击防御；持续收集数据平面的Packet-in消息并根据收集到的Packet-in消息更新所维护的端口信息，同时重复执行攻击检测和防御的步骤。

[0008] 缺点：该方法需要训练链路模型，使得所述链路检测模型学习到正常链路和异常链路的流量特征，以此判断链路是正常链路还是异常链路，因此当攻击者通过LLDP中继攻击伪造了一条链路后，只需要在这条链路上伪造出类似正常链路的流量特征即可绕过该防御方法。

[0009] 现有技术二：一种拓扑污染攻击防御方法和系统

[0010] 原理：1)通过监听SDN控制器收到的Packet-In消息，记录网络中主机，判断该主机是否是真实的主机，所述真实主机是指该主机使用本机的IP和MAC地址发送主机流量；2)通过监听SDN控制器下发流表项信号和SDN交换机上传的流表项删除消息，维护每个交换机端口流表项的记录表，并且通过该表判断某个端口的主机是否离开了网络，以防止流量劫持攻击；3)通过给SDN控制器下发的LLDP帧加上随机字符串作为校验字段，并对SDN控制器收到的LLDP帧进行检查，以防止利用LLDP帧来伪造链路的攻击。

[0011] 缺点:该方法在防御LLDP中继攻击时,攻击者只需要重启相应主机的网卡再发起LLDP中继攻击即可绕过该方法成功伪造链路,因此无法完全防御LLDP中继攻击。

[0012] 现有技术三:TopoGuard+

[0013] 原理:记录所有LLDP的延时,通过四分位法计算出延时阈值,再将每个LLDP延时与延时阈值进行比较,若LLDP延时大于阈值,则该LLDP是通过LLDP中继的,若LLDP延时小于阈值则该LLDP代表的链路是真实的。

[0014] 缺点:由于TopoGuard+的延时阈值是通过所有LLDP的延时阈值计算的,所以攻击者只要想网络中注入数据包,缓慢增加链路延时即可导致控制器计算的LLDP延时阈值变大,最终使得该延时阈值无法用来区分当前的LLDP是否是攻击这中继的。

[0015] 综上所述现有的防御方法,要么依赖额外的训练数据,要么无法完全防御LLDP中继攻击,要么本身存在逻辑漏洞导致攻击者依然可以实现LLDP中继攻击,适用场景有限。

发明内容

[0016] 本发明的目的是为了解决现有技术中的上述缺陷,提供一种防御软件定义网络中LLDP中继攻击的方法,用以防御攻击者使用两台主机进行LLDP中继攻击,提高SDN控制器的安全性。

[0017] 本发明的目的可以通过采取如下技术方案达到:

[0018] 一种防御软件定义网络中LLDP中继攻击的方法,所述方法包括下列步骤:

[0019] S1、在SDN控制器中记录每个端口和其连接的设备类型,记录链路信息;

[0020] S2、在SDN控制器中记录LLDP帧延时,并根据延时计算出当前的网络拥塞状态以及延时阈值;

[0021] S3、判断网络中新增链路的两个端口的设备类型是否都是HOST-REMOVED,如果不是则认为不满足LLDP中继攻击条件,将该LLDP帧判定为正常,如果是则认为该链路满足LLDP中继攻击条件,转入下一步骤对该LLDP帧进一步判断;

[0022] S4、若满足LLDP中继攻击的条件,此时结合网络拥塞状态判断该LLDP帧延时是否大于延时阈值,若大于延时阈值则判定为攻击并丢弃当前LLDP帧。

[0023] 进一步地,所述步骤S1过程如下:

[0024] 在SDN控制器中维护一张DeviceType表,以记录每个端口和其接连的设备类型;其中,所述DeviceType表由PortID和Device组成,PortID使用数据路径DPID和端口号Port唯一标识网络中交换机的端口,Device表示该端口连接的设备类型,该字段的值共有四种类型:HOST、SWITCH、HOST-REMOVED、SWITCH-REMOVED,分别表示相应端口当前所连的设备为主机、交换机、空、空,HOST-REMOVED代表上一次连接的设备为主机;SWITCH-REMOVED代表上一次连接的设备为交换机;

[0025] 在SDN控制器中维护一张Link表,以记录链路信息;其中,所述Link表由SrcPort和DestPort组成,SrcPort使用DPID和Port标识链路的源端口,DestPort使用DPID和Port标识链路的目的端口;

[0026] 当SDN控制器收到代表某个端口关闭的Port_down消息时,需要同时更新DeviceType表和Link表,当该端口存在于DeviceType表中时,若相应的Device字段为HOST则修改为HOST-REMOVED,若该字段为SWITCH则修改为SWITCH-REMOVED,当该端口存在于

Link表中时，则需要删除SrcPort等于该端口的所有记录以及DestPort等于该端口的所有记录。

[0027] 进一步地，所述LLDP帧延时的计算方法如下：

[0028] 修改SDN控制器生成的LLDP帧，在LLDP帧中的Optional TLV字段添加发送时间戳TLV，其值为每个LLDP帧的发送时间，当SDN控制器收到LLDP帧时，用当前收到的时间减去发送时间得到每个LLDP帧的传输延时。

[0029] 进一步地，所述步骤S2过程如下：

[0030] 在SDN控制器中设置大小为50的延时队列，用以记录最新的50个LLDP帧的延时时间；

[0031] 在SDN控制器中设置初始值为0的Entropy_before、Entropy_current、NetState、Threshold，分别表示上一组延时队列的信息熵、当前延时队列的信息熵、当前网络的拥塞状态、延时阈值；

[0032] 每当延时队列满时，首先将Entropy_current赋值给Entropy_before，接着统计当前延时队列中每个延时值出现的概率P_i，若延时值重复则只统计一次，因此i＝1,2,……，m,0＜m≤50，其中P_i＝N_i/50，N_i为第i个延时在当前延时队列中出现的次数，再根据P_i计算出延时队列的信息熵H，其中$H = -\sum_{i=1}^{n} P_i \log_2 P_i$，$P_i$为第i个延时在当前延时队列中出现的概率，最后将H值赋值给Entropy_current；

[0033] 当Entropy_current更新后，比较Entropy_before与Entropy_current的大小，若出现熵增，即Entropy_before＜Entropy_current则NetState值+1，若没有出现熵增，即Entropy_before≥Entropy_current则NetState值-1；

[0034] 当NetState更新后，若此时Entropy_before≥Entropy_current且NetState≤0，则计算当前延时队列的平均值，并将该值乘以3后赋值给延时阈值Threshold，否则不更新延时阈值Threshold。

[0035] 进一步地，所述步骤S3过程如下：

[0036] 当SDN控制器收到一个Packet_in消息时，首先检查该Packet_in消息封装的消息类型，若封装的不是LLDP帧则根据Packet_in消息解析出交换机的接收端口Port，此时在DeviceType表中查找LLDP帧记录，若在DeviceType表中未查找到相应的记录则根据Port创建该记录，并将相应的Device字段设为HOST，若在DeviceType表中找到相应的记录，则无需更新DeviceType表；

[0037] 若Packet_in消息封装的是LLDP帧时，则从Packet_in消息中取出链路信息，即链路源端口SrcPort和目的端口DestPort，然后判断该链路信息是否已存在于Link表中，若存在则代表该链路不是新增链路，此时计算得到该LLDP帧的延时值，并将该延时值交付延时队列，若该链路信息在Link表中不存在，那么判定该链路是一条新增链路，继续判断链路源端口SrcPort和目的端口DestPort在DeviceType表中的记录；

[0038] 若链路源端口SrcPort和目的端口DestPort在DeviceType表中都有记录，且相应的Device字段都为HOST，那么直接丢弃该包并发出警报：“该链路是通过LLDP中继攻击伪造的”；若链路源端口SrcPort和目的端口DestPort在DeviceType表中都有记录，且都是HOST-REMOVED，此时该新增链路满足了LLDP中继攻击发起的条件，需要结合网络拥塞状态判断该LLDP延时是否正常；

[0039] 若链路源端口SrcPort和目的端口DestPort不满足上述的两种情况，此时判断该链路不是LLDP中继攻击伪造的，使用该LLDP帧的延时更新延时队列，在Link表中添加源端口为SrcPort、目的端口为DestPort的链路，将DeviceType表中PortID分别为SrcPort和DestPort的两条记录的Device字段值设为SWITCH，即SrcPort和DestPort两个端口所连的设备为交换机，若在DeviceType表中没有相关记录则创建相应的记录，并将Device字段值设为SWITCH。

[0040] 进一步地，所述步骤S4过程如下：

[0041] 首先检查NetState值，若该值大于0则丢弃当前的LLDP帧并发出警报：当前网络拥塞，不允许添加满足LLDP攻击条件的链路；

[0042] 若NetState值小于等于0，比较当前LLDP帧的延时与延时阈值Threshold，若当前LLDP帧延时大于延时阈值Threshold则丢弃当前LLDP帧，并发出警报：“该链路是通过LLDP中继攻击伪造的”；若当前LLDP帧延时小于等于延时阈值Threshold，则该新增链路一定为真，使用该LLDP帧的延时更新延时队列，在Link表中添加源端口为SrcPort、目的端口为DestPort的链路，同时将DeviceType表中PortID分别为SrcPort和DestPort的两条记录的Device字段值设为SWITCH，即SrcPort和DestPort两个端口所连的设备为交换机。

[0043] 本发明相对于现有技术具有如下的优点及效果：

[0044] 1、本发明在防御LLDP中继攻击时不依赖第三方安全性，比如在现有技术“一种软件定义网络的拓扑保护方法”中其安全性依赖额外的训练集是否完善，训练集越完善则其方法越安全，但本发明不依赖第三方的安全性，而是充分利用了SDN自身的特性实现LLDP中继攻击的防御；

[0045] 2、本发明防御更加全面，比如现有技术“一种拓扑污染攻击防御方法和系统”中攻击者可以通过重启网卡的方式来实现LLDP中继攻击，但在本发明中会被有效防御；

[0046] 3、本发明没有引入新的安全漏洞，比如现有技术“TopoGuard+”中，TopoGuard+对每个LLDP的延时都进行了校验，攻击者可以通过向网络中恶意注入数据包提高网络延时的方式让控制器无法识别真实的链路，但本发明没有引入这种新漏洞。

附图说明

[0047] 图1是本发明实施例提供的一种防御软件定义网络中LLDP中继攻击的方法组成示意图；

[0048] 图2是本发明实施例提供的一种在LLDP中添加额外发送时间戳TLV的结构组成示意图；

[0049] 图3是本发明实施例提供的一种防御软件定义网络中LLDP中继攻击的流程图。

具体实施方式

[0050] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例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。

[0051] 实施例一

[0052] 针对现有SDN网络中,控制器无法有效防御LLDP中继攻击的问题,本实施例在SDN控制器中记录每个端口和其连接的设备类型,记录链路信息;在SDN控制器中记录LLDP延时,并根据延时计算出当前的网络拥塞状态以及延时阈值;判断网络中新增链路的两个端口的设备类型是否都是HOST-REMOVED,如果是则认为该链路满足LLDP中继攻击条件,需要对该LLDP帧进一步判断,如果不是则认为不满足LLDP中继攻击条件,将该LLDP帧判定为正常;若满足LLDP中继攻击的条件,此时结合网络拥塞状态判断该LLDP延时是否大于延时阈值,若大于延时阈值则判定为攻击并丢弃当前LLDP帧;从而实现了防御LLDP中继攻击。

[0053] 如图1所示,本发明提供一种防御软件定义网络中LLDP中继攻击的方法,包括以下步骤:

[0054] S1、在SDN控制器101中记录每个端口和其连接的设备类型102以及链路信息103;

[0055] S2、在SDN控制器101记录LLDP帧延时104并根据延时计算出当前的网络拥塞状态105以及延时阈值106;

[0056] S3、判断网络107中新增链路的两个端口的设备类型是否都是HOST-REMOVED,如果是则认为满足LLDP中继攻击条件,需要进一步判断,如果不是则认为不满足LLDP中继攻击条件,将该LLDP帧判定为正常;

[0057] S4、若满足LLDP中继攻击的条件,此时结合网络拥塞状态判断该LLDP帧延时是否大于延时阈值,若大于延时阈值则判定为攻击并丢弃当前LLDP帧。

[0058] 在本实施例中,步骤S1、在SDN控制器中记录每个端口所连的设备类型,记录链路信息的过程如下:

[0059] 在SDN控制器中维护一张DeviceType表,以记录每个端口和其接连的设备类型;

[0060] DeviceType表由PortID和Device组成,PortID使用数据路径(DPID)和端口号(Port)唯一地标识了网络中交换机的端口,Device表示该端口连接的设备类型,该字段的值共有四种类型:HOST、SWITCH、HOST-REMOVED、SWITCH-REMOVED,分别表示相应端口当前所连的设备为主机、交换机、空(上一次连接的设备为主机)、空(上一次连接的设备为交换机),具体可见下表1;

[0061] 表1.DeviceType表

[0062]

PortID	Deivce
【S1】【P1】	HOST
【S1】【P2】	SWITCH
【S2】【P1】	HOST-REMOVED
【S2】【P2】	SWITCH-REMOVED

[0063] 现有技术“TopoGuard+”只记录了HOST、SWITCH、ANY三种状态,因此无法判别LLDP中继攻击的条件。本发明的DeviceType表记录了更为详细的设备连接情况,可以看出LLDP中继攻击的条件。

[0064] 在SDN控制器中维护一张Link表,以记录链路信息。

[0065] Link表由SrcPort和DestPort组成,SrcPort使用DPID和Port标识链路的源端口,DestPort使用DPID和Port标识了链路的目的端口,具体可见下表2;

[0066] 表2.Link表

[0067]

SrcPort	DestPort

【S1】【P1】	【S2】【P1】
【S2】【P2】	【S3】【P1】

[0068] 当SDN控制器收到代表某个端口关闭的Port_down消息时，需要同时更新DeviceType表和Link表，当该端口存在于DeviceType表中时，若相应的Device字段为HOST则修改为HOST-REMOVED，若该字段为SWITCH则修改为SWITCH-REMOVED，当该端口存在于Link表中时，则需要删除SrcPort等于该端口的所有记录以及DestPort等于该端口的所有记录。

[0069] 现有技术如“TopoGuard+”、“一种拓扑污染攻击防御方法和系统”没有维护此类表格，因此会对所有LLDP帧都进行校验。本发明通过Link只对新增链路进行校验，在提高效率的同时也防止攻击者对已经存在的链路发起攻击。

[0070] 在本实施例中，LLDP帧延时的计算方法如下：

[0071] 修改SDN控制器生成的LLDP帧，在LLDP帧中添加发送时间戳TLV，其值为每个LLDP帧的发送时间，当SDN控制器收到LLDP帧时，用当前收到的时间减去发送时间得到每个LLDP帧的传输延时。修改后的LLDP帧具体可见图2。

[0072] 在本实施例中，步骤S2、在控制器中记录LLDP帧延时并根据延时计算出当前的网络拥塞状态以及延时阈值的过程如下：

[0073] 在SDN控制器中设置大小为50的延时队列，用以记录最新的50个LLDP帧的延时时间；

[0074] 在SDN控制器中设置初始值为0的Entropy_before、Entropy_current、NetState、Threshold，分别表示上一组延时队列的信息熵、当前延时队列的信息熵、当前网络的拥塞状态、延时阈值；

[0075] 每当延时队列满时，首先将Entropy_current赋值给Entropy_before，接着统计当前延时队列中每个延时值出现的概率P_i，若延时值重复则只统计一次，因此i＝1,2,……，m,0＜m≤50，其中$P_i＝N_i/50$，N_i为第i个延时在当前延时队列中出现的次数，再根据P_i计算出延时队列的信息熵H，其中$H = -\sum_{i=1}^{n} P_i \log_2 P_i$，$P_i$为第i个延时在当前延时队列中出现的概率，最后将H值赋值给Entropy_current；

[0076] 当Entropy_current更新后，比较Entropy_before与Entropy_current的大小，若出现熵增，即Entropy_before＜Entropy_current则NetState值+1，若没有出现熵增，即Entropy_before≥Entropy_current则NetState值-1；

[0077] 当NetState更新后，若此时Entropy_before≥Entropy_current且NetState≤0，则计算当前延时队列的平均值，并将该值乘以3后赋值给延时阈值Threshold，否则不更新延时阈值Threshold。

[0078] 现有技术“一种软件定义网络的拓扑保护方法”的安全性依赖训练集的完善程度，训练集越完善则安全性越高。本发明不需要依赖第三方，且可以自适应调整阈值。

[0079] 在本实施例中，步骤S3、判断网络中新增链路的两个端口的设备类型是否都是HOST-REMOVED，如果是则认为满足LLDP中继攻击条件，需要进一步判断，如果不是则认为不满足LLDP中继攻击条件，将该LLDP判定为正常的过程如下：

[0080] 当SDN控制器收到一个Packet_in消息时，首先检查该Packet_in消息封装的消息类型，若封装的不是LLDP帧则根据Packet_in消息解析出交换机的接收端口Port，此时在

DeviceType表中查找LLDP帧记录,若在DeviceType表中未查找到相应的记录则根据接收端口Port创建该记录,并将相应的Device字段设为HOST,若在DeviceType表中找到相应的记录,则无需更新DeviceType表;

[0081] 若Packet_in消息封装的是LLDP帧时,则从Packet_in消息中取出链路信息,即链路源端口SrcPort和目的端口DestPort,然后判断该链路信息是否已存在于Link表中,若存在则代表该链路不是新增链路,此时计算得到该LLDP帧的延时值,并将该延时值交付延时队列,若该链路信息在Link表中不存在,那么判定该链路是一条新增链路,继续判断链路源端口SrcPort和目的端口DestPort在DeviceType表中的记录;

[0082] 若链路源端口SrcPort和目的端口DestPort在DeviceType表中都有记录,且相应的Device字段都为HOST,那么直接丢弃该包并发出警报:“该链路是通过LLDP中继攻击伪造的”;若链路源端口SrcPort和目的端口DestPort在DeviceType表中都有记录,且都是HOST-REMOVED,此时该新增链路满足了LLDP中继攻击发起的条件,需要结合网络拥塞状态判断该LLDP延时是否正常;

[0083] 若链路源端口SrcPort和目的端口DestPort不满足上述的两种情况,此时判断该链路不是LLDP中继攻击伪造的,使用该LLDP帧的延时更新延时队列,在Link表中添加源端口为SrcPort、目的端口为DestPort的链路,将DeviceType表中PortID分别为SrcPort和DestPort的两条记录的Device字段值设为SWITCH,若在DeviceType表中没有相关记录则创建相应的记录,并将Device字段值设为SWITCH。

[0084] 在本实施例中,步骤S4、若满足LLDP中继攻击的条件,此时结合网络拥塞状态判断该LLDP帧延时是否大于延时阈值,若大于延时阈值则判定为攻击并丢弃当前LLDP帧的过程如下:

[0085] 首先检查NetState值,若该值大于0则丢弃当前的LLDP帧并发出警报:当前网络拥塞,不允许添加满足LLDP攻击条件的链路;

[0086] 若NetState值小于等于0,比较当前LLDP帧的延时与延时阈值Threshold,若当前LLDP帧延时大于延时阈值Threshold则丢弃当前LLDP帧,并发出警报:“该链路是通过LLDP中继攻击伪造的”;若当前LLDP帧延时小于等于延时阈值Threshold,则该新增链路一定为真,因此使用该LLDP帧的延时更新延时队列,在Link表中添加源端口为SrcPort、目的端口为DestPort的链路,同时将DeviceType表中PortID分别为SrcPort和DestPort的两条记录的Device字段值设为SWITCH,即SrcPort和DestPort两个端口所连的设备为交换机。

[0087] 现有技术如“TopoGuard+”直接比较LLDP帧延时与阈值的大小,而不考虑网络的拥塞程度,因此会引入新的安全问题。本发明则将该问题考虑在内,在判断LLDP帧延时的判断了当前网络拥塞程度。

[0088] 实施例二

[0089] 如图3所示,本实施例公开了一种防御软件定义网络中LLDP中继攻击的方法,根据流程图,该方法包括下列步骤:

[0090] S301、当SDN控制器收到一个Packet_in消息时,首先判断该消息封装的是LLDP帧还是非LLDP帧,若是LLDP帧则转到步骤S302,若不是LLDP帧则转到步骤S315;

[0091] S302、通过Link表判断当前LLDP帧代表的链路是否是新增链路,若是新增链路则转到步骤S303,若不是则转到步骤S308;

[0092] S303、通过DeviceType表判断该链路的两个端口的Device字段是否包含HOST，若包含则转到步骤S317，否则转到步骤S304；

[0093] S304、通过DeviceType表判断该链路的两个端口的Device字段是否都HOST-REMOVED，若都是则转到步骤S305，否则转到步骤S309；

[0094] S305、判断当前NetState值是否小于等于0，若NetState≤0则转到步骤S306，否则转到步骤S318；

[0095] S306、判断当前LLDP延时是否大于Threshold，若大于则转到步骤S307，否则转到步骤S309；

[0096] S307、丢弃当前LLDP帧并发出警报：“该新增链路是通过LLDP中继攻击伪造的”，此流程结束。

[0097] S308、将当前LLDP帧延时直接添加进延时队列；

[0098] S309、当前新增链路为真，将该链路的源端口SrcPort与目的端口DestPort添加进DeviceType表中，相应的Device字段都设置为SWITCH，同时在Link表中添加源端口为SrcPort、目的端口为DestPort的链路，最后将该LLDP帧延时添加到延时队列；

[0099] S310、当延时队列更新后，判断此时队列是否已满，若队列已满则转到步骤S311，否则转到步骤S314；

[0100] S311、将当前的Entropy_current赋值给Entropy_before，计算当前延时队列的信息熵并将熵值赋给Entropy_current，然后比较Entropy_current与Entropy_before的大小，若出现熵增则转到步骤312，否则转到步骤S313；

[0101] S312、此时不更新Threshold值，将NetState值加1，并清空延时队列，此流程结束。

[0102] S313、计算当前延时队列的平均值，并将该值乘以3后赋给延时阈值Threshold，同时NetState值减1，并清空延时队列，此流程结束。

[0103] S314、此时不需要更新延时阈值Threshold与NetState值，此流程结束。

[0104] S315、从Packet_in消息中取出端口Port信息，并在DeviceType表中查找是否存在PortID为Port的记录，若有记录则此流程结束，若无记录则转到步骤S316；

[0105] S316、在DeviceType表中添加PortID为Port的记录，同时将Device字段设为HOST，此流程结束。

[0106] S317、丢弃当前LLDP帧并发出警报：“该新增链路是通过LLDP中继攻击伪造的”，此流程结束。

[0107] S318、当前网络出于拥塞状态，丢弃当前LLDP帧并发出提示：“在网络拥塞时不允许添加满足LLDP中继攻击条件的链路”，此流程结束。

[0108] 上述实施例为本发明较佳的实施方式，但本发明的实施方式并不受上述实施例的限制，其他的任何未背离本发明的精神实质与原理下所作的改变、修饰、替代、组合、简化，均应为等效的置换方式，都包含在本发明的保护范围之内。

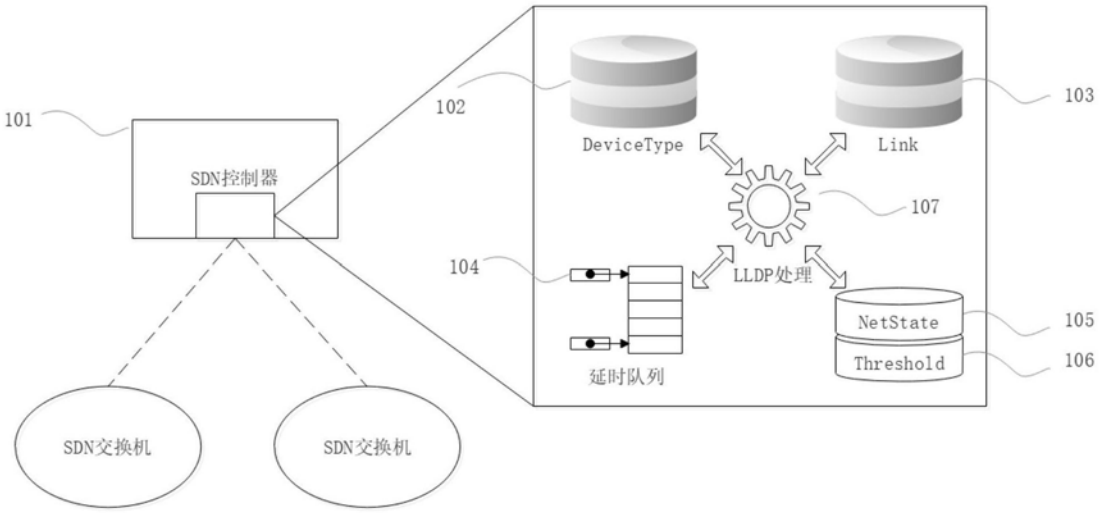

101
SDN控制器
102
DeviceType
Link
103
107
104
LLDP处理
NetState
105
Threshold
106
延时队列
SDN交换机
SDN交换机

图1

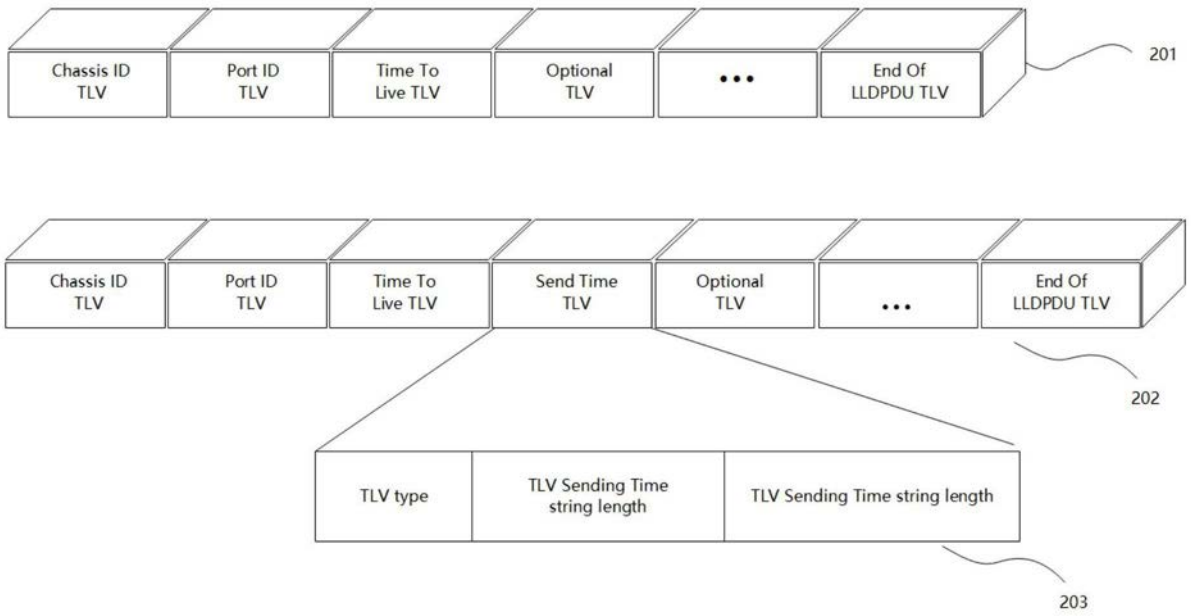

Chassis ID TLV
Port ID TLV
Time To Live TLV
Optional TLV
...
End Of LLDPDU TLV
201
Chassis ID TLV
Port ID TLV
Time To Live TLV
Send Time TLV
Optional TLV
...
End Of LLDPDU TLV
202
TLV type
TLV Sending Time string length
TLV Sending Time string length
203

图2

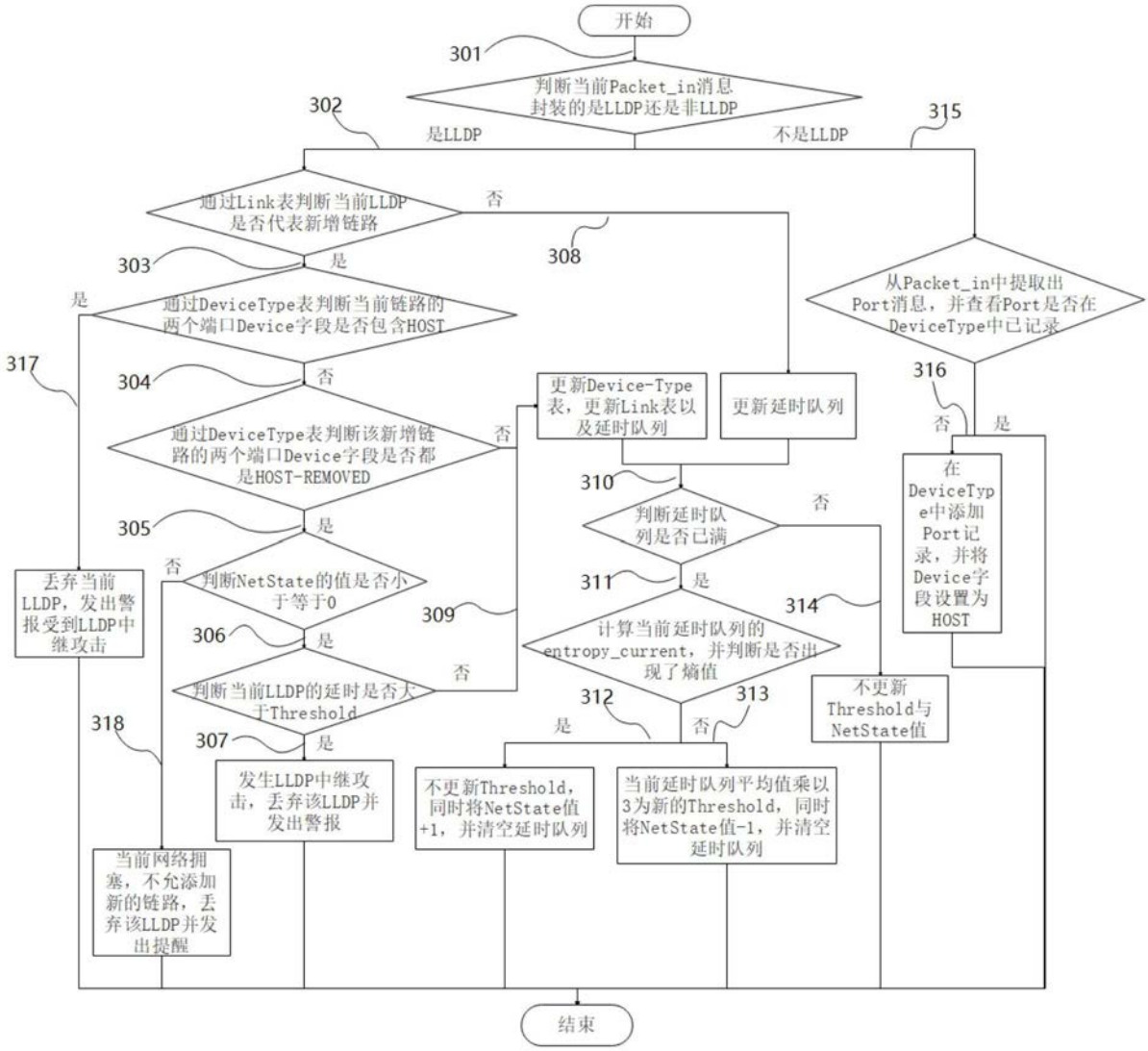

开始
301
判断当前Packet_in消息封装的是LLDP还是非LLDP
302
是LLDP
不是LLDP
315
通过Link表判断当前LLDP是否代表新增链路
否
308
303
是
通过DeviceType表判断当前链路的两个端口Device字段是否包含HOST
是
317
304
否
通过DeviceType表判断该新增链路的两个端口Device字段是否都是HOST-REMOVED
否
更新Device-Type表，更新Link表以及延时队列
更新延时队列
从Packet_in中提取出Port消息，并查看Port是否在DeviceType中已记录
316
否
是
在DeviceType中添加Port记录，并将Device字段设置为HOST
310
判断延时队列是否已满
否
305
是
否
判断NetState的值是否小于等于0
丢弃当前LLDP，发出警报受到LLDP中继攻击
309
311
是
314
306
是
否
计算当前延时队列的entropy_current，并判断是否出现了熵值
判断当前LLDP的延时是否大于Threshold
不更新Threshold与NetState值
318
307
是
312
是
313
否
发生LLDP中继攻击，丢弃该LLDP并发出警报
不更新Threshold，同时将NetState值+1，并清空延时队列
当前延时队列平均值乘以3为新的Threshold，同时将NetState值-1，并清空延时队列
当前网络拥塞，不允许添加新的链路，丢弃该LLDP并发出提醒
结束

图3