(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 105939207 B
(45)授权公告日 2017.06.23

(21)申请号 201510844018.4

(22)申请日 2015.11.26

(65)同一申请的已公布的文献号
申请公布号 CN 105939207 A

(43)申请公布日 2016.09.14

(73)专利权人 北京匡恩网络科技有限责任公司
地址 100102 北京市昌平区未来科技城定泗路237号都市绿洲304室

(72)发明人 孙易安

(74)专利代理机构 北京润平知识产权代理有限公司 11283
代理人 王崇

(51)Int.Cl.
H04L 12/24(2006.01)

(56)对比文件
CN 101163109 A,2008.04.16,
CN 101252488 A,2008.08.27,
WO 03019870 A2,2003.03.06,
杨杉等.基于路由协议分析的路由管理系统.《信息安全与通信保密》.2009,(第03期),第72-73页.

审查员 谢琳

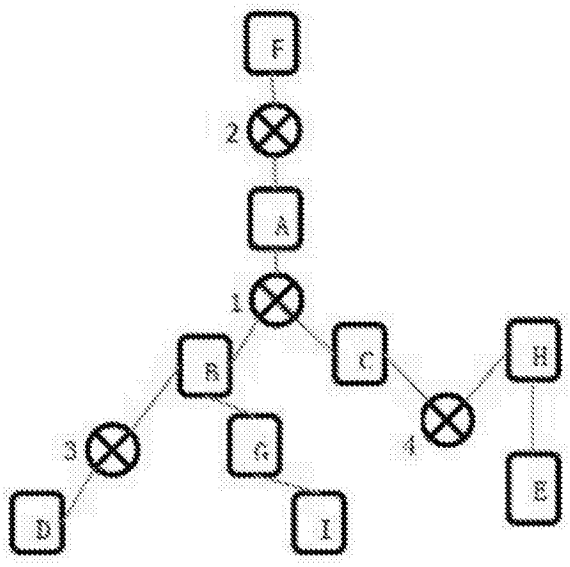
权利要求书1页 说明书4页 附图1页

(54)发明名称

一种基于网络探针的网络拓扑自动发现方法

(57)摘要

本发明提供一种基于网络探针的网络拓扑自动发现方法，该方法包括以下步骤：步骤一：在所需发现网络中置入网络探针，收集探针上下游数据；步骤二：列出每个探针对网络的划分，采用寻找划分的方法，找到一个对网络的划分；步骤三：采用寻找连接的方法，找到探针与分区的连接关系，从而发现拓扑。本发明所述的基于网络探针的网络拓扑自动发现方法，无需特殊的硬件支持，不需要主动发送数据包去干扰网络，并且可重复利用探针对网络结构进行逐步细化，具有广泛的适用性。



CN 105939207 B

1.一种基于网络探针的网络拓扑自动发现方法，包括以下步骤：

步骤一：在所需发现网络中置入网络探针，收集探针上下游数据；

步骤二：列出每个探针对网络的划分，采用寻找划分的方法，找到一个对网络的划分；

步骤三：采用寻找连接的方法，找到探针与分区的连接关系，从而发现拓扑；

其中，所述寻找划分的方法如下：

1）列出对应每个探针的初始划分D_i，i＝1...m，令k为k＝1；其中，m为探针个数，D_i为探针i对网络节点的划分，即s_i+1个分区所构成的集合；

2）取分区$z_k^{(1)}$依次与其它划分的每一个分区$z_l^{(j)}$，j≠1进行比较，若$z_k^{(1)} \bigcap z_l^{(j)} = C \neq \Phi$，且C为$z_k^{(1)}$的真子集，则将原来的一个分区分割成新的两个分区，即

$$z_k^{(1)} \rightarrow z_k^{(1)} = z_k^{(1)} \setminus C \quad , \quad z_{s_1+1}^{(1)} = C$$

并更新下标s_1为s_1+1，令下标k为k－1，跳到第3）步；

3）如果k＝s_1，停止，令D＝D_1，输出D所对应的划分，否则，令下标k为k+1，返回上述2）；

其中$z_l^{(j)}$的含义为探针j对网络节点划分中的第l个分区；

其中，所述寻找连接基于找到的划分寻找探针与分区之间的连接信息，其具体方法如下：

1）列出每个探针的划分$\{D_i\}$，i＝1...m；

2）遍历$\{D_i\}$，若某一个划分D_j中存在与划分D相同的分区，即存在

$z_k^{(j)} \in D_j$且$z_k^{(j)} \in D$，则探针j与分区$z_k^{(j)}$相连；

3）比较任意两个来自属不同探针划分的分区，若两个分区为包含关系且两分区的差集属于D，则此差集与两探针相连，也即或存在$z_k^{(j)} \subset z_l^{(s)}$且$z_l^{(s)} \setminus z_k^{(j)} = C \in D$，则C与探针s和j相连。

2.根据权利要求1所述的基于网络探针的网络拓扑自动发现方法，其中，所述网络探针可重复多次在网络不同位置进行使用。

一种基于网络探针的网络拓扑自动发现方法

技术领域

[0001] 本发明设计网络管理领域，特别涉及一种基于网络探针对网络拓扑结构进行自动发现的方法。

背景技术

[0002] 随着网络信息时代的不断发展，网络应用在日常生产生活中的日益普及，人们对计算机网络的依赖程度越来越高。网络自身的安生性和可靠性变的尤为重要，特别是例如工业控制这样的特殊应用领域。随着工业控制自动化进程的深入，工业控制网络不断面临着来自外部互联网的恶意攻击和内部人员的误操作等威胁。因为早期工控设备使用环境相对封闭，工控系统缺少对网络安全自身的关注，这导致工业控制系统中存在不可避免的安全缺陷。因此，对与之相关的网络管理系统也提出了越来越高的要求。

[0003] 网络拓扑发现(Network Topology Discovery)是网络管理系统的一个最基本的功能和要求。基于发现的网络拓扑信息，网络管理系统能够快速锁定网络错误，发现网络瓶颈，更好的理解和获取当前网络状态等，从而更好对网络进行管理和优化。网络拓扑发现是指发现网络元素并确定元素之间的互连关系，从而在此基础上绘制出网络拓扑图。其考虑因素包括互连设备(如路由器、网桥、交换机等)、主机和子网。网络拓扑发现主要包含两方面内容：一是发现设备节点的存在；二是确定设备节点的拓扑位置(即节点连接信息)。最初网络OSI结构和TCP/IP进行构建时，并没有将网络拓扑发现作为设计目标，因此目前并没有一个完美的方案可以在无拓扑先验知识的情况下对网络拓扑进行完美的绘制。目前存在的一些解决方法(如802.11ab，LLTD协议等)都存在一些缺陷，例如需要特殊硬件支持等。

发明内容

[0004] 为解决上述现有技术中存在的问题，本发明提出了一种基于网络探针的网络拓扑自动发现方法，其包含以下步骤：

[0005] 步骤一：在所需发现网络中置入网络探针，收集探针上下游数据；

[0006] 步骤二：列出每个探针对网络的划分，采用寻找划分的方法，找到一个对网络的划分；

[0007] 步骤三：采用寻找连接的方法，找到探针与分区的连接关系，从而发现拓扑。

[0008] 进一步地，其中所述寻找划分的方法如下：

[0009] 1)列出对应每个探针的初始划分D_i，i＝1...m(m为探针个数)，令下标k为k+1；其中D_i为探针i对网络节点的划分，即s_i+1个分区所构成的集合。

[0010] 2)取分区$z_k^{(1)}$依次与其它划分的每一个分区，$z_l^{(j)}$(探针j对网络节点划分中的第1个分区)，j≠1进行比较，若$z_k^{(1)} \cap z_l^{(j)} = C \neq \Phi$，且C为$z_k^{(1)}$的真子集，则将原来的一个分区分割成新的两个分区，即

[0011] $$z_k^{(1)} \rightarrow z_k^{(1)} = z_k^{(1)} \setminus C \quad , \quad z_{s_1+1}^{(1)} = C$$

[0012] 并更新下标s_1为s_1+1，令下标k为k－1，跳到第3)步；

[0013] 3)如果k＝s_1，停止，令D＝D_1，输出D所对应的划分，否则，令下标k为k+1，返回第2步。

[0014] 进一步地，其中所述寻找连接基于找到的划分寻找探针与分区之间的连接信息，其具体方法如下：

[0015] 1)列出每个探针的划分{D_i}，i＝1...m；

[0016] 2)遍历{D_i}，若某一个划分D_j中存在与划分D相同的分区，即存在

[0017] $z_k^{(j)} \in D_j$且$z_k^{(j)} \in D$，则探针j与分区$z_k^{(j)}$相连；

[0018] 3)比较任意两个来自属不同探针划分的分区，若两个分区为包含关系且两分区的差集属于D，则此差集与两探针相连，也即或存在$z_k^{(j)} \subset z_l^{(s)}$且$z_l^{(s)} \backslash z_k^{(j)} = C \in D$，则C与探针s和j相连。

[0019] 更进一步地，所述网络探针可重复多次在网络不同位置进行使用，从而可对网络拓扑信息的发现进行逐步细化。

[0020] 本发明所产生的有益效果在于：

[0021] 本发明基于网络探针，通过特定的方法，利用探针所获取的上下游信息，将网络有效的分成若干个区，并得到探针与各分区间的连接关系。从而有助于发现网络拓扑，对网络作进一步优化及提高网络安全性能等。对比现有方法，本发明无需特殊的硬件支持，不需要主动发送数据包去干扰网络，并且可重复利用探针对网络结构进行逐步细化，具有广泛的适用性。

附图说明

[0022] 图1为使用本发明的基于网络探针的网络拓扑自动发现的网络连接图。

具体实施方式

[0023] 下面以简单的网络结构为例对本发明进行详细阐述。应当注意的是，下面的实施例仅用于对本发明进行说明而非作为对本发明的限制。本发明的基于网络探针的网络拓扑自动发现方法除了可以应用在工业网络中，还可以用于任何其它的分布式网络。

[0024] 对于一个含有n个节点的网络，为得到其网络拓扑结构，在网络中放置m个具有监测功能的探针(例如具有TAP功能的路由器等)。每个探针具有一定数目的端口并且可以检测到通过每个端口进行通信的设备信息，例如发送数据包设备的IP地址等。假设所考虑网络是一个无环的连通图，本发明在完全信息的情况下，即每两个网络节点都有通信(例如向全网发送广播)的情况下，综合各个探针所汇报的上下游设备节点信息，对所观察到的节点进行分区，每个区(zone)是一个包含数个节点的集合，然后再绘制出探针与分区间的连接关系，从而发现网络拓扑。

[0025] 首先对网络节点分区的方法进行说明。探针每个端口所获取的信息可将网络节点划分为两个区，因此一个具有s个端口的探针可将网络节点划分为s+1个互不相交的分区，称一个探针对网络节点的分区所构成的集合为一个划分。因此，m个探针对应网络节点的m

个划分。记网络探针i对网络节点的划分为$D_i=\{z_1^{(i)},\cdots,z_{s_i}^{(i)}\}$,其中$z_k$为一个区,是一部分网络节点所构成的集合,$s_i-1$是此探针端口数量,每个探针的划分只反映部分网络拓扑信息,下面的方法可找到一种划分与所有已知划分相一致,即能反映出所有网络结构的信息。寻找划分的方法如下:

[0026] 1.列出对应每个探针的初始划分D_i,i=1...m,令k为k=1;

[0027] 2.取分区$z_k^{(1)}$依次与其它划分的每一个分区$z_l^{(j)}$,$j\neq 1$进行比较,若$z_k^{(1)}\cap z_l^{(j)}=C\neq\Phi$,且C为$z_k^{(1)}$的真子集,则将原来的一个分区分割成新的两个分区,即

[0028] $$z_k^{(1)}\rightarrow z_k^{(1)}=z_k^{(1)}\setminus C\ ,\quad z_{s_1+1}^{(1)}=C$$

[0029] 并更新下标s_1为s_1+1,令下标k为k-1,跳到第3步;

[0030] 3.如果k=s_1,停止,令D=D_1,输出D所对应的划分,否则,令下标k为k+1,返回第2步。

[0031] 下面说明如何基于找到的划分D寻找探针与分区之间的连接信息,从而得到网络拓扑。探针与分区的连接关系是一个二步图,即边只存在于探针和分区之间。寻找连接的具体方法如下:

[0032] 1.列出每个探针的划分{D_i},i=1...m;

[0033] 2.遍历{D_i},若某一个划分D_j中存在与划分D相同的分区,即存在

[0034] $z_k^{(j)}\in D_j$且$z_k^{(j)}\in D$,则探针j与分区$z_k^{(j)}$相连;

[0035] 3.比较任意两个来自属不同探针划分的分区,若两个分区为包含关系且两分区的差集属于D,则此差集与两探针相连,也即或存在$z_k^{(j)}\subset z_l^{(s)}$且$z_l^{(s)}\setminus z_k^{(j)}=C\in D$,则C与探针s和j相连。

[0036] 如图1所示的网络连接图,方框表示网络设备或子网,用大写英文字母进行标记,交叉的圆代表网络探针,用数字进行标记。由图可以看出4个网络探针将整个网络分割成了6个分区,分别为z1=｛F｝、z2=｛A｝、z3=｛D｝、z4=｛B,G,I｝、z5=｛C｝和z6=｛H,E｝。每个探针所探测到的数据如表1所示。

[0037] 表1网络探针数据

[0038]

网络探针	连接端口数	通信数据
1	3	z1-z3, z1-z4, z1-z5, z1-z6, z2-z3, z2-z4, z2-z5, z2-z6, z3-z5, z3-z6, z4-z5, z4-z6
2	2	z1-z2, z1-z3, z1-z4, z1-z5, z1-z6
3	2	z1-z3, z2-z3, z3-z4, z3-z5, z3-z6
4	2	z1-z6, z2-z6, z3-z6, z4-z6, z5-z6

[0039] 各个网络探针根据自己观测到的通信数据汇报自己观察到的各端口分区信息,如表2所示为探针网络划分信息。

[0040] 表2探针网络划分信息

[0041]

网络探针	网络划分
1	AF | BDGI | CEH
2	F | ABCDEGHI
3	D | ABCEFGHI
4	HE | ABCDFGI

[0042] 利用前面所述的寻找划分的方法，可以找到网络的一个划分与所有探针的划分相一致，得到的网络划分为{A}，{B,G,I}，{C}，{D}，{F}，{E,H}，与图1的分区一致。再利用本发明所述的寻找连接的方法，可找到探针与分区之间的连接，如表3所示。

[0043] 表3网络连接

[0044]

网络探针	连接分区
1	{A}，{C}，{B,G,I}
2	{F}，{A}，
3	{B,G,I}，{D}
4	{E,H}，{C}

[0045] 由表3可知，所发现的拓扑连接与图1所示的网络连接图相一致。

[0046] 以上所述实例仅表达了本发明的实施方式，其描述较为具体和详细，但并不能因此而理解为对本发明专利的限制。应该指出的是，对于本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范围。因此，本发明专利的保护范围应以所附权利要求为准。

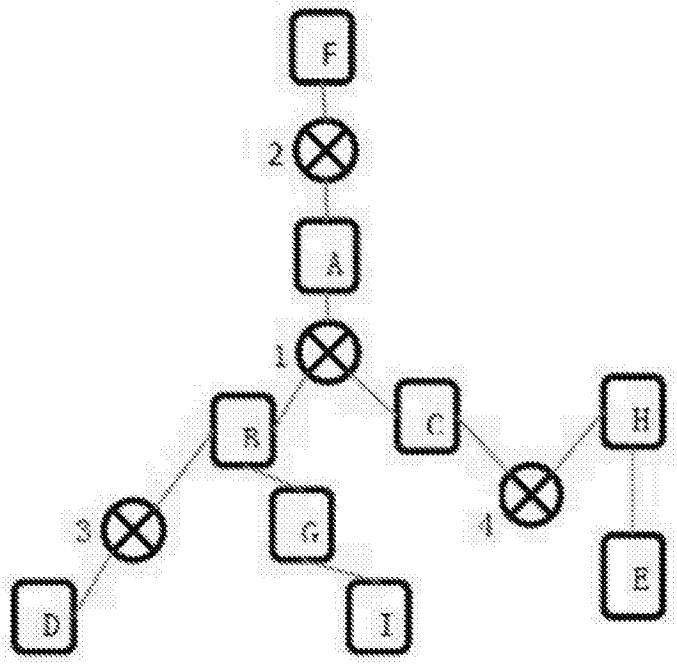


图1