(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112491663 A
(43)申请公布日 2021.03.12

(21)申请号 202011465645.4

(22)申请日 2020.12.13

(71)申请人 北京哈工信息产业股份有限公司
地址 100052 北京市西城区宣武门外28号富卓大厦A座4层

(72)发明人 冷雪飞

(74)专利代理机构 北京挺立专利事务所(普通合伙) 11265
代理人 高福勇

(51)Int.Cl.
H04L 12/26(2006.01)
H04L 29/08(2006.01)

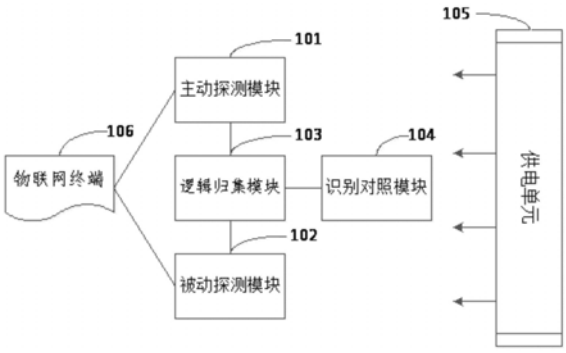
权利要求书3页 说明书7页 附图1页

(54)发明名称

一种探测、识别物联网终端的系统及方法

(57)摘要

本发明一种探测、识别物联网终端的系统及方法，包括：主动探测模块、被动探测模块、逻辑归集模块、识别对照模块以及供电单元；所述主动探测模块的一端与所述逻辑归集模块的一端电连接，所述被动探测模块的一端与所述逻辑归集模块的另一端电连接，所述逻辑归集模块的又一端与所述识别对照模块的一端电连接；采用P0f被动探测结合Nmap主动探测双探测技术，大大增加了对终端的探测精度；通过终端类型字典对同步时钟下的双探测数据进行识别，从而达到高精度的终端识别效果；通过科学的滞后时间函数设计，大大增加了本发明的探测范围以及后期的识别精度，设计简洁，维护方便，适合推广。



CN 112491663 A

1.一种探测、识别物联网终端的系统,其特征在于,包括:主动探测模块、被动探测模块、逻辑归集模块、识别对照模块以及供电单元;所述主动探测模块的一端与所述逻辑归集模块的一端电连接,所述被动探测模块的一端与所述逻辑归集模块的另一端电连接,所述逻辑归集模块的又一端与所述识别对照模块的一端电连接;

所述主动探测模块内置有Nmap软件程序,用于主动扫描物联网终端的身份信息;所述身份信息包括:主机信息、端口信息、操作系统信息以及网络传输信息;

所述被动探测模块内置有POf软件程序,用于被动的探测物联网终端的其他信息;所述其他信息包括:端口信息、数据传输信息以及ISP信息;

所述逻辑归集模块采用逻辑控制算法控制所述主动探测模块与被动探测模块的探测顺序,并对所述主动探测模块与被动探测模块探测的结果采用时间同序算法进行归集,输出各组同时钟状态下的归集结果值;

所述识别对照模块内置有终端类型字典,用于对所述同时钟状态下的归集结果值进行逐一比对分析,得出各组物联网终端的精确识别结果;

所述供电单元用于所述主动探测模块、被动探测模块、逻辑归集模块以及识别对照模块的供电。

2.根据权利要求1所述的一种探测、识别物联网终端的系统,其特征在于,所述识别对照模块可以对每个主动探测模块或被动探测模块的探测信息进行单独比对,输出识别结果。

3.一种探测、识别物联网终端的方法,其特征在于,包括:

步骤一、逻辑归集模块的工作方案:

Ⅰ、本发明一种探测、识别物联网终端的系统并入待识别终端的物联网后,所述逻辑归集模块控制主动探测模块与被动探测模块进行探测、识别操作;

Ⅱ、所述逻辑归集模块控制所述被动探测模块先行探测,得出探测结果B;所述逻辑归集模块将探测结果B中的端口信息Dcc发送给所述主动探测模块,控制所述主动探测模块进行指定端口信息Dcc的主动探测;

Ⅱ、所述被动探测模块得出探测结果B时,逻辑归集模块设定该探测结果时钟点为t,此时所述主动探测模块在时钟t点时同步进行指定端口信息Dcc的主动探测,得出探测结果Z,此时探测结果Z所用时间T,利用滞后时间函数公式可以计算得出;

所述滞后时间函数公式为:

T=t1+max{t2,t3,t4};

进一步的,只有t2,t3,t4的探测结果全部出来,主动探测模块才算探测完成,即探测结果Z所用时间T为:t1与[t2,t3,t4]逻辑比对后的最大值的求和,因Nmap主动探测到端口Dcc时,获取物联网终端的主机信息、网络传输信息和操作系统信息的主动探测操作为同步,故而[t2,t3,t4]的时间值取值最大,即可涵盖另外两个探测所需时间的时间值;

t1时间值的获取方案采用快扫Nmap端口探测报告的方式获得;

t2时间值的获取方案采用快扫Nmap主机探测报告的方式获得;

t3时间值的获取方案采用快扫Nmap网络传输信息探测报告的方式获得;

t4时间值的获取方案采用快扫Nmap操作系统信息探测报告的方式获得;

其中:T为探测结果Z所用时间;t1为主动探测模块探测物联网终端指定端口Dcc所用时

间;t2:为主动探测模块获取物联网终端的主机信息所用时间;t3:为主动探测模块获取物联网终端的网络传输信息所用时间;t4:为主动探测模块获取物联网终端的操作系统信息所用时间;max{}为求取最大值的函数公式;t为所述被动探测模块得出探测结果B时,逻辑归集模块设定该探测结果时钟点为t;

Ⅲ、将所述时钟t与时间段T相加后,可保证基于同一被探测物联网终端的被动探测数据时钟与主动探测数据时钟同步,所述逻辑归集模块归集探测结果B与探测结果Z,形成基于同一时钟下的归集结果值后,传送至识别对照模块进行信息识别;

步骤二、被动探测模块的探测方案:

Ⅰ、端口信息被动探测:POf被动探测连入网络的物联网终端的流量数据,通过对数据的被动识别,得出端口信息Dcc;

所述端口信息的数值可以是多组或者单组,取决于并入物联网待识别终端的数量多少;

Ⅱ、ISP信息被动探测:读取由抓包工具得到的数据包文件,通过POf程序解析,即可求证出ISP信息以及数据传输信息;

步骤三、主动探测模块的探测方案:

Ⅰ、端口信息扫描设定:Nmap主动发射ping命令:探测物联网终端的指定端口;通过命令Nmap done:target Dccaddress from gateway,找到待探测的物联网终端的端口;

Ⅱ、主机信息扫描设定:Nmap通过对端口信息Dcc的主动扫描,获取物联网终端的主机信息;主动发射ping命令:Nmap done:sp<Dcc>;

Ⅲ、网络传输信息扫描设定:Nmap通过对端口信息Dcc的主动扫描,获取物联网终端的网络传输信息;主动发射ping命令:Nmap done:traceroute<Dcc>,

Ⅳ、操作系统信息探测设定:Nmap通过对端口信息Dcc的主动扫描,获取物联网终端的操作系统信息;Nmap主动发射ping命令:Nmap done:O<Dcc>;

步骤四、识别对照模块内置有终端类型字典,所述终端类型字典包括多种主机数据、操作系统数据、网络传输数据以及ISP数据;根据所述同时钟状态下的归集结果值,对所述同时钟状态下的归集结果值进行比对分析,一次比对即可得出准确的终端识别结果。

4.根据权利要求3所述的一种探测、识别物联网终端的方法,其特征在于,所述终端类型字典为开口数据库,可随时进行终端类型字典上传数据补丁或修改数据操作。

5.根据权利要求3所述的一种探测、识别物联网终端的方法,其特征在于,所述t1时间值的获取方案采用快扫Nmap端口探测报告的方式获得,即:

clock<t>Nmap scan report for Dcc

starting Nmap(https://Nmap.org)at<t>CST

If it is really up,blocking our ping probes

Nmap done:DccIP address scanned in“t1”seconds

由此得出t1实际值。

6.根据权利要求3所述的一种探测、识别物联网终端的方法,其特征在于,所述t2时间值的获取方案采用快扫Nmap主机探测报告的方式获得,即:

clock<t>Nmap scan report for sp<Dcc>

starting Nmap(https://Nmap.org)at<t>CST

If it is really up,blocking our ping probes

Nmap done:hosts up scanned in“t2”seconds

由此得出t2实际值。

7.根据权利要求3所述的一种探测、识别物联网终端的方法,其特征在于,所述t3时间值的获取方案采用快扫Nmap网络传输信息探测报告的方式获得,即:

clock<t>Nmap scan report for traceroute<Dcc>

starting Nmap(https://Nmap.org)at<t>CST

If it is really up,blocking our ping probes

Nmap done:net information scanned in“t3”seconds

由此得出t3实际值。

8.根据权利要求3所述的一种探测、识别物联网终端的方法,其特征在于,所述t4时间值的获取方案采用快扫Nmap操作系统信息探测报告的方式获得,即:

clock<t>Nmap scan report for 0<Dcc>

starting Nmap(https://Nmap.org)at<t>CST

If it is really up,blocking our ping probes

Nmap done:0host system scanned in“t4”seconds

由此得出t4实际值。

一种探测、识别物联网终端的系统及方法

技术领域

[0001] 本发明专利涉及探测、识别技术领域，尤其是一种探测、识别物联网终端的系统及方法。

背景技术

[0002] 物联网又称“万物相连的互联网”，是互联网基础上的延伸和扩展的网络，将各种信息传感设备与互联网结合起来而形成的一个巨大网络，实现在任何时间、任何地点，人、机、物的互联互通；

[0003] 物联网是新一代信息技术的重要组成部分，这有两层意思：

[0004] 第一，物联网的核心和基础仍然是互联网，是在互联网基础上的延伸和扩展的网络；

[0005] 第二，其用户端延伸和扩展到了任何物品与物品之间，进行信息交换和通信，按约定的协议，把任何物品与互联网相连接，进行信息交换和通信，以实现对物品的智能化识别、定位、跟踪、监控和管理的一种网络；

[0006] 物联网的应用领域涉及到方方面面，在工业、农业、环境、交通、物流、安保等基础设施领域的应用，有效的推动了这些方面的智能化发展，使得有限的资源更加合理的使用分配，从而提高了行业效率、效益。在家居、医疗健康、教育、金融与服务业、旅游业等与生活息息相关的领域的应用，从服务范围、服务方式到服务的质量等方面都有了极大的改进，大大的提高了人们的生活质量；

[0007] 物联网终端是物联网中连接传感网络层和传输网络层，实现采集数据及向网络层发送数据的设备；它担负着数据采集、初步处理、加密、传输等多种功能；物联网各类终端设备总体上可以分为情景感知层、网络接入层、网络控制层以及应用/业务层；每一层都与网络侧的控制设备有着对应关系。物联网终端常常处于各种异构网络环境中，为了向用户提供最佳的使用体验，终端应当具有感知场景变化的能力，并以此为基础，通过优化判决，为用户选择最佳的服务通道；终端设备通过前端的RF模块或传感器模块等感知环境的变化，经过计算，决策需要采取的应对措施；

[0008] 随着物联网快速的发展，万物互联的时代已经到来，越来越多的物联网终端加入到物联网中，方便了人们的生产与生活，但是过多的物联网终端的加入，大大降低了物联网终端管理的效率，随着物联网终端的多样化，对物联网终端的识别也越发复杂，而现实管理中，又需要对物联网终端所属的类别进行有效的识别；

[0009] 现有技术中，对物联网终端的识别技术存在较多不足，例如：识别类型不够广泛，识别效率较低，识别的准确性不高；而物联网终端身份的正确识别是建立物联网安全连接的重要前提，从物联网安全的角度分析，现有物联网终端的安全管理问题越发突出。

发明内容

[0010] 为了解决上述技术问题，本发明提供一种探测、识别物联网终端的系统及方法，本

发明针对现有技术无法对物联网终端设备进行有效的识别管理缺陷，通过P0f被动探测识别技术并结合Nmap主动探测识别技术，根据探测到的物联网终端的探测信息，比对系统中内置的终端类型字典，通过对照操作，准确的探测和识别了物联网终端。

[0011] 一种探测、识别物联网终端的系统及方法，其中：

[0012] 一种探测、识别物联网终端的系统，包括：主动探测模块、被动探测模块、逻辑归集模块、识别对照模块以及供电单元；

[0013] 进一步的，所述主动探测模块内置有Nmap软件程序，用于主动扫描物联网终端的身份信息；所述身份信息包括：主机信息、端口信息、操作系统信息以及网络传输信息；

[0014] 进一步的，所述被动探测模块内置有P0f软件程序，用于被动的探测物联网终端的其他信息；所述其他信息包括：端口信息、数据传输信息以及ISP信息；

[0015] 进一步的，所述逻辑归集模块采用逻辑控制算法控制所述主动探测模块与被动探测模块的探测顺序，并对所述主动探测模块与被动探测模块探测的结果采用时间同序算法进行归集，输出各组同时钟状态下的归集结果值；

[0016] 作为一种举例说明，所述主动探测模块的探测机理，是规避物联网终端设备的监控软件进行的，其主动探测模式容易引发被探测终端输出的各项数据发生变化，造成所述被动探测模块接收到的探测数据不准确，影响最终的物联网终端识别；

[0017] 进一步的，所述识别对照模块内置有终端类型字典，用于对所述各组同时钟状态下的归集结果值进行逐一比对分析，得出各组物联网终端的精确识别结果；

[0018] 作为一种举例说明，所述识别对照模块可以对每个主动探测模块或被动探测模块的探测信息进行单独比对，输出识别结果；但这种识别结果是基于单个主动或被动探测模块的探测信息进行识别，仅对单组探测数据的识别会造成物联网终端识别的精确度不高，而同时比对主动与被动探测模块的数据，又需要上述两个模块的数据时钟同步，方能得到统一的精确识别结果输出；

[0019] 进一步的，所述供电单元用于所述主动探测模块、被动探测模块、逻辑归集模块以及识别对照模块的供电；所述主动探测模块的一端与所述逻辑归集模块的一端电连接，所述被动探测模块的一端与所述逻辑归集模块的另一端电连接，所述逻辑归集模块的又一端与所述识别对照模块的一端电连接；

[0020] 一种探测、识别物联网终端的方法，包括：

[0021] 步骤一、逻辑归集模块的工作方案：

[0022] Ⅰ、本发明一种探测、识别物联网终端的系统并入待识别终端的物联网后，所述逻辑归集模块控制主动探测模块与被动探测模块进行探测、识别操作；

[0023] Ⅱ、所述逻辑归集模块控制所述被动探测模块先行探测，得出探测结果B；所述逻辑归集模块将探测结果B中的端口信息Dcc发送给所述主动探测模块，控制所述主动探测模块进行指定端口信息Dcc的主动探测；

[0024] Ⅱ、所述被动探测模块得出探测结果B时，逻辑归集模块设定该探测结果时钟点为t，此时所述主动探测模块在时钟t点时同步进行指定端口信息Dcc的主动探测，得出探测结果Z，此时探测结果Z所用时间T，利用滞后时间函数公式可以计算得出；

[0025] 所述滞后时间函数公式为：

[0026] $T=t1+\max\{t2,t3,t4\}$；

[0027] 其中:T为探测结果Z所用时间;t1为主动探测模块探测物联网终端指定端口Dcc所用时间;t2:为主动探测模块获取物联网终端的主机信息所用时间;t3:为主动探测模块获取物联网终端的网络传输信息所用时间;t4:为主动探测模块获取物联网终端的操作系统信息所用时间;max{}为求取最大值的函数公式;t为所述被动探测模块得出探测结果B时,逻辑归集模块设定该探测结果时钟点为t;

[0028] 进一步的,只有t2,t3,t4的探测结果全部出来时,主动探测模块才算探测完成,即探测结果Z所用时间T为:t1与[t2,t3,t4]逻辑比对后的最大值的求和,因Nmap主动探测到端口Dcc时,获取物联网终端的主机信息、网络传输信息和操作系统信息的主动探测操作为同步,故而[t2,t3,t4]的时间值取值最大,即可涵盖另外两个探测所需时间的时间值;所述滞后时间函数公式逻辑设计严谨、简洁,易于实现,算法不复杂,安全性高,维护容易;

[0029] ①t1时间值的获取方案采用快扫Nmap端口探测报告的方式获得,即:

[0030] clock<t>Nmap scan report for Dcc

[0031] starting Nmap(https://Nmap.org)at<t>CST

[0032] If it is really up,blocking our ping probes

[0033] Nmap done:DccIP address scanned in“t1”seconds

[0034] 由此得出t1实际值;

[0035] ②t2时间值的获取方案采用快扫Nmap主机探测报告的方式获得,即:

[0036] clock<t>Nmap scan report for sp<Dcc>

[0037] starting Nmap(https://Nmap.org)at<t>CST

[0038] If it is really up,blocking our ping probes

[0039] Nmap done:hosts up scanned in“t2”seconds

[0040] 由此得出t2实际值;

[0041] ③t3时间值的获取方案采用快扫Nmap网络传输信息探测报告的方式获得,即:

[0042] clock<t>Nmap scan report for traceroute<Dcc>

[0043] starting Nmap(https://Nmap.org)at<t>CST

[0044] If it is really up,blocking our ping probes

[0045] Nmap done:net information scanned in“t3”seconds

[0046] 由此得出t3实际值;

[0047] ④t4时间值的获取方案采用快扫Nmap操作系统信息探测报告的方式获得,即:

[0048] clock<t>Nmap scan report for O<Dcc>

[0049] starting Nmap(https://Nmap.org)at<t>CST

[0050] If it is really up,blocking our ping probes

[0051] Nmap done:Ohost system scanned in“t4”seconds

[0052] 由此得出t4实际值;

[0053] Ⅲ、将所述时钟t与时间段T相加后,可保证基于同一被探测物联网终端的被动探测数据时钟与主动探测数据时钟同步,所述逻辑归集模块归集探测结果B与探测结果Z,形成基于同一时钟下的归集结果值后,传送至识别对照模块进行信息识别;

[0054] 步骤二、被动探测模块的探测方案:

[0055] Ⅰ、端口信息被动探测:P0f被动探测连入网络的物联网终端的流量数据,通过对数

据的被动识别,得出端口信息Dcc;

[0056] 所述端口信息的数值可以是多组或者单组,取决于并入物联网待识别终端的数量多少;

[0057] Ⅱ、ISP信息被动探测:读取由抓包工具得到的数据包文件,通过P0f程序解析,即可求证出ISP信息以及数据传输信息;

[0058] 步骤三、主动探测模块的探测方案:

[0059] Ⅰ、端口信息扫描设定:Nmap主动发射ping命令:探测物联网终端的指定端口;通过命令Nmap done:target Dccaddress from gateway,找到待探测的物联网终端的端口;

[0060] Ⅱ、主机信息扫描设定:Nmap通过对端口信息Dcc的主动扫描,获取物联网终端的主机信息;主动发射ping命令:Nmap done:sp<Dcc>;

[0061] Ⅲ、网络传输信息扫描设定:Nmap通过对端口信息Dcc的主动扫描,获取物联网终端的网络传输信息;主动发射ping命令:Nmap done:traceroute<Dcc>,

[0062] Ⅳ、操作系统信息探测设定:Nmap通过对端口信息Dcc的主动扫描,获取物联网终端的操作系统信息;Nmap主动发射ping命令:Nmap done:O<Dcc>;

[0063] 步骤四、识别对照模块内置有终端类型字典,所述终端类型字典包括多种主机数据、操作系统数据、网络传输数据以及ISP数据;根据所述同时钟状态下的归集结果值,对所述同时钟状态下的归集结果值进行比对分析,一次比对即可得出准确的终端识别结果;

[0064] 作为一种举例说明,所述终端类型字典为开口数据库,可随时进行终端类型字典上传数据补丁或修改数据操作;

[0065] 有益效果:

[0066] 1、本发明针对现有物联网终端设备探测、识别管理手段单一,探测、识别精度低的不足,采用P0f被动探测结合Nmap主动探测双探测技术,大大增加了对终端的探测精度;

[0067] 2、通过终端类型字典对同步时钟下的双探测数据进行识别,从而达到高精度的终端识别效果,又不产生主动探测技术影响被动探测数据准确性的缺陷;

[0068] 3、通过科学的滞后时间函数设计,大大增加了本发明的探测范围以及后期的识别精度,设计简洁,维护方便,适合推广。

附图说明

[0069] 图1是本发明一种探测、识别物联网终端的系统的整体结构示意图

具体实施方式

[0070] 下面,参考附图1所示,一种探测、识别物联网终端的系统及方法,其中:

[0071] 一种探测、识别物联网终端的系统,包括:主动探测模块101、被动探测模块102、逻辑归集模块103、识别对照模块104以及供电单元105;

[0072] 进一步的,所述主动探测模块101内置有Nmap软件程序,用于主动扫描物联网终端106的身份信息;所述身份信息包括:主机信息、端口信息、操作系统信息以及网络传输信息;

[0073] 进一步的,所述被动探测模块102内置有P0f软件程序,用于被动的探测物联网终端106的其他信息;

[0074] 作为一种举例说明,所述其他信息包括:端口信息、数据传输信息以及ISP信息;

[0075] 进一步的,所述逻辑归集模块103采用逻辑控制算法控制所述主动探测模块101与被动探测模块102的探测顺序,并对所述主动探测模块101与被动探测模块102探测的结果采用时间同序算法进行归集,输出各组同时钟状态下的归集结果值;

[0076] 作为一种举例说明,所述主动探测模块101的探测机理,是规避物联网终端设备的监控软件进行的,其主动探测模式容易引发被探测终端输出的各项数据发生变化,造成所述被动探测模块102接收到的探测数据不准确,影响最终的物联网终端识别;

[0077] 进一步的,所述识别对照模块104内置有终端类型字典,用于对所述同时钟状态下的归集结果值进行逐一比对分析,得出各组物联网终端的精确识别结果;

[0078] 作为一种举例说明,所述识别对照模块104可以对每个主动探测模块101或被动探测模块102的探测信息进行单独比对,输出识别结果,但这种识别结果是基于单个主动或被动探测模块的探测信息进行识别,对单组探测数据的识别会造成物联网终端106识别的精确度不高,而同时比对主动与被动探测模块的数据,又需要上述两个模块的数据时钟同步,方能得到统一的精确识别结果输出;

[0079] 进一步的,所述供电单元105用于所述主动探测模块101、被动探测模块102、逻辑归集模块103以及识别对照模块104的供电;所述主动探测模块101的一端与所述逻辑归集模块103的一端电连接,所述被动探测模块102的一端与所述逻辑归集模块103的另一端电连接,所述逻辑归集模块103的又一端与所述识别对照模块104的一端电连接;

[0080] 一种探测、识别物联网终端的方法,包括:

[0081] 步骤一、逻辑归集模块的工作方案:

[0082] Ⅰ、本发明一种探测、识别物联网终端的系统并入待识别终端的物联网后,所述逻辑归集模块103控制主动探测模块101与被动探测模块102进行探测、识别操作;

[0083] Ⅱ、所述逻辑归集模块103控制所述被动探测模块102先行探测,得出探测结果B;所述逻辑归集模块103将探测结果B中的端口信息Dcc发送给所述主动探测模块101,控制所述主动探测模块101进行指定端口信息Dcc的主动探测;

[0084] Ⅱ、所述被动探测模块102得出探测结果B时,逻辑归集模块103设定该探测结果时钟点为t,此时所述主动探测模块101在时钟t点时同步进行指定端口信息Dcc的主动探测,得出探测结果Z,此时探测结果Z所用时间T,利用滞后时间函数公式可以计算得出;

[0085] 所述滞后时间函数公式为:

[0086] T=t1+max{t2,t3,t4};

[0087] 进一步的,只有t2,t3,t4的探测结果全部出来,主动探测模块101才算探测完成,即探测结果Z所用时间T为:t1与[t2,t3,t4]逻辑比对后的最大值的求和,因Nmap主动探测到端口Dcc时,获取物联网终端的主机信息、网络传输信息和操作系统信息的主动探测操作为同步,故而[t2,t3,t4]的时间值取值最大,即可涵盖另外两个探测所需时间的时间值;

[0088] ①t1时间值的获取方案采用快扫Nmap端口探测报告的方式获得,即:

[0089] clock<t>Nmap scan report for Dcc

[0090] starting Nmap(https://Nmap.org)at<t>CST

[0091] If it is really up,blocking our ping probes

[0092] Nmap done:DccIP address scanned in“t1”seconds

[0093] 由此得出t1实际值；

[0094] ②t2时间值的获取方案采用快扫Nmap主机探测报告的方式获得，即：

[0095] clock<t>Nmap scan report for sp<Dcc>

[0096] starting Nmap(https://Nmap.org)at<t>CST

[0097] If it is really up,blocking our ping probes

[0098] Nmap done:hosts up scanned in“t2”seconds

[0099] 由此得出t2实际值；

[0100] ③t3时间值的获取方案采用快扫Nmap网络传输信息探测报告的方式获得，即：

[0101] clock<t>Nmap scan report for traceroute<Dcc>

[0102] starting Nmap(https://Nmap.org)at<t>CST

[0103] If it is really up,blocking our ping probes

[0104] Nmap done:net information scanned in“t3”seconds

[0105] 由此得出t3实际值；

[0106] ④t4时间值的获取方案采用快扫Nmap操作系统信息探测报告的方式获得，即：

[0107] clock<t>Nmap scan report for O<Dcc>

[0108] starting Nmap(https://Nmap.org)at<t>CST

[0109] If it is really up,blocking our ping probes

[0110] Nmap done:Ohost system scanned in“t4”seconds

[0111] 由此得出t4实际值；

[0112] 其中：T为探测结果Z所用时间；t1为主动探测模块101探测物联网终端指定端口Dcc所用时间；t2：为主动探测模块101获取物联网终端的主机信息所用时间；t3：为主动探测模块101获取物联网终端的网络传输信息所用时间；t4：为主动探测模块101获取物联网终端的操作系统信息所用时间；max{}为求取最大值的函数公式；t为所述被动探测模块102得出探测结果B时，逻辑归集模块103设定该探测结果时钟点为t；

[0113] Ⅲ、将所述时钟t与时间段T相加后，可保证基于同一被探测物联网终端的被动探测数据时钟与主动探测数据时钟同步，所述逻辑归集模块103归集探测结果B与探测结果Z，形成基于同一时钟下的归集结果值后，传送至识别对照模块104进行信息识别；

[0114] 步骤二、被动探测模块102的探测方案：

[0115] Ⅰ、端口信息被动探测：P0f被动探测连入网络的物联网终端的流量数据，通过对数据的被动识别，得出端口信息Dcc；

[0116] 所述端口信息的数值可以是多组或者单组，取决于并入物联网待识别终端的数量多少；

[0117] Ⅱ、ISP信息被动探测：读取由抓包工具得到的数据包文件，通过P0f程序解析，即可求证出ISP信息以及数据传输信息；

[0118] 步骤三、主动探测模块101的探测方案：

[0119] Ⅰ、端口信息扫描设定：Nmap主动发射ping命令：探测物联网终端的指定端口；通过命令Nmap done:target Dccaddress from gateway，找到待探测的物联网终端的端口；

[0120] Ⅱ、主机信息扫描设定：Nmap通过对端口信息Dcc的主动扫描，获取物联网终端的主机信息；主动发射ping命令:Nmap done:sp<Dcc>；

[0121] Ⅲ、网络传输信息扫描设定:Nmap通过对端口信息Dcc的主动扫描,获取物联网终端的网络传输信息;主动发射ping命令:Nmap done:traceroute<Dcc>,

[0122] Ⅳ、操作系统信息探测设定:Nmap通过对端口信息Dcc的主动扫描,获取物联网终端的操作系统信息;Nmap主动发射ping命令:Nmap done:O<Dcc>;

[0123] 步骤四、识别对照模块104内置有终端类型字典,所述终端类型字典包括多种主机数据、操作系统数据、网络传输数据以及ISP数据;根据所述同时钟状态下的归集结果值,对所述同时钟状态下的归集结果值进行比对分析,一次比对即可得出准确的终端识别结果;

[0124] 作为一种举例说明,所述终端类型字典为开口数据库,可随时进行终端类型字典上传数据补丁或修改数据操作;

[0125] 本发明针对现有物联网终端设备探测、识别管理手段单一,探测、识别精度低的不足,采用POf被动探测结合Nmap主动探测双探测技术,大大增加了对终端的探测精度;通过终端类型字典对同步时钟下的双探测数据进行识别,从而达到高精度的终端识别效果;通过科学的滞后时间函数设计,大大增加了本发明的探测范围以及后期的识别精度,设计简洁,维护方便,适合推广。

[0126] 以上公开的仅为本申请的一个具体实施例,但本申请并非局限于此,任何本领域的技术人员能思之的变化,都应落在本申请的保护范围内。

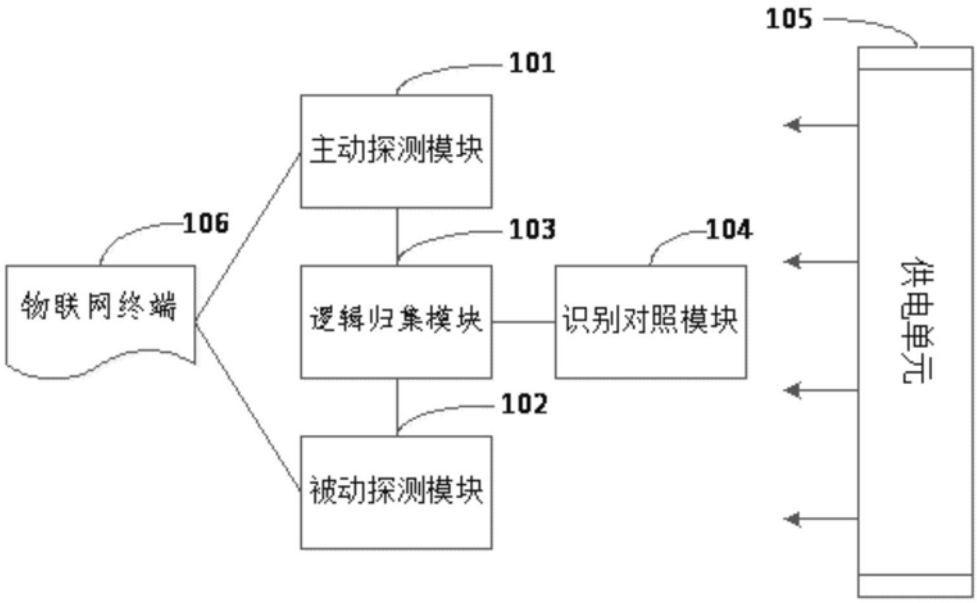

105
101
主动探测模块
106
103
104
物联网终端
逻辑归集模块
识别对照模块
供电单元
102
被动探测模块

图1