(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2019 年 10 月 24 日 (24.10.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/200944 A1

(51) 国际专利分类号:
G06F 21/85 (2013.01)

(21) 国际申请号: PCT/CN2018/120178

(22) 国际申请日: 2019 年 1 月 22 日 (22.01.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810361229.6 2018年4月20日 (20.04.2018) CN

(71) 申请人: 西安交通大学 (XI'AN JIAOTONG UNIVERSITY) [CN/CN]; 中国陕西省西安市咸宁西路28号, Shaanxi 710049 (CN)。

(72) 发明人: 刘烃 (LIU, Ting); 中国陕西省西安市咸宁路28号, Shaanxi 710049 (CN)。 刘鹏飞 (LIU, Pengfei); 中国陕西省西安市咸宁路28号, Shaanxi 710049 (CN)。 王稼舟 (WANG, Jiazhou); 中国陕西省西安市咸宁路28号, Shaanxi 710049 (CN)。 周亚东 (ZHOU, Yadong); 中国陕西省西安市咸宁路28号, Shaanxi 710049 (CN)。

(74) 代理人: 西安通大专利代理有限责任公司 (XI'AN TONG DA PATENT AGENCY CO., LTD.); 中国陕西省西安市咸宁路28号, Shaanxi 710049 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,

(54) **Title:** PHYSICAL INTRUSION ATTACK DETECTION METHOD FOR INDUSTRIAL CONTROL SYSTEM BASED ON SERIAL COMMUNICATION BUS SIGNAL ANALYSIS

(54) **发明名称:** 基于串行通信总线信号分析的工控系统物理入侵攻击检测方法

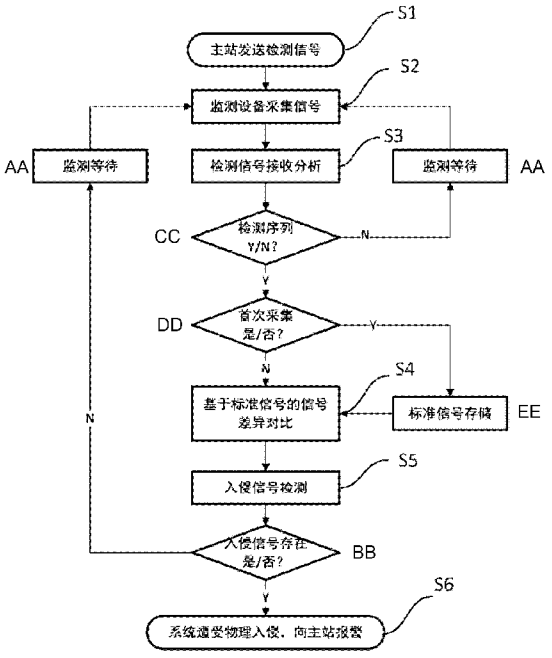

图 6

S1 A MAIN STATION SENDS A DETECTION SIGNAL
S2 A MONITORING DEVICE ACQUIRES SIGNALS
S3 RECEIVE AND ANALYZE THE DETECTION SIGNAL
S4 SIGNAL DIFFERENCE COMPARISON BASED ON A STANDARD SIGNAL
S5 DETECT AN INTRUSION SIGNAL
S6 WHEN A SYSTEM IS SUBJECTED TO A PHYSICAL INTRUSION, RAISE AN ALARM ON THE MAIN STATION
AA WAIT TO PERFORM MONITORING
BB DOES AN INTRUSION SIGNAL EXIST?
CC DETECT A SEQUENCE?
DD IS IT THE FIRST ACQUISITION?
EE STORE THE STANDARD SIGNAL

(57) **Abstract:** Provided is a physical intrusion attack detection method for an industrial control system based on serial communication bus signal analysis. A detection signal is actively sent to a communication bus by means of a bus controller. After a monitoring device carries out sampling and analysis on signals of the communication bus, differential comparison is performed on the signals with a standard signal stored in a device database, and noise reduction technology and weak signal detection technology are used to detect an

WO 2019/200944 A1

[见续页]

MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

intrusion signal in difference signals. According to a detection result of an intrusion signal caused by a physical intrusion device, any external malicious device in a system can be quickly and effectively determined, and the security state regarding whether the system is subjected to a physical intrusion attack is determined. The technical problem that the network security of a serial communication bus of an industrial control system attacked by a physical intrusion cannot be effectively detected by an existing network defense method is solved.

(57) 摘要: 一种基于串行通信总线信号分析的工控系统物理入侵攻击检测方法，通过总线控制器主动向通信总线中发送检测信号，监测设备对通信总线进行信号的采样分析后，与设备数据库中存储的标准信号进行差分对比，并利用降噪技术、弱信号检测技术在差异信号中进行入侵信号的检测，根据由物理入侵设备所引起的入侵信号的检测结果，能快速、有效地判断出系统中是否存在外部恶意设备，确定系统是否遭受物理入侵攻击的安全状态，解决了现有利用网络防御方法无法有效检测物理入侵攻击的工控系统串行通信总线网络的安全性技术问题。

基于串行通信总线信号分析的工控系统物理入侵攻击检测方法

技术领域

本发明属于工业控制系统攻击检测技术领域，特别涉及一种基于串行通信总线信号分析的工控系统物理入侵攻击检测方法。

背景技术

工业控制系统是应用于电力、工业生产、交通、加工制造等领域的自动化控制系统，该系统主要依靠控制中心对各层级网络中设备的运行状态进行监测，并对现场采集到的物理量测数据进行处理分析，从而维持系统的稳定和安全。随着通信技术的发展和信息网络的融合，各领域间工控系统的级联关系使得其整体变得日益庞大和复杂，在工控系统从集中式控制到分布式控制的转变过程中，虽然提升了系统整体的控制效率和响应速度，但却降低了控制中心对处于底层或边缘的总线级网络的安全监管能力。尤其是对于处于无人监守场所中的工业基础设施，更无法保证设备本身的安全性。

2017 年，美国塔尔萨大学的 Staggs 博士及其团队公布了一种针对风电场的攻击“Windshark”，他们通过撬开风力发电设备的服务器机柜，在其中物理接入了通信设备，从而实现对风电场内部系统的控制和恶意操作，对风电场内的涡轮机和自动化控制器都造成了损坏。从这一案例中可以看出，当前大多数的工业控制系统都无法很好地防护物理式入侵攻击，攻击者甚至可以很轻易的在工控系统终端的串行通信总线网络内物理接入通信设备，利用接入设备篡改通信总线上的通信信号，亦或是伪造恶意指令、数据发送到串行通信总线上，造成串行通信总线网络中设备工作的异常，甚至扰乱系统的稳定运行，这对于工控系统来说是极大地威胁。

在传统的工控系统中，对于常见的网络入侵式攻击，已经有很多安全防御方法的研究，

例如通过网络通信加密算法来保证信息安全，通过流量监测来防止恶意数据注入，通过入侵检测系统来识别恶意攻击行为等，然而上述方法在工控系统的物理入侵攻击面前却很难适用。一方面，工控系统的串行总线通信网络缺乏安全保障，在遭受物理入侵之后没有很有效的方法去检测系统中是否存在外部设备，在通信时又缺乏相应的身份认证机制；另一方面，在串行通信总线网络中，由于工业设备通信的实时性要求，以及设备本身的弱计算能力，串行通信总线协议中很难依靠设计完善的加密算法来保证信息可靠，且这些协议在设计之初都是对外界公开的，攻击者很容易利用这些协议截获信息或是伪造指令。以上两点都说明，工控系统串行通信总线网络存在物理入侵的安全隐患，同时又很难对入侵系统的外接设备进行检测，这将会给工控系统的稳定运行造成极大的不良影响。

发明内容

本发明的目的在于提供一种基于串行通信总线信号分析的工控系统物理入侵攻击检测方法，用于防止工控系统可能面临的物理入侵攻击威胁，并能有效解决在工控系统串行通信总线网络中利用传统的网络入侵防御方法不能有效检测系统中存在的恶意外接设备的安全问题。

为了实现上述目的，本发明采用如下技术方案：

基于串行通信总线信号分析的工控系统物理入侵攻击检测方法，包括：通过串行通信总线网络中的总线控制器主动向通信总线中发送检测信号，监测设备对通信总线进行信号的采样分析后，与设备数据库中存储的标准信号进行差分对比，并利用降噪技术、弱信号检测技术在差异信号中进行入侵信号的检测，根据由物理入侵设备所引起的入侵信号的检测结果，有效地判断出系统中是否存在外部恶意设备，确定系统是否遭受物理入侵攻击。

进一步的，具体包括以下步骤：

S1：串行通信总线网络中的总线控制器按照设定的时间周期监听工控系统中串行通信总

线的使用情况：

若通信总线处于空闲状态，则由总线控制器发送一次检测信号；

若通信总线处于数据传输状态，则控制器继续监听等待，直到通信总线处于空闲状态时，由总线控制器发送一次检测信号；

S2：工控系统中部署的监测设备对串行通信总线上所有的通信信号进行采样接收和协议解析；

S3：监测设备对解析后的接收信号进行分析，判断是否开始执行工控系统串行通信总线网络的物理入侵攻击检测；

S4：将接收到的信号数据与监测设备信号数据库中的标准信号数据进行差分对比，得到两个信号之间的差异信号；

S5：对差异信号进行入侵信号检测，若在差异信号中检测出入侵信号，则判断此时工控系统串行通信总线网络中已遭受物理入侵攻击，继续执行 S6；若在差异信号中没有检测出入侵信号，则判断此时工控系统串行通信总线网络没有受到物理入侵攻击，监测设备继续监听总线接收下一次通信信号；

S6：根据入侵信号的检测结果，若工控系统串行通信总线网络中遭受物理入侵攻击，则将检测结果上报给串行通信总线网络中的总线控制器，总线控制器对物理入侵攻击作出快速判断和应急响应。

进一步的，步骤 S1 中，检测信号根据串行通信总线的协议规范设定，并且检测信号在数字序列上有别于所有正常的通信信号，检测信号只能被串行通信总线网络中相应的监测设备进行识别和解析，其他设备不会对检测信号作出响应。

进一步的，步骤 S2 具体为：

根据工控系统中串行通信总线类型，采用对应的 Modbus 协议、CANBus 协议、P-Net

协议、ProfiBus 协议、WorldFIP 协议、ControlNet 协议、FF 协议或 HART 协议对通信信号进行协议解析，得到数字信号序列。

进一步的，步骤 S3 具体包括：

S301：将步骤 S2 所解析得到的数字信号序列与检测信号的数字序列进行一致性检测，若接收到的信号是检测信号，则开始进行工控系统串行通信总线网络物理入侵攻击的检测，执行步骤 S302；若接收到的信号不是检测信号，则不作任何响应，继续监听总线接收下一次通信信号；

S302：根据接收信号与检测信号一致的检测结果，继续判断监测设备是否第一次接收到检测信号，若监测设备的信号数据库为空，则将接收到的信号数据存储在本地数据库中，并认为此信号是系统正常情况下的标准信号；若监测设备的信号数据库中已存储有信号数据，则继续执行步骤 S4。

进一步的，步骤 S5 中，入侵信号是由于物理入侵攻击所引起的在总线控制器发送的原有检测信号上增加的确知信号，入侵信号具有与检测信号相同的周期。

进一步的，步骤 S5 具体包括：

S501：对步骤 S4 获得的差异信号数据进行降噪处理；

S502：利用弱信号检测技术，对差异信号中可能存在的入侵信号进行检测，根据弱信号检测的结果判断入侵信号是否存在。

进一步的，还包括以下步骤：总线控制器收到物理入侵攻击的检测信号后，向主站报警。

相对于现有技术，本发明具有以下有益效果：

本发明提供的一种基于串行通信总线信号分析的工控系统物理入侵攻击检测方法，通过监测设备对串行通信总线信号采样分析后，与设备信号数据库中存储的标准信号进行差分对比，并利用降噪技术、弱信号检测技术在差异信号中进行入侵信号的检测，根据由物理入侵

设备所引起的入侵信号的检测结果，能快速、有效地判断出系统中是否存在外部恶意设备，确定系统是否遭受物理入侵攻击的安全状态，解决了现有利用网络防御方法无法有效检测物理入侵攻击的工控系统串行通信总线网络的安全性技术问题。

此外，本发明利用工控系统串行通信总线网络中的总线控制器发送检测信号，再利用部署在网络中的监测设备对信号进行采样接收、差分对比分析以及信号检测，既不会增加原有通信设备的改造成本，也不会破坏原有通信网络的连接结构。

本发明的检测信号是根据工控系统串行通信总线类型以及协议来设定的，而且检测信号在数字序列上与所有正常的通信信号均不相同，且只有在串行通信总线空闲时发送检测信号，既不会影响通信设备间的正常通信，也不会因为其他设备接收检测信号而作出异常响应导致系统紊乱。

本发明中监测设备在接收到信号后，首先进行接收信号序列与检测信号序列一致性检测，在检测结果不一致情况下继续监听，以及在入侵检测结果中未发现入侵信号后监测设备转为继续监听状态，都可进一步减小工控系统串行通信总线物理入侵攻击的检测时间和资源，提升整体检测方法应用的快速性和高效性。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍。

图 1 为工控系统 RS485 通信总线网络结构图；

图 2 为工控系统 RS485 通信总线网络的等效模型图；

图 3 为工控系统 RS485 通信总线网络的稳态模型图；

图 4 为监测设备对差异信号数字平均法降噪处理图；其中，图 4（a）为带有噪声的差异信号，图 4（b）为数字平均处理后的差异信号；

图 5 为监测设备对差异信号中入侵信号互相关检测结果图；其中，图 5（a）为有入侵的检测结果，图 5（b）为无入侵的检测结果；

图 6 为本发明的流程图。

具体实施方式

本发明实施例提供了一种基于串行通信总线信号分析的工控系统物理入侵攻击检测方法，解决了现有利用网络防御方法无法有效检测物理入侵攻击的工控系统串行通信总线网络的安全性技术问题。

为使得本发明的发明目的、特征、优点能够更加的明显和易懂，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。本发明实施例提供的一种基于串行通信总线信号分析的工控系统物理入侵攻击检测方法的一个应用例的攻击情景，为在工控系统 RS485 总线网络中，攻击者通过物理入侵方式在系统中植入外接设备，利用该设备获取通信信息并伪造控制指令，危及系统安全和稳定，通过以下案例具体分析。

图 1 为工控系统 RS485 通信总线 1 的网络结构图，该系统主要由总线控制器 2 和各类通信设备如量测设备 3、控制设备 4 组成，所有设备都以菊花链式的结构挂接在 RS485 总线之上；所有设备连接电力传输线的火线 L、零线 N 和接地线 E。在所有设备中，只有控制器有权限向总线上发送信号，根据 RS485 平衡发送、差分接收的通信模式，两条信号线中的信号为相反信号，其他设备以两个信号的差值作为接收信号，并根据协议以及地址对信号过滤或响应。

图 2 为工控系统 RS485 通信总线网络的等效模型图，在该模型中控制器等效为两个同步的相反信号源，其他通信设备均看作定值输入阻抗，传输线末端还跨接用以消除反射的匹配电阻。当系统遭受攻击者的物理入侵攻击后，攻击者在原系统中接入的一个外接设备也被看作模型中的输入阻抗。为了更好地反应出系统通信稳态情况下的信号波形，工控系统 RS485

通信总线网络的稳态模型图如图 3 所示。

在稳态模型中，传输线也进一步等效为具有定值的稳态阻抗，该稳态阻抗有别于传输线路在瞬态情况下的特性阻抗，因为传输线中的电容电感在稳态情况下不再对信号产生影响，稳态阻抗只与传输线本身的电阻和其长度、粗细、材质等固有参数有关。如图 3 所示，$Z_i(i=1,2,...,n)$ 表示第 i 个设备的输入阻抗，Z_M 是消除信号反射的终端匹配电阻，Z_r 是信号源内阻，而 $Z^l_{i\_i+1}(i=0,1,...,n-1)$ 表示系统稳态情况下第 i 个设备到第 $i+1$ 个设备之间传输线路的等效阻抗，其中当 $i=0$ 时视为信号源位置。攻击者通过物理入侵在系统中插入的外接设备的输入阻抗记为 Z_A。

因此，暂不考虑攻击者在系统中插入的外接设备的情况下，在计算图 3 稳态模型的系统阻抗时，需要经过以下两个迭代过程：

1) 赋初值 $r_0 = Z_r$，计算 Z_M 后项阻抗：

$$r_i = \frac{Z_i \cdot (Z^l_{i-1\_i} + r_{i-1})}{Z_i + Z^l_{i-1\_i} + r_{i-1}}, i = 1,2,....,n$$

2) 用上述迭代结果 r_n 计算 Z_M 前项阻抗：

$$r_{n+1} = \frac{Z_n \cdot (Z_0 + r_n)}{Z_n + Z_0 + r_n}$$

$$r_i = \frac{Z_{2n-i+1} \cdot (Z^l_{2n-i+1\_2n-i+2} + r_{i-1})}{Z_{2n-i+1} + Z^l_{2n-i+1\_2n-i+2} + r_{i-1}}, i = n+2,....,2n$$

而当攻击者通过物理入侵将一个外接设备接入系统中时，假设外接设备的接入位置位于第 k 个设备和第 $k+1$ 个设备之间，那么在上述阻抗迭代计算的过程中，将会发生如下两个变化：

1) 计算 $r_k \to r_{k+1}$ 时：

$$r_x = \frac{Z_A \cdot (\eta Z^l_{k\_k+1} + r_k)}{Z_A + \eta Z^l_{k\_k+1} + r_k}$$

$$r_{k+1} = \frac{Z_{k+1} \cdot [(1-\eta) Z^l_{k\_k+1} + r_x]}{Z_{k+1} + (1-\eta) Z^l_{k\_k+1} + r_x}$$

2) 计算 $r_{2n-k} \to r_{2n-k+1}$ 时：

$$r_y = \frac{Z_A \cdot [(1-\eta) Z^l_{k\_k+1} + r_{2n-k}]}{Z_A + (1-\eta) Z^l_{k\_k+1} + r_{2n-k}}$$

$$r_{2n-k+1} = \frac{Z_{k+1} \cdot (\eta Z^l_{k\_k+1} + r_y)}{Z_{k+1} + \eta Z^l_{k\_k+1} + r_y}$$

针对此类攻击情况，结合图 3 和上述系统阻抗的推导，具体说明本发明中的一种基于串行通信总线信号分析的工控系统物理入侵攻击检测方法，其包括以下步骤：

当系统初次使用本发明的物理入侵攻击检测方法时，具体执行过程以及步骤如下：

步骤 S1：RS485 通信总线网络中的总线控制器监听总线使用状态，当检测到总线处于空闲状态时，向 RS485 两条信号线发送检测信号 $U(t)$ 以及根据 RS485 平衡发送模式对检测信号作相反处理后的信号 $-U(t)$，检测信号是周期为 200μs、幅值为-5V~5V 的方波信号；

步骤 S2：部署在 RS485 通信总线网络中的监测设备对总线上出现的信号进行采集，根据图 3 的稳态模型，假设系统中第 m 个位置的设备是监测设备，那么在总线控制器发出检测信号 $U(t)$ 的情况下，监测设备所采集到的两条信号线的差分信号为：

$$V_{diff}(m,t) = 2(\rho_m - \mu_m)U(t) + \upsilon(t)$$

其中 $\upsilon(t)$ 是环境噪声和量测噪声的总和，ρ_m 和 μ_m 是第 m 个监测设备处的电压信号分配系数：

$$\rho_m = \frac{\prod_{j=1}^{m} r_{2n-j+1}}{(r_{2n} + Z_r + Z_{0\_1}^{l}) \prod_{j=2}^{m} (r_{2n-j+1} + Z_{j-1\_j}^{l})}$$

$$\mu_m = \rho_m \cdot \frac{\prod_{j=m}^{n} r_j}{(r_n + Z_M) \prod_{j=m}^{n-1} (r_j + Z_{j\_j+1}^{l})}$$

然后监测设备会根据 RS485 常用协议—ModBus 协议对信号进行解析，得到相应的数字信号序列；

步骤 S3：监测设备对解析后的信号进行分析处理，具体包括以下步骤：

步骤 S301：将收到信号对应的数字序列与检测信号的数字序列进行一致性检测，如果二者不一致，这说明此信号并非用以执行物理入侵攻击检测的检测信号，监测设备继续保持监听状态；如果二者一致，这说明收到检测信号，转为执行步骤 S302；

步骤 S302：监测设备判断检测信号是否为首次收到，经过对设备本地信号数据库的检测发现，数据库中并无数据，则判断此时的检测信号为系统初始状态下的标准信号，将标准信号的数据存储到信号数据库中，并结束本次物理入侵攻击检测过程。

当系统非初次使用本发明的物理入侵攻击检测方法时，具体执行过程以及步骤如下：

步骤 S1：当 RS485 总线处于空闲状态时，总线控制器向 RS485 两条信号线发送检测信号 $U(t)$ 以及根据 RS485 平衡发送模式对检测信号作相反处理后的信号 $-U(t)$；

步骤 S2：监测设备对总线上出现的信号进行采集，根据图 3 的稳态模型，当攻击者通过物理入侵在系统接入了外部设备后，在相同检测信号的情况下，监测设备所采集到的信号变为：

$$V'_{diff}(m,t) = 2(\rho'_m - \mu'_m)U(t) + \omega(t)$$

其中 $\omega(t)$ 是环境噪声和量测噪声的总和，ρ'_m 和 μ'_m 变为以下两种情况：

1) 若第$k+1$个设备在第 m 个设备之前，则：

$$\rho'_m = \rho_m \cdot \frac{r_y(r_{2n-k} + Z^l_{k\_k+1})}{(r_y + \eta Z^l_{k\_k+1})[r_{2n-k} + (1-\eta)Z^l_{k\_k+1}]}$$

$$\mu'_m = \mu_m \cdot \frac{r_x(r_k + Z^l_{k\_k+1})}{[r_x + (1-\eta)Z^l_{k\_k+1}](r_k + \eta Z^l_{k\_k+1})}$$

2) 若第k个设备在第 m 个设备之后，则：

$$\rho'_m = \rho_m$$

$$\mu'_m = \mu_m \cdot \frac{r_y(r_{2n-k} + Z^l_{k\_k+1})}{(r_y + \eta Z^l_{k\_k+1})[r_{2n-k} + (1-\eta)Z^l_{k\_k+1}]} \cdot \frac{r_x(r_k + Z^l_{k\_k+1})}{[r_x + (1-\eta)Z^l_{k\_k+1}](r_k + \eta Z^l_{k\_k+1})}$$

然后监测设备根据 RS485 常用协议—ModBus 协议对信号进行解析，得到相应的数字信号序列；

步骤 S3：监测设备对解析后的信号进行分析处理，具体包括以下步骤：

步骤 S301：将收到信号对应的数字序列与检测信号的数字序列进行一致性检测，如果二者不一致，这说明此信号并非用以执行物理入侵攻击检测的检测信号，监测设备继续保持监听状态；如果二者一致，这说明收到检测信号，转为执行步骤 S302；

步骤 S302：监测设备判断检测信号是否为首次收到，经过对设备本地信号数据库的检测发现，数据库中已经存储有标准信号，则继续执行物理入侵攻击检测过程，转为执行步骤 S4；

步骤 S4：将接收到的检测信号数据与监测设备信号数据库中的标准信号数据进行差分对比，得到两个信号之间的差异信号；

若系统并未受到攻击者的物理入侵攻击，即无外接设备，那么差分信号的结果应为：

$$\Delta V_{diff}(m,t) = \upsilon(t) - \omega(t)$$

若系统遭受攻击者的物理入侵攻击，系统中存在外接设备，那么差分信号的结果应为：

$$\Delta V_{diff}(m,t) = \delta(t) + \upsilon(t) - \omega(t)$$
$$\delta(t) = 2[(\rho_m - \rho'_m) - (\mu_m - \mu'_m)]U(t)$$

其中$\delta(t)$就是由于外接设备所引起的入侵信号；

步骤 S5：对差异信号进行入侵信号检测，其检测方法与步骤具体包括：

步骤 S501：对差异信号数据进行降噪处理；在本实施例中采用数字平均法提高差异信号的信噪比，并利用 MATLAB 软件对监测设备上的差异信号降噪处理进行了仿真，图 4 为差异信号数字平均法降噪处理图，从图中可以看出，数字平均法可以有效降低环境噪声、量测噪声对差异信号的影响；

步骤 S502：对入侵信号的存在进行检测；在本实施例中的检测方法使用了互相关检测技术，并利用 MATALB 软件对监测设备上的差异信号进行了入侵检测的仿真，图 5 为入侵信号互相关检测结果图，从图中可以看出，利用互相关检测技术可以明显区分入侵信号的有无，从而为系统的物理入侵攻击作出判断；

若在差异信号中检测出入侵信号，则判断 RS485 通信总线网络中已遭受物理入侵攻击，继续执行 S6；若在差异信号中没有检测出入侵信号，则判断 RS485 通信总线网络没有受到物理入侵攻击，监测设备转为继续监听状态，并结束本次物理入侵攻击检测的过程；

步骤 S6：根据入侵信号的检测结果，若 RS485 通信总线网络中遭受物理入侵攻击，则将检测结果上报给 RS485 控制器，以便于控制器对物理入侵攻击作出快速判断和应急响应。

由以上叙述可得，利用本发明提出的物理入侵攻击检测方法，可以在 RS485 通信总线网络中快速而准确的判别系统中是否存在外接设备，确定系统遭受物理入侵攻击。

权 利 要 求 书

1、一种基于串行通信总线信号分析的工控系统物理入侵攻击检测方法，其特征在于，包括：通过串行通信总线网络中的总线控制器主动向通信总线中发送检测信号，监测设备对通信总线进行信号的采样分析后，与设备数据库中存储的标准信号进行差分对比，并利用降噪技术、弱信号检测技术在差异信号中进行入侵信号的检测，根据由物理入侵设备所引起的入侵信号的检测结果，有效地判断出系统中是否存在外部恶意设备，确定系统是否遭受物理入侵攻击。

2、根据权利要求 1 所述的一种基于串行通信总线信号分析的工控系统物理入侵攻击检测方法，其特征在于，具体包括以下步骤：

S1：串行通信总线网络中的总线控制器按照设定的时间周期监听工控系统中串行通信总线的使用情况：

若通信总线处于空闲状态，则由总线控制器发送一次检测信号；

若通信总线处于数据传输状态，则控制器继续监听等待，直到通信总线处于空闲状态时，由总线控制器发送一次检测信号；

S2：工控系统中部署的监测设备对串行通信总线上所有的通信信号进行采样接收和协议解析；

S3：监测设备对解析后的接收信号进行分析，判断是否开始执行工控系统串行通信总线网络的物理入侵攻击检测；

S4：将接收到的信号数据与监测设备信号数据库中的标准信号数据进行差分对比，得到两个信号之间的差异信号；

S5：对差异信号进行入侵信号检测，若在差异信号中检测出入侵信号，则判断此时工控系统串行通信总线网络中已遭受物理入侵攻击，继续执行 S6；若在差异信号中没有检测出入侵信号，则判断此时工控系统串行通信总线网络没有受到物理入侵攻击，监测设备继续监听

总线接收下一次通信信号；

S6：根据入侵信号的检测结果，若工控系统串行通信总线网络中遭受物理入侵攻击，则将检测结果上报给串行通信总线网络中的总线控制器，总线控制器对物理入侵攻击作出快速判断和应急响应。

3、根据权利要求 1 所述的一种基于串行通信总线信号分析的工控系统物理入侵攻击检测方法，其特征在于，步骤 S1 中，检测信号根据串行通信总线的协议规范设定，并且检测信号在数字序列上有别于所有正常的通信信号，检测信号只能被串行通信总线网络中相应的监测设备进行识别和解析，其他设备不会对检测信号作出响应。

4、根据权利要求 1 所述的一种基于串行通信总线信号分析的工控系统物理入侵攻击检测方法，其特征在于，步骤 S2 具体为：

根据工控系统中串行通信总线类型，采用对应的 Modbus 协议、CANBus 协议、P-Net 协议、ProfiBus 协议、WorldFIP 协议、ControlNet 协议、FF 协议或 HART 协议对通信信号进行协议解析，得到数字信号序列。

5、根据权利要求 1 所述的一种基于串行通信总线信号分析的工控系统物理入侵攻击检测方法，其特征在于，步骤 S3 具体包括：

S301：将步骤 S2 所解析得到的数字信号序列与检测信号的数字序列进行一致性检测，若接收到的信号是检测信号，则开始进行工控系统串行通信总线网络物理入侵攻击的检测，执行步骤 S302；若接收到的信号不是检测信号，则不作任何响应，继续监听总线接收下一次通信信号；

S302：根据接收信号与检测信号一致的检测结果，继续判断监测设备是否第一次接收到检测信号，若监测设备的信号数据库为空，则将接收到的信号数据存储在本地数据库中，并认为此信号是系统正常情况下的标准信号；若监测设备的信号数据库中已存储有信号数据，

则继续执行步骤 S4。

6、根据权利要求 1 所述的一种基于串行通信总线信号分析的工控系统物理入侵攻击检测方法，其特征在于，步骤 S5 中，入侵信号是由于物理入侵攻击所引起的在总线控制器发送的原有检测信号上增加的确知信号，入侵信号具有与检测信号相同的周期。

7、根据权利要求 1 所述的一种基于串行通信总线信号分析的工控系统物理入侵攻击检测方法，其特征在于，步骤 S5 具体包括：

S501：对步骤 S4 获得的差异信号数据进行降噪处理；

S502：利用弱信号检测技术，对差异信号中可能存在的入侵信号进行检测，根据弱信号检测的结果判断入侵信号是否存在。

8、根据权利要求 1 所述的一种基于串行通信总线信号分析的工控系统物理入侵攻击检测方法，其特征在于，还包括以下步骤：总线控制器收到物理入侵攻击的检测信号后，向主站报警。

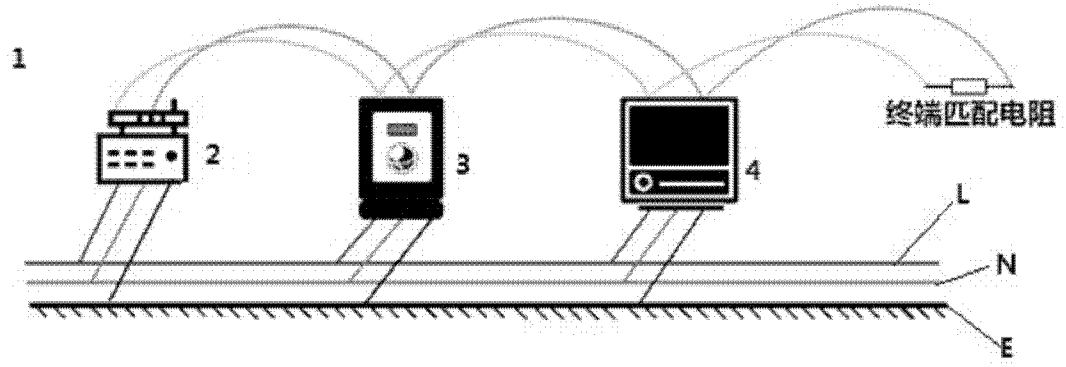
1
2
3
4
终端匹配电阻
L
N
E

图 1

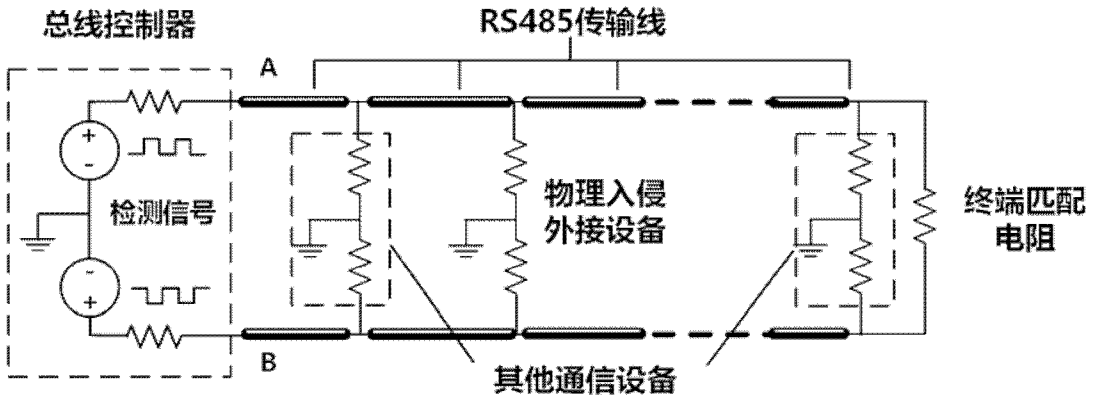
总线控制器
RS485传输线
A
B
检测信号
物理入侵
外接设备
终端匹配
电阻
其他通信设备

图 2

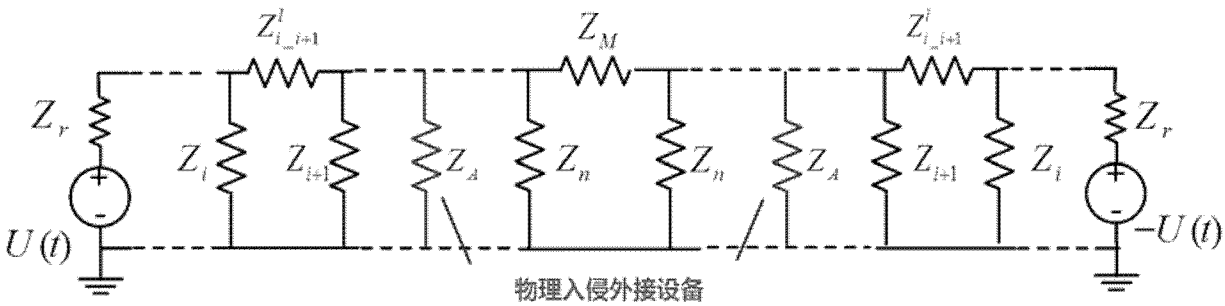
$Z^{l}_{i\_i+1}$
Z_M
$Z^{l}_{i\_i+1}$
Z_r
Z_i
Z_{i+1}
Z_A
Z_n
Z_n
Z_A
Z_{i+1}
Z_i
Z_r
$U(t)$
$-U(t)$
物理入侵外接设备

图 3

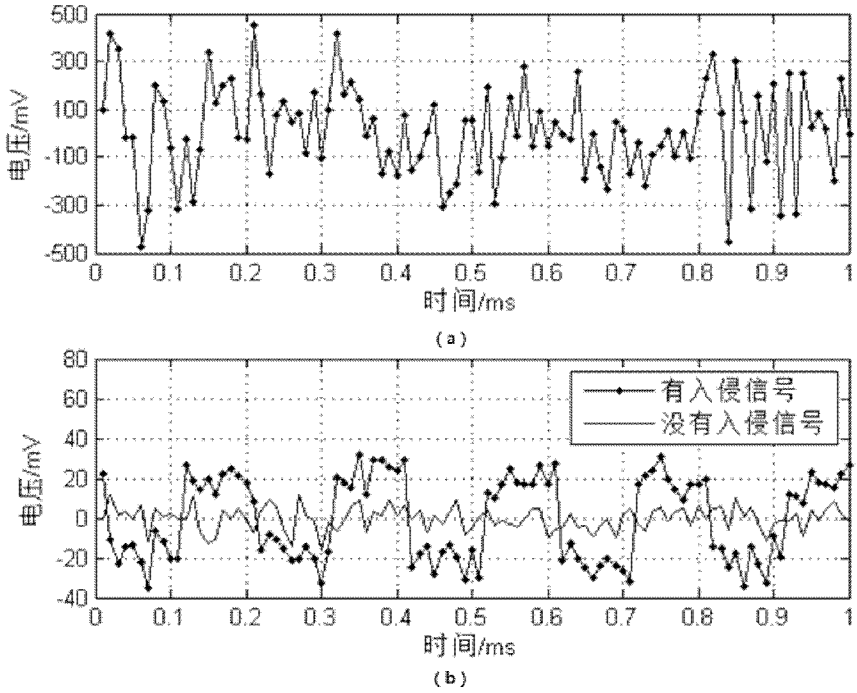

图 4

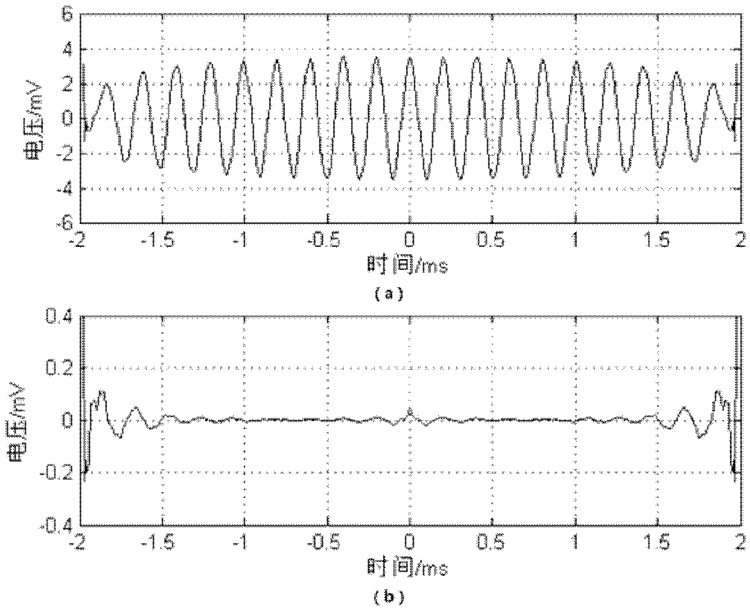

图 5

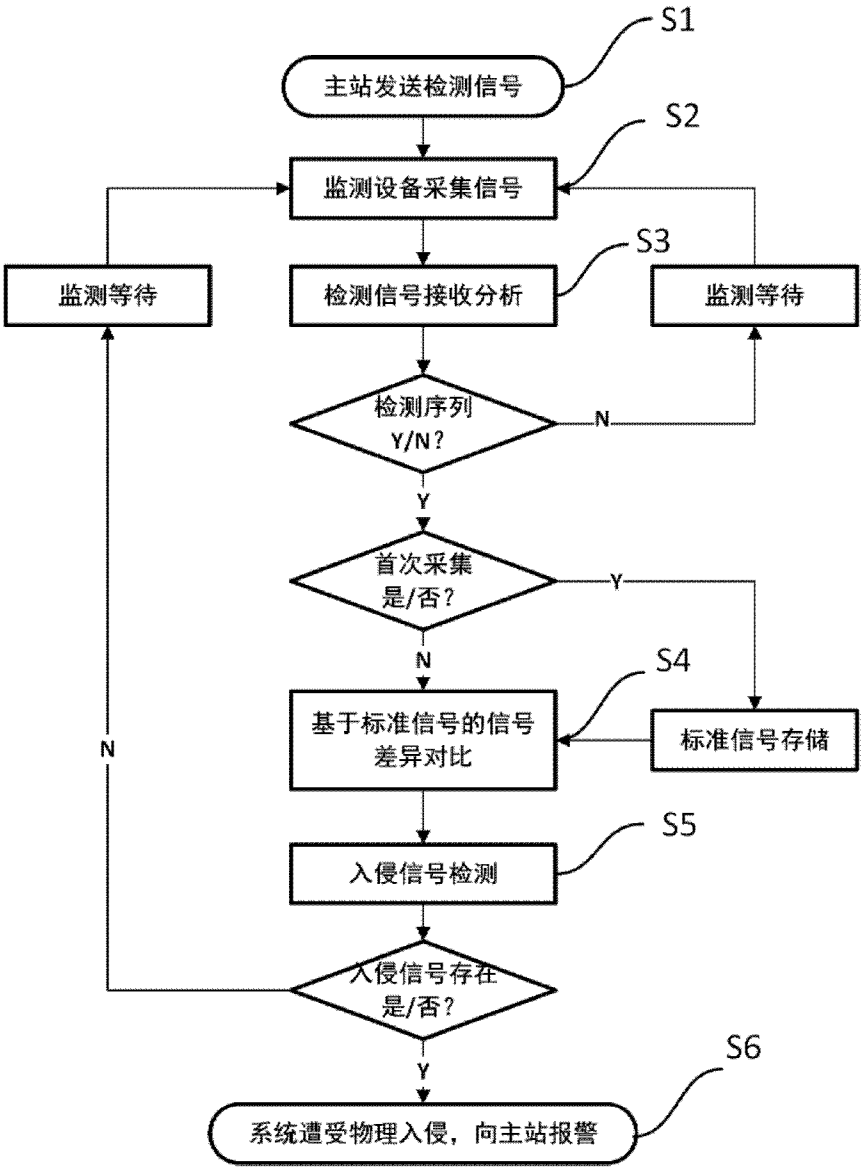
S1
主站发送检测信号
S2
监测设备采集信号
S3
检测信号接收分析
监测等待
监测等待
检测序列
Y/N?
N
Y
首次采集
是/否?
Y
N
S4
基于标准信号的信号
差异对比
标准信号存储
N
S5
入侵信号检测
入侵信号存在
是/否?
Y
S6
系统遭受物理入侵，向主站报警

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/120178

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/85(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI; EPODOC; CNKI; CNPAT: 串行通信总线, 物理入侵, 攻击, 检测, 采样, 差分对比, 监听, usb, attack, sampling, monitor

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 108520187 A (XI'AN JIAOTONG UNIVERSITY) 11 September 2018 (2018-09-11) claims 1-8	1-8
A	CN 107065838 A (GUANGDONG XI'AN JIAOTONG UNIVERSITY ACADEMY) 18 August 2017 (2017-08-18) description, paragraphs [0006]-[0036]	1-8
A	CN 106209870 A (UNIVERSITY OF SCIENCE & TECHNOLOGY BEIJING) 07 December 2016 (2016-12-07) entire document	1-8
A	US 8832783 B2 (INTEL CORPORATION) 09 September 2014 (2014-09-09) entire document	1-8

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 April 2019	**18 April 2019**

Name and mailing address of the ISA/CN	Authorized officer
State Intellectual Property Office of the P. R. China **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing** **100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/120178

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	108520187	A	11 September 2018	None	
CN	107065838	A	18 August 2017	None	
CN	106209870	A	07 December 2016	None	
US	8832783	B2	09 September 2014	None	

国际检索报告

国际申请号
PCT/CN2018/120178

A. 主题的分类

G06F 21/85(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

WPI;EPODOC;CNKI;CNPAT: 串行通信总线，物理入侵，攻击，检测，采样，差分对比，监听，usb,attack,sampling,monitor

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 108520187 A (西安交通大学) 2018年 9月 11日 (2018-09-11) 权利要求1-8	1-8
A	CN 107065838 A (广东顺德西安交通大学研究院) 2017年 8月 18日 (2017-08-18) 说明书第[0006]-[0036]段	1-8
A	CN 106209870 A (北京科技大学) 2016年 12月 7日 (2016-12-07) 全文	1-8
A	US 8832783 B2 (INTEL CORPORATION) 2014年 9月 9日 (2014-09-09) 全文	1-8

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2019年 4月 11日	2019年 4月 18日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	从磊
传真号 (86-10)62019451	电话号码 (86-10)-53961305

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/120178

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	108520187	A	2018年 9月 11日	无	
CN	107065838	A	2017年 8月 18日	无	
CN	106209870	A	2016年 12月 7日	无	
US	8832783	B2	2014年 9月 9日	无	