(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 106125643 A
(43)申请公布日 2016.11.16

(21)申请号 201610456944.9

(22)申请日 2016.06.22

(71)申请人 华东师范大学
地址 200062 上海市普陀区中山北路3663号

(72)发明人 黄滟鸿 郭欣 史建琦 李昂 方徽星

(74)专利代理机构 北京乾诚五洲知识产权代理有限责任公司 11042
代理人 付晓青 杨玉荣

(51)Int.Cl.
G05B 19/048(2006.01)

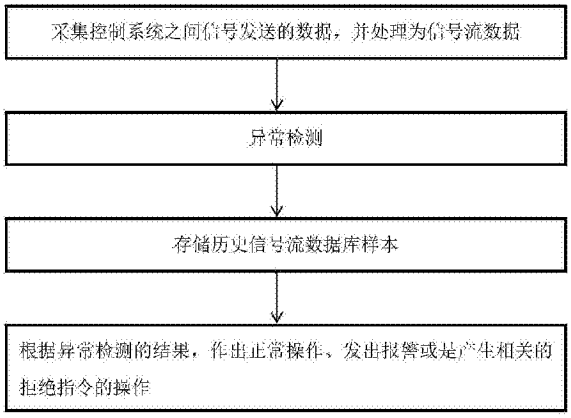
权利要求书1页 说明书4页 附图3页

(54)发明名称

一种基于机器学习技术的工控安防方法

(57)摘要

本发明公开一种基于机器学习技术的工控安防方法，其包括：采集控制系统之间信号发送的数据，并处理为反应信号发送方向与顺序的信号流数据；异常检测；接收处理的信号流数据，并对所述数据基于机器学习框架进行异常性检测，得出是否有异常于常规操作的情况发生的结论；存储历史信号流数据库样本；根据异常检测的结果，作出正常操作、发出报警或是产生相关的拒绝指令的操作。通过本方法将采集工控系统之间信号发送的数据并进行预处理后，对所述数据基于机器学习框架的异常性进行检测，当有异常于常规操作的情况发生时，自动发出报警或是产生相关的拒绝指令。



CN 106125643 A

1.一种基于机器学习技术的工控安防方法,其包括:

步骤101、采集控制系统之间信号发送的数据,并处理为反应信号发送方向与顺序的信号流数据;

步骤103、异常检测;

步骤105、存储历史信号流数据库样本;

步骤107、根据异常检测的结果,作出正常操作、发出报警或是产生相关的拒绝指令的操作。

2.如权利要求1所述基于机器学习技术的工控安防方法,其中所述步骤103包括以下步骤:

2.1、在假设无异常的情况下,获取所述信号流数据,形成信号流数据集,并对其进行基于机器学习技术的预处理;

2.2、对下一次信号流数据集的异常性进行分析;

2.3、判断控制系统是否有异常;

2.4、根据判断结果进行相关操作。

3.如权利要求2所述基于机器学习技术的工控安防方法,其中所述步骤2.2具体为:接收步骤2.1得出的统计预测数据,并根据所述预测数据估算从数据采集和预处理模块获取的下一次信号流数据。

4.如权利要求2所述基于机器学习技术的工控安防方法,其中所述步骤2.3具体为:根据下一次信号流数据集的预测值和实际值,对所述下一次信号流数据集的异常性进行判断。

5.如权利要求2所述基于机器学习技术的工控安防方法,其中所述步骤2.4具体为:根据所述异常性判断结果作出正常操作、发出报警或是产生相关的拒绝指令的操作的决策,同时根据所述异常性判断结果对所述预测数据作出更新,将本次信号流数据集发送给数据存储单元以更新历史信号流数据库样本。

6.如权利要求2所述基于机器学习技术的工控安防方法,其中所述步骤2.2中对所述下一次信号流数据集的异常性进行判断的方法具体包括以下步骤:

3.1、比较所述预测值与获取的下一次信号流数据的实际值,得出两者的差值Δ;

3.2、获取与所测信号流数据具有相同的时间步长和系统操作背景的历史数据库样本,计算该样本的标准差;

3.3、比较所述差值与标准差范围:

如果差值Δ不在[-δ,δ]的范围之内,计算偏离值P,其中P=||Δ|-δ|;如果差值Δ在[-δ,δ]的范围之内,则发送一个肯定信号,确定无异常情况。

7.如权利要求2所述基于机器学习技术的工控安防方法,其中所述步骤2.3进行决策的方法具体包括以下步骤:

4.1、若判断结果为偏离值P,则进行步骤4.2,若数据为一个肯定信号,则进行步骤4.3;

4.2、若接收偏离值P,将偏离值P与已设定的判定值λ进行比较,若偏离值P小于判定值λ,发送报警信号;若偏离值P大于等于判定值λ,则发送保护信号,同时,更新本次的信号流数据样本,并标记为异常事件;

4.3、若接收到肯定信号,则将样本数据进行更新,用于检测下一次的信号流数据。

一种基于机器学习技术的工控安防方法

技术领域

[0001] 本发明涉及一种基于机器学习技术的工控安防方法，属于工控安全技术领域。

背景技术

[0002] 工业控制系统是运用控制理论、计算机科学、仪器仪表等技术，对生产过程的各种信息采集、分析、处理，并进行优化控制和合理的调度、管理，以达到提高生产效率的一种控制系统。工业控制系统安全可以分成三个方面，即功能安全、物理安全和信息安全。其中功能安全是为了达到设备和工厂安全功能，受保护的、和控制设备的安全相关部分必须正确执行其功能，而且当失效或故障发生时，设备或系统必须仍能保持安全条件或进入到安全状态。我们可以通过采集工控系统之间的信号发送的数据来进行异常检测，通过历史模式和模型预测来判断数据异常。

发明内容

[0003] 本发明的目的是提供了基于机器学习技术的工控安防方法，其基于机器学习技术，监测控制系统之间的信号发送。当有异于常规操作的情况发生时，自动产生报警或是保护相关的设备拒绝指令。

[0004] 所述方法包括：

[0005] 步骤101、采集控制系统之间信号发送的数据，并处理为反应信号发送方向与顺序的信号流数据；

[0006] 步骤103、异常检测；

[0007] 步骤105、存储历史信号流数据库样本；

[0008] 步骤107、根据异常检测的结果，作出正常操作、发出报警或是产生相关的拒绝指令的操作。

[0009] 其中，所述步骤103包括以下步骤：

[0010] 2.1、在假设无异常的情况下，获取所述信号流数据，形成信号流数据集，并对其进行基于机器学习技术的预处理；

[0011] 2.2、对下一次信号流数据集的异常性进行分析；

[0012] 2.3、判断控制系统是否有异常；

[0013] 2.4、根据判断结果进行相关操作。

[0014] 其中，所述步骤2.2具体为：接收步骤2.1得出的统计预测数据，并根据所述预测数据估算从数据采集和预处理模块获取的下一次信号流数据。

[0015] 其中，所述步骤2.3具体为：根据下一次信号流数据集的预测值和实际值，对所述下一次信号流数据集的异常性进行判断。

[0016] 其中，所述步骤2.4具体为：根据所述异常性判断结果作出正常操作、发出报警或是产生相关的拒绝指令的操作的决策，同时根据所述异常性判断结果对所述预测数据作出更新，将本次信号流数据集发送给数据存储单元以更新历史信号流数据库样本。

[0017] 其中，所述步骤2.2中对所述下一次信号流数据集的异常性进行判断的方法具体包括以下步骤：

[0018] 3.1、比较所述预测值与获取的下一次信号流数据的实际值，得出两者的差值Δ；

[0019] 3.2、获取与所测信号流数据具有相同的时间步长和系统操作背景的历史数据库样本，计算该样本的标准差；

[0020] 3.3、比较所述差值与标准差范围：

[0021] 如果差值Δ不在[-δ,δ]的范围之内，计算偏离值P，其中P＝||Δ|-δ|；如果差值Δ在[-δ,δ]的范围之内，则发送一个肯定信号，确定无异常情况。

[0022] 其中，所述步骤2.3进行决策的方法具体包括以下步骤：

[0023] 4.1、若判断结果为偏离值P，则进行步骤4.2，若数据为一个肯定信号，则进行步骤4.3；

[0024] 4.2、若接收偏离值P，将偏离值P与已设定的判定值λ进行比较，若偏离值P小于判定值λ，发送报警信号；若偏离值P大于等于判定值λ，则送保护信号，同时，更新本次的信号流数据样本，并标记为异常事件；

[0025] 4.3、若接收到肯定信号，则将样本数据进行更新，用于检测下一次的信号流数据。

[0026] 本发明的有益效果包括：

[0027] 1、通过机器学习技术对控制系统之间信号发送进行异常检测，从而提供在假设无异常情况下信号流状态的统计分布预测，提高了工控系统的异常识别率，同时节约了大量的人力。

[0028] 2、所述工控安全防护与报警方法可自感知异常，并在发现异常后，作出自动产生报警或是保护相关的设备拒绝指令的操作。

[0029] 3、可将本地服务器主机中的历史数据的镜像副本定期更新在云服务器中，避免因服务器主机损坏造成的损失。

附图说明

[0030] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0031] 图1是本发明基于机器学习技术的工控安防方法的流程图。

[0032] 图2是本发明中检测步骤示意方框图。

[0033] 图3是本发明中信号流数据集的异常性判断方法流程图。

[0034] 图4是本发明中决策模块进行决策的步骤示意方框图。

具体实施方式

[0035] 下面将参照附图更详细地描述本公开的示例性实施方式。虽然附图中显示了本公开的示例性实施方式，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施方式所限制。相反，提供这些实施方式是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0036] 如图1所示，本发明公开一种基于机器学习技术的工控安防方法，其包括：

[0037] 步骤101、采集控制系统之间信号发送的数据，并处理为反应信号发送方向与顺序的信号流数据。

[0038] 其中，通过数据采集和预处理模块监控控制系统之间的信号发送，采集控制系统之间信号发送的数据，并将这些数据处理成反应信号发送方向与顺序的信号流的形式。

[0039] 步骤103、异常检测。

[0040] 其中，接收步骤101中处理的信号流数据，并对所述数据基于机器学习框架进行异常性检测，得出是否有异常于常规操作的情况发生的结论。

[0041] 步骤105、存储历史信号流数据库样本。

[0042] 步骤107、根据异常检测的结果，作出正常操作、发出报警或是产生相关的拒绝指令的操作。

[0043] 如图2所示，本发明提出的所述基于机器学习技术的工控安防方法中，检测步骤包括：2.1、在假设无异常的情况下，获取所述信号流数据，形成信号流数据集，并对其进行基于机器学习技术的预处理；2.2、对下一次信号流数据集的异常性进行分析；2.3、判断控制系统是否有异常；2.4、根据判断结果进行相关操作。

[0044] 其中，以上步骤具体为：步骤2.2，接收步骤2.1得出的统计预测数据，并根据所述预测数据估算从数据采集和预处理模块获取的下一次信号流数据；在步骤2.3，根据下一次信号流数据集的预测值和实际值，对所述下一次信号流数据集的异常性进行判断；在步骤2.4，根据所述异常性判断结果作出正常操作、发出报警或是产生相关的拒绝指令的操作的决策，同时根据所述异常性判断结果对所述预测数据作出更新，将本次信号流数据集发送给数据存储单元以更新历史信号流数据库样本。

[0045] 如图3所示，本发明提出的所述基于机器学习技术的工控安防方法中，所述步骤2.2中对所述下一次信号流数据集的异常性进行判断的方法具体包括以下步骤：

[0046] 3.1、比较所述预测值与获取的下一次信号流数据的实际值，得出两者的差值Δ；

[0047] 3.2、获取与所测信号流数据具有相同的时间步长和系统操作背景的历史数据库样本，计算该样本的标准差；

[0048] 3.3、比较所述差值与标准差范围：

[0049] 如果差值Δ不在[-δ,δ]的范围之内，计算偏离值P，其中P＝||Δ|-δ|；如果差值Δ在[-δ,δ]的范围之内，则发送一个肯定信号，确定无异常情况。

[0050] 如图4所示，本发明提出的所述基于机器学习技术的工控安防方法中，所述步骤2.3进行决策的方法具体包括以下步骤：

[0051] 4.1、若判断结果为偏离值P，则进行步骤4.2，若数据为一个肯定信号，则进行步骤4.3；

[0052] 4.2、若接收偏离值P，将偏离值P与已设定的判定值λ进行比较，若偏离值P小于判定值λ，发送报警信号；若偏离值P大于等于判定值λ，则送保护信号。同时，更新本次的信号流数据样本，并标记为异常事件；

[0053] 4.3、若接收到肯定信号，则将样本数据进行更新，用于检测下一次的信号流数据。

[0054] 本发明提出的所述基于机器学习技术的工控安防方法中，可本地存储信号流数据集、样本数据，将所述数据存储在本地服务器主机中；也可以将本地服务器主机中的历史数据的镜像副本定期更新在云服务器中，避免因本地服务器主机损坏造成的损失。

[0055] 本发明提出的所述基于机器学习技术的工控安防方法中，当接收到发送的报警信号时，产生报警；当接收到发送的保护信号时，会发出拒绝操作的指令，使控制系统无法进行相关操作。

[0056] 本发明与传统工控安全防护与报警方法相比，通过机器学习技术对控制系统之间信号发送进行异常检测，从而提供在假设无异常情况下信号流状态的统计分布预测，提高了工控系统的异常识别率，同时节约了大量的人力。

[0057] 本发明与传统工控安全防护与报警方法相比，所述工控安全防护与报警方法可自感知异常，并在发现异常后，作出自动产生报警或是保护相关的设备拒绝指令的操作。

[0058] 本发明与传统工控安全防护与报警方法相比，通过网络存储方式可将本地服务器主机中的历史数据的镜像副本定期更新在云服务器中，避免因服务器主机损坏造成的损失。

[0059] 以上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应所述以权利要求的保护范围为准。

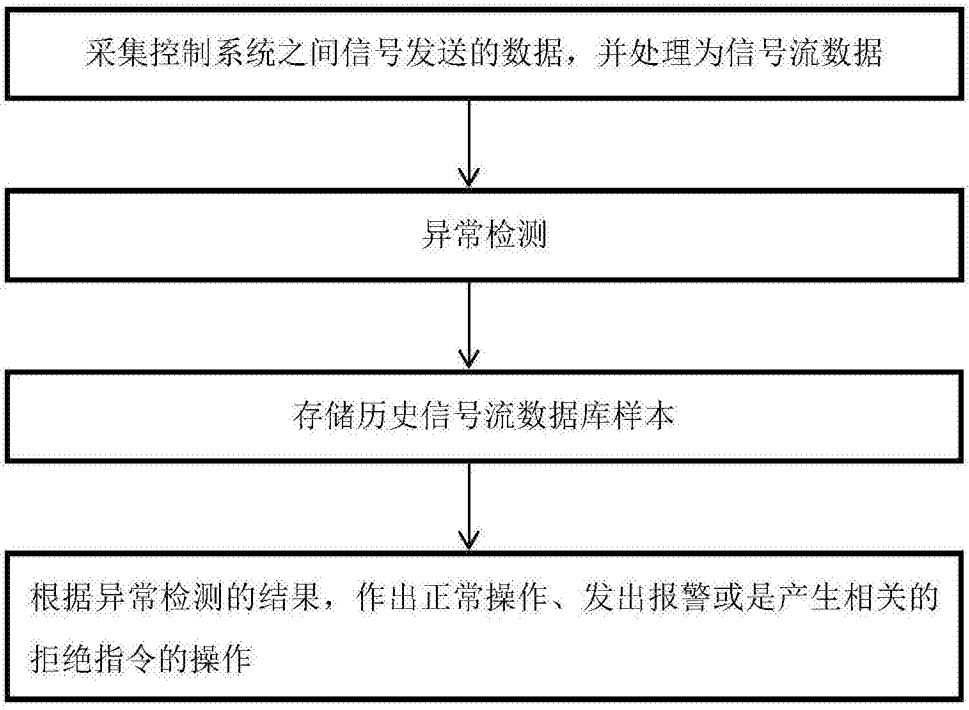

采集控制系统之间信号发送的数据，并处理为信号流数据
异常检测
存储历史信号流数据库样本
根据异常检测的结果，作出正常操作、发出报警或是产生相关的拒绝指令的操作

图1

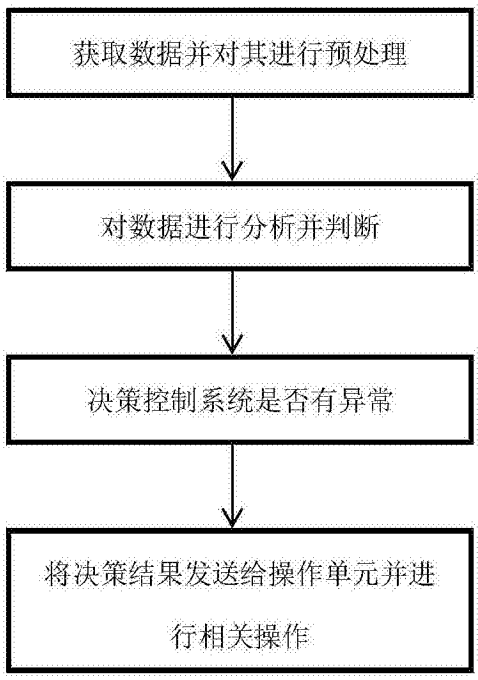

获取数据并对其进行预处理
对数据进行分析并判断
决策控制系统是否有异常
将决策结果发送给操作单元并进行相关操作

图2

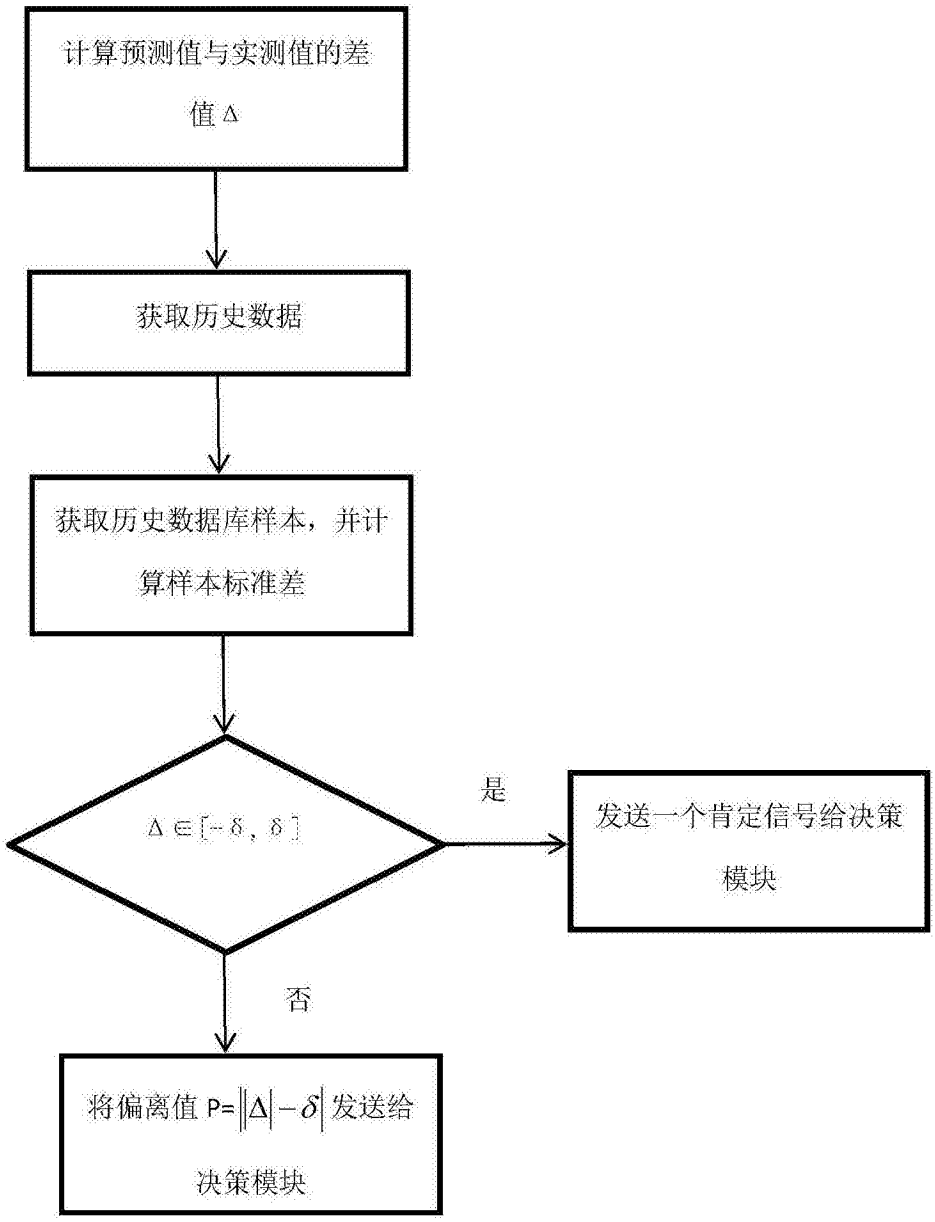

计算预测值与实测值的差值Δ
获取历史数据
获取历史数据库样本，并计算样本标准差
Δ∈[-δ，δ]
是
发送一个肯定信号给决策模块
否
将偏离值P=||Δ|-δ|发送给决策模块

图3

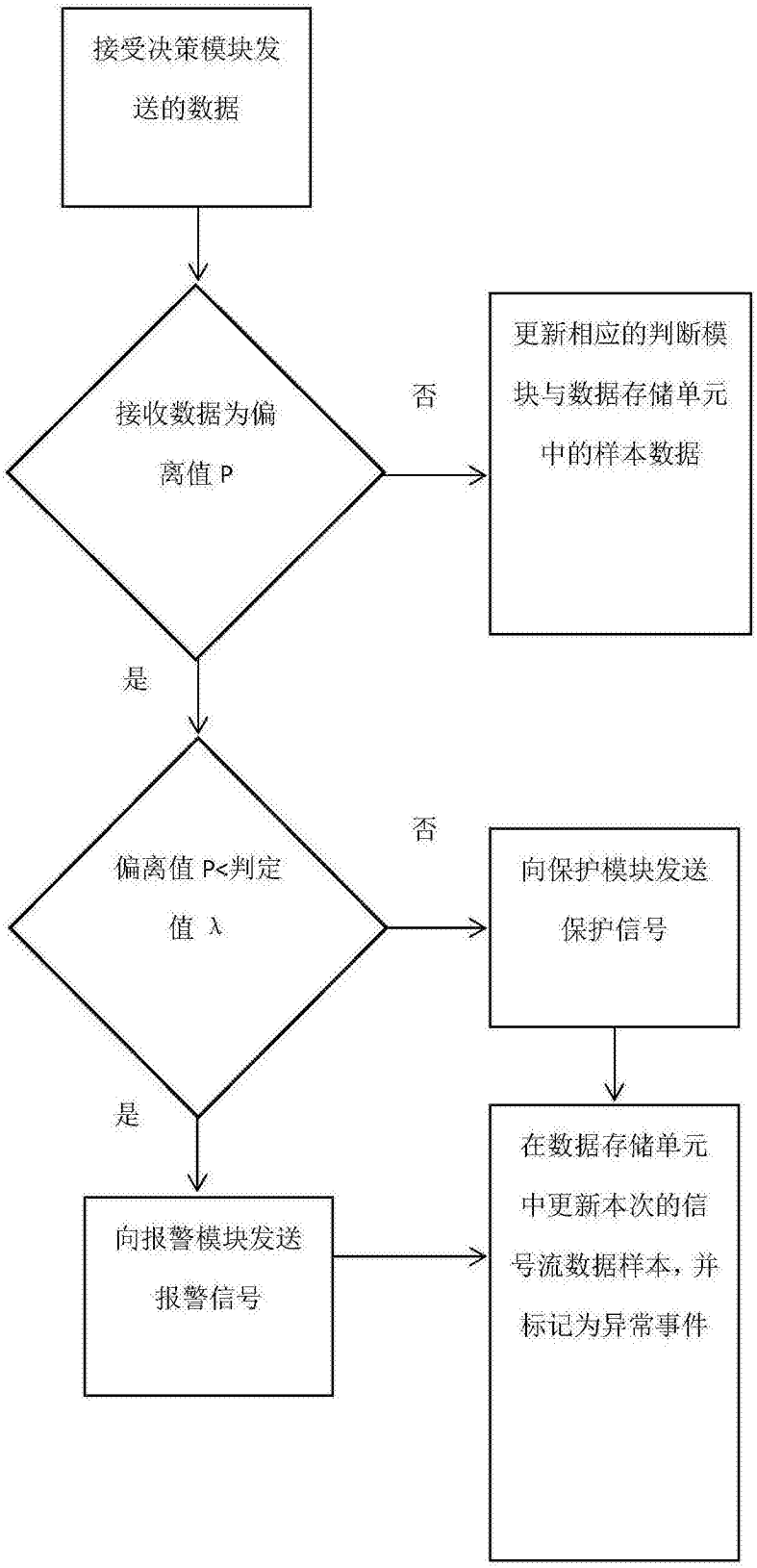

接受决策模块发送的数据
接收数据为偏离值 P
否
更新相应的判断模块与数据存储单元中的样本数据
是
偏离值 P<判定值 λ
否
向保护模块发送保护信号
是
向报警模块发送报警信号
在数据存储单元中更新本次的信号流数据样本，并标记为异常事件

图4