[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04W 92/10 (2009.01)
H04W 88/02 (2009.01)
H04W 88/08 (2009.01)

[12] 发明专利说明书

专利号 ZL 03822731.2

[45] 授权公告日 2009 年 11 月 11 日

[11] 授权公告号 CN 100559906C

[22] 申请日 2003.9.24 [21] 申请号 03822731.2

[30] 优先权

[32] 2002.9.24 [33] DE [31] 10244462.5

[86] 国际申请 PCT/EP2003/010637 2003.9.24

[87] 国际公布 WO2004/030285 德 2004.4.8

[85] 进入国家阶段日期 2005.3.24

[73] 专利权人 西门子公司

地址 德国慕尼黑

[72] 发明人 T·亚特施卡

[56] 参考文献

CN1259000A 2000.7.5

GB2342010A 2000.3.29

审查员 庞 艳

[74] 专利代理机构 中国专利代理(香港)有限公司

代理人 吴立明 张志醒

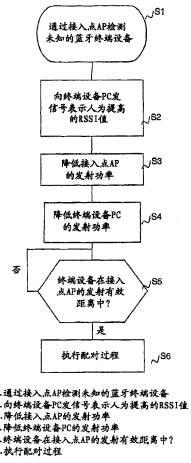
权利要求书 2 页 说明书 5 页 附图 2 页

[54] 发明名称

用于在本地通信网络的接入点上注册移动终端设备的方法以及用于执行该方法的接入点和终端设备

[57] 摘要

本发明涉及一种在本地通信网络的接入点上第一次注册一个、特别是移动的、终端设备的方法，其中接入点的第一无线电发射/无线电接收设备的第一发射功率在检测终端设备之后被这样降低，使得发射/接收过程可仅仅在接入点的近场中完成，此外本发明涉及一种用于执行该方法的接入点以及终端设备。



1. 用于在本地通信网络的接入点上第一次注册终端设备的方法，其特征在于，

a）该接入点的第一无线电发射/无线电接收设备的第一发射功率在检测（S1）终端设备之后被降低（S3），使得第一次注册的发射/接收过程仅仅在该接入点的近场中实现，其中，

b）在检测之后通过接入点执行针对所述终端设备的信令，这促使该终端设备降低（S2）第二无线电发射/无线电接收设备的第二发射功率，其中，第二发射功率被降低，使得发射/接收过程仅仅在终端设备的近场中实现，并且其中该信令在降低第一发射功率之前实现，以及其中，

c）所述信令通过传送第一消息来实现，该第一消息针对具有比通过接入点确定的所接收的“接收信号强度指示符”值更高的值的信号电平的说明而被规定（S2）。

2. 根据上述权利要求所述的方法，其特征在于，所述信令（S2）包含第二消息，该第二消息为了向所述终端设备的用户输出一个提示而如下要求该终端设备，即将该终端设备引入接入点的近场中。

3. 根据权利要求 2 所述的方法，其特征在于，在经过预定的时间间隔之后，所述第二消息被重新发送，其中为此至少暂时将第一发射功率提高到在检测时刻存在的电平。

4. 根据权利要求 3 所述的方法，其特征在于，重新发送周期性地分别在经过所述预定的时间间隔之后被重复（S5）。

5. 根据上述权利要求之一所述的方法，其特征在于，所述第一和第二无线电发射/无线电接收设备按照近程无线电标准运行。

6. 根据权利要求 5 所述的方法，其特征在于，蓝牙标准被用作近程无线电标准。

7. 接入点，其特征在于，

－第一无线电发射/无线电接收设备，用于提供终端设备位于其中的第一无线电覆盖区（N1），以及

－装置（μP1），用于在检测终端设备之后降低第一无线电发射/无线电接收设备的第一发射功率，以致在接入点上第一次注册终端设备的发射/接收过程仅仅在该接入点的近场中实现，

其中，在检测之后通过该接入点执行针对终端设备的信令，这促使终端设备降低第二无线电发射/无线电接收设备的第二发射功率，其中，第二发射功率被降低，使得发射/接收过程仅仅在终端设备的近场中实现，并且其中该信令在降低第一发射功率之前实现以及通过传送第一消息来实现，该第一消息针对具有比通过接入点确定的所接收的“接收信号强度指示符”值更高的值的信号电平的说明而被规定。

8. 终端设备，其特征在于，

－第二无线电发射/无线电接收设备，用于提供接入点位于其中的第二无线电覆盖区（N2），以及

－装置（μP2），用于降低第二无线电发射/无线电接收设备的第二发射功率，其中，第二发射功率被降低，使得在接入点上第一次注册终端设备的发射/接收过程仅仅在终端设备的近场中实现，

其中，在检测终端设备之后，接入点的第一无线电发射/无线电接收设备的第一发射功率被降低，使得第一次注册的发射/接收过程仅仅在该接入点的近场中实现，在检测之后通过接入点执行针对终端设备的信令，以促使该终端设备降低第二无线电发射/无线电接收设备的第二发射功率，其中该信令在降低第一发射功率之前实现以及通过传送第一消息来实现，该第一消息针对具有比通过接入点确定的所接收的“接收信号强度指示符”值更高的值的信号电平的说明而被规定。

用于在本地通信网络的接入点上注册移动终端设备的方法以及用于执行该方法的接入点和终端设备

本发明涉及一种用于在本地通信网络的接入点上注册移动终端设备的方法、用于执行该方法的接入点以及用于执行该方法的终端设备。

信息网和通信网的融合已导致，数据传输网、如局域网 LAN 越来越多地配备无线接入点（所谓的 Acess Point），该无线接入点允许也称为网络节点的新的网络用户无线连接在 LAN 上。该发展甚至进行地如此广泛，以致这种网络部分地主要或者完全无线交换数据。

这类网络在网络内部也针对未授权的存取数据提供空间，以至于为此发展多种用于保障安全的方法。

这些方法之一是将网络内部的数据交换限制在已知的网络节点上，其中网络由此已知一个新的网络节点，即该新的网络节点在初次注册、第一次注册时与各自的接入点交换鉴权数据、大多为在传输时用于加密数据的密匙。

当所述交换无线完成时，得出一个缺点。在这种情况下，可能的入侵者可截获鉴权数据，以针对不被允许的访问冒充为已知的终端设备或借助该密匙解密被加密的数据。

本发明所基于的任务在于，给出一种方法和装置，该方法和装置允许，利用无线接入点尽可能地阻止未授权的接入本地通信网。

所述任务由用于在本地通信网络的接入点上第一次注册移动终端设备的方法通过以下特征来解决：a）该接入点（AP）的第一无线电发射/无线电接收设备（TRX1）的第一发射功率在检测（S1）终端设备（PC）之后被这样降低（S3），使得第一次注册的发射/接收过程仅仅在该接入点（AP）的近场中实现；b）在检测之后通过接入点执行针对所述终端设备（PC）的信令，这促使该终端设备（PC）降低（S2）第二无线电发射/无线电接收设备（TRX2）的第二发射功率，其中，第二发射功率被这样降低，使得发射/接收过程仅仅在终端设备（PC）的近场中实现，并且其中该信令在降低第一发射功率之前

实现；以及 c）所述信令通过传送第一消息来实现，该第一消息针对通过接入点（AP）确定的所接收的“接收信号强度指示符”RSSI 值的说明而被规定（S2），其中替代所述 RSSI 值给出具有更高值的信号电平。此外，该任务由接入点通过用于执行上述方法的装置以及由终端设备通过用于执行上述方法的装置来解决。

在根据本发明的用于在本地通信网络的接入点上第一次注册尤其是移动的终端设备的方法中，该接入点的第一无线电发射/无线电接收设备的第一发射功率在检测该终端设备后这样被减少，使得发射/接收过程可仅仅在该接入点的近场中完成。

通过该接入点的第一无线电发射/无线电接收设备的第一发射功率的单方面的降低，以至于接收仅仅在该接入点的近场是可能的，达到，借助一个其他的不是作为属于本地通信网的终端设备（窃听者）至少明显降低窃听的机会。首先避免，在第一次注册时窃听者通常可分析所传输的安全相关的数据、诸如鉴权密匙，因为通常窃听者不停留在接入点的近场中并且针对该分析结果不仅必需接入点的数据而且必需第一次注册的终端设备的数据。其他优点是，针对窃听入侵的终端设备的防御的转换不必被改变，例如当终端设备不能改变其发射功率时，该防御也可以被保证。

在本发明的可能的扩展方案中，在检测后，接入点有利地执行给终端设备的信令，这促使终端设备降低第二无线电发射/无线电接收设备的第二发射功率，其中第二发射功率被这样降低，使得发射/接收过程可以仅仅在终端设备的近场中完成并且其中在降低第一发射功率前完成信令。由此达到，停留在近场之外的窃听者既不可截获由接入点发送的数据又不可截获由终端设备在注册过程的范围中要发送的数据，以至于所交换的数据的分析完全被阻止。

优选地，该信令通过传送第一消息来完成，该第一消息针对由接入点测定的所接收的第一信号电平、特别是“接收信号强度指示符（Received Signal Strength Indicator）”RSSI 值的说明而被规定，其中替代所规定的第一信号电平给出特别是具有更高值的第二信号电平。该扩展方案的优点是通过由此可能的更简单的实施在已经存在的系统中给出，该系统至少部分地使用通过无线电的传输，因为实质上每个无线电通信标准保留这样的消息作为针对各自的信

号的源的反馈信息的发送。因而利用该扩展方案可能的是,没有变化的终端设备可支持根据本发明的方法。该接入点必须仅仅这样来被安排,使得该接入点针对另外的目的使用根据无线电通信标准保留的消息,也就是说不依赖于实际接收的信号电平的高度来发信号表示这样高的所接收的信号电平,使得该终端设备(源)在大小上降低其发射功率,即数据接收仅仅在终端设备的近场中是可能的。

如果该信令包含第二个消息,该第二个消息为了向终端设备的用户输出提示而如下要求终端设备,即将该终端设备引入该接入点的近场中,则避免,为了转换终端设备的第一次注册而由此无意识地中断数据交换,即终端设备的用户没有关于此的知识,即该用户必须利用用于第一次注册的终端设备停留在接入点的近场中。

为了确保第二个消息达到所期望的效果(告知用户),第二个消息在扩展方案中在经过一预定的时间间隔之后被重新发送,其中为了确保终端设备可接收这些消息,至少暂时将第一发射功率提高到在检测时刻存在的电平上。

这也是可以想象的,重新发送周期性地分别在经过预定的时间间隔之后重复,以至于以较高概率可排除,用户没有获悉该消息。

如果第一和第二无线电发射/无线电接收设备按照近程无线电标准运行,则在该标准中本来已经很短的传输距离还被减小,以至于当窃听者尝试进入通过第一和第二无线电发射/无线电接收方向无线电覆盖的近场中时,看到该窃听者。此外,新发展的一代无线电发射/无线电接收设备、特别是按照蓝牙标准运行的无线电发射/无线电接收设备具有芯片组,该芯片组允许终端设备中的发射功率的变化。

根据本发明的接入点以及根据本发明的终端设备以用于执行该方法的装置出众,以至于根据本发明的方法在相应的设备中找到支持。

本发明的其他细节和优点在图 1 至 2 中被解释。由此

图 1 示出布局场景的描述,其中窃听入侵的尝试是可能的。

图 2 示出在采用按照该场景的布局时根据本发明的方法的流程图。

在图 1 中, 示例性地示出一种布局,该布局根据本发明阻止通过

用于窃听的终端设备 LA 尝试窃听入侵，其中这由此被达到，即局域网 LAN 还未知的终端设备位于局域网 LAN 的接入点(Access Point) AP 的第一无线电覆盖区 N1 中，该终端设备在所示的实施例中按照蓝牙标准运行。

第一无线电覆盖区 N1 由第一无线电发射/无线电接收设备 TRX1 来提供，其中第一无线电发射/无线电接收设备 TRX1 的第一发射功率具有由第一微处理器 μP1 调节的值，该值将第一无线电覆盖区 N1 的有效距离限制在接入点 AP 的近场上，也就是说第一发射功率具有通常为几个分米、可替换地也直至一米的半径。

除了第一无线电覆盖区 N1，在这个实施例中，要新注册的终端设备 PC 的第二无线电覆盖区 N2 也被限制在通常与第一无线电覆盖区 N1 的有效距离相同的有效距离的近场上。这通过调节终端设备 PC 的第二无线电发射/无线电接收设备 TRX2 的第二发射功率由第二微处理器 μP2（蓝牙芯片组）来达到。

接入点 AP 位于第二无线电覆盖区 N2 之内，以至于沿两个方向的数据传输是无问题地可能的，其中窃听入侵的尝试通过另一个没有申请的终端设备 LA 来阻止或至少使它变得困难，该终端设备 LA 没有位于两个人为限制的无线电覆盖区 N1、N2 之内。

按照蓝牙标准称为“配对过程”的第一次注册是特别关键的，因为在该过程中蓝牙终端设备通过密匙的传输在网络中被一次验证并因此从此以后被存储为已知的值得信任的终端设备“信用设备（trusted device）”，以至于信息（密匙）的截获将使得窃听者针对其他未授权的接入网络的可能性成为可能。

在图 1 中所示出的布局通过根据本发明的方法的实施例阻止这样的入侵，该方法的流程图在图 2 中被示出。

在图 2 中所描述的流程图示出在上述场景中在根据本发明的方法的范围中待执行的步骤。

该方法通常以此开始，即通过接入点 AP 检测未知的终端设备 PC，并且因此接入点 AP 在第一步 S1 中位于“未知的蓝牙终端设备”的状态中。

从该第一步 S1 出发，紧接着在随后的第二步 S2 中通常发信号给蓝牙终端设备 PC 一人为提高的所接收的信号电平（RSSI 值）。在这

种情况下，人为提高意味着，通常不是发信号表示实际上测定的信号电平值，而是根据本发明发信号表示这样高的值，使得终端设备PC将他的发射功率降低到一个水平，该水平导致终端设备PC的第二无线电覆盖区N2，该第二无线电覆盖区N2被限制在近场上。

如果该方法在无线电系统中被采用，则第二步S2可停止，该无线电系统具有不支持调节发射功率的终端设备。可替换地也可考虑，即使将涉及不支持调节的终端设备PC，也可有意识地执行第二步S2。在这种情况下，监听保护仅仅由此被保证，即接入点AP在第三步S3中将他的发射功率降低到一个值，该值将第一无线电覆盖区N1限制在近场上。

相反，如果该终端设备PC支持发射功率的调节（如针对该实施例所假设的那样），则既通过在第三步S3中接入点AP的发射功率的降低又通过在第四步S4中终端设备PC的发射功率的降低来保证可能的窃听者LA的防御。

紧接着此，在第五步S5中完成检查，终端设备PC是否位于接入点AP的第一无线电发射/无线电接收装置TRX1的有效距离中，其中这例如由此来实现，即在终端设备PC方面不向接入点传送应答。

第五步S5在回路中如此长地重复，也就是说向终端设备PC发送询问，直到接收一个应答，以至于该终端设备位于接入点的近场中是明显的。

为了加速或支持这一点，可替换地或补充地利用信令在第二步中也可传送消息，该消息促使终端设备PC给他的用户对此的提示，即用户利用针对配对过程的终端设备必须进入接入点AP的近场中。

可替换地，与第五步结合，这些要求可一次完成和/或按照每个否定的检测结果周期性地重复，以向用户给出关于此的反馈，即该用户最终还没有足够接近接入点AP。

如果在第五步S5中得到检测结果，即该终端设备PC位于接入点AP的近场中，如图1中所示，则在第六步S6中可以开始真正的配对过程并结束根据本发明的方法。

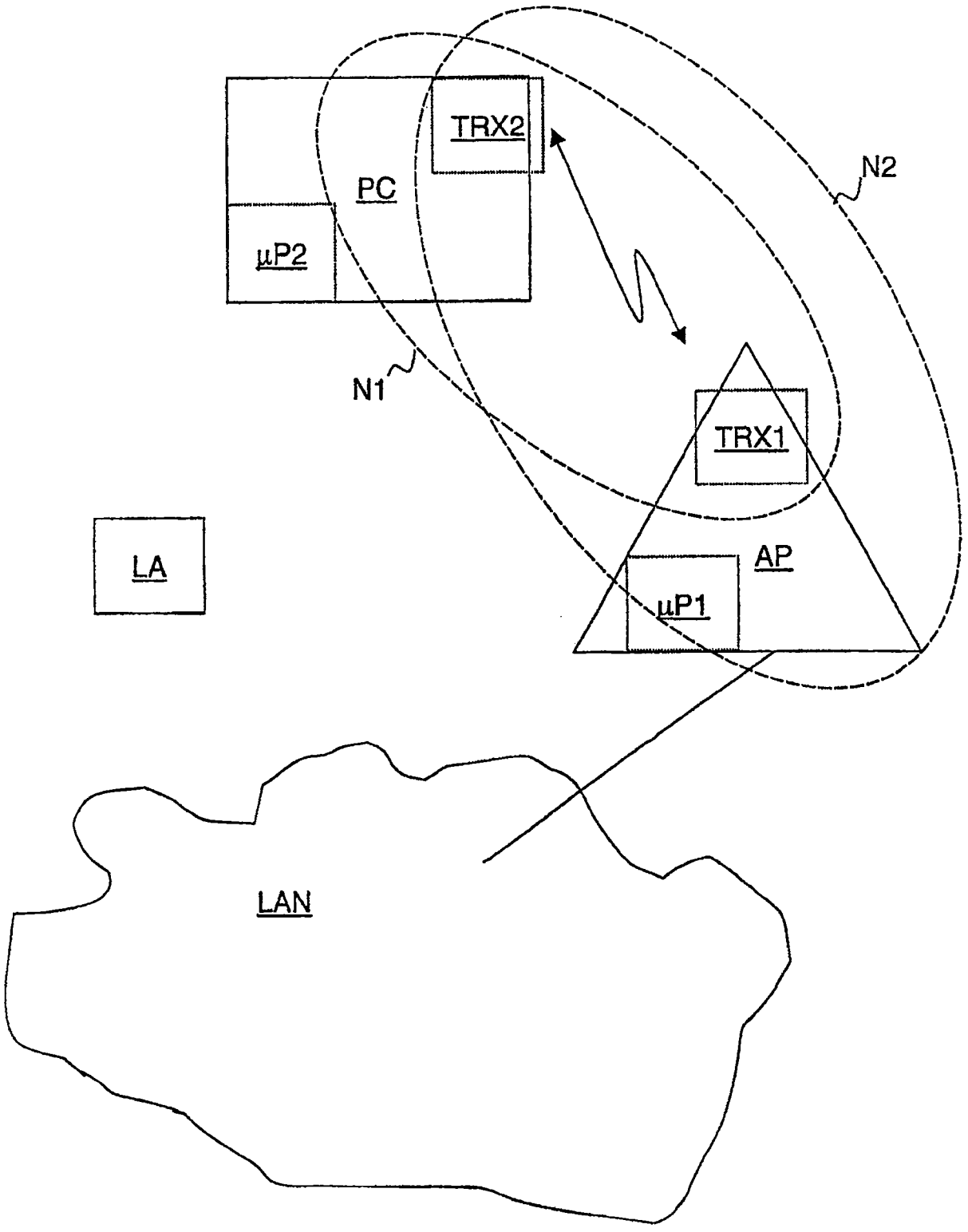


图 1

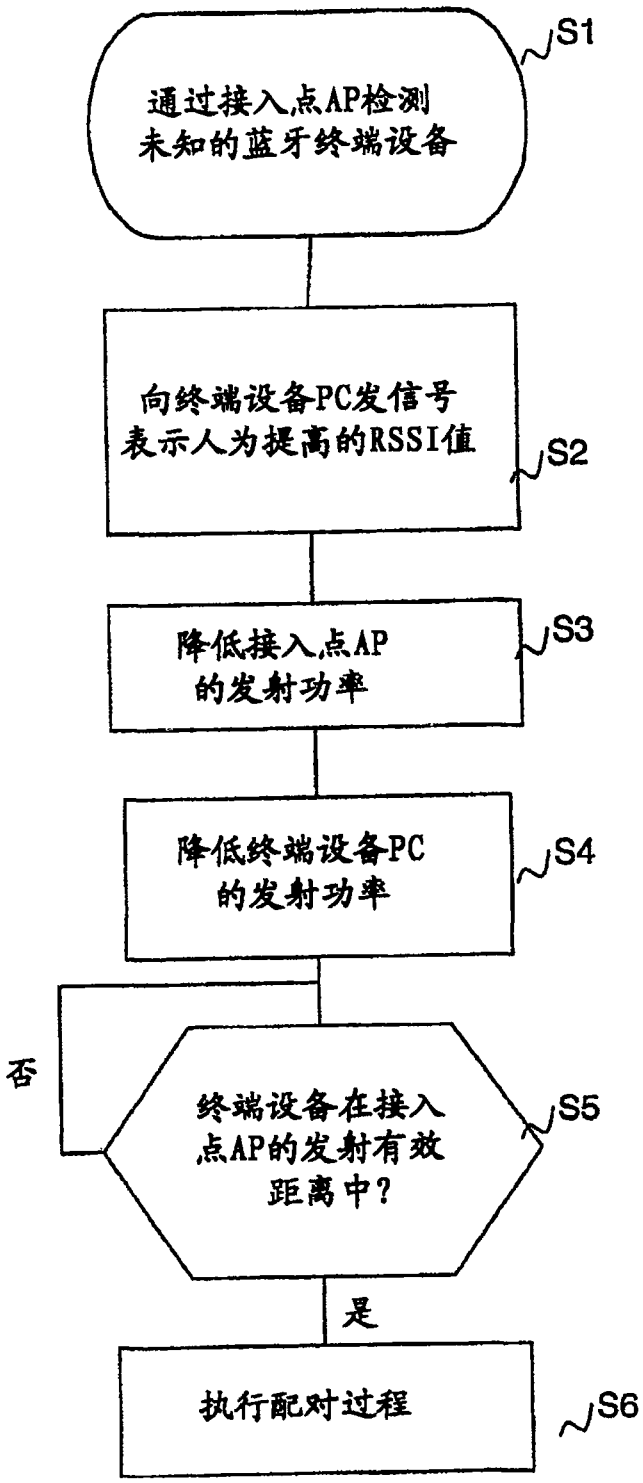

S1
通过接入点AP检测
未知的蓝牙终端设备
向终端设备PC发信号
表示人为提高的RSSI值
S2
降低接入点AP
的发射功率
S3
降低终端设备PC
的发射功率
S4
否
终端设备在接入
点AP的发射有效
距离中?
S5
是
执行配对过程
S6

图 2