基于已知异常的异常检测。 X 轴的每一段代表一个异常事件。 正常线上方是真实异常标签，正常线下方是我们模型的预测警报。 我们使用不同类别的模型来检测这些事件，观察网络的持续影响，并在大量异常事件发生时展示异常类别之间的关系。

即时零误报：如图、所示，我们用不同的异常模型可视化事件的识别。我们的实验表明，可以立即识别异常。我们还发现，异常发生后，网络中的重路由会持续一段时间。

不同异常类别的关系：对于TTNet（AS9121）和IndoSat（AS4761）事件，我们可以观察到可以准确识别出路由泄漏引起的中断。我们还可以发现，该路由在中断后会立即重新路由，并带有大量新的路由路径，我们的模型将其识别为路由劫持。此外，对于TM（AS 4788）和AWS（AS 200759），虽然发生了路由泄漏，但并没有导致网络中断，说明这两个网络对异常的鲁棒性更强。通过这样的分析，我们发现了当大量异常事件发生时异常类别之间的关系。同时，这突出了我们的方法在其他数据集上的推广。

These include data from Turkish Telecom (TTnet) [3], Indosat (Indonesia) [42], Telecom Malaysia (TM) [2], and the attack on Amazon Web Services (AWS) [4].

