1.ML+NIDS：[16],[17],[18],[19]

2.DM+DA: [24]

3.DM/ML+NIDS:[25]

4.DL+NIDS:[13]

5.SURVEY:DM,DL,ML,BIGDATA:[26]

6.ML+IDS:[27]

7.IOT+IDS:[28],[8]

IDS：a combination of software and hardware which monitors network or systems to identify malicious activities.

NIDS：

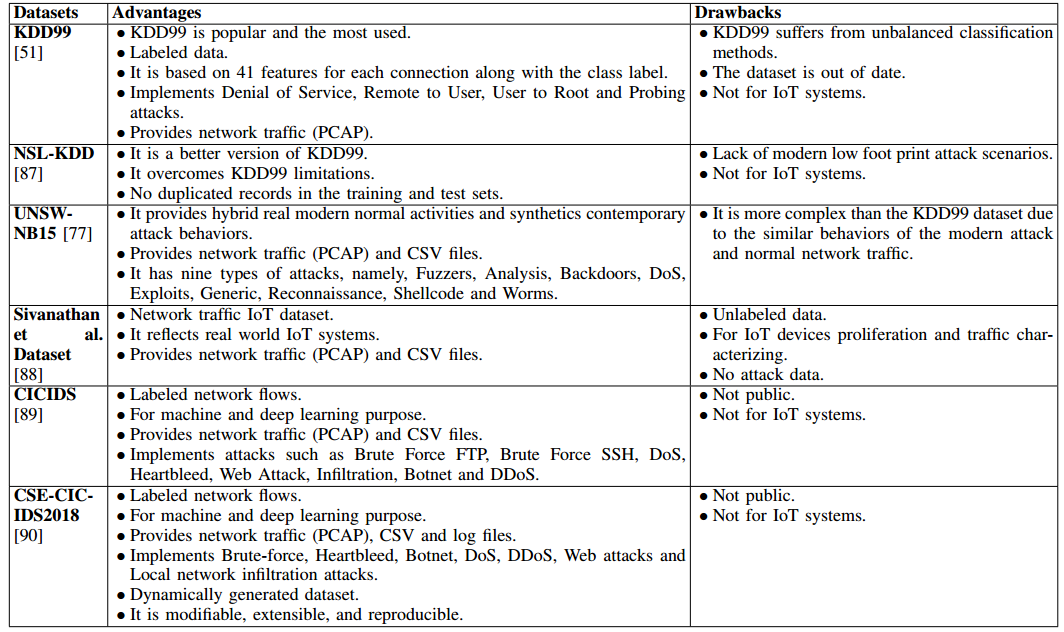
a.基于签名(误用检测)：输入非法规则

b.基于异常:对正常流量进行建模，与正常模型产生偏差即认为异常

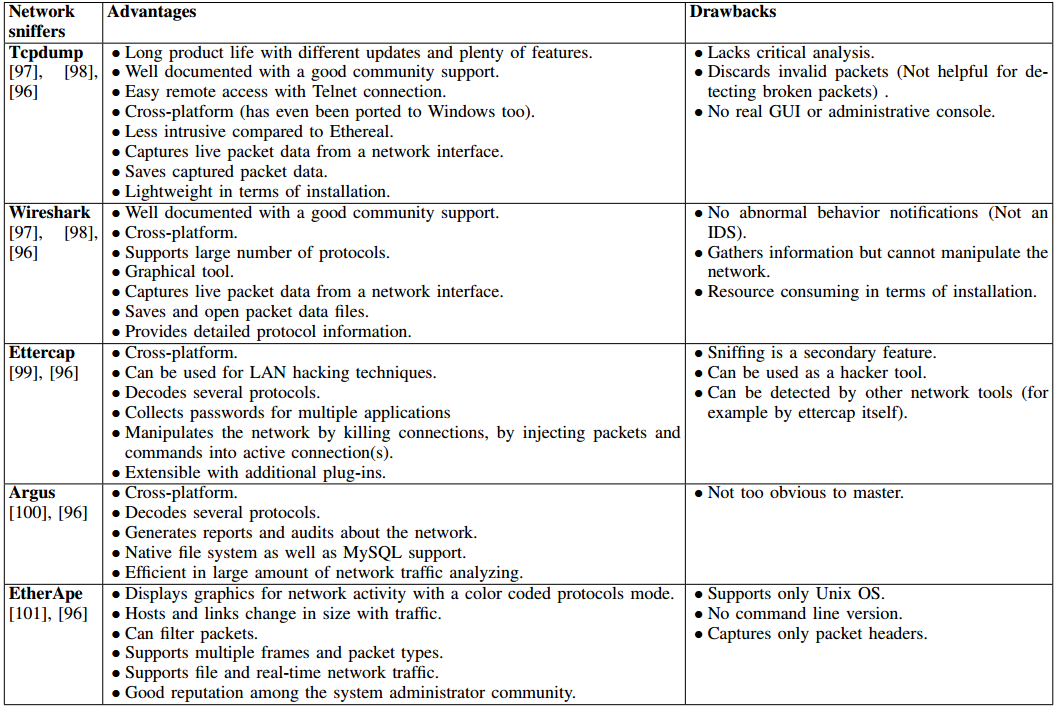
c.基于规范:手动输入合法的规则

d.混合检测

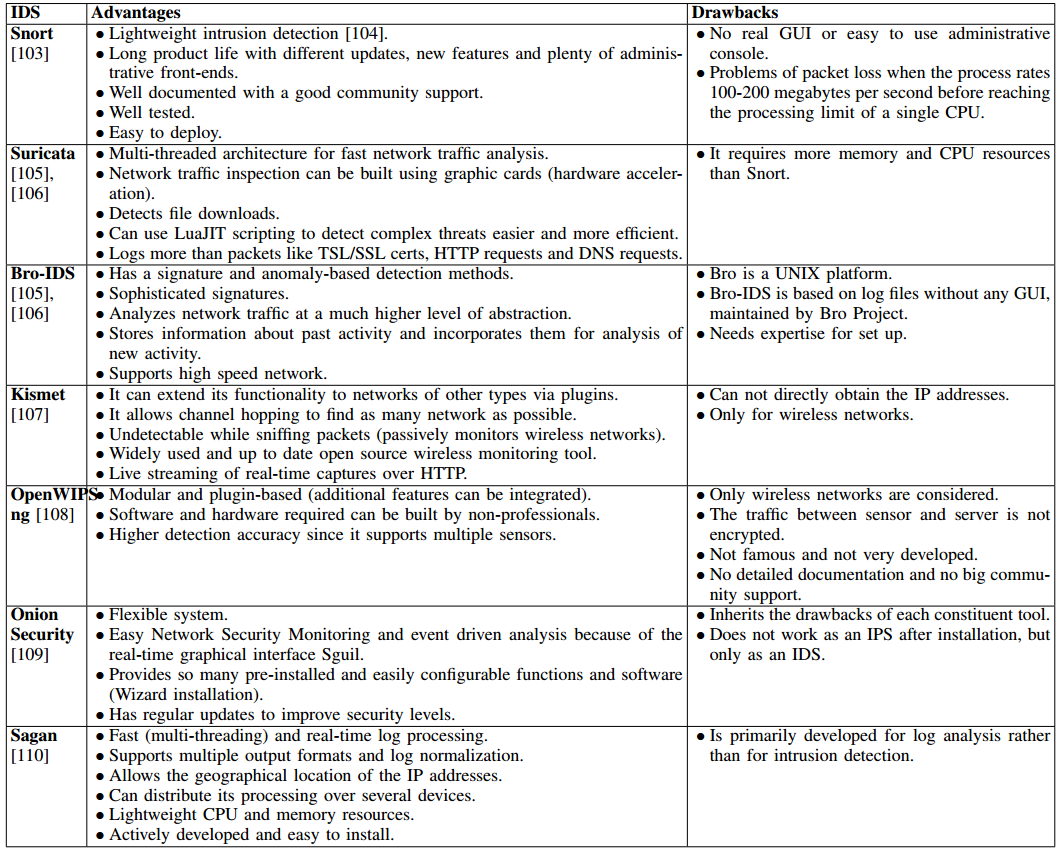
部署：一个系统检测整个网络更适合物联网，但小型物联网仍需要NIDS

数据集：

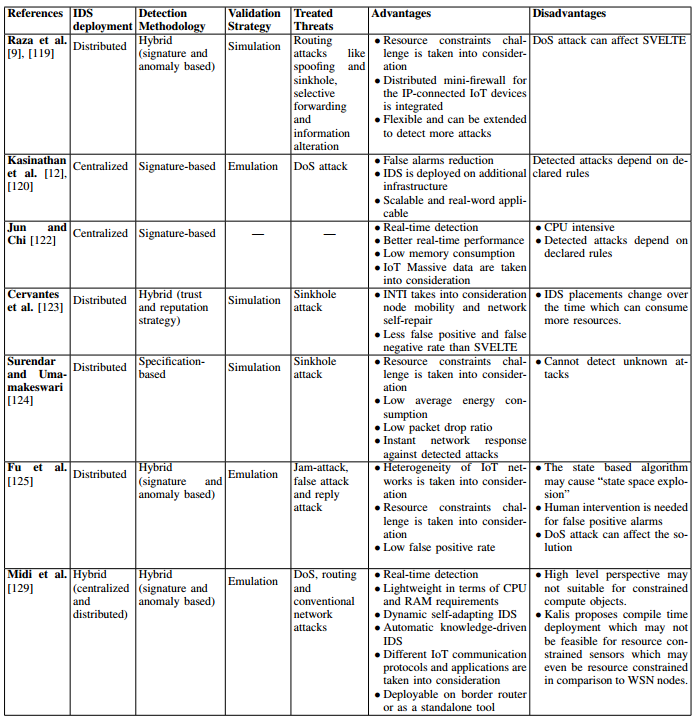
网络嗅探器：

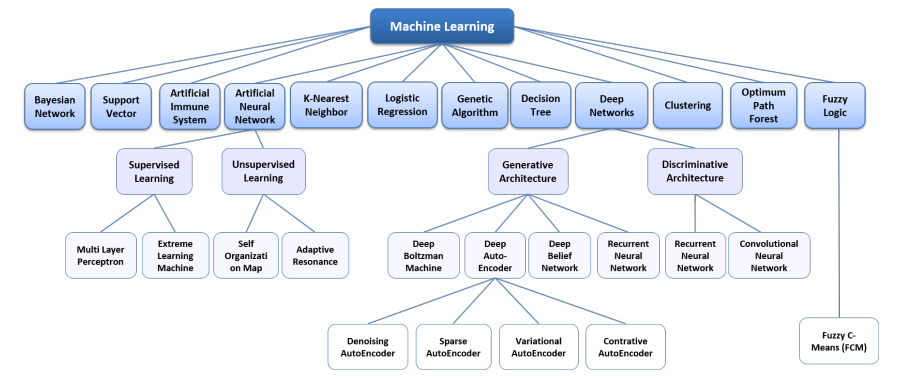


开源NIDS：

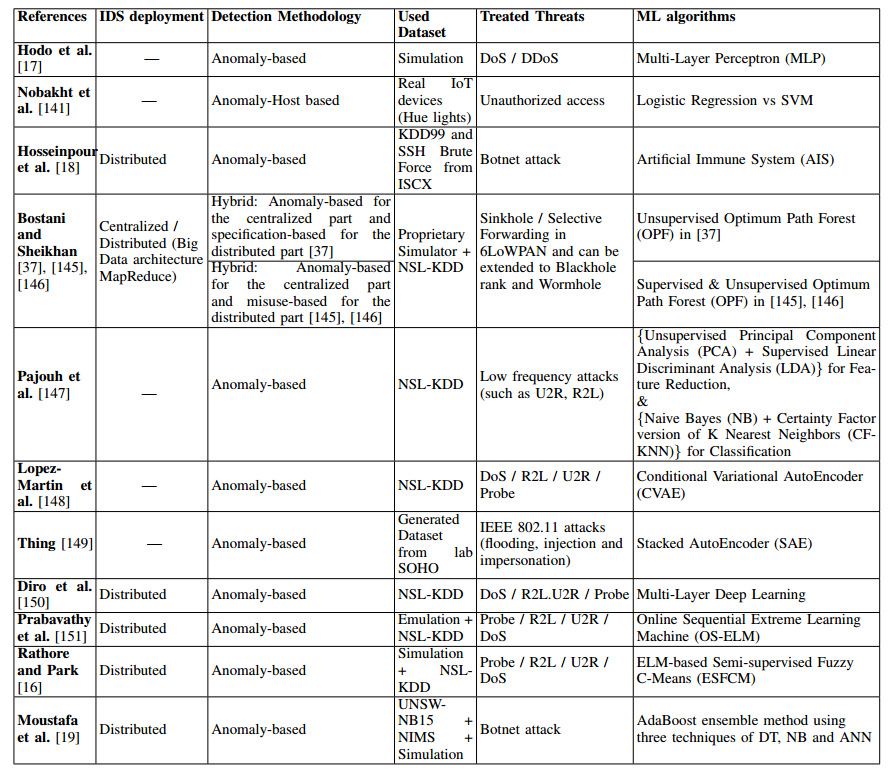


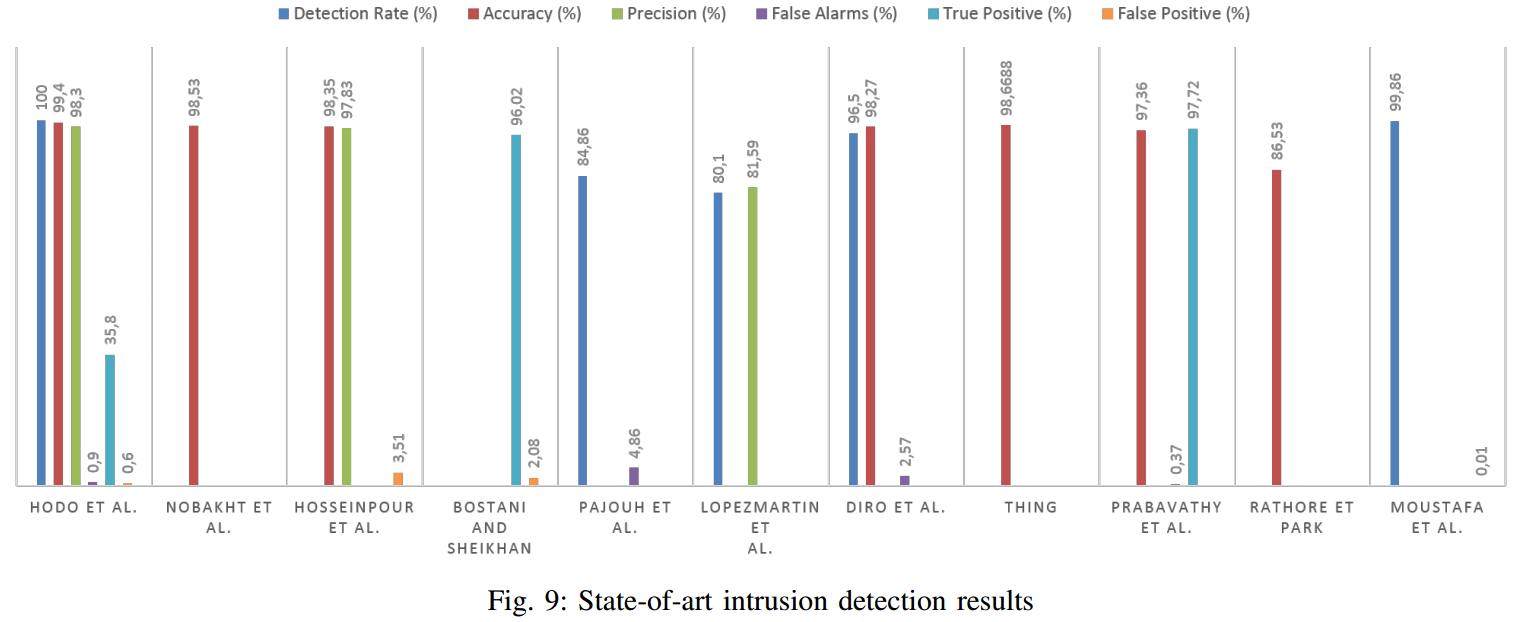
IOT NIDS:



机器学习：

IOT+LEARNING+NIDS：



Result: 

趋势：边缘计算和雾计算，边缘计算则是在设备上，雾计算计算在局域网级别。

基于学习技术的入侵检测系统存在“结果与操作解释之间的语义鸿沟”。不幸的是，基于学习技术的入侵检测系统通常以准确率、误判率和假阴性率进行评估。我们认为仅仅提供这些指标是不够的。研究人员应该对结果进行解释，并理解特征选择和检测过程的语义。语义也有助于区分异常行为和恶意行为。因此，检测与学习过程之间的语义关系似乎是一个值得探讨的问题。

通过特征重构，特征降维加快运算，如自动编码器。

检测0日攻击和未知攻击

不区分协议进行检测