中国科学技术大学
University of Science and Technology of China

关于基于网络的入侵检测系统的调查

林静雯、胡冬寅、李锭轩

中国科学技术大学，信息安全系

2019 年 6 月 6 号

大纲

中国科学技术大学
University of Science and Technology of China

大纲

应用层	基于协议	利用NXDomain检测DGA 基于HTTP的恶意软件检测 基于HTTP的负载聚合技术
	基于内容	通过网页元素标识检测广告注入 基于非文本特征的钓鱼邮件检测
网络层 传输层	机器学习	使用TLS证书进行检测 使用数据报报头信息进行检测
	非机器学习	使用熵和评分方法检测 检测目标链路泛洪攻击 使用有限状态机检测TCP拥塞攻击
链路层 物理层	链路层	直接利用字节流进行入侵检测 基于802.11的欺骗与干扰检测
	物理层	基于信噪比的干扰攻击入侵检测

大纲

1 导言

2 NIDS 技术
- 应用层
- 网络层、传输层
- 链路层、物理层

3 未来方向

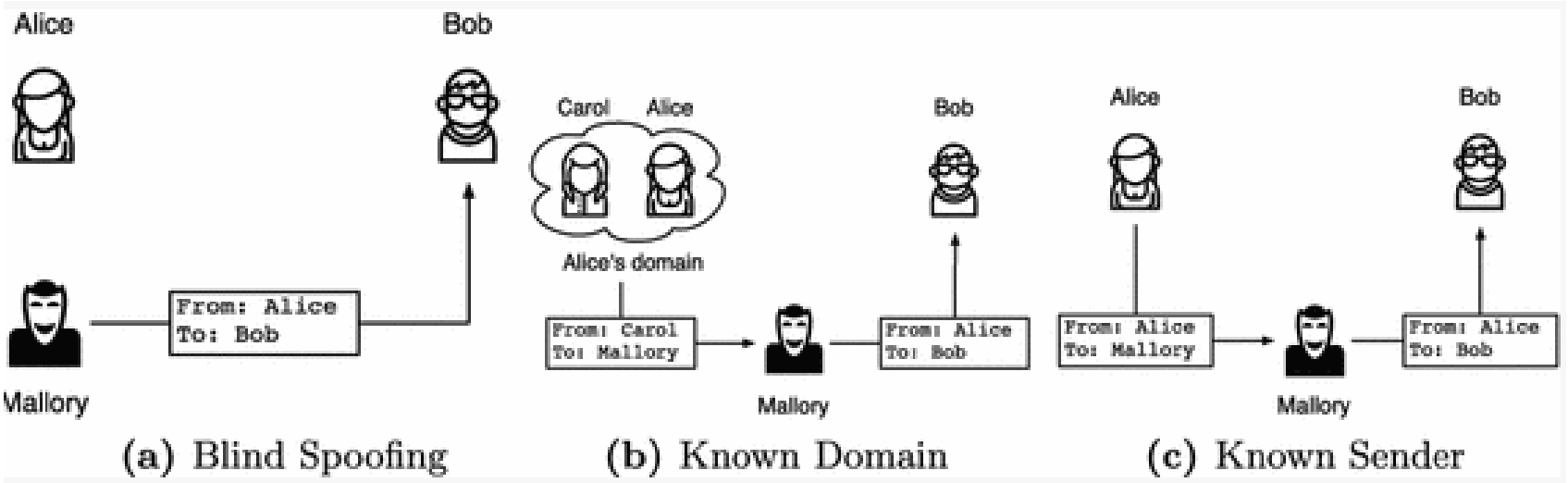
大纲

1 导言

2 NIDS 技术
- 应用层
- 网络层、传输层
- 链路层、物理层

3 未来方向

鱼叉式钓鱼邮件检测


Alice
Bob
From: Alice
To: Bob
Mallory
(a) Blind Spoofing
Carol
Alice
Alice's domain
From: Carol
To: Mallory
Mallory
Bob
From: Alice
To: Bob
(b) Known Domain
Alice
From: Alice
To: Mallory
Mallory
Bob
From: Alice
To: Bob
(c) Known Sender

鱼叉式钓鱼邮件检测

行为特征	是否使用数字签名
	附件类型和顺序
	使用抄送或者收件人
组成特征	公共头标的顺序和语法
	主题字段中的国际字符编码
	电子邮件地址的格式
传输特征	Received 头标的数量和顺序
	Received标头中提供的TLS功能

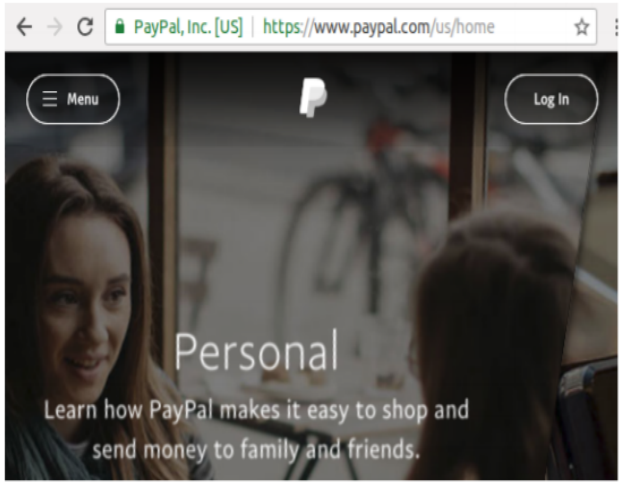
大纲

1 导言

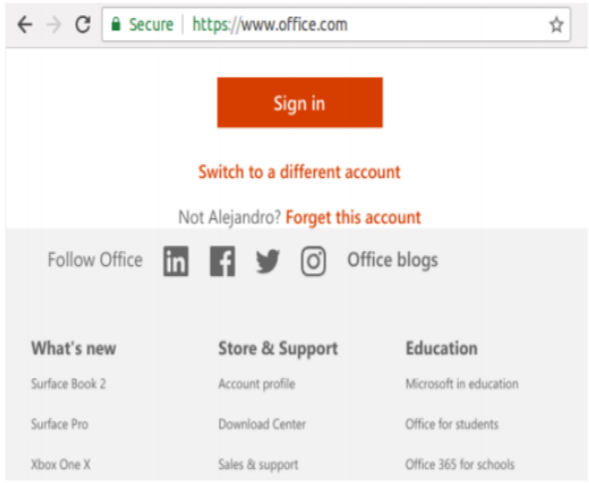
2 NIDS 技术

- 应用层
- 网络层、传输层
- 链路层、物理层

3 未来方向

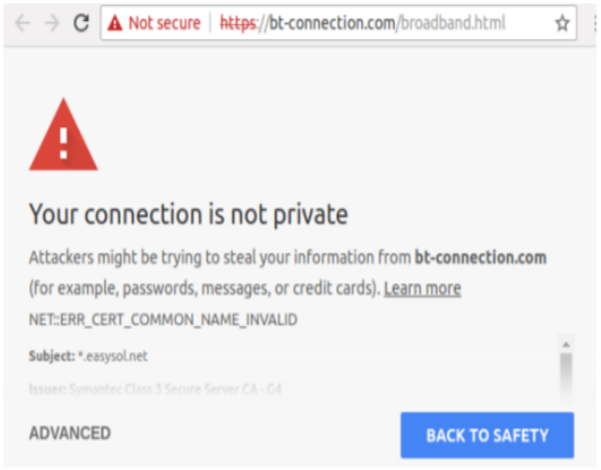


(a) Extended validation message.



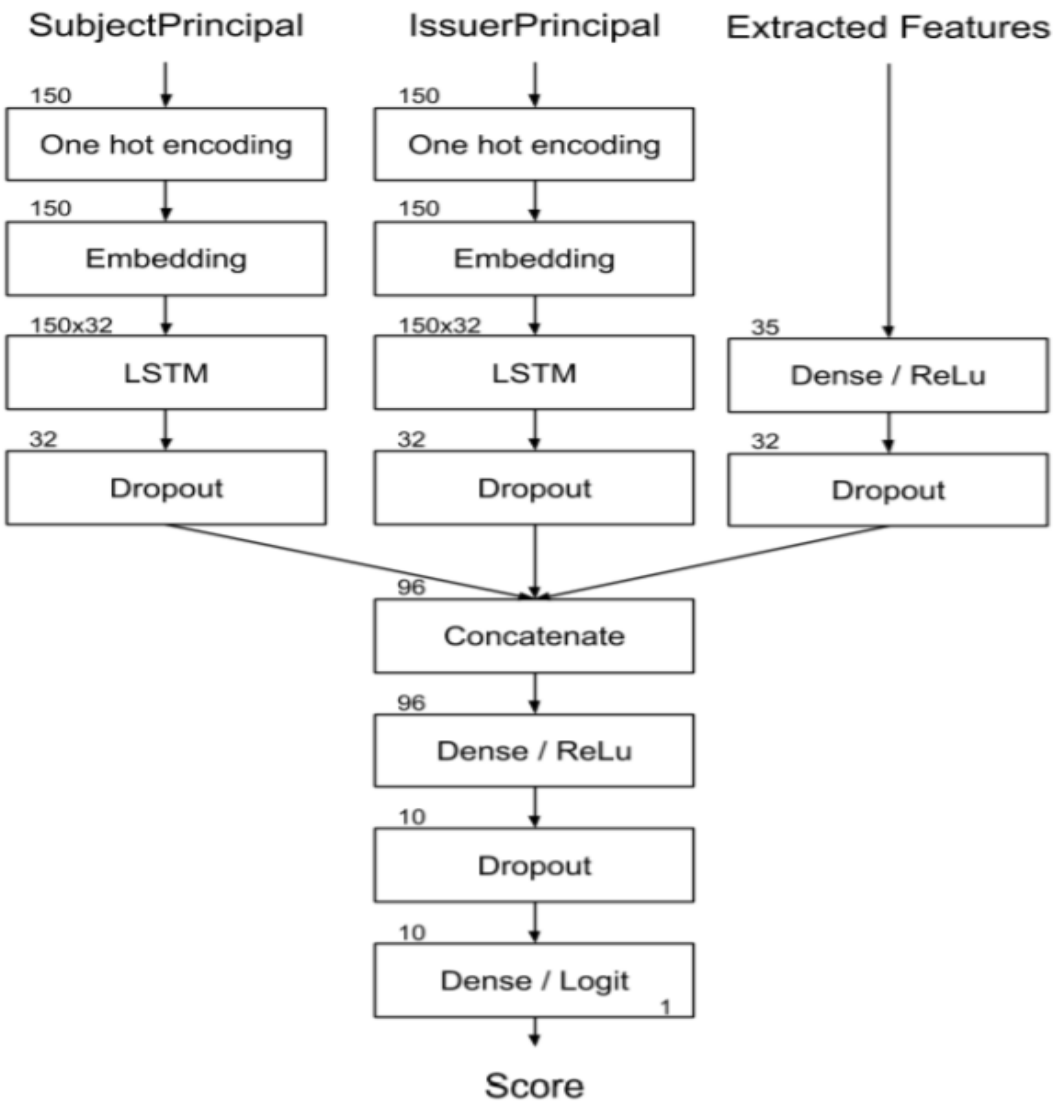
(b) Domain validation and organization validation message.

(c) No validation message.

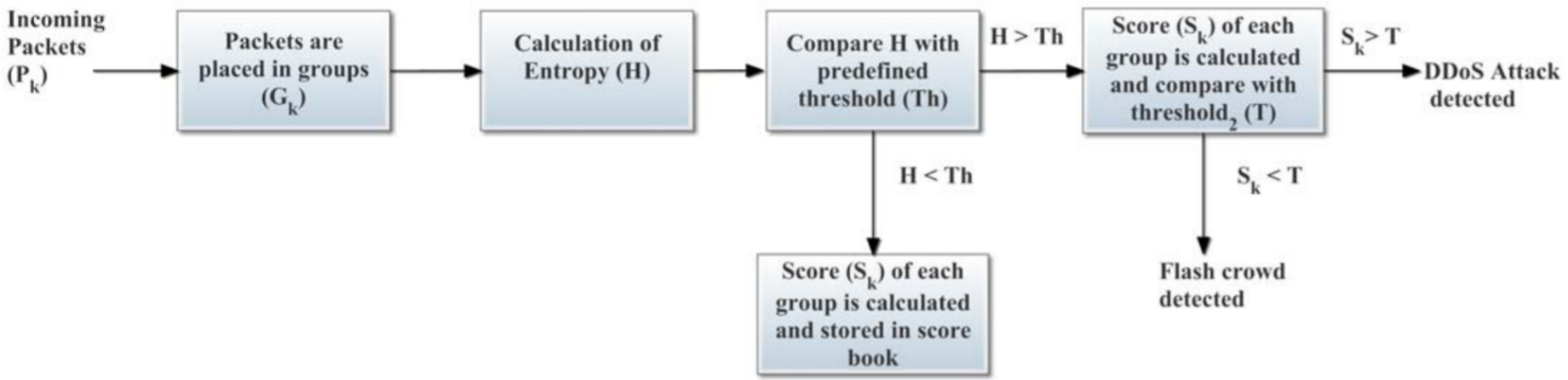


(d) Broken certificate message.

机器学习方法


SubjectPrincipal
IssuerPrincipal
Extracted Features
150
One hot encoding
150
Embedding
150x32
LSTM
32
Dropout
150
One hot encoding
150
Embedding
150x32
LSTM
32
Dropout
35
Dense / ReLu
32
Dropout
96
Concatenate
96
Dense / ReLu
10
Dropout
10
Dense / Logit
1
Score

非机器学习方法


Incoming Packets (P_k)
Packets are placed in groups (G_k)
Calculation of Entropy (H)
Compare H with predefined threshold (Th)
H > Th
Score (S_k) of each group is calculated and compare with threshold$_2$ (T)
S_k > T
DDoS Attack detected
H < Th
Score (S_k) of each group is calculated and stored in score book
S_k < T
Flash crowd detected

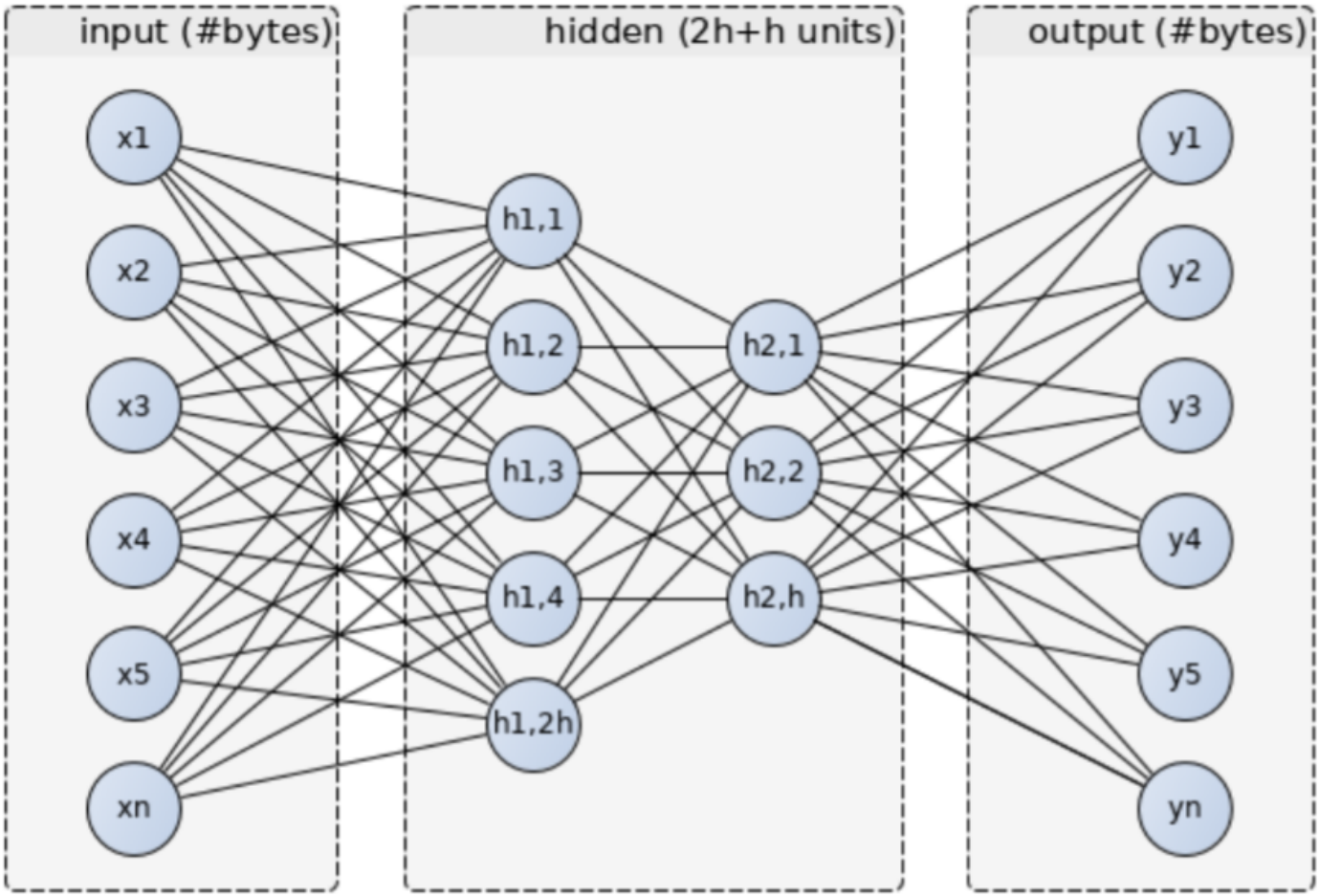
大纲

1 导言

2 NIDS 技术
- 应用层
- 网络层、传输层
- 链路层、物理层

3 未来方向

利用字节流的入侵检测


input (#bytes)
hidden (2h+h units)
output (#bytes)
x1
x2
x3
x4
x5
xn
h1,1
h1,2
h1,3
h1,4
h1,2h
h2,1
h2,2
h2,h
y1
y2
y3
y4
y5
yn

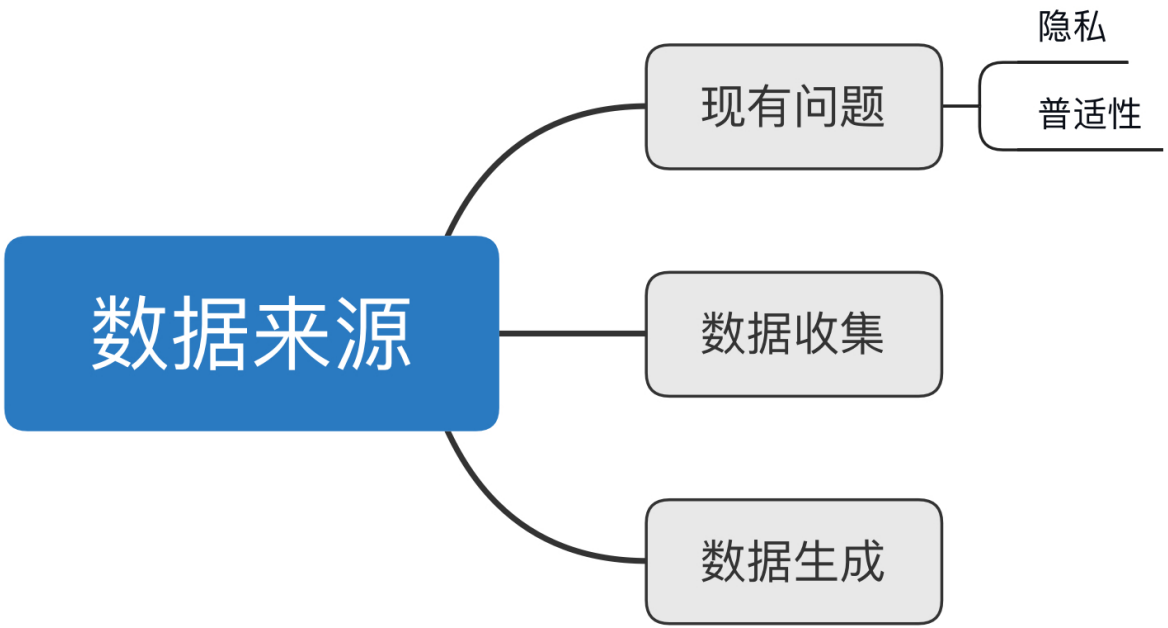
大纲

中国科学技术大学
University of Science and Technology of China

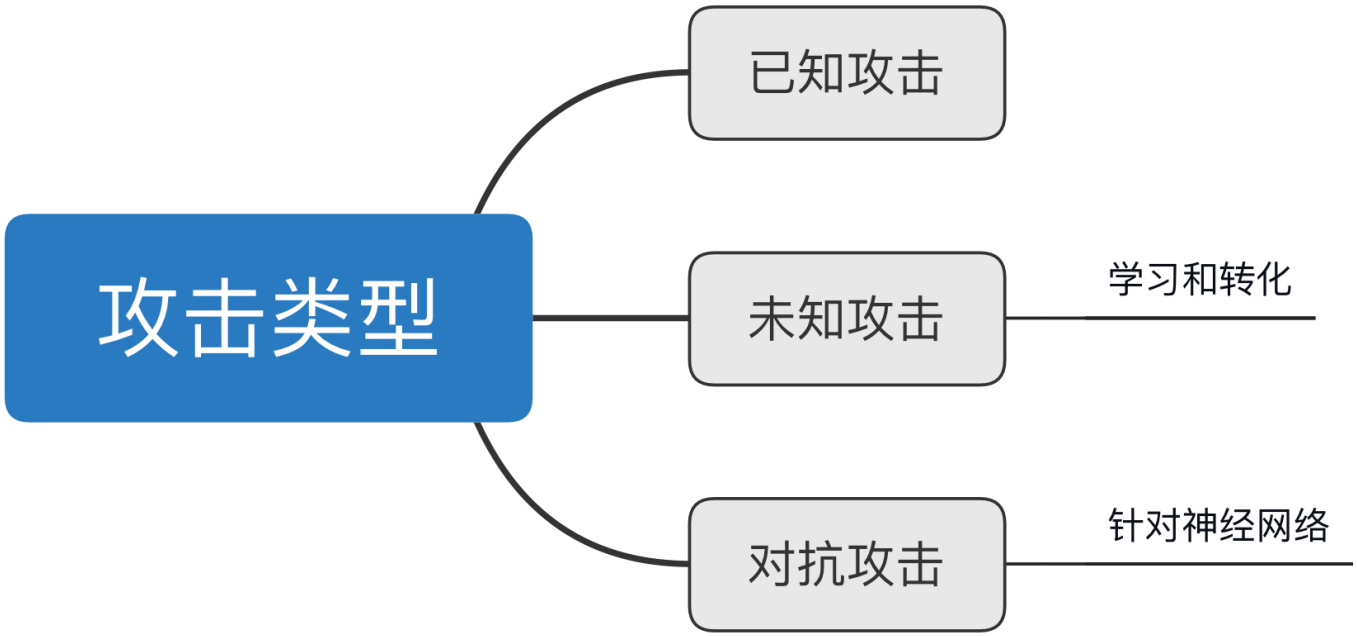
未来方向

- 数据来源
- 面向连接型网络
- 协议栈各层
- NIDS 检测的攻击类型
- 使用非统计方法

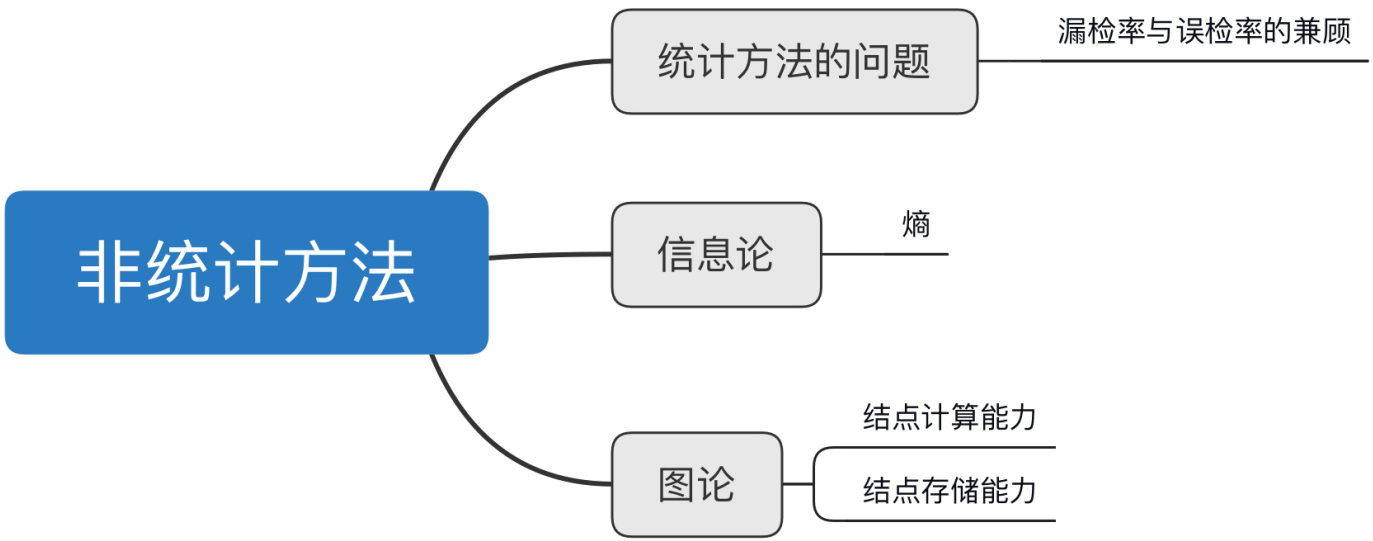
数据来源



攻击类型



非统计方法



谢谢!