动态双绑：
一种ARP缓存污染解决方案

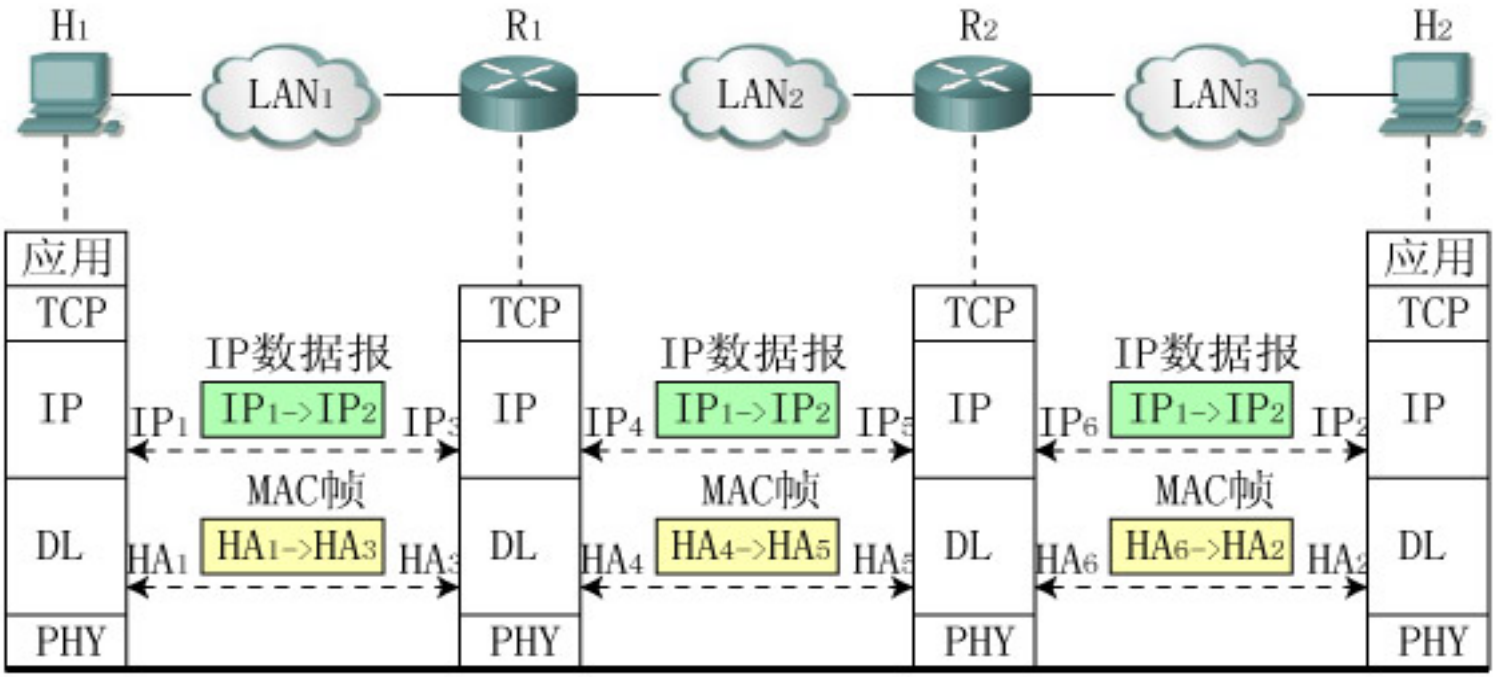
北京大学　计算中心

2008年10月

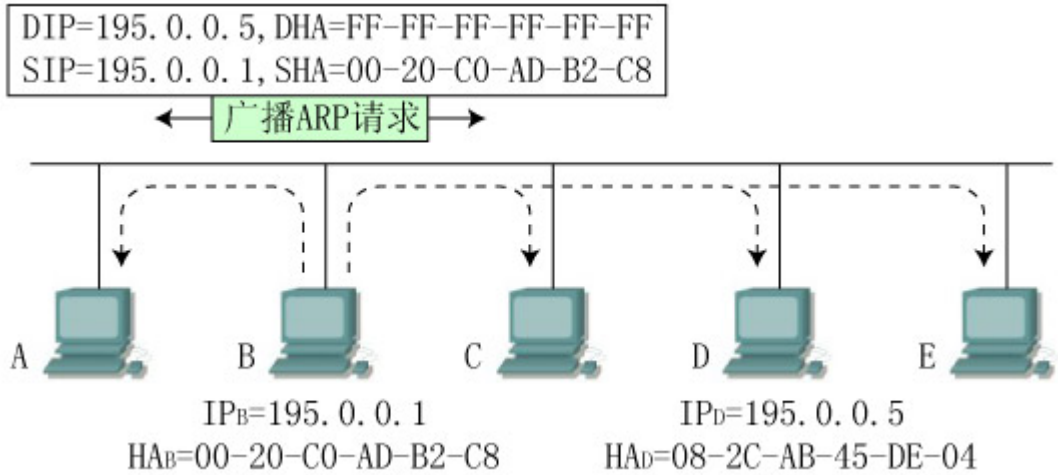
引言

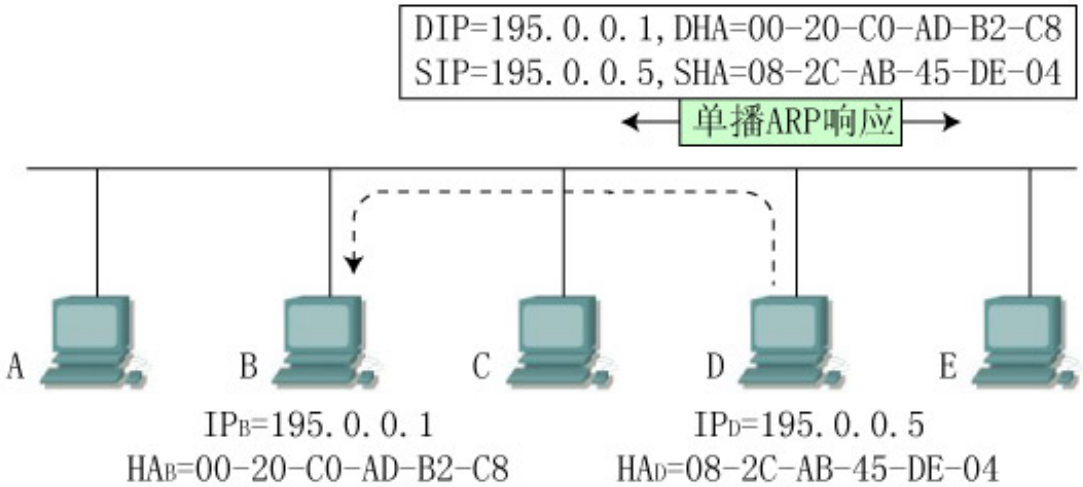
- ARP协议位于第二、三层之间
  ARP协议是脆弱的
  ARP协议是必不可少的
- ARP缓存污染攻击
- 保护网关及主机的ARP缓存

IP/MAC映射


H1
R1
R2
H2
LAN1
LAN2
LAN3
应用
TCP
IP
DL
PHY
IP数据报
IP1->IP2
IP1
IP3
IP4
IP5
IP6
IP2
MAC帧
HA1->HA3
HA1
HA3
HA4->HA5
HA4
HA5
HA6->HA2
HA6
HA2

ARP的请求和响应


DIP=195.0.0.5, DHA=FF-FF-FF-FF-FF-FF
SIP=195.0.0.1, SHA=00-20-C0-AD-B2-C8
广播ARP请求
A
B
C
D
E
IPB=195.0.0.1
HAB=00-20-C0-AD-B2-C8
IPD=195.0.0.5
HAD=08-2C-AB-45-DE-04


DIP=195.0.0.1, DHA=00-20-C0-AD-B2-C8
SIP=195.0.0.5, SHA=08-2C-AB-45-DE-04
单播ARP响应
A
B
C
D
E
IPB=195.0.0.1
HAB=00-20-C0-AD-B2-C8
IPD=195.0.0.5
HAD=08-2C-AB-45-DE-04

ARP缓存污染的方法

- 伪造ARP响应
- 伪造ICMP ECHO请求
- 监听ARP请求

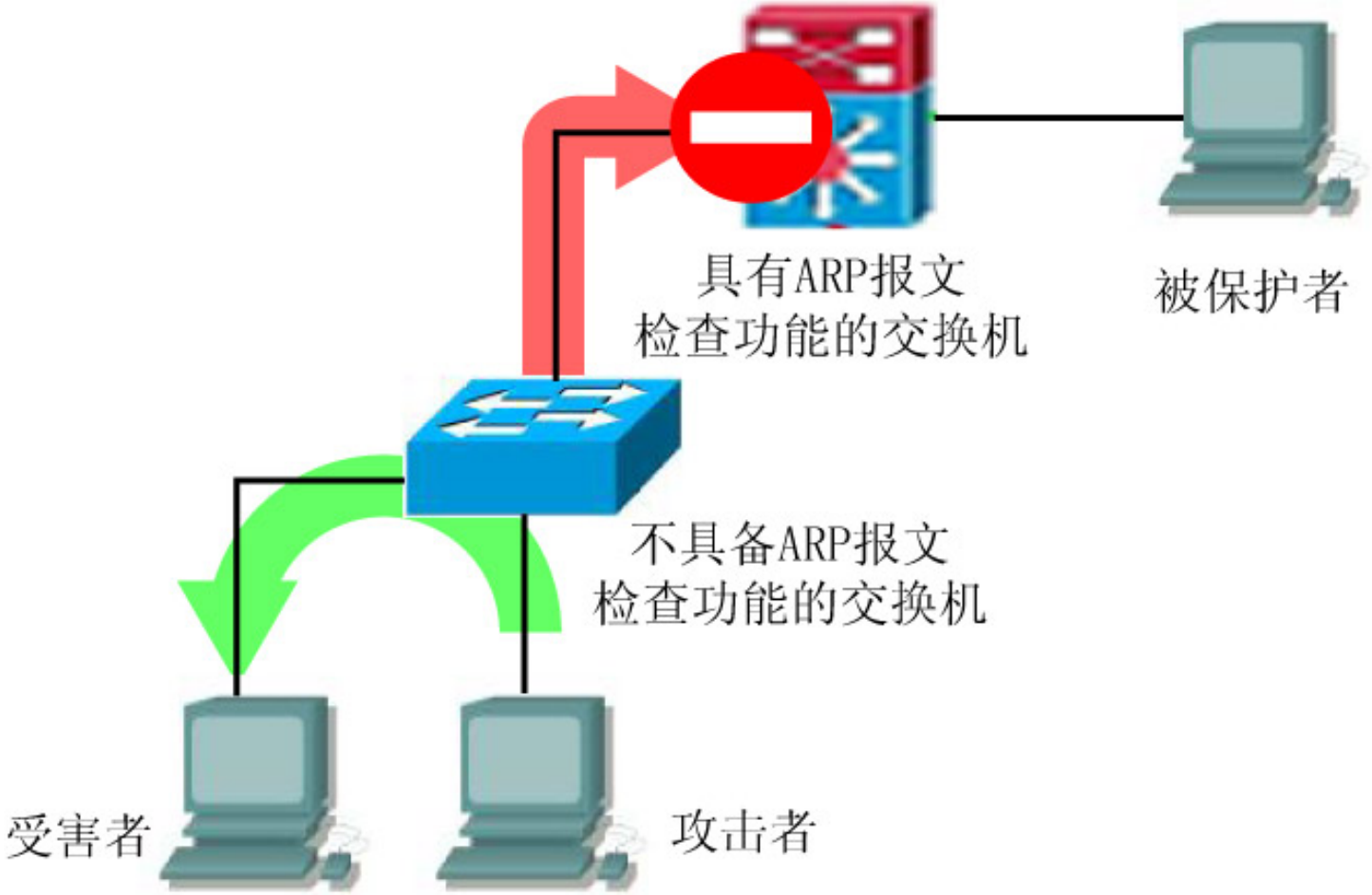
利用ARP的攻击

- DoS
- 角色冒充
- 中间人攻击

相关的工作

- 进行安全加密改造
- 缓存污染攻击探测
- 静态绑定网关的IP-MAC
- 网络设备厂商的工作

网络现状分析



解决方案的主要思想

- 保护网关和主机间的通信
- 保护DNS与主机间的通信
- 解决方法
  - 交换机ARP报文检查
  - 网关IP-MAC绑定
  - 主机IP-MAC绑定

DNS服务器的保护

- DNS服务器置于安全网段
- 被具备ARP报文检查功能的交换机与网段内的其他主机分开。

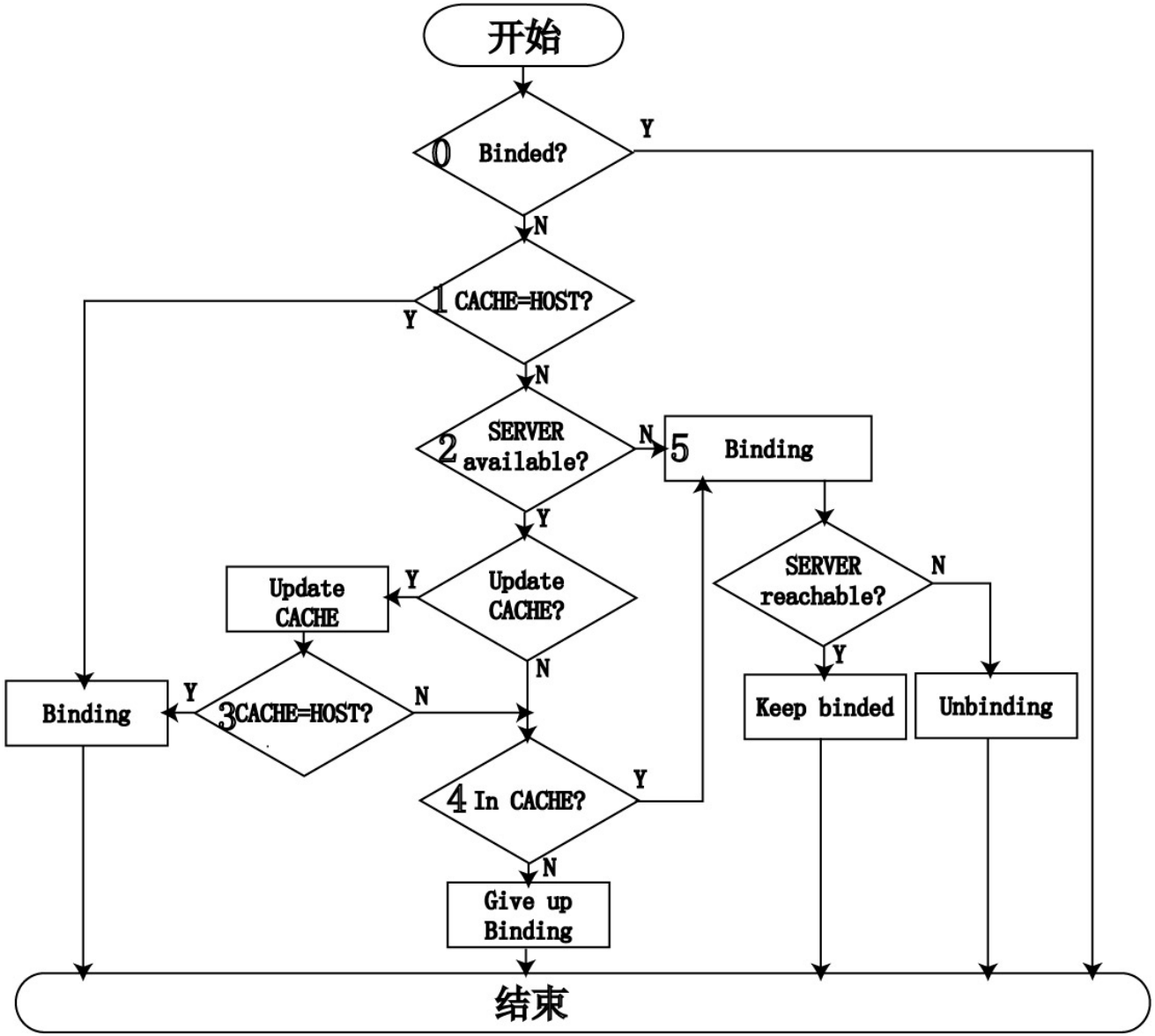
解决方案的组成

- 基准服务器
- 主机端IP-MAC绑定算法
- 由交换机支持的ARP报文检查功能
- 动态网关IP-MAC绑定

基准服务器

- 提供网关IP-MAC对应关系
- 提供最新版本的时间戳
- 加密访问
- 允许ICMP ECHO请求

主机IP-MAC绑定算法



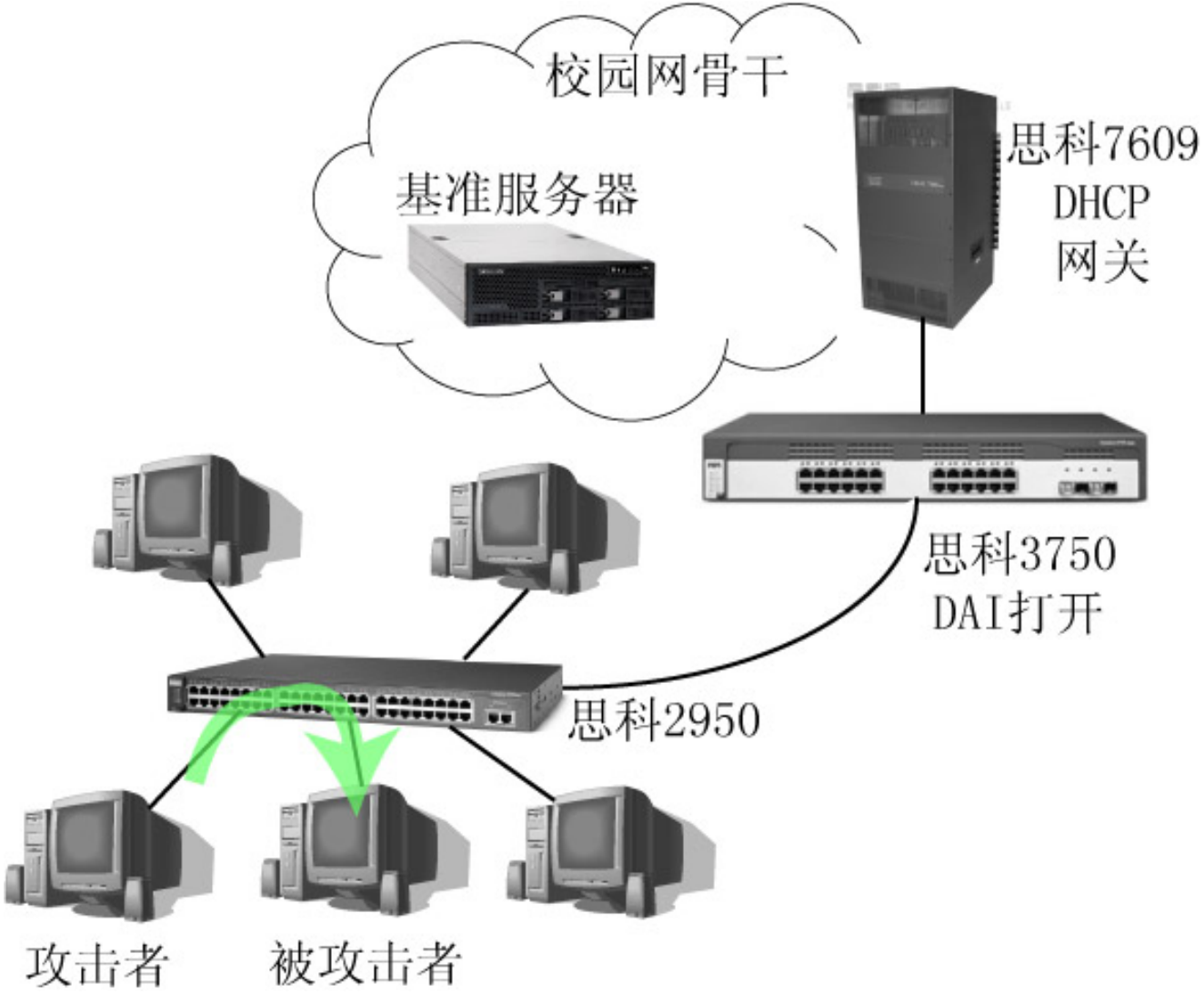
ARP报文检查

- IP-MAC-Interface对应关系
  - 利用DHCP Sooping
  - 管理员手工配置
- 检查进入交换机的报文
- 位于网关和主机之间

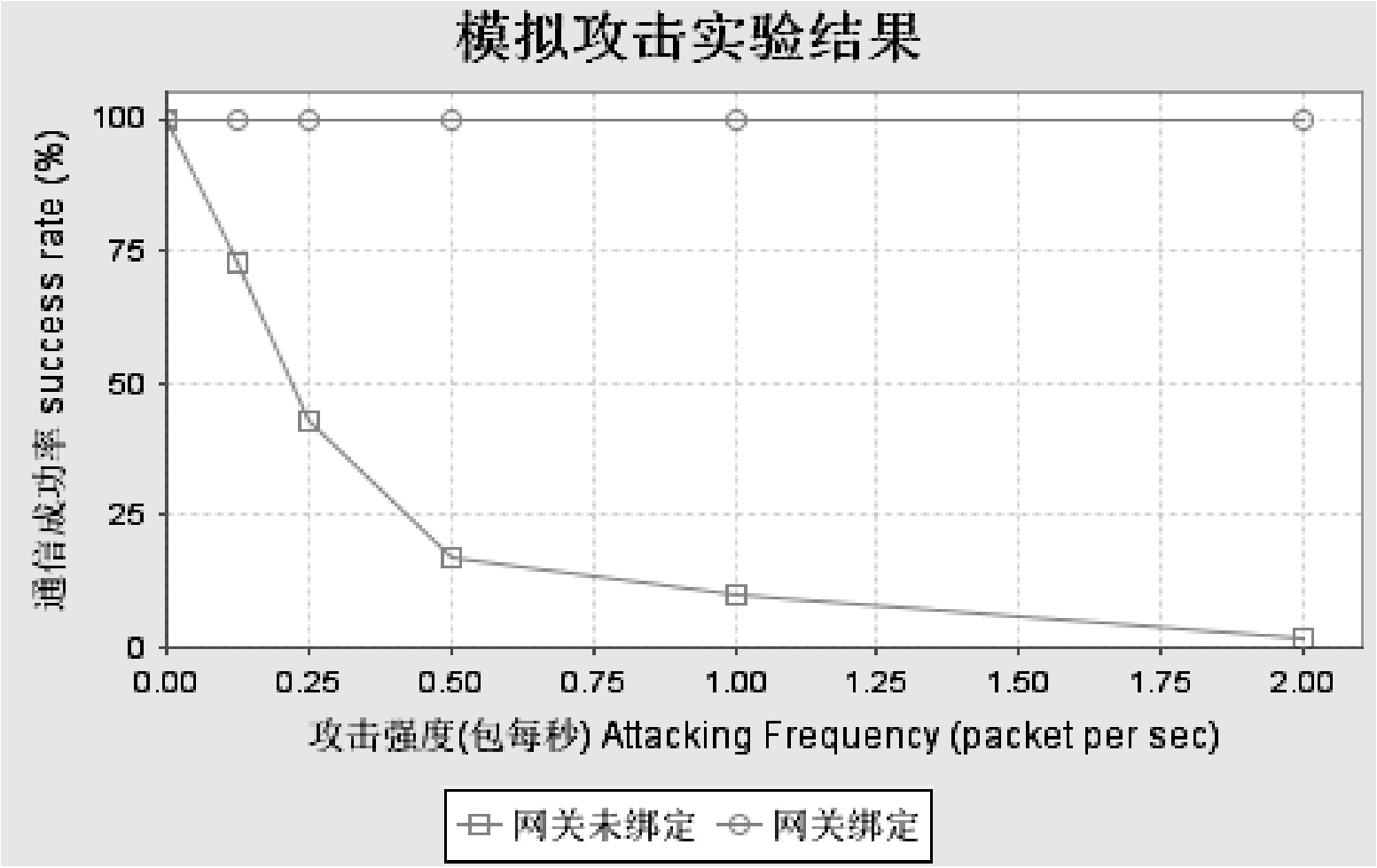
网关IP-MAC绑定

- 部署在基准服务器上
- 从DHCP服务器获得IP-MAC对应关系
- 通过SNMP设定网关上的IP-MAC对应关系

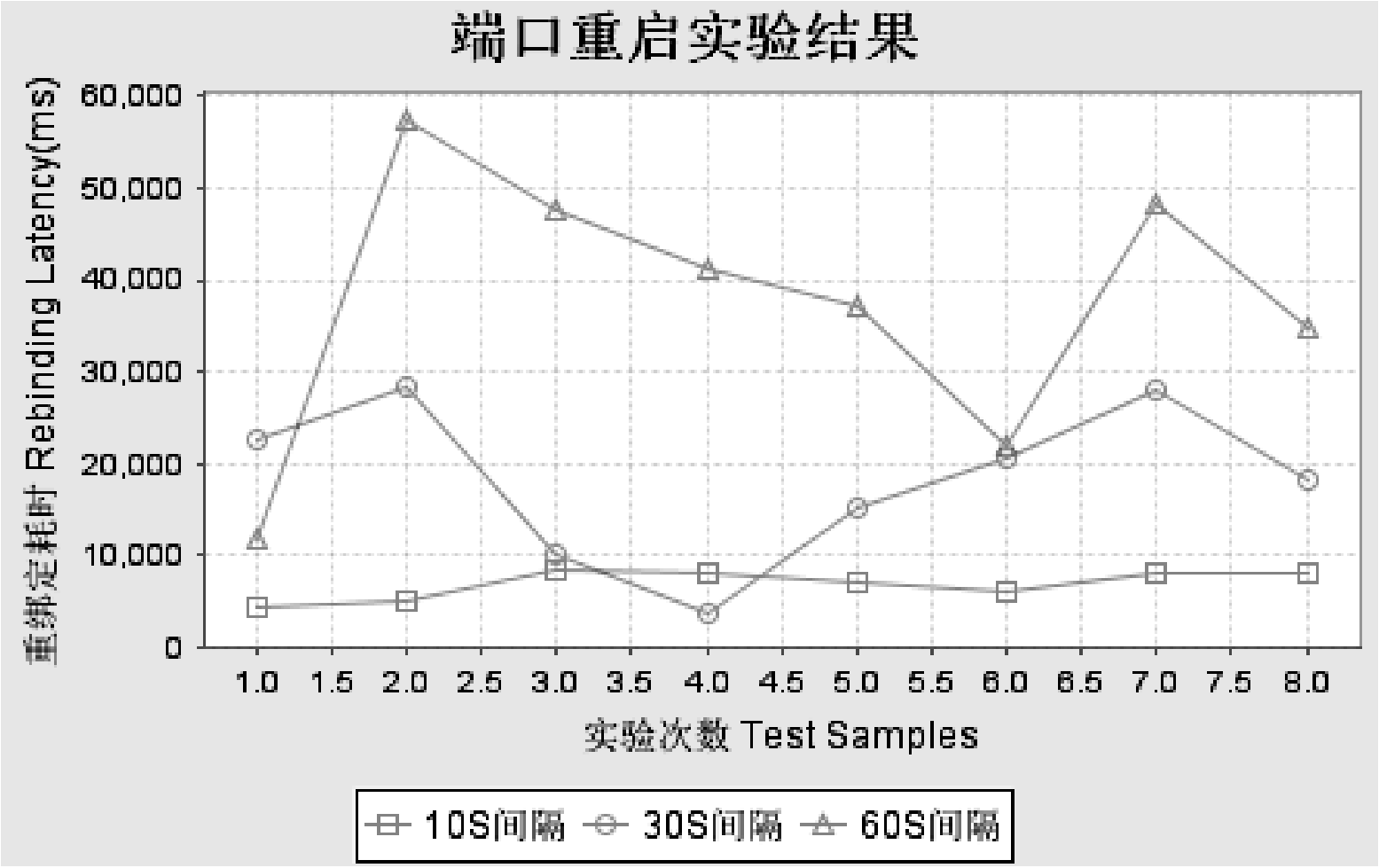
实验环境



模拟实验结果


模拟攻击实验结果
通信成功率 success rate (%)
100
75
50
25
0
0.00
0.25
0.50
0.75
1.00
1.25
1.50
1.75
2.00
攻击强度(包每秒) Attacking Frequency (packet per sec)
网关未绑定
网关绑定

端口重起实验结果


端口重启实验结果
重绑定耗时 Rebinding Latency(ms)
60,000
50,000
40,000
30,000
20,000
10,000
0
1.0
1.5
2.0
2.5
3.0
3.5
4.0
4.5
5.0
5.5
6.0
6.5
7.0
7.5
8.0
实验次数 Test Samples
10S间隔
30S间隔
60S间隔

结论

- 易于在校园网内部署
- 多种手段相互结合
- 确保主机对网关的通信
- 确保网关上ARP表的正确性

致谢

谢谢