Ad Hoc 安全防护

——Ad Hoc的安全分析和IDS模型

Benjurry

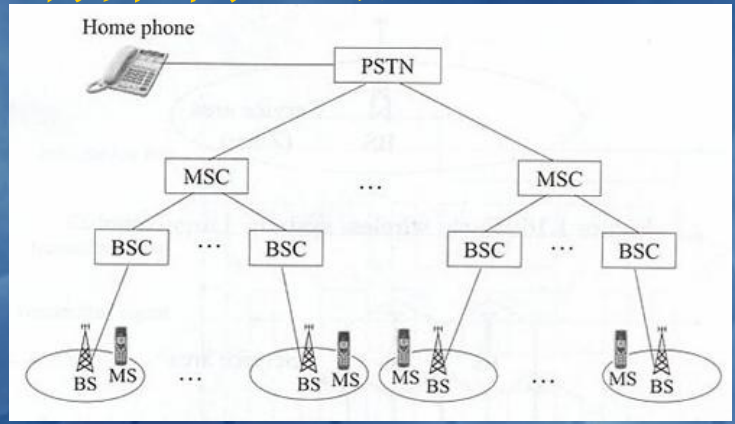
2002.12

主要内容

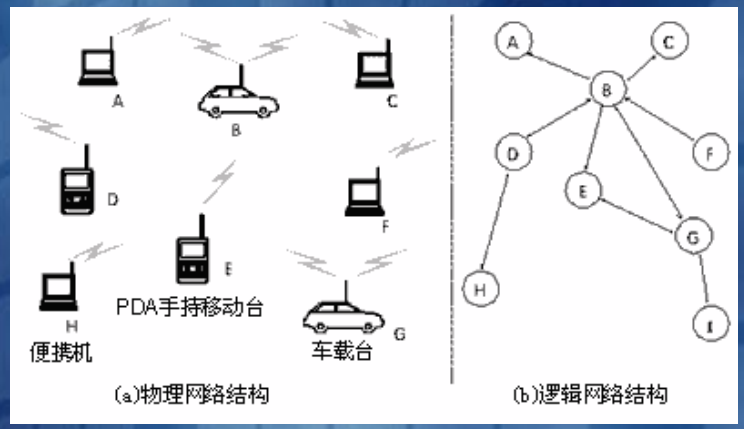
- Ad Hoc网络介绍
- Ad Hoc 路由分析
- Ad Hoc 安全分析
- Ad Hoc 鉴权路由
- Ad Hoc IDS模型设计

Ad Hoc 网络概述

- Infrastructure Networks :有架构网络
  - 常规有线网络
  - GSM通讯系统
  - 用AP连接的WLAN



- Infrastructureless Networks :无架构网络
  - Ad Hoc



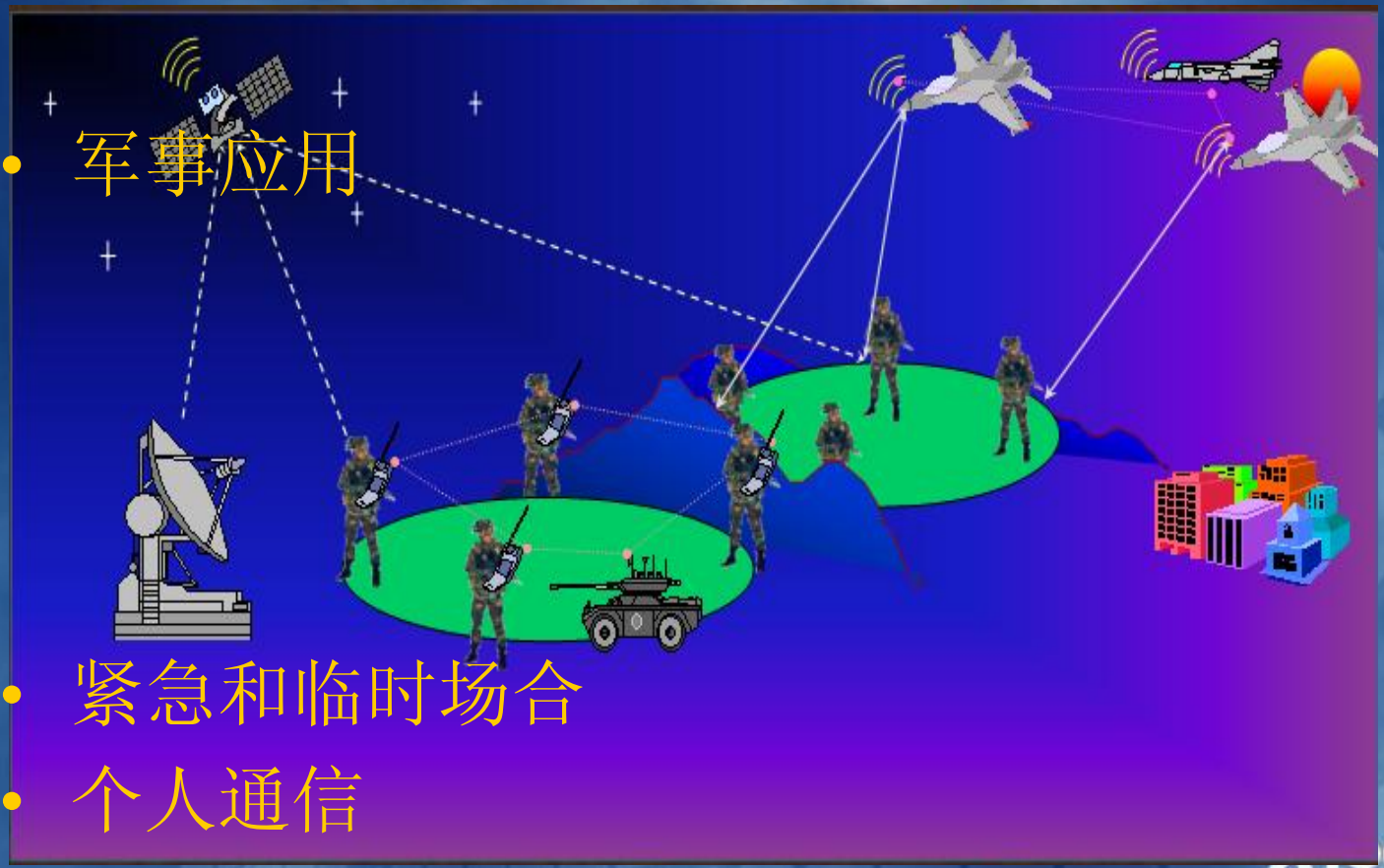
Ad Hoc网络历史

- 军事，美国DARPA
  - 1972年，分组无线网 （Packet Radio Network）
  - 1993年，高残存性自适应网络（SURAN, SURvivable Adaptive Network）
  - 1994年，全球移动信息系统 （GloMo,Globle Mobile Information Systems）
  - 1996年，联合战术无线网系统JTRS（Joint Tactical Radio System）
- 民用，IETF&IEEE
  - 1991年，IETF成立了移动Ad hoc网络工作组(MANET)
  - 1999年，RFC 2501给出了MANET的应用场合
  - 2000年, IETF在公布了一系列的有关Ad hoc 路由的草案
  - 2000年，IEEE成立Ad hoc技术分委员会

Ad Hoc网络特点

- 网络自主性
- 动态拓扑
- 带宽限制和变化的链路容量
- 能量限制节点
- 多跳通信
- 分布式控制
- 有限的安全性

Ad hoc网络的应用领域



- 军事应用
- 紧急和临时场合
- 个人通信

Ad Hoc 路由分析

- 先应式（Proactive）： 表驱动式（Table Driven）
  - 平路由方案（Flat Routing）：DSDV，WRP，FSR
  - 分级路由方案（Hierarchical Routing）：Bergano
- 反应式（Reactive）： 随选式（On-Demand)
  - LMR,AODV,DSR
- 混合式（Hybrid）： 区域路由（Zone）

DSR路由算法

DSR（Dynamic Source Routing）包括2个机制:

- 路由发现（Route Discovery）
- 路由维持（Route Maintenance）

DSR 路由发现

- 发起者本地广播一个route request包
- 每个节点接受route request包
  - 如果最近看到过从发起者发出的请求标识符，丢弃这个请求
  - 否则自己的节点地址添加到request包列表中，然后再次广播这个request包
- route request包到达目标节点，目标发送Route Reply返回给发起者，包含了Request包中所有累积的地址

DSR 路由维护

- 遇到Route Error包
- 发起者删除缓存路由表该记录
- 重新选择路由或者进行新的路由

DSR路由安全威胁

- 任意相邻结点之间盲目信任
- 路由协议字段可以被任意修改
- 假冒IP或者MAC攻击
- 伪造虚假路由信息攻击
  - 伪造路由错误消息
  - 路由缓存毒药
  - 路由表缓冲溢出攻击
- 无法探测和孤立错误动作结点
- 无法避免信息泄漏

鉴权路由

- 采用密钥管理，对每个结点信息进行认证
- 能够保证信息的完整性、机密性和不可抵赖性
- 用watchdog探测非法结点

鉴权过程

- 初步鉴权
  - 需要一个可信的认证服务器T
  - 每个结点得到一个证书
  - T->A:$Cert_A$ =[IP_A,K_A+,t,e]K_T-

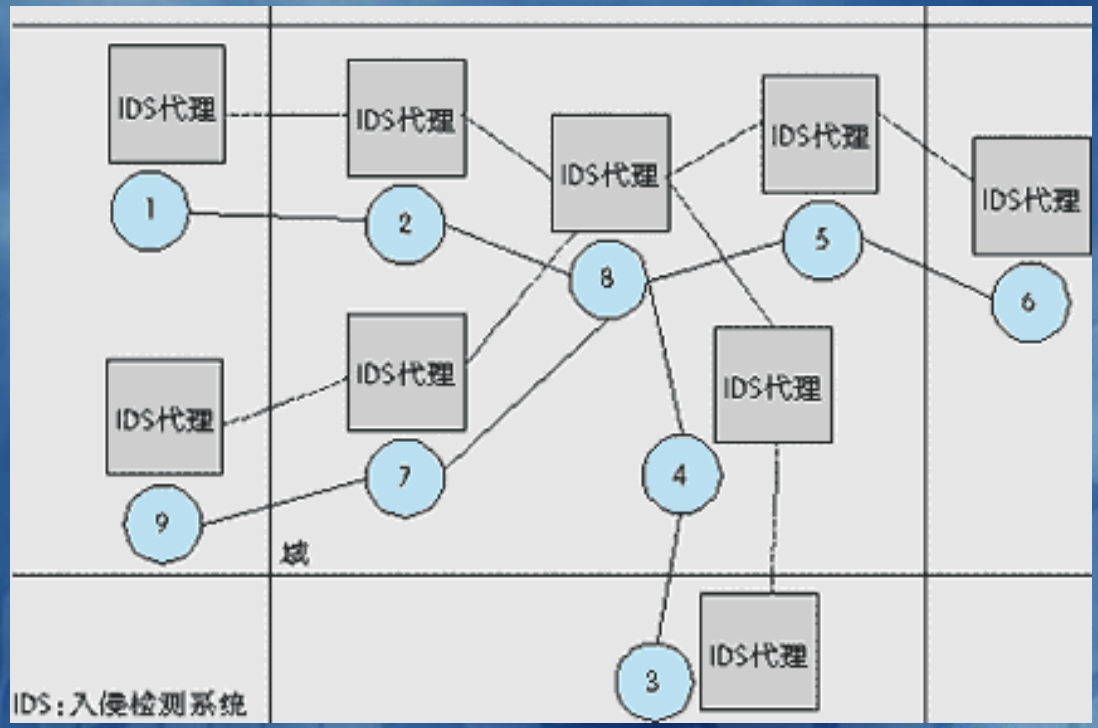
鉴权过程 (cont.)

- 端到端认证
  - 源结点： A->Broadcast:[RDP,IPx, $Cert_A$,N_A,t]K_A-
  - 中间结点:B->Broadcast:[[RDP,IPx, $Cert_A$,N_A,t]K_A-] K_B-, $Cert_B$
  - C->Broadcast:[[RDP,IPx, $Cert_A$,N_A,t]K_A-] K_c-, $Cert_c$
  - 目标结点： X->D:[REP,IP_A, $Cert_x$,N_A,t]K_x-
  - 中间结点:D->C:[[REP,IP_A, $Cert_x$,N_A,t]K_x-] K_D-, $Cert_D$
  - C->B:[[REP,IP_A, $Cert_x$,N_A,t]K_x-] K_C-, $Cert_C$

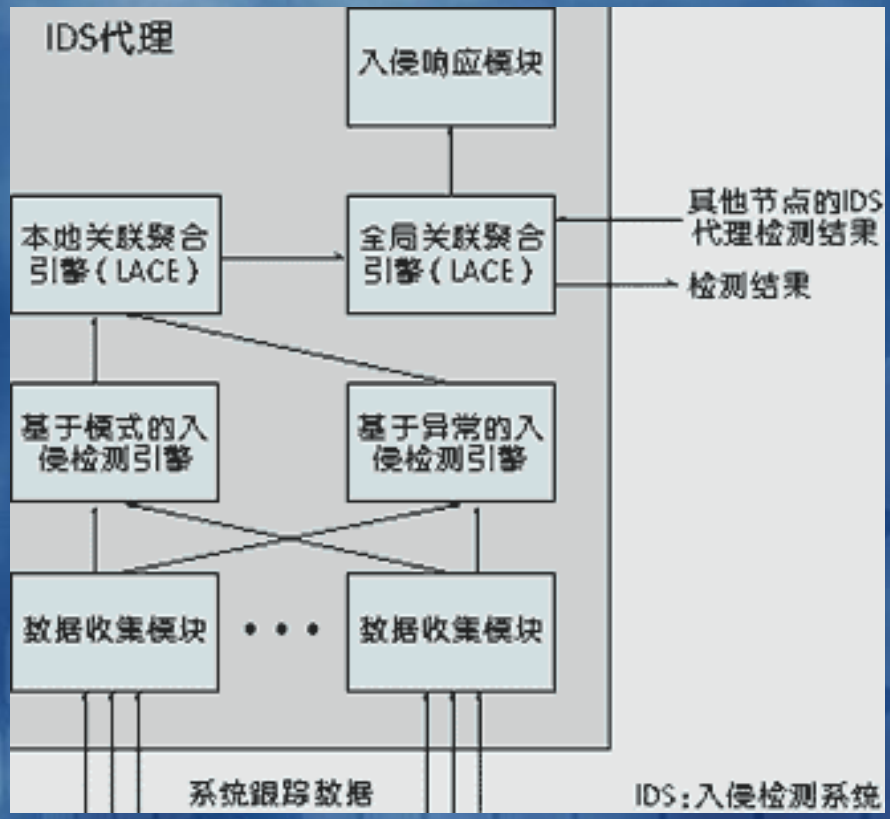
Ad Hoc入侵检测

- 必要性：
  - 加密和鉴权不能解决被俘节点发动的袭击
- 和传统IDS区别
  - 传统IDS能通过交换机或者网关收到所有数据进行判断（集中式）
  - AD Hoc IDS只能收集局部不完整信息综合判断（分布式）

Ad Hoc 结构模型



Ad hoc IDS代理模型

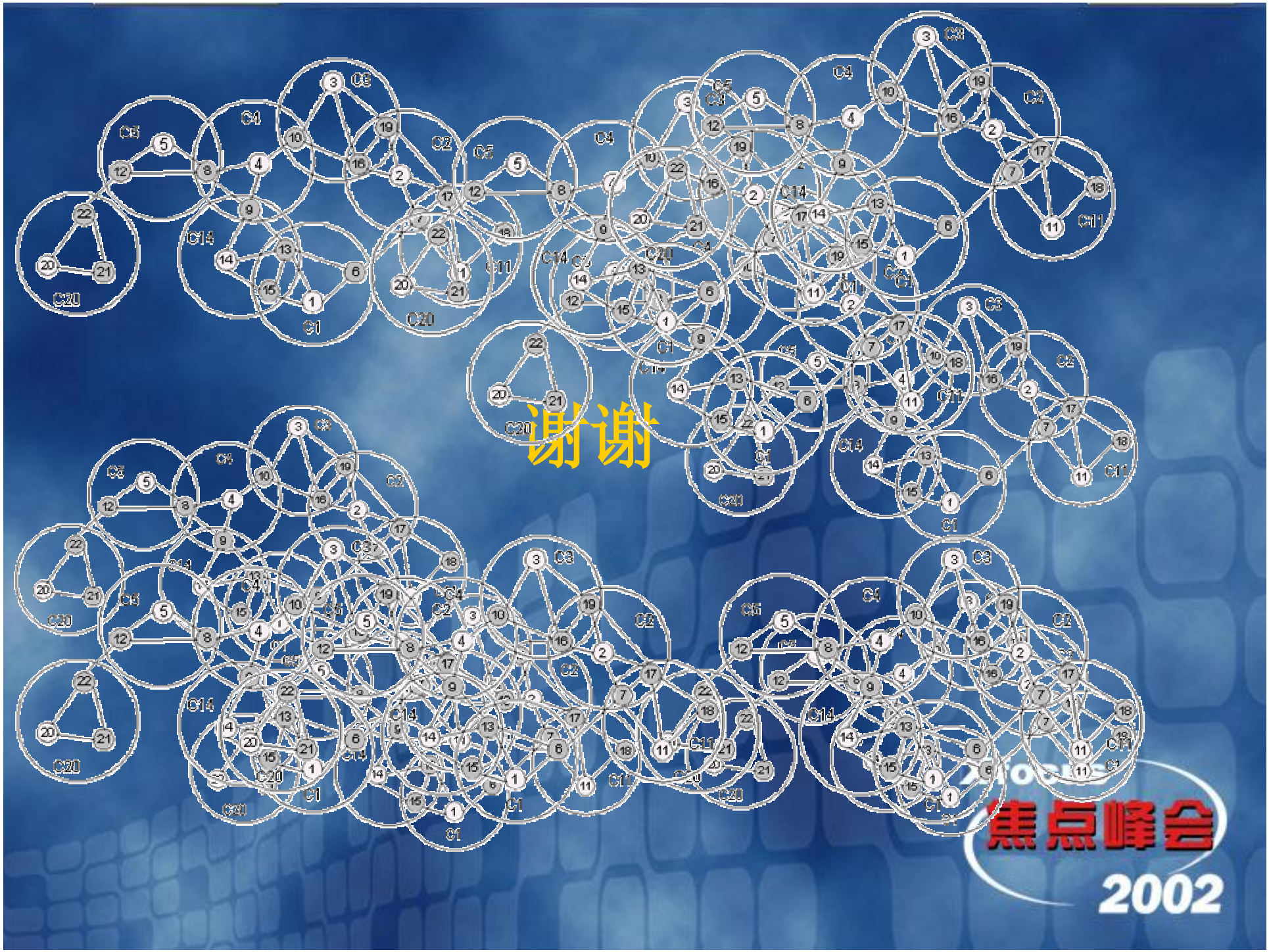


Ad Hoc IDS存在的问题

- 数据不充分，容易漏报
- 由于经常需要全局联合分析，对性能影响大
- 无法区分DOS服务还是结点移动到服务区外
- 无法解决假报情况

Ad Hoc需要解决的安全问题

- Ad hoc是一个对等网络，就像原始社会一样，没有人领导和负责，因此关键就是要寻求一个自治系统
  - 安全路由
  - 密钥管理
  - 被俘结点探测
  - 入侵检测


谢谢
焦点峰会
2002