



# 《无线传感器网络技术》讲义

宁波中科无线通信事业部  
<http://www.wsn.org.cn>

宁波中科无线通信事业部  
<http://www.wsn.org.cn>

## 第九章、安全设计技术

2007年8月20日



中国科学院计算技术研究所

Institute of Computing Technology, Chinese Academy of Sciences



# 内容提要

1. WSN安全挑战
2. WSN安全需求
3. WSN安全威胁
4. WSN基本安全技术
5. WSN加密技术
6. 节点加密技术
7. WSN服务组件安全
8. 总结

1. WSN安全挑战
2. WSN安全需求
3. WSN安全威胁
4. WSN基本安全技术
5. WSN加密技术
6. 节点加密技术
7. WSN服务组件安全
8. 总结

- 两点认识
  - WSN应用需要强力的安全支持
  - WSN的特点决定实现WSN安全支持不是一件容易的事，是一大挑战
- 安全设计中，WSN和Ad hoc的区别
  - ⤴ 网络模型不同
  - ⤴ 网络规模不同
  - ⤴ 网络终端能力不同
  - ⤴ 通信模型不同
  - ⤴ 网络拓扑变化频繁
  - ⤴ 网络应用环境带来新的安全威胁

- 安全设计时，须着重考虑的无线传感器网络的三大特点：
  - 资源非常有限（存储、计算、电池）
  - 不可靠的无线通信、网络规模大
  - 非受控操作、面向应用
- 无线信道的开放性需要加密体制，资源约束的节点需要**轻量级、高效安全**实现方案，非受控操作需要传感器网络安全策略具有较高的**安全弹性**。

1. WSN安全挑战
2. WSN安全需求
3. WSN安全威胁
4. WSN基本安全技术
5. WSN加密技术
6. 节点加密技术
7. WSN服务组件安全
8. 总结

- 通信安全需求
  - 数据机密性
    - 防窃听
  - 数据完整性
    - 防篡改
  - 真实性
    - 防伪造
  - 数据新鲜性
    - 防重放

- 网络服务安全需求
  - 可用性
  - 自组织
  - 其它服务组件的安全需求
    - 时间同步
    - 定位
    - 网内融合

1. WSN安全挑战
2. WSN安全需求
3. WSN安全威胁
4. WSN基本安全技术
5. WSN加密技术
6. 节点加密技术
7. WSN服务组件安全
8. 总结

- 与传统无线网络一样，传感器网络的消息通信会受到监听、篡改、伪造和阻断攻击。

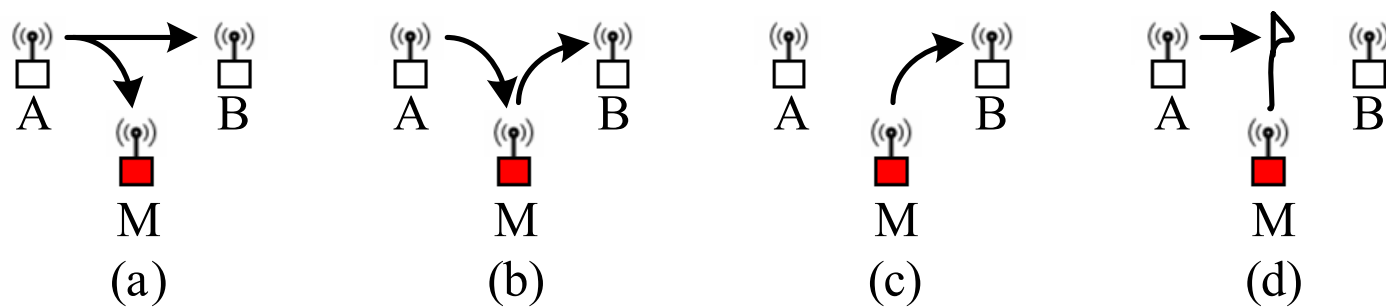


图 9-1：无线网络中4种通信安全威胁：  
(a) 监听， (b) 篡改， (c) 伪造， (d) 阻断

- 攻击者特征
  - 精明的外行
  - 知识渊博的内行
  - 受到政府或组织资助的团队
    - 可以轻易拥有超强的计算能力和灵敏的无线通信能力
- 攻击分类之一
  - 外部攻击
  - 内部攻击

- 从传感器节点看安全威胁
  - 欺骗：主要来自于环境和网络
  - 控制：是最具威胁的攻击行为
    - 物理控制
    - 逻辑控制
- 从网络通信看安全威胁
  - 被动攻击和主动攻击
  - 重放攻击、DoS攻击和Sybil攻击

- 从系统角度看安全威胁
  - 多跳自组织路由
  - 时间同步
  - 定位
  - 数据融合
  - 甚至安全服务
  - 特别的：能量消耗攻击



# 内容提要

1. WSN安全挑战
2. WSN安全需求
3. WSN安全威胁
4. WSN基本安全技术
5. WSN加密技术
6. 节点加密技术
7. WSN服务组件安全
8. 总结

- 基本安全框架（SPINS）
  - SPINS安全协议族是最早的无线传感器网络的安全框架之一，包含了SNEP和 $\mu$  TESLA两个安全协议。
  - SNEP协议提供点到点通信认证、数据机密性、完整性和新鲜性等安全服务。
  - $\mu$  TESLA协议则提供对广播消息的数据认证服务。

- SNEP协议提供点到点通信认证、数据机密性、完整性和新鲜性等安全服务
  - 加密：数据机密性
  - **MAC**：点到点通信认证、完整性和新鲜性

$A \rightarrow B : N_A, R_A$

$B \rightarrow A : \{R_B\}_{\langle K_{BA}, C_B \rangle}, \text{MAC}(K'_{BA}, N_A \parallel C_B \parallel \{R_B\}_{\langle K_{BA}, C_B \rangle})$

- $\mu$  TESLA协议则提供对广播消息的数据认证服务
  - 需要松散（精度不高）的同步支持

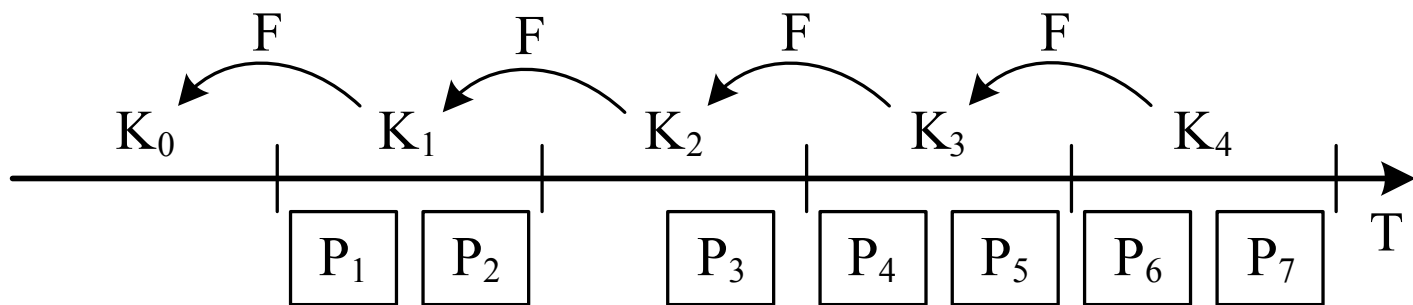


图 9-2:  $\mu$  TESLA协议单向密钥链实例

- 几种安全解决方案比较

	SPINS	TinySec	参数化跳频	LiSP	LEAP
认证	✓	✓	✗	✓	✓
访问控制	✗	✗	✗	✓	✗
抗抵赖性	✗	✗	✗	✗	✗
完整性	✓	✓	✓	✓	✓
机密性	✓	✓	✓	✓	✓
可用性	✗	✗	✓	✓	✗

- 密钥的分配问题是密钥管理中最核心问题
- WSN密钥管理问题通常需要解决的问题
  - 抗俘获攻击的安全弹性问题
  - 轻量级问题
  - 分布式网内处理问题
  - 网络的安全扩展问题
  - 密钥撤销问题

- 主要方案
  - 信任服务器分配模型
  - 密钥分配中心模型
  - 基于公钥密码体制的密钥协商
- 在低成本、低功耗、资源受限的传感器节点上现实可行的密钥分配方案是基于对称密码体制的密钥预分配模型
  - 预安装模型、确定预分配模型和随机预分配模型

- 随机预分配模型基于随机图连通原理，并由Eschenauer和Gligor首次提出了基本随机密钥预分配方案，包括4个步骤：
  - 生成一个足够大的密钥池
  - 随机密钥环预装入
  - 共享密钥发现
  - 安全路径建立

- 理论基础： Erdős和Rényi的随机图理论在大规模随机图 $G(n,p)$ 中，对于其连通属性，若 $p$ 满足阈值函数

$$p = \frac{\ln(n)}{n} + \frac{c}{n} \quad (\text{这里 } c \text{ 为常数})$$

时，随机图 $G(n,p)$ 连通的概率 $P_r$ 满足：

$$P_c = \lim_{n \rightarrow \infty} P_r([G(n,p) \text{ 连通}]) = e^{-e^{-c}}$$

因此，在大规模随机图中， $p$ 和 $P_c$ 有如下（近似）关系：

$$p = \frac{\ln(n)}{n} - \frac{\ln(-\ln(P_c))}{n}$$

- 理论基础（续）

因此，在大规模随机图中， $p$ 和 $P_c$ 有如下（近似）关系：

$$p = \frac{\ln(n)}{n} - \frac{\ln(-\ln(P_c))}{n}$$

设期望出度（关联边）为 $d$ ，则

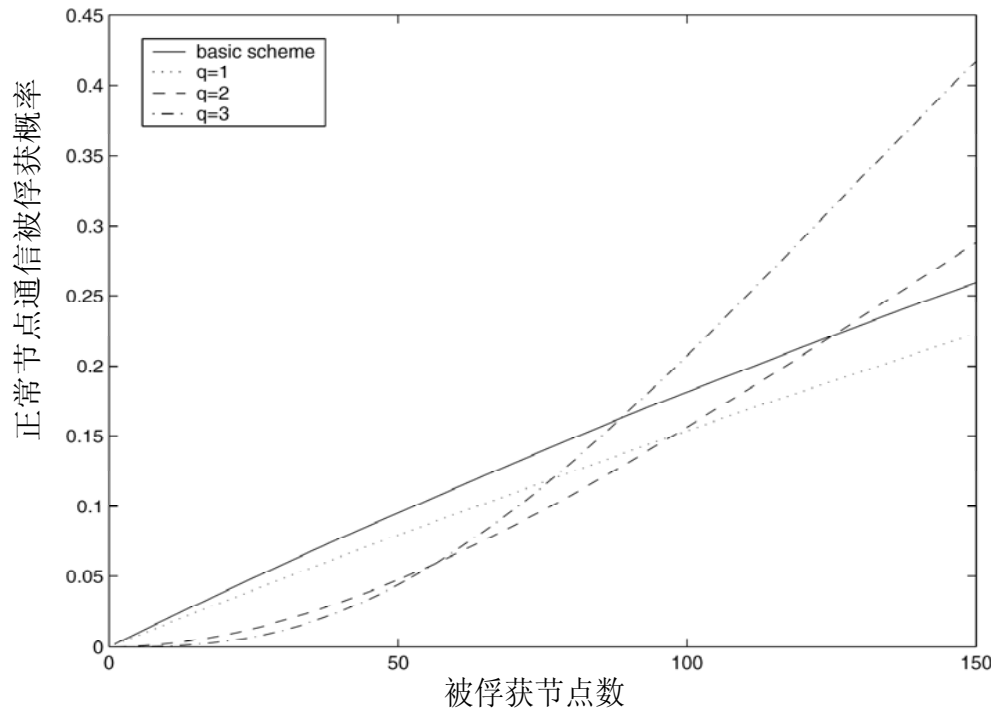
$$p = \frac{d}{n-1}$$

所以：

$$d = (n-1) \left( \frac{\ln(n)}{n} - \frac{\ln(-\ln(P_c))}{n} \right) = n - \frac{1}{n} (\ln(n) - \ln(-\ln(P_c)))$$

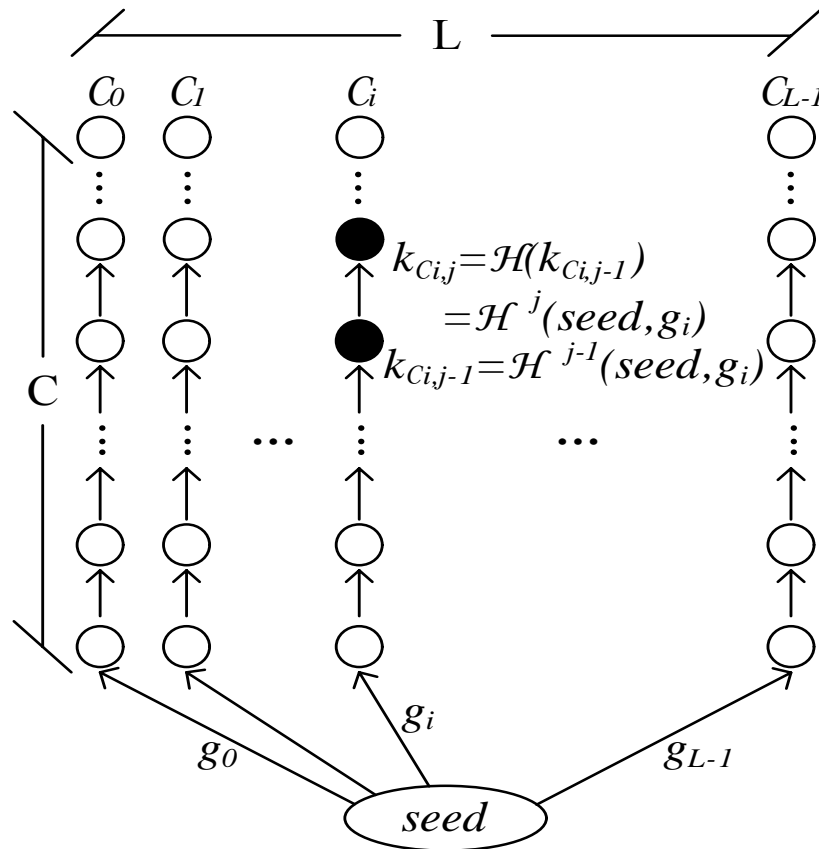
# Random key predistribution schemes for sensor networks

- $q$ -composite 协议直接扩展了 E&G 基本方案，即要求节点对之间至少共享  $q$  个密钥才能建立安全通信



# A new approach for random key pre-distribution in large-scale wireless sensor networks: Research Articles

- 密钥池构造和密钥环预分配方面做了改进



- 网络层攻击
  - 路由信息欺骗
  - 选择性转发
  - 污水坑（Sinkhole）攻击
  - Sybil攻击
  - 虫洞（Wormholes）攻击
  - Hello数据包洪泛攻击
  - ACK欺骗
  - 流量分析攻击

- 安全路由协议（INSENS）：  
INSENS是一个面向无线传感器网络的安全的入侵容忍路由协议
- INSENS路由协议的主要策略包括：
  - 使用单向散列链（OHC）限制广播以限制洪泛攻击。
  - 多路径路由增强入侵容忍
  - 路由更新限制

- WSN IDS实现不能回避的问题是：由于资源受限，不可能在每个节点上都运行一个全功能IDS代理；而且，WSN通常是高密度冗余部署，让每个节点都参与分析邻居传来的所有数据包明显多余和浪费资源；那么如何在WSN中合理地分布IDS代理，进而合理分配IDS任务。
- 回避IDS即入侵容忍是一种方法。

- A Non-cooperative Game Approach for Intrusion Detection in Sensor Networks是一个基于博弈论的入侵检测方法。



# 内容提要

<http://www.wsn.org.cn>

宁波中科无线通信事业部

1. WSN安全挑战
2. WSN安全需求
3. WSN安全威胁
4. WSN基本安全技术
5. WSN加密技术
6. 节点加密技术
7. WSN服务组件安全
8. 总结

<http://www.wsn.org.cn>

宁波中科无线通信事业部

- 位置相关应用安全

- SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks.
- Secure Verification of Location Claims.
- Towards Resilient Geographic Routing in Wireless Sensor Networks.
- Detecting Malicious Beacon Nodes for Secure Location Discovery in Wireless Sensor Networks.
- Attack-Resistant Location Estimation in Sensor Networks.

- 安全时间同步协议
  - Time synchronization attacks in sensor networks.
  - An efficient and secure protocol for sensor network time synchronization.
  - Secure time synchronization in sensor networks.
  - Attack-resilient time synchronization for wireless sensor networks.

- 安全数据融合
  - Statistical en-route detection and filtering of injected false data in sensor networks.
  - Resilient aggregation in sensor networks.
  - Sia: Secure information aggregation in sensor networks.
  - Secure aggregation for wireless networks



# 内容提要

1. WSN安全挑战
2. WSN安全需求
3. WSN安全威胁
4. WSN基本安全技术
5. WSN加密技术
6. 节点加密技术
7. WSN服务组件安全
8. 总结

- WSN安全领域的开放问题：
  - 面向应用的安全需求
  - 现实的攻击模型
  - 跨层安全整合
  - 构建安全传感器网络方案
- 对于WSN安全问题，概率算法是一种较好的候选手段。它们简明且不可预知，从某种意义上说，好似游击战。

## 主要参考文献（详见原著）

- [8] V. Giruka, M. Singhal, J. Royalty, and S. Varanasi, "Security in Wireless Sensor Networks", Wireless Communications and Mobile Computing, Wiley InterScience, 2006, No. 6, pp. 1-24.
- [11] John P. Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, Wireless Sensor Networks Security: A Survey, book chapter of Security in Distributed, Grid, and Pervasive Computing, Yang Xiao (Eds.), CRC Press, 2007
- [14] Han, Song and Chang, Elizabeth and Gao, Li and Dillon, Tharam. Taxonomy of attacks on sensor networks. Proceedings of the First European Conference on Computer Network Defense (EC2ND), Glamorgan, UK, December 2005, pp. 97-105
- [16] Perrig A, Szewczyk R, Wen V, Culler D, Tygar JD. SPINS: security protocols for sensor networks. Wireless Networks 2002; 8(5): 521–534.
- [25] Eschenauer L, Gligor VD. A key-management scheme for distributed sensor networks. Conference on Computer and Communications Security. Proceedings of the 9th ACM Conference on Computer and Communications Security 2002, Washington, DC, USA.
- [27] Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. In Proceedings of IEEE Symposium on Research in Security and Privacy, 2003.
- [30] R. Kui, Z. Kai, and L. Wenjing. A new approach for random key pre-distribution in large-scale wireless sensor networks: Research Articles. Wirel. Commun. Mob. Comput., vol. 6, pp. 307-318, 2006.
- [32] Karlof C, Wagner D. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. Elsevier's AdHoc Networks Journal, 1(2-3), 2003.



## 主要参考文献（详见原著）

- [34] C. Baslie, M. Gupta, Z. Kalbarczyk, and R. K. Iyer. An Approach for Detecting and Distinguishing Errors versus Attacks in Sensor Networks. In Performance and Dependability Symposium, International Conference on Dependable Systems and Networks, 2006.
- [39] A. Agah, S. K. Das and K. Basu. A Non-cooperative Game Approach for Intrusion Detection in Sensor Networks. VTC 2004, Fall 2004.
- [62] N. Sastry, U. Shankar, and D. Wagner. Secure Verification of Location Claims. In the ACM workshop on Wireless Security, 2003.
- [64] D. Liu, P. Ning, and W. Du. Detecting Malicious Beacon Nodes for Secure Location Discovery in Wireless Sensor Networks. In The 25th International Conference on Distributed Computing Systems, June 2005.
- [73] B. Przydatek, D. Song, and A. Perrig. Sia: Secure information aggregation in sensor networks, 2003.



# 《无线传感器网络技术》讲义

---

宁波中科无线通信事业部  
<http://www.wsn.org.cn>

谢谢!

宁波中科无线通信事业部  
<http://www.wsn.org.cn>