

无线传感器网络中的安全问题综述

作者：Yong Wang, Garhan Attebury, and Byrav Ramamurthy

汇报人：王豫韬



目录

- ▶ 01 概述与背景
- ▶ 02 安全需求与威胁模型
- ▶ 03 常见攻击类型与防御措施
- ▶ 04 密码学应用与密钥管理
- ▶ 05 未来研究方向与总结

概述与背景

01



引言

- 无线传感器网络 (WSNs) 的定义和应用：

无线传感器网络是一种由大量低成本、低功耗、多功能的传感器节点组成的网络，这些节点能够感知、处理和传输数据。WSNs在军事（如战场上监测敌军动向）、生态（如环境污染监测）、健康（如病人监测）等多个领域有广泛应用。

- 研究背景和重要性：

随着无线通信和电子技术的进步，WSNs的应用越来越广泛，然而，安全问题成为了阻碍其进一步发展的主要障碍之一。文旨在综述WSNs中的安全问题及其解决方案。



WSNs的特点

节点数量多：传感器网络中的节点数量可以比传统的无线自组网络中的节点多几个数量级。

部署密度高：传感器节点通常密集部署在监测区域内，以保证数据的准确性和覆盖范围。

容易故障：由于部署环境恶劣和能量限制，传感器节点容易发生故障。

拓扑变化频繁：由于节点故障或移动，网络拓扑结构会频繁变化。

计算、内存和能量限制：传感器节点的计算能力、内存容量和能量资源非常有限。。



02

安全需求与威胁模型

安全需求

可用性：确保网络服务在受到拒绝服务攻击时仍然可用。

授权：确保只有授权的传感器节点能够参与网络服务。

认证：确保节点间通信的真实性，防止恶意节点冒充合法节点。

保密性：确保消息只能被指定的接收者理解。

完整性：确保消息在传输过程中未被篡改。

不可否认性：确保节点不能否认已发送的消息。

新鲜度：确保数据是最新的，防止重放旧消息。



威胁模型

外部攻击与内部攻击：外部攻击来自于不属于网络的节点，内部攻击则来自于已被攻陷的合法节点。

被动攻击与主动攻击：被动攻击指窃听或监视网络通信，主动攻击则包括篡改、伪造或重放消息。

节点级攻击与高端设备攻击：节点级攻击利用与网络节点性能相似的设备，高端设备攻击则使用性能更强的设备（如笔记本电脑）来攻击网络。

常见攻击类型与防御措施

03



安全攻击类型

保密性与认证攻击：包括窃听、消息重放、篡改或伪造消息等。

网络可用性攻击：包括各种拒绝服务攻击，旨在破坏网络的正常运行。

隐蔽攻击：攻击者通过传感器节点注入错误数据，使网络接受虚假数据。



物理层攻击

干扰：通过干扰传感器节点使用的无线电频率来中断网络通信。

篡改：通过物理接触节点来提取密钥或其他敏感信息，或替换节点。

防御措施：使用跳频扩频技术、物理防篡改措施等。



链路层攻击

碰撞：故意制造数据包碰撞，导致数据包被丢弃。

资源耗尽：通过重复碰撞消耗节点能量。

不公平竞争：利用上述攻击手段使某些节点在通信中占优势。

防御措施：使用错误检测编码、速率限制等方法。



网络层攻击

伪造、篡改或重放路由信息：通过伪造或篡改路由信息破坏网络通信。

选择性转发：恶意节点选择性地丢弃或转发数据包。

汇聚攻击：恶意节点吸引周围节点的数据流通过自己，从而实施攻击。

Sybil攻击：单个节点伪装成多个节点。

虫洞攻击：在网络中创建一个低延迟的链接，重放网络消息。

Hello泛洪攻击：利用高功率发射器发送Hello消息，使大量节点误认为其是邻居节点。

确认欺骗：伪造数据包的确认消息，提供错误的网络状态信息。



传输层攻击

洪水攻击：不断发起新连接请求，耗尽节点资源。

反同步攻击：通过伪造消息扰乱现有连接的同步，消耗节点能量。

防御措施：使用客户谜题机制、消息认证等方法。



04

密码学应用与密钥管理

密码学在WSNs中的应用

公钥密码学：如RSA、ECC，用于密钥交换和签名。

对称密钥密码学：如AES、RC5，用于数据加密。



公钥密码学

RSA：基于大整数分解的加密算法，计算复杂，能量消耗高。

ECC：椭圆曲线密码学，相同安全级别下，密钥长度更短，能量消耗较低。

性能比较：ECC在能量消耗和计算时间上优于RSA，适合用于传感器网络。



对称密钥密码学

RC5: 一种基于分组加密的算法, 计算效率高, 能量消耗低。

TEA: 简洁高效的分组加密算法, 适合嵌入式系统。

AES: 高级加密标准, 安全性高, 广泛应用于各种安全系统。



密钥管理协议

集中式密钥管理：由中心节点管理密钥分发和更新。

分布式密钥管理：由多个节点协作管理密钥，提高网络的健壮性。



集中式密钥管理方案

LKHW方案：基于逻辑密钥层次结构，由基站作为密钥分发中心。



分布式密钥管理方案

LEAP协议：支持多种类型的密钥，包括个体密钥、群组密钥、对等密钥和簇密钥。

BROSK协议：通过广播会话密钥协商，实现高效的密钥分发。

CDTKeying方案：基于组合设计理论，提供确定性的密钥分发方案。

随机密钥方案：基于随机图理论，实现高效的密钥管理。



未来研究方向与总结

05



未来研究方向

密钥管理协议改进：设计更高效、更安全的密钥管理方案。

适用于WSNs的公钥密码学方法：研究低能耗的公钥密码学算法。

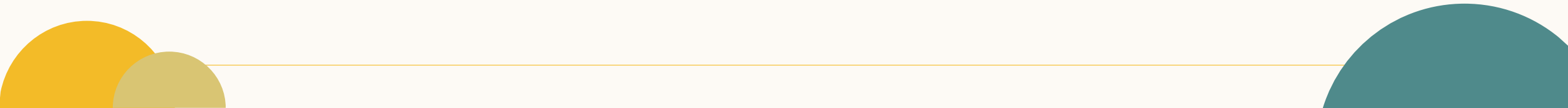
基站安全性考虑：设计保护基站安全的机制，防止其被攻陷。



总结

本文贡献：本文综述了无线传感器网络（WSNs）中的主要安全问题，详细分析了各种攻击类型及其对应的防御措施。同时，本文还对现有的安全协议进行了比较和评估，指出了各协议的优缺点，并提出了一些可能的改进方向。本文通过系统地整理和分析WSNs中的安全研究成果，为研究人员提供了有价值的参考。

未来工作展望：随着WSNs的应用领域不断扩展，未来的研究可以重点关注以下几个方面：（1）设计更加高效和安全的密钥管理协议，以应对WSNs中的资源限制和安全需求；（2）研究低能耗的公钥密码学算法，使其在实际应用中变得可行；（3）加强对基站安全的研究，设计有效的机制来保护基站免受攻击，并在基站被攻陷时能够快速恢复网络的正常运行。通过这些研究，能够进一步提高WSNs的安全性，促进其在各个领域中的广泛应用。



THANK YOU

汇报人：王豫韬

