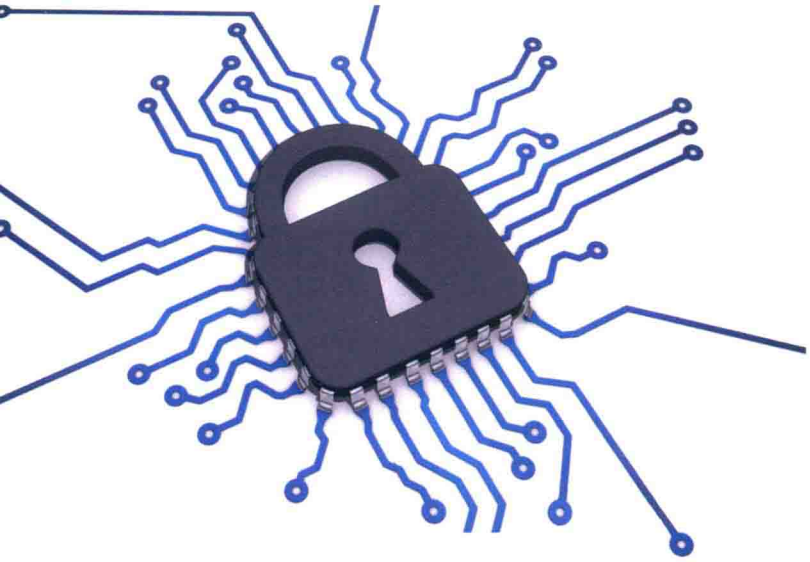
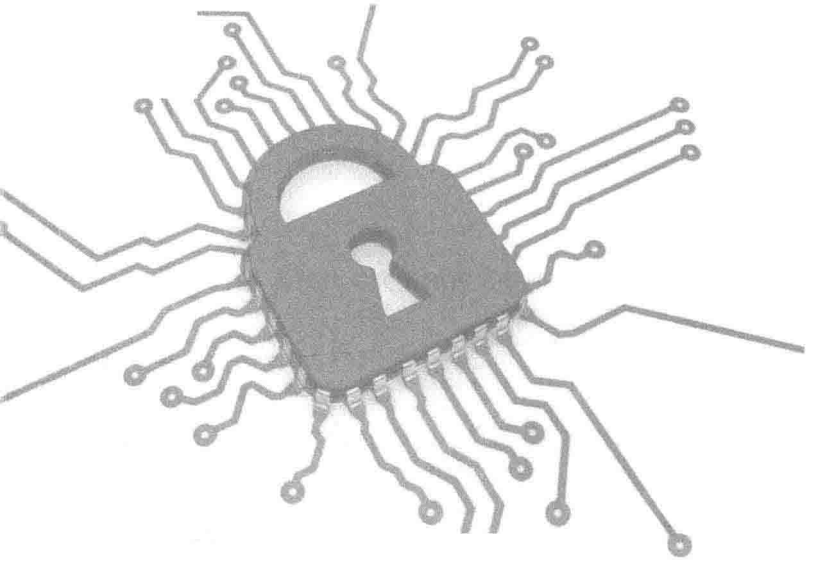


Studies on Security Attacks and Prevention Approaches in 802.11 Wireless Local Area Network Applications

802.11无线局域网应用中的安全攻击防护策略的研究

刘持标 著

WUHAN UNIVERSITY PRESS
武汉大学出版社



Studies on Security Attacks and Prevention Approaches in 802.11 Wireless Local Area Network Applications

802.11无线局域网应用中的安全攻击防护策略的研究

刘持标 著

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

802.11无线局域网应用中的安全攻击防护策略的研究/刘持标著.
—武汉:武汉大学出版社,2016.3
ISBN 978-7-307-17384-2

Ⅰ.8… Ⅱ.刘… Ⅲ.无线电通信—局部网络—安全技术—研究
Ⅳ.TN925

中国版本图书馆CIP数据核字(2015)第303027号

责任编辑:叶玲利　　责任校对:周丁玲　　版式设计:大春文化

出版发行:武汉大学出版社(430072　武昌　珞珈山)
(电子邮件:cbs22@whu.edu.cn　网址:www.wdp.com.cn)
印　　刷:虎彩印艺股份有限公司
开　　本:720mm×1000mm　1/16　　印　　张:15.75　　字数:282千字
版　　次:2016年3月第1版　　2016年3月第1次印刷
ISBN 978-7-307-17384-2　　定　　价:52.00元

刘持标，现任三明学院信息工程学院副院长，福建省农业物联网应用重点实验室主任，物联网应用福建省高校工程研究中心负责人。具有丰富的国内外环境友好化工生产监控技术开发、信息安全及物联网应用实践经历：1997 年 7 月获得中国科学院长春应用化学研究所物理化学博士，2002 年 11 月获美国德保罗大学(DePaul University)计算机科学硕士，2010 年 3 月获美国德保罗大学计算机科学博士。2010 年 9 月至今，在三明学院工作期间，同三明市三元区林业局和三明市格氏栲省级自然保护区合作，开发出了基于 3G 物联网技术的新型森林火情监控系统；积极同福建三钢合作，对物联网技术在炼钢生产过程监控中的应用展开研究；同福建高斯贝尔电子科技有限公司合作，研发智能家居技术；同福建光华百斯特生态农牧发展有限公司合作，共同研发物联网技术在大型养猪场健康养殖智能监控中的应用。此间主持福建省自然科学基金项目一项，主持福建省科技厅重点项目一项，主持福建省教育厅重点项目一项，主持三明市重点科技项目一项。2012、2013、2015 年被评为三明学院优秀科研工作者，2013 年被评为三明市优秀教师，2014 年被评为福建省优秀教师。科研重点为物联网应用、物联网安全及无线网络安全。在中国科学及国外期刊发表论文 30 余篇(SCI 检索 14 篇，EI 检索 5 篇)，2015 年出版教材《物联网工程与实践》。

三明学院科研基金资助项目

前　言

802.11 无线通信技术广泛应用于工业生产线监控、城市安全巡查、城市交通监控、食品物流监控、火灾现场抢救监控、供水监控、洪灾现场抢救监控、电力监控、油田监测、环境监测、学校安全监控、反恐防暴安全监控及小区安全监控等。基于 802.11 无线通信技术的实时信息化应用大多涉及工业生产及民生的关键领域，对无线数据传输的安全性、实时性及可靠性要求较高，如有信息泄露、数据丢失或传输滞后，将会影响信息化系统决策的及时性和准确性，也会进一步造成重大经济及生命损失。

目前，造成无线数据传输过程中信息泄露的因素主要包括流量分析、中间人攻击、会话劫持、未经授权的访问、伪装、重播、窃听、篡改和伪造。同时，数据传输实时性及可靠性不稳定的首要因素为 802.11 无线拒绝服务攻击(Denial of Service, DoS)。802.11 DoS 攻击将导致 802.11 无线网关、802.11 无线节点与无线接入点(Access Point,AP)之间的通信资源耗尽或者无法做出正确的响应而瘫痪，从而无法提供正常的通信服务。

本书主要从如何解决信息化应用中的信息泄露问题，如何避免 802.11 无线拒绝服务攻击两个方面来对无线安全问题进行深入研究。在研究成果的基础上，进一步探讨了安全高效 802.11 无线通信技术在不同领域的应用。

感谢三明学院信息工程学院、福建省农业物联网应用重点实验室及物联网应用福建省高校工程研究中心为本书的顺利完成提供了各方面的大力支持。感谢福建省科技计划项目（2013N0031）、福建省自然科学基金资助项目(2012J01283)、福建省教育厅省属高校科研专项计划项目(JK2012051)、2012 年省级质量工程与教学改革项目——网络工程专业综合改革（ZL2012ZG4)和三明学院科研启动基金的支持。

Preface

The growing popularity of 802.11-based Wireless LANs (WLAN) also increases the risk of security attacks, which include crypto attacks and Denial of Service (DoS) attacks. To prevent crypto attacks, we propose an integrated approach to enhance the 802.11i standard with IP-based Virtual Private Network (VPN). The empirical results of the integrated approach show improved security protection with little performance degradation. However, this approach does not protect WLANs against DoS attacks, which include authentication request flooding (AuthRF), association request flooding (AssRF), deauthentication flooding (DeauthF), and disassociation flooding (DisassF).

This research is the first comprehensive study of AuthRF and AssRF attacks, and our empirical study shows that these attacks cause significant performance degradation. A queuing model is presented to study the attacking mechanisms and the causes of performance degradation. The queuing model is then validated by the simulation model, and the results from both analytical and simulation models are consistent with the empirical data. The analytical model leads to the development of four solutions: Request Authentication (RA), Reduction of Duplicate Requests (RDR), Reduction of Response Retransmissions (RRR), and Round Robin Transmission(RRT). These solutions are also validated by the experimental data, along with the analytical and simulation data of the queuing model. A comparison of these four solutions is presented to show their strengths and weaknesses in resolving AuthRF/AssRF attacks.

This research is the first implementation of the 802.11w standard on the

ns2 environment, and our experimental data demonstrates the effectiveness of 802.11w in resolving the low rate fake DeauthF and DisassF attacks. However, it does not address the issues of flooding-type DoS attacks. Based on 802.11 wireless station (STA) service modules, we develop a STA-based queuing model to study the relationship of TCP/UDP performance vs. attacking rates. Meanwhile, we also apply Markov chain model to investigate DeauthF and DisassF attacks. Analysis of these models leads to a solution of Traffic Shaping (TS) to enhance 802.11w. The results yield satisfactory performance under various attacking scenarios.

In summary, this research studies major attacks on WLANs and provides solutions to resolve them. Furthermore, based on research achievements, we proposed and implemented several high security wireless applications in the areas of voice over IP, Layer-3 Forwarding, wireless device server and Internet of Things (IOT) applications.

Contents

CHAPTER 1 Introduction

CHAPTER 2 Experimental Methodologies

CHAPTER 3 Protect Wireless LANs using VPN over 802.11i

CHAPTER 6 RAP DoS Attacks with Markov Chain Model

CHAPTER 7 DoS Attacks against Wireless VoIP

CHAPTER 1

Introduction

1.1 Motivations

Since the standardization of 802.11 wireless communication[1], we have seen an increase in popularity of the WLAN and its wide deployment at home, Small Office/Home Office (SOHO), campus networks, enterprise networks, hot spots, and wireless Internet of Things (IOT) applications[2-15]. The network architecture of a typical WLAN is illustrated in Figure 1.1.

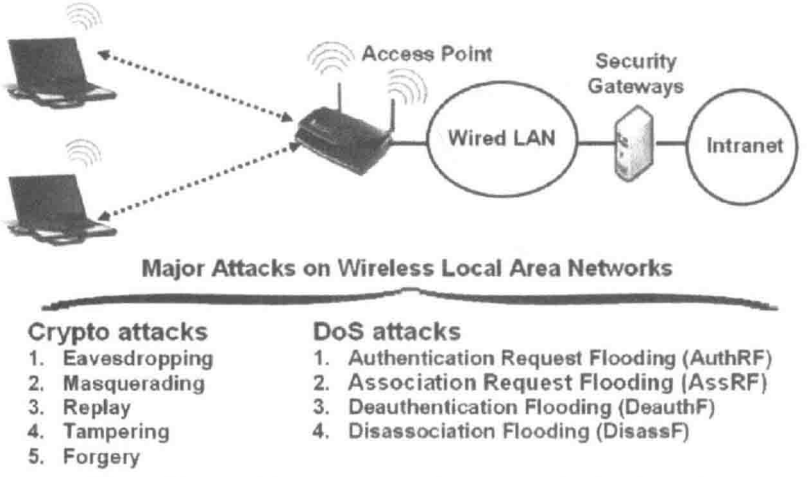


Figure 1.1 WLAN network architecture and related attacks

The advantages of WLANs (in comparison to other LAN technologies) are

flexibility, ease of installation and configuration, high performance, and relatively low cost. However, the popularity of WLANs also encounters a continual increase in security attacks[16-28]. The latest survey from Computer Security Institute (CSI) shows that WLAN abuses (i.e., security attacks) are the major growing threat of computer crimes[29]. As shown in Figure 1.1, we classify WLAN security attacks into two categories: crypto attacks and DoS attacks.

Crypto attacks include traffic analysis, man-in-the-middle, session hijack, unauthorized access, masquerading, eavesdropping, replay, tampering and forgery. Crypto attacks are related to the weaknesses of user authentication and data encryption, and they can be resolved with strong authentication and encryption. DoS attacks are related to 802.11 protocol operations, and they cannot be resolved by only using cryptographic methods. In this research, we identify four major DoS attacks: authentication request flooding (AuthRF), association request flooding (AssRF), deauthentication flooding (DeauthF) and disassociation flooding (DisassF). Currently, there are no standard solutions and few publications to resolve these attacks. Our research objectives are to study and model the behaviors of these attacks, and to develop effective solutions to resolve them.

1.2 Crypto attacks on WLANs

There are many crypto attacks against WLANs, and we group them into nine major categories: traffic analysis, eavesdropping, man-in-the-middle(MITM), session hijack, masquerading, unauthorized access, replay (or playback), tampering, and forgery.

1.2.1 Traffic analysis

Traffic analysis examines communication patterns and derives significant information from it. To launch such an attack, the hacker needs only a wireless card operating in promiscuous mode and a wireless sniff software, such as Netstumbler[30] or commview WiFi[31]. A screen dump of the traffic analysis is illustrated in Figure 1.2.