• 专栏 • 文章编号：1000—3428(2014)01—0011—04 文献标识码：A 中图分类号：TP18

蓝牙通信中的射频指纹识别技术

李文龙[1]，陈 悦[2]，许金勇[3]，梁 涛[3]

(1. 解放军理工大学通信工程学院，南京 210007；2. 南京理工大学，南京 210094；3. 解放军总参谋部第 63 研究所，南京 210007)

摘 要：利用开机瞬态特征对蓝牙传输设备进行射频指纹识别时，开机瞬态信号的捕获与提取存在一定的局限性。为此，提出将频率跳变瞬态特征用于蓝牙设备的唯一性鉴别，以克服开机瞬态特征的局限性。在射频指纹识别中的数据获取、瞬态信号检测、指纹提取和分类过程中对该特征进行验证，根据实验数据对鉴别性能进行评估。分析结果表明，利用频率跳变瞬态特征能够成功鉴别蓝牙设备。以对虫洞攻击的检测和防御为例，进一步分析射频指纹识别在蓝牙网络安全协议中的应用，并给出基于蓝牙指纹识别的安全链路管理协议。

关键词：蓝牙指纹识别；频率跳变瞬态特征；开机瞬态特征；射频指纹识别

Radio Frequency Fingerprinting Technology in Bluetooth Communication

LI Wen-long[1], CHEN Yue[2], XU Jin-yong[3], LIANG Tao[3]

(1. Institute of Communication Engineering, PLA University of Science and Technology, Nanjing 210007, China;
2. Nanjing University of Science and Technology, Nanjing 210094, China;
3. The 63rd Research Institute of PLA General Staff Headquarters, Nanjing 210007, China)

【Abstract】 It is limitary to classify the radio devices by utilizing the turn-on transients character, when the turn-on transient signals are captured and extracted. Aiming at this problem, this paper investigates Frequency Hopping(FH) transients character which can be used to classify the bluetooth devices alike the Turn-on Transients(TOT) character but get rid of the limitation which the RFF based TOT character has. The FHT-Character based on the Radio Frequency Fingerprinting(RFF) process is validated, which includes data acquisition, transient detection, radio frequency fingerprint extraction, and classification subsystems. A classification performance of the identification system is evaluated from experimental data. It is demonstrated that the FHT character can be used to classify the bluetooth devices successfully. It further analyzes the implications of device fingerprinting on the security of bluetooth networking protocols which is illustrated by the example of the detection and combat for wormhole attacks. From this, a safe link management protocol is given which is based on bluetooth fingerprinting.

【Key words】 bluetooth fingerprinting; Frequency Hopping(FH) transients character; Turn-on Transients(TOT) character; Radio Frequency Fingerprinting(RFF)

DOI: 10.3969/j.issn.1000-3428.2014.01.003

1 概述

近年来，从符合 802.11 协议的无线网卡到基于 802.15 协议的蓝牙模块等大量设备都已经实现远程的设备指纹识别，不久之前更是在 Internet 上实现了远程的设备指纹识别。到目前为止，射频指纹识别技术利用无线电收发机的开机瞬态特征几乎能鉴别出任何设备。不可否认，开机瞬态特征在所有无线电设备中是独一无二和普遍存在的[1-3]。然而射频指纹识别过程[4]利用开机瞬态特征来鉴别无线电设备是受一定限制的。首先，必须成功捕获只存在几毫秒的开机瞬态信号；其次，瞬态信号提取过程就是检测瞬态信号开始点的过程，而不精确的检测会对指纹识别阶段产生有害影响进而造成可能的设备鉴别错误[5]。实际上，一些开机瞬态信号是不能检测开始点的。最后，瞬态信号受一系列系统源的影响，包括锁相环系统、调制子系统、射频放大器、天线系统以及交换和中继系统[6]。由于环境温度的波动以及电源供电电压不稳定，来自相同设备的 2 个指纹也可能存在特定差异。因此，指纹数据库的更新也是需要慎重

基金项目：国家自然科学基金资助项目(61102092)；中国博士后科学基金资助项目(20070411066)

作者简介：李文龙(1982－)，男，博士研究生，主研方向：射频指纹识别，无线网络编码；陈 悦，本科生；许金勇，工程师、博士；梁 涛，研究员、博士生导师

收稿日期：2013-07-30 **修回日期：**2013-09-03 **E-mail：**ppl007m@126.com

考虑的问题。

在某些特定通信模型中有可能找到取代开机瞬态特征的更好的特征指纹。本文选择对蓝牙通信模型进行研究。Hall 等人[7]已经开展了应用开机瞬态特征对蓝牙无线设备进行射频指纹识别的相关研究。然而在相关研究中发现了一个类似于开机瞬态特征的新特征，可用于鉴别蓝牙设备，即频率跳变瞬态特征。本文论证频率跳变瞬态特征存在的原因，指出应用频率跳变瞬态特征进行射频指纹识别的优点，并分析射频指纹识别在蓝牙无线网络安全协议中的应用。

2 蓝牙指纹识别

尽管频率跳变瞬态特征与开机瞬态特征都可以应用于射频指纹识别过程，但这 2 种特征有显著差异。

2.1 蓝牙设备的开机瞬态特征

一个开机瞬态信号可以分割成 3 个部分：信道噪声，瞬态信号和传输的数据。图 1 中指出了瞬态信号的位置，整个信号来自于一个 3Com 公司生产的蓝牙收发机。

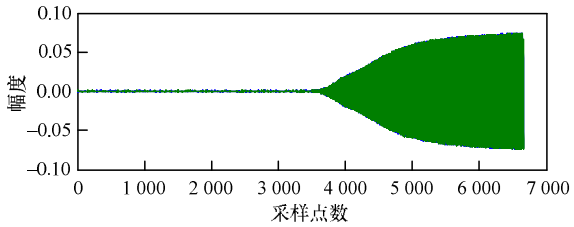


图 1 蓝牙发送器的信号

开机瞬态信号的主要优点是瞬态信号反映了一个无线电设备的独一无二的硬件特性，除非一个无线电设备的整个电路结构被精确地复制，否则只有窃取此无线电设备进行伪造。

2.2 蓝牙设备的频率跳变瞬态特征

蓝牙技术应用基于跳频码分多址(FH-CDMA)的高斯型频率键控调制，使用工业、科学、医学(ISM)波段[8]。由于应用跳频技术，蓝牙通信避免了大多数在 ISM 波段的潜在干扰。对于跳频通信来说，频率合成器是必不可少的元件。然而，由于频率合成器的电子组件的性能是非理想化的，从而带来了频率变化时间(如图 2 所示)。频率变化时间被划分为 3 个部分，包括功率下降时段、零功率时段和功率上升时段。这就是一个功率变化的过程，其中可能包含着瞬态特征。

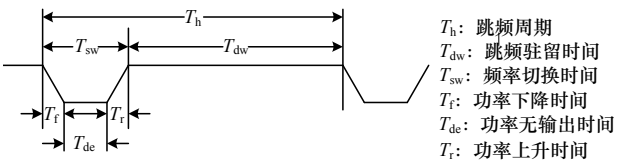


图 2 频率跳变时期的时间关系

图 3 所示为某个蓝牙设备在一段时间内产生的跳频信号。图 3 中的图案为对跳频信号进行局部放大得到的，从中可以清楚地观察到，此跳频信号包含有一个瞬态过程，与开机瞬态过程类似，这就是频率跳变瞬态特征。

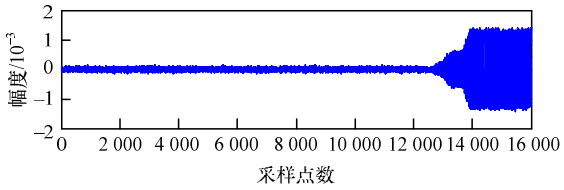


图 3 频谱分析仪捕获的蓝牙跳频信号

基于以下原因可以完美地用于识别蓝牙设备：

(1)在蓝牙设备传输无线电信号时，可以很容易地成功捕获跳频信号；

(2)频率跳变瞬态信号的包络足够规则和稳定，瞬态信号的开始点可以很容易成功检测到；

(3)频率合成器是产生频率跳变瞬态信号的主要元件，因此，对蓝牙频率跳变瞬态信号指纹的更新相对于应用开机瞬态信号指纹更方便和容易。

2.3 蓝牙瞬态信号的捕获

图 4 所示为瞬态信号捕获系统，用于在 2.4 GHz 的 ISM 波段分析基于 802.15 协议的蓝牙信号。本文选择了 4 种蓝牙设备，一共从中捕获了 1 100 个蓝牙信号(如表 1 所示)。Tektronix 公司型号为 RSA3408A 实时频谱分析仪被用来捕获蓝牙信号，它拥有 1 个局域网接口和 2 个 USB 接口用于控制数据的探测与传输。电磁屏蔽环境可以确保在 ISM 波段的潜在干扰。以采样速率为 51.2 MHz 得到的信号保存到个人电脑中备处理。

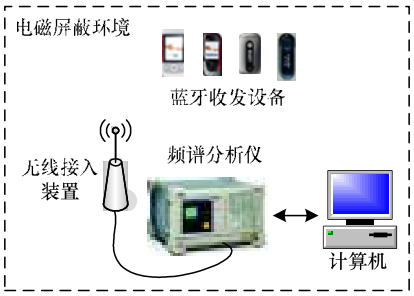


图 4 数据采集的实验装置

表 1 实验信号来源

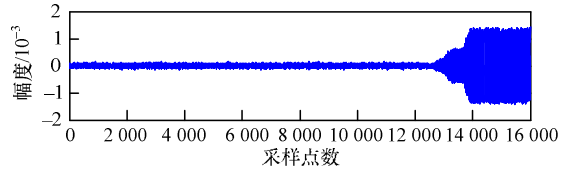
蓝牙设备	生产商	信号数目
Mobile Phone 5300	Nokia	250
Mobile Phone 7610	Nokia	250
U6	Motorola	300
Bluetooth USB Adapter	Ourstin	300

2.4 蓝牙信号频率跳变瞬态特征的提取

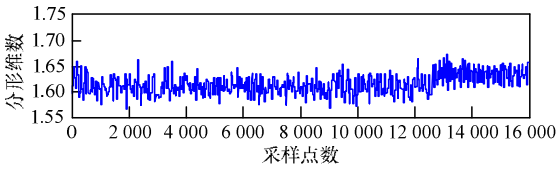
瞬态信号的开始点检测方法共有 3 种：阈值检测，贝叶斯步进检测和相位检测，其中阈值检测方法[9]拥有较低的计算复杂度但需要通过试验确定阈值的大小，相位检测方法也是如此。而贝叶斯步进检测器[10]不需要实现确定大概的触发位置或者阈值就能够检测到突发变化。本文选择贝

叶斯步进检测器对频率跳变瞬态信号进行开始点检测，因为本文实验设置中的电磁屏蔽环境消除了此方法易受噪声和干扰影响的顾虑。

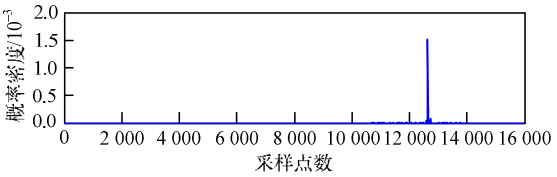
图 5 所示为对来自于诺基亚移动电话 5300 蓝牙发射器的信号应用贝叶斯步进检测器的检测结果。图 5(b)表示利用不规则轨迹(设置滑动因子为 32 个采样)来对瞬态信号开始点进行检测的结果(概率密度函数(式(9)所示)的最大值)。图 5(c)表示所检测出瞬态信号的开始点，相对应为最大后验概率密度，为第 10 144 个采样。



(a)瞬态信号



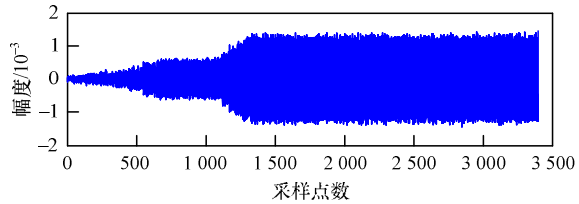
(b)分形轨迹



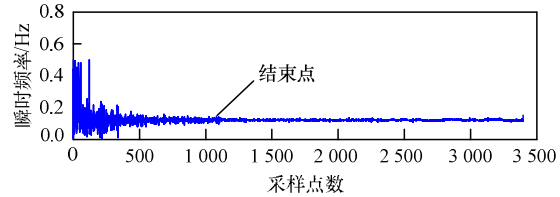
(c)贝叶斯步进检测器的后验概率密度函数

图 5　贝叶斯步进检测结果

瞬态信号的结束点可以通过试验的方式来确定。但是更精确地确定瞬态信号结束点的方法是利用蓝牙通信具有在 79 个频率中跳变的特性，如图 6 所示。图 6(a)表示删除了位于开始点之前采样部分的瞬态信号；图 6(b)表示对瞬态信号进行时频分析得到的相应的瞬时频率，它类似于阻尼振动的波形，容易确定趋向直线的位置就是瞬态信号的结束点。这也证明了频率跳变过程存在瞬态信号。



(a)瞬态信号



(b)瞬时频率

图 6　时频分析

2.5　瞬态信号的特征提取

一旦分离出瞬态信号，下一项工作就是进行主成分分析(PCA)，包括瞬态信号的以下 3 种成分：瞬时幅度，瞬时相位和离散小波变换(DWT)系数。由这 3 种主成分衍生的信号特征具有较低的设备内变化性(来源于同一设备的信号样本)和较高的设备间变化性(来源于不同设备的信号样本)。根据从实验中得到的经验，下面的信号特征可用于区分蓝牙设备：(1)瞬态信号沿着 x 轴的长度；(2)瞬态信号归一化幅度的方差；(3)瞬态信号的归一化幅度(中心均值的)；(4)归一化 DWT 系数；(5)归一化 DWT 系数(中心均值的)。

2.6　指纹分类与蓝牙设备鉴别

为评估蓝牙指纹识别的性能，本文进行了设备鉴别测试。从 4 个蓝牙设备(见上文 2.3 节)中捕获了 1 100 个蓝牙信号，其中有 100 个信号为训练样本，其余 1 000 个样本为实验样本。训练样本用于产生一个概率神经网络，然后用实验样本来评估它的性能。

由于受到捕获自 USB 蓝牙适配器的瞬态信号长度的限制，特征向量(特征 2 和特征 3)的长度选为 512 个采样。归一化 DWT 系数(或中心均值的)的数目为 64。进行了 20 次鉴别实验，鉴别结果错误概率范围为 16%~21%。显然，这个实验结果不够理想。问题的关键在于贝叶斯步进检测器的检测成功(即估计的开始点与实际的开始点距离 64 个采样以内)概率大约为 83%~86%。因此，通过一个观察者的视觉上确定瞬态信号的开始点，得到的鉴别结果错误概率范围为 2%~5%。

值得注意的是，来自于 USB 蓝牙适配器的瞬态信号可以完全正确鉴别，因为捕获自 USB 蓝牙适配器的瞬态信号长度太短了以至于应用特征(1)就可以将其与其他蓝牙设备区分开来。

3　射频指纹识别的应用

本节分析射频指纹识别技术在蓝牙无线网络安全协议中的应用。根据本文前述内容，假如给定 2 个各包含 20 个或更多分组(每个跳频时隙对应一个分组)的蓝牙信号样本，是有可能确定它们是不是来自于同一个蓝牙设备。本文假设现在设备检测性能达到实用化的程度，来考察射频指纹识别对蓝牙无线网络安全协议的影响。进一步假设攻击者不能对蓝牙设备进行完美复制，因此，也不能伪造相应的射频指纹。下面首先描述蓝牙指纹识别如何检测到外部复制和虫洞攻击。

3.1　虫洞攻击检测

在虫洞攻击[11]中，攻击者从网络中的某节点接收分组，将分组通过秘密隧道传输到网络中另一个节点，然后从刚才节点中复制分组数据注入到网络中。如图 7 所示，2 个蓝牙微微网组成了一个分布网，每个微微网包含有 8 个蓝牙设备。每一个微微网都有一个节点被攻击者控制，攻击者可以创造一个虫洞。这是由于攻击者可以在无线信道中偷

听到发送的分组数据并通过秘密隧道将其传输给虫洞末端的共谋节点上。虫洞攻击是最难检测到的攻击之一，因为它不仅可以单独由外部攻击者完成，而且攻击者不需要对分组里的信息进行改变就可以工作。这就意味着甚至加密或数字签名的信息都将面临着虫洞攻击。

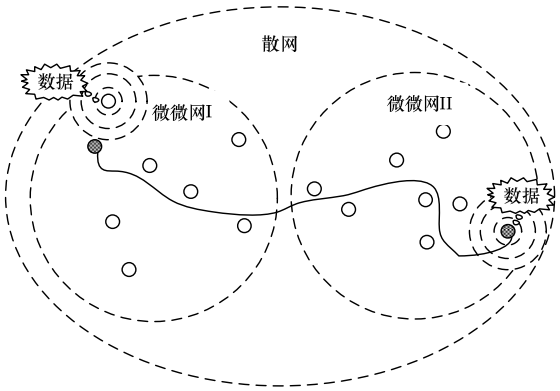


图 7 虫洞模型

蓝牙无线网络属于无线自组织网络结构。假如针对无线自组织路由协议进行虫洞攻击，在虫洞攻击中的隧道距离大于一跳距离情况下，攻击者可以很容易使通过隧道的分组比其他通过一般多跳路由的分组更早地到达目的节点。假如攻击者故意传输分组的一部分或者篡改分组的内容，分组就有可能丢失或者受到损害。同时，由于虫洞带来的虚假路由的距离比实际的路由短，基于节点距离的路由协议被破坏以至于无法找到路由。

有很多方法用于处理虫洞攻击，例如基于地理信息(需要 GPS 定位)的检测方法[12]和基于时间同步和 TIK 协议的检测方法[11]。然而，用于蓝牙无线通信的设备必须同时具有很小的网络通信距离，低廉的花费成本和功率消耗，已存在的检测方法无法达到这些相应目标。

本文第 2 节表明了蓝牙指纹识别技术可以用来鉴别个体蓝牙节点，因此，它可以成为对抗蓝牙无线网络中虫洞攻击的有效工具。图 8 所示为虫洞攻击的一个例子，节点 B 能够检测到虫洞攻击，因为虽然分组的内容里声称他是发自于节点 A，但是对信号进行指纹识别可知它来自于节点 E2。如果分组通过微微网路由，分组内容里会声称他发自于节点 M，信号指纹也会确认这一点。

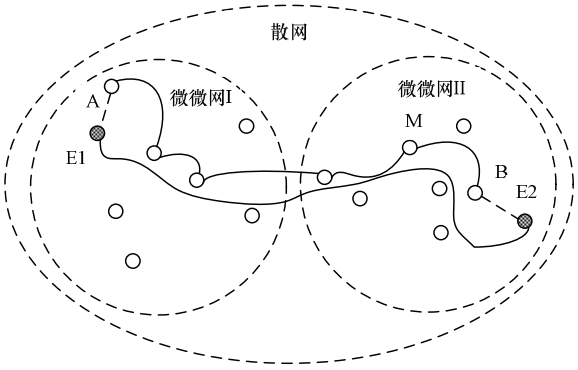


图 8 虫洞攻击示意图

此外，图 8 也表明基于开机瞬态特征的射频指纹识别检测虫洞攻击是有一定局限性的。首先，蓝牙节点必须拥有一个完全信号触发装置随时准备捕获开机瞬态信号。无疑这会增加蓝牙设备的成本和功耗。其次，假如一个蓝牙节点想要加入一个微微网，它必须重复开关机以确保它的开机瞬态信号被捕获到。基于频率跳变瞬态特征的射频指纹识别能够比较完美地解决上述问题。

3.2 关于射频指纹识别的链路管理协议

为对抗虫洞攻击和加强安全链路管理，本文给出一个安全链路管理协议，如图 9 所示。

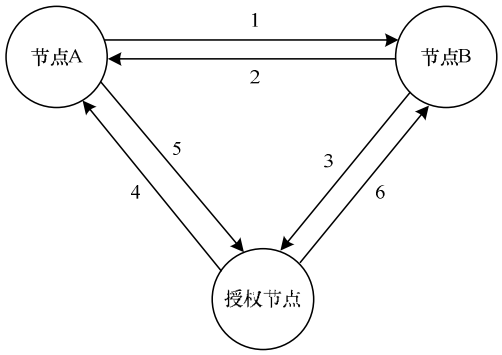


图 9 拥有指纹鉴别的链路管理协议

图 9 中有 3 个蓝牙节点：节点 A，节点 B 和授权节点。图中数字含义如下：

1：节点 A 发送一个请求信息用于发现邻居节点。节点 B 接收到包含有请求信息的射频信号，然后提取信号指纹与节点 B 内存中存储的指纹数据进行比较。如果发现同样的指纹数据，转到 2；如果发现不了，转到 3。

2：节点 B 发送一个回应消息给节点 A，然后它们决定进行下一个工作。例如它们开始进行配对程序。

3：节点 B 发送一个报告消息给授权节点来通过授权节点确认节点 A 的身份。

4、5：授权节点与节点 A 进行交互来确定是否允许节点 A 加入到微微网中。

6：授权节点发送一个回应消息给节点 B，消息中包含有如何处理节点 A 的信息。

与多数网络安全协议类似，以上的安全链路管理协议比旧协议更有效，大大提高了安全性。

4 结束语

本文讨论了蓝牙通信中应用射频指纹识别技术的可行性。在实验中提取了基于频率跳变瞬态特征的射频指纹，并将其用于蓝牙设备之间交换信息的来源鉴别。实验结果表明，分类错误概率的范围在 2%~5%。本文还分析了射频指纹识别技术在蓝牙网络安全协议中的应用。然而笔者的研究课题还有大量需要解决的实际问题，这需要在下一步工作中继续研究，包括低信噪比下的特征提取以及节点的移动性对指纹识别过程的影响等问题。 (下转第 19 页)

5 结束语

针对现有可视化系统的不足，本文利用新颖的辐射状面板视图表示入侵数据，采用颜色混合算法提高用户体验，改进贝塞尔曲线减低图像蔽塞性，通过主机警报优先权加权算法来突出关注因子的显示，采用端口映射算法合理布置低端口与高端口的显示布局，从而快速评估网络安全态势，发现新的攻击模式，弥补传统分析方法的不足。但本文提出的可视化系统暂时只涉及 IDS 警报数据分析，网络态势感知的方向应是各种安全数据的融合，因此，下一步的研究方向是将 Netflow 数据流、Firewall、IDS、主机状态等信息融合为一体，以便更好地评估与预测网络安全态势。

参考文献

[1] 中国互联网络信息中心. 2011 年中国网络信息中心年度报告[Z]. 2012.

[2] 国家互联网应急中心. 2011 年我国互联网网络安全态势综述[Z]. 2012.

[3] Becker R A, Eick S G, Wilks A. Visualizing Network Data[J]. IEEE Transactions on Visualization and Computer Graphic, 1995, 1(1):16-28.

[4] Fortier S C, Shombert L, Network Profiling and Data Visualization[C]//Proceedings of the 2000 IEEE Workshop on Information Assurance and Security. [S. 1.]: IEEE Press, 2000: 166-169.

[5] 吕良福, 张加万, 孙济洲. 网络安全可视化研究综述[J]. 计算机应用, 2008, 28(8): 1924-1927.

[6] 穆成坡, 黄厚宽, 田盛丰. 入侵检测系统报警信息聚合与关联技术研究综述[J]. 计算机研究与发展, 2006, 43(1): 1-8.

[7] Koike H, Ohno K. SnortView: Visualization System of Snort Logs[C]//Proceedings of ACM Workshop on Visualization and Data Mining for Computer Security. [S. 1.]: ACM Press, 2004: 143-147.

[8] Koike H, Ohno K, Koizumi K. Visualizing Cyber Attacks Using IP Matrix[C]//Proceedings of VizSEC'05. [S. 1.]: IEEE Press, 2005: 91-98.

[9] Abdullah K, Lee C, Conti G. IDS Rainstorm: Visualizing IDS Alarms[C]//Proceedings of VizSEC'05. [S. 1.]: IEEE Press, 2005: 1-10.

[10] Livnat Y, Agutter J, Moon S. A Visualization Paradigm for Network Intrusion Detection[C]//Proceedings of 2005 IEEE Workshop on Information Assurance And Security. [S. 1.]: IEEE Press, 2005: 92-99.

[11] Shiravi H, Shirav A, Ghorbani A. IDS Alert Visualization and Monitoring Through Heuristic Host Selection[C]// Proceedings of the 12th International Conference on Information and Communications Security. Barcelona, Spain: IEEE Press, 2010: 445-458.

[12] Zhao Ying, Zhou Fangang, Fan Xiaoping. IDSRadar: a Real-time Visualization Framework for IDS Alerts[J]. Science China Information Sciences, 2013, 56(8): 1-12.

[13] Xi Rongrong, Yun Xiaochun, Jin Shuyuan. Research Survey of Network Security Situation Awareness[J]. Journal of Computer Applications, 2012, 32(1):1-4.

编辑 索书志

(上接第 14 页)

参考文献

[1] 袁红林. 射频指纹识别系统的数学模型研究[J]. 通信技术, 2009, 42(6): 113-114, 117.

[2] 袁红林. 射频指纹的产生机理与唯一性[J]. 东南大学学报: 自然科学版, 2009, 39(2): 230-233.

[3] 袁红林, 胡爱群, 陈开志. 射频指纹的唯一性研究[J]. 应用科学学报, 2009, 27(1): 1-5.

[4] Rasmussen K B, Capkun S. Implication of Radio Fingerprinting on the Security of Sensor Networks[C]//Proc. of International Conference on Security and Privacy in Communications Networks and the Workshops. Nice, France: [s. n.], 2007.

[5] Ureten O, Serinken N. Wireless Security Through RF Fingerprinting[J]. Canadian Journal of Electrical and Computer Engineering, 2007, 32(1): 27-33.

[6] Ureten O, Serinken N. Bayesian Detection of Radio Transmitter Turn-on transients[C]//Proc. of NSIP'99. Antalya, Turkey: [s. n.], 1999.

[7] Hall J, Barbeau M, Kranakis E. Enhancing Intrusion Detection in Wireless Networks Using Radio Frequency Fingerprinting (Extended Abstract)[C]//Proc. of IEEE Congress on Communications, Internet, and Information Technology. [S. l.]: IEEE Press, 2004.

[8] Haartsen J C. The Bluetooth Radio System[J]. IEEE Personal Communications, 2000, 7(1): 28-36.

[9] Hall J, Barbeau M, Kranakis E. Detection of Transient in Radio Frequency Fingerprinting Using Signal Phase[C]//Proc. of Conference on Wireless and Optical Communications. [S. l.]: ACTA Press, 2003.

[10] Ureten O, Serinken N. Detection of Radio Transmitter Turn-on Transients[J]. Electronics Letters, 1999, 35(23): 1996-1997.

[11] Hu Yih-Chun, Perrig A, Johnson D B. Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks[C]// Proc. of IEEE Conference on Computer Communications. [S. l.]: IEEE Press, 2003.

[12] Wang Xia, Wong J. An End-to-end Detection of Wormhole Attacks in Wireless Ad-hoc Networks[C]//Proc. of COMPSAC'07. Beijing, China: [s. n.], 2007.

编辑 金胡考