基于无线信道特征的密钥生成与提取研究

隋 雷[1,2] 郭渊博[1,2,3] 姜文博[1,2] 杨奎武[1,2]
(中国人民解放军信息工程大学 郑州 450001)[1] (数学工程与先进计算国家重点实验室 郑州 450001)[2]
(通信信息控制和安全技术重点实验室 嘉兴 314033)[3]

摘 要 基于无线物理层信道特征参数构建密钥是依据无线信道衰落和噪声的客观存在,利用通信双方共享信道的时变性、互易性及唯一性,在评估彼此高度相关的信道参数的基础上协商提取密钥的一种物理层安全"一次一密"解决方案,具有无条件安全的属性。由于这方面的研究在现实应用中既可避免现行"四次握手"导致的安全漏洞,又摆脱了预分发密钥机制的限制,从而成为了无线网络安全领域的热点之一。对此领域的理论基础进行了分析,对物理层信道特征密钥生成和密钥提取这两个关键技术问题的研究现状进行了梳理,并按照评价指标探讨了现有方案存在的一些问题。最后,讨论了下一步研究的重点。

关键词 无线信道,特征参数,物理层安全,密钥生成与提取
中图法分类号 TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.2.030

Generation and Extraction of Secret Keys Based on Properties of Wireless Channels

SUI Lei[1,2] GUO Yuan-bo[1,2,3] JIANG Wen-bo[1,2] YANG Kui-wu[1,2]
(PLA Information Engineering University, Zhengzhou 450001, China)[1]
(State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China)[2]
(Science and Technology on Communication Information Security Control Laboratory, Jiaxing 314033, China)[3]

Abstract Generating secret keys based on properties of wireless channels is a secure "one pad one key" solution at the physical layer, having the property of unconditional security, where secret keys are extracted collaboratively. According to fading wireless channels noises, evaluation of highly correlated channel parameters, the time-variable, reciprocal and unique natures of channels shared by both parties of communications are used. The work becomes one of the hotspots in wireless network security, because it can avoid security vulnerabilities in the 4-way handshake of the prevailing wireless networks and free itself of the limits in pre-distributing secret keys in practical application. The theoretical foundation of this field was analyzed. The related work of these two key issues, generation and extraction of secret keys based on properties of wireless channels was summarized. The problems of existing schemes according to performance principles were discussed. Finally, the focus of the future work based on existing problems was presented.

Keywords Wireless channel, Characteristic parameter, Security of the physical layer, Generation and extraction of secret keys

1 引言

随着物联网、移动互联网等技术从概念走向应用,无线网络移动性好、扩展能力强、布控灵活等有线网络所无法比拟的优势,使得其应用和覆盖范围越来越广。然而,无线通信由于采用了广播信道的开放性,易遭受窃听、信息篡改、节点模拟等威胁,因此面临着与有线网络安全所不同的新挑战。

在安全技术中,密码是提供网络安全保护最可靠有效的手段,是保障网络安全的基本支撑。但在无线网络环境下,利用密码机制提供机密性、完整性、认证性等服务面临着与有线网络不同的难题,其中最核心的问题就是密钥的生成与管理。首先,基于预分发的密钥分配方法难以适用于无线环境,主要原因在于现有成熟的预分发密钥技术大多都对终端的计算、存储和续航能力要求较高,而无线终端先天具有计算能力有限、有效存储空间小、电源续航能力差等特点,性能上难以满足要求;此外,在战场等应用环境中,一旦发生个别节点被敌方俘获的情况,采用预分发密钥机制就会给整个网络的安全带来巨大的灾难。其次,在没有预共享随机数的情况下进行安全的无线密钥协商存在很大困难,原因在于无线信号具有在空中自由传播的特性,因此很难将密钥协商信息定向地传输到预定的接收端,当信号有效覆盖范围内的同频终端有可能接收到所传输的密钥协商信息时,就给密钥协商过程带来了很大风险。现行的802.11协议无法为管理帧和控制帧提供保护,缺乏认证机制。攻击者可以通过修改MAC地址欺

到稿日期:2014-03-31 返修日期:2014-07-09 本文受国家部委基金资助项目(9140C130103120C13062),河南省科技创新杰出青年计划项目(104100510025)资助。

隋 雷(1986—),男,硕士生,主要研究方向为无线网络安全,E-mail:SuiLeiCourage@163.com;郭渊博(1975—),男,博士,副教授,主要研究方向为无线网络安全;姜文博(1987—),男,硕士生,主要研究方向为无线网络安全;杨奎武(1979—),男,博士,主要研究方向为无线网络安全。

骗合法节点，节点无法确定消息来源的真实性，导致在“四次握手”过程中易遭受中间人等攻击。再次，密钥有效管理难度大。网络拓扑变化快对密钥更新提出了很高的实时性及安全性要求；指数级增长的对称密钥数量使得管理变得复杂而难以实现；对于通信实体依靠空中建立的点对点连接而言，证书发放机构和密钥管理中心的可靠性很难得到保证。鉴于以上原因，迫切需要新型密钥生成管理模型与方法。

Maurer[1]、Hershey[2]等人先后发现无线通信双方使用的信道具有随机源特性并可作为随机信号源。基于无线信道特征的密钥生成与提取方法是一种研究无线物理层固有特性的信息论安全方案，与传统的 Diffie-Hellman 密钥协商协议所不同，其不假设对手计算能力受限，这引发了人们极大的兴趣，各种算法相继被提出和改进。

基于无线信道特征生成密钥的方法之所以能够有效应用于无线安全通信环境中，主要原因在于：(1)从管理方式上讲，规避了传统无线密钥协商带来的安全风险，无需“四次握手”环节，无线通信双方可在不依靠安全基础设施或其它可信第三方存在的前提下自主完成密钥的生成与提取，无需预分发密钥；(2)从安全性上讲，将信息论安全理念应用到无线网络，具有无条件安全的特性，同时也去除了预分发密钥的弊端。

当前，已有相当数量的密钥生成及提取技术被提出，但总体来看仍处于探索阶段，距离实用化尚有一段距离。本文将介绍基于物理层信道特征生成和提取密钥的基本和通用框架，对已有协议和方案从密钥不一致率、密钥比特生成速率、密钥比特位的随机性 3 方面进行性能比较，并对未来的研究重点提出建议。

2 理论基础

因反射体、衍射体及散射体在通信实体间或周围的客观存在，实际无线通信传播多为多径环境，接收机接收的信号是不同时延的多径之和。此外，环境和终端的相对变动都可能随机改变路径，导致接收信号幅度和相位的随机变化。这种随机变化产生了以下 4 个属性作为基于无线物理层信道特征生成和提取密钥的基础[3,4]。

随机性：源信号从发送机经复杂的多径衰落过程到达接收机，多路径的信号复合使得到达接收机的信号是关于发送机信号的一个随机失真，具有随机源特性。

快速时变性：客观无线环境随时间快速变化，使得信道特征，在时间间隔大于信道一致时间的条件下，彼此是独立的。快速时变性有助于实现一次一密。

快速空变性：依据微波理论得出相距半个波长以上的两个天线经历的衰落是不相干的结论[5]。对处于信号若干个波长以外位置的窃听者而言，窃取有用信息是不可能的。

短时互易性：在相干时间内，信道对于同时同频通信的无线链路两端的收发器产生的衰落理论上是一致的，满足短时互易性。

因此，利用无线信道特征构建密钥是一个合理的思路，能够有效解决无线环境中的密钥生成与分发问题。为了更直观地说明物理层密钥生成方法，本节详细阐述其重要基础：信道互易模型(见图 1)，Alice(简记 A)和 Bob(简记 B)为处在多径衰落环境下采用 TDD 模式的合法通信节点，Eve(简记 E)为不能产生强干扰的被动窃听者，h_{XY} 代表 Y 所感知到的 X 与 Y 间的信道响应(其中 $X,Y\in S(A,B,E)$)。为了评估随机信道参数，Alice 和 Bob 必须交替地给对方发送探测信号 $s(t)$。Alice 和 Bob 作为接收机时接收到的信号可以表示为：

$$r_{BA}(t)=s(t)h_{BA}(t)+n_{BA}(t) \tag{1}$$

$$r_{AB}(t)=s(t)h_{AB}(t)+n_{AB}(t) \tag{2}$$

Eve 作为窃听者接收到的 Alice、Bob 所发送的信号分别为：

$$r_{AE}(t)=s(t)h_{AE}(t)+n_{AE}(t) \tag{3}$$

$$r_{BE}(t)=s(t)h_{BE}(t)+n_{BE}(t) \tag{4}$$

以上等式中，$s(t)$代表训练信号；$n(t)$为各接收机处彼此不相关的随机噪声；利用收到的信号，Alice 和 Bob 分别对信道参数进行评估。由互易性原理可知，在相干时间内信道参数变化量很小，h_{AB} 与 h_{BA} 有极强的相似性，可假定二者相等。当 Eve 距离任一合法通信方大于半个波长时，其所感知的信道状态与该合法用户有极低的相关性[3]，即 $h_{AE}(t)$、$h_{BE}(t)$ 与 $h_{AB}(t)$、$h_{BA}(t)$ 是不相关的。由于 $h_{AE}(t)\neq h_{BE}(t)\neq h_{AB}(t)$ $(h_{BA}(t))$，$n_{AE}(t)\neq n_{BE}(t)\neq n_{AB}(t)\neq n_{BA}(t)$，$r_{AE}(t)$、$r_{BE}(t)$ 与 $r_{BA}(t)$ 、$r_{AB}(t)$互不相关，Eve 不可能估计出与 Alice、Bob 完全相同的信道特征。合法节点通过量化及密钥一致性协商可以将信道参数评估值转化为相同的比特串，再利用隐私加强技术，也就是筛选一部分作为密钥，去除在协商过程中可能造成泄露的成分。需指出的是，信道参数是时变的，基于信道特征参数提取出来的密钥序列也具有定时更新的动态性，这使得窃听者破解变得更加困难，从而保证了通信的安全需求。

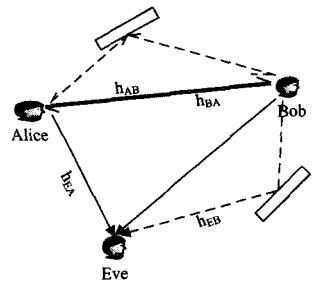

图 1 有窃听者 Eve 存在的情况下信道互易性模型

3 相关研究

自基于物理层信道参数构建密钥概念提出以来，已展开相当数量的研究，取得了很多成果。下面从密钥生成技术、提取技术和结合性研究 3 个方面对现有研究工作进行归纳总结。

3.1 密钥生成技术研究

密钥生成技术是指利用通信技术和手段生成为通信双方安全所共享的随机信道参数，作为密钥提取材料。其研究的主要目标在于确保通信双方信道参数的高一致性和在确保参数随机性的前提下加快参数的评估速率。

密钥生成技术依据所采用的信号源可分为两类，以第一类研究为主。具体如下。

第一类是通信双方互发训练序列，通过对比接收信号与训练序列的幅度和相位等信息差异来评估高度相关的信道参数。这类研究中以针对单天线的通信系统研究为主。其中，文献[6]使用基于波束形成技术(beam-forming)的 ESPAR 天线(electronically steerable parasitic array radiator)通过调节天线的阻抗值来改变天线的波束，双方收发通信过程中步调一致，确保窃听者不能够获得良好的信道参数信息的同时，能够提高信道的波动幅度，加速密钥的生成。文献[3]实验中采

用基于 802.11 中 MAC 地址过滤来提取 Ping request、Ping response、ACK1 和 ACK2 4 种数据包，用时间戳记录和区分各个包的信号强度，有效解决了所提取参数先后顺序的精确性问题。创新型密钥生成研究还包括协作生成密钥研究[7]、多输入多输出条件下密钥生成研究[8]等，其中已有研究指出多天线技术能大大提高密钥的生成速率。利用协作技术生成密钥主要是在密钥生成的过程中引入合法的协作者，通过增强信道的波动幅度，来提高密钥的生成速率并降低窃听导致的安全风险；多输入多输出技术能增强通信双方共有信道信息的数量和熵值，提升了系统的安全性能。

第二类是物理上临近的无线设备可以利用共有的公开 RF 源，比如电视信号、蜂窝信号等进行密钥提取，根据通信安全保密半径的需要动态地选择公开 RF 源[3]，合法通信双方进行安全的密钥生成匹配速率取决于二者的物理距离及共有公开 RF 源衰落的变化快慢。可以通过同时监测多个公开 RF 源或同时摇动双方合法通信节点来达到提升密钥生成匹配速率的目的，此项研究已经从理论和实验两个层面得到了证明。

3.2 密钥提取技术研究

已有密钥提取研究主要包括基于接收信号强度 RSS(Received Signal Strength)和信道相位(Channel Phase)两大类，此外还有少量关于其它参数的提取算法研究，如信道状态信息(CSI)、信道脉冲响应(CIR)、信号包络等信道特征。总体上讲，无论基于何种特征参数，方案大致都包括 3 个部分：(1)信道特征参数评估阶段；(2)参数量化阶段；(3)密钥一致性协商及隐私加强阶段。合法用户密钥建立流程如图 2 所示。

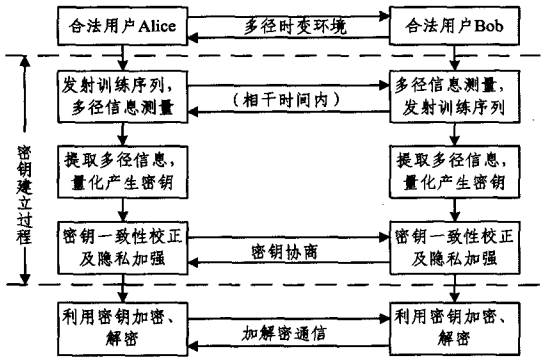

图 2 合法用户密钥建立流程图

3.2.1 已有方案归纳

A. 基于 RSS 生成方案。RSS 是一种对所接收无线电信号能量的一种度量，利用 RSS 生成密钥的研究多是依据所设定门限对采样值进行量化判决，经典的是 Level-crosing 算法[3]，核心是量化器 $Q(x)$：

$$Q(x)=\begin{cases}1, & \text{if } x>q_+\\ 0, & \text{if } x<q_-\end{cases}$$

其中，x 为测量值，q_+、q_-)分别为上门限值和下门限值，大于 q_+ 的值量化为 1，小于 q_-)的值量化为 0，处于上下门限值之间的测量值被丢弃。现有的算法使用不同的规则来确定门限值和选取采样值。文献[9]的门限值取决于采样值的平均值及标准方差，为提高一致率，其采取了连续 m 个(m 为可设置的变量参数)同一量化区间值产生 1 比特，这大大降低了密钥生成速率。文献[4]在文献[9]的基础上，提出一种自适应的密钥生成算法(Adaptive Secret Bit Generation)，将 RSS 值序列分为小块，各块单独计算门限，这样能去除变化缓慢的成分，提高密钥熵值，同时文献采用基于格雷码的多比特量化方法，这对测量的精确性及信道互易性提出更高的要求，易导致较高的不一致率。文献[6]使用 RSS 测量值的平均值作为单一门限，去除门限值附近的测量值。文献[4]通过实验指出，此种算法输出的比特流有很低的一致性和熵值。文献[10]采用线性内插法来解决通信双方探测时间不一致的问题，并且采用 KLT 策略(Karhunen-Loeve Transform)去除测量值间的相关性，最高的密钥速率可达 22b/s。

B. 基于信道相位生成方案。相比基于 RSS 的密钥生成，基于相位生成密钥有 3 个主要的优势：(1)在窄带衰落信道中接收信号的信道相位满足均匀分布。(2)现有的信号处理技术允许对于接收信号的高速率的分解评估，这意味着高速率的密钥生成是可以达到的。(3)相位评估能在多个节点间累积，这就为组密钥生成创造了条件。文献[11]是最早的基于相位生成密钥的可查文献，其将多路频率正交的正弦信号作为导频发送，并利用其相位差分发密钥。文献[12,13]是关于 OFDM 系统信道相位生成密钥的文献，文献[14]提出一种通过提取各子载波相位生成密钥的方案，不足之处是仅针对 Rayleigh 衰落信道，并未扩展到其它衰落环境的情形。文献[15]设计了一种同时适用单对密钥及组密钥的方案。

C. 基于其它特征参数的生成方案。除了 RSS 和相位两类主要的特征外，还有少量基于其它信道状态信息(CSI)[16]、信道脉冲响应(CIR)[9,17]等信道特征的提取算法研究。文献[16]给出了利用 CSI 进行密钥提取的方案，CSI 较 RSS 能提供更为丰富的信道信息，在 OFDM 中 CSI 能够提供各子载波的信号强度而不仅仅是整个信号的强度。文献[9,17]分别给出了两种利用 CIR 提取密钥的方法，不足之处是针对的是理想环境，没有考虑噪声的影响。

3.2.2 各类方案性能指标对比

总体上讲，基于 RSS 与基于信道相位的最大区别在于：因 RSS 在现行网卡中易于提取，未来也最有可能率先在实际中得到应用，所以基于 RSS 的研究最为广泛；基于信道相位的方案显现出较 RSS 更准确和更高速的密钥提取效果，然而因其需要工作在奈奎斯特频率的模数转换器上，而现有无线设备不具有这一功能，大大限制了其实现和应用。

生成与提取物理层密钥提取算法性能评价指标主要有 3 个[3]：(1)密钥的生成速率 R_k，$R_k=N/T$(bit/s)，其中 N 为时间 T 内生成的比特流的数目。R_k 反映着算法的效率；(2)所提取密钥的不一致率 $P_K=1-(1-P_e)^N$，其中 P_e 表示单个比特出错的概率，N 为比特流长度。P_K 反映着算法的强壮性；(3)密钥随机性，随机性反映着密钥的安全性。现在随机性普遍使用 NIST(National Institute of Standards and Technology)测试[18]。

密钥生成速率：为了保证随机性，基于 RSS 的方案因其在相干时间内只能探测一次，基本的 RSS 方案密钥的生成速率仅为 1～3bit/s，制约了密钥的生成速率，加快信道的变化能提高密钥的生成速率；CSI 能提供各子载波的信号强度，明显提高密钥生成速率；而基于信道相位的密钥生成不受此限制。

密钥不一致率：静态环境下基于 RSS 的密钥不一致率很高，达到 50%。移动环境下有很大改善。CIR 的测量较 RSS 精确，所以同等条件下其不一致率要高于 RSS 方案。文献[14]指出基于相位的方案的不一致率取决于信噪比 SNR

(signal-to-noise ratio)。

随机性：文献[4]指出基于 RSS 生成密钥的随机性取决于信道的变化快慢。当信道变化缓慢时，由 RSS 生成的密钥变化非常单调，会导致出现多比特连续 0 或 1，易被破解，并且随机性与密钥生成速率存在着矛盾。而文献[14]指出基于相位的方案不存在这样的限制，即使信道变化缓慢，初始相位也能给密钥比特提供很高熵值，保证了随机性。

3.2.3 小结

不同参数的无线信道、不同调制方式的信号具有迥异的衰落特性，所以很难提出一个普适方案，而应根据传输信道的特征及传输信号的特点，提取适宜的信道参数，配上与之相符的密钥提取算法。

基于不同特征参数的方案的密钥一致性协商及隐私放大技术具有通用性。现有的策略主要包括基于 Cascade 的协商机制[4]、采用 Hash 函数进行密钥一致性确认[3]、利用低密度奇偶校验码(Low Density Parity Check Code，LDPC)编码校正[19]等，根据无线系统信道状态合理地选取协商策略，能够提高密钥一致率和降低密钥协商带来的资源消耗。

3.3 与认证系统的融合性研究

对于基于无线信道参数生成密钥的结合性研究主要体现在与认证技术的结合性。

信息机密性与鉴权认证一体化成为本研究的又一亮点。通信双方在密钥生成的同时，利用相邻测量值的相干性来进行鉴权认证，进而确认目的节点的合法性[20]。文献[21]提出了一个基于信道冲击响应(CIR)结合假设检验的物理层认证方案，该方案依据连续的 CIR 变化来鉴别发射机的身份，比较的是噪声缓解后的 CIR，减轻了噪声对判定结果的影响。作者采用 OFDM 系统进行了验证及相关理论分析。文献[22]分析了在 802.11 系统中鉴权与密钥生成相结合的增强加密方案，分析了该新思路与现有加密系统的融合问题，为实际应用提供了指导。文献[23]指出了基于无线信道特征认证在非密码认证体系中的地位及优缺点。文献[24]指出现有的研究主要是基于认证和密钥提取，且二者多是分开研究的，首次针对无线体域网(Body Area Networks)将两者结合来研究，不依赖特殊的硬件设备及带外信道。方案采用相对静态的环境进行身份认证，相对动态的环境进行密钥生成。

有相当数量研究是利用物理层信道特征进行针对身份验证的攻击检测。文献[25]提出在 Ad hoc 网络中基于信道状态信息来进行对黑洞攻击的检测。文献[26]指出利用 RSS 对静态环境中基于身份的攻击进行检测，并基于 802.11 协议进行了验证。

然而，已有方案因在安全通信建立之前未能拥有通信对方的任何特有信息，通信节点首次通信时存在着若仅仅依靠物理层信道特征认证则无法确定对方真实身份的问题。现有研究多是假定通信双方已经通过上层协议的密码机制实现了双方的首次身份认证，这往往代价较大，且没有利用物理层本身优势。事实上，可以考虑利用设备的物理指纹，设计高效的认证协议来解决首次通信的身份认证问题[27]。

4 可进一步研究的方向

以上问题产生的根源在于现行物理硬件上及通信技术的限制及所设计方案的不足，针对这些问题，下述方向值得进一步深入地研究。

首先，加强信道估计一致性研究。

信道估计的一致性难以保证的原因有 3 个：(1)现用的无线网卡多是半双工的，通信双方进行信道评估不可能完全时间一致；(2)通信双方独立噪声的存在以及量化等人为噪声的干扰；(3)通信双方的网卡等硬件的差异。而信道估计一致性对于密钥提取至关重要，能提高密钥生成速率和降低密钥比特不一致率。

其次，加强性能指标间矛盾调和策略研究。

性能指标间矛盾难以调和，具体原因为要达到密钥高生成速率的目标就需加快对信道特征信息的探测，而这会导致前后所提取信息的高相关性，降低随机性，大大增加了被敌方破解的危险系数，同时干扰双方信号的高相关性，导致较高的不一致率。而要增加密钥生成的高一致性往往需要增加通信双方彼此间的信息协商，这在降低系统安全性的同时也大大增加了系统的通信代价，制约了密钥生成速率的提升。如何能权衡三者间的代价关系，寻求次优的调和策略值得深入研究。

再次，抗新型窃听模式研究。

现有的方案模型主要考虑的是被动窃听模型，而实际应用中主动窃听更普遍且对密钥的建立过程造成的干扰和威胁更大，因此应加强对主动窃听情形的研究。同时，物理层通信新技术的发展丰富了窃听形式，即不再仅仅是单用户单天线窃听一种模式，增加了诸如多用户窃听、多天线窃听、中继窃听、协作窃听等形式。为确保安全性，应加强抗这些新型窃听模式的研究。

最后，考虑与 PUF 技术的结合。

将物理层密钥生成技术与 PUF 技术结合，优化身份认证方案。轻量级的物理不可克隆 PUF(Physical Unconable Function)技术也是一项全新的研究课题。它是利用设备特有的物理特性，产生一个不可复制、防篡改的唯一激励响应，进而实现认证[28-30]。若能与物理层密钥生成技术结合起来，则能有效解决首次通信节点的认证问题，同时因其与密钥生成同步进行也能提高认证效率。

结束语 基于无线物理层生成密钥作为物理层安全的一个分支，是一个具有很大潜力的研究课题。针对现有无线物理层生成和提取密钥的研究工作进行了概述，阐述了理论依据、归纳了已有研究及在总结分析现有研究进展的基础上对下步研究需要注意的问题及给出了研究方向的扩展的建议。总体上看，基于无线信道特征参数的密钥生成与提取技术还处在理论研究阶段，但其给无线网络的安全保密指引了新的方向。当前的研究还未充分利用无线信道丰富的衰落信息资源，在下一代无线通信的体制建设中，可以考虑基于无线物理层特性生成密钥技术的应用，使其从理论研究走向实际应用。

参 考 文 献

[1] Maurer U M. Secret key agreement by public discussion from common information[J]. IEEE Transactions on Information Theory, 1993, 39(3): 733-742

[2] Hershey J E, Hassan A A, Yarlagadda R. Unconventional cryptographickeying variable management[J]. IEEE Transactions on Communicat-ions, 1995, 43(1): 3-6

[3] Mathur S. Building information-theoretic confidentiality and traffic privacy into wireless networks[D]. New Brunswick: Rut-

gers University Graduate School, 2010

[4] Jana S, Premnath S N, Clark M, et al. On the effectiveness of secret key extraction from wireless signal strength in real environments[C]// Proceedings of the 15th Annual International Conference on Mobile Computing and Networking. ACM, 2009: 321-332

[5] Jakes W C, Cox D C. Microwave mobile communications[M]. Piscataway, NJ, USA: Wiley-IEEE Press, 1994: 11-50

[6] Aono T, Higuchi K, Ohira T, et al. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels[J]. IEEE Transactions on Antennas and Propagation, 2005, 53(11): 3776-3784

[7] 王莅康, 吴越. 基于信道特征的协作密钥提取技术研究[J]. 信息安全与通信保密, 2011, 9(6): 98-101

[8] Wallace J W, Chen C, Jensen M A. Key generation exploiting MIMO channel evolution: algorithms and theoretical limits[C]// 3rd European Conference on Antennas and Propagation, 2009 (EuCAP 2009). IEEE, 2009: 1499-1503

[9] Mathur S, Trappe W, Mandayam N, et al. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel [C]// Proceedings of the 14th ACM International Conference on Mobile Computing and Networking. ACM, 2008: 128-139

[10] Patwari N, Croft J, Jana S, et al. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements[J]. IEEE Transactions on Mobile Computing, 2010, 9 (1): 17-30

[11] Hassan A A, Stark W E, Hershey J E, et al. Cryptographic key agreement for mobile radio[J]. Digital Signal Processing, 1996, 6 (4): 207-212

[12] Sayeed A, Perrig A. Secure wireless communications: Secret keys through multipath[C]// IEEE International Conference on Acoustics, Speech and Signal Processing, 2008 (ICASSP 2008). IEEE, 2008: 3013-3016

[13] Kitaura A, Sasaoka H. A scheme of private key agreement based on the channel characteristics in OFDM land mobile radio[J]. Electronics and Communications in Japan (Part III: Fundamental Electronic Science), 2005, 88(9): 1-10

[14] Wang Q, Su H, Ren K, et al. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks [C]// 2011 Proceedings IEEE INFOCOM. IEEE, 2011: 1422-1430

[15] Wilson R, Tse D, Scholtz R A. Channel identification: Secret sharing using reciprocity in ultrawideband channels[J]. IEEE Transactions on Information Forensics and Security, 2007, 2 (3): 364-375

[16] Zhao J, Xi W, Han J, et al. Efficient and secure key extraction using CSI without chasing down errors[OL]. http://arxiv.org/abs/1208.0688

[17] Hsmida S T B, PierrotJ B, Castelluccia C. An adaptive quantization alg-orithm for secret key generation using radio channel measurements[C]// 2009 3rd International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 2009: 1-5

[18] Rukhin A, Soto J, Nechvatal J, et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications[R]. Booz-Allen and Hamilton Inc Mclean Va, 2001

[19] Ye C, Reznik A, Shah Y. Extracting secrecy from jointly Gaussian random variables[C]// 2006 IEEE International Symposium on Information Theory. IEEE, 2006: 2593-2597

[20] Xiao L, Greenstein L J, MandaYam N B, et al. Using the physical layer for wireless authentication in time-variant channels[J]. IEEE Transactions on Wireless Communications, 2008, 7(7): 2571-2579

[21] Liu F J, Wang X, Tang H. Robust physical layer authentication using inherent properties of channel impulse response[C]// Military Communications Conference, 2011 (MILCOM 2011). IEEE, 2011: 538-542

[22] Mathur S, Reznik A, Ye C, et al. Exploiting the physical layer for enhanced security [J]. IEEE Transactions on Wireless Communications, 2010, 17(5): 63-70

[23] Zeng K, Govindan K, Mohapatra P. Non-cryptographic authentication and identification in wireless networks [J]. IEEE Transactions on Wireless Communications, 2010, 17(5): 56-62

[24] Shi L, Yuan J, Yu S, et al. ASK-BAN: authenticated secret key extraction utilizing channel characteristics for body area networks[C]// Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks. ACM, 2013: 155-166

[25] Jain S, Ta T, Baras J S. Wormhole detection using channel characteristics[C]// 2012 IEEE International Conference on Communications (ICC). IEEE, 2012: 6699-6704

[26] Zeng K, Govindan K, Wu D, et al. Identity-based attack detection in mobile wireless networks[C]// INFOCOM, 2011 Proceedings IEEE. IEEE, 2011: 1880-1888

[27] 张紫楠, 郭渊博, 杨奎武, 等. 通用可组合认证密钥交换协议[J]. 西安电子科技大学学报: 自然科学版, 2014, 41(5): 209-215

[28] Hammouri G, Ozturk E, Sunar B. A Tamper-Proof and lightweight aut-hentication scheme[J]. Pervasive and Mobile Computing, 2008, 4(6): 807-818

[29] Ozturk E, Hammouri G, Sunar B. Towards robust low cost authentication for pervasive devices[C]// Sixth Annual IEEE International Conference on Pervasive Computing and Communications, 2008 (PerCom 2008). IEEE, 2008: 170-178

[30] Schulz S, Sadeghi A R, Wachsmann C. Short paper: lightweight remote attestation using physical functions[C]// Proceedings of the Fourth ACM Conference on Wireless Network Security. ACM, 2011: 109-114

(上接第 113 页)

[7] 潘晓, 郝兴, 孟小峰. 基于位置服务中的连续查询隐私保护研究[J]. 计算机研究与发展, 2010, 47(1): 121-129

[8] 陈玉凤, 刘学军, 李斌. 基于博弈论的用户相互协作的位置隐私保护方法[J]. 计算机科学, 2013, 40(10): 92-97

[9] 黄毅, 霍峥, 孟小峰. CoPrivacy: 一种用户协作无匿名区域的位置隐私保护方法[J]. 计算机学报, 2011, 34(10): 1976-1985

[10] 潘晓, 肖珍, 孟小峰. 移动位置隐私保护[J]. 计算机科学与探索, 2007(10): 268-281

[11] Bamba B, Liu L. Supporting anonymous location queries in mobile environments with privacy grid[C]// Proc of Int Conf on World Wide Web (WWW). New York: ACM, 2008: 237-246

[12] Brinkhoff T. A framework for generating network based moving objects[J]. GeoInformatica, 2002, 6(2): 153-180