基于虚拟信道的快速密钥生成协议的安全性分析

陈大江[1]，秦 臻[2]，秦志光[1]，王瑞锦[1]

(1. 电子科技大学计算机科学与工程学院 成都 611731；2. 电子科技大学通信与信息工程学院 成都 611731)

【摘要】在无线安全通信中，产生密钥并且保持其安全性是至关重要的。然而，由于无线信道的广播特性，在密钥分发阶段很容易受到各种攻击。利用多径信道的随机性是解决这一问题的可行方案。为了解决现有的基于物理层的密钥分配协议效率低并且依赖节点或者环境移动性的缺点，文献[12]提出了基于虚拟信道的快速密钥生成协议。该文通过理论证明：在多天线敌手的前提下，该协议不能在实现信息论安全的同时提高密钥生成率的理论上界。因此，该协议不是信息论安全的。

关 键 词 信息论安全； 密钥分配； 物理层； 虚拟信道； 无线通信

中图分类号 TP309 文献标志码 A doi:10.3969/j.issn.1001-0548.2015.01.019

On the Security of Fast Secret Key Generation Protocol with Virtual Channel Approach

CHEN Da-jiang[1], QIN Zhen[2], QIN Zhi-guang[1], and WANG Rui-jing[1]

(1. School of Computer Science & Engineering, University of Electronic Science and Technology of China Chengdu 611731;

2. School of Communication and Information Engineering, University of Electronic Science and Technology of China Chengdu 611731)

Abstract It is vitally important to generate keys and keep them secret in secure wireless communications. Due to the broadcast nature of wireless channels, secret key distribution is more vulnerable to attacks in wireless communication. An ingenious solution is to generate secret keys by using the multipath channel as a source of common randomness. To address the problems that the existing physical-based protocols have low key generation rate and high reliance on mobile nodes or environments, a fast secret key generation protocol with virtual channel approach was proposed by HUANG and WANG for static wireless networks. In this paper, we show that, in the presence of an eavesdropper with multiple antennas, the scheme does not improve the theoretical upper bound of the key generation rate with information-theory security. Thus, the protocol is not information-theory security.

Key words information-theory security; key distribution; physical layer; virtual channel; wireless communication

随着无线网络的飞速发展以及无线设备的大量使用，无线通信中的安全问题引起了人们的广泛关注。由于无线通信的广播特性，很容易受到窃听、消息篡改、节点冒充等攻击。为了实现信息的可靠性、完整性和认证性，必须在通信之前实现密钥的安全分配。一方面，由于无线设备往往是电池供能，且计算能力较弱，这使得现有的基于传统密码学方法的密钥分配协议(现有的密钥分配协议通常采用可信第三方体系或者公钥体系，如常用的Diffie-Hellman协议[1]，其特点是计算量大、能耗高)面临着巨大的挑战。另一方面，随着计算机的高速发展以及云计算[2]等新领域的兴起，敌手可获取的计算能力不断提高，这也使得基于计算安全的密钥分配算法不再满足人们对安全的需求。因此，寻求一种计算量小、能耗低且安全性高的密钥分配协议已显得尤为重要。

1 基于物理层的密钥分配协议概述

目前，基于物理层的密钥分配协议[3-10]是解决无线安全中上述难题的可行方法之一。该方法利用通信双方的无线信道特征[3]，通过测量刻画信道多径效应的物理量(如信道增益、相位平移、接收信号强度等)产生密钥。这些信道特征包括：1) 无线信道的时变性：由于多径效应使得信道衰落随着时间而随机变化，且具有较强的随机性；2) 无线信道的空变性：在不同空间位置两个链接的终端的无线信道是独立的；3) 无线信道的自反性：无线信道的多径特征(如信道增益、相位平移、时延等)在链路的两个方

收稿日期：2013－09－12；修回日期：2014－02－17

基金项目：国家科技重大专项(20112X03002-002-03)；国家自然科学基金重点项目(61190110)

作者简介：陈大江(1982－)，男，博士生，主要从事信息论安全、物理层安全、无线安全等方面的研究.

向都是相关的、一致的。基于上述观察，发现在无线通信中存在自然的“随机源”(无线信道的物理特征：信道增益、相位平移、时延等)用于密钥提取，且利用这种随机源能够帮实现信息论安全。

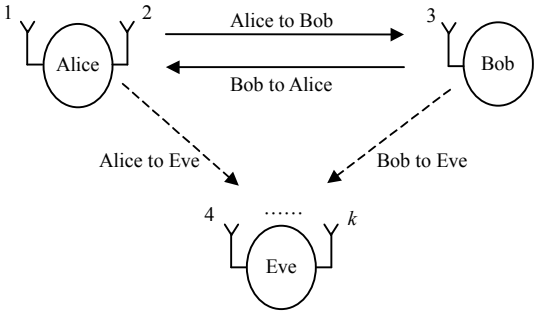

图1　系统模型

现存的基于物理层的密钥提取方案存在着诸多限制，如密钥率低、密钥熵值低、依赖节点或者环境的移动性。目前最高的密钥生成效率只有40 bits/s[7]，达到这一效率要求节点的移动性，且在协议双方还造成了4%的比特错误。造成这一现象的原因是现存的协议依赖信道变化，即如果信道不发生变化就不能产生新的密钥。在静止的环境中信道变化是非常缓慢的，这就使得这些协议不能应用在静止的环境中。根据分析[5]，在静止的环境中窃听者可以判断出密钥信息，这使得密钥的安全性得不到保障。文献[11]引入了一种信道独立的物理层方法来提高信道的变化率。该协议的安全性是基于OFDM系统的数据传输的统计特性实现的，所以该协议并不适用于其他通信系统。

为了解决这一问题，文献[12]提出了通过两根天线改变信道的随机性来提高密钥速率。该协议同时假设敌手也是多天线的，且对敌手天线的数量没有限制。本文中通过实验数据分析指出，对于多天线的敌手，该协议是安全的。但作者并没有证明该协议是信息论安全的。那么该协议是否能在信息论安全的前提下提高密钥生成效率呢？

本文从信息论的角度出发，通过理论证明：文献[12]所提出协议在多天线敌手的前提下，协议中通过改变信道的随机性并不能增加密钥的信息熵。因此，该协议不能实现信息论安全的同时提高密钥生成效率的理论上界。故该协议不是信息论安全的。

2　基于虚拟信道的密钥生成协议

2.1　系统模型

无线通信中，合法用户Alice和Bob在敌手Eve窃听信道的情况下，要实现安全对称密钥的分发来达到安全通信。本文假设Eve知道合法用户间的通信协议，且可以对接收到的信号所在的信道进行信道测量[13]；同时假设Alice具有两根天线，Bob有一根天线，而Eve具有多根天线，如图1[12]所示，将天线按顺序1,2,⋯,k编号。假设通信方式为窄带通信，其结果可以自然地推广到宽带通信。还假设通信信道是相互关联的，即前向信道(从Alice到Bob)和反向信道(从Bob到Alice)的信道增益在相干时间内是相等的。记 h_{13} 和 h_{23} 分别是从Alice的天线1和天线2到Bob的天线3的信道增益，h_{1k} 和 h_{2k} 表示从Alice到Eve的天线k的信道增益。

信道探测方式：当发送方Alice发送已知探测包 $x[m]$，Alice用 $\sqrt{\alpha}\mathrm{e}^{\mathrm{j}\theta_1}$ 乘以$x[m]$在天线1上发射，同时用 $\sqrt{1-\alpha}\mathrm{e}^{\mathrm{j}\theta_2}\,x[m]$在天线2上发射，其中 $\alpha\in[0,1]$，$\theta_1,\theta_2\in[0,2\pi]$。此时，接收方Bob接收的信号可以表示为：

$$y_{\mathrm{AB}}[m]=(\sqrt{\alpha}\mathrm{e}^{\mathrm{j}\theta_1}h_{13}+\sqrt{1-\alpha}\mathrm{e}^{\mathrm{j}\theta_2}h_{23})x[m]+\omega_{\mathrm{AB}} \quad (1)$$

式中，ω_{AB} 表示在Alice和Bob之间的两个信道的高斯白噪声之和，其分布服从期望为0方差为 σ_ω^2 的高斯分布 $N(0,\sigma_\omega^2)$。

为了简化模型，本文只考虑小尺度衰落，没有考虑路径长度对协议的影响，但结论同样适用于大尺度衰落。

同时，敌手Eve的第k根天线所接收到的信号可表示为：

$$y_{\mathrm{AE}^k}[m]=(\sqrt{\alpha}\mathrm{e}^{\mathrm{j}\theta_1}h_{1k}+\sqrt{1-\alpha}\mathrm{e}^{\mathrm{j}\theta_2}h_{2k})x[m]+\omega_{\mathrm{AE}^k} \quad (2)$$

式中，ω_{AE^k} 表示在Alice和Eve的第k根天线之间的两个信道的高斯白噪声之和，其分布服从高斯分布 $N(0,\sigma_\omega^2)$。

从式(1)可以得出，Alice的两根天线到Bob合成的信道增益可以表示为：

$$\boldsymbol{h}_{\mathrm{AB}}=\sqrt{\alpha}\mathrm{e}^{\mathrm{j}\theta_1}h_{13}+\sqrt{1-\alpha}\mathrm{e}^{\mathrm{j}\theta_2}h_{23} \quad (3)$$

称 $\boldsymbol{h}_{\mathrm{AB}}$ 为虚拟信道增益。

2.2　密钥生成协议

关于基于虚拟信道的密钥生成协议的详细阐述，请参考文献[12]。该协议主要包括虚拟信道测量和测量值的量化两个阶段。

虚拟信道测量阶段：首先，Alice确定L组三维向量 $(\alpha,\theta_1,\theta_2)$，从而利用这些向量构成虚拟信道增益：

$$\boldsymbol{h}_{\mathrm{AB}}=[h_{\mathrm{AB}}(1),h_{\mathrm{AB}}(2),\cdots,h_{\mathrm{AB}}(L)] \quad (4)$$

其次，对每一组 $(\alpha,\theta_1,\theta_2)$，Alice利用上节所述的信道探测方式向Bob发送长度为M的复探测信号X；最

后，对于每一组 $(\alpha,\theta_1,\theta_2)$，Bob接收到分量如式(1)所示的$M$长信号序列，并利用基于训练的信道评估方法[13]测量出虚拟信道增益。Bob得到的虚拟信道增益记为：

$$\boldsymbol{h}_{\mathrm{AB}}^{*}=[h_{\mathrm{AB}}^{*}(1),h_{\mathrm{AB}}^{*}(2),\cdots,h_{\mathrm{AB}}^{*}(L)] \tag{5}$$

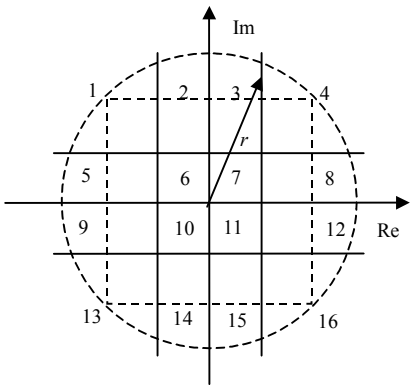

图2 量化区域的划分

测量值的量化阶段：记 r 为向量[h_{13}，h_{23}]的模长。将以原点为中心 r 为半径的复圆面分割成如图2[12]所示的16个区域。其中，第6、7、10区域是边长为0.25的正方形。Alice首先在16个区域中随机(均匀的)选择一个区域，然后在该区域中随机(均匀的)选择一个点作为虚拟信道增益，最后，确定一组三维向量 $(\alpha,\theta_1,\theta_2)$ 来合成这个点。Bob通过信道测量把每个测量值对应到相应的区域。Alice和Bob利用Gary编码把区域编号映射成比特流。

3 信息论安全基础

3.1 信息熵与互信息

在信息论中，信息熵刻画了一个随机变量的不确定程度。记 X 是一个连续型随机变量，则 X 的信息熵 $H(X)$ 如下所示：

$$H(X)=\int_S f(X)\log f(x)\mathrm{d}x$$

式中，$f(X)$ 表示变量的概率密度函数；S 表示变量的支撑集。给定随机变量 Y 的条件下，变量 X 的条件熵记为 $H(X\mid Y)=H(X,Y)-H(Y)$。随机变量 X 和 Y 的互信息 $I(X,Y)=H(X)-H(X\mid Y)$。在给定随机变量 Z 的条件下，随机变量 X 和 Y 的互信息记为 $I(X,Y\mid Z)=H(X\mid Z)-H(X\mid Y,Z)$。

3.2 信息论安全

传统的密码学的安全性都是基于某一个计算假设，称之为计算安全，如常用公钥密码体系RSA，其安全性是基于“大整数的因式分解是NP问题”。计算安全的弱点包括：1) 假设敌手的计算能力是有限的。当敌手的计算能力在假设的范围内，系统是安全的；当敌手的计算能力高于假设，则系统将不再安全。2) 计算安全的安全性验证是基于复杂性理论，而一个问题的复杂度是由最极端的情况决定的，即存在这样的情况：虽然问题的复杂度很高，但对于该问题的某些情况甚至很大一部分情况的复杂度却是比较低的。3) 随着“云计算”的不断发展，人们所拥有计算能力也在不断提高，这对计算安全的系统是一个巨大的挑战。4) 量子计算的飞速发展，使得基于量子计算模型的量子计算机逐步成为可能。大量研究证明在图灵机模型下许多NP问题在量子计算模型下具有快速算法。

如果一个密码体系从信息论的角度是安全的，称之为信息论安全[14]。信息论安全的密码体系假设敌手具有无限计算能力，也称之为无条件安全。显然，信息论安全是比计算安全更强的安全定义。

定义 1 称随机变量 M 在一个通信系统中是信息论安全的，当且仅当 $I(M;X)=0$。其中，X 表示敌手的观察到的随机变量。

4 基于信息论的攻击分析

文献[15]给出了基于物理层安全的密钥分配协议的生成密钥率的理论上界。这里的密钥率指的是单位时间内生成密钥的比特数。该上界可表示为：在给定敌手Eve已知信息的条件下，Alice和Bob在单位时间内的所得到的信息的条件互信息。

如果将传统的基于多天线的物理层的密钥分配协议[16]应用到本文中的通信模型(即Alice两根天线，Bob一根天线)，容易证明其理论上界为：

$$\frac{1}{T_{\mathrm{C}}}[H(h_{13})+H(h_{23})]$$

式中，T_{C} 为相干时间。

当敌手Eve的天线数目大于等于 2 时，Eve可以通过信道监听来获取得有用的信息，从而降低密钥的生成效率。因此，基于虚拟信道的协议不能增加密钥生成效率。

下面的定理是本文的主要结论。

定理 1 当敌手的天线数大于 2 (即 $k\geq 4$)时，基于虚拟信道的密钥生成协议的密钥率 $\mathrm{R_M}$ 不大于传统的基于多天线的物理层密钥生成协议的密钥率，即：

$$R_M\leq\frac{1}{T_{\mathrm{C}}}[H(h_{13})+H(h_{23})] \tag{6}$$

式中，h_{13} 和 h_{23} 分别是从Alice的天线1和天线2到Bob的天线3的信道增益；$\mathrm{T_C}$ 为相干时间。如果 h_{13} (h_{23})

服从期望为0方差为 σ_{13}^2 (σ_{23}^2)的高斯分布，则：

$$R_M \le \frac{1}{T_C}\ln 2\pi e\sigma_{13}\sigma_{23}$$

证明：不妨假设Eve有两根天线，即 $k=4$。由文献[5]可知，基于虚拟信道的密钥分配协议的理论上界为：

$$R_M = \frac{1}{T_C} I(\boldsymbol{h}_{AB}, \boldsymbol{h}_{AB}^* | \text{View(Eve)}) \tag{7}$$

式中，View(Eve)表示Eve所能得到的所有信息。

对于每一个对于 l ($1 \le l \le L$)，若探测信号序列 X足够长，则Bob能精确的评估出虚拟信道增益，即有：

$$h_{AB}^*(l) = h_{AB}(l) = h_{13}a(l) + h_{23}b(l)$$

令：$\sqrt{\alpha}e^{j\theta_1} = a(l)$，$\sqrt{1-\alpha}e^{j\theta_2} = b(l)$，

故式(7)可改写成：

$$\frac{1}{T_C}H(\boldsymbol{h}_{AB}|\text{View(Eve)}) - H(\boldsymbol{h}_{AB} | \boldsymbol{h}_{AB}^* \text{View(Eve)}) =$$

$$\frac{1}{T_C}H(\boldsymbol{h}_{AB}|\text{View(Eve)}) \tag{8}$$

同样的，Eve可以利用监听到的信号集(如等式(3)所示)采用相同的信道评估方法计算出如下结果：

$$\begin{cases} h_{AE^4}(l) = h_{14}a(l) + h_{24}b(l) \\ h_{AE^5}(l) = h_{15}a(l) + h_{25}b(l) \end{cases} \tag{9}$$

在静态的环境下(此时，相干时间 T_C 相对较长)，Eve能准确地测量出信道增益 h_{14}、h_{24} 和 h_{15}、h_{25}。

解线性方程组(9)可得到：

$$\begin{cases} a(l) = \dfrac{h_{25}h_{AE^4}(l) - h_{24}h_{AE^5}(l)}{h_{14}h_{25} - h_{15}h_{24}} \\ b(l) = \dfrac{h_{15}h_{AE^4}(l) - h_{14}h_{AE^5}(l)}{h_{15}h_{24} - h_{14}h_{25}} \end{cases} \tag{10}$$

故可将等式(8)改写为：

$$\frac{1}{T_C}H(\boldsymbol{h}_{AB}|\text{View(Eve)}) =$$

$$\frac{1}{T_C}H(\boldsymbol{h}_{AB}|\text{View(Eve)}, \{a(l)\}_{l=1}^L, \{b(l)\}_{l=1}^L) \le$$

$$\frac{1}{T_C}H(\boldsymbol{h}_{AB}|\{a(l)\}_{l=1}^L, \{b(l)\}_{l=1}^L) =$$

$$\frac{1}{T_C}H(\{h_{13}a(l) + h_{23}b(l)\}_{l=1}^L | \{a(l)\}_{l=1}^L, \{b(l)\}_{l=1}^L) \le$$

$$\frac{1}{T_C}H(\{h_{13}, h_{23}|\{a(l)\}_{l=1}^L, \{b(l)\}_{l=1}^L) =$$

$$\frac{1}{T_C}[H(h_{13}) + H(h_{23})]$$

其中，最后一个等式成立的原因是序列 $\{a(l)\}_{l=1}^L$ 和 $\{b(l)\}_{l=1}^L$ 的选取与 h_{13}, h_{23} 是独立的。

如果 h_{13} (h_{23})服从期望为0方差为 σ_{13}^2 (σ_{23}^2)的高斯分布，则：

$$R_M \le \frac{1}{T_C}[H(h_{13}) + H(h_{23})] =$$

$$\frac{1}{T_C}\left[\frac{1}{2}\ln 2\pi e\sigma_{13}^2 + \frac{1}{2}\ln 2\pi e\sigma_{23}^2\right] =$$

$$\frac{1}{T_C}\ln 2\pi e\sigma_{13}\sigma_{23}$$

证毕。

上述定理说明在多天线敌手的场景下，利用虚拟信道来实现信息论安全的密钥分配在理论上不能增加密钥的生成效率。进一步，基于虚拟信道的密钥分配协议所产生的密钥只用到了Alice和Bob间的两个信道的信道增益的熵(不确定性)，而随机向量组 (α，θ_1，θ) 并不能增加密钥的熵。这是因为敌手可以利用两根天线所得到的信息来估算出 $\sqrt{\alpha}e^{j\theta_1}$ 和 $\sqrt{1-\alpha}e^{j\theta_2}$。

5　结　论

在基于物理层的密钥分配的研究领域中，如何针对多天线的敌手(特别是天线大于密钥协商方的时候)实现信息论安全的高效密钥分配一直是该领域的一个研究难点。本文从信息论的角度出发，发现文献[12]所提出的密钥分配协议并不是信息论安全的。今后，将对多天线敌手下的信息论安全的快速密钥分配协议的设计进行研究。

参　考　文　献

[1] DIFFIE W, HELLMAN M. New directions in cryptography [J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

[2] ARMBRUST M, FOX A, GRIFFITH R, et al. A view of cloud computing[J]. Communications of the ACM, 2010, 53(4): 50-58.

[3] AZIMI-SADIADI B, KIAYIAS A, MERCADO A, et al. Robust key generation from signal envelopes in wireless networks[C]//Proceedings of ACM CCS. [S.l]: ACM, 2007: 401-410.

[4] MATHUR S, TRAPPE W, MANDAYAM N, et al. Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel[C]//Proceedings of ACM Mobicom. [S.l]: ACM, 2008:128-139.

[5] 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 ACM Mobicom. [S.l.]: ACM, 2009: 321-332.

[6] 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 Wireless Communication, 2010, 9(1): 17-30.

[7] CROFT J, PATWARI N, KASERA S K. Robust uncorrelated bit extraction methodologies for wireless sensors[C]// Proceedings of ACM/IEEE ICNP. [S.l.]: [s.n.], 2010: 70-81.

[8] CHEN D J, QIN Z, MAO X F, et al. SmokeGrenade: an efficient key generation protocol with artificial interference [J]. IEEE Transactions on Information Forensics & Security, 2013, 8(11): 1731-1745.

[9] WANG Q, SU H, REN K, et al. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks[C]//Proceedings of IEEE INFOCOM. [S.l.]: IEEE, 2011: 1422-1430.

[10] CHEN D J, MAO X F, QIN Z, et al. SmokeGrenade: a key generation protocol with artificial interference in wireless networks[C]//Proceedings of IEEE MASS. [S.l.]: IEEE, 2013: 200-208.

[11] GOLLAKOTA S, KATABI D. Physical layer wireless security made fast and channel independent[C]// Proceedings of IEEE INFOCOM. [S.l.]: IEEE, 2011: 1125-1133.

[12] HUANG P, WANG X. Fast secret key generation in static wireless networks: A virtual channel approach[C]// Proceedings of IEEE INFOCOM. [S.l]: IEEE, 2013: 2292-2300.

[13] TUGNAIT J K, TONG L, DING Z. Single-user channel estimation and equalization[J]. IEEE journal of Signal Processing Magazine, 2000, 17(3): 16-28.

[14] LIANG Y, POOR H V. Information theoretic security[J]. Foundations and Trends in Communications and Information Theory, 2009, 5(4-5): 355-580.

[15] AHLSWEDE R, CSISZAR I. Common randomness in information theory and cryptography, part I: Secret sharing[J]. IEEE Transactions on Information Theory, 1993, 39(4): 1121-1132.

[16] ZENG K, WU D, CHAN A, et al. Exploiting multiple antenna diversity for shared secret key generation in wireless networks[C]//Proceedings of IEEE INFOCOM. [S.l.]: IEEE, 2010: 1-9.

编 辑 税 红