文章编号：2095-2163(2019)02-0108-04 中图分类号：TP212.3 文献标志码：A

第三方验证下的基于无线信道特征的密钥提取

丁佳蓉，朱淑文
（上海工程技术大学 电子电气工程学院，上海 201620）

摘 要：随着可穿戴设备的应用越来越广泛，基于体域网医疗监测的数据隐私保护工作日益突出。基于信道特征的密钥提取，可以消除复杂的密钥分发过程和计算开销，但是现有的工作不能有效防止合谋攻击且量化后的密钥传输易受到合谋攻击。为此引入第三方可信机构 Victor 来对体域网通信双方 Alice 和 Bob 进行密钥的校验和分发，不仅可以防止合谋攻击，还承担了信息协调的工作，减少了一部分 Alice 和 Bob 的能源消耗。此外，利用矩形帧结构对量化后的密钥进行处理，便于对密钥运行 ShiftRows 和 ColumnMix 运算，从而保证了量化后的密钥传输的安全性，有效阻止了中间人的攻击。

关键词：体域网；信道特征；合谋攻击；密钥提取；可穿戴传感器；安全通信

Key extraction based on wireless channel characteristics under third-party verification

DING Jiarong, ZHU Shuwen
(School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201620, China)

【Abstract】 With the increasing use of wearable devices, data privacy and confidentiality based on body area network medical monitoring has become increasingly prominent. Key extraction based on channel characteristics can eliminate complex key distribution process and computational overhead, but existing work cannot prevent collusion attacks and the quantized key transmission is susceptible to collusion.To this end, the third-party trusted organization Victor is introduced to verify and distribute the keys of Alice and Bob on both sides of the body area network communication, which not only prevents collusion attacks, but also undertakes information coordination work, reducing some energy consumption of Alice and Bob. In addition, the quantized key is processed by a rectangular frame structure, which is convenient for running ShiftRows and ColumnMix operations on the key, thereby ensuring the security of the quantized key transmission and effectively preventing the attack of the middleman.

【Key words】 body area network; channel characteristics; collusion attack; key extraction; wearable sensor; secure communication

0 引 言

随着无线设备的普及，安全无线通信日渐受到人们的关注，无线体域网技术是目前实现个性化卫生保健的新兴技术。典型的体域网通常由小型传感器组成，安装在身体上记录生命体征并与基站（固定接入点或便携式设备）进行无线通信，以便提供远程监控、实时分析和远程诊断等，从而减轻医疗行业中医护人员的负担。

考虑到体域网中设备资源有限，要保障安全通信，显然无法直接应用传统的加密技术，而是需要采用轻量级的密码技术。经过研究可知，对称密码体制时间复杂度与空间复杂度不高，但存在密钥分发问题。使用 Diffie-Hellman 生成共享密钥交换[1]，部署和执行成本很高，不适合资源受限的传感器设备。基于生理特征的密钥提取伴有高度的噪音和可变性。最近的研究已经将注意力转移到仅基于物理层特征的无线通信安全[2-4]，可以消除复杂的密钥分发过程和计算开销，利用信道特征来进行密钥提取，这种特征是独一无二的，攻击者很难伪造。支持这种方法的理论可描述为[5]：2 个通信节点 Alice 和 Bob 之间的无线信道在本质上是对称的，也就是如果 Alice 和 Bob 使用相同的收发器和天线，并且传输相同的信号，那么这两者也会收到相同的信号。当传感器和基站进行通信时，通过传输数据消息可以对各自的无线链路信道特征进行采样，每一方产生一个独特的密钥，在理想条件下，除了干扰和噪音外，得到的测量结果也是一致的，因此双方获得相同的密钥，可以作为会话密钥。

但是实际情况下，双方提取的信道特征并不是完全对称的，所以通常会引入信息协调来改善不匹配率，这会增加可穿戴设备的能源开销，基于此本文

基金项目：国家自然科学基金(61603242,61702322)。

作者简介：丁佳蓉(1995-)，女，硕士研究生，主要研究方向：智能感知、计算机控制。
通讯作者：丁佳蓉 Email：553353009@qq.com

收稿日期：2018-11-13

拟引入 Victor 来对密钥进行校验和分发，而且 Victor 将同时监控 Alice 到 Bob、Bob 到 Victor、Victor 到 Alice 三条信道，Victor 的引入就可以有效阻止合谋攻击；此外，在现有的研究工作中，没有对量化后的数据进行保护，这就使得核心研究数据更容易受到中间人的攻击，故而本文的方案也便于对量化后的数据进行处理，即使密钥在传输过程中被 Eve 意外监听，也无法直接对生理数据进行加解密，可有效减少中间人的攻击。

1　系统模型

目前，保险公司承保风险和保费精算工作，依赖人的健康信息和对健康行为的遵守。假设 Alice 的大病初愈，保险人为了保证 Alice 能够主动配合康复治疗，长期保持正常的生活作息，便决定在 Alice 身上植入可穿戴传感器，以达到约束和检测 Alice 的目的。假设 Alice 和 Victor 都是符合研究的规定而存在的，Alice 是前期预先设置好的，无法对其内部结构进行修改，当 Alice 想篡改数据时，就必须引入 Eve 参与到信息传输的进程中[6]，通过假冒 Alice 的方法向 Bob 传递信息。无线信道迅速解耦距离大约在半个波长内（在 2.4 GHz 的频率下，$\lambda/2 = 6.25$ cm），对于距离比一个波长更远，信道可以被假定为独立的[7]。为此，研究中即引入了可信第三方 Victor 如图 1 所示，来监视 Alice 和 Bob 的信道特征，当 Alice 引入 Eve 在半波长内，介入 Alice 和 Bob 间会话时，Victor 会发现信道特征的波动，由此可以实现 Alice 的身份信息的认证；并且 Victor 的存在可以避免 Alice 和 Bob 在众目睽睽下传播后，攻击者可以复制密钥指纹并声称与自己有联系，引起关于实际的数据卸载点的混淆。

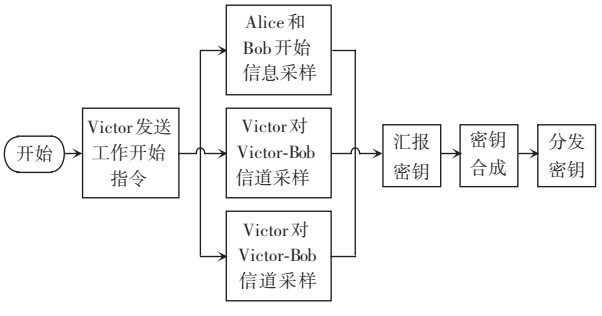

图 1　密钥提取方案

Fig. 1　Key extraction scheme

当 Bob 到达指定现场时，Alice 广播一个 A_Hello 数据包给 Bob；Bob 收到信息后，同时发送 B_Hello 数据包给 Alice，如此反复，当信息量达到足够的比特量，Alice 和 Bob 就会对信道的特征获取足够的采样，再对采样数据进行抽样、量化，即可形成密钥。

可信任的第三方 Victor 使用特定的传输功率 P 向 Alice 和 Bob 广播 Hello 信息 $H(t)$，要求二者在 t s 后响应，Alice 和 Bob 将自己的密钥分享给 Victor，在这里则需要保证 Alice 和 Bob 不知道互相的密钥指纹。Victor 对双方的密钥进行比对，把修正后的密钥发送给 Alice 和 Bob。当不匹配率超过 15%时，Victor 依据对 3 条信道监控获取的信息，即如图 2 所示。当出现连续的两端不匹配率超过 15%时，通过 Victor 对 3 条信道的同步监控，假如发现某条信道检测出数据包的来源不只一个时，便会传送报警提示，告知网络中有 Eve 入侵。

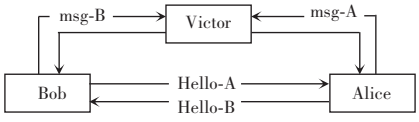

图 2　密钥的获取

Fig. 2　Key acquisition

理想情况下，Alice 和 Bob 接受的 RSS 应该是完全对称的[8]，但实际情况下，Alice 和 Bob 提取的密钥无法完美匹配[9-10]，究其原因可阐释如下。

（1）典型的商用无线收发器是半双工，不能同时发送和接收信号，因此，Alice 和 Bob 必须一次测量一个方向的无线电频道。

（2）存在噪音和干扰、硬件限制、制造变化的差异。在设备静止和较为缓慢移动的环境中，相干时间较长，信道变化也会趋于缓慢，信道探测比特量的熵无法满足密钥的生成所需的熵数。以往的解决方案是在体域网设备中加入信息协调和隐私增强，这会引起很大的内存消耗和传输开销[11]。在本文中，研究把所有高开销、高能耗的任务交给 Victor，可以尝试只在特定的情况下增加运算的开销，大部分时间 Alice 和 Bob 都始终处于低能耗状态，Victor 则会根据动态、静态来调整能耗与开销，达到节约资源、提升设备续航力的目的。

2　密钥提取

2.1　过滤

研究中使用 Savitzky－Golay 滤波器，这种滤波器为低通滤波，最大的特点就在于当滤除噪声的同时，还可以确保信号的形状、宽度不变，适用于不连续的 RSS 变化[11]。在 Alice 和 Bob 之间的共享信道指纹中，研究也能提供信道轮廓过滤的结果。过滤减少了不对称双方之间的差异（如随机噪声、端点

采样延迟等),虽然已经依靠 Victor 帮助完成密钥的不匹配问题,但是过滤的作用依然不可忽视,即能够有效减小双方 RSS 不匹配率大于 15%的可能性。

2.2 量化

量化的目的是为了将原始的 RSS 数据转化为比特串,进一步隔离 Alice 和 Bob 之间的非对称噪声,提高密钥匹配率,减少 Victor 的冗余工作。在量化方法上,研究本着经济优先的原则(尽可能地减小传输成本),将对量化方法做出相应的综合评价[11]。

最终,研究选择等级交叉量化,Alice 和 Bob 互发探测数据包时,如果数据包的发送是连续的,数据包会组成一组时间序列作为 RSS 序列,然后,将插入多个节点量化时间序列以生成密钥比特序列。综上量化过程的设计展示参见图 3。

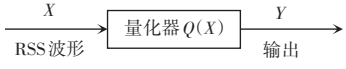

图 3 量化过程

Fig. 3 Quantification process

以图 3 为基础,可将这一量化过程解析为如下数学公式:

$$y = Q(x) = Q\{x_k < x \leqslant x_k + 1\} = y_k(1)$$
$$k = 1,2,\cdots,L. \qquad (1)$$

研究中,可以在 Victor 中计算出量化的阈值,下限和上限之间的值被删除,大于上限的阈值被编码为 1,小于下限阈值编码为 0。

Victor 保持对密钥位进行校验和修正,当达到了 128 位长度时,便可以向 Alice 和 Bob 分发密钥,而在 Alice 和 Bob 获取可用的密钥后,就可以进行加密和解密,即可以开始通信了。本文的实验结果表明,在动态的条件下,这个方案每小时可以产生 2 ~ 4 个可用密钥。

现有的研究工作中,Alice 和 Bob 的密钥信息,都是在开放的环境中产生的,但是采样量化后的数据不受保护,这里即有针对性地引入 AES 算法中的 ShiftRows 和 ColumnMix 算法来有效调整此时得到的密钥信息,为了便于工程实现,则利用矩形帧结构来表示量化后的数据,使得 ShiftRows 和 ColumnMix 运算过程对设计人员将更加直观。

到目前为止,密钥信息仍然可能被隐藏在 Alice 和 Bob 之间的 Eve 获取,如果 Alice 或 Bob 有意接受 Eve 的存在,密钥信息也依旧无法保证数据的安全。因此,本文就给 Alice 和 Bob 定下规则,要求 Alice 和 Bob 在获得密钥后,要把密钥按照矩形帧结构的形式,排列成矩阵,对于 128 位密钥,排成 8 行 16 列的矩形帧结构,Alice 和 Bob 将依据同样的规则,对密钥运行 ShiftRows 和 ColumnMix 运算,此后即便密钥信息被监听,也不会被 Eve 窃取,从而有效阻止了中间人的有效攻击。

3 实验和评测

3.1 密钥生成

研究中使用了 3 台笔记本电脑,用 IEEE 802.11 网卡互联,在 60 m^2的住房内,无规律地走动。实验时间为 10 h。研究发现,在完全静止的状态下,无法在一个信道上产生足够的高熵比特流,为此,推出如下规定:当 Alice 和 Bob 无法从 RSS 特征中获取能够产生 128 位的密钥信息,Victor 会同时对 Alice 到 Victor、Bob 到 Victor、Bob 到 Alice 的信道进行 RSS 特征的捕捉,在完全静止的状态下,当启动如此处理后就会发现,只要对 3 个信道都进行比特流提取,每小时就可以捕捉大约 2~4 个 128 位密钥信息,基本可以满足本文的研发要求,由于 Victor 的通信成本不受体域网的限制,本文对此将不再赘述。

文中的构想设计是每小时产生一个密钥,本次实验中在 10 h 内总共获取了 9 个密钥,这 10 次中,发生一次 Bob 和 Alice 密钥不匹配度超过 15%,而在这一次即是由 Victor 下发重新生成密钥信息的指令;再次生成密钥的过程中,试图略微移动实验中的笔记本电脑,在下一小时中,密钥成功生成。所以,本文设计的实验证明,在相对稳定的电磁环境中,Alice 和 Bob 在 Victor 的校正下可以完成密钥的生成。

3.2 中间人攻击

研究假设,Eve 已经可以在 Alice 和 Bob 间的信道插入数据,但是,插入数据就会引起信道的变化,这将势必导致密钥不匹配率的提高。本文在实验运行中发现,当 Eve 冒充 Alice 给 Bob 发送数据的过程导致了 Victor 从两端所接收到的密钥不匹配率提高到了 15%以上,严重时可达 19%,导致 Victor 多次自行修正。

当出现连续的两端不匹配时,Victor 会同时监控所有的 3 条信道,当某一条信道检测出来自 2 个设备发送的数据包时,便发出告警指示,告知网络中有 Eve 入侵。在为 Victor 设定了上述功能后,研究进行了 10 次测试,让 Eve 代替 Alice 向 Bob 发送数据。而在每一次测试中,Victor 都能在 Eve 向 Bob 发送第 2 个数据包之前,即检测出 Eve 的存在。

3.3 合谋攻击

实验中,又将 3 台笔记本电脑分别设定为 Victor、Eve、Bob。在这里,也可以称为冒充攻击,因

为文中假设 Eve 不仅掌握了 hello 信息的准确值，并且掌握了发送数据包的结构且获取了 Alice 故意泄露的密钥，相当于 Eve 在 Alice 的协助下已经成功冒充了 Alice。但是因为 Victor 的存在，当 Eve 试图向 Bob 发送数据包时，Alice 到 Bob 的信道 RSS 特征便发生了变化，Victor 在检测时，很快就可以发现 Alice 到 Bob 信道两端的不匹配问题。

实验中在 1 h 内，Eve 尝试了与 Bob 发送 10 次数据包，每一次对 Alice 的数据包进行覆盖，都在 Bob 端发生明显的信号增益，Victor 始终能正确响应、发出告警。

3.4　干扰因素

在城市内的电磁环境中，无线电信号的变化波动无论是动态还是静态，基本都能满足研究时对高熵比特的需求，但是此次实验中却意外发现，在特别环境中，比如说，长时间完全静止的状态（人睡觉时）、空气中静电含量较高、湿度极大的天气等，会对本文的实验结果产生影响，这是由于空气中静电含量与信道中的噪声系数成正比。在极为干燥的环境中，过多的静电造成信号波形的变化除了影响此次的量化研究工作，也会导致设备间通信丢包率的上升，传感器和基站则会长时间满负荷工作，数据的传输终端将会增多，耗电量也会增加。根据文中给出的大量实验数据表明，建议工作在温度 17 ℃～26 ℃，湿度不足 15% 的环境中，如果装修材料没有静电吸附能力，则需要在环境中加装静电过滤器，静电的产生与湿度成反比关系，湿度越大，静电越少。由于条件有限，研究中即采取了温度和湿度的测量来间接反映出静电对数据传输的影响。通过实验测得最佳的工作环境是温度在 22 ℃～26 ℃之间，湿度为 35%RH～65%RH 之间，一旦超出这个范围，设备的传输就有可能发生丢包的情况。

4　结束语

在本文中，研究针对体域网中基于信道特征的密钥提取问题引入了 Victor 来实现对 Alice 和 Bob 的监控，有效防止了合谋攻击。通过测试，研究验证了这种方案的可行性，只有在 Eve 完全复制了 Alice 所有的功能、算法、信号发送规律且关闭 Alice 的情况下，才可能瞒过 Victor，向远端传送虚假信息。同时，也可以用 Victor 来处理 Alice 和 Bob 所产生的 RSS 的误配率的问题，减少可穿戴设备的能源消耗。另外，之前的工作中没有任何措施保证量化后的密钥安全性，本次研究则对量化后的数据进行了处理，从而达到了密钥的安全性要求。此后的实验也出色验证了本文方案的可行性。

参考文献

[1] 彭巧，田有亮. 基于多线性 Diffie-Hellman 问题的秘密共享方案[J]. 电子学报，2017，45(1)：200-205.

[2] MATHUR S，TRAPPE W，MANDAYAM N，et al. Radio-telepathy：Extracting a secret key from an unauthenticated wireless channel[C]// Proceedings of the 14th Annual International Conference on Mobile Computing and Networking，MOBICOM 2008. San Francisco，California，USA：ACM，2008：128-139.

[3] 胡爱群，李古月. 无线通信物理层安全方法综述[J]. 数据采集与处理，2014，29(3)：341-350.

[4] 高宁. 基于无线信道特征的加密和协商方案[D]. 青岛：山东科技大学，2015.

[5] LIU Hongbo，WANG Yang，YANG Jie，et al. Fast and practical secret key extraction by exploiting channel response[C]// Proceedings of IEEE INFOCOM. Turin，Italy：IEEE，2013：3048-3056.

[6] 高昂，李增智. 一种无需全局 ID 抗共谋攻击的属性加密算法及其在传感器网络中的应用[J]. 四川大学学报（工程科学版），2012，44(5)：115-120.

[7] LIBURDY R P，PENN A. Microwave bioeffects in the erythrocyte are temperature and pO2 dependent：Cation permeability and protein shedding occur at the membrane phase transition[J]. Bioelectromagnetics，1984，5(2)：283-291.

[8] 李洁，黄鹏，李兴华. 无线移动环境下密钥协商机制的设计[J]. 铁路计算机应用，2013，22(12)：47-49，58.

[9] 黄晶晶. 基于无线信道环境的密钥生成机制研究[D]. 北京：北京邮电大学，2015.

[10] SCHAFER R W. On the frequency-domain properties of Savitzky-Golay filters[C]// Digital Signal Processing Workshop and IEEE Signal Processing Education Workshop. Sedona，AZ：IEEE，2011：54-59.

[11] 田玉兰. 传感网基于接收信号强度的密钥生成匹配性的研究[D]. 西安：西安电子科技大学，2014.

（上接第 107 页）

[3] 王双成，杜瑞杰，刘颖，等. 连续属性完全贝叶斯分类器的学习与优化[J]. 计算机学报，2012，35(10)：2129-2138.

[4] 陈景年，黄厚宽，田凤占，等. 用于不完整数据的选择性贝叶斯分类器[J]. 计算机研究与发展，2007，44(8)：1324-1330.

[5] RISH I. An empirical study of the naive Bayes classifier[C]// Proceedings of IJCAI 2001 Workshop on Empirical Methods in Artificial Intelligence. Seattle，USA：Morgan Kaufmann，2001，3(22)：41-46.

[6] WANG Jiannan，KRISHNAN S，FRANKLIN M J，et al. A sample-and-clean framework for fast and accurate query processing on dirty data[C]// Proceedings of the 2014 ACM SIGMOD International Conference on Management of Data. Snowbird，Utah，USA：ACM，2014：469-480.