Journal of System Simulation

Volume 29 | Issue 4 Article 23

6-3-2020

BLE Key Agreement Scheme Based on RSSI Variation Trend

Xinghao Zhang
PLA Information Engineering University, Zhengzhou 450004, China;

Yicai Huang
PLA Information Engineering University, Zhengzhou 450004, China;

Bin Yu
PLA Information Engineering University, Zhengzhou 450004, China;

BLE Key Agreement Scheme Based on RSSI Variation Trend

Abstract

Abstract: Based on the variation trend of received signal strength index, a lightweight BLE key agreement scheme was proposed. *Using adaptive frequency hopping, the variation of channel characteristics was strengthened. According to the randomness and reciprocity of BLE channel characteristics in coherence time, the RSSI of BLE signal was measured. And the real-time key was produced by calculating the variation trend.* On the basis of experiments results, the randomness of key can be ensured, and a high key generation rate has been reached at the same time. The scheme can be applied to resource-constrained applications.

Keywords

BLE, coherence time, RSSI, frequency hopping, key agreement

第 29 卷第 4 期 系统仿真学报© Vol. 29 No. 4
2017 年 4 月 Journal of System Simulation Apr., 2017

基于 RSSI 变化趋势的 BLE 密钥协商方案

张星昊，黄一才，郁滨
（解放军信息工程大学，河南 郑州 450004）

摘要：基于接收信号强度 RSSI (Receive Signal Strength Indicator)的变化趋势，设计了一种轻量级的 BLE (Bluetooth Low Energy)密钥协商方案。*利用自适应跳频机制增强信道特征的变化趋势，依据相干时间内 BLE 信道特征的随机性和相关性，对接收信号的 RSSI 进行测量，最终通过计算其变化趋势实现实时的密钥协商。*实验结果表明，该方案在保证随机性的前提下，具有较高的密钥生成速率，适用于资源受限的应用场景。

关键词：BLE；相干时间；RSSI；跳频；密钥协商
中图分类号：TP309.1 文献标识码：A 文章编号：1004-731X (2017) 04-0873-07
DOI: 10.16182/j.issn1004731x.joss.201704023

BLE Key Agreement Scheme Based on RSSI Variation Trend

Zhang Xinghao, Huang Yicai, Yu Bin
(PLA Information Engineering University, Zhengzhou 450004, China)

Abstract: Based on the variation trend of received signal strength index, a lightweight BLE key agreement scheme was proposed. *Using adaptive frequency hopping, the variation of channel characteristics was strengthened. According to the randomness and reciprocity of BLE channel characteristics in coherence time, the RSSI of BLE signal was measured. And the real-time key was produced by calculating the variation trend.* On the basis of experiments results, the randomness of key can be ensured, and a high key generation rate has been reached at the same time. The scheme can be applied to resource-constrained applications.

Keywords: BLE; coherence time; RSSI; frequency hopping; key agreement

引言

无线体域网(WBAN)[1]是以人体为中心，多个植入体内或附着在体表的通信节点组成的移动网络，是一种特殊的传感器网络，适用于战场上的士兵身体状态监控[2]、智能医疗[3]等重要领域。

低功耗蓝牙技术(BLE)是基于经典蓝牙提出的新兴无线通信标准，以超低的功耗为主要特点，针对低数据量、突发性的通信需求[4]，是面向 WBAN 最具前景的技术之一。由于 BLE 所使用的 2.4GHz 开放无线信道面临窃听、篡改、中间人攻击等威胁，限制了其在军事、医疗等特殊领域的应用。

BLE 通过安全简单配对协议 SSP 实现设备配对和密钥协商，文献[5-6]分别对蓝牙 4.0 和 BLE 中的 SSP 协议进行了安全性分析，文章均指出由于 JW 模式下的 PIN 码被设置为零，导致密钥协商过程易遭到窃听。BLE 也提供了更安全的 PE 和 OOB 的关联模式，但这两种模式都需要在节点上添加额外的硬件设施，增加了功耗，难以适应

收稿日期：2016-05-22 修回日期：2016-08-04;
作者简介：张星昊(1992-)，男，四川广安，硕士生，研究方向为蓝牙、信息安全技术；黄一才(1985-)，男，湖北巴东，硕士，讲师，研究方向为蓝牙、信息安全技术等；郁滨(1964-)，男，河南郑州，博士，教授，博导，研究方向为信息安全、无线网络安全技术、视觉密码等。

WBAN 等资源受限的应用场景。因此，如何提高资源受限环境下密钥协商过程的安全性，对 BLE 技术的应用推广具有重要的意义。

最常见的解决方案是基于 Diffie-Hellman 的公钥密码体制[7]。徐等[8]利用计算复杂度较低的 LUC 公钥算法改进了蓝牙密钥协商过程，防止配对过程受到窃听和中间人攻击的威胁，但使用公钥密码体制必然会提高计算和存储资源的消耗。Heiner Perrey 等[9]利用 Merkle 谜题代替原有的 PIN 码，设计了一种轻量级的 BLE 密钥协商方案，适用于诸如体域网等资源受限的应用场景。相对于 ECDH 公钥体制，该方案对每个传感器节点来说计算量较小，并且能使多个设备同时进行密钥协商。但方案消耗的时间较长，产生和分发 MP 谜题的中心设备负担较重。

在如 WBAN 等计算和存储资源有限的应用场景下，常规的基于密码学加密算法的安全方案在资源调度时显得捉襟见肘。基于无线信道特征的安全方案利用无线信道特征的随机性、快速空变性、短时互易性[10-11]等特点，无需添加额外硬件，计算和存储开销较小，具有很高的利用价值。将无线信道特征用于密钥协商和认证等安全方案的思想最早由 Maurer 和 Hershey 的理论[12-13]提出。Mathur[14]在 2008 年初步实现了基于共同无线信道特征的密钥共享。文献[15-16]分别利用无线信号的 RSSI 值和相位进行密钥协商，这些方案均是针对 WIFI 等 802.11 标准的无线技术。Sriram N. Premnath[17]利用蓝牙信道完成密钥协商，解决了利用 WIFI 信道进行密钥提取时易受信道阻塞影响的问题，方案依据 RSSI 测量值的均值和标准差设置上下限，对测量值进行量化，将处于上下限之间的测量值均舍去，这样的做法在一定程度上造成了测量值的浪费，降低了密钥的生成速率。

本文利用 BLE 通信过程中接收信号的 RSSI 值变化趋势，设计密钥协商方案，保证了协商过程的安全性，具有较高的密钥生成速率和随机性，适用于资源受限的应用场景。

1 系统模型

在无线环境中，每一条信道对某一频段上的无线信号产生的衰落是独一无二的。这一特点决定了处于空间中不同位置的节点所接收到具有唯一性的无线信号是攻击者无法伪造的。信道衰落的随机性使得通信双方可以通过信道特征协商共享密钥。为方便描述，方案所用的符号及其含义如表 1 所示。

表 1 符号定义
Tab. 1 Symbol definition

符号	含义	符号	含义
h	随机信道增益	t_c	信道相干时间
r(t)	接收信号	v	主从设备相对移动速度
s(t)	发送信号	T	信道采样周期
H_M	主设备测得的信号强度值序列	hop	跳频步长
H_S	从设备测得的信号强度值序列	n	密钥长度

1.1 模型建立

基于经典的移动通信系统模型，本文建立了一个存在窃听者的 BLE 无线通信系统模型，如图 1 所示。其中，Master 是合法主设备，Slave 是合法从设备，Eve 是窃听者。Eve 可对 BLE 信道中所有的数据包进行窃听。

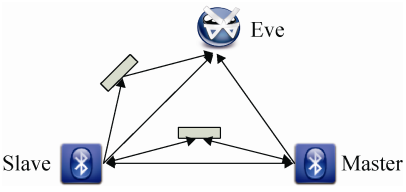

图 1 BLE 无线通信系统模型
Fig. 1 BLE wireless communication system model

在无线环境中，接收信号可用下面的公式表示：

$$r(t) = s(t) \times h + n(t) \quad (1)$$

式中：$r(t)$ 表示接收信号；$s(t)$ 表示发送信号；h 表示信道增益；$n(t)$ 表示信道中的随机噪声。

在静止的环境下，信道增益 h 可视为不变，其值可看作一个常数。

移动环境下的信道是一个时变系统，信道增益 h 可以看作一个随机的时变函数 $h(t)$。因此，可将通信模型中的 Master、Slave 和 Eve 的接收信号用

下面的公式表示：

$$r_{ms}(t) = s_s(t) \times h_{sm}(t) + n_{sm}(t) \quad (2)$$

$$r_{sm}(t) = s_m(t) \times h_{ms}(t) + n_{ms}(t) \quad (3)$$

$$r_{em}(t) = s_m(t) \times h_{me}(t) + n_{me}(t) \quad (4)$$

$$r_{es}(t) = s_s(t) \times h_{se}(t) + n_{se}(t) \quad (5)$$

在上述模型中：$s_s(t)$ 表示 Slave 发送的信号；$r_{ms}(t)$ 表示 Master 接收到 Slave 发送的信号；$h_{sm}(t)$ 表示从 Master 到 Slave 的信道增益；$n_{sm}(t)$ 表示 Master 接收到 Slave 发送的信号中携带的随机噪声。由于发送信号仅由发送端决定，将模型中所有的发送信号设置为相同，即 $s_m(t) = s_s(t)$。随机噪声强度很小，不考虑 $n(t)$ 的影响。此时，接收信号 $r(t)$ 仅受信道增益 $h(t)$ 影响。

1.2 理论依据及设计思想

密钥随机性、一致性、生成速率及协商过程安全性，是衡量密钥协商方案的主要标准。本节从理论上推导方案的安全性和可行性。

1、理论依据

相干时间指信道保持恒定的最大时间间隔。根据信道的短时互易性可知，在相干时间内，$h_{ms}(t)$ 与 $h_{sm}(t)$ 高度相似，一般假设二者相同。因此，主从设备的接收信号 $r_{ms}(t)$ 和 $r_{sm}(t)$ 可视为相同的时变函数。

根据信道的快速空变性可知，相距无线信号半波长距离的两设备所接收到的无线信号特征不相关。当窃听者 Eve 与主从设备的距离超过了半波长(2.4 GHz 下为 6.25 cm)时，$h_{me}(t)$、$h_{se}(t)$ 与 $h_{ms}(t)$ 属于不同的信道，导致其接收信号的特征与主从设备的特征有较大差异，窃听者无法由 $r_{em}(t)$ 和 $r_{es}(t)$ 推测 $r_{ms}(t)$ 和 $r_{sm}(t)$。

根据信道特征的随机性可知，由于信道增益 $h(t)$ 具有随机性，导致接收信号相对于发送信号会产生随机性的变化。因此，可以利用接收信号 $r_{ms}(t)$ 和 $r_{sm}(t)$ 的功率、相位、幅度等特征参数作为主从设备间共享的秘密信息生成密钥。由于生成的密钥与传输的数据内容没有任何关系，所以窃听者无法通过窃听探测报文获得密钥信息。

2、设计思想

BLE 采用半双工的传输方式，主从设备对信道的探测无法在同一时刻进行，因此得不到完全相同的信道特征。在相干时间 t_c 内，$h_{ms}(t_0)$ 与 $h_{sm}(t_0 + \Delta t)$ 相同 $(\Delta t < t_c)$，由此可见，$r_s(t_0)$ 与 $r_m(t_0 + \Delta t)$ 也是相同的。所以，Master 与 Slave 对信道相邻的两次探测必须在相干时间内完成。

受多径效应影响，同一信道对不同频率信号的衰减作用具有一定差异，这种信道称为频率选择性衰落信道。利用 BLE 的自适应跳频机制，可以通过改变载波频率改变信道增益。此时信道增益可用时变频变函数 $h(t, f)$ 表示，接收信号可用公式(6)表示：

$$r(t) = s(t) \times h(t, f) + n(t) \quad (6)$$

若在相干时间内对信道进行多次采样，测得的信道特征具有较高的相关性，不适于生成随机密钥。通过引入跳频机制，不仅能避免信道拥塞造成的探测报文丢失，而且在保证信道特征随机性的基础上，降低了对信道探测次数的限制。

利用接收信号强度指示 RSSI 生成密钥是常用的密钥协商方案之一。RSSI 是一种易测的无线信号特征，其与信号功率 P 的换算公式为 $RSSI(\text{dBm}) = 10\log P(\text{mW})$，接收信号功率的变化反应了信道增益的变化。RSSI 值的测量易受信号发送设备的发射功率、接收天线灵敏度等条件影响，引起测量误差，而信道变化趋势只与信道本身特性有关，受设备自身条件影响较小，利用 RSSI 变化趋势生成的密钥在一致性方面具有较大的优势。

由于主从设备的 RSSI 测量值存在误差，若某一节点在某一时刻的 RSSI 变化趋势不变，另一节点在相同时刻的 RSSI 变化趋势可能为上升或下降。因此，本方案将 RSSI 变化趋势不变的位置视为无效位，通过协商将无效位上对应的参数去掉，最终得到一致的密钥。

2 密钥协商

密钥协商首先通过信道探测得到 RSSI 测量值，再利用不同时刻测量值的变化趋势计算密钥。信号处理流程如图 2 所示。

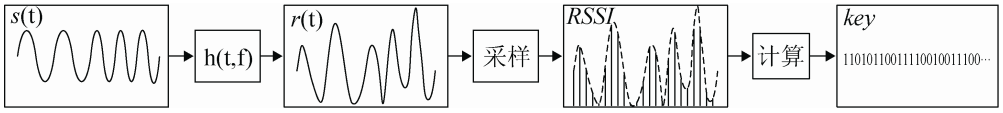

图 2 信号处理流程图

Fig. 2 Signal processing flow chart

BLE 采用 GFSK 调制方式，发送信号 $s(t)$ 由不同频率的正弦波组成。受随机信道增益 $h(t, f)$ 影响，接收信号会产生不规则的幅度、相位、强度变化。通过对接收信号的采样获得不同时刻的信号强度 RSSI 值。最终利用不同时刻的信号强度变化趋势计算出密钥。

2.1 信道探测

信道探测是决定密钥随机性和一致性的关键步骤，其主要的影响因素包括相干时间 t_c、信道采样周期 T 和跳频步长 hop。

相干时间与信道最大多普勒频移 f_d 成反比例关系。其计算公式通常近似为

$$t_c = 0.423 / f_d = 0.423\lambda / v = 0.423c / (vf) \quad (7)$$

式中：v 为通信节点间的相对移动速率；λ为无线信号的波长；f 为无线信号的频率；c 为无线信号的传播速度。

为确保生成密钥的一致性，t_c，T 和 hop 应满足以下两个条件：

(1) $T < t_c$。通信双方相继的两次探测必须在相干时间内进行，才能获得相似的测量值。探测周期 T 受限于硬件条件，需根据 BLE 设备的传输能力进行设置。

(2) 在相干时间内，$h(t, f)$ 可以视为一个频变函数 $h(f)$，跳频步长越长，信道增益变化越大，增强了信道的多变性，降低了同一设备相邻两次探测信道特征的相关性。BLE 共有 37 条数据报文跳频信道，在相干时间内应尽量增大相邻两次探测的载波频率差异。因此，设计跳频步长 hop 的计算如公式(8)所示。

$$hop = \left\lfloor \frac{37}{\lfloor t_c / T \rfloor} \right\rfloor \quad (8)$$

跳频算法如公式(9)所示。

$$f_{i+1} = (f_i + hop) \bmod 37 \quad (9)$$

将 RSSI 值作为接收信号特征，在信道探测阶段，Master 和 Slave 互发探测报文，并以周期 T 对 $r(t)$ 进行采样，分别获得 n 个 RSSI 测量值。即：

$$\hat{H}_M = \{RSSI_{ms}(t_0), RSSI_{ms}(t_0 + T), ..., RSSI_{ms}(t_0 + (n-1)T)\}$$

$$\hat{H}_S = \{RSSI_{sm}(t_0 + T/2), RSSI_{sm}(t_0 + 3T/2), ..., RSSI_{sm}(t_0 + (n-1/2)T)\}$$

2.2 密钥生成

利用测量值的变化趋势计算密钥是将 $\Delta RSSI(t_i) = RSSI(t_i) - RSSI(t_i + T)$ 的值映射到{0,1}集合的过程。映射过程用公式(10)表示：

$$key(t_i) = \begin{cases} 0, & \Delta RSSI(t_i) < 0 \\ 1, & \Delta RSSI(t_i) > 0 \\ invalid, & \Delta RSSI(t_i) = 0 \end{cases} \quad (10)$$

$key(t_i)$ 表示在 t_i 时刻获得的密钥，每一位密钥需要两个测量值，若两测量值之间呈上升趋势，则 $key(t_i) = 1$；若呈下降趋势，则 $key(t_i) = 0$；若呈不变趋势，则该时刻的变化趋势无效。具体密钥生成过程分为以下几步：

(1) Master 和 Slave 利用公式(10)对每一个时刻的测量值变化趋势进行计算，分别得到一组{0,1}比特串 $\hat{K}_M$ 和 $\hat{K}_S$。

(2) Master 将 $\hat{K}_M$ 中无效位对应的位置序号组成序列 seq_iv_m，并发送至 Slave。

(3) Slave 接收消息后将 $\hat{K}_S$ 中无效位对应的位置序号组成序列 seq_iv_s，并发送回 Master。

(4) Master 和 Slave 依据 seq_iv_m 和 seq_iv_s 生成完整的无效位序列，并将对应位置上的比特舍弃，双方获得一致的密钥 key。

3 实验及结果分析

为了对方案性能进行测试，选用 TI 公司生产的 CC2541 低功耗蓝牙开发板作为主从设备，使用 IAR 编写开发板通信固件。实验环境选用普通的办公室，$v=0.5$ m/s，$t_c\approx102.4$ ms。在信道探测阶段，将 BLE 连接间隔设置为 10 ms，采样周期 $T=10$ ms，跳频步长 $g=3$。

3.1 实验测试

依据 WBAN 的自身特点，将 BLE 主、从设备间的距离分别设置为 0.5 m、1 m 和 2 m，对信道进行多次探测，取前 1 000 次测量值进行分析，测试方案的密钥生成速率，探测报文利用率和不一致比特率。测试结果如图 3 所示。

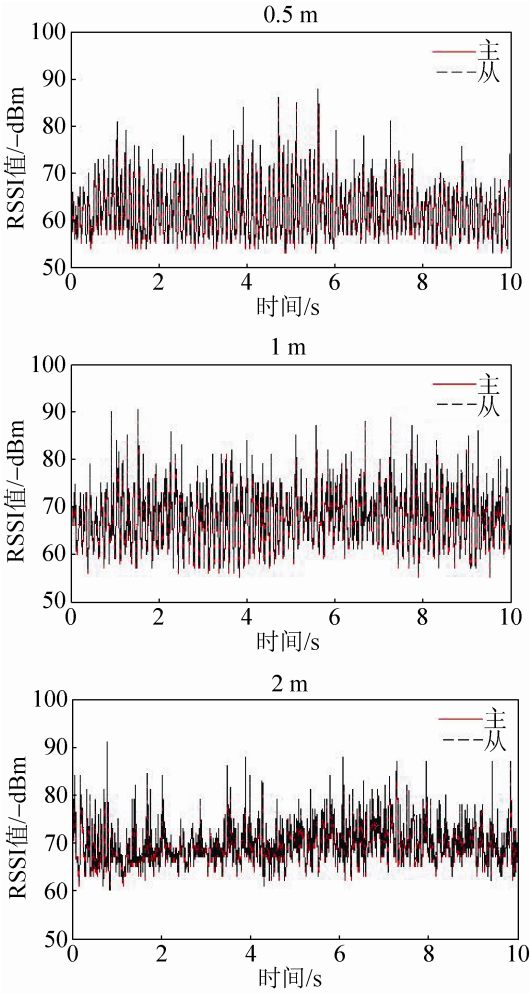

图 3 方案测试
Fig. 3 Scheme test

三组实验 RSSI 测量值的特征如表 2 所示。

表 2 RSSI 测量值特征
Tab. 2 Measured value characteristics of RSSI

实验距离/m	不一致率	相关系数	无变化趋势位置比例	
			主设备	从设备
0.5	0.432	0.996 2	0.076	0.084
1	0.430	0.996 7	0.105	0.117
2	0.422	0.994 3	0.083	0.078

由表 2 可看出，主从设备测量值序列中无变化趋势的位置比例约占 1/10，可以推测出密钥的无效位约占总数的 1/5，但仍可以达到接近 0.8 的生成效率，这比以往的方案有较大的提高。

三组实验协商出的密钥特征如表 3 所示。

表 3 密钥特征
Tab. 3 Characteristics of key

实验距离/m	密钥总数/个	不一致率	生成速率/bps	探测报文利用率/%
0.5	841	0	84.1	0.841
1	856	0	85.6	0.856
2	872	0	87.2	0.872

结合表 2 和表 3，从测量值的高不一致率及密钥的一致性可以看出方案设置无效位的合理性。方案在保证密钥高度一致的同时，具有较高的密钥生成速率和报文利用率。

根据 NIST 随机数测试标准，对方案生成的密钥进行随机性测试。NIST 一共规定了 16 项测试，由于密钥长度限制，部分测试无法进行，每项测试的 p_value 结果如表 4 所示。

表 4 密钥随机性测试
Tab. 4 Key's randomness test

测试项目	测试距离		
	0.5 m	1 m	2 m
频数检验	0.863	0.259	0.919
块内频数检验	0.999	0.998	0.999
游程检验	0.011	0.010	0.016
块内最长游程检验	0.013	0.050	0.018
离散傅立叶变换检验	0.576	0.014	0.526
非重叠模块匹配检验	0.180	0.060	0.059
线性复杂度检验	0.011	0.018	0.015
近似熵检验	0.012	0.015	0.011
累加和检验	0.882	0.365	0.480

若 p_value 的值>0.01，则表示通过该项测试，密钥可视为具有随机性。由表 4 可知，生成的密钥通过了所有的随机性测试。

3.2 性能分析

表 5 是方案与文献[8-9]在存储、计算和通信开销三方面的比较。存储开销为方案需要预先存储的数据大小。计算开销用各种运算的次数和运算所消耗时间的乘积表示，主要包括公钥加解密算法 T_{ASYM}，生成和求解 MPT_{MP} 和整数减法运算 T_d。通信开销用通信轮数表示。其中，r 为文献[8]方案选取的大素数的长度，m 为文献[9]方案中需要的 MP 的数量，n 为本方案中密钥长度。

表 5 方案开销对比
Tab. 5 Schemes' comsumption comparison

方案	存储开销		计算开销		通信开销	
	主设备	从设备	主设备	从设备	主设备	从设备
文献[8]	4r	4r	8T_{ASYM}	10T_{ASYM}	3	2
文献[9]	40 m Byte	—	mT_{MP}	T_{MP}	M	1
本文	—	—	nT_d	nT_d	n+1	n+1

注：— 不需要预先存储数据

本方案基于无线信道的实时通信特征，不需要提前存储任何信息，在存储开销方面明显优于文献[8-9]的方案。

在计算开销方面，假设芯片完成一次异或运算的时间为 T_u，由于 $T_d \approx 2T_u$、$T_{MP} \approx 10^3 T_u$，公钥加解密算法耗时 T_{ASYM} 与具体算法实现程序相关，但一般而言 $T_{ASYM} > 10^2 T_u$。因此，本方案的计算开销明显低于前两个方案。

本方案的通信开销由密钥长度决定，通信轮数高于前两个方案，但每次通信数据量很小，通信速度较快，最快可以在 1 s 内协商出 100 bit 密钥，不会影响用户体验。

4 结论

本文在深入研究无线信道特征和 BLE 技术的基础上，利用 BLE 自适应跳频机制，增强了信道增益的变化特性，结合相干时间、采样周期等参数计算跳频步长。依据相干时间内信道增益的相关性，利用 RSSI 变化趋势协商出共享密钥。最后通过大量实验对方案的性能进行验证，结果表明，本文方案无需添加额外硬件或预存储信息，实现代价小，能实时生成任意长度的密钥，并较好地平衡了密钥的随机性和生成速率，提高了资源受限环境下 BLE 设备的安全性。

参考文献：

[1] 宫继兵, 王睿, 崔莉, 等. 体域网BSN的研究进展及面临的挑战 [J]. 计算机研究与发展, 2010, 47(5): 737-753. (Gong Jibin, Wang Rui, Cui Li, et al. Reasearch advances and challenges of body sensor network [J]. Journal of Computer Research and Development, 2010, 47(5): 737-753.)

[2] Venkatasubramanian K K, Banerjee A, Gupta S K S. Plethysmogram-based secure inter-sensor communication in Body Area Networks [C]// Military Communications Conference. California, USA: IEEE Milcom, 2008: 1-7.

[3] Rong C, Cheng H. Authenticated health monitoring scheme for wireless body sensor networks [C]// International Conference on Body Area Networks. Oslo, Norway: EAI, 2012: 31-35.

[4] 陈灿峰. 低功耗蓝牙技术原理与应用 [M]. 北京: 北京航空航天大学出版社, 2013. (Chen Canfeng. BLE technology theory and application [M]. Beijing, China: Beijing University of Aeronautics and Astronautics Press, 2013.)

[5] Xu J, Zhang T, Lin D, et al. Pairing and Authentication Security Technologies in Low-Power Bluetooth [C]// Green Computing and Communications, Beijing, China. USA: IEEE, 2013:1081-1085.

[6] Sandhya S, Sumithra Devi K A. Analysis of Bluetooth threats and v4.0 security features [C]// International Conference on Computing, Communication and Applications (ICCCA), Tamilnadu, India. USA: IEEE, 2012: 1-4.

[7] Rahman S, He Y, Wu H. Public-Key Based Efficient Key Distribution in Bluetooth [C]// 10th International Conference on Information Technology: New Generations. Las Vegas, USA: IEEE, 2013: 727-728.

[8] Xu Guangliang, B Yu. Security enhanced design of the Bluetooth simple pairing protocol [C]// Computer Science and Network Technology (ICCSNT), China.

USA: IEEE, 2011: 292-296.

[9] Perrey H, Ugus O, Westhoff D. WiSec' 2011 poster: security enhancement for bluetooth low energy with Merkle's puzzle [J]. Acm Sigmobile Mobile Computing & Communications Review (S1559-1662), 2011, 15(3): 45-46.

[10] Mathur S. Building information-theoretic confidentiality and traffic privacy into wireless networks [D]. New Brunswick, USA: Graduate School, Rutgers University, 2010.

[11] 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. USA: ACM, 2009: 321-332.

[12] Maurer U M. Secret key agreement by public discussion from common information [J]. IEEE Transactions on Information Theory (S0018-9448), 1993, 39(3): 733-742.

[13] Hershey J E, Hassan A A, Yarlagadda R. Unconventional cryptographic keying variable management [J]. IEEE Transactions on Communications (S0090-6778), 1995, 43(1): 3-6.

[14] 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. USA: ACM, 2008: 128-139.

[15] Neal Patwari, Jessica Croft, Suman Jana. High Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements [J]. IEEE Transactions on Mobile Computing (S1536-1233), 2010, 9(3): 17-30.

[16] Qian Wang, Kaihe Xu, Kui Ren. Cooperative Secret Key Generation from Phase Estimation in Narrowband Fading Channels [J]. IEEE Journal on selected areas in communication (S0733-8716), 2012, 30(9): 1666-1674.

[17] Premnath S N, Gowda P L, Kasera S K, et al. Secret key extraction using Bluetooth wireless signal strength measurements [C]// Sensing, Communication, and Networking (SECON), 2014 Eleventh Annual IEEE International Conference on. USA: IEEE, 2014: 293-301.

(上接第 872 页)

[5] Zimmerman C, Dukeman G A, Hanson J M. An Automated Method to Compute Orbital Reentry Trajectories with Heating Constraints [J]. Journal of Guidance, Control, and Dynamics (S0731-5090), 2003, 26(4): 523-529.

[6] 方洋旺, 柴栋, 毛东辉, 等. 吸气式高超声速飞行器制导与控制研究现状及发展趋势 [J]. 航空学报, 2014, 35(7): 1776-1786.(Fang Y W, Chai D, Mao D H, et al. Status and development trend of the guidance and control for air-breathing hypersonic vehicle [J]. Acta Aeronautica et Astronaurica Sinica, 2014, 35(7): 1776-1786.)

[7] Hussein Y, Rajiv S C, Howard L, et al. Predictor-corrector Entry Guidance for Reusable Launch Vehicles [C]// AIAA Guidance, Navigation, and Control Conference. Chicago, Illinois, USA: AIAA, 2001.

[8] Xue S, Lu P. Constrained Predictor-Corrector Entry Guidance [J]. Journal of Guidance, Control, and Dynamics (S0731-5090), 2010, 33(4): 1273-1281.

[9] 李慧峰, 谢陵. 基于预测校正方法的 RLV 再入制导律设计 [J]. 北京航空航天大学学报, 2009, 35(11): 1344-1348. (Li H F, Xie L. Reentry guidance law design for RLV based on predictor corrector method [J]. Journal of Beijing University of Aeronautics and Astronautics, 2009, 35(11): 1344-1348.)

[10] 水尊师, 周军, 葛志磊. 基于高斯伪谱法方法的再入飞行器预测校正制导方法研究 [J]. 宇航学报, 2011, 32(6): 1249-1255. (Shui Z S, Zhou J, Ge Z L. On-line predictor-corrector reentry guidance law based on Gauss pseudospectral method [J]. Journal of Astronautics, 2011, 32(6): 1249-1255.)

[11] Zhu G D, Shen Z J. Three Dimensional Trajectory Linearization Control for Flight of Air-birthing Hypersonic Vehicle [J]. Procedia Engineering (S1877-7058), 2015, 99: 1108-1119.