文章编号：1005-8451（2013）12-0047-04

无线移动环境下密钥协商机制的设计

李　洁，黄　鹏，李兴华
（北京交通大学　电子信息工程学院，北京　100044）

摘　要：在动态无线信道中，通信双方测得的接收信号强度（RSS）的变化特性具有较高相似性，而处于距通信双方一个载波波长范围外的攻击者则不能测得与通信双方相似的RSS变化特性。基于无线信道这一特性，本文提出了在动态无线信道中提取特征信息的方法，并结合Fuzzy Vault 算法提出在移动环境下有效的无线终端密钥安全协商机制，从而保证信息的安全传输。

关键词：移动无线网络；接收信号强度；无线终端通信；密钥协商；模糊金库算法
中图分类号：U285：TP39　**文献标识码：**A

Design of key agreement mechanism in mobile wireless networks

LI Jie, HUANG Peng, LI Xinghua
(School of Electronic and Information Engineering, Beijing Jiaotong University,
Beijing　100044, China)

Abstract: The characteristics of RSS were similar between two communication wireless devices on the dynamic wireless channel, whereas the characteristics of RSS varied from the former devices to an eavesdropper that located outside a distance greater than about one radio wavelength. Based on the properties, the method of feature extraction on the dynamic wireless channel was presented in the paper, and a reliable key agreement mechanism with Fuzzy Vault Algorithm was proposed to ensure the security of information transmission.

Key words: mobile wireless networks; received signal strength(RSS); wireless devices communication; key agreement; fuzzy vault mechanism

铁路无线通信中一般采用对称加密算法来保证信息的安全传输，而在对称密钥加密过程中，如何保证密钥的安全分配对于加密过程至关重要。

传统的密钥分配机制一般是将密钥提前分配给固定有读取权限的用户，而在某些特殊的环境下，这种密钥分配机制并不合理。例如，当密钥被遗忘、丢失或窃取时，加密算法没有任何意义。当密钥过于简单或具有较强特征性时，很可能受到蛮力攻击。另外，当通信终端临时发生改变时，算法很难在短时间内做出调整。因此，有必要设计一套有效的动态密钥分配机制以保证在铁路通信系统中无线终端安全通信。

1　系统模型

该密钥分配方案主要应用于无线终端间动态分配密钥的情况。本文主要考虑了一个简单的通信模型，如图 1 所示。该系统包括发送方 Alice 和接收方 Bob，以及多个攻击者 Eve。区域 A 表示距离 Alice 小于或等于一个波长的区域，区域 B 表示距离 Bob 小于或等于一个波长区域，区域 E 表示 Eve1、Eve2 所处的区域（距离通信双方一个波长范围外），即 $E \notin (A \cup B)$。假设在给定的系统模型下通信双方都是诚信的，并且攻击者处于距通信双方一个波长（2.4 GHz 条件下一个波长约为 12.5 cm）的范围外[1~2]。同时，还假设通信双方或其中一方通信过程是移动的。由于攻击者可以窃听通信内容或利用自身采集的接收信号强度（RSS）信息扰乱通信，因此是无线终端密钥分配过程中所面临的主要威胁。此外，本文没有考虑拒绝服务攻击的情况。

收稿日期：2013-06-28
作者简介：李　洁，在读硕士研究生；黄　鹏，在读硕士研究生。

2　基于Fuzzy Vault算法的密钥分配机制设计

2.1　Fuzzy Vault 算法

Fuzzy Vault 算法是一种有效保护传输信息安全、真实与完整的特殊密钥算法[3]。要成功在通信双方间分配密钥，首先由通信的一方将要传输的

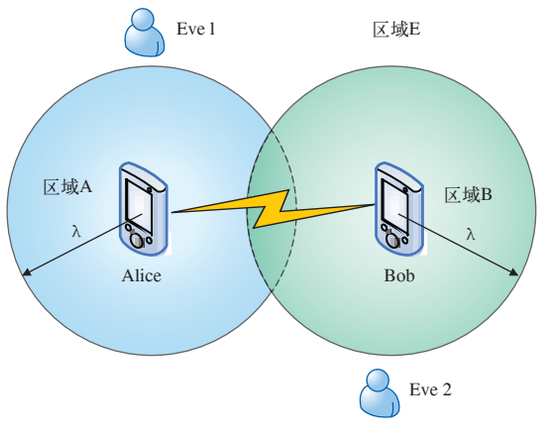

图1　系统模型

密钥信息隐藏在多项式的系数中，当接收方拥有与发送方相似的信息特征时才能成功获取密钥[4]。下面通过举例的方式来介绍 Fuzzy Vault 算法。假设 Alice、Bob 为通信的双方，Eve 为攻击者。若多项式为 $p(x)=x+1$，Alice 与 Bob 具有的特征信息分别为 $A=\{1, 2, 3, 4\}$ 和 $B=\{1, 3, 4, 5\}$。首先 Alice 根据 A 中的信息计算得到集合 $A'=\{(1, 2), (2, 3), (3, 4), (4, 5)\}$，为了保证 A' 中点的安全性，随机加入冗余点后生成集合 $Q=\{(1, 2), (2, 3), (3, 4), (4, 5), (0, 2), (7, 4), (9, 6)\}$。Bob 结合 R 中的信息以及自身采集的特征信息 B 寻找匹配点，得到点集 $Q=\{(1, 2), (3, 4), (4, 5)\}$。最后，Bob 利用集合 Q 中的点重建多项式，根据多项式的系数即可获得所需的密钥信息。

2.2　问题构建

在动态无线信道中，当通信双方对信道测量的时间差小于信道变化的速率时，通信双方测得的接收信号强度（RSS）的变化特性具有高度的相似性。处于距通信双方一个波长范围外的攻击者则不能测得与通信双方相似的 RSS 变化特性。基于无线信道的这一特性，通信双方可以获取大量相同的特征信息，若将这些特征信息作为 fuzzy vault 算法的输入，即可保证无线设备在移动环境下安全分配密钥。

2.3　基于Fuzzy Vault算法的密钥分配机制

无线终端在移动环境下的密钥分配过程如图 2 所示，其中包括初始化模块、密钥特征获取模块、生成多项式模块、生成金库模块、交换金库模块和多项式重建模块等。

密钥分配机制过程中各部分模块的功能与算法设计为：

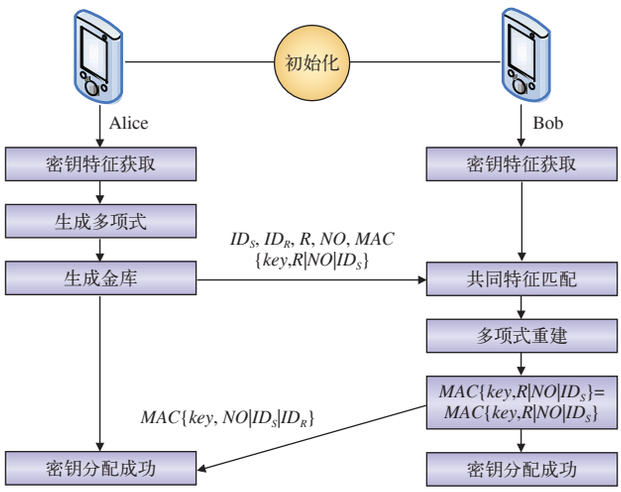

图2　无线终端密钥分配机制

（1）初始化：为了保证通信双方同步采集 RSS 信息，发送方 Alice 首先发送给接受方 Bob 一条会话信息，通知 Bob 开始采集 RSS 信息。Bob 收到该信息后发送 ACK 信息作为回复告知 Alice 可以进入密钥分配阶段。

（2）密钥特征获取：保证通信双方获取具有高度相似性的特征信息，主要包括 4 步，如图 3 所示。

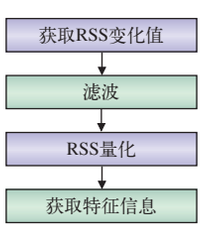

图3　密钥特征获取

a. 通信双方首先利用复杂度较低的滤波器过滤要接收的信号，以降低接收信号的差异。

b. 通过 RSS 量化器将测得的 RSS 变化特性进行量化。该量化过程是基于指定的 RSS 量化门限进行的，不同的量化门限值及量化门限个数都将会导致量化过程的差异。在指定的 2 个 RSS 量化门限下的量化过程如图 4 所示：大于上门限的采样点被量化为 1，小于下门限的采样点被量化为 0，处于上门限与下门限之间的采样点则被丢弃，那么图 4 中量化输出结果为 1 010 111。

c. 将量化值每 4 bit 进行编码并形成一个 q 码，3 个连续的 q 码相连即可生成一个 12 bit 的密钥特征。根据文献 [2] 中的研究，通信双方 q 码的匹配度为 80 %，即通信双方密钥匹配度可达到 51 %。而攻击者获得的密钥特征较发送方而言匹配度仅为 0.19 %。

d.Alice 和 Bob 分别获得特征向量 $F_S=\{f_S^1, f_S^2, \cdots f_S^N\}$ 和 $F_R=\{f_R^1, f_R^2, \cdots, f_R^N\}$，N 表示特征向量的

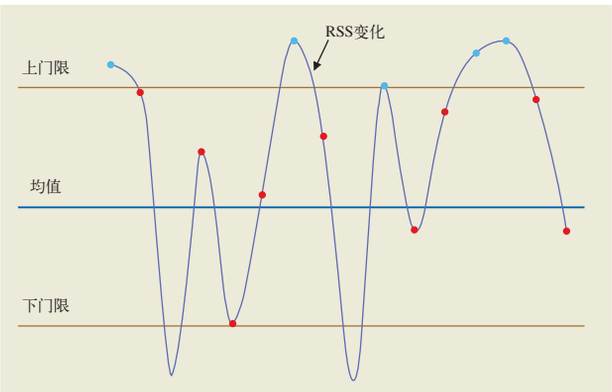

图4　RSS量化过程

大小。

（3）生成多项式：随机生成一个 v 阶的多项式，即：

$$p(x)=c_v x^v+c_{v-1}x^{v-1}+\cdots+c_1 x+c_0 \quad (1)$$

其中 v 是公开的，将多项式的系数 c_v, c_{v-1}, …, c_0 相连得到要分配的密钥 key=$c_v|c_{v-1}|\cdots|c_0$（要求密钥长度≥ 128 bit）[5]。

（4）生成金库：生成一个包含合法点与冗余点的混合点集，以便将合法点安全传送给接收方。在这一步中，根据生成的多项式（1），计算得到合法点集合 $P=(f_S^i, p(f_S^i))$，其中 f_S^i 表示特征向量 F_S 中的特征值，即 $f_S^i \in F_S$，$1 \leqslant i \leqslant N$，$p(f_S^i)$ 为将 f_S^i 作为 x 带入公式（1）得到的 $p(x)$ 值。为了保证集合 P 中点的安全，构造冗余点集合 $C=\{C_j, 1 \leqslant j \leqslant M\}$，其中 C_j 表示任一冗余点，其构成与集合 P 中的合法点一致，即 $C_j=\{cf_j, d_j\}$，同时要求冗余点 C_j 的结构参数 $cf_j \notin F_S$，$d_j \neq p(cf_j)$。此方案保证任一个冗余点 cf_j 与密钥特征均在相同的范围（0 ~ 2^{14}）内可以避免攻击者正确区分出合法点与冗余点。

为了进一步提高合法点集合 P 与冗余点集合 C 中元素的安全性，接收方 Alice 对集合 P 以及 C 中的元素进行混排，得到金库 R，即 $R=RandPermute(P \cup C)$，其中 $|R|=|N|+|M|$。

（5）交换金库：发送方 Alice 将信息 ID_S, ID_R, R, No, $MAC\{key, R|NO|ID_S\}$ 传送给接受方 Bob。其中 ID_S 和 ID_R 分别表示发送方 Alice 和接收方 Bob 的身份标识，No 为一个随机数用来保证信息的时效性，MAC 函数表示信息认证码，key 为发送方 Alice 要分配的密钥。

（6）重建多项式：接收方 Bob 根据重建的多项式获取密钥。在收到金库 R 之后，Bob 首先寻找金库 R 与集合 F_R 中匹配的部分，计算得到集合 $Q=\{(b,c)|\ (b,c) \in R, b \in F_R\}$。根据建立 v 阶多项式至少需要 v+1 个点这一原理，从 Q 中任选 v+1 个点 $\{(x_0, y_0), (x_1, y_1), \cdots, (x_v, y_v)\}$ 重建多项式 $p'(x)$，将 $p'(x)$ 的系数相连即可得到新建密钥 key'。因此要成功重建多项式 Q 需要满足 $|Q| \geqslant v+1$。接收方 Bob 进一步验证 key' 的正确性，若 $MAC\{key', R|NO|ID_S\}=MAC\{key, R|NO|ID_S\}$，则表明 $key'=key$，即密钥分配成功。

（7）重建多项式：接收方 Bob 将信息 $MAC\{key, NO|ID_S|ID_R\}$ 传送给发送方 Alice，即通知发送方 Alice 密钥分配成功，可以开始进行加密通信。

3　密钥分配机制安全性分析

通信双方密钥匹配度可达 51 %，高出攻击者获得的密钥匹配度 0.19 %，即攻击者不能通过采集信道的 RSS 变化特性获得正确的密钥，同时 RSS 变化特性具有随机性，因此将 RSS 变化特性作为特征信息满足 Fuzzy Vault 算法提取的基本要求。

对于 Fuzzy Vault 算法，当通信双方拥有较为相似的密钥特征时即可保证成功分配密钥。本文给出的方案中密钥的安全性在很大程度上取决于重建密钥的复杂度。同时，冗余点与合法点在相同的范围内，极大地增加了攻击者查找合法点的难度。对于一个不知道任何特征信息的攻击者而言，需要多次从集合 R 中随机抽取 v+1 个点来重建多项式以寻找正确的密钥。因此，获得的密钥特征越多，越容易建立密钥。冗余点个数以及多项式次数与密钥安全性之间的关系如图 5 所示。由图 5 可以看出，冗余点个数越多，密钥的安全性越高。同时，多项式阶数越高，重建密钥需要的密钥特征也会越多，从而使密钥具有更高的安全性。

4　结束语

本文基于在动态无线信道中通信双方可以获得具有较高相似度的 RSS 变化特性，而处于距通

（下转 P58）

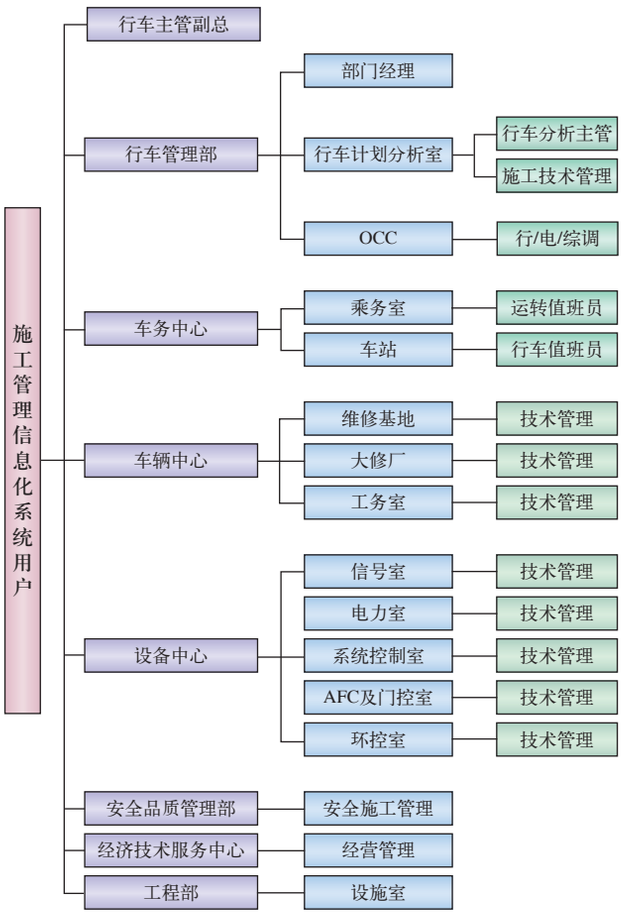

图6　施工管理系统用户结构

3　结束语

在城市轨道交通技术快速发展的背景下，智能、简单、高效将成为运营管理的基本趋势，以信息系统为辅助进行施工管理是提高管理效率、降低错误风险的必然选择。天津地铁施工管理系统建设完成后，可以辅助管理部门对当前 3 条线路、61 座车站、6 个站场施工进行高效管理，促进地铁运营管理水平的整体提升。

参考文献：

[1] 天津地铁行车管理制度 [G]. 天津：天津市地下铁道运营有限公司，2012.

[2] 史小俊，王亚超 . 天津地铁运营线路的维修施工管理 [J]. 城市轨道交通研究，2009（5）：58-60.

[3] 薛华成 . 管理信息系统 [M]. 北京 : 清华大学出版社，2007.

[4] 王创奇 . 地铁运营“智能化施工管理系统”实施可行性分析 [J]. 经济技术协作信息，2009（36）：111.

[5] 张学兵，俞太亮，张正贵 . 地铁运营线路施工安全控制要点 [J]. 现代城市轨道交通，2012（2）：65-67.

责任编辑　陈　蓉

（上接 P49）

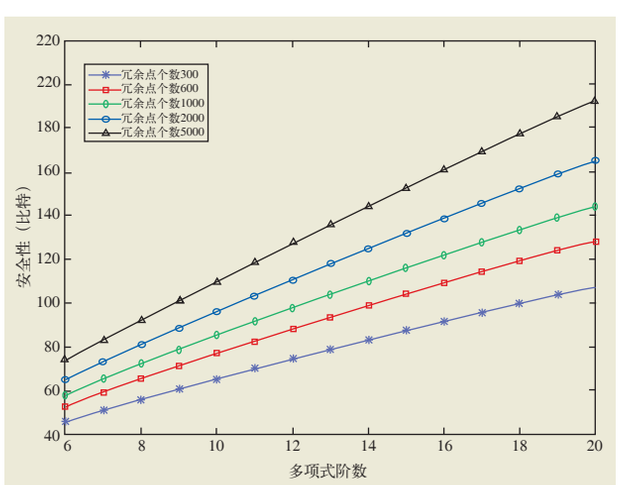

图5　冗余点个数、多项式阶数与密钥安全性的关系

信双方一个波长范围外的攻击者由不能获取与通信实体相似的 RSS 变化特性这一原理，给出了合理的在动态无线信道中提取密钥特征的方法。同时，本文将该密钥特征提取方法与 Fuzzy Vault 算法相结合，提出了无线终端在移动无线环境下密钥的安全分配机制，从而保证了铁路通信系统中利用无线终端安全传送信息。

参考文献：

[1] S. Jana,S. N. Premnath, M. Clark, S. Kasera, N. Patwari, and S. Krishnamurthy. On the effectiveness of secret key extraction from wireless signal strength in real environments [C]. Beijing: In ACM MobiCom, 2009: 321-332.

[2] Ali, Syed Taha, Vijay Sivaraman, and Diethelm Ostry. Zero reconciliation secret key generation for body-worn health monitoring devices [C]. Proceedings of the 5th ACM conference on Security and Privacy in Wireless and Mobile　Neworks. ACM, 2012: 39-49.

[3] A. Juels and M. Sudan. A fuzzy vault scheme [J]. Designs, Codes, and Cryptography, 2006, 38(2): 237-257.

[4] 刘艳涛，游　林 . 一种改进的随机性模糊金库算法 [J]. 科技通报，2011，27（2）：288-292.

[5] 宋　伟，王阿川 . 基于纠错码的指纹加密算法研究 [J]. 中国安全科学学报，2009，19（9）：97-101.

责任编辑　陈　蓉