Hans Journal of Wireless Communications 无线通信, 2020, 10(6), 84-90
Published Online December 2020 in Hans. http://www.hanspub.org/journal/hjwc
https://doi.org/10.12677/hjwc.2020.106012

Hans汉斯

基于EMD的物理层生成密钥方案在车辆通信中的研究

张红华，白恩健

东华大学信息科学与技术学院，上海
Email: m18879752216@163.com

收稿日期：2020年11月10日；录用日期：2020年11月21日；发布日期：2020年12月4日

摘　要

利用信道内在的随机性和互惠性来生成实现车辆安全通信所需的共享密钥是一种有效的方法。然而，由于一些因素，当通信双方完成相互探测信道后，获得的信道测量序列之间存在许多差别。当这些测量值直接用来生成密钥序列，会导致较高的比特不匹配率，给信息协商阶段增加一定的负荷。在这篇文章中，我们利用经验模态分解(EMD)来预处理这些测量序列，得到的序列经过量化及编码、信息协商和保密增强等步骤，生成最后的共享密钥。我们做了一些实验来评估该方案，实验结果表明，经过EMD方法预处理后，通信双方的信道探测序列间差异明显减少，并且生成的共享密钥通过了随机性测试。

关键词

车辆通信，物理层安全，预处理，经验模态分解

Research on EMD-Based Physical Layer Key Generation Scheme in Vehicle Communication

Honghua Zhang, Enjian Bai

College of Information Science and Technology, Donghua University, Shanghai
Email: m18879752216@163.com

Received: Nov. 10th, 2020; accepted: Nov. 21st, 2020; published: Dec. 4th, 2020

Abstract

It is an effective method to use the inherent randomness and reciprocity of the channel to gener-

文章引用: 张红华, 白恩健. 基于 EMD 的物理层生成密钥方案在车辆通信中的研究[J]. 无线通信, 2020, 10(6): 84-90.
DOI: 10.12677/hjwc.2020.106012

ate the shared key needed to realize the secure communication of the vehicle. However, due to some factors, there are some discrepancies between the channel measurement sequences obtained after the two communication parties complete the mutual detection of channels. In addition, when these measured values are directly used to generate the key sequence, it will lead to a high bit mismatch rate and add a certain load to the information reconciliation stage. In this article, we use Empirical Mode Decomposition (EMD) to preprocess these measurements, and the resulting sequence undergoes quantification and coding, information reconciliation and privacy amplification steps to generate the final shared key. Moreover, we have done some experiments to evaluate the scheme. The results demonstrate that after the preprocessing of the EMD scheme, the difference between the channel detection sequences of the communicating parties is significantly reduced, and the generated shared key has passed the randomness test.

Keywords

Vehicle Communication, Physical Layer Security, Preprocess, Empirical Mode Decomposition

1. 引言

相比于基于计算复杂度的传统密钥确立方案，物理层生成密钥方案更适合车辆通信。因为窃听者 Eve 的计算能力在不断增强，并且高速移动的合法车辆 Alice 和 Bob 通信对实时性要求很高。随着时间和空间的变化，Alice 和 Bob 之间的信道也一直在变化，因此随机性作为生成密钥源是合理的。在相干时间内，由于信道互惠性，通信双方会获得几乎相同的信道探测，这为生成共享密钥提供有利条件[1] [2]。

合法通信双方 Alice 和 Bob 要得到共享密钥，都需要完成以下工作：信道探测，量化及编码，信息协商，保密增强等。在信道测量，通信车辆分别测量之间的信道，得到接受信号强度(RSS)数据集[3]。然后将这数据集分别应用相同的量化方案，映射成比特序列；并且采用网络编码方案，生成二进制比特序列，提高数据的利用率[4]。实际上，由于信道互惠性，这些比特序列是高度相关的，但也存在一些差别。幸运的是，应用信息协商技术能纠正这些不匹配的比特[5]。通常而言，在信息协商阶段会泄露一些重要信息，被 Eve 获得。因此，我们应用保密增强等技术来删除这些泄露的信息，同时提高共享密钥的随机性[6]。

在信道探测期间，尽管通信双方每一轮探测都在一个相干时间内完成，然而由于通信是半双工模式，并且信道环境存在许多干扰等因素，Alice 和 Bob 各自获得的 RSS 数据集之间存在一些差别。这些差别会量化成不同的比特，在信息协商阶段造成一定程度的负荷，不仅消耗更多的能量，还可能会泄露更多的信息给 Eve [7]。因此，对于通信双方而言，需要预处理这些 RSS 数据集，以减少之间的不匹配，保证有效地生成共享密钥。

最近，许多结合数据预处理技术的密钥生成方案在车辆通信中被提出。其中，使用 RSS 数据集来生成共享密钥最为常见，因为它与几乎所有现成的设备兼容[8]。而对 RSS 数据集进行预处理是我们最关注的。论文[9]中，使用移动平均法来减小 RSS 数据集中小波动的影响，然后再从每个 RSS 样本中提取一个比特。但是，该方案只能过滤 RSS 样本平均值带来的效果，并不能有效解决通信双方 RSS 样本之间的不匹配问题。在论文[10]中，提出一种加权滑动窗口平滑方法，能有效地去除噪声带来的影响。然而这并

不能解决车辆半双工通信造成 RSS 数据间的差异。在论文[11]中，基于离散小波变换(DWT)的压缩器被用于预处理相关收发器的测量。众所周知，RSS 数据集是非线性非平稳的，而应用 DWT 处理非线性非平稳数据的效果并不良好。

鉴于以上存在问题，我们提出一种方案，为车辆通信生成共享密钥。其中，应用经验模态分解(EMD)来预处理 RSS 数据集，该方案能减少 RSS 数据集量化后生成的比特序列之间不匹配的比特数量[12]。预处理过后的 RSS 需要经过量化和编码，生成二进制比特序列；然后再应用量子密码学中的两种技术，信息协调和隐私放大，来确定最后的共享密钥。与此同时，我们也做了一些实验来验证该方案。我们的工作主要贡献如下：

1) 提出一种生成共享密钥方案，该方案可以应用于环境复杂的车辆通信中。

2) 应用 EMD 处理 RSS 数据集，降低噪声等因素的影响，提高数据的利用率。

3) 这种数据处理方法在一定程度上能改善其他技术，如傅里叶变换、小波变换等，处理非线性、非平稳的数据不够良好的效果，并将其引入到车辆通信中。

2. 理论知识

2.1. RSS 的定义

RSS 是当前在密钥生成中使用的最流行的信道参数，由于其可用性，对于实际实施而言尤其如此。假设发射信号$x(t)$，经历多径信道 h，则接收信号可以写为

$$y(t)=\int_{0}^{\tau_{\max}} h(\tau,t)x(t-\tau)\mathrm{d}\tau+n(t), \tag{1}$$

其中，$n(t)$表示信道噪声。并且，接收信号 $y(t)$ 的平均功率称为 RSS [13]。因此，我们可以发现，通信双方相互探测信道，得到的 RSS 样本是非线性非平稳的数据集。

2.2. 数据预处理技术

尔伯特 - 黄变换(HHT)是一项伟大的发明，在许多领域发挥着重要作用。它采用两种方法来解决问题，其中一种是经验模态分解(EMD)，另一种是希尔伯特谱分析(HAS) [14]。在我们的工作中，只需要用到 EMD 来处理非线性非稳态的 RSS 样本，减少之间的不匹配量。

EMD 往往被称为是一个“筛选”过程。这个筛选过程依据信号特点自适应地把任意一个复杂信号分解为若干固有模态函数(IMFs)。这些 IMF 是满足一定条件的分量：1) 信号极值点的数量与零点数相等或相差是一，2) 信号的由极大值定义的上包络和由极小值定义的下包络的局部均值为零。因此，给定任意一维离散信号，EMD 最终可以编写成

$$\xi(t)=\sum_{i=1}^{K} IMF_i(t)+r_K(t), \tag{2}$$

其中 $\xi(t)$ 是原始信号，$IMF_i(t)$ 是K个固有模态函数，r_K 是原始信号减完IMF后剩下的余项。具体的筛选过程基本上是这样完成的：

1) 首先，必须识别局部极限的数据，即信号$\xi(t)$的最小值和最大值。

2) 最大值与插值连接，创建信号的顶部包络。

3) 最小值与插值相连，产生信号的下包络。

4) 计算上下包络的平均值。

5) 从原始信号中减去局部平均值。

6) 剩下的数据被认为是相同的数据，重复以上步骤相同的过程。

当 r_K 的极大值或极小值点数目有一个为零，或者 r_K 已经是单调时，表示 r_K 无法分离出 IMF，此时 EMD 这一步就彻底结束了[15] [16]。

3. 提出的方案

在这篇论文中，我们提出利用信道环境的随机性、互惠性等来为车辆通信确立共享密钥的方案。该方案中主要的工作包括：信道探测，预处理，量化及编码，信息协商和保密增强。该方案有望适用于复杂的真实车辆通信场景和信道环境。

3.1. 信道探测

通信车辆双方 Alice 和 Bob，连续地测量之间的公共信道，来导出信道状态。这些信道状态能作为随机性公共源，来生成共享密钥。在我们的工作中，RSS 测量值用于表示信道状态。并且，每一轮测量需要在一个相干时间内完成。因为根据信道互惠性，相干时间期间的信道可以认为是恒定的。因此，在一个相干时间内，Alice 和 Bob 在两次探测中，得到的信道测量近乎相等。Alice 和 Bob 将重复上述过程，直到收集到足够的测量为止。

3.2. 预处理

在预处理阶段，Alice 和 Bob 应用 EMD 方法，分别处理各自的 RSS 样本，以减少样本之间的差异，进一步增强信道互惠性。我们说的差异是量化后得到的比特不一样，而不是样本值之间存在不同。处理过后的数据应用到下一个阶段，即量化和编码，来提高数据的利用率。

为了保证通信双方使用相同的预处理方案，Alice 首先确定选择 EMD 方案，通过公共信道将消息发送给 Bob；然后，Bob 收到消息后，通过原来的信道，返回一个确认(ack)给 Alice。此时，表明双方已建立连接。最后，Bob 确定选择第i个 *IMF* 作为新的 RSS 样本，并将i发送给 Bob，Bob 根据接收到的消息，完成自己的数据预处理过程。此时，双方已确定完全相同的 EMD 方案。

在一方面，每个 *IMF* 都是线性平稳的，这能保证在量化阶段，能有效地减少因为数据之间较大的差异，而被量化成不同的比特值的情况发生。虽然这可能会损失一些随机性，但是我们在后面阶段会应用保密增强技术，来提高生成密钥的随机性。当然，我们也会做一些相应的实验来验证。在另一方面，因为平均 RSS 值会以某种方式暴露合法车辆间的一些信息，比如距离。而新的 RSS 是 *IMF*，每一个 *IMF* 的生成过程都删除了平均 RSS 值。因此该方案在另一方面能为共享密钥确立方案提供一定的安全性。虽然，一些信息，比如处理方案，i的选择等，在公共信道传输可能会被窃听者 Eve 获得。但是，得益于空间去相关特性，窃听者无法正确估计 Alice 和 Bob 间的信道探测。

3.3. 量化及编码

在我们的方案中，不是直接将 RSS 样本生成共享密钥，而是将其先映射成二进制比特序列，作为初始密钥。为了避免数据的浪费，我们使用论文[17]中提出的方法，将可用的一个 RSS 映射成两个比特，来提高数据的利用率。首先，确定四个阈值，

$$q_n = \mu + \alpha_k \sigma, \tag{3}$$

其中 $k = 1,2,3,4$，μ，σ 是 RSS 读数的平均值和标准偏差，α_1，α_2，α_3，α_4 的值是电平微调系数，并且 $\alpha_1 \geq 1$、$\alpha_4 \geq 1$、$0 < \alpha_3 < 1$、$0 < \alpha_2 < 1$，$q_4 > q_3 > q_2 > q_1$。然后，Alice 和 Bob 通过判断各自的每一个 RSS 测量值坐落在公式(4)中的哪一个区间，来提取对应的两个比特。最后，当所有的 RSS 样本判断完毕后，生成

各自初始比特流。具体的编码规则为

$$Q(r)=\begin{Bmatrix}00 & 若r\le q_1\\ 01 & 若q_1<r\le q_2\\ 10 & 若q_3\le r<q_4\\ 11 & 若r>q_4\end{Bmatrix}, \tag{4}$$

其中，r 表示一个 RSS，Q 对应量化及编码阶段完成得到的二进制序列。因此，q_2 和 q_3 之间的 RSS 样本被丢弃。为了提高数据利用率，α_2 和 α_3 应该设置为最小可能值。并且，α_1，α_2，α_3，α_4 应适当调整，以适应车辆通信复杂的信道环境。

3.4. 信息协商和保密增强

由于一些因素，如噪声、车辆通信系统半双工模式等，合法车辆的信道测量值之间存在一些差别，这给确立相同的共享密钥带来挑战。因此，我们在量化及编码步骤后，应用信息协商技术。在我们的方案中，我们应用 Cascade 协议来纠正这些存在差异的比特。通过将完整的比特序列划分成多个小块，合法车辆检查每个小块的比特流，来纠正之间的不匹配的比特，确立相同的比特序列。

为了删除在信息协商阶段泄露的信息，并且提高共享密钥的随机性，需要用保密增强技术。我们采用论文[3]中提出的方法，其中，Alice 首先确定参数，然后将这些参数发送给 Bob，最后 Alice 和 Bob 应用该方法，生成比特序列，作为最后的共享密钥，实现安全通信。

4. 仿真结果与分析

我们从真实车辆通信环境中获得 RSS 样本，然后应用我们的预处理方案，观察比特不匹配率(BMR)的情况，来验证方案的性能。其中，BMR 定义为量化及编码后不匹配的比特数与应用量化及编码方案生成的比特总数的比例。同时，我们验证生成的最后共享密钥的随机性，判断我们提出的共享密钥确立方案是否可行。

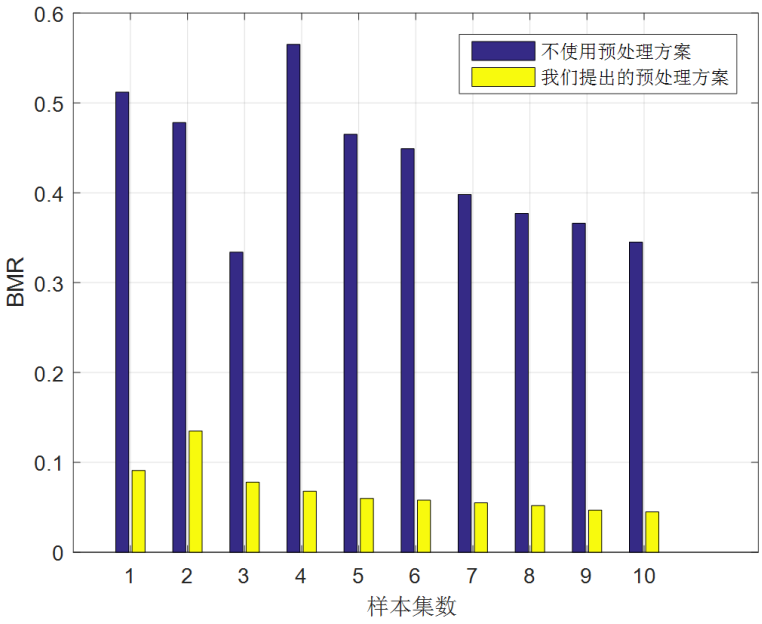

Figure 1. BMR comparison of different methods under different data sets.
图 1. 不同方法在不同数据集下的 BMR 比较

4.1. 比特不匹配率 BMR

我们首先计算在不同的数据集下的 BMR，并与不使用预处理方案得到的进行对比，如图 1 所示。从图上，我们能清楚地发现，当将 RSS 数据直接量化成比特时，BMR 在(0.3, 0.6)之间浮动。这意味着有大量 RSS 样本被量化成不同的比特，这给信息协商阶段带来巨大的挑战，严重降低共享密钥确立方案的性能；而当使用 EMD 预处理方案对 RSS 数据进行处理，很明显，不论数据集的个数，BMR 的值都有很大程度地下降。这表明，我们提出的 EMD 方案能很好的应用到共享密钥确立方案中，有效地减少因为各种因素导致的通信车辆双方信道探测样本之间的差异。

4.2. 密钥序列随机性

我们提出了一种能应用到复杂车辆通信环境中的共享密钥确立方案。为了验证该方案的可行性，我们应用 NIST 测试套件来测试应用该方案获得的共享密钥序列的随机性。其中，NIST 测试套件包含 15 项测试，每一项测试完成后都会返回对应的 p 值。当且仅当 $0.01 < p \leq 1$ 时，比特序列通过了该项测试。因为车辆通信所需密钥的长度是 256 bit，而 NIST 测试套件有一部分测试需要较长的比特序列。因此，我们只需要进行 9 项测试即可，测试结果如表 1 所示。所有返回的 p 值，也即测试结果，都大于 0.01。这表明应用该共享密钥确立方案得到的密钥序列，通过了所有的所需测试，具有很好的随机性，能够应用在车辆通信中。

Table 1. Randomness test of key sequence obtained by applying our scheme
表 1. 应用我们的方案得到的密钥序列随机性测试

测试类型	p 值	通过/失败
ApproximateRntropy	0.653629	通过
BlockFrequency	0.175089	通过
CumulativeSums	0.222775	通过
FFT	0.621622	通过
Frequency	0.498531	通过
Runs	0.371308	通过
Serial	0.498613	通过
NonOverlappingTemplate	0.064646	通过
LongestRun	0.234677	通过

5. 结论

本文提出了一种有效应用于车辆通信的共享密钥确立方案，其中 EMD 方法用于预处理数据样本，能有效地处理样本间的不匹配的数据。实验结果也表明，EMD 方法能有效降低比特不匹配率；并且，应用该共享密钥确立方案得到的密钥序列具有较好的随机性，能够应用于车辆安全通信。

参考文献

[1] Perrig, A., Szewczyk, K., Wen, V., Culler, D. and Tygar, J. (2002) Spins: Security Protocols for Sensor Networks. *Wireless Networks*, **8**, 521-534. https://doi.org/10.1023/A:1016598314198

[2] Mathur, S., Trappe, W., Mandayam, N., Ye, C. and Reznik, A. (2008) Radiotelepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel. *Proceedings of the* 14*th ACM International Conference on Mobile Computing and*

Networking, New York, September 2008, 128-139.

[3] Jana, S., Premnath, S.N., Clark, M., Kasera, S.K., Patwari, N. and Krishnamurthy, S.V. (2009) On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments. *Proceedings of the* 15*th Annual International Conference on Mobile Computing and Networking*, *MOBICOM* 2009, Beijing, 20-25 September 2009, 321-332. https://doi.org/10.1145/1614320.1614356

[4] Patwari, N., Croft, J., Jana, S. and Kasera, S.K. (2010) High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements. *IEEE Transactions on Mobile Computing*, **9**, 17-30. https://doi.org/10.1109/TMC.2009.88

[5] Brassard, G. and Salvail, L. (1994) Secret-Key Reconciliation by Public Discussion. In: *Advances in Cryptology EUROCRYPT*93, Springer, Berlin, 410-423. https://doi.org/10.1007/3-540-48285-7_35

[6] Jana, S., Premnath, S.N., Clark, M., Kasera, S.K., Patwari, N. and Krishnamurthy, S.V. (2009) On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments. *Proceedings of the Annual International Conference on Mobile Computing and Networking*, *MOBICOM*, Beijing, 20-25 September 2009, 321-332.

[7] Azimi-Sadjadi, B., Kiayias, A., Mercado, A. and Yener, B. (2007) Robust Key Generation from Signal Envelopes in Wireless Networks. *Proceedings of the* 2007 *ACM Conference on Computer and Communications Security*, *CCS* 2007, Alexandria, 28-31 October 2007, 401-410. https://doi.org/10.1145/1315245.1315295

[8] Ye, C., Mathur, S., Reznik, A., Shah, Y., Trappe, W. and Mandayam, N.B. (2010) Information-Theoretically Secret Key Generation for Fading Wireless Channels. *IEEE Transactions on Information Forensics and Security*, **5**, 240-254.

[9] Zan, B., Gruteser, M. and Hu, F. (2013) Key Agreement Algorithms for Vehicular Communication Networks Based on Reciprocity and Diversity Theorems. *IEEE Transactions on Vehicular Technology*, **62**, 4020-4027. https://doi.org/10.1109/TVT.2013.2254507

[10] Zhu, X., Xu, F., Novak, E., Tan, C.C., Li, Q. and Chen, G. (2013) Extracting Secret Key from Wireless Link Dynamics in Vehicular Environments. 2013 *Proceedings IEEE INFOCOM*, Turin, 14-19 April 2013, 2283-2291. https://doi.org/10.1109/INFCOM.2013.6567032

[11] Zhan, F.R. and Yao, N.M. (2017) On the Using of Discrete Wavelet Transform for Physical Layer Key Generation. *Ad Hoc Networks*, **64**, 22-31. https://doi.org/10.1016/j.adhoc.2017.06.003

[12] Huang, N., Wu, Z.H. and Long, S. (2008) Hilbert-Huang Transform. *Scholarpedia*, **3**, 2544. https://doi.org/10.4249/scholarpedia.2544

[13] Zhang, J., Duong, T.Q., Marshall, A. and Woods, R. (2016) Key Generation from Wireless Channels: A Review. *IEEE Access*, **4**, 614-626. https://doi.org/10.1109/ACCESS.2016.2521718

[14] Huang, N. and Wu, Z.H. (2008). A Review on Hilbert-Hung Transform Method and Its Applications to Geophysical Studies. *Reviews of Geophysics*, **46**, RG2006. https://doi.org/10.1029/2007RG000228

[15] Rong, F., Chen, N., Guo, C. and Yang, M. (2018) New Method for Speed Curve Estimation by Using the EEMD-HHT Combined with Time-Frequency Reassignment. *Journal of Vibration and Shock*, **37**, 81-87.

[16] Córdova, F., Cifuentes, F. and Atero, R. (2018) Hilbert Huang Transform (HHT) Applied to Memorization of Objects Using the Tactile Sense. 2018 7*th International Conference on Computers Communications and Control* (*ICCCC*), Oradea, 8-12 May 2018, 23-28. https://doi.org/10.1109/ICCCC.2018.8390432

[17] Salih Abdelgader, A.M., Feng, S. and Wu, L. (2018) Exploiting the Randomness Inherent of the Channel for Secret Key Sharing in Vehicular Communications. *The International Journal of Intelligent Transportation Systems Research*, **16**, 39-50. https://doi.org/10.1007/s13177-017-0136-4