Cascade 密钥协商的改进方案

贾仁庆,吴晓富,朱卫平
(南京邮电大学 通信与信息工程学院,江苏 南京 210003)

摘 要:随着移动互联网业务的快速发展,无线通信安全已成为一个重要课题。近年来,无线密钥提取技术引起了研究者们的关注,通过无线密钥提取技术促使合法通信双方拥有大量的共享密钥,结合一次一密机制,使实现信息论意义上的绝对安全成为可能。密钥协商是提取物理层密钥的关键步骤。在众多的密钥协商方案中,Cascade 协商方案由于能够高效地协商出一致的密钥而备受关注。然而,Cascade 协商采用二分法进行纠错,在纠错的过程中需要通信双方不断交互校验信息,从而导致 Cascade 对网络延迟较为敏感。为了降低 Cascade 协商的交互次数,提出 Cascade 的一种改进方案,利用截止二分搜索方案进行密钥协商。实验仿真结果表明:所提方案可以在保证密钥协商效率的同时,有效降低了通信双方的交互次数。

关键词:物理层安全;Cascade 协商;交互次数;效率
中图分类号:TN918 **文献标识码**:A **文章编号**:1673-629X(2016)11-0097-04
doi:10.3969/j.issn.1673-629X.2016.11.022

An Improved Scheme of Cascade Protocol

JIA Ren-qing, WU Xiao-fu, ZHU Wei-ping
(College of Telecommunication & Information Engineering, Nanjing University of Posts and Telecommunication, Nanjing 210003, China)

Abstract: With the rapid development of mobile Internet services, information security for wireless communication is becoming a very important research topic. Recently, there has been great interest in generating the shared secret key based on the physical layer security techniques, which could achieve the perfect secrecy combined with a one-time pad. Information reconciliation is a key step of secret key generation. Cascade is the most famous reconciliation protocol duo to the high efficiency. However, Cascade is highly interactive protocol which makes it very sensitive to network latencies. In order to reduce the number of communications, a modifying strategy of Cascade is proposed by Abort-BINARY searching. Extensive simulation results show that the modifying strategy could ensure high efficiency of information reconciliation and reduce the number of communications effectively.

Key words: physical layer security; Cascade; number of communications; efficiency

0 引 言

近年来,物理层安全技术引起了研究者们的广泛关注。合法用户可以利用无线信道固有的随机性协商出一致的密钥,而不需很大的计算复杂度[1-2]。实际的物理层密钥提取方案可分为三个步骤进行:第一步为优势提取阶段[3-4],在 TDD 半双工模式下,无线信道具有互易性,且当窃听者 Eve 与 Alice、Bob 的距离都大于波长的一半 $\lambda/2$ 时,合法信道与窃听信道基本不相关,Alice、Bob 分别提取信道特征并进行量化,得到不一致的初始密钥序列[5];第二步为密钥协商阶段[6],Alice、Bob 在公共信道上交换纠错信息以达到协商出一致密钥序列的目的。由于密钥协商需要在公共信道上传递纠错信息,向窃听者 Eve 泄露了部分信息。为了增强密钥的安全性,协商出来的密钥需要通过 Hash 进行密钥增强[7-10]。

密钥协商是物理层提取密钥的关键一步。针对协商技术,文献[11]提出了 BBBSS 协议,后来文献[5]提出了著名的 Cascade 协商技术。在这两种协议中,首先 Alice、Bob 分别对密钥进行分组,并交换每组的奇偶值。若某一个分组的奇偶性不同,则说明在该分

收稿日期:2016-01-25 **修回日期**:2016-05-11 **网络出版时间**:2016-10-24
基金项目:国家自然科学基金资助项目(61372123)
作者简介:贾仁庆(1989-),男,硕士,研究方向为物理层安全;吴晓富,教授,研究方向为物理层安全;朱卫平,教授,研究方向为无线通信信号处理。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20161024.1117.064.html
万方数据

组内至少会有一个错误比特,然后 Alice、Bob 通过二分法进行纠错。在二分法纠错过程中,需要 Alice、Bob 之间多次交互每组的奇偶值,从而导致了这种协商技术对网络延时等较为敏感[12]。文献[13-15]提出了利用汉明码的伴随式进行前向纠错—Winnow 技术,尽管该技术降低了协商的交互次数,但是纠错效率出现了大幅度的折损。文献[14]提出利用前向纠错码(如 LDPC 码)进行协商。LDPC 协商技术可以降低交互次数,并提高协商效率。但是,LDPC 码进行协商时需要终端进行比较多的计算,并且协商效率受到码长的影响。

Cascade 采用二分法进行纠错,二分法可以迅速锁定错误比特的范围,直到最后找到错误比特的位置。然而,一方面二分法纠错需要 Alice、Bob 不断地交互信息,另一方面当分组长度锁定到 $s \leqslant 3$ 以下时,若继续使用二分法查询错误比特的位置,则这 s 个比特密钥信息几乎会全部暴露,此时仍然利用二分法搜索错误的位置就没有任何实际意义。

为此文中提出了截止二分法搜索方案,当分块长度缩小到 3 时,不再继续使用二分法纠错,而是直接删除,不再作为协商的密钥部分;为了支持 Cascade 中回溯二分纠错功能,Alice 把待删除位置的密钥直接发送给 Bob,从而达到减少 Alice、Bob 交互次数的目的。仿真结果表明,提出的 Cascade 改进方案能够降低 Alice、Bob 之间的交互次数。

1 Cascade 协商

Cascade 协商是在二分法纠错基础上的一种密钥协商协议。为了完整地介绍 Cascade 协商方案,本节将首先介绍二分法纠错,然后详细介绍 Cascade 协商方案。

1.1 二分法

二分法纠错是 Cascade 协商的核心步骤,通过二分法可以迅速锁定错误比特的所在位置,并进行纠错。

令 Alice、Bob 进行协商的密钥序列分别为 $A = A_1, A_2, \cdots, A_N, B = B_1, B_2, \cdots, B_N$,密钥长度为 N,误码率为 ε。如图 1 所示,假定序列 A,B 中有奇数个不同的比特,Alice、Bob 通过二分法可纠正一个比特,纠错的具体步骤如下[4]:

步骤 1:Alice 把序列 A 等分为两部分,并把第一部分的奇偶值 a 发送给 Bob;

步骤 2:Bob 按照同样的方式把 B 分为两部分,并计算第一部分的奇偶值 b,若 $a \neq b$,说明在第一部分有奇数个错误比特,否则说明在第二部分中有奇数个错误比特;

步骤 3:重复步骤 2,直到获取错误比特的位置,并对该位置的比特进行纠正。

Alice	Bob
1 1 0 1 1 0 0 0 1 0 1 1 ⊕=1	1 1 0 0 1 0 0 0 1 0 1 1 ⊕=0
1 1 0 1 1 0 ⊕=0	1 1 0 0 1 0 ⊕=1
1 1 0 ⊕=0	1 1 0 ⊕=0
1 1 ⊕=0	0 1 ⊕=1
1 ⊕=1	0 ⊕=0 0→1

图 1 二分法纠错

如图 1 所示,Alice、Bob 中有一个不同的比特信息(第 4 个),通过二分法搜索可迅速锁定错误比特所在的位置,并对错误比特进行纠正。然而,当二分法把错误比特所在的范围锁定到 $s \leqslant 3$ 个比特以内时,若继续使用二分法查询错误比特,这 s 个比特几乎会全部泄露给窃听者。

1.2 Cascade 协商方案

文献[12]提出了 Cascade 密钥协商机制。Cascade 通过多轮反复纠正错误比特,在第一轮通过二分法纠错使得每个小组内含有偶数个错误的比特;在第 $i > 1$ 轮中,Alice、Bob 对密钥串进行随机分组,比较每组的校验值并用二分法进行纠错。当发现一个新的错误时,在之前轮中对应的分组内必含有奇数个错误比特,再次通过二分法纠错,从而使得纠正的比特数倍增,提高了密钥的协商效率。Cascade 协商机制的具体步骤如下:

步骤 1:Alice、Bob 对密钥串进行分组,每组密钥长度为 k_1,其中第 v 组密钥的位置应满足 $K_v^1 = \{l \mid (v-1)k_1 < l \leqslant vk_1\}$。Alice 计算每组密钥的奇偶性,并把每组的奇偶性发送给 Bob。Bob 按照同样的方法计算奇偶性并进行比较,对于奇偶性不相等的组,Alice、Bob 通过二分法纠正错误比特。经过步骤 1,每组只可能含有偶数个错误的比特(包括 0)。在进行分组时,分组长度 k_1 取决于误比特率 p,为了使平均每组包含的错误比特数小于 1,文献[8]取 $k_1 = 0.73/p$。

步骤 $i(i > 1)$:Alice、Bob 通过随机函数 f_i:$[1 \cdots n] \rightarrow [1 \cdots \lceil n/k_i \rceil]$ 对 N 个比特重新分组,每组的密钥长度为 k_i。经过第 i 轮分组后,序号 j 对应的分组为 $K_j^i = \{l \mid f_i(l) = j\}$。Alice 计算此时各分组的奇偶性 $a_j = \bigoplus_{l \in K_j^i} A_l$;Bob 按照同样的方式计算奇偶性 b_j 并与 a_j 进行比较。若 $a_j \neq b_j$,Bob 通过二分法搜索错误比特所在的位置 $l \in K_j^i, B_l \neq A_l$,并纠正错误比特。这样,从步骤 1 到步骤 $i-1$ 阶段所有包含位置 l 的分组 $K_v^u (1 \leqslant u < i, l \in K_v^u)$,都会含有奇数个错误比特。设这些分组的集合为 Γ,Alice、Bob 对集合 Γ 内的分组都进行二分法纠错。Bob 纠正位于 l' 的错误比特 B_l' 后,可以确定包含 B_l' 的所有分组集合 Λ,从而更新含有奇数的错误比特的分组集合 $\Gamma' = (\Lambda \cup \Gamma) \backslash (\Lambda \cap$

万方数据

Γ)。当 $\Gamma' \neq \varnothing$ 时,说明位于 Γ' 集合中的分组含有奇数个错误比特,Alice、Bob 持续通过上述回溯进行纠错,直到 $\Gamma' = \varnothing$ 为止。

Alice、Bob 重新随机分组并比较每组奇偶性,当某个分组的奇偶性不一样时,就进行新一轮的纠错。当第 i 轮纠错结束时,从 Pass1 到 Pass$i$ 所有分组内都包含偶数个错误比特(包括 0)。文献[5]中推荐 Cascade 执行 $i=4$ 轮纠错,每轮分组的长度可设定为 $k_i = 2k_{i-1}$, $k_1 = 0.73/p$。

从 Cascade 密钥协商步骤可以看出,在步骤 $i \geqslant 1$ 纠错的过程中,若在 K_v^1 中发现了一个错误比特,则 K_v^1 中必定会有第二个错误比特。在分组 K_v^1 内,经过第 $i > 1$ 步纠错后含有 $2j$ 个错误比特,用 $\delta_1(j)$ 表示,由 $X \approx \mathrm{Bin}(k_1, p)$ 知 $\delta_1(j) = \mathrm{prob}(X = 2j) + \mathrm{prob}(X = 2j+1)$。根据文献[5],经过步骤 ω 后,每个长度为 k_1 的分组所泄露的信息量为:

$$I(\omega) \leqslant 2 + \frac{1-(1-2p)^{k_1}}{2}\lceil \log k_1 \rceil + 2\sum_{l=2}^{\omega}\sum_{j=1}^{\lfloor k_l/2 \rfloor}\frac{j\delta_1(j)}{2^{l-1}}\lceil \log k_1 \rceil \quad (1)$$

经过 Cascade 协商后,Alice、Bob 可以获取一致的密钥序列,由于在协商过程中泄露了密钥信息,完成协商后需要进行密钥增强[13]以得到安全的密钥。Cascade 协商的效率较高且实现简单,然而 Cascade 需要 Alice、Bob 之间不断地相互传递信息。若设分组长度为 k,则一次二分法纠错需要交互 $\log_2 k$ 次,尤其是在回溯纠错的过程中,交互次数会猛增,从而导致传输网络的延迟等情况会影响到 Cascade 协商的性能。

2　Cascade 协商的改进

2.1　改进方案的思路

Cascade 采用二分法进行纠错,二分法可以迅速锁定错误比特的范围,直到最后找到错误比特的位置,进而纠正错误比特。通过第 1 节中的介绍可以看出,Cascade 密钥协商的效率是很高的。然而,Cascade 密钥协商算法也具有一些不可避免的缺陷。一方面二分法需要在合法通信双方 Alice、Bob 之间不断地交互信息,在一个长度 k 的分组内,一次二分法纠错过程需要 $\log_2 k$ 次交互,由于在回溯过程中需要多次二分纠错,从而导致在 Cascade 密钥协商过程中 Alice、Bob 之间的交互通信次数会大幅度增加,因此当网络环境出现延迟等特殊情况时可能会对 Cascade 协商的效率产生不利的影响。另一方面,二分法可以迅速锁定单个错误比特所在的范围,然而当错误比特所在范围锁定到 3 个比特以下时,若继续利用二分法进行搜索,则会把小组内比特几乎会全部泄露给窃听者 Eve。以错误位置锁定到 3 个比特为例,判断错误比特位于这三个比特之内需要 1 个比特校验信息,利用二分法找到错误比特所在位置又需要 $\lceil \log 3 \rceil = 2$ 个比特的校验信息,这 3 个比特基本上全部泄露给了窃听者 Eve,继续利用二分法搜索错误的位置已没有任何实际意义。为此,文中提出了截止二分法协商方案。如图 2 所示,当分块长度缩小到 3 以内时就不再继续二分查找,而是直接删除该部分的比特,不再作为协商的密钥部分。为了支持 Cascade 密钥协商中的回溯二分纠错功能,合法通信双方暂且保留要删除的数据,Alice 把待删除位置的密钥直接发送给 Bob,同时记录需要删除数据的位置,从而达到减少合法通信双方 Alice、Bob 交互通信次数的目的。

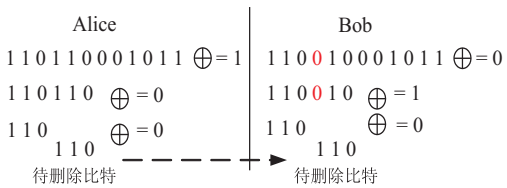

图 2　截止二分协商

2.2　改进方案的主要步骤

如图 2 所示,截止二分协商的步骤如下:

步骤 1:Alice 把序列 A 分为两部分,并把第一部分的奇偶值 a 发送给 Bob。

步骤 2:Bob 按照同样的方式把 B 分为两部分,并计算第一部分的奇偶值 b,若 $a \neq b$,说明在第一部有错误比特,否则说明在第二部分中有错误比特。

步骤 3:计算错误比特所在部分的序列长度 s,当 $s \leqslant 3$ 时,停止迭代;否则重复步骤 2。

步骤 4:Alice 把锁定的待删除比特信息发送给 Bob,Bob 对密钥信息进行修正。

当 Alice、Bob 进行 Cascade 协商时,利用回溯、截止二分协商方案,同时记录待删除比特的位置信息。当协商完成以后去掉密钥序列中的待删除比特。

3　仿真与结果分析

对原始 Cascade 与改进的 Cascade 协商方案进行了仿真比较。文献[6,16]把在公共信道上交换的比特数与密钥长度的比值作为统计的协商效率。然而,实际上根据交换的校验值可以确定部分密钥信息,以搜索范围是 6 个比特为例,首先需要 1 比特校验值判断该区间内含有错误比特,然后 Alice、Bob 比较前 3 个比特的校验值,若相同,则把搜索范围确定在后 3 个比特中,尽管继续使用二分法纠错需要 2 个比特校验值,但实际上此时后 3 个比特已经全部泄露了,若只统计交换的比特数则少统计了一个比特的泄露信息。文中统计协商效率时,以公共信道上交换的比特数与窃听

万方数据

者根据校验值可确定的密钥数之和为泄露的密钥长度,该长度与密钥总长度的比值为协商效率。

在协商之前,为了达到错误比特随机分布的目的,Alice、Bob 同步打乱密钥序列的顺序。仿真参数设定如下:步骤 i 的分组长度设定为 $k_i = 2k_{i-1}$, $k_1 = 0.73/p$, p 为误比特率 BER,密钥长度 N = 10 000,仿真结果为 20 000 次实验的平均值。

协商效率比较见图 3。

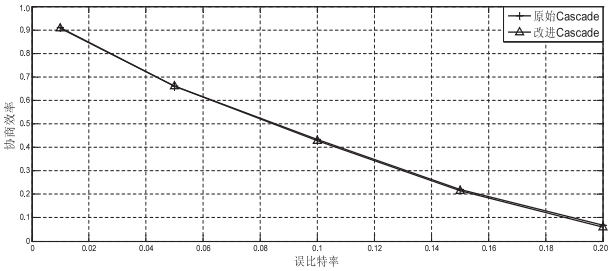

图 3 协商效率比较

由图 3 可知,改进的 Cascade 协商效率与原始 Cascade 协商效率基本一样,并无明显差距。这主要是因为当搜索长度锁定到 3 以下时,若继续利用二分法进行搜索会泄露 2 ~ 3 个校验比特的信息,从而导致该部分的密钥全部泄露出去;而在截止二分协商中,当分组长度小于等于 3 时,不再搜索错误比特的位置,而是把这些比特作为待删除的比特信息直接发送给对方,同样泄露了比特信息。因此改进的 Cascade 协商效率基本与原始 Cascade 相同。

交互次数比较见图 4。

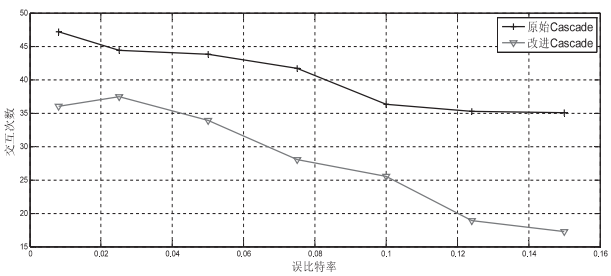

图 4 交互次数比较

由图 4 可知,与原始 Cascade 协商方案相比较,改进 Cascade 协商方案的交互次数明显下降。Cascade 协商过程中,回溯过程会使 Alice、Bob 之间的交互次数出现大幅度的增加。而在改进的 Cascade 协商方案中,采用截止二分协商,当错误比特所在位置锁定到 3 个比特时,不再继续二分查询,从而降低了 Alice、Bob 之间的交互次数。

4 结束语

Cascade 是经典的密钥协商方案,由于该方案需要 Alice、Bob 之间不断交互信息,从而导致 Cascade 协商对网络延迟等较为敏感。文中提出了 Cascade 的一种改进方案。仿真结果表明,改进方案保证了高效率协商,同时降低了 Alice、Bob 之间的交互次数。

万方数据

参考文献:

[1] Hao Z, Zhong S, Li L. Towards wireless security without computational assumptions-an oblivious transfer protocol based on an unauthenticated wireless channel [C]//Proceedings of IEEE. Shanghai: IEEE, 2011: 2156-2164.

[2] 李古月,胡爱群,石 乐. 无线信道的密钥生成方法[J]. 密码学报,2014,1(3):211-224.

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

[4] Cachin C, Maurer U. Linking information reconciliation and privacy amplification[J]. Journal of Cryptology, 1997, 10(2): 97-110.

[5] Ye C X, Mathur S, Reznik A, et al. Information-theoretically secret key generation for fading wireless channels[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(2): 240-254.

[6] Brassard G, Salvail L. Secret key reconciliation by public discussion[C]//Workshop on the theory and application of cryptographic techniques. [s. l.]: [s. n.], 1994: 410-423.

[7] Premnath S N, Jana S, Croft J, et al. Secret key extraction from wireless signal strength in real environments[J]. IEEE Transactions on Mobile Computing, 2013, 12(5): 917-930.

[8] Bennett C, Bessette G, Salvail L, et al. Experimental quantum cryptography[J]. Journal of Cryptology, 1992, 5(1): 3-28.

[9] 徐 津,温巧燕,王大印. 一种基于 Hash 函数和分组密码的消息认证码[J]. 计算机学报,2015,38(4):793-803.

[10] 王张宜,李 波,张焕国. Hash 函数的安全性研究[J]. 计算机工程与应用,2005,41(12):18-19.

[11] 张晓梅. 概率统计在密码学中的 Hash 函数中的应用[J]. 中国高新技术企业,2010(22):56-58.

[12] Martinez-Mateo J, Elkouss D, Martin V. Key reconciliation for high performance quantum key distribution[R]. [s. l.]: [s. n.], 2013.

[13] Zhao F, Fu M X, Wang F Q, et al. Error reconciliation for practical quantum cryptography[J]. Optik-International Journal for Light and Electron Optics, 2007, 118(10): 502-506.

[14] Buttler W T, Lamoreaux S K, Torgerson J R, et al. Fast, efficient error reconciliation for quantum cryptography[J]. Physical Review A, 2003, 67(5): 052303.

[15] Pearson D. High-speed QKD reconciliation using forward error correction[C]//Proceedings of 7th international conference on quantum communication, measurement and computing. Glasgow: [s. n.], 2004: 299-302.

[16] Yan H, Ren T, Peng X, et al. Information reconciliation protocol in quantum key distribution system[C]//IEEE fourth international conference on natural computation. Jinan: IEEE, 2008: 637-641.