一种新的信息理论安全信道模型

王保仓[1,2] 刘 辉[2] 胡予濮[2]
(西京学院 西安 710123)[1]
(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)[2]

摘 要 卫星信道模型是实现无条件安全的实用的模型之一,然而该模型却存在接收同步、通信成本高等缺点。为克服这些缺点,提出了虚拟卫星信道模型。该模型使用虚拟二元对称信道来实现对卫星信道的模拟,并仅使用比特异或运算来完成密钥协商的初始化过程,因此具有易实现、易同步、花费小、效率高等优点。证明了在虚拟卫星信道模型中,窃听者具有更大的接收信道误比特率。

关键词 密码学,无条件安全,密钥协商,卫星信道模型,初始化
中图法分类号 TN918.1 **文献标识码** A

New Information-theoretic Security Channel Model

WANG Bao-cang[1,2] LIU Hui[2] HU Yu-pu[2]
(Xijing University, Xi'an 710123, China)[1]
(Key Laboratory of Computer Networks & Information Security, Ministry of Education, Xidian University, Xi'an 710071, China)[2]

Abstract The satellite broadcasting channel model is one of the practical models to realize unconditional security. However, the satellite scenario suffers from some drawbacks such as the receiving synchronization and high communication costs. To overcome these drawbacks, a virtual satellite broadcasting channel model was proposed. The proposed model uses virtual binary symmetric channels to simulate a satellite model. The model only uses XOR operations to perform the initialization process of the secret-key agreement. Therefore, the proposed model is efficient, and easy to implement, to synchronize, and has lower communication costs. It was proven that in the proposed model, the wiretapper has a larger receiving bit-error probability.

Keywords Cryptography, Unconditional security, Secret-key agreement, Satellite scenario, Initialization

无条件安全或信息理论安全[1]指的是如果一个密码体制即使在敌人拥有无限的计算资源和计算能力的情况下仍然不能被破解,就称该密码体制是无条件安全的。无条件安全可以采用一次一密体制实现。一次一密体制所使用的密钥,其长度不能小于明文的长度[2],因此获取共享密钥流是实现无条件安全的关键。目前通过量子密钥协商[3]和基于公开讨论的密钥协商[4]来获取共享的密钥。

基于公开讨论的密钥协商,初始化阶段需要使用卫星信道模型来完成。而卫星广播信道模型中存在需同步、通信成本高等缺陷。为克服卫星广播信道模型中的上述缺陷,提出了虚拟卫星广播信道模型,证明了该模型和卫星广播信道模型在功能上是等价的,指出该模型不存在接收同步的问题,而且易于软件实现,通信成本低。

1 基于公开讨论的密钥协商

卫星广播信道模型[4]如图1所示。基于公开讨论的信息理论安全密钥协商[4]的一般过程叙述如下。

初始化阶段(Initialization Stage):通信双方 Alice,Bob 及窃听方 Eve 分别通过误比特率为 p_A,p_B 和 p_E 的有扰信道接收卫星发射的低功率信号或者都接收远太空的电波信号,记作比特串 P。由于噪声的存在,Alice,Bob 及窃听方 Eve 接收到的是随机信号 P 的衰落版本,记作比特串 X,Y 及 Z,X,Y 和 Z 分别作为 Alice,Bob 及 Eve 的初始信息。

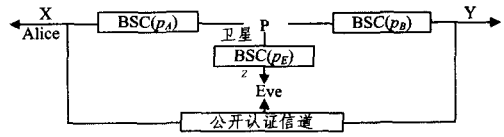

图1 卫星广播信道模型

通信阶段(Communication Stage):Alice 和 Bob 通过公开信道(认证的[5]或者是非认证的[6])公开地交换信息,这一过程称为公开讨论(public discussion),它可以分为如下3个阶段。

优先提取(Advantage Distillation)[7,8]:Alice 和 Bob 通过交换信息 U,Alice 从 X 和 U 得到一个新的随机比特串 X_A,

到稿日期:2009-03-06 返修日期:2009-05-20 本文受国家自然科学基金(60803149),国家973计划(2007CB311201)及111计划(B08038)资助。

王保仓(1979—),男,博士,副教授,主要研究方向为密码学与数论,E-mail:bcwang79@yahoo.com.cn;刘 辉(1979—),男,博士生,助教,主要研究方向为密码学等;胡予濮(1956—),男,博士,教授,博士生导师,主要研究方向为密码学与信息安全等。

同样，Bob 根据 Y 和 U 可以获得一个新的随机比特串 Y_B。优先提取阶段的最终结果是要使 Bob 比 Eve 拥有更多的关于 Alice 的比特串 X_A 的信息，或者是使 Alice 比 Eve 拥有更多的关于 Bob 的比特串 Y_B 的信息。

信息协调(Information Reconciliation)[9,10]：通信双方 Alice 和 Bob通过公开信道交换冗余信息，从而消除他们的比特串中不一致的比特。把冗余信息记作 V，Alice 和 Bob 分别根据 V 以及在优先提取阶段所获取的随机变量 X_A 和 Y_B 协商出一个共同的比特串 S。在信息协调阶段还必须使 Eve 对比特串 S 仍然有一定程度的不确定性。

保密增强(Privacy Amplification)[11,12]：Alice 和 Bob 从一个部分保密的比特串 S 产生一个高度保密的比特串 S'，而且使 Eve 对比特串 S' 几乎一无所知。可以通过选取合适的杂凑函数来实现保密增强：Alice 选定一个杂凑函数 G 并通过公开信道把它发送给 Bob。通信双方计算 $S'=G(S)$ 并把 S' 作为协商出来的共享密钥，希望此时 Eve 对比特串 S' 几乎一无所知。

决策阶段(Decision Stage)：如果 Alice 和 Bob 觉得 S' 可以作为共享的密钥，则他们就接受密钥协商协议执行的结果，否则他们就丢弃 S' 并且重新进行密钥协商。

须注意，窃听方可能会拥有比合法的通信方更好的接收信道，因此窃听者的接收信号可以比合法的通信双方更忠实于原始信号。合法的通信双方在公开讨论过程中，窃听者可以窃听到公开讨论的全部内容，但是在公开认证信道中，窃听方不能对公开讨论的内容进行篡改。文献[4]中证明，如果通信双方所拥有的信息毫不相关的话，那么无条件安全密钥协商的速率为零，即不可能实现无条件安全的密钥协商。因此，密钥协商总有一个初始化阶段来产生通信双方间的相关信息：借助于量子信道得到量子传输，或借助于有扰信道(如卫星广播信道)来接收广播信息。如果通信双方使用量子信道进行密钥协商的话，则无需优先提取。

在 Maurer 的卫星广播信道模型中，存在以下几个问题：

1)接收同步的问题；

2)在进行密钥协商的过程中，通信双方必须对窃听方所使用的接收信道的误比特率有一个保守估计。而实际上，通信双方一般情况下对窃听方是一无所知的。

通信收发双方需要接收卫星信号的设备，因此通信成本高。

2 虚拟卫星广播信道模型

2.1 模型描述

分析 Maurer 的信息理论安全卫星广播信道模型不难发现，卫星广播信道模型就是借助接收信道中的噪声加大窃听方对原始信号的不确定性。换言之，合法的通信双方和窃听方都通过各自的接收信道获得原始卫星广播信号的衰落版本。而事实上，Alice 和 Bob 可以人为地为通信信号加入噪声，从而实现对 Eve 所掌握的信息进行退化。根据这些考虑，提出了图 2 所示的虚拟卫星广播信道模型。其基本思想是，通信双方 Alice 和 Bob 分别独立地随机选择比特串 A 和 B，Alice 让 A 通过一个虚拟的误比特率为 $0<\varepsilon<1/2$ 的二元对称信道并把信道输出的结果 A^* 通过公开认证信道(PAC)传送给 Bob，Bob 让 B 通过一个虚拟的误比特率为 $0<\delta<1/2$ 的二元对称信道并把信道输出的结果 B^* 通过公开信道传送给 Alice。Alice 和 Bob 所使用的虚拟二元对称信道是保密的，别人无法访问。因此，Eve 只能获取 A 和 B 的衰落版本 A^* 和 B^*。Alice 和 Bob 分别计算 $A\oplus B^*$ 和 $B\oplus A^*$ 并将其作为他们的初始化密钥，而窃听方 Eve 可以根据在公开认证信道上窃听到的 A^* 和 B^* 计算 $A^*\oplus B^*$，此处⊕表示比特串的逐比特异或运算。

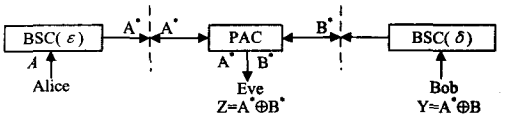

图 2 虚拟卫星广播信道模型

下一节将说明本文的虚拟卫星广播信道模型和卫星广播信道模型在功能上是等价的，并对虚拟卫星广播信道模型进行分析。

2.2 模型分析

卫星广播信道模型的目的就是实现基于公开讨论的密钥协商的初始化阶段，即让通信双方 Alice 和 Bob 分别接收到一个比特串 X 和 Y。X 和 Y 与原始卫星信号 P 之间存在一定的误比特率，而窃听方 Eve 也可以通过窃听获得原始卫星信号 P 的退化版本 Z。本文的虚拟卫星信道模型和卫星广播信道模型在功能上是等价的，如图 3 所示。

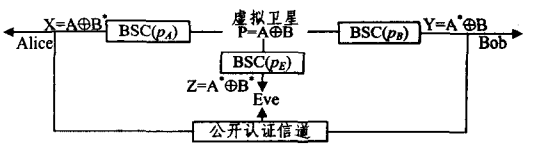

图 3 虚拟卫星广播信道模型与卫星广播信道模型的等价性

在虚拟卫星广播信道模型中，可以把 $P=A\oplus B$ 看作原始卫星信号，而 $X=A\oplus B^*$，$Y=A^*\oplus B$，$Z=A^*\oplus B^*$ 分别视为通信双方 Alice 和 Bob 以及窃听方 Eve 接收到的原始卫星信号 P 的衰落版本。下面分析 Alice 和 Bob 以及窃听方 Eve 接收信道的误比特率 p_A，p_B，p_E。注意到 A^* 和 B^* 分别是 A 和 B 通过误比特率为 ε 和 δ 的二元对称信道的输出结果，因此有

$$Pr(A^*\neq A)=\varepsilon, Pr(B^*\neq B)=\delta$$

容易计算

$$p_A=Pr(X\neq P)=Pr(A\oplus B^*\neq A\oplus B)=Pr(B^*\neq B)=\delta$$

$$p_B=Pr(Y\neq P)=Pr(A^*\oplus B\neq A\oplus B)=Pr(A^*\neq A)=\varepsilon$$

$$\begin{aligned}p_E&=Pr(Z\neq P)=Pr(A^*\oplus B^*\neq A\oplus B)\\&=Pr[(A^*\neq A)\wedge(B^*=B)]+Pr[(A^*=A)\wedge(B^*\neq B)]\\&=Pr(A^*\neq A)\times Pr(B^*=B)+Pr(A^*=A)\times Pr(B^*\neq B)\\&=\delta(1-\varepsilon)+\varepsilon(1-\delta)=\varepsilon+\delta-2\varepsilon\delta\end{aligned}$$

再注意到

$$0<p_E=\varepsilon+\delta(1-2\varepsilon)<\varepsilon+\frac{1-2\varepsilon}{2}=\frac{1}{2}$$

因此，在虚拟卫星广播信道模型中，通信双方及窃听方分别通过误比特率为 $0<p_A, p_B, p_E<1/2$ 的虚拟二元对称信道接收原始虚拟卫星信号 P，接收到的衰落比特串 X,Y,Z 就是基于公开讨论的密钥协商中通信双方和窃听方的初始比特

(下转第 119 页)

参 考 文 献

[1] 陈飞翔,周治武,张建兵. 基于动态规划算法的矢量数据压缩改进算法[J]. 计算机应用,2008,28(2):168-170

[2] 赵锴,李建中,骆吉洲. 基于谓词索引的海量数据压缩存储及数据操作算法[J]. 计算机科学,2005,32(9):86-90

[3] 陈艳拢. 等值线数据压缩算法研究[J]. 大连理工大学学报,2005(10):18-19

[4] 关宗安,仲丛久. 数据加密标准算法的 DSP 实现[J]. 数据采集与处理,2006,21(12):266-268

[5] Schneier B. 应用密码学[M]. 吴世忠,祝世雄,译. 北京:机械工业出版社,2001

[6] Ahlswede R,Cai N,Li S R,et al. Network information flow[J]. IEEE Trans. On Information Theory,2000,46(4):1204-1216

[7] Ho T,Karger D R,Medard M,et al. The benefits of coding over routing in a randomized setting[A] // Hideki I,eds. The 2003 IEEE International Symposium on Information Theory[C]. San Jose:IEEE Press,2003:442-447

[8] Jaggi S,Sanders P,Chou P A,et al. Polynomial time algorithms for multicast network code construction[J]. IEEE Transactions on Information Theory,2003,49:831- 836

[9] Chou P A,Wu Y,Jain K. Practical network coding[A] // Proceedings of 41st Allerton Conference on Communication,Control and Computing[C]. Allerton:Monticello House,2003:473-482

[10] 吴景裕. 浅谈图书馆数字化建设中数据恢复[J]. 情报探索,2007(12):53-55

(上接第 98 页)

串。因此,虚拟卫星广播信道模型和 Maurer 的卫星广播信道模型在功能上是等价的。

2.3 模型比较

对虚拟卫星广播信道模型与卫星广播信道模型做如下方面的比较。

接收同步问题:虚拟卫星广播信道模型不存在接收同步问题。而卫星广播信道模型中通信双方为实现同步接收,须在初始化阶段之前至少通信一次,以协调同步接收的问题。

误比特率比较:一般来说,在卫星广播信道模型中,合法的通信双方对窃听方知之甚少。在密钥协商阶段,通信双方需要对窃听方接收信道的误比特率有一个保守的估计。而在虚拟卫星广播信道模型中,通信双方不仅可以计算出窃听方接收信道的误比特率 $p_E=\varepsilon+\delta-2\varepsilon\delta$,而且完全掌握了窃听方接收到的比特串 $Z=A^*\oplus B^*$。如果再注意到,

$$p_E=\delta+\varepsilon(1-2\delta)>\delta=p_A,\ p_E=\varepsilon+\delta(1-2\varepsilon)>\varepsilon=p_B$$

则可以断定,在虚拟卫星广播信道模型中,窃听方的接收信道的误比特率 p_E 要大于合法通信双方的接收信道的误比特率 p_A,p_B。这样,Alice 和 Bob 就赢得了优势。

通信成本:较之虚拟卫星广播信道模型,在卫星广播信道模型中,通信双方除了要为协调同步接收而多进行至少一次通信外,还需要新信号的接收设备。在虚拟卫星广播信道模型中,虽然也使用了虚拟二元对称信道,但实际上通信双方的虚拟二元对称信道完全可以通过软件模拟来实现。换言之,通信双方分别随机选取比特串 A 和 B,然后根据选定的误比特率 ε 和 δ 来随机地改变 A 和 B 中某些比特的值,所得到的比特串 A^* 和 B^* 就是 A 和 B 通过误比特率为 ε 和 δ 的虚拟二元对称信道的输出结果。因此,本文给出的虚拟卫星广播信道模型易于软件实现。

综上所述,本文的模型较之卫星广播信道模型具有无需同步、易于控制窃听方接收信道的误比特率、通信成本低、易于软件实现等优点。

结束语 针对信息理论安全卫星广播信道模型中存在的一些缺陷,给出了虚拟卫星广播信道模型。模型无需同步,且通信成本低,易于软件实现,可以人为地对窃听方的初始信息进行控制等。一方面,在卫星广播信道模型中的优先提取、信息协调和保密增强协议可以原封不动地移植到虚拟卫星广播信道模型中;另一方面,虚拟卫星广播信道模型比卫星广播信道模型具有诸多优点。因此,如何根据这些优点设计在虚拟卫星广播信道模型中更为高效的优先提取、信息协调和保密增强协议,则属于将来需要进一步研究的工作。

参 考 文 献

[1] Maurer U. Information-theoretic cryptography[C] // Advances in Cryptology-CRYPTO'99. LNCS 1666. Berlin:Springer-Verlag,1999:47-64

[2] Shannon C E. Communication theory of secrecy systems[J]. Bell System Technical Journal,1949,28:656-715

[3] Zhao Yi-bo,Gui You-zhen,Chen Jin-jian,et al. Computational complexity of continuous variable quantum key distribution[J]. IEEE Trans. on Information Theory,2008,54(6):2803-2807

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

[5] 王保仓. 基于有扰认证信道的信息理论安全密钥协商[D]. 西安:西安电子科技大学,2004

[6] Maurer U. Information - theoretically secure secret - key agreement by not authenticated public discussion[C] // Advances in Cryptology-EUROCRYPT'97. LNCS 1233. Berlin: Springer-Verlag,1997:209-225

[7] Jones N S,Masanes L. Key distillation and the secret-bit fraction [J]. IEEE Trans. on Information Theory,2008,54(2):680-691

[8] Maurer U. Protocols for secret key agreement based on common information[C] // Advances in Cryptology-CRYPTO'92. LNCS 740. Berlin:Springer-Verlag,1993:461-470

[9] Yan Hao,Ren Tienan,Peng Xiang,et al. Information reconciliation protocol in quantum key distribution system[C] // The Fourth International Conference on Natural Computation-ICNC'08. Jinan,China,Oct. 2008,3:637-641

[10] 王保仓,杨波,胡予濮. 一种新的信息协调协议[J]. 西安电子科技大学学报,2006,33(3):486-490

[11] Watanabe Y. Privacy amplification for quantum key distribution [J]. Journal of Physics A:Mathematical and Theoretical,2007,40(3):99-104

[12] Liu Shengli,Wang Yumin. Privacy amplification against active attacks with strong robustness[J]. Electron. Lett.,1999,35(9):712-713