



中国北斗卫星导航系统对全球 PNT 用户的贡献

杨元喜^①, 李金龙^②, 徐君毅^②, 汤静^①, 郭海荣^③, 何海波^③

① 中国卫星导航定位与应用管理中心, 北京 100088;

② 信息工程大学测绘学院, 郑州 450052;

③ 北京环球信息应用开发中心, 北京 100094

E-mail: yuanxi_yang@163.com

2011-04-06 收稿, 2011-06-03 接受

国家自然科学基金(41020144004, 40841021)和国家高技术研究发展计划(2007AA12Z331)资助项目

摘要 北斗卫星导航系统作为全球四大卫星导航系统之一, 不仅增加中国及周边地区定位、导航和授时(PNT=Positioning, Navigation and Timing)用户的卫星可见性和可用性, 而且也将提高全球用户的 PNT 精度. 在全球导航卫星系统(GNSS)兼容与互操作条件下, 分析全球导航定位定时用户的卫星可见性和精度衰减因子改善情况; 利用仿真数据分析北斗卫星导航系统对全球用户的贡献, 侧重分析北斗卫星导航系统与 GPS, GLONASS 和 Galileo 多卫星导航系统组合模式下用户获得的收益.

关键词

北斗卫星导航系统
定位
导航
授时
精度衰减因子
卫星可见性

全球导航卫星系统 GNSS(Global Navigation Satellite System)正呈现百花齐放的局面. 美国 GPS(Global Positioning System)、俄罗斯的 GLO-NASS(GLObal NAVigation Satellite System, 与 GNSS 取至相同的英文单词)、欧盟伽利略系统(Galileo)、中国北斗系统(Beidou/Compass)、日本准天顶卫星系统(QZSS)以及印度的区域导航卫星系统(IRNSS)等, 使卫星导航星空群星璀璨, 卫星导航用户的可用信号资源极大丰富. 2020年后, 天空将有 30 颗 GPS 卫星(3 个频率信号), 24 颗 GLONASS 卫星(3 个频率信号), 30 颗 Galileo 卫星(4 个频率信号), 35 颗 Compass/北斗卫星(3 个频率信号), 3 颗 QZSS 卫星(4 个频率信号)和 7 颗 IRNSS 卫星(2 个频率信号)^[1~3]. 全球用户可以无限制地使用多星座提供的多频观测信息进行定位、导航、定时(PNT)应用, 可减弱对单一星座的依赖, 降低电磁干扰、地形/建筑物遮挡、电离层闪烁、拒绝服务等因素导致的性能下降或服务中断风险.

在 GNSS 多星座多频数据融合下, 经过数据探测、筛选、组合, 将显著增加卫星和测距信号的数量, 大幅提升各个导航性能指标. 其主要优点如下^[4]: (1)

可见卫星数目增多, 可减小精度衰减因子(DOP), 提高导航精度(accuracy); (2) 各卫星系统具有不同的时间系统差和坐标系统差及轨道系统差, 通过多卫星系统信号融合, 可补偿单一导航系统的系统误差影响, 进而精化各星座的卫星轨道、卫星钟差以及监测站坐标, 提高导航卫星系统及用户 PNT 的可靠性(reliability); (3) 多频率信号的综合利用可有效解决非故意干扰问题, 减弱某单一卫星系统出现重大故障或拒绝服务等带来的隐忧, 提高导航的可用性(availability); (4) 观测冗余信息增多, 便于故障诊断、报警和隔离, 提高卫星导航用户的完好性(integrity); (5) 多卫星观测几何结构的改善, 有利于诊断因电离层闪烁、多径、遮挡而导致的观测异常, 提高用户系统的异常误差影响控制能力, 提高用户 PNT 的抗差性(robustness); (6) 卫星数目增多可极大地减弱卫星导航盲区, 缓解单一星座下卫星故障、地形/建筑物/树木遮蔽等因素引起的导航信号缺失问题, 提高卫星导航系统的连续性(continuity); (7) 综合利用多星座的多频信号, 能大幅缓解单一星座卫星信号随时间变化的有色噪声的影响, 提高动态

用户 PNT 的收敛性(convergence); (8) 多频率信号的使用更能消除或精确估计电离层延迟的影响; (9) 综合利用多星座多频信号, 可望实现载波相位模糊度的快速固定, 并在中长距离情况下也能可靠地确定模糊度, 提高对流层延迟参数估计的时间分辨率, 进而全方位提升高精度实时与近实时测量的性能; (10) 各星座卫星的高度、轨道面倾角不同, 可改善地球自转、极移等参数的估计精度。

为了分析 Compass 对用户 PNT 的贡献, 需要描述多卫星导航系统环境下, 相应的随机误差、系统误差的影响。其中, 精度衰减因子(DOP)是随机误差补偿和系统误差补偿能力以及可用性、完好性的重要指标。DOP 值反映的是测距信号统计量和位置参数统计量之间的误差传播关系^[5]。点位误差正是测距误差与水平精度衰减因子(HDOP)及垂直精度衰减因子(VDOP)的乘积^[6]。

本文采用仿真计算分析 Compass 的贡献。类似的研究分析工作已有大量成果^[7-10]。本文侧重讨论 Compass 对用户卫星可见性的改善, 用户 PNT 的 DOP 理论值改善, 并通过仿真计算分析 Compass 对全球用户的卫星可见数和精度衰减因子(DOP)的改善。

1 增加卫星星座对用户导航定位 DOP 值的贡献

精度衰减因子(DOP)被广泛用于分析导航精度和观测几何结构强度。关于精度衰减因子(DOP)的定义, 有许多文献可供参考^[5,6,11]。假定伪距观测量是 P_i , 则观测模型可写为

$$P_i = \rho_i + c(dt_u - dt_i) + I_i + T_i + e_i, \quad (1)$$

其中, ρ_i 是信号接收时刻接收机天线相位中心到信号发射时刻卫星天线相位中心间的几何距离, dt_u 和 dt_i 分别为接收机钟差和卫星钟差; I_i 和 T_i 分别为电离层延迟和对流层延迟; e_i 为观测噪声和未模型化误差, 如, 多路径效应等; c 是真空中光速。

进一步, 假定伪距观测量中的卫星钟差和大气层延迟已经得以改正, 在观测模型中只考虑接收机钟差。如此, 观测模型可表示成^[6]

$$\mathbf{L} = \mathbf{A}\mathbf{X} + \mathbf{e}, \quad (2)$$

其中, $\mathbf{L}$ 是观测向量, 该观测向量是改正后的伪距观测量与由坐标近似值计算的伪距之差。 $\mathbf{X}$ 是包含 3 维位置和接收机钟差(单位: m)在内的未知参数向量, $\mathbf{A}$ 是 $n \times 4$ 设计矩阵, 若考虑观测向量 $\mathbf{L}$ 的权矩阵 $\mathbf{P}$,

则未知参数向量的最小二乘解为

$$\hat{\mathbf{X}} = (\mathbf{A}^T \mathbf{P} \mathbf{A})^{-1} \mathbf{A}^T \mathbf{P} \mathbf{L} = \mathbf{Q}_{\hat{\mathbf{X}}} \mathbf{A}^T \mathbf{P} \mathbf{L}, \quad (3)$$

其中, $\mathbf{Q}_{\hat{\mathbf{X}}} = (\mathbf{A}^T \mathbf{P} \mathbf{A})^{-1}$ 。几何精度衰减因子(GDOP)定义为

$$\text{GDOP} = \sqrt{\text{tr}(\mathbf{Q}_{\hat{\mathbf{X}}})}. \quad (4)$$

水平精度衰减因子(HDOP)为^[5,11]

$$\text{HDOP} = \sqrt{q_{nn} + q_{ee}}. \quad (5)$$

垂直精度衰减因子(VDOP)为

$$\text{VDOP} = \sqrt{q_{uu}}. \quad (6)$$

时间精度衰减因子(TDOP)为

$$\text{TDOP} = \sqrt{q_{tt}}. \quad (7)$$

为了分析 Compass 对 PNT 用户的贡献, 先假设由其他卫星导航系统解得的未知参数向量 $\hat{\mathbf{X}}_0$ 的协因素矩阵为 $\mathbf{Q}_{\hat{\mathbf{X}}_0}$ 。而加入 Compass 信号后相应的观测方程变为

$$\begin{bmatrix} \mathbf{L} \\ \mathbf{L}_c \end{bmatrix} = \begin{bmatrix} \mathbf{A} \\ \mathbf{A}_c \end{bmatrix} \mathbf{X} + \begin{bmatrix} \mathbf{e} \\ \mathbf{e}_c \end{bmatrix}, \quad (8)$$

其中, $\mathbf{L}_c$ 和 $\mathbf{P}_c$ 分别为 Compass 的观测向量及其权矩阵, $\mathbf{A}_c$ 为 Compass 设计矩阵。从而加入 Compass 信号后未知参数向量 $\hat{\mathbf{X}}$ 的新协因素矩阵:

$$\begin{aligned} \mathbf{Q}_{\hat{\mathbf{X}}} &= \left(\begin{bmatrix} \mathbf{A}^T \\ \mathbf{A}_c^T \end{bmatrix} \begin{bmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{0} & \mathbf{P}_c \end{bmatrix} \begin{bmatrix} \mathbf{A} \\ \mathbf{A}_c \end{bmatrix} \right)^{-1} = (\mathbf{A}^T \mathbf{P} \mathbf{A} + \mathbf{A}_c^T \mathbf{P}_c \mathbf{A}_c)^{-1}, \\ &= \mathbf{Q}_{\hat{\mathbf{X}}_0} - \mathbf{Q}_{\hat{\mathbf{X}}_0} \mathbf{A}_c^T (\mathbf{Q}_c + \mathbf{A}_c \mathbf{Q}_{\hat{\mathbf{X}}_0} \mathbf{A}_c^T)^{-1} \mathbf{A}_c \mathbf{Q}_{\hat{\mathbf{X}}_0} \end{aligned} \quad (9)$$

其中, $\mathbf{Q}_{\hat{\mathbf{X}}_0} = (\mathbf{A}^T \mathbf{P} \mathbf{A})^{-1}$, $\mathbf{Q}_c = \mathbf{P}_c^{-1}$ 是 Compass 观测向量权矩阵的逆矩阵。则 PNT 参数的协因素矩阵的改善值为

$$\mathbf{Q}_{\hat{\mathbf{X}}_0} - \mathbf{Q}_{\hat{\mathbf{X}}} = \mathbf{Q}_{\hat{\mathbf{X}}_0} \mathbf{A}_c^T (\mathbf{Q}_c + \mathbf{A}_c \mathbf{Q}_{\hat{\mathbf{X}}_0} \mathbf{A}_c^T)^{-1} \mathbf{A}_c \mathbf{Q}_{\hat{\mathbf{X}}_0}. \quad (10)$$

精度衰减因子 DOP 的改善值为

$$\Delta \text{DOP} = \sqrt{\text{tr}(\mathbf{Q}_{\hat{\mathbf{X}}_0})} - \sqrt{\text{tr}(\mathbf{Q}_{\hat{\mathbf{X}}})}. \quad (11)$$

精度衰减因子 DOP 值的改善百分比为

$$\xi_{\text{DOP}} = \frac{\sqrt{\text{tr}(\mathbf{Q}_{\hat{\mathbf{X}}_0})} - \sqrt{\text{tr}(\mathbf{Q}_{\hat{\mathbf{X}}})}}{\sqrt{\text{tr}(\mathbf{Q}_{\hat{\mathbf{X}}_0})}}. \quad (12)$$

多模导航条件下, 需要考虑各系统之间的不兼容性, 主要有各系统坐标系统差和时间系统差, GPS 坐标系统 WGS-84、Galileo 坐标参考框架 GTRF 以及 Compass 坐标系统 CGCS2000 与国际地球参考框架

(ITRF)之间仅相差几个厘米,对于导航应用来说,它们之间的差别均可忽略^[1,12]. GLONASS 坐标系统 PZ-90 与 ITRF 略有差异,但许多组织已经求出了其与 WGS-84 的转换参数,对于米级精度的导航应用来说,只要顾及这些转换参数即可,无需在函数模型中增加待定的转换参数,于是不影响 DOP 值计算.

对时间系统差,一般采取以下两种处理方式^[1,13]: (1) 在导航电文中将各系统之间的时间系统差发播给用户^[14]; (2) 在参数估计时附加一个未知的时间系统差参数进行估计. 在仿真时,我们将分两种情况来计算 DOP 值,并分析 Compass 的贡献.

2 仿真计算与分析

本次仿真时间段为 2010 年 3 月 28 日 0 时~2010 年 3 月 29 日 0 时,共 24 h,采样率为 300 s. GPS 和 GLONASS 星座使用当天广播星历计算卫星位置,Compass 和 Galileo 星座采用表 1 所列开普勒轨道根数计算卫星位置. 仿真时间内,有 30 颗 GPS 卫星,21 颗 GLONASS 卫星,27 颗 Galileo 卫星和 35 颗 Compass 卫星.

Compass 星座 5 颗 GEO 卫星的轨道位置分别为 58.75°, 80°, 110.5°, 140°和 160°E. 3 颗 IGSO 的倾角为 55°,交叉点经度为 118°E. 计算分为 8 个方案:

- 方案一: GPS (G);
- 方案二: GPS+Compass (G+C);
- 方案三: GPS+GLONASS (G+R);
- 方案四: GPS+GLONASS+Compass (G+R+C);
- 方案五: GPS+Galileo (G+E);
- 方案六: GPS+Galileo+Compass (G+E+C);
- 方案七: GPS+GLONASS+Galileo (G+R+E);
- 方案八: GPS+GLONASS+Galileo+Compass (G+R+E+C).

括号内为各系统缩写,“G”代表 GPS,“R”代表俄罗斯的 GLONASS,“E”代表欧洲的 Galileo,“C”代表中国的 Compass,以下部分将使用这些缩写来表示各方案.

以经度间隔 5°,纬度间隔 2.5°,高程取为 25 m,计算了经度范围-180°~180°、纬度范围-90°~90°内高度截止角为 10°和 20°,30°和 40°时不同系统的卫星可见数以及在高度截止角为 10°时的卫星可见性(95%>)、DOP 值(95%<)、DOP 值的改善百分比,计算结果见表 2~7. 图 1~10 为考虑各时间系统差、高度截止角为 10°时各系统可见卫星数、可见卫星增加数及 DOP 值改善百分比空间分布图.

由计算结果可以看出:

(1) 比较表 2 中的方案 1 和方案 2 可见,当卫星截止高度角为 10°时,单卫星星座 GPS 基础上加入 Compass 后,全球平均可见卫星数从 7.3 增加为 17.1,增加约 134%;比较方案 3 和 4、方案 5 和 6 可见,在 GPS+GLONASS 和 GPS+Galileo 的基础上,加入

表 1 Compass 和 Galileo 星座参数^{a)}

	Compass	Galileo
a (km)	27878.1	29601.297
i (°)	55	56
e (°)	0	0
ω (°)	0	0
Ω (°)	0, 120, 240	60, 180, 300
M_0	每个轨道上的第一颗卫星在仿真起始时刻的平近点角分别为 0°, 15°, 30°, 其余卫星平近点角依次增加 45°, 此外 3 个轨道面上备用卫星的平近点角分别为 10°, 55°, 105°	每个轨道上的第一颗卫星在仿真起始时刻的平近点角分别为 0°, 15°, 30°, 其余卫星平近点角依次增加 40°

a) a 为卫星轨道的长半轴; i 为轨道倾角; e 为轨道离心率; ω 是轨道近地点角距; Ω 代表升交点赤经; M_0 为平近点角

表 2 不同高度截止角各方案的卫星可见性

	10°		20°		30°		40°	
	min-max	mean	min-max	mean	min-max	mean	min-max	mean
G	6~9	7.3	4~7	5.2	2~5	3.3	1~3	1.7
G+C	12~25	17.1	9~20	12.6	5~15	8.8	3~11	5.1
G+R	9~15	12.6	6~12	9.2	4~9	6.2	1~5	3.5
G+R+C	16~30	22.6	11~24	16.7	7~17	11.7	4~12	7.0
G+E	12~18	15.2	9~14	11.4	6~10	7.9	3~6	4.6
G+E+C	20~34	25.6	15~26	19.0	10~19	13.3	5~14	8.2
G+R+E	16~24	20.7	12~19	15.5	7~14	10.9	3~8	6.5
G+R+E+C	24~39	31.1	17~30	23.2	11~22	16.3	6~16	10.1

表 3 高度截止角为 10° 时各方案 DOP 值(考虑时间系统差)

	GDOP		PDOP		HDOP		VDOP	
	min-max	mean	min-max	mean	min-max	mean	min-max	mean
G	2.33~4.59	3.43	2.06~3.90	2.96	0.90~2.17	1.33	1.77~3.57	2.67
G+C	1.27~2.36	1.84	1.04~2.02	1.52	0.54~0.97	0.72	0.90~1.90	1.35
G+R	1.85~2.95	2.25	1.55~2.43	1.87	0.71~1.16	0.87	1.34~2.13	1.67
G+R+C	1.30~2.03	1.67	0.94~1.59	1.26	0.49~0.78	0.60	0.81~1.49	1.12
G+E	1.62~2.47	1.99	1.34~2.03	1.65	0.60~0.94	0.76	1.18~1.84	1.48
G+E+C	1.22~1.91	1.57	0.90~1.48	1.18	0.45~0.68	0.55	0.78~1.39	1.05
G+R+E	1.51~2.05	1.75	1.16~1.58	1.34	0.52~0.81	0.64	0.99~1.39	1.19
G+R+E+C	1.30~1.79	1.54	0.84~1.26	1.05	0.42~0.60	0.49	0.72~1.17	0.93

表 4 高度截止角为 10° 时各方案 DOP 值(不考虑时间系统差)

	GDOP		PDOP		HDOP		VDOP	
	min-max	mean	min-max	mean	min-max	mean	min-max	mean
G	2.33~5.59	3.43	2.06~3.90	2.96	0.90~2.17	1.33	1.77~3.57	2.67
G+C	1.16~2.29	1.71	1.02~2.02	1.49	0.53~0.94	0.70	0.87~1.89	1.33
G+R	1.69~2.57	2.07	1.50~2.15	1.80	0.69~1.13	0.85	1.29~1.94	1.60
G+R+C	1.04~1.70	1.39	0.92~1.48	1.22	0.48~0.76	0.59	0.79~1.39	1.07
G+E	1.50~2.32	1.85	1.33~1.98	1.61	0.60~0.93	0.75	1.16~1.83	1.44
G+E+C	0.98~1.64	1.31	0.88~1.45	1.15	0.45~0.66	0.54	0.75~1.37	1.02
G+R+E	1.27~1.71	1.48	1.13~1.46	1.29	0.52~0.78	0.62	0.97~1.34	1.14
G+R+E+C	0.91~1.37	1.15	0.81~1.21	1.01	0.42~0.58	0.48	0.70~1.11	0.89

表 5 高度截止角为 10° 时 Compass 对不同系统 DOP 值改善百分比(考虑时间系统差)

	GDOP		PDOP		HDOP		VDOP	
	min-max	mean	min-max	mean	min-max	mean	min-max	mean
G	28.6~66.5	46.1	32.4~68.2	48.5	27.1~69.2	45.3	31.5~69.1	49.1
G+R	14.3~45.4	25.6	21.0~51.4	32.4	20.7~44.9	30.7	19.9~52.6	33.0
G+E	11.0~36.8	21.1	17.5~46.0	28.3	17.5~40.7	27.6	17.5~47.7	28.7
G+R+E	3.1~25.4	11.6	13.2~35.7	22.0	14.3~34.3	22.3	12.2~38.1	22.2

表 6 高度截止角为 10° 时 Compass 对不同系统 DOP 值改善百分比(只考虑 Compass 时间系统差)

	GDOP		PDOP		HDOP		VDOP	
	min-max	mean	min-max	mean	min-max	mean	min-max	mean
G	28.6~66.5	46.1	32.4~68.2	48.5	27.1~69.2	45.3	31.5~69.1	49.1
G+R	14.8~44.6	27.5	18.2~48.0	31.1	19.7~44.1	29.9	16.0~51.4	31.6
G+E	12.8~41.7	23.8	18.0~45.7	27.7	17.7~41.1	27.3	17.1~46.4	28.0
G+R+E	6.5~32.5	16.2	10.4~34.6	21.0	14.3~33.8	21.7	9.8~36.0	21.2

表 7 高度截止角为 10° 时 Compass 对不同系统 DOP 值改善百分比(不考虑时间系统差)

	GDOP		PDOP		HDOP		VDOP	
	min-max	mean	min-max	mean	min-max	mean	min-max	mean
G	32.8~70.3	50.1	32.9~68.7	49.5	27.1~69.7	46.3	32.0~69.6	50.1
G+R	18.0~48.7	32.7	18.2~49.0	32.3	20.9~46.9	31.0	18.0~52.5	32.8
G+E	18.1~48.3	29.5	18.2~47.3	29.0	18.0~42.2	28.1	17.1~49.4	29.5
G+R+E	11.1~37.7	22.6	10.4~36.4	22.2	14.3~35.6	22.5	9.76~36.8	22.5

图 1 高度截止角为 10° 时方案 8 的卫星可见数分布

图 2 方案 8 相对于方案 7 的可见卫星增加数空间分布

图 3 方案 2 相对于方案 1 的 GDOP 值改善百分比

图 4 方案 2 相对于方案 1 的 PDOP 值改善百分比

图 5 方案 4 相对于方案 3 的 GDOP 值改善百分比

图 6 方案 4 相对于方案 3 的 PDOP 值改善百分比

图 7 方案 6 相对于方案 5 的 GDOP 值改善百分比

图 8 方案 6 相对于方案 5 的 PDOP 值改善百分比

图9 方案8相对于方案7的GDOP值改善百分比

Compass后,可见卫星数分别增加约79%和68%;即使在GPS+GLONASS+Galileo基础上,加入Compass后,可见卫星数也从20.7增加到31.1,增加约50%。可见卫星数的增加,将极大改善卫星的几何分布,改善PNT服务的连续性。

(2) 从表5~7可见,Compass对不同系统GDOP值的改善百分比随着各系统兼容性的增强而增大。若所有导航星座信号完全兼容(即各系统间无系统误差)(表7),则在GPS星座的基础上,增加Compass后对全球地区GDOP值改善约为50%;在GPS与GLONASS共同使用的基础上,加入Compass后GDOP值改善约32.7%;在GPS与Galileo共同使用的基础上,加入Compass后对GDOP值改善约29.5%;即使在GPS, GLONASS和Galileo同时使用的基础上,加入Compass后, GDOP值依然能改善约22.6%。各系统兼容性的加强将获得GDOP值的改善,进而改善PNT的精确性。

(3) 从表5~7可见,不管是否考虑各系统时间差,在GPS星座的基础上,增加Compass后对PDOP值改善为49%左右;在GPS与GLONASS共同使用的基础上,加入Compass后对PDOP值改善为32%左右;

图10 方案8相对于方案7的PDOP值改善百分比

在GPS与Galileo共同使用的基础上,加入Compass后对PDOP值改善为28%左右;即使在GPS, GLONASS和Galileo同时使用的基础上,加入Compass后,PDOP值依然能改善22%左右。PDOP值的改善将提高用户导航定位的精确性,进而提高系统服务的可用性。

(4) 对于一些受遮挡较为严重的地区,如高楼林立的城市街道,单一系统的卫星数较少,且几何分布也较差。当卫星高度角达到 40° 时,单一系统在大多数时段卫星数达不到4颗,将给用户应用带来不便,而4个系统同时使用时,可见卫星数将平均达到10.1颗,因此,多个导航系统的共同使用,将显著提高导航定位服务的可用性。

最后必须指出,当卫星星座兼容性较差时,GNSS数据融合时需要增加过多兼容性补偿参数,此时,增加卫星星座也不会明显改善GDOP值;此外,当各类导航卫星观测之间具有不同的随机模型,不同的观测权,则分析各类卫星的贡献时不能简单通过等权DOP值计算,实践中可采用方差分量估计实时标定各类卫星观测的权,并计算具有不等权的DOP值,这类问题将另文讨论。

参考文献

- 1 Hofmann-Wellenhof B, Lichtenegger H, Wasle E, 著. 程鹏飞, 蔡艳辉, 文汉江, 等, 译. 全球卫星导航系统 GPS, GLONASS, Galileo 及其他系统. 北京: 测绘出版社, 2009
- 2 陈忠贵, 帅平, 曲广吉. 现代卫星导航系统技术特点与发展趋势分析. 中国科学 E 辑: 技术科学, 2009, 39: 686-695
- 3 陈俊勇. GPS 技术进展及其现代化. 大地测量与地球动力学, 2010, 30: 1-4
- 4 杨元喜. 北斗卫星导航系统的进展、贡献与挑战. 测绘学报, 2010, 39: 1-6
- 5 Milbert D. Improving dilution of precision, a companion measure of systematic effects. GPS World, 2009, 20: 38-47
- 6 Langley R B. Dilution of precision. GPS World, 1999, 10: 52-59
- 7 赵春梅, 欧吉坤, 袁运斌. 基于单点定位模型的 GALILEO 及 GPS-GALILEO 组合系统的定位精度和可靠性的仿真分析. 科学通报, 2005, 50: 811-819
- 8 蔡孟伦. 未来全球导航卫星系统于台湾地区效能分析. 硕士学位论文. 台湾: 成功大学, 2008

- 9 Huang Y S, Tsai M L. The impact of Compass/Beidou-2 on future GNSS: A perspective from Asia. In: ION GNSS 21st International Technical Meeting of the Satellite Division, 2008. 2227–2238
- 10 庄新彦, 赵晓东, 谭述森, 等. Compass 系统与 GPS 系统 L1 频段信号干扰仿真分析. 测绘科学技术学报, 2009, 26: 216–219
- 11 Milbert D. Dilution of precision. J Inst Navi, 2008, 55: 67–81
- 12 杨元喜. 2000 中国大地坐标系. 科学通报, 2009, 54: 2271–2276
- 13 Kaplan D, Hegarty C J, 著. 寇艳红, 译. GPS 原理与应用(第 2 版). 北京: 电子工业出版社, 2007
- 14 Hahn J, Powers E. GPS and Galileo timing interoperability. In: Proc. of GNSS 2004, Rotterdam, the Netherlands, 2004

· 动态 ·

一种定量分析量子秘密共享方案安全性的新方法

由于量子加密的无条件安全性和窃听的可检测性, 在过去的二十多年里, 量子加密引起了国内外科学界和工业界的研究热潮, 并已成为计算机科学和物理中的一个重要研究方向. 量子加密将量子力学和经典密码学相结合, 利用量子物理的客观规律来保证通信的安全. 量子秘密共享是量子密码中的重要分支之一, 主要研究如何借助于量子资源, 将一个秘密分拆给 n 个接收方, 并使得只有 m 个接收方($m \leq n$)合作时才能重建这个秘密. 近 10 年来, 量子秘密共享受到了广泛的关注. 量子秘密共享方案可分为基于纠缠和不基于纠缠两种. 由于不基于纠缠的方案更易实现, 因此已经开始走向实用化. 在走向实用化的过程中, 对量子秘密共享方案安全性的分析, 尤其是定量分析, 显得更为重要和迫切.

为此, 东南大学计算机科学与技术学院的陈汉武教授带领其团队在这个方向上做了一系列的研究工作. 近期, 通过对量子秘密共享的深入研究, 许娟等人给出了一种安全性定量分析的新思路, 并得到了对无纠缠量子秘密共享方案的设计和实施都具有重要指导意义的结果. 该成果发表在《中国科学 信息科学》2011 年第 7 期上.

目前, 对量子秘密共享方案安全性分析的主要思路是设计各种巧妙的量子攻击策略, 验证方案对此攻击是否安全; 而对方案安全性进行定量分析是一个难点, 目前这方面的研究成果较少, 主要是针对特定的方案利用信息论方法给出错误上界或某些关系式. 论文作者原创性地从酉操作这个关键操作入手, 在充分研究和分析不使用纠缠的量子秘密共享方案的基础上, 设计了一种对这类方案通用的

攻击策略, 命名为“Bell 态替换攻击策略”, 并给出了衡量攻击效果的“Bell 态替换攻击的最小失败概率”公式; 然后, 对方案的酉操作进行了细化和分类, 给出了“一步酉操作”和“两步酉操作”的定义, 并针对这两类酉操作的几种可能而典型的组合, 给出了方案安全程度的具体计算结果; 最后, 通过对结果的分析, 给出了设计和实施这类方案时该如何选择酉操作的具体指导意见, 即: 有些酉操作组合绝对不能采用, 而有些酉操作是较优的选择; 并不是酉操作组合中的种类越多, 方案安全性就越高; 酉操作种类相同时, 两步酉操作的安全性并不一定大于一步酉操作; 在安全程度相同的情况下, 建议使用种类少的酉操作组合.

该研究工作是对量子秘密共享方案安全性定量分析方法的一种探索, 有别于现有的从窃听者和攻击者角度的分析方法; 是从一类方案本身固有的关键操作入手, 给出了一整套新的完整的分析和解决思路, 或将给这个领域的研究工作带来一定的启发. 该文得出的结论无论是对量子秘密共享方案的理论研究还是实用化研究都具有重要的参考价值, 并能指导这类方案在设计或实施时选择合适的关键操作以达到预期的安全性能. 论文作者目前已经完成论文所设定的范围内所有可能操作组合的计算和分析工作, 并将研究工作逐步辐射到更大的范围和更复杂的情况.

该研究得到了国家自然科学基金(60873101)和江苏省自然科学基金(BK2007104, BK2008209)的资助.

《科学通报》编辑部