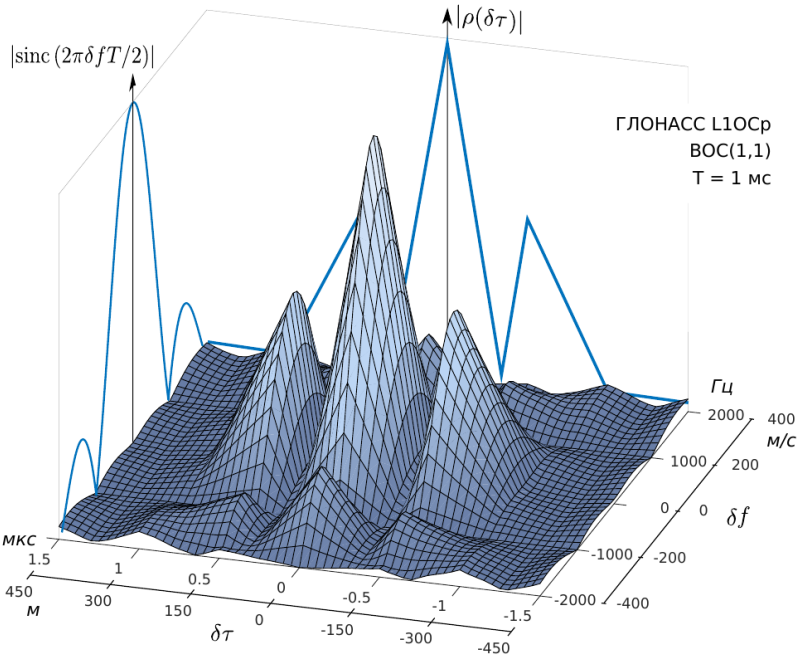
Korogodin
2 авг 2022 в 08:00

Сигналы глобальных навигационных систем

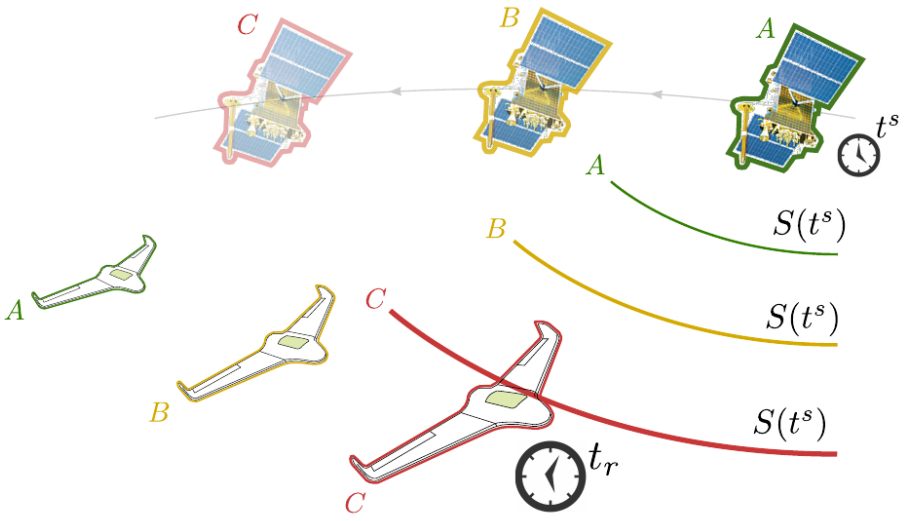
7 мин **57K**

Спутниковые системы навигации*, Беспроводные технологии*, Производство и разработка электроники*, Электроника д



В наши дни в навигации доминируют глобальные навигационные спутниковые системы (ГНСС) второго поколения: GPS, ГЛОНАСС, Galileo и Beidou. Они развиваются и управляются разными странами, но очень похожи по своей структуре, техническим решениям и возможностям.

Каждая из систем содержит несколько десятков спутников, которые движутся по круговым орбитам на высоте около 20 000 км и содержат на своем борту высокостабильные часы. Спутники наблюдаются станциями наземного комплекса управления, что позволяет предсказывать положение спутников и уход их часов с точностью в метры и наносекунды.



Фронт сигнала, соответствующий одному и тому же времени излучения, в моменты A, B и C

Каждый из спутников излучает навигационный радиосигнал, формируя его в собственной шкале

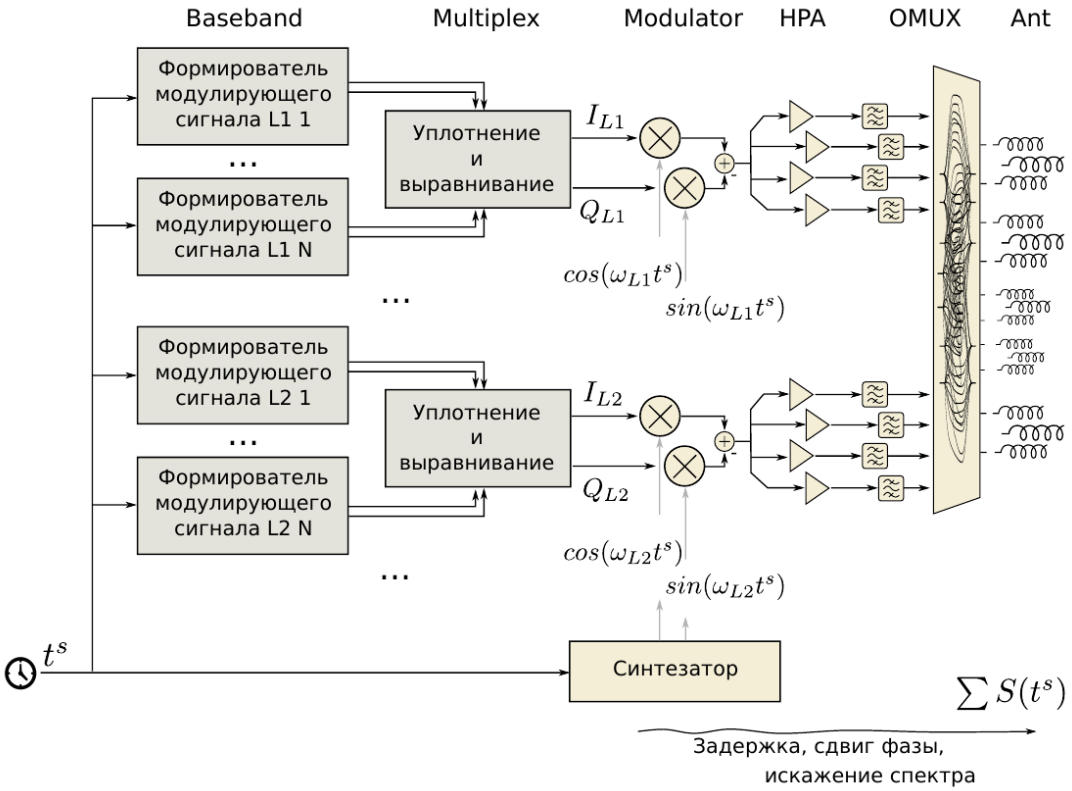
времени:

$$t^s \mapsto S(t^s)$$

Сигнал выступает оберткой, физическим носителем показаний часов спутника. Это способ обеспечить "видимость" этих часов за тысячи километров, несмотря на облака, листву и прочие препятствия.

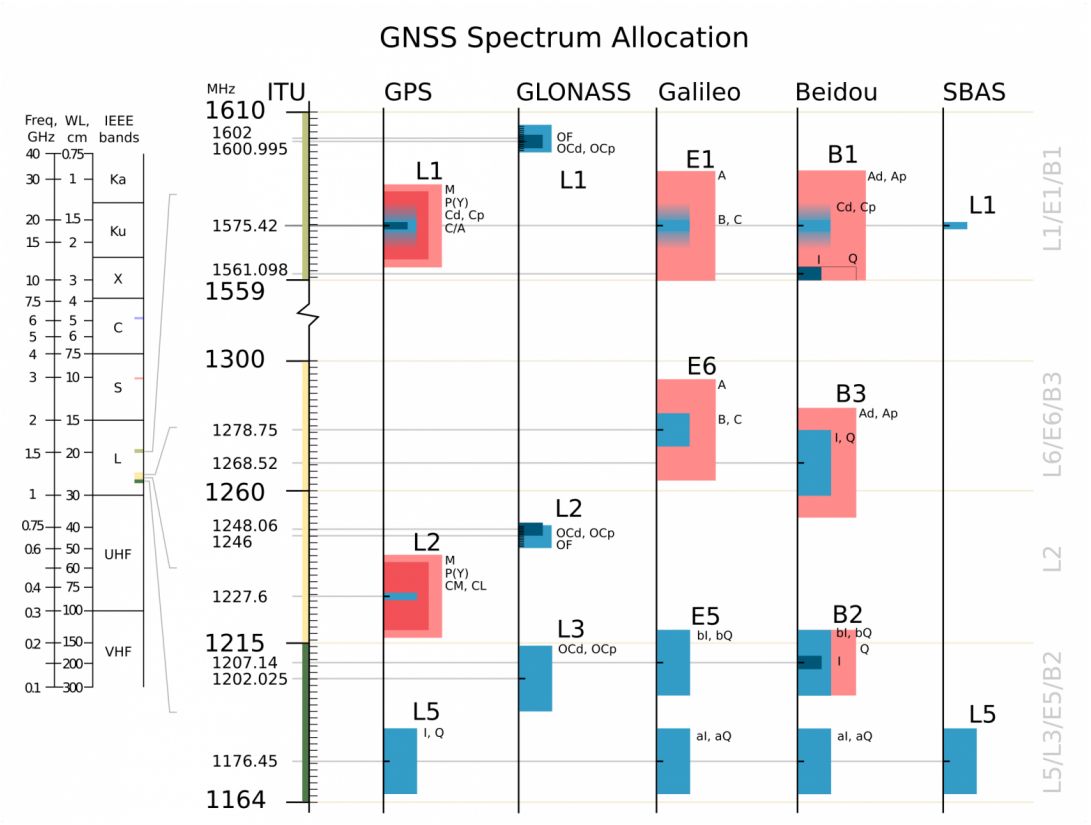
Структура функции S(t) известна и описана в контрольных документах системы. Имея математическую модель сигнала, приемник определяет заложенное в сигнал время и сравнивает его с собственными часами. Разница сигнального времени и часов приемника связана с расстоянием до спутника, а расстояние до спутника - с местоположением приемника. Собрав наблюдения от нескольких спутников, приемник составляет несложную систему уравнений и определяет где он находится.

Навигационный сигнал принимается на фоне шумов, помех и других сигналов. Мощность этих мешающих воздействий в сотни и более раз превышает мощность самого навигационного сигнала. По этой причине обработка сигнала не сводится к взятию обратной функции. Вместо этого приемник создает локальную копию сигнала на основе его математической модели, а затем подстраивает параметры этой копии до максимального совпадения (корреляции).



Формирование группового навигационного сигнала на борту спутника

Алгоритмы обработки навигационных сигналов определяются математической моделью навигационного сигнала. И на этом шаге современные ГНСС преподносят нам сюрприз. Оказывается, что разные системы используют разные сигналы. Более того, каждый спутник не ограничивается одним типом сигнала, а излучает целый набор. Так на новых спутниках ГЛОНАСС можно выделить до 14 разных навигационных сигналов! А в совокупности по всем системам типов сигналов больше 50.



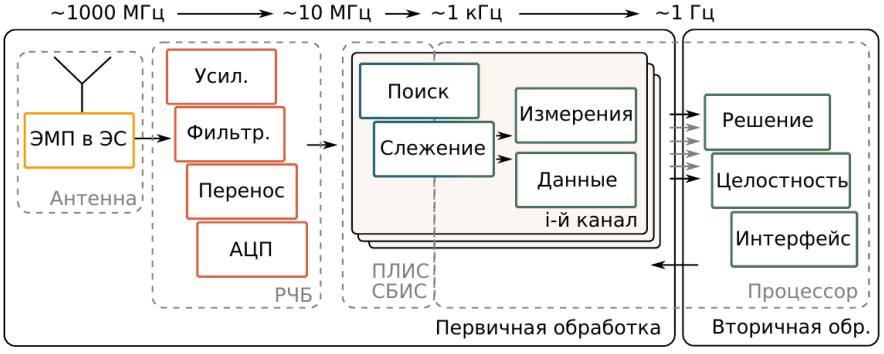
Распределение сигналов различных типов по нижнему L-диапазону частот

Если попытаться к радионавигации применить модель OSI, то разные системы и сигналы задают разные протоколы физического уровня. Информативный процесс отражается на физический по немного разным правилам. И если мы хотим построить мультисистемный навигационный приемник, мы должны добавить поддержку всех этих протоколов.

Но не спешите расчехлять ваши IDE. У разных сигналов слишком много общего, поэтому писать независимый код под каждый тип сигнала - плохая идея:

1. Поддерживать и тестировать множество реализаций однотипных функций тяжело и дорого, к тому же распухает объем прошивки.
2. При сигнальной обработке часть функций реализуется аппаратно (в ПЛИС или модулях СБИС), а значит мы займем кристалл множеством специализированных каналов, потеряем в гибкости настроек.

Что если попробовать другую крайность: обобщить разные сигналы до одной математической модели, а нюансы разных сигналов описывать параметрами этой модели? К такому подходу моя команда пришла после разработки нескольких навигационных приемников. Сейчас мы используем унифицированные каналы, инициализируя их нужными параметрами при старте слежения за тем или иным сигналом.



Функциональная схема навигационного приемника

Модель традиционных сигналов

Положение потребителя оценивается по задержкам сигналов, поэтому навигационные сигналы специально спроектированы так, чтобы упростить оценку этих задержек на фоне шумов и мешающих факторов.

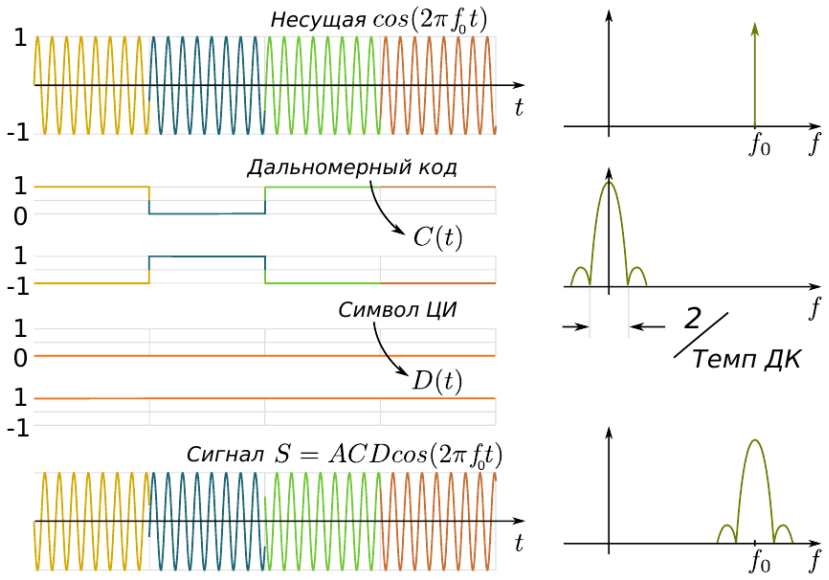
Согласно формуле Вудворда, чем большую полосу занимает сигнал, и чем больше его спектр сосредоточен на краях выделенного диапазона, тем меньше шумовая ошибка оценки задержки его огибающей. Спутник передает навигационные данные (информацию о своем положении и т.п.) с низкой скоростью, что не приводит к существенному расширению спектра сигнала. Поэтому для увеличения точности оценки задержки сигнала его дополнительно модулируют спектрорасширяющей последовательностью.

Пожалуй самые популярные сигналы, которые можно встретить в каждом смартфоне, - это сигналы GPS L1C/A и ГЛОНАСС L1OF. В этих сигналах в качестве спектрорасширяющей последовательности используются дальномерные коды с периодом в 1 мс и длиной 1023 и 511 символов соответственно. Эти последовательности являются псевдослучайными, формируются с помощью линейных генераторов на сдвиговых регистрах. Модель таких традиционных сигналов, как C/A и OF, проста:

$$S(t) = ACD\cos(2\pi f_0 t + \varphi),$$

где

- A = A(t) - амплитуда сигнала, пропорциональная корню из его мощности,
- C = C(t) - модуляция дальномерным кодом, принимает значения +1 и -1, смена значений происходит часто (2 мкс или менее),
- D = D(t) - модуляция символами навигационного сообщения, смена значений происходит редко (2 мс или более), а сами значения заранее не известны приемнику,
- f_0 - несущая частота, например, 1575.42 МГц для GPS L1C/A, φ - начальная фаза.



Сигнал ГНСС с модуляцией дальномерным кодом и навигационным сообщением

Обобщаем на новые сигналы

После нескольких десятков лет эксплуатации GPS и ГЛОНАСС с традиционными сигналами встал

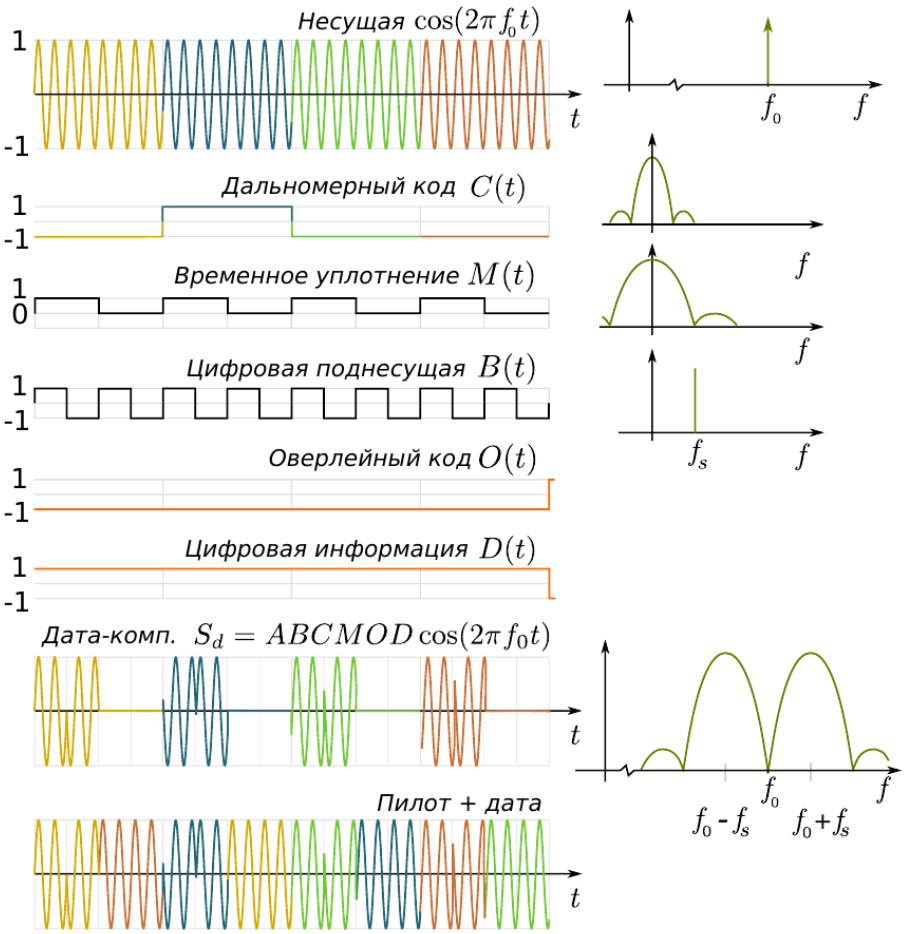
вопрос о модернизации систем, включая добавление новых сигналов. Задача разработки сигналов возникла и в Galileo с Beidou, создаваемых с нуля. Разработчики стали упражняться в попытках угодить всем потребителям одновременно, героически борясь с конфликтующими требованиями:

- высокая потенциальная точность и низкая ошибка многолучевости;
- простота приемной аппаратуры и низкое энергопотребление;
- минимизация влияния от/на другие радиосистемы;
- постоянство огибающей (высокий КПД усилителя на спутнике) и уплотнение со старыми сигналами;
- использование ранее распределенных под спутниковую навигацию частот;
- чувствительность и помехоустойчивость при большей скорости передачи данных.

Схемы модуляции усложнились. Например, в GPS L2C применили посимвольное уплотнение двух сигнальных компонент, когда они передаются по-очереди: символ от одного, символ от другого. Эта же схема используется в сигналах ГЛОНАСС с кодовым разделением.

В некоторых сигналах применили оверлейные (они же вторичные) коды. С их помощью улучшаются корреляционные свойства сигналов, один сигнал меньше мешает приему другого.

Отдельная хитрость - использование цифровой поднесущей, т.е. умножение сигнала на меандр. Это приводит к расщеплению спектра сигнала, на нем появляются два лепестка. Если использовать новый сигнал на одной несущей со старым, это разнесет их по спектру, и они меньше будут влиять друг на друга. В зависимости от особенностей реализации этот прием называют BOC (binary offset carrier), AltBOC, TMBOC, CBOC, QMBOC и т.д.



Сигнал ГНСС с модуляцией дальномерным кодом, цифровой поднесущей, оверлейным кодом и навигационным сообщением

Если всё объединить, получаем обобщенную модель навигационного сигнала:

$$S(t) = ABCMOD\cos(2\pi f_0 t + \varphi)$$

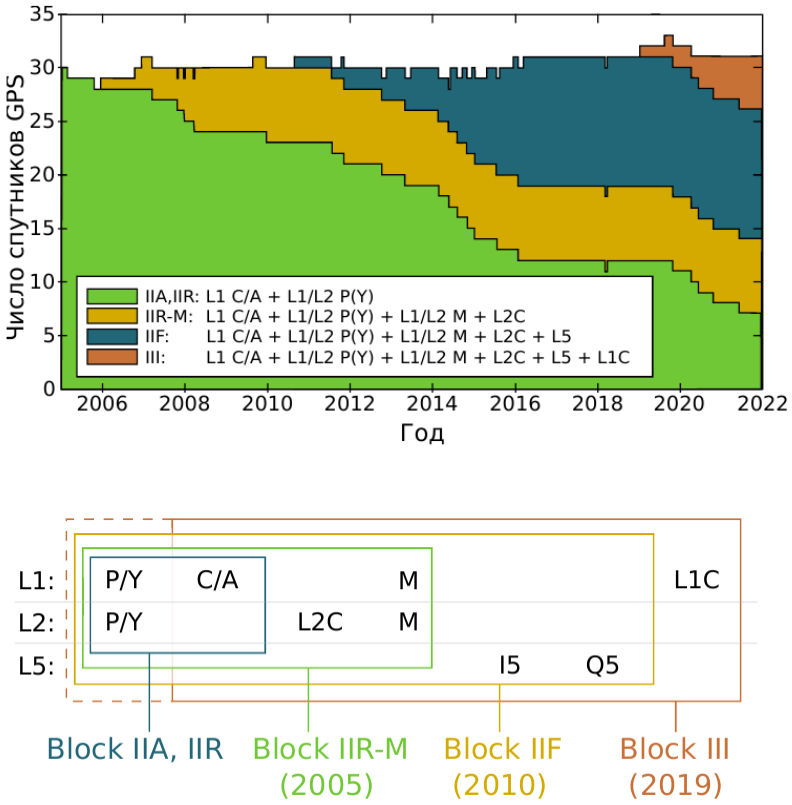
где в дополнение к введенным ранее функциям

- B = B(t) - модуляция цифровой поднесущей, принимает значения +1 и -1, смена значений происходит часто (половина мкс или менее),
- M = M(t) - П-функция размещения во временном слоте, принимает значения +1 и 0 внутри и вне временного слота соответственно, смена значений происходит часто (половина мкс или менее),
- O = O(t) - модуляция оверлейным кодом, принимает значения +1 и -1, смена значений происходит редко (1 мс или более).

Модели сигналов более простой структуры могут быть получены из общей модели путем исключения лишних множителей или приемом их равными единице.

Сигналы системы GPS

Система GPS сменила уже несколько поколений спутников, сейчас продолжают функционировать аппараты от Block IIA до Block III.



Связь излучаемых сигналов с типом навигационного спутника GPS

В процессе модернизаций были добавлены гражданские сигналы L2C на второй несущей частоте, военные криптозащищенные M сигналы. С Block IIF начали вводиться сигналы L5 на третьей несущей частоте с полосой 20 МГц, а Block III подарил нам сигналы L1C. Последние со временем могут заменить C/A в наших смартфонах и сделать доступной для гражданских пользователей функцию цифровой подписи для защиты от спуфинговых атак.

Параметры обобщенной модели для сигналов GPS собраны в таблице (кликните для увеличения):

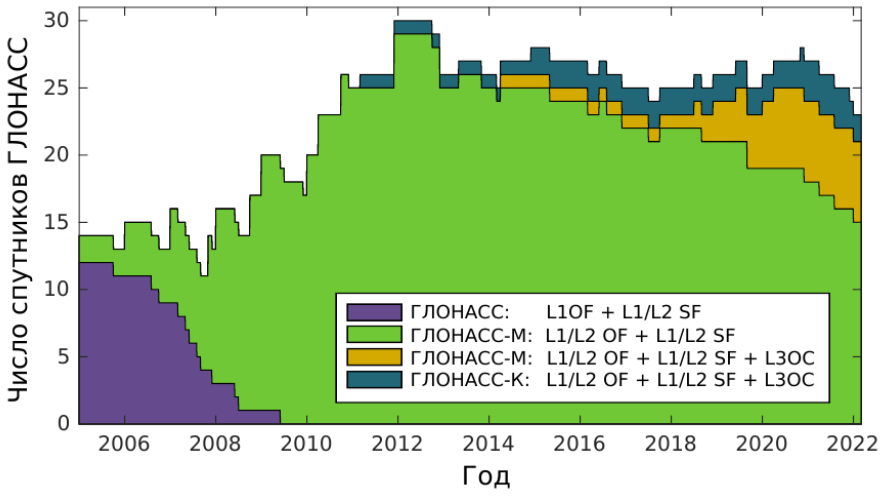
Система	Несущая f_0, МГц	I/Q	Тип		Полоса МГц	$\overline{A}$ дБВт	B	Дальномерный код C				M	Оверлейный код O			Навигационное сообщение D			
							m	Генер.	Длина симв	Темп симв/мс	Период мс	Темп слот/мс	Длина симв	Символ мс	Период мс	Тип	Кодер	Символ мс	Поток бит/с
GPS	1575.42	I	L1C/A		2.046	-158.5	-	Рег	1023	1023	1	-	-			LNAV	CRC16	20	< 40
		Q	L1C	L1Cd	4.092	-163	1	Рег/таб	10230	1023	10	-	-			CNAV2	BCH(51,8) LDPC CRC24Q Интерливер	10	< 46
				L1Cp	4.092	-158.8	1	Рег/таб	10230	1023	10	1023: 29 из 33	1800	10	18000	-			
					14.322	-167.4	6					1023: 4 из 33							
			L1P(Y)		20.46	-164.5/ -161.5	-	Рег (хэш)	$6.2 \cdot 10^{12}$ (∞)	10230	7 дней (нет)	-	-			с.д.		20	< 40
			L1M		25.5	-158 (-138)	10	с.д.		5115	с.д.					MNAV	с.д.		
	1227.6	I	L2C	L2CM	2.046	-167.5/ -161.5	-	Рег	10230	511.5	20	1023	-			CNAV	FEC(133,171) CRC	20	< 25
				L2CL	2.046	-167.5/ -161.5	-	Рег	767250	511.5	1500	1023	-			-			
		Q	L2P(Y)		20.46	-164.5/ -161.5	-	Рег (хэш)	$6.2 \cdot 10^{12}$ (∞)	10230	7 дней (нет)	-	-			с.д.		20	< 40
			L2M		25.5	-158 (-138)	10	с.д.		5115	с.д.					MNAV	с.д.		
	1176.45	I	L5	L5I	20.46	-157.9/ -157.0	-	Рег	10230	10230	1	-	10	1	10	CNAV	FEC(133,171) CRC	10	< 50
		Q		L5Q	20.46	-157.9/ -157.0	-	Рег	10230	10230	1	-	20	1	20	-			

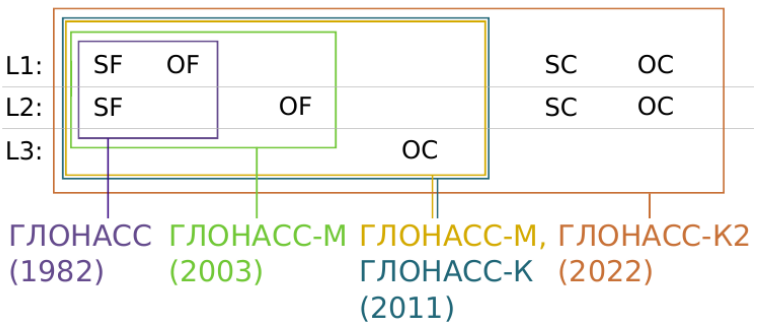
Примечания:

1. В сигнале L1Cp используется модуляция TMBOC. Поднесущая периодически увеличивает частоту в 6 раз: каждый 1-й, 5-й, 7-й и 30-й символ дальномерного кода из 33.
2. Дальномерный код сигналов L1C формируется на регистрах сдвига из длинной табличной последовательности Лежандра.
3. При включении режима antispoofing сигналы L1P, L2P дополнительно модулируется непериодической последовательностью.

Сигналы системы ГЛОНАСС

Количество модификаций спутников ГЛОНАСС меньше, чем в GPS. Но по разнообразию заявленных сигналов они не отстают. Основными сигналами остаются традиционные сигналы с частотным разделением, но с выводом новых спутников ГЛОНАСС-К2 мы увидим и новые сигналы с кодовым разделением. А там и BOC модуляция, и временное уплотнение, и прочие изыски.





Параметры обобщенной модели для сигналов ГЛОНАСС собраны в таблице (кликните для увеличения):

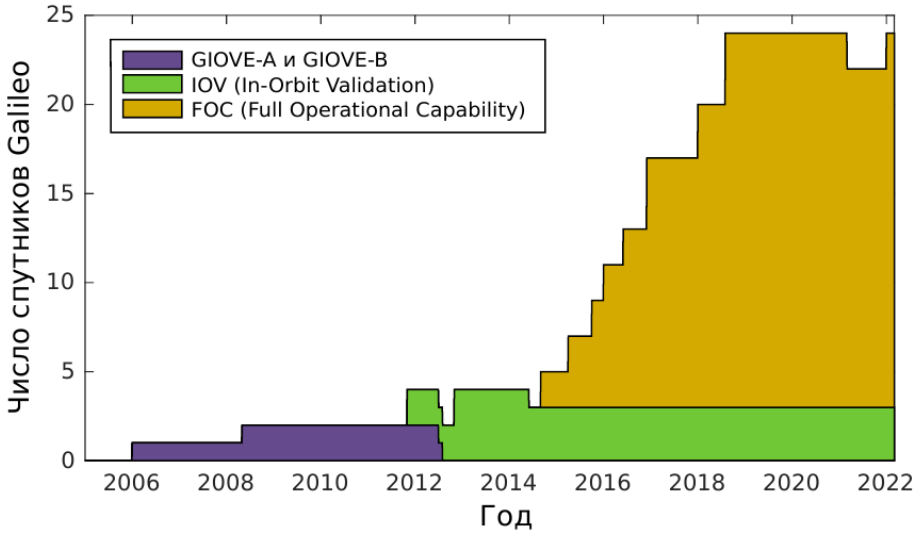
Система	Несущая f_0, МГц	I/Q	Тип		Полоса МГц	$\overline{A}$ дБВт	B	Дальномерный код C				M	Оверлейный код O			Навигационное сообщение D			
							m	Генер.	Длина симв	Темп симв/мс	Период мс	Темп слот/мс	Длина симв	Символ мс	Период мс	Тип	Кодер	Символ мс	Поток бит/с
ГЛНС	1602 +k·0.5625 k=-7..+6	Q	L1OF (L1 СТ)		1.022	-161	-	Per	511	511	1	-	-			FDMA	Хэмминг Меандр	10	< 50
		I	L1SF (L1 ВТ)																
	1600.995	Q	L1OC	L1OCd	2.046	-161.5	-	Per	1023	511.5	2	1023	2	2	4	инд.	FEC(171,133) CRC	4	< 125
				L1OCp	4.092	-161.5	1	Per	4092	511.5	8	1023	-			-			
		I	L1SC																
	1248.06	Q	L2q (L2OC)	L2КСИ (L2OCd)	2.046	-161.5	-	Per	1023	511.5	2	1023	-			с.д.	с.д.	2	< 250
				L2OCp	4.092	-161.5	1	Per	10230	511.5	20	1023	50	20	1000	-			
		I	L2SC																
	1246 +k·0.4375 k=-7..+6	Q	L2OF (L2 СТ)		1.022	-161	-	Per	511	511	1	-	-			FDMA	Хэмминг Меандр	10	< 50
		I	L2SF (L2 ВТ)																
	1202.025	I	L3OC	L3OCd	20.46	-161.5	-	Per	10230	10230	1	-	5	1	5	инд.	FEC(171,133) CRC	5	< 100
		Q		L3OCp	20.46	-161.5	-	Per	10230	10230	1	-	10	1	10	-			

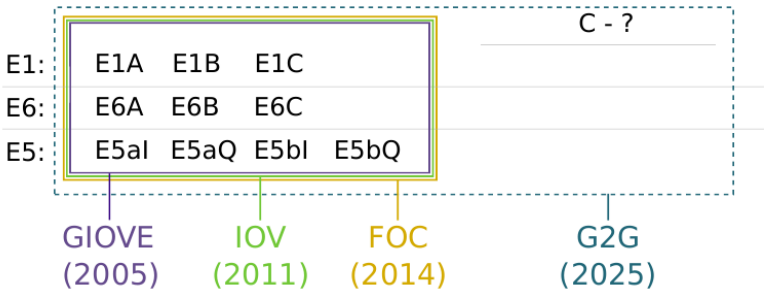
Примечания:

1. FEC-кодер ГЛОНАСС использует инвертированный порядок в выходных парах бит относительно аналогичного кодера GPS.
2. Название для типа навигационного сообщения сигналов L1OC и L3OC в RINEX 4.0 [104] не определено.
3. Отнесение сигналов L1OF и L1SF, L2OF и L2SF к квадратурам условное на основе [56]. Они в квадратуре, но кто кого опережает – ИКД не определяет.
4. Сигналы L1OF и L2OF используют одну и ту же последовательность дальномерного кода для сигналов всех спутников.

Сигналы системы Galileo

Галилео изящно вписался в частотный план навигационных систем. Его сигнал E1 по назначению и параметрам близок к L1C GPS и B1C BDS. В тестовом режиме он уже сейчас включает цифровую подпись для защиты от спуфинга. Сигнал E5 использует модуляцию AltBOC и образует самый широкополосный совокупный сигнал из всех существующих, целых 50 МГц. При разработке системы сигнал E6 предполагался коммерческим, по отдельной подписке. Но несколько лет назад его дальномерные коды были открыты, а на днях опубликована и спецификация сообщения C/NAV.





Параметры обобщенной модели для сигналов Galileo собраны в таблице (кликните для увеличения):

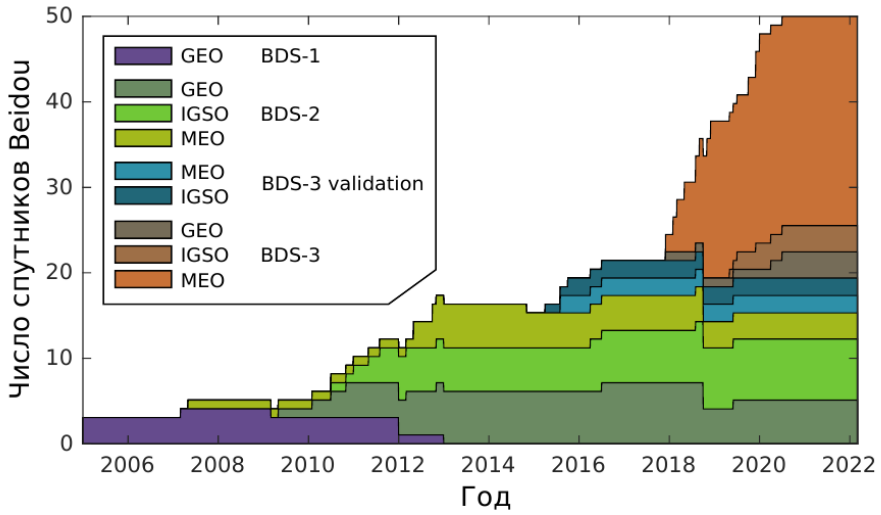
Система	Несущая f_0, МГц	I/Q	Тип		Полоса МГц	$\overline{A}$ дБВт	B	Дальномерный код C				M	Оверлейный код O			Навигационное сообщение D			
							m	Генер.	Длина симв	Темп симв/мс	Период мс	Темп слот/мс	Длина симв	Символ мс	Период мс	Тип	Кодер	Символ мс	Поток бит/с
Galileo	1575.42	Q	E1A		35.8	с.д.	15	Хэш	с.д.	2557.5	с.д.	с.д.	с.д.			G/NAV	с.д.		
		I	E1 OS	E1B	4.092	-160.4	1	Таб	4092	1023	4	-	-			I/NAV	FEC($\overline{133}$,171) CRC Интерливер	4	< 125
					14.322	-170.4	6												
				E1C	4.092	-160.4	1	Таб	4092	1023	4	-	25	4	100	-			
					14.322	-170.4	6												
	1278.75	Q	E6A		30.7	с.д.	10	Хэш	с.д.	5115	с.д.	с.д.	с.д.			G/NAV	с.д.		
		I	E6 HAS	E6B	10.23	-158	-	Таб	5115	5115	1	-	-			C/NAV	FEC($\overline{133}$,171) CRC Интерливер	1	< 492
				E6C	10.23	-158	-	Таб	5115	5115	1	-	100	1	100	-			
	1207.14	I	E5b	E5bI	20.46	-158	-	Рег	10230	10230	1	-	4	1	4	I/NAV	FEC($\overline{133}$,171) CRC Интерливер	4	< 125
		Q		E5bQ	20.46	-158	-	Рег	10230	10230	1	-	100	1	100	-			
	1176.45	I	E5a	E5aI	20.46	-158	-	Рег	10230	10230	1	-	20	1	20	F/NAV	FEC($\overline{133}$,171) CRC Интерливер	20	< 25
		Q		E5aQ	20.46	-158	-	Рег	10230	10230	1	-	100	1	100	-			

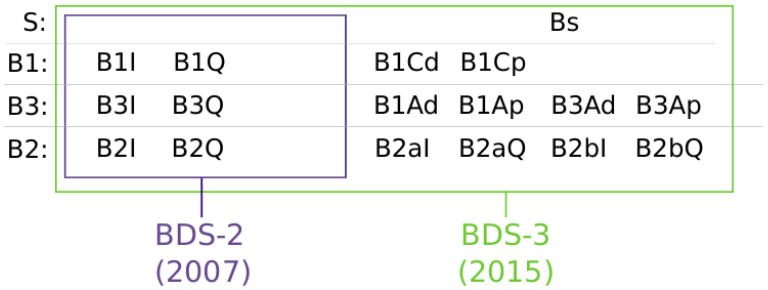
Примечания:

1. В сигналах E1B, E1C используется модуляция CBOC: из основной поднесущей вычтена ещё одна, ослабленная в десять раз, но идущая с частотой в шесть раз выше.
2. По состоянию на 2022 год структура и состав сообщения C/NAV не утверждены.
3. Один из выходов FEC кодера инвертирован по сравнению с аналогичным кодером, используемым в GPS.
4. Сигналы E5a и E5b образуют совокупный сигнал E5, обладающий модуляцией AltBOC(15, 10).

Сигналы системы Beidou

Темпы обновления и развития системы Beidou поражают. Сейчас система находится в третьей фазе, за прошлые 2-3 года спутниковая группировка почти полностью обновлена. Сигналы третьей фазы напоминают сигналы Galileo и хорошо дополняют американскую и европейскую системы.





Параметры обобщенной модели для сигналов Beidou собраны в таблице (кликните для увеличения):

Система	Несущая f_0, МГц	I/Q	Тип		Полоса МГц	$\overline{A}$ дБВт	B	Дальномерный код C				M	Оверлейный код O			Навигационное сообщение D			
							m	Генер.	Длина симв	Темп симв/мс	Период мс	Темп слот/мс	Длина симв	Символ мс	Период мс	Тип	Кодер	Символ мс	Поток бит/с
Beidou	1575.42	I	B1A	B1Ad	32.7	-156.9	14	с.д.		2046	с.д.					с.д.		10	< 50
		Q		B1Ap												-			
		I	B1C	B1Cd	4.092	-165	1	Рег/таб	10230	1023	10	-	-			B-CNAV1	BCH 2 вида LDPC 2 вида CRC Интерливер	10	< 50
		Q		B1Cp	4.092	-160.8	1	Рег/таб	10230	1023	10	-	1800	10	18000	-			
		I			14.322	-169.4	6												
	1561.098	I	B1I		4.092	-163	-	Рег	2046	2046	1	-	20	1	20	D1	BCH(15,11,1) CRC	20	< 36
													-			D2		2	< 366
		Q	B1Q		4.092	с.д.													
	1268.52	I	B3I		20.46	-163	-	Рег	10230	10230	1	-	20	1	20	D1	BCH(15,11,1) CRC	20	< 36
													-			D2		2	< 366
		Q	B3Q		20.46	-163	-	н.д.		10230	с.д.								
		I	B3A	B3Ad	35.8	-156	15	с.д.		2557.5	с.д.					с.д.		10	< 50
		Q		B3Ap												-			
	1207.14	I	B2I		4.092	-163	-	Рег	2046	2046	1	-	20	1	20	D1	BCH(15,11,1) CRC	20	< 36
													-			D2		2	< 366
		Q	B2Q		20.46	с.д.													
		I[6]	B2b	B2bI	20.46	-160	-	Рег	10230	10230	1	-	-			CNAV3 PPPB2b	LDPC(162,81) CRC24Q	1	< 500
		Q[6]		B2bQ	20.46	н.д.	-	н.д.	н.д.	10230	н.д.	-	н.д.			н.д.			
	1176.45	I	B2a	B2aI	20.46	-159	-	Рег	10230	10230	1	-	5	1	5	B-CNAV2	LDPC(96,48) CRC	5	< 92
		Q		B2aQ	20.46	-159	-	Рег	10230	10230	1	-	100	1	100	-			

Примечания:

1. В сигнале B1Cp используется модуляция QMBOC: помимо основной поднесущей BOC(1,1) в квадратуре добавлена поднесущая BOC(6,1), ослабленная в пропорции 4 к 29.
2. Специфицируемая мощность сигналов B1C, B2a, B2b у поверхности земли для спутников на наклонной ГСО на 2 дБ ниже, чем для среднеорбитальных (указанна в таблице).
3. Дальномерный и оверлейный коды сигналов B1C формируются на регистрах сдвига из длинной табличной последовательности Лежандра.
4. Сообщения D1 и CNAV3 используются на среднеорбитальных и наклонных геосинхронных спутниках, D2 и PPPB2b — на геостационарных.
5. Сигналы B2a и B2b образуют совокупный сигнал с модуляцией ACE-BOC (asymmetric constant envelope BOC), но ИКД [66; 67] не задают соотношение их мощностей.
6. В несущей сигнала B2b при его формировании может использоваться дополнительный фазовый сдвиг на 45 градусов [68].

Заключение

При всем разнообразии навигационные сигналы современных ГНСС могут быть приведены к общему описанию, что позволяет унифицировать программные и аппаратные блоки, их обрабатывающие. Эта унификация упрощает разработку и тестирование приемника, подсказывает как выстраивать архитектуру программного обеспечения и какие интерфейсы использовать. Упрощаются аналитические расчеты, их достаточно провести для обобщенной модели, а затем редуцировать до требуемого сигнала.

Приведенное в статье описание является высокоуровневым и не затрагивает реализацию блоков обработки таких сигналов. Кроме того, за бортом остался канальный уровень передачи данных (data link layer) с вопросами синхронизации, декодирования и хранения сообщений. Он тоже требует обобщения, но об этом как-нибудь в другой раз.

Теги: gps, glonass, ГЛОНАСС, Galileo, Beidou, DSP, navigation, signal, processing, GNSS

Хабы: Спутниковые системы навигации, Беспроводные технологии, Производство и разработка электроники, Электроника для начинающих

+42 101 52



83
Карма

Илья Корогодин @Korogodin

Спутниковые навигационные системы

Подписаться

Сайт

Комментарии 52





lab412
2 авг 2022 в 09:06

У меня давно был вопрос. Все говорят до сих пор что GPS имеет "военные" частоты и "гражданские". Первые дают точность в миллиметры чтобы самолёты летали и ракеты падали куда надо. Вторые частоты для "обычных людей" и там точность такая что не всегда машина даже может понять на какой полосе она едет... Но это все "слухи", а на практике как? Вся эта байка в моем представлении разбивается о то, что если сигнал излучается и нет фидбэка назад, то никто не запретит принять "военный" сигнал и использовать для того чтобы кататься на велике. Вопрос лишь в том, что может быть закрытый протокол, но за 30 лет использования его бы уже давно изучили и разобрали по полочкам, хотя бы потому что он был 30 лет назад придуман а не вчера. Тот же GSM давно "реверснули" и получили кучу плюшек...

Ответить

Korogodin
2 авг 2022 в 09:19

"Военные" сигналы GPS - это сигналы с P(Y) (L1P, L2P в таблице) и M (L1M, L2M в таблице) кодом. У них в 10-20 раз шире полоса, чем у соседних гражданских сигналов. Это позволяет существенно снизить ошибку многолучевости и шумовую ошибку, но все остальные источники ошибок никуда не уходят. Поэтому при прочих равных можно говорить об увеличении точности позиционирования раза в два.

Прелесть M и P сигналов в другом:
1. Их дальномерный код является, по-сути, хэшем от текущего времени. Ключики периодически меняют, сломать их тяжело. Это защитает от спуфинга и ретрансляционных помех.
2. Широкая полоса увеличивает на порядок помехоустойчивость, что в разы сокращает радиус действия помехопостановщика
3. У M сигнала есть режим spot beam, когда его мощность поднимается на два порядка на ограниченной территории

Ответить

lab412
2 авг 2022 в 11:35

ну я так и не понял, почему они "военные" и "не для всех" если известно что это за сигнал? ну так почему в машины ставят "плохой" приёмник? если есть спецификация - то почему никто не разработал приёмник и не продаёт?

Ответить

Korogodin
2 авг 2022 в 11:39

Ключи распространяются только среди специальных потребителей, да и спецификация открыта лишь частично.

Есть приемы, позволяющие принимать эти сигналы без ключа, но с существенной потерей в отношении сигнал/шум. Несколько десятелетий назад сигналов и спутников было мало, это было актуально. Реализация встречается в старых геодезических приемниках

Ответить

lab412
2 авг 2022 в 14:22

берем готовый девайс с ключом, его всё равно никто не будет проверять так как обратной связи нет... реверсим... профит... такое делается на право и налево во всех отраслях и софтовах, видимо просто GPS нафик никому не сдался, как тот самый неуловимый Джо...

Ответить

Korogodin
2 авг 2022 в 14:30

Ключи индивидуальные для каждого приемника, они хранятся в аппаратном SAASM блоке. Даже если его расковырять, ключ скоро сменится и старый станет бесполезным.

Ответить

pulsework
3 авг 2022 в 10:24

каким образом новый ключ попадет в девайс?

Ответить

Korogodin
3 авг 2022 в 10:31

Мне, к счастью, не приходилось получать такой ключ. Но могу предположить, что по любому доверенному каналу.

Тут главное обеспечить целостность ключа. Если он будет перехвачен, то ничего страшного. А вот если искажен, то с приемом сигналов будут проблемы.

Ответить

vadimr
3 авг 2022 в 10:35

Секретчик из штаба приедет с секретным чемоданом и его прошьёт.

Ответить

vadimr
2 авг 2022 в 21:34

У военных, в отличие от гражданских применений, шифрование построено на одноразовых ключах из шифроблокнотов. Его нельзя вскрыть раз и навсегда, а только на время действия ключа, которое весьма невелико. Дальше придётся снова с нуля вскрывать вторую строчку шифроблокнота и т.д.

Но в реальности военные просто аннулируют шифроблокнот утраченного девайса.

Ответить

pulsework
3 авг 2022 в 10:25

откуда пентагон узнает что девайс утрачен? их же миллионы?

Ответить

vadimr
3 авг 2022 в 10:32

Их далеко не миллионы.

Если он работает в военном режиме GPS (а это, в основном, только стратегические вооружения), то в нём содержатся секретные ключи и, соответственно, применяется совершенно секретный шифроблокнот. Утрату секретного или, тем более, сов. секретного носителя невозможно не заметить даже при том бардаке, который, по слухам, бывает иногда в Пентагоне.

Подавляющее большинство военной техники работает в гражданском режиме, именно чтобы не связываться с суровыми мерами по поддержанию секретности.

Ответить

pulsework
3 авг 2022 в 10:37

HIMERAS оснащены GPS - их сейчас в У используют сотнями если не тысячами, несколько из них захвачена на складах. Часть упала не взорвавшись... Возможно похожа ситуация с натовскими 155 мм с цифровым наведением...

Ответить

vadimr
3 авг 2022 в 10:39

Они используют гражданский режим GPS, как и любая другая экспортная техника.

Причём думаю, что и в армии США HIMARS используют только гражданский режим. Не с руки артиллеристам связываться со всей этой бодягой.

Спецпотребители GPS – это, в основном, аппаратура вроде ядерных подводных лодок, авианосцев, стратегических бомбардировщиков и т.п.

Ответить

khe404
2 авг 2022 в 18:33

Мне казалось, что GPS излучал на двух частотах L1 и L2. При этом L1 кодировался гражданским Y ключом, а L2 как гражданским Y так и военным P и в мирное время P ключ был в принципе доступен, но система имела возможность закрываться, и на гражданское использование налагать ограничения. Дополнительная же точность военного приемника достигалась за счет того, что время прохождения ионосферы для сигналов разной частоты разное, но различие этого времени дает понимание о состоянии среды между спутником и приемником.

Что касается расковырять - то ключ не является фиксированным и может меняться.

Ответить

TyVik
4 авг 2022 в 19:21

Но тем не менее, спуфинг GPS - вполне реальная тема даже для военных дронов.

Ответить

select26
2 авг 2022 в 10:19

В статье написано, что точная временная метка находится внутри сигнала. Функция сигнала может включать генератор псевдослучайных последовательностей, например. Или симметричное шифрование/кодирование.

Как реверснуть такое решение?

Ну и из за однонаправленности потока ассиметричное шифрование применить сложно. А симметричное - предполагает хранение обеих частей шифра. А военные хранить умеют.

Ответить

Korogodin
2 авг 2022 в 10:29

Тут два варианта:
1. Обеспечить формирование одних и тех же последовательностей как на борту спутника, так и в приемнике. Для этого ключ передавать по отдельным каналам (сигналы санкционированного доступа).
2. Накладывать случайные последовательности так, чтобы они не исключали прием сигнала отдельными кусочками (codeless режим для сигналов санкционированного доступа, цифровая подпись для сигналов гражданских).

Ответить

saege5b
3 авг 2022 в 08:32

Миллиметровую точность можно добиться и другим способом:

Ставишь в точке с известными координатами второй приемник, обеспечиваешь устойчивую связь между двумя приемниками. Специальный софт. Готово. Не всегда, не везде, но в большинстве работает, все будет зависеть от "мобильного" приемника.

Ответить

suhoveev
2 авг 2022 в 09:14

Напишите пожалуйста про развитие глобальных навигационных спутниковых систем.

Ответить

Korogodin
2 авг 2022 в 09:24

Тема широкая, но я подумаю. Как минимум, потребуется разбить на статьи о разных системах, а может и отдально писать про спутники, отдельно про наземный сегмент, отдельно про приемники.

Ответить

Korogodin
2 авг 2022 в 14:13

И таймлайн развития приемников неплохо, я надеюсь, отражают две вот эти статьи:

https://habr.com/en/post/664110/

https://habr.com/en/post/664132/

Ответить

Shiva-TM
2 авг 2022 в 12:25

Очень плотно, сжато и по делу.

Ответить

НЛО прилетело и опубликовало эту надпись здесь

Korogodin
2 авг 2022 в 15:00

В этой задержке, собственно, и находится полезная информация. Для каждой точки пространства характерно своё сочетание задержек сигналов разных спутников.

Уход собственных часов дает одинаковый вклад во все наблюдаемые задержки, как подставка. Эта подставка оценивается наравне с координатами приемника. Она выступает четвертой неизвестной в системе уравнений. По этой причине для первого определения нужны наблюдения хотя бы от четырех спутников.

Ответить

JPEGEC
3 авг 2022 в 07:29

Зачем тогда вообще свое время? Ну сравнивать с нулем например.

Ответить

VT100
3 авг 2022 в 09:13

Вот за ноль и берётся сигнал 4-го спутника, часы которого высоко синхронны с остальными. Иначе — в трёх уравнениях дальности от 3-х спутников будет свободная переменная и решая их систему можно оказаться в другой точке.

Ответить

Chupaka
3 авг 2022 в 09:20

Время обычно идёт, а вот ноль со временем не меняется :)

Ответить

Korogodin
3 авг 2022 в 09:49

Можно и с нулем, но это не сократит число необходимых спутников.

Собственно, если при старте приемника недоступна сотовая сеть, а его RTC по какой-то причине на работают (батарейка села), то он и стартует с нуля. В нашем приемнике таким нулем выступает 1 января 1970 года.

Ноль - это частный случай плохих часов. Часы, которые встали. В этом случае поправка, которая будет получена в результате решения навигационной задачи, составит 52 года.

Ответить

alexhott
2 авг 2022 в 15:35

Так есть или нет приемник работающий сразу со всеми 4-я системами навигации?

Ответить

Korogodin
2 авг 2022 в 15:49

Конечно. И в виде части сотового телефона, и в виде отдельных модулей. Изделия разработки моей команды так вообще закрывают все диапазоны и все системы, отсюда и вся боль этой статьи

Ответить

Un_ka
2 авг 2022 в 18:42

Почему GPS, Galileo, ГЛОНАСС имеют группировку спутников, насчитывающую 24-30 аппаратов, а Китай решил использовать 48?

Ответить

Korogodin
2 авг 2022 в 18:44

Сейчас одновременно работают спутники и второй фазы, и третьей. Со временем отключат аппараты второй фазы и переведут в резерв.

Ответить

vadimr
3 авг 2022 в 10:55

Нельзя напрямую сравнивать, у них орбитальные плоскости тоже расположены по-разному. Бейдоу спроектирована так, чтобы очень плотно покрывать низкие широты, что ценно в условиях высотной городской застройки в городах Китая. А в Арктике, например, гораздо лучшее покрытие у ГЛОНАСС.

Ответить

Tangaroa
3 авг 2022 в 03:52

статью можно дополнить вот такой ссылкой на самодельный приёмник GPS из палки-верёвки (ну, почти): http://www.aholme.co.uk/GPS/Main.htm

Ответить

vadimk91
3 авг 2022 в 07:59

Не знаю с чем это связано, но на телефоне GPS test при старте первым делом находит спутники GPS и только примерно через полминуты ГЛОНАСС, BEIDOU и прочие. Особенность чипсета, мощность передатчиков, зона обслуживания или что-то другое?

И даже когда приёмник поддерживает несколько систем, в работе больше десятка спутников, хороший SNR - ошибка определения высоты по прежнему может быть +-50 метров, хотя точность определения координат например 3 метра.

Ответить

Korogodin
3 авг 2022 в 09:58

Вероятно, от сотовой сети получает эфемериды только для GPS

Ответить

Soukhinov
3 авг 2022 в 10:56

Правильно ли я понимаю, что если оснастить GPS-приёмник атомными часами, то будет достаточно принимать 3 спутника «за раз» для навигации, а если ещё оснастить «идеальным» (в некотором смысле этого слова) инерциальным модулем, то достаточно будет одного спутника «за раз»?

Ответить

Korogodin
3 авг 2022 в 11:04

Идеальные атомные часы и идеальный инерциальный модуль - это идеальные значения производных геометрических параметров, а не их абсолютные значения. В этом случае вы можете выставить начальную точку по старой доброй ГНСС, а дальше работать по идеальным приборам, отсчитывая от этой начальной точки.

Альтернативный вариант - разыграть количество спутников на время. По вращению Земли определить направление на север, по реакции опоры - вертикаль, пронаблюдав несколько часов один спутник - определить своё местоположение. В этом случае да, навигационная система могла бы состоять из одного спутника, идеальных часов и идеальных инерциальных датчиков. Но часа 2-3 на инициализацию уйдет.

Ответить

Soukhinov
3 авг 2022 в 22:33

Спасибо. Мой вопрос был по второму сценарию — без возможности инициализации точными значениями.

Допустим, я просыпаюсь в какой-то неизвестной пустыне (в более сложном случае — дрейфующим где-нибудь в океане). У меня есть навигационный приёмник с идеальными часами и идеальной инерциальной системой, но он выключен — не инициализирован. А в космосе только один рабочий спутник. Я своё оборудование включаю и начинаю принимать сигнал.

Ответить

Korogodin
3 авг 2022 в 22:40

Если при выключении питание сбрасывалось с часов и инерциалки, то придется подождать, как я сказал, 2-3 часа. За это время можно сделать гирокомпасирование и пронаблюдать спутник в разных точках небосклона. Гирокомпасирование даст ориентацию, спутник - положение. А дальше можно уже работать по инерциалке.

Ответить

v-oz
9 авг 2022 в 14:01

Очень интересно будет почитать про реализацию универсальных каналов. Не получается там так, что для каких-то систем реализация слишком усложняется?

Галилео, это ж какой-то головняк, говорят, в сравнении с первыми двумя(ми).

З.Ы. привет, МЭИ! (А-12-96)

Ответить

Korogodin
9 авг 2022 в 14:06

Как-нибудь распишу на досуге. Ну или приходите в МЭИ на лекции :)

Я бы сказал, больше головняка было с GPS L1C. Галилео заставил реализовать поиск сигналов с табличным кодом, остальное относительно безболезненно у нас прошло.

Ответить

Konstantinus
2 мар 2023 в 23:53

Можно ли отключать сигнал над определенной территорией? Какой минимальный при санкционировании такого действа получается тогда участок территории?

Ответить

Korogodin
5 мар 2023 в 16:16

Сделать небольшое выколотое пятно размером со страну не получится, если вы об этом

Ответить

aabzel
19 мая 2024 в 04:38

Что Вы можете порекомендовать прочитать про цос обработку внутри gps приёмников?

Ответить

Korogodin
19 мая 2024 в 15:00

Могу нескромно дать ссылку на свое учебное пособие по курсу навигационных приемников:

https://github.com/Korogodin/gnssrec

К сожалению, оно так и не опубликовано, поэтому часть глав в незавершенном виде, и нет редактуры

Ответить

aabzel
26 мая 2024 в 17:34

Спасибо за учебник.
Я почитал ту часть, которая меня сейчас интересует: Система слежения за фазой.
Подстраивание фазы NCO. Однако порог вхождения очень высокий. Я не понимаю как это реализовать в Си-коде.

Никак не получается выделить биты NavData из лога однобитных семплов I, и я не понимаю как это отладить.

Ответить

aabzel
20 мая 2024 в 02:37

Как подстраивать фазу Local Oscillator при приёме GPS сигнала?
Каков механизм работы контура Phase Lock Loop?

Ответить

Korogodin
20 мая 2024 в 20:46

Ни разу не встречал приемник, в котором требовалось бы подстраивать фазу LO. Максимум - фазу клока. Такая мысль может возникнуть, если у вас многоантенная обработка и важно сохранить фазовое распределение между каналами различных антенн. Но в этом случае проще выполнить доворот фазы уже на этапе цифровой обработки. Типично - просто довернуть квадратуры на выходе коррелятора.

LO формируется с помощью PLL: VCO, дискриминатора и делителя. Берете сигнал опорного колебания - кварца на 10 МГц. Стабилизируете фазу сигнала, полученного от VCO делением, сравнивая его

дискиминатором с опорным колебанием. Связав фазу VCO с фазой опорного колебания, из VCO получаете LO для всех частотных диапазонов делением. В навигации, как правило, используются целые коэффициенты, т.е. не используется fractional режим синтезатора. Иначе фаза сигнала и фаза огибающей начинают расходиться.

Подстраивать частоту LO смысла нет, не IXX век. Даже дешевый OCXO дает разброс частоты LO около 1 кГц. Сигнал точно пройдет ПЧ фильтры. Но в некоторых приемниках может быть физическое дисциплинирование не LO, а опорного генератора, если он потом используется для тактирования каких-то внешних устройств. Но это экзотика

Ответить

aabzel
22 мая 2024 в 19:25

> Ни разу не встречал приемник, в котором требовалось бы подстраивать фазу LO

Если не подстраивать фазу LO, то сигнальное созвездие вырождается в круг.

Как же тогда добиться того чтобы сигнальное созвездие было два пятна на оси I?

Ответить

Korogodin
22 мая 2024 в 21:25

Если использовать англоязычные термины, то для этого подстраивается фаза NCO, а не LO. NCO - это цифровые генераторы колебаний, индивидуальные для каждого сигнала. Подстраиваются они PLL канала обработки этого сигнала. В простейшем случае это классическая следящая система: фазовый дискриминатор, фильтр, по выходному сигналу фильтра коррекция частоты NCO. Фильтр, как правило, 3 порядка, полоса от 3 до 30 Гц. Дискриминатор - простая функция корреляционных сумм, полученных взятием скалярного произведения обрабатываемого и опорного сигналов. Опорный сигнал - тот самый, частотой которого управляет фильтр через NCO.

В более сложных случаях данные разных каналов могут объединяться для устранения общей составляющей, вызванной нестабильностью опорного генератора (coop tracking), разные сигналы одного спутника могут объединяться в один метасигнал, может компенсироваться движение приемника на базе данных от инерциальных датчиков, объединяться наблюдения от нескольких антенн и т.д., но это все специальные решения

Ответить

Зарегистрируйтесь на Хабре, чтобы оставить комментарий

ЕЖЕДНЕВНЫЙ ХАБР | 18 АВГ 2026

63K