

REDS 2021

№2

СОДЕРЖАНИЕ

Воронцов А.П. АКТУАЛЬНЫЕ ПРОБЛЕМЫ МОНИТОРИНГА И КОНТРОЛЯ СПУТНИКОВОЙ СОСТАВЛЯЮЩЕЙ ЕДИНОЙ ГЛОБАЛЬНОЙ КОНВЕРГЕНТНОЙ ИНФОКОММУНИКАЦИОННОЙ СРЕДЫ	3
Иванюшкин Р.Ю., Севериненко А.А., Волков И.А. ПРОБЛЕМАТИКА ПОСТРОЕНИЯ ПЕРЕДАТЧИКОВ ЦИФРОВОГО РАДИОВЕЩАНИЯ ДИАПАЗОНА ОВЧ НА ОСНОВЕ ПОЛЯРНОЙ АРХИТЕКТУРЫ	9
Дембицкий Н.Л. ВЫДЕЛЕНИЯ ПЕРИОДИЧЕСКОГО СИГНАЛА ИЗ ШУМОВ НЕЙРОФИЛЬТРОМ НА КОНТИНУАЛЬНЫХ ПРОЦЕССОРАХ	16
Мазуренко Д.К. ТРЕБОВАНИЯ К ЧАСТОТНО-ВРЕМЕННОМУ ОБЕСПЕЧЕНИЮ И синхронизации систем спутниковой радиосвязи	23
Мансуров Т.М., Зеневич А.О., Мамедов И.А. ВОЛОКОННО-ОПТИЧЕСКИЙ ОТВЕТВИТЕЛЬ/ПЕРЕКЛЮЧАТЕЛЬ МОЩНОСТИ ОПТИЧЕСКОГО ИЗЛУЧЕНИЯ	29
Панков К.Н., Эйрман А.Д. СЕРТИФИКАЦИЯ СИСТЕМ РАСПРЕДЕЛЕННОГО РЕЕСТРА КАК ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	37
Петров Д.С. РАЗРАБОТКА МОДЕЛИ И АЛГОРИТМОВ ОЦЕНКИ ЭФФЕКТИВНОСТИ ПРОЦЕДУРЫ РАСПРЕДЕЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫХ РЕСУРСОВ В СЕТЯХ 5G	50
Шелухин О.И., Желнов М.С. ИДЕНТИФИКАЦИЯ АНОНИМНЫХ ПОЛЬЗОВАТЕЛЕЙ ВЕБ-РЕСУРСА НА ОСНОВЕ НЕЧЕТКИХ ХЭШ – ФУНКЦИЙ ЦИФРОВЫХ ОТПЕЧАТКОВ УСТРОЙСТВ	57
Гадасин Д.В., Шведов А.В., Клыгина О.Г., Гадасин Д.Д. РЕАЛИЗАЦИЯ ПЛАТФОРМЫ ТУМАННЫХ ВЫЧИСЛЕНИЙ ДЛЯ ПРЕДОСТАВЛЕНИЯ СЕРВИСОВ IoT	64
Дрюпина Н.С., Кузьмин М.С., Манохина В.И., Нелюбина А.Е., Пшеничников А.П. АНАЛИЗ РАДИОТЕХНОЛОГИЙ ПРИ РЕАЛИЗАЦИИ ИНТЕЛЛЕКТУАЛЬНЫХ АВТОТРАНСПОРТНЫХ СИСТЕМ	75

АКТУАЛЬНЫЕ ПРОБЛЕМЫ МОНИТОРИНГА И КОНТРОЛЯ СПУТНИКОВОЙ СОСТАВЛЯЮЩЕЙ ЕДИНОЙ ГЛОБАЛЬНОЙ КОНВЕРГЕНТНОЙ ИНФОКОММУНИКАЦИОННОЙ СРЕДЫ

Воронцов Алексей Петрович,

ФГУП НИИР, заместитель директора центра, Москва, РФ

vap2201@gmail.com

Аннотация

Спутниковые системы связи всегда составляли важную часть формирующейся единой глобальной конвергентной инфокоммуникационной среды (ИКС), благодаря созданию которой стало возможным реализация планов цифровизации информационного общества. В настоящее время и в ближайшем будущем мировая тенденция по наращиванию существующих и созданию новых спутниковых группировок сохраниться. В статье будет показано, что российская наука в состоянии обеспечить адекватную темпам развития спутниковых группировок модернизацию существующих систем мониторинга и контроля. Рассмотрены предлагаемые авторские решения, в основе которых заложены технические решения, которые защищены патентами РФ.

Ключевые слова

Спутниковые группировки, Международный союз Электросвязи, системы контроля и мониторинга, антенная система РЛС, шумовая добротность антенны.

Введение

Спутниковые системы связи всегда составляли важную часть формирующейся единой глобальной конвергентной инфокоммуникационной среды (ИКС), благодаря созданию которой стало возможным реализация планов цифровизации информационного общества. В настоящее время и в ближайшем будущем мировая тенденция по наращиванию существующих и созданию новых спутниковых группировок сохраниться.

Так как обеспечение эффективного мониторинга и контроля спутниковой составляющей ИКС необходимо для обеспечения ее успешной эксплуатации, представляет интерес рассмотреть две взаимосвязанные проблемы: тренд развития спутниковой составляющей и модернизации существующих радиолокационных станций, которые должны осуществлять мониторинг.

Далее в статье будет показано, что новые разработки российских ученых в состоянии модернизировать существующие РЛС с учетом планируемых темпов развития спутниковых группировок. Так как обеспечение эффективного мониторинга и контроля спутниковой составляющей ИКС необходимо для обеспечения ее успешной эксплуатации, представляет интерес рассмотреть две взаимосвязанные проблемы: тренд развития спутниковой составляющей и модернизации существующих радиолокационных станций, которые должны осуществлять мониторинг.

Далее в статье будет показано, что новые разработки российских ученых в состоянии модернизировать существующие РЛС с учетом планируемых темпов развития спутниковых группировок.

Результаты исследований

Направления развития спутниковых группировок косвенно можно оценить на основе заявок в Международный союз электросвязи (МСЭ-Р) [1]. В статье в таблицах №1 и №2 приведен перечень и анализ заявлений в Международный союз электросвязи спутниковых сетей на геостационарной орбите, а так же на негеостационарной орбите проводился в следующих диапазонах частот: L диапазон (1452-1492 МГц, 1518-1559 МГц, 1610-1660.5 МГц, 1668 1675 МГц,

1930-1970 МГц), S- диапазон (1980-2025 МГц, 2120-2200 МГц, 2483.5-2535 МГц, 2655-2690 МГц), C-диапазон (3400-4200 МГц, 4500 4800 МГц, 5000-7075 МГц), X- диапазон (7250-7750 МГц, 7900 8400 МГц), Ku-диапазон (10700-13250 МГц, 13750-14500 МГц, 15300 15630 МГц) Ka-диапазон (17300-20200 МГц и 20200-21200 МГц, 24650-25250 МГц, 27000-30000 МГц и 30000-31000 МГц) и Q/V-диапазонов (37500-47000 МГц, 47200-50200 МГц и 50400-51400 МГц).

Ниже в таблице 1 приведено распределение заявлений геостационарных спутниковых сетей по диапазонам частот за все время и за 2020 год.

В таблице 2 приведено распределение заявлений не геостационарных спутниковых систем по диапазонам частот за все время и за 2020 год.

Анализ Таблицы 1 и Таблицы 2 показывает, что в настоящий момент наиболее загруженными диапазонами частот являются «С-диапазон» и «Ка-диапазон», а наиболее перспективными диапазонами являются «Ка-диапазон» и «Q/V-диапазон». Перспективы развития «Ка-диапазона» и «Q/V-диапазона» обусловлены возможностью реализации в них спутниковых сетей с высокой пропускной способностью за счет многократного использования радиочастотного спектра в многолучевых зонах покрытия.

Проведенный выше анализ позволяет задать вектор развития систем мониторинга и контроля космического пространства. Данные системы базируются на специальных радиолокационных станциях (РЛС). РЛС классифицируют по следующим признакам [2]:

- происхождению радиосигнала, принимаемого приемником РЛС;
- используемому диапазону (декаметрового, метрового, дециметрового, сантиметрового и миллиметрового диапазонов)
- виду зондирующего сигнала (с непрерывным (немодулированным или частотно-модулированным) и импульсным (некогерентным, когерентно-импульсным с большой и малой скважностью, с внутриимпульсной частотной или фазовой модуляцией) излучением);
- числу применяемых каналов излучения и приема сигналов (одноканальные и многоканальные с частотным или пространственным разделением каналов);
- числу и виду измеряемых координат (одно- двух-и трехкоординатные);
- способу измерения, отображения и съема координат объекта;
- месту установки РЛС (наземные, корабельные, самолетные, спутниковые);
- функциональному назначению РЛС (от малогабаритных переносных РЛС измерения скорости автомобилей до огромных наземных РЛС систем противовоздушной и противоракетной обороны).

Таблица 1

Распределение заявлений геостационарных спутниковых сетей по диапазонам частот за все время и за 2020 год

Диапазон частот, МГц		За все время		За 2020 год	
		Запросы о координации	Заявки на нотификацию	Запросы о координации	Заявки на нотификацию
L	1452-1492	111	19	27	2
	1518-1559	286	70	71	8
	1610-1660,5	198	54	50	4
	1668-1675	248	15	68	2
S	1980-2010	446	9	118	1
	2010-2025	26	2	5	0
	2120-2160	3	4	2	0
	2160-2170	19	4	2	0
	2170-2200	451	15	123	1
	2483,5-2500	166	16	45	1
	2500-2520	136	11	36	0

	2520-2535	23	7	6	0
	2655-2690	126	12	32	0
C	3400-4200	975	524	210	51
	4500-4800	0	3	0	0
	5000-5150	89	3	15	0
	5150-5250	1	0	1	0
	5250-5725	1	0	0	0
	5725-5850	582	84	134	8
	5850-6700	969	519	211	52
	6700-7075	830	94	173	7
X	7250-7750	490	135	68	14
	7900-8400	491	148	72	16
Ku	10700-12500	972	573	187	67
	12500-12750	899	346	179	34
	12750-13250	0	1	0	0
	13750-14500	968	585	128	65
	15300-15630	0	10	0	1
Ka	17300-17800	1116	129	236	22
	17800-19700	1195	227	246	42
	19700-20100	1197	212	169	44
	20100-20200	1202	209	146	43
	20200-21200	922	189	138	29
	24650-24750	661	5	167	2
	24750-25250	809	12	169	2
	27000-27500	868	35	184	12
	27500-29900	1205	199	163	47
	29900-30000	1193	179	146	45
	30000-31000	873	130	128	24
Q/V	37500-39500	924	0	213	0
	39500-43500	932	25	194	0
	43500-47000	823	73	156	5
	47200-49200	925	1	215	0
	49200-50200	925	0	216	0
	50400-51400	882	0	203	0
	51400-52400	57	0	57	0

Все вышеперечисленные классы РЛС по функциональному признаку можно разделить на следующие составные части: исполнительную, информационную и управляющую [2].

Исполнительная часть располагает некоторыми возможностями или ресурсами, расходующимися в соответствии с целевым назначением системы.

Информационная часть (радиолокационная система) доставляет в систему управления и непосредственно в исполнительную подсистему всю информацию о состоянии внешней среды (СВКН) и результатах взаимодействия с ней.

Управляющая часть перерабатывает информацию, поступающую от информационной и исполнительной части, и распределяет возможности и ресурсы информационной и исполнительной части в соответствии с полученной информацией.

Информационная часть РЛС базируется на антенной системе характеризующуюся следующими основными техническими характеристиками: коэффициент усиления антенны, форма диаграмма направленности, чувствительность, уровень боковых лепестков, рабочим диапазоном частот, коэффициент шума, коэффициент усиления [2, 3].

Для обеспечения контроля за существующим и вновь создаваемыми спутниковыми группировками, различными искусственными спутниками Земли (ИСЗ), антенная система РЛС должна обладать расширенным рабочим диапазоном частот, позволяющим обеспечить работу в С-, Ku-, Ka-, Q/V-диапазонах частот, и обладать высокими значения шумовой добротности.

Антенная система состоит из следующих основных элементов:

- основной рефлектор;
- опорно-поворотное устройство;
- облучающая система с облучателем;
- волноводный тракт;
- электропривод системы наведения антенны;
- систему наведения антенны.

Таблица 2

Распределение заявлений не геостационарных спутниковых систем по диапазонам частот за все время и за 2020 год

Диапазон частот, МГц		За все время			За 2020 год		
		Предварит. публикация	Запросы о координации	Заявки на нотификацию	Предварит. публикация	Запросы о координации	Заявки на нотификацию
L	1518-1559	2	41	4	2	12	0
	1610-	17	26	8	9	6	2
	1668-1675	0	32	1	0	9	0
	1930-1970	4	0	0	4	0	0
S	1980-2010	1	19	1	1	5	1
	2010-2025	4	14	5	3	3	4
	2120-2160	4	0	3	4	0	0
	2160-2170	1	13	3	1	3	0
	2170-2200	1	19	6	1	5	1
	2483.5-	10	20	4	4	5	1
	2500-2520	1	8	0	0	0	0
	2520-2535	1	2	0	0	0	0
	2655-2690	0	8	0	0	0	0
	3400-4200	32	0	6	7	0	0
C	4500-4800	0	0	1	0	0	0
	5000-5150	1	19	15	1	5	1
	5150-5250	1	26	12	0	6	2
	5250-5725	9	0	19	5	0	1
	5725-5850	19	0	7	3	0	0
	5850-6700	31	0	8	5	0	0
	6700-7075	1	29	7	0	5	0
	7250-7750	5	2	3	2	2	1
X	7900-8400	172	5	168	86	2	24
Ku	10700-	1	52	2	1	24	0
	12500-	0	50	0	0	25	0
	12750-	0	47	0	0	27	0
	13750-	1	53	5	1	26	0
	15300-	2	1	1	1	0	0
Ka	17300-	0	62	0	0	28	0
	17800-	6	91	19	1	38	2
	19700-	1	80	2	0	32	0
	20100-	1	81	2	0	33	0
	20200-	26	0	3	4	0	0
	24650-	14	0	1	5	0	0
	24750-	3	0	1	2	0	0
	27000-	18	1	5	8	0	1
	27500-	0	91	4	0	35	0
	29900-	2	80	0	1	34	0
	30000-	22	2	1	4	0	0
Q/V	37500-	20	0	30	7	0	28
	39500-	22	0	29	9	0	26
	43500-	15	0	11	8	0	7
	47200-	18	0	29	6	0	26
	49200-	17	0	30	6	0	27
	50400-	18	0	27	7	0	25

Для обеспечения работы антенной системы РЛС в расширенном рабочем необходимо провести исследования по нескольким направлениям, а именно: по созданию устройств разделения диапазонов; по созданию устройств разделения поляризаций, по созданию облучателей с расширенным рабочим диапазоном частот и др.

С целью создания широкополосного облучателя необходимо провести анализ существующих облучателей и их моделирование. Наиболее полно получить информацию об расчетно-технических характеристиках излучающих элементов, а также провести оценку их работы в составе комплексов возможно с применением вычислительных машинных методов расчета основанных на решении строгой задачи электродинамики с моделью, максимально приближенной к реальной, учетом граничных условий и источников возбуждения электромагнитных волн. Существующие на этой основе методы конечных элементов и методы моментов, методы матриц передачи, а также методы физической оптики, заложены в основу работы различных САПР, таких как, CST Microwave Studio (CST Design Studio Suite).

Поведенный анализ, по созданию широкополосных облучателей позволив определить следующие направления исследований и основные типы:

- логопериодическая антенная решетка петлевых вибраторов;
- коническая синусная антенна;
- совмещенная спиральная антенна;
- плоская сверхширокополосная логопериодическая
- плоская диэлектрическая антенна вытекающей волны;
- антенны на основе плавного перехода от микро полосковой линии к щелевой антенне.

В рамках исследований по повышению шумовой добротности земной станции было разработано специальное программное обеспечение и получено свидетельство о государственной регистрации программы для ЭВМ № 2019663787 от 23.10.2019 «Программа расчета двухзеркальной антенны с незамкнутыми противозумовыми экранами для земной станции спутниковой связи» и № 2019663623 от 21.10.2019 «Программа расчета эффективности незамкнутых экранов по периметру рефлектора зеркальной антенны». Данные программы позволили оценить повышение шумовой добротности антенных систем спутниковой связи при минимальном возможном уменьшении значения коэффициента усиления [6].

Заключение

Программа расчёта эффективности незамкнутых экранов с учётом конструктивных особенностей незамкнутого противозумового экрана по периметру рефлектора антенны позволяет рассчитать шумовую температуру антенны и шумовую добротность приёмной системы, определяющую качество приёма. В программе используются алгоритмы расчёта воздействия на антенну теплового излучения окружающей среды. Программа полезна специалистам спутниковых систем связи и может быть использована в учебных целях.

Программа расчёта двухзеркальной антенны с незамкнутыми противозумовыми экранами для земной станции спутниковой связи позволяет с высокой точностью оценить шумовую температуру антенны и всей приёмной системы земных станций спутниковой связи с геостационарной орбитой. При больших расстояниях от земной станции до спутника сигнал при распространении испытывает большое затухание, сравнимое по величине с мощностью естественных шумов, принимаемых антенной. Мощность этих шумов определяется действующей шумовой температурой окружающей антенну среды, зависит от диапазона рабочих частот, физического состояния почвы и атмосферы и конструктивных особенностей антенны. С учётом конструктивных особенностей антенны, а именно незамкнутых противозумовых экранов по нижней части периметров контррефлектора и рефлектора, программа позволяет рассчитать шумовую температуру антенны, шумовую добротность приёмной системы и выигрыш в шумовой добротности за счёт применения экранов. В программе используются алгоритмы расчёта воздействия на антенну теплового излучения окружающей среды, разработанные авторами.

Таким образом, как показывают приведенные анализ, исследования и разработанные в том числе и автором и защищенные патентами РФ технические решения, российская наука и промышленность в состоянии модернизировать существующие РЛС для обеспечения перспективного направления спутниковой составляющей ИКС.

Литература

1. Регламент Радиосвязи, Издание 2020 года, ISBN 978-92-61-30304-4, Электронная публикация МСЭ, Женева, 2020.
2. *Тяпкин В.Н., Фомин А.Н., Гарин Е.Н. и др.* Основы построения радиолокационных станций радиотехнических войск: учебник. Под общ.ред. В.Н. Тяпкина. Красноярск: Сиб.федер.ун-т. 2011. 536 с.
3. *Покрас А.М., Сомов А.М., Цуриков Г.Г.* Антенны земных станций спутниковой связи. М.: Радио и связь, 1985. 288 с.
4. *Сомов А.М., Воронцов А.П., Титовец П.А.* Программа расчета двухзеркальной антенны с незамкнутыми противозумовыми экранами для земной станции спутниковой связи, ЭВМ, патент № 2019663787 от 23.10.2019.
5. *Сомов А.М., Воронцов А.П., Титовец П.А.* Программа расчета эффективности незамкнутых экранов по периметру рефлектора зеркальной антенны, ЭВМ, патент № 2019663623 от 21.10.2019.
6. *Титовец П.А.* Методики повышения шумовой добротности осесимметричных зеркальных антенных систем земных станций спутниковой связи. Кандидатская на соискание ученой степени кандидата технических наук, 2020 – 155с, 09.10.2020 на заседании диссертационного совета Д 219.003.02 при Поволжском государственном университете телекоммуникаций и информатики в конференц-зале корпуса № 1 по адресу: Льва Толстого ул., д.23, г. Самара, 443010.

ПРОБЛЕМАТИКА ПОСТРОЕНИЯ ПЕРЕДАТЧИКОВ ЦИФРОВОГО РАДИОВЕЩАНИЯ ДИАПАЗОНА ОВЧ НА ОСНОВЕ ПОЛЯРНОЙ АРХИТЕКТУРЫ

Иванюшкин Роман Юрьевич,

Московский технический университет связи и информатики, доцент, к.т.н., Москва, Россия
rivanyushkin@gmail.com

Севериненко Александр Андреевич,

Московский технический университет связи и информатики, аспирант, Москва, Россия
kuju1ster@yandex.ru

Волков Иван Андреевич,

Московский технический университет связи и информатики, студент, Москва, Россия
ivan26897@outlook.com

Аннотация

Обсуждаются основные сложности, возникающие при реализации полярной архитектуры (на основе метода Л. Кана) в передатчиках цифрового радиовещания диапазона ОВЧ. Рассматривается не только проблематика специфических нелинейных искажений, возникающих при применении метода Л. Кана в усилителях мощности на современных полевых транзисторах, но и ограничения возможностей практического применения высокоэффективных ключевых усилителей мощности, как в радиочастотном канале полярных трактов, так и в канале огибающей.

Ключевые слова

Цифровое радиовещание, линейное усиление мощности, метод Л. Кана, полярная архитектура, ключевые усилители мощности, широтно-импульсная модуляция, нелинейные искажения, энергетическая эффективность.

Введение

Несмотря на массовый переход во многих странах, включая Россию, от аналогового эфирного телевизионного вещания к цифровому, в сфере звукового радиовещания этот процесс проходит существенно медленнее, несмотря на уже имеющийся положительный опыт многих стран в этом направлении. При этом, внедрение систем цифрового радиовещания в диапазонах НЧ-СЧ и ВЧ позволяет существенно улучшить качество получаемой радиослушателями аудиоинформации, а учитывая уникальные механизмы распространения декаметровых волн, обеспечивается широкий территориальный охват радиовещанием. На сегодняшний день, единственным рекомендованным Международным союзом электросвязи ITU стандартом цифрового радиовещания в вышеназванных диапазонах является стандарт DRM. Цифровое радиовещание на основе этого стандарта находит ограниченное применение в ряде стран. Во многих странах, включая и Российскую Федерацию [10-12] периодически осуществляется опытное / тестовое радиовещание на основе этого стандарта.

В отличие от диапазонов НЧ-СЧ и ВЧ, внедрение цифрового радиовещания в диапазоне ОВЧ не дает существенного выигрыша в качестве принимаемых радиослушателями передач. Однако, как и для случая внедрения цифрового эфирного телевизионного вещания, появляется возможность высвобождения ряда частотных каналов, занимаемых аналоговым радиовещанием, что является дополнительным стимулом для перехода от аналогового радиовещания к цифровому и в этом диапазоне. Среди стандартов цифрового радиовещания в диапазоне ОВЧ известны DAB/DAB+, DRM+(DRM Plus), а также отечественная разработка РАВИС.

Одной из проблем внедрения эфирного цифрового радиовещания в диапазоне ОВЧ является сложность обеспечения приемлемой энергетической эффективности радиовещательных пе-

редатчиков, по сравнению с построением передатчиков для аналогового радиовещания с частотной модуляцией, которая применяется в настоящее время. Если при усилении частотомодулированных радиосигналов высокая энергетическая эффективность обеспечивается за счет нелинейных режимов работы усилителей мощности [1] – применение граничного либо слабоперенапряженного режима с отсечкой выходного тока, то при усилении сложных радиосигналов OFDM, применяемых в системах цифрового радиовещания, требуется обеспечить высокую линейность усилительного тракта, что несовместимо с работой усилительных каскадов в нелинейных режимах [1]. В тоже время, низкая энергетическая эффективность тракта усиления мощности радиопередатчика приводит не только к повышению энергопотребления, но и к целому ряду других проблем. В первую очередь это касается проблематики теплоотведения от мощных усилительных элементов (транзисторов). Еще одной проблемой является неизбежное снижение использования усилительного прибора по мощности, которое ограничивается допустимыми тепловыми потерями на нем, с одной стороны, а с другой стороны – ростом нелинейных искажений, при приближении мгновенных значений амплитуды усиливаемого радиосигнала к точке компрессии.

В разные годы был разработан целый ряд специальных методов повышения коэффициента полезного действия усилителей мощности радиосигналов с меняющейся амплитудой [1], а также методов линеаризации усилителей мощности [1]. Большинство из этих методов нашли свое применение в радиопередатчиках различного назначения [1]. Так, например, при построении телевизионных передатчиков для цифрового эфирного телевидения, в настоящее время достаточно широко применяются линейные усилители мощности с повышенным КПД, которые строятся на основе схемы, предложенной еще в 1930-е годы инженером Уильямом Догерти [1, 2, 9].

Одним из наиболее известных и перспективных методов построения линейных усилителей мощности с повышенной энергетической эффективностью, является синтетический метод, предложенный в 1950-е инженером Л. Каном [1] и названный им «Устранение и восстановление огибающей» (Envelope elimination and restoration). В современной литературе, применительно к построению радиооборудования для цифровых телекоммуникаций и цифрового телерадиовещания, такой подход все чаще называют полярной модуляцией (поскольку передаваемый радиосигнал, на этапе его формирования методами цифровой обработки, формируется из отсчетов магнитуды и фазового угла текущего вектора сигнала), либо полярной архитектурой [1].

Основная часть

На сегодняшний день, на основе полярной архитектуры (с применением метода Л. Кана) строятся передатчики цифрового радиовещания диапазонов НЧ-СЧ и ВЧ [1], в том числе, предназначенные для работы в стандарте DRM. При построении таких передатчиков полярная архитектура оказывается достаточно легко реализуемой на практике, позволяя обеспечить высокую энергетическую эффективность тракта усиления мощности передатчика, при условии строго соблюдения требуемых показателей качества передаваемого сигнала, а также соответствия излучаемого радиопередатчиком спектра требованиям Норм электромагнитной совместимости. При этом, как тракт усиления огибающей передаваемого радиосигнала, так и тракт его фазомодулированного радиочастотного заполнения, строятся с применением высокоэффективных ключевых режимов работы усилительных приборов (транзисторов). В радиочастотном тракте применяются ключевые усилители мощности классов D и F (DF) [1, 3], а в тракте усиления огибающей – ключевые усилители (модуляторы) класса D с широтно-импульсной модуляцией [1, 4-6, 13-18].

В процессе обсуждения проблематики применения полярной архитектуры, применительно к построению радиовещательных передатчиков диапазона ОВЧ, целесообразно напомнить основные трудности практической реализации метода Л. Кана [1], поскольку именно они являются критическими, с точки зрения практической реализуемости этого метода, для тех или иных приложений.

Из наиболее известных проблем этого метода – специфические нелинейные искажения, вызываемые несинхронностью подачи на оконечный каскад передатчика (амплитудный модуля-

тор / перемножитель) огибающей и фазомодулированного заполнения усиливаемого радиосигнала [1]. При формировании этих составляющих методами цифровой обработки сигналов, главной причиной такой рассинхронизации являются задержки распространения огибающей сигнала в ключевом тракте ее усиления (в модуляторе класса D), и, в первую очередь, в его выходном фильтре нижних частот. Эта временная задержка зависит от текущего значения огибающей, а ее компенсация возможна введением цифровой временной и фазовой коррекции на этапе цифрового формирования передаваемого сигнала. Следует помнить, что чем выше верхняя частотная граница спектра огибающей передаваемого радиосигнала, тем более жесткие требования предъявляются к допустимой величине этой задержки, исходя из требований к показателям качества передаваемого радиосигнала (в частности, к коэффициенту ошибок модуляции MER), а также исходя из требований Норм электромагнитной совместимости (касаясь допустимого уровня излучений в соседний канал и других внеполосных составляющих радиоспектра излучаемого передающей станцией сигнала). С этой точки зрения, построение передатчиков цифрового радиовещания диапазона ОВЧ, потребует более точной временной синхронизации тракта огибающей, поскольку полоса радиовещательного сигнала существенно шире, чем для случая диапазонов НЧ-СЧ и ВЧ, и, соответственно, выше и верхняя частота спектра огибающей.

Другой проблемой являются нелинейные искажения, возникающие из-за амплитудно-фазовой конверсии [1, 2, 5]. По сравнению с линейным усилением радиосигналов с непостоянной огибающей (как классических [1], так и с автоматической регулировкой режима [1, 2, 4, 5, 9], а также построенных по схеме У. Догерти [1, 2, 9]), в трактах усиления мощности, построенных на основе метода Л. Кана, фазоамплитудные нелинейные искажения должны проявляться в меньшей степени. Это связано с тем, что в отличие от других вышеуказанных подходов к построению линейных усилителей мощности, при полярной архитектуре амплитуда напряжения возбуждения усилительных приборов (транзисторов) окончного каскада передатчика постоянная (поскольку огибающая фазомодулированного заполнения постоянна), а переменная амплитуда возникает только в выходной цепи усилительного прибора, где огибающая усиленного радиосигнала восстанавливается (из ШИМ-последовательности) путем амплитудной модуляции по питанию (стоковой, коллекторной, анодной) окончного каскада усиления мощности радиочастотного тракта. Таким образом, в усилительных трактах, построенных на основе метода Л. Кана, амплитудно-фазовая конверсия возникает, в основном, за счет нелинейности выходных вольт-фарадных характеристик усилительных приборов окончного каскада передатчика, а нелинейность их входных вольт-фарадных характеристик, в первом приближении, можно не учитывать.

Компенсацию фазо-амплитудных искажений также целесообразно осуществлять методами цифровой фазовой предкоррекции, на этапе цифровой обработки и формирования передаваемого радиосигнала. Дополнительно, следует обратить внимание на то, что вольт-фарадные характеристики современных мощных радиочастотных полевых транзисторов (являющихся, на сегодняшний день, наиболее часто используемыми усилительными приборами для построения тракта усиления мощности радиопередатчиков) существенно нелинейные [8]. Нелинейности этих характеристик могут приводить к специфическим нелинейным искажениям, при усилении радиосигналов с непостоянной огибающей. В отличие от усилителей с распределенным усилением, в более простых схемах каскадов усиления радиочастоты, рассмотренные в [8] специфические параметрические нелинейные искажения проявляются менее существенно. Но, при разработке мер линеаризации линейных усилителей мощности, не следует пренебрегать учетом нелинейностей вольт-фарадных характеристик полевых транзисторов.

Одной из наиболее существенных проблем, возникающих при построении радиопередатчиков с полярной архитектурой, являются требования к полосе пропускания тракта огибающей. С точки зрения обеспечения восстановления усиливаемого радиосигнала на выходе схемы Л. Кана, необходимо обеспечить в тракте огибающей прохождение, по крайней мере, первых пяти гармоник спектра огибающей усиливаемого радиосигнала. При узкой полосе радиоканала это не представляет проблем. Так, при цифровом радиовещании в диапазонах НЧ-СЧ и ВЧ, где ширина полосы частот, занимаемой радиоканалом, составляет не более 10 кГц. Требуемая ши-

рина полосы пропускания тракта огибающей составляет 50 кГц. При этом, ключевые усилители-модуляторы класса D, работающие в тракте огибающей, обеспечивают коэффициент полезного действия около 95%, поскольку максимальная тактовая частота широтно-импульсной управляющей последовательности составляет не более 400 кГц (т. е. в 8 раз выше верхней частоты спектра в тракте огибающей).

При построении передатчиков цифрового радиовещания диапазона ОВЧ, где ширина полосы частот, занимаемой радиоканалом, может составлять от 150 кГц до 300 кГц, ситуация уже совершенно иная. В этом случае требуется обеспечить полосу пропускания канала огибающей от 750 кГц до 1,5 МГц. Тактовая частота управляющих импульсов потребуется уже от 6 МГц до 12 МГц. При таких значениях тактовой частоты широтно-импульсной последовательности, энергетическая эффективность ключевых усилителей-модуляторов класса D окажется намного хуже, чем для случаев передатчиков диапазонов НЧ-СЧ и ВЧ. А поскольку общая энергетическая эффективность радиопередатчика с полярной архитектурой определяется произведением коэффициентов полезного действия оконечного усилителя мощности радиочастотного тракта и ключевого модулятора класса D, общий энергетический выигрыш от применения метода Л. Кана окажется весьма несущественным, а его применение – бессмысленным.

В этой связи, представляется весьма актуальным построение передатчиков цифрового радиовещания диапазона ОВЧ с автоматической регулировкой режима работы линейного усилителя мощности по питанию [1, 4, 5]. В этом случае, требования к ширине полосы пропускания тракта огибающей снижаются до 5 раз, что позволяет строить высокоэффективный ключевой тракт управления напряжением питания мощных усилительных каскадов передатчика. Разумеется, при построении радиопередатчиков широкополосных сигналов (например, передатчиков эфирного цифрового телевидения, где ширина полосы частот радиоканала может достигать 8 МГц), изложенная выше проблема низкой эффективности ключевых модуляторов класса D (для тракта огибающей в полярной архитектуре) становится совершенно непреодолимой (при применении «традиционного» подхода к построению ключевых модуляторов класса D).

В тоже время, на сегодняшний день известны различные способы повышения энергетической эффективности ключевых усилителей-модуляторов класса D, для случаев, когда требуется обеспечить широкую полосу усиливаемого ими сигнала [6, 7]. Кроме вполне очевидных решений, связанных с применением сверхбыстродействующих ключевых транзисторов (например, полевых транзисторов с высокой подвижностью электронов НЕМТ), существуют и другие решения. Прежде всего это относится к применению так называемой многофазной широтно-импульсной модуляции. С одной стороны, это ведет к усложнению схемы и конструкции оконечного ключевого каскада модулятора класса D, поскольку теперь, вместо одного модуля ключевых транзисторов, потребуется устанавливать несколько (N модулей). Однако, с другой стороны, при многофазной реализации, тактовая частота управляющей широтно-импульсной последовательности, подаваемой на вход каждого из таких модулей, оказывается в N раз ниже, по сравнению с «классической» «однофазной» схемой усилителя-модулятора класса D.

В этой связи, развитие этой технологии позволит решить проблему низкой энергетической эффективности ключевых модуляторов класса D, когда требуется обеспечить достаточно широкую полосу пропускания в тракте огибающей. Так, например, если в вышеприведенном примере передатчика цифрового радиовещания диапазона ОВЧ, требуется тактовая частота управляющей широтно-импульсной последовательности, равная 12 МГц, то при применении многофазного ключевого модулятора с N=4, требуемая тактовая частота снизится до 3 МГц, что вполне позволяет реализовать высокоэффективные ключевые модуляторы класса D, особенно учитывая современные технологии создания быстродействующих мощных полевых транзисторов. Возможность практической реализации передатчиков диапазона ОВЧ на основе полярной архитектуры, позволит улучшить показатели, по сравнению с применением метода автоматической регулировки режима.

Также очевидны и перспективы применения многофазных ключевых модуляторов класса D при реализации автоматической регулировки режима по питанию в усилителях мощности передатчиков цифрового телевидения: как «классических» линейных усилителей мощности, так и усилителей мощности, построенных по схеме У. Догерти [1, 2, 9].

При реализации полярной архитектуры предъявляются достаточно жесткие требования и к полосе пропускания радиочастотного тракта фазомодулированного заполнения. Если ширина полосы пропускания тракта огибающей должна быть в пять раз шире полосы частот радиоканала, то в радиочастотном тракте, при реализации метода Л. Кана, ширина полосы пропускания должна быть еще в два раза шире. Разумеется, это создает дополнительные сложности при реализации радиочастотных трактов передатчиков с полярной архитектурой, но методы решения задач построения широкополосных усилителей мощности достаточно хорошо известны и отработаны [1].

Не менее важной проблемой (как и рассмотренной выше проблематики построения ключевых усилителей-модуляторов класса D для передатчиков с полярной архитектурой), является обеспечение высокой энергетической эффективности радиочастотного тракта усиления фазомодулированного заполнения усиливаемого радиосигнала, а также оконечного каскада передатчика, в котором осуществляется восстановление передаваемого радиосигнала методом амплитудной модуляции по питанию (стоковой, коллекторной, анодной). С одной стороны, здесь можно пойти по тому же пути, что и при построении ныне находящихся в эксплуатации передатчиков аналогового радиовещания диапазона ОВЧ с частотной модуляцией, т. е. строить эти каскады усиления на основе «классических» «неключевых» подходов, добиваясь относительно высокой энергетической эффективности путем применения граничного и слабоперенапряженного режимов их работы с отсечкой выходного тока (т. е. при работе в классах В и С).

Применение более энергетически эффективных ключевых радиочастотных усилителей мощности (генераторов) [1] на частотах выше 30 ÷ 50 МГц всегда считалось затруднительным, вследствие существенного снижения их энергетического выигрыша с ростом рабочей частоты (прежде всего, за счет коммутативных и инерционных потерь в транзисторах [1]). Эти ограничения, относятся, в первую очередь к ключевым усилителям классов D и F (DF) [1], а также к некоторым их модификациям. В тоже время, ключевые усилители класса E [1] являются достаточно высокочастотными, поскольку принцип их действия подразумевает практически полное исключение коммутативных потерь. Однако, такие усилители, по своей сути, являясь резонансными, обладают существенным недостатком – узкополосностью, в то время как для радиовещательных передатчиков диапазона ОВЧ целесообразно строить универсальный тракт усиления мощности радиочастоты, не требующий точной настройки под конкретный радиоканал.

С учетом современных тенденций развития, как быстродействующих мощных радиочастотных полевых транзисторов, так и различных модификаций ключевых усилителей мощности, появляется смысл обсуждать и альтернативные возможности применения ключевых усилителей в радиочастотных трактах передатчиков диапазона ОВЧ. Кроме того, что новые разработки в области радиочастотных транзисторов (прежде всего уже упоминавшиеся выше полевые транзисторы с высокой подвижностью электронов НЕМТ), позволяют добиться значительного снижения частотозависимых потерь в ключевых схемах, а, следовательно, и заметного повышения энергетической эффективности ключевых усилителей мощности классов D и F (DF), также существует целесообразность рассмотреть вопрос применения (при построении радиопередатчиков в этом диапазоне частот) так называемых «модифицированных» схем ключевых усилителей классов DE и FE [1, 3].

Такие разновидности ключевых усилителей мощности, с одной стороны, обладают более высоким коэффициентом полезного действия на повышенных частотах (по сравнению с ключевыми усилителями классов D и F), а, с другой стороны, они не обладают столь явно выраженной узкополосностью, как ключевые усилители класса E. Более низкие потери ключевых усилителей мощности классов DE и FE на высоких частотах обусловлены особенностями их схемотехники [1]. Как и в случае ключевых усилителей класса E, в схемах усилителей классов DE и FE присутствует так называемый формирующий контур. Однако, в отличие от усилителей класса E, этот контур включается в работу только во время процессов переключения транзистора, когда требуется снижать коммутативные потери. Коэффициент полезного действия таких «модифицированных» ключевых усилителей мощности, при работе на частотах диапазона ОВЧ, оказывается выше, чем у ключевых усилителей классов D и F, но ниже, чем у ключевых усилителей класса E.

С одной стороны, применение ключевых усилителей классов DE и FE позволит упростить задачу построения передатчиков цифрового радиовещания диапазона ОВЧ на основе полярной архитектуры, но, с другой стороны, это может привести к усложнению передатчика и к некоторому ухудшению его эксплуатационных свойств, поскольку такие «модифицированные» ключевые усилители, все же, требуют достаточно сложной настройки (хотя и более простой, по сравнению с ключевыми усилителями класса E). Тем не менее, в ближайшем будущем заведомо предвидится дальнейшее улучшение частотных свойств ключевых усилителей мощности радиосигналов, что будет способствовать более широкому их применению при построении радиопередатчиков диапазона ОВЧ (в том числе и для цифрового радиовещания).

Заключение

Рассмотренная проблематика применения полярной архитектуры, при построении передатчиков цифрового радиовещания диапазона ОВЧ, показывает основные направления перспективных разработок, направленных, как на упрощение практической реализации таких передатчиков, так и, разумеется, на дальнейшее повышение их энергетической эффективности. Во многом, решению обозначенных задач будет способствовать дальнейшее развитие технологий мощных радиочастотных полевых транзисторов, направленных в сторону дальнейшего повышения их быстродействия.

В тоже время, в последние два десятилетия наблюдается достаточное интенсивное развитие техники радиочастотных ключевых усилителей мощности, что сопровождается, как разработкой новых схем таких усилителей, так и различных модификаций самих ключевых режимов работы усилителей. Во многом, повышенное внимание разработчиков и исследователей по всему миру к радиочастотным ключевым усилителям мощности определяется и все более широкими возможностями применения различных синтетических нелинейных методов линейного усиления (включая и применение полярной архитектуры, на основе метода Л. Кана) применительно к передатчикам современных сложных радиосигналов цифровых телекоммуникаций, включая телерадиовещание.

Литература

1. Дингес С.И., Иванюшкин Р.Ю., Козырев В.Б. и др. Радиопередающие устройства. Учебник для вузов. Под общей редакцией Иванюшкина Р.Ю. М.: Горячая линия: Телеком, 2019. 1200 с.
2. Иванюшкин Р.Ю., Разин К.О. Исследование нелинейных искажений в усилителе мощности по схеме У. Догерти с двойной автоматической регулировкой режима по питанию // Технологии информационного общества: Сборник трудов XIV отраслевой научно-технической конференции. М.: Издательский дом Медиа паблишер, 2020. С. 184-186.
3. Иванюшкин Р.Ю., Терёшин М.Н. Компьютерное моделирование ключевых усилителей мощности классов D и DE для передатчиков цифрового радиовещания диапазона ОВЧ // Всероссийская конференция: «Радиоэлектронные устройства и системы для инфокоммуникационных технологий – РЭУС-2020», доклады. М.: РНТОРЭС им. А.С. Попова, 2020. С. 122-126.
4. Иванюшкин Р.Ю., Дулов И.В. Исследование энергетической эффективности передатчика цифрового радиовещания с автоматической регулировкой режима по питанию. // Электросвязь. 2013. № 1. С. 46-47.
5. Дулов И.В., Иванюшкин Р.Ю. Нелинейная АРР по питанию для усилителя мощности передатчика цифрового радиовещания // Т-Comm: Телекоммуникации и транспорт. 2013. Т. 7, № 9. С. 63-69.
6. Берман А.А., Иванюшкин Р.Ю. Проблематика построения тракта огибающей передатчиков с полярной архитектурой для цифрового радиовещания в диапазоне ОВЧ // Телекоммуникации и информационные технологии. 2016. Т. 3. № 2. С. 47-48
7. Волков И.А., Иванюшкин Р.Ю., Мусатов К.В. Разработка модели многофазного широтно-импульсного модулятора, на основе ПЛИС, для высокоэффективного ключевого усилителя звуковой частоты / Физика, техника и технология сложных систем: тезисы докладов Всероссийской с международным участием молодежной научно-практической конференции. Под редакцией С.П. Зимина, А.С. Гвоздарева. Ярославль: Ярославский государственный университет им. П.Г. Демидова, 2020. С. 166-167.

8. *Иванюшкин Р.Ю., Шмаков Н.Д.* Компьютерное моделирование и исследование параметрических нелинейных искажений в усилителях с распределенным усилением ВЧ-ОВЧ диапазона // Системы синхронизации, формирования и обработки сигналов. Т. 11. № 1, 2020. С. 50-56.
9. *Разин К.О., Иванюшкин Р.Ю.* Повышение энергетической эффективности линейного усилителя мощности У. Догерти методом двойной автоматической регулировки режима по питанию // Международная научно-техническая конференция "Перспективные технологии в средствах передачи информации" – ПТСПИ-2019. 2019. Т. 2. С. 253-256.
10. *Варламов О.В.* Организация одночастотных сетей цифрового радиовещания стандарта DRM. Особенности и результаты практических испытаний // Т-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 11. С. 4-20.
11. *Варламов О.В.* Технология создания сети цифрового радиовещания стандарта DRM для Российской Федерации // Диссертация на соискание ученой степени доктора технических наук / Московский технический университет связи и информатики. Москва, 2017
12. *Варламов О.В., Варламов В.О., Долгопятова А.В.* Международная сеть DRM вещания для создания информационного поля в арктике // Т-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 9. С. 9-16.
13. *Иванюшкин Р.Ю., Юрьев О.А.* Перспективы применения ключевых усилителей мощности классов D и DE при построении радиовещательных передатчиков диапазона ОВЧ // Т-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 5. С. 21-26.
14. *Иванюшкин Р.Ю., Разин К.О., Шмаков Н.Д.* Перспективные пути построения тракта усиления мощности передатчиков эфирного цифрового телевизионного вещания // Системы синхронизации, формирования и обработки сигналов. 2018. Т. 9. № 3. С. 96-103.
15. *Иванюшкин Р.Ю., Юрьев О.А.* Способы построения передатчиков цифрового радиовещания диапазона ОВЧ // Системы синхронизации, формирования и обработки сигналов. 2016. Т. 7. № 1. С. 27-29.
16. *Разин К.О., Иванюшкин Р.Ю.* Энергетический выигрыш от введения автоматической регулировки режима по питанию в линейный усилитель мощности по схеме У. Догерти // Телекоммуникации и информационные технологии. 2019. Т. 6. № 2. С. 12-18.
17. *Холюков Р.Г., Варламов О.В.* Разработка формирователя ШИМ сигнала с дополнительной дельта-сигма модуляцией на ПЛИС и измерение его характеристик // Системы синхронизации, формирования и обработки сигналов. 2019. Т. 10. № 5. С. 79-84.
18. *Варламов О.В., Чузунов И.В.* Моделирование энергетических характеристик УКВ усилителя мощности класса D с сигма-дельта модулятором // Системы синхронизации, формирования и обработки сигналов. 2017. Т. 8. № 2. С. 14-18.

ВЫДЕЛЕНИЯ ПЕРИОДИЧЕСКОГО СИГНАЛА ИЗ ШУМОВ НЕЙРОФИЛЬТРОМ НА КONTИНУАЛЬНЫХ ПРОЦЕССОРАХ

Дембицкий Николай Леонидович,

Московский авиационный институт, доцент, к.т.н., Москва, Россия,

ndembitsky@gmail.com

Аннотация

В статье представлено решение задачи выделения периодических сигналов из помех высокой интенсивности с применением обучаемых аналоговых нейроподобных устройств. Целью разработки являются: достижение эффективных показателей распознавания сигнала сигналов, сочетание быстрого действия вычислений со снижением функциональной и конструктивной сложности устройства.

Ключевые слова:

Радиолокационные системы, выделение сигнала из шума, аналоговые сигналы, нейрофильтр, континуальные процессоры.

Введение

Совершенствование радиолокационных систем связывают с развитием цифровой обработки информации [3]. Цифровые устройств и микропроцессоры стали основными компонентами большинства радиосистем. Во многом благодаря высокому быстродействию вычислительных систем и мощному программному обеспечению современные РЛС осуществляют обнаружение и распознавание объектов на больших и сверхбольших расстояниях в условиях интенсивных помех [4]. В них все более важную роль играют методы искусственного интеллекта, а применение нейроподобных устройств является одним из перспективных направлений обработки радиосигналов сигналов [2]. Являясь перспективным направлением развития нового поколения вычислительной техники, нейропроцессоры начинают завоевывать области применения, в которых решаются очень сложные математические и логические задачи. К таким областям относятся системы управления, распознавания образов, системы коммутации в сетях передачи данных, радиолокация и др. [1, 2]. В наибольшей степени преимуществ нейрочипов проявляется во встроенных системах.

В природе нейронных сетей изначально заложен принцип параллельной обработки информации. Поступающие на вход сигналы мгновенно меняют состояние всех ее компонентов (нейронов). В цифровых системах последовательный характер вычислений, задержки передачи импульсов и сложные алгоритмы могут существенно снизить быстродействие искусственной нейросети. Особенно сильно ограниченные возможности цифровых процессоров проявляются в малогабаритной цифровой аппаратуре. В условиях жестких ограничений на объем, вес и энергопотребление аппаратуры сложно обеспечить распараллеливание вычислений. Возникает необходимость искать альтернативные технологии повышения быстродействия.

В данной статье представлено решение задачи распознавания сигналов в интенсивных помехах с применением обучаемых аналоговых нейроподобных устройств. Целью разработки являются: достижение высоких показателей распознавания сигнала сигналов и быстродействия вычислений в сочетании со снижением функциональной и конструктивной сложности. Поставленная цель достигается отказом от оцифровки сигналов и заменой программно-алгоритмических методов аппаратной реализацией нейронного фильтра, применением аналоговой логики управления устройством.

Постановка задачи

Рассмотрим периодический полезный сигнал $X(t)$ с периодом повторения T и помеху $Y(t)$, поступающие на вход системы распознавания. Их комбинация аддитивная $Z(t)=X(t) + Y(t)$ или мультипликативная $Z(t)=X(t) \cdot Y(t)$ должна быть обработана за время, не превышающее $\tau = m \cdot T$, которое определяется задачей, решаемой системой распознавания сигнала, где m – это количество циклов обработки. Периодический сигнал $X(t)$ представлен функцией $f(t)$, определенной на интервале $[0, T]$. Помеха $Y(t)$ может быть либо аperiodическим сигналом, либо периодическим сигналом с периодом повторения, не равным T , либо белым шумом.

Пусть в моменты времени $t_1, t_1+T, t_1+2 \cdot T, \dots, t_1+n \cdot T$ накапливаются и вычисляются средние значения

$$Z_{cp} = \frac{\sum_{i=1}^n Z(t_1+iT)}{n} \quad (1)$$

входного сигнала $Z(t)$. При достаточно большом объеме обработанных данных, то есть при достаточно больших $n > N$, накопленное среднее значение $Z_{cp}(t)$ будет стремиться к значению периодического полезного сигнала $X(t)$ в моменты времени $t_1+N \cdot T, t_1+(N+1) \cdot T, (N+2) \cdot T, \dots$ Воспользуемся этим свойством периодического сигнала для его выделения из помех.

В фильтре сигнала за промежуток времени T необходимо выполнить следующие операции: считывание исходных данных из оперативной памяти, вычисление по формуле (1), запись результатов в оперативную память. При аппроксимации функции $f(t)$ перечисленные операции должны быть выполнены в k точках каждого временного интервала T .

Если реализовать рассматриваемые вычисления с помощью цифровых процессоров, то расчетным операциям следует добавить оцифровку значений сигнала в каждой точке вычислений. Тогда время выделения периодического сигнала из помехи методом накопления данных можно рассчитать по формуле

$$T_p = (\tau_{АЦП} + \tau_{В} + \tau_{З}) \cdot N_p, \quad (2)$$

где $\tau_{АЦП}$ – время аналогово-цифровых преобразований, $\tau_{В}$ – время работы программы вычисления усредненных значений сигнала, $\tau_{З}$ – время записи усредненного значения в оперативную память, N_p – количество циклов накопления для уверенного распознавания сигнала.

Формула (2) задает ограничение возможности распознавания периодического сигнала статистическим методом с помощью цифровых технологий, т.к. быстродействие процессора для уверенного распознавания должно обеспечивать выполнение неравенства $T_p < T_3$, где T_3 – максимальное время решения тактической задачи. Неравенство определяет требование по быстродействию фильтра сигнала, выполняющего программно-алгоритмическое распознавание периодического сигнала на фоне помех. В малогабаритной аппаратуре существуют ограничения на вычислительные возможности цифрового процессора. Это может стать критическим фактором снижения эффективности обработки сигнала. Ниже рассмотрим методологию решения задач выделения сигнала из помех, устраняющую противоречие между быстродействием и конструктивными ограничениями.

Континуальный процессор системы распознавания сигналов

Основными преимуществами искусственных нейронных сетей являются способность обучения и самообучения решению ряда трудно формализуемых и требующих сложных алгоритмов задач. Благодаря этим возможностям нейросетевые технологии открывают новые перспективы в адаптивном управлении, классификации, распознавании и идентификации объектов. К данному классу задач можно отнести и задачу выделения полезного сигнала из помех.

Распознавание радиосигнала на фоне интенсивных шумов с отношением сигнал-шум менее 1 дБ требует высокого быстродействия процессоров. В нейроподобных структурах на цифровых процессорах вычисления в целом носят последовательный характер, которые определяют ограничения на скорость решения задачи. Применение многопроцессорных систем позволяет значительно увеличить быстродействие нейронных сетей [5, 6]. Вместе с тем повышение вычислительной мощности приводит к росту энергетических затрат и увеличению массогабаритных параметров устройств распознавания. Это противоречие в наибольшей степени заметно в малогабаритной аппаратуре, например, в аппаратуре беспилотных летательных аппаратов.

В природе аналоговых схем изначально заложен принцип параллельности вычислений, что позволяет считать их применение одним из наиболее перспективных направлений развития систем искусственного интеллекта [7]. *Континуальные системы* формируются на основе непрерывных сред (физических полей), свойства которые определяются физикой процессов и в общем виде они выполняют операцию пространственно-временного функционального преобразования сигналов [8]. Создание такой среды является сложной теоретической и технологической задачей.

В данной статье рассматривается подход к созданию среды на основе континуальной модели вычислений, образованной аналоговыми вычислительными устройствами, выполняющими функционально-логические преобразования аналоговых сигналов без их оцифровки.

Континуальный процессор (КП) является развитием принципов аналоговых вычислений в область логической обработки результатов. Основным отличием КП от существующих аналоговых процессоров [9] является способность ситуационного моделирования во временном континууме систем взаимодействующих физических процессов (СВП) $\Pi(t) = \{\Pi_1(t), \Pi_2(t), \dots, \Pi_S(t)\}$. Благодаря соединению функциональных преобразований и логических процедур в непрерывных вычислениях (без квантования временных интервалов и уровней напряжения), устройство воспринимается как единый информационный объект, который в реальном времени реагирует на изменения физических параметров. КП является аналоговой моделью непрерывных процессов и поэтому может встраиваться в любые СВП в виде адекватной математической модели реального времени. При этом вычислительная система становится частью непрерывных физических процессов, образуя киберфизическую систему. С позиций вычислительной математики КП является интерполятором табулированных функций. С позиций моделируемых процессов КП является логическим устройством управления СВП. С позиций когнитивной логики КП обладает возможностями самоорганизации, может накапливать информацию и настраиваться на решение конкретных задач по результатам экспериментальных исследований моделируемых процессов, обучаться и самообучаться.

Управление работой КП осуществляется по правилам предикатной логики. Передача значения расчетного параметра r на выход устройства происходит только в том случае, если выполняются все условия вычислений. Если условия не выполняются вывод расчетного параметра r блокируется размыканием ключа.

Организация памяти нейрофильтра сигналов

Для КП ключевым компонентом является запоминающее устройство, которое записывает, хранит и считывает аналоговые значения параметров. В известных устройствах аналоговая память обычно использует различные эффекты накопления зарядов [10, 11]. Такой подход имеет ряд существенных недостатков: малое время хранения информации, большие габариты, низкая скорость записи и считывания.

В рассматриваемой системе распознавания сигналов используются специально разработанные ячейки памяти, выполняющие преобразование напряжений в фазовые сдвиги генератора пилообразного напряжения. Запоминаемое напряжение $U_{\text{вых}}$ находится в диапазоне значений $[-E; E]$ и формируется в виде суммы двух линейно изменяющихся напряжений $U_1(t)$ и $U_2(t)$ с одинаковой амплитудой $2E$, периодом T_T и сдвинутых относительно друг друга на временной интервал τ

$$U_{\text{вых}}(t) = \begin{cases} U_1(t) + U_2(t) & \text{при } \delta + nT_r \leq t < (n+1)T_r \\ 2E + U_1(t) + U_2(t) & \text{при } (n+1)T_r \leq t < \delta + (n+1)T_r \end{cases}, \quad (3)$$

где задержка $\delta < T_r$ определяет значение записанного напряжения.

Линейно нарастающее напряжение $U_1(t)$, изменяется по закону

$$U_1(t) = \begin{cases} -E & \text{при } t = nT_r^+ \\ (-1 + 2\frac{t - nT_r}{T})E & \text{при } nT_r < t < (n+1)T_r \\ E & \text{при } t = (n+1)T_r^- \end{cases} \quad (4)$$

Линейно нарастающее напряжение $U_2(t)$, изменяется по закону

$$U_2(t) = \begin{cases} 0 & \text{при } t = \delta + nT_r^+ \\ -2\frac{t - nT_r - \delta}{T}E & \text{при } \delta + nT_r < t < \delta + (n+1)T_r \\ -2E & \text{при } t = \delta + (n+1)T_r^- \end{cases} \quad (5)$$

Записанное в ячейке напряжение можно менять, регулируя фазовый сдвиг δ напряжений $U_1(t)$ и $U_2(t)$. В отличие от конденсаторных ячеек предлагаемый способ не требует инерционного накопления зарядов на обкладках конденсатора. Управление процессом записи выполняется аналоговым автоматом, который при изменении фазового сдвига δ переходит в новое устойчивое состояние, генерируя соответствующее ему постоянное напряжение $U_{\text{вых}}$. Максимальная задержка перехода из одного состояния в другое не превышает период T_r . Уход значения напряжения $U_{\text{вых}}$ определен стабильностью и симметрией параметров генераторов.

В памяти построенного на основе КП нейронного фильтра (НФ) хранятся узловые значения $f_1^*, f_2^*, \dots, f_N^*$ функции $f(t)$, моделирующей полезный сигнал $X(t)$ в фиксированные моменты времени t_1, t_2, \dots, t_N периода T . Соседние узлы используются для вычисления промежуточных значений функции $f_i(t)$ сплайна в интервале (t_i, t_{i+1}) . Количество расчетных узлов сплайна зависит от метода интерполяции.

Структура и принцип работы самообучаемого нейрофильтра выделения периодических сигналов из помех

Цифровая обработка сигналов имеет фундаментальную теоретическую и практическую базу. Перевод анализа сигнала в частотную область и цифровые методы являются основой построения большинства существующих радиотехнических систем. Высокая скорость обработки сигналов в КП позволяет применять их для решения задачи распознавания периодического сигнала во временной области.

В режиме самообучения (Рис.1) на вход НФ в течение каждого периода T непрерывно поступает смесь радиосигнала с помехой $Z(t)$. Сигнал $Z(t)$ подается на вход сумматора. На инверсный вход сумматора подается сигнал $f(t)$, интерполирующий записанные в памяти узловые значения $f_1^*, f_2^*, \dots, f_N^*$ табулированной модели сигнала. Каждое узловое напряжение привязано к одному из моментов времени $t_0, t_0 + \tau, t_0 + 2\tau, \dots, t_0 + n\tau$ периода сигнала. Разность напряжений

$$\varepsilon(t) = Z(t) - f(t) \quad (6)$$

является невязкой. Невязка непрерывно подается на вход блока вычисления узловых невязок ε_j^* сплайна интервала интерполяции. Полученная в результате усреднения невязка сплайна

$$\varepsilon_j^* = \frac{1}{\tau} \int_{t_i}^{t_i + \tau} \eta_j(t) \cdot \varepsilon(t) dt \quad (7)$$

используется для корректирования значений узловых напряжений в окрестности интервала интерполяции, где η_j – коэффициент обучения j -го узла, зависящий от его положения относительно момента времени t .

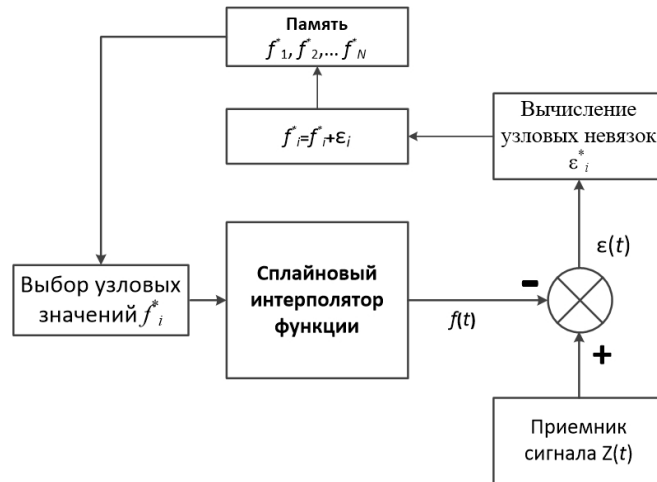


Рис. 1. Обучение нейрофильтра поступающим сигналом

С позиций управления НФ является киберфизической системой, в которой физические и вычислительные процессы взаимодействуют при выполнении связанных функционально-логических преобразований сигналов. Функциональные преобразования включают в себя интерполяционную генерацию функции сигнала и формирование в памяти узловых напряжений с помощью фазовых сдвигов пилообразных сигналов (3-5). Встроенная в процесс логическая составляющая управляет режимами работы НФ.

В существующих киберфизических системах интеграция вычислительных и физических процессов осуществляется на основе цифровых технологий встраиванием цифровых контроллеров в контур управления [12]. Хотя современные микропроцессорные системы обладают достаточно высокой производительностью их быстродействие не всегда может обеспечить требуемую скорость взаимодействия физических процессов. В радиотехнических цепях это ощущается особенно сильно. Для их успешного взаимодействия требуются согласованная обработка сигналов в реальном масштабе времени с задержками, не превышающими 10^{-6} - 10^{-9} с.

В контуре самообучения НФ задержка формирования и записи невязки ε не должна превышать период дискретизации сигнала. Для вычисления предельного быстродействия НФ необходимо связать эти задержки с периодом повторения распознаваемого сигнала.

В отличие от цифровых систем сплайновые интерполирующие генераторы не требуют высоких тактовых частот дискретизации. За счет эффекта сглаживания небольшое количество выборок вполне могут обеспечить передачу формы сигнала. В сплайновых моделях количество выборок зависит от вида аппроксимируемой функции. Например, сплайновая модель пилообразного напряжения для адекватного воспроизведения параметров задания потребует всего трех узлов. Если функция достаточно гладкая, то в модели можно снизить частоту дискретизации. Например, для точного воспроизведения синусоиды на период потребуется не более одного-двух десятков значений.

В НФ обучение происходит на множестве узловых напряжений $f_1^*, f_2^*, \dots, f_N^*$ внутри периода сигнала T . В каждом интервале $[t_i, t_{i+1}]$ вычисляется невязка, которая складывается с крайними значениями

$$f_i^* = f_i^* + \varepsilon_i^*, f_{i+1}^* = f_{i+1}^* + \varepsilon_i^* \quad (8)$$

Предельные возможности НФ по частоте следования импульсов распознаваемого периодического сигнала определяется частотными свойствами сплайнового интерполятора и

формой распознаваемого сигнала. В сплайновом интерполяторе применяются интеграторы узловых напряжений, максимальная частота работы которых ограничена частотой среза, которая подбором элементов поднимается до ста МГц.

При выделении сигнала из помех за одну эпоху обучения выполняется N операций вычисления невязок. С учетом предельных частотных свойств сплайновых интерполяторов частота следования импульсов распознаваемого сигнала находится в мегагерцовом диапазоне. Следует заметить, что при расширении спектра сигнала количество узлов интерполяции N увеличивается, что приведет к ограничениям на минимально допустимую частоту импульсов.

Минимальное допустимое время срабатывания НФ в режиме самообучения должна быть менее T/N . Отсюда можно выполнить расчет максимальной частоты распознаваемых периодических сигналов. Быстродействие НФ определяется скоростью записи узловых невязок ε_j^* в память. Для этого необходимо скорректировать фазовый сдвиг генератора линейно возрастающего напряжения $U_2(t)$. Максимальное время изменения узлового напряжения ограничивается периодом генерирования линейного напряжения T_1 в ячейках аналоговой памяти.

В НФ применяется событийное управление режимами работы. На базе КП выстраиваются цепочки последовательных процедур: выбора узловых значений очередного сплайна, вычисления невязок, корректировки значений узловых напряжений, завершения эпохи обучения. При переключении процедур необходимо учитывать время срабатывания ключей в цепях логического управления НФ, которое для современных аналоговых коммутаторов составляет около 10 нс.

Общая задержка контура управления складывается из задержки на корректировку фаз генератора, задержки вычисления невязок, задержки срабатывания схем переключения режимов обработки сигнала. Суммарная задержка определяет максимально допустимую частоту выделяемого из помехи сигнала.



Рис. 2. Сплайновый автомат обучения

При последовательной обработке интервалов дискретизации периодического сигнала перечисленные задержки суммируются, замедляя процесс обучения НФ. Событийное управление работой КП позволяет расширить возможности распознавания НФ высокочастотных сигналов. Оно допускает распараллеливание записи невязок в узлах дискретной модели. На рисунке 2 показан вариант НФ, в котором каждую пару соседних интервальных напряжений обучают отдельным сплайновым автоматом.

Каждый автомат формирует и добавляет значение невязки в выделенную ему пару ячеек аналоговой памяти. В данном случае задержка корректировки напряжений в памяти

определяется только временем формирования фазового сдвига ε_j^* и может быть равна нескольким десяткам наносекунд. Т.к. корректировка узловых напряжений f_{2i-1}^*, f_{2i}^* происходит в период вычисления невязок в узлах t_{2i}, t_{2i+1} , время одной эпохи обучения НФ определяется как сумма интервалов работы всех сплайновых интерполяторов суммируемое с временем корректировки фазового сдвига

$$t_{\Sigma} = N \cdot t_{\text{итн}} + t_{\text{ффз}}, \quad (9)$$

где $t_{\text{итн}}$ - интервал интерполирования сплайна, $t_{\text{ффз}}$ - максимальное время корректирования фазового сдвига δ , N – количество сплайнов в периоде T .

Например: Пусть $N = 30$, $t_{\text{итн}} = t_{\text{ффз}} \approx 20 \text{ нс}$. Тогда одна эпоха обучения будет $T \approx 0,63 \text{ мкс}$. Следовательно, НФ сможет выделять сигналы с частотой импульсов до 1 МГц.

Заключение

Разработанный аналоговый нейрофильтр предназначен для решения задач распознавания периодических сигналов в условиях помех большой интенсивности. Время выделения полезной составляющей из радиосигнала зависит от количества эпох обучения и от периода повторения сигнала. Применения аналоговой логики в схемах управления и безнерционной аналоговой памяти позволяет распараллелить обработку информации, выполняя ее в высоком темпе.

Полученные результаты позволяют сделать вывод о перспективности применения методов аналоговой нейротехники в качестве альтернативы цифровым системам обработки радиосигналов.

Литература

1. Интеллектуальные системы автоматического управления. / Под ред. И.М. Макарова, В.М. Лохина. М.: ФИЗМАТЛИТ, 2001. 576 с.
2. Татузов А.Л. Нейронные сети в задачах радиолокации. Издательство «Радиотехника», 2009 г. серия «Нейрокомпьютеры и их применение». 432 с.
3. Кузьмин С.З. Основы цифровой обработки радиолокационной информации. М.: Сов. радио, 1974. 432 с.
4. Боев С.Ф., Ступин Д.Д., Савченко В.П. и др. Мощные надгоризонтные РЛС дальнего обнаружения. Разработка, испытания, функционирование; под ред. С.Ф. Боева. М.: Радиотехника, 2013. 168 с.
5. Колесницкий О.К., Бокоцей И.В., Яремчук С.С. Аппаратная реализация элементов импульсных нейронных сетей с использованием биспин-приборов, Часть 1 // XII Всероссийская научно-техническая конференция «Нейроинформатика». М.: МИФИ, 2010. С. 122-127.
6. Анисимов А.С., Калачев А.В. Реализация искусственных нейронных сетей на многоядерном процессоре. Электронный журнал, eISSN 1684-1719 «Журнал Радиоэлектроники». №9. 2010.
7. Путилин А.Б. Введение в теорию преобразования и обработки сигналов. (Основы пространственно-временного и нелинейного преобразования сигналов) М.: Квадрат-С, 2000. 130 с.
8. Путилин А.Б. Континуальные системы обработки информации. М.: Квадрат-С, 2005. 156 с.
9. Bratt A., Macbeth I. DPAD2 – A Field Programmable Analog Array // Analog Integrated Circuits and Signal Processing. 1998. Vol. 17. Iss. 1-2. P. 67-89.
10. Патент на изобретение РФ № 1149792 МПК G11C27/02 Аналоговый элемент памяти., Патентная библиотека РФ, 27.09.2013.
11. Патент США № 4190851 Аналоговый элемент памяти, 1980.
12. Cyber-Physical Systems – Are Computing Foundations Adequate Edward A. Lee Department of EECS, UC Berkeley Position Paper for NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap October 16 – 17, 2006 Austin, TX.

ТРЕБОВАНИЯ К ЧАСТОТНО-ВРЕМЕННОМУ ОБЕСПЕЧЕНИЮ И СИНХРОНИЗАЦИИ СИСТЕМ СПУТНИКОВОЙ РАДИОСВЯЗИ

Мазуренко Дмитрий Константинович,

Федеральное государственное унитарное предприятие Центральный научно-исследовательский институт связи (ФГУП ЦНИИС), главный научный сотрудник, к.т.н., Москва, Россия

dm.ma2010@yandex.ru

Аннотация

В статье рассматриваются требования к частотно-временному обеспечению (ЧВО) для систем спутниковой радиосвязи. При этом уделено внимание принципам построения системы тактовой сетевой синхронизации (ТСС) для систем спутниковой радиосвязи, техническим требованиям к оборудованию ЧВО. Кроме того, приведены первичные эталонные источники (ПЭИ), сертифицированные в системе сертификации в области связи.

Ключевые слова

Спутниковая радиосвязь, тактовая сетевая синхронизация, первичный эталонный генератор, вторичный задающий генератор, центр управления связью.

Введение

Синхронизация наземного комплекса оборудования спутниковой радиосвязи может быть осуществлена, как на основе получения необходимых синхросигналов от сети ТСС единой системы электросвязи (ЕСЭ) России, так и на основе использования сигналов спутниковой радионавигационной системы (СНС).

Приемник сигналов СНС обеспечивает поиск и слежение за сигналами СНС ГЛОНАСС и GPS, автоматическое непрерывное, в реальном масштабе времени с целью определения и выдачи потребителю: следующей информации:

- координат местоположения объекта в геодезической и геоцентрической системах координат;
- высоты относительно референц-эллипсоида и относительно центра Земли;
- трех составляющих вектора скорости перемещения в геодезической и геоцентрической системах координат;
- среднеквадратического значения прогнозируемой точности координат;
- сигнала метки времени (МВ) 1 Гц со стабильностью $3 \cdot 10^{-11}$ и погрешностью 100 нс.

Синхронизация станций сопряжения системы спутниковой радиосвязи, может быть обеспечена с помощью тактовых синхросигналов, получаемых от сети тактовой сетевой синхронизации телефонной сети общего пользования (ТФОП) в частности от сети ТСС ПАО «Ростелеком». Тактовые сигналы от сети ТСС рекомендуется использовать как основные синхросигналы и синхросигналы первого резерва.

Для синхронизации станций сопряжения системы спутниковой радиосвязи можно также использовать зарубежные спутниковые системы, например, GPS применяемых, при необходимости, в качестве дополнительного резерва.

1. Построение системы тактовой сетевой синхронизации для систем спутниковой радиосвязи

Система синхронизации комплекса спутниковой радиосвязи предназначена для обеспечения тактовыми синхросигналами аппаратуры центра управления связью (ЦУС), земных региональных станций связи (РС-С), а также другой аппаратуры, нуждающейся в синхросигналах.

С этой целью в аппаратуре ЦУС, а также земных РС-С, нуждающейся в ТСС, должны быть предусмотрены входы для внешней синхронизации от первичного эталонного генератора/источника (ПЭГ/ПЭИ)) или вторичного задающего генератора (ВЭГ) для сигналов синхронизации частотой 2048 кГц и/или 2048 кбит/с, отвечающих требованиям Рекомендации МСЭ-Т G.703 со стабильностью не хуже 10^{-11} для ПЭГ и 10^{-9} для ВЭГ в режиме удержания.

Получение тактовых сетевых синхросигналов для оборудования комплекса спутниковой радиосвязи может быть обеспечено, например, от ТфОП, имеющей систему ТСС.

Получение синхросигналов может быть организовано, в частности, на договорной основе с ПАО «Ростелеком», располагающим в регионах страны соответствующими ПЭГ и ВЭГ, от которых синхронизируется аппаратура ТфОП этого оператора связи или других операторов связи, имеющих право и возможность предоставлять их на договорной основе сторонним потребителям.

Кроме того, возможно получать синхросигналы необходимого качества, например, с помощью приемников системы ГЛОНАСС и подобных ей зарубежных спутниковых систем, например, GPS используемых, при необходимости, в качестве дополнительного резерва.

При синхронизации аппаратуры комплекса спутниковой радиосвязи от тактовых сетевых синхросигналов, получаемых от ТфОП необходимы распределители сигналов синхронизации на необходимое число выходов, с которых тактовые синхросигналы поступают на синхронизируемую аппаратуру, входящую в состав ЦУС, а также региональных РС-С, показанных на рис. 1.

При этом рекомендуется синхросигналы, полученные от ТфОП, использовать как основные синхросигналы первого приоритета, а синхросигналы, получаемые от системы ГЛОНАСС можно использовать в качестве первого резерва.

Дополнительный резерв, при необходимости, может быть обеспечен с помощью зарубежных навигационных спутниковых систем, но только в качестве более низкого приоритета [1].

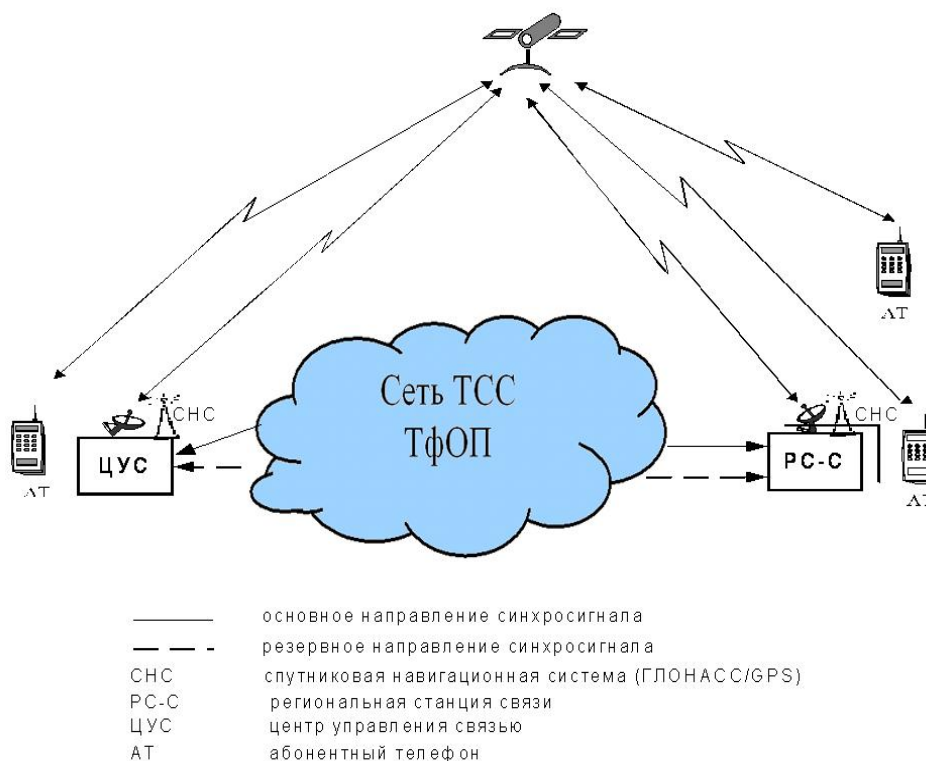


Рис. 1. Синхронизация ЦУС и РС-С комплекса спутниковой радиосвязи

Наиболее предпочтительно при синхронизации аппаратуры комплекса спутниковой радиосвязи использовать устройства ЧВО, которые, имея в своем составе приемники глобальной на-

вигационной спутниковой системы (ГНСС), выполняют функции не только формирования тактовых синхросигналов, но и функции первичных серверов времени.

Применение первичных серверов времени, имеющих выходные интерфейсы 2048 кГц и/или 2048 кбит/с., позволяет, дополнительно к получению тактовых синхросигналов, обеспечить ЦУС и РС-С сигналами единого точного времени.

Система синхронизации аппаратуры земного комплекса спутниковой радиосвязи, что было отмечено выше, может быть построена, как на основе получения необходимых синхросигналов от ТФОП, имеющей систему ТСС, так и на основе использования сигналов СНС.

В соответствии с принципами передачи и приема частотно-временной информации с использованием приёмников СНС, в СНС, состоящей из наземного комплекса и совокупности космических аппаратов (КА), имеет место привязка бортовой шкалы времени (БШВ) каждого КА к шкале времени системы (ШВС). С этой целью осуществляется:

- формирование ШВС и ее поддержание в заданных пределах относительно Всемирного координированного времени (United Time Coordinated (UTC));
- синхронизация БШВ КА относительно UTC (SU) с точностью не хуже 1 мс на любой момент времени полосы КА;
- привязка БШВ КА к ШВС с наносекундной точностью путем расчета составляющих частотно-временных поправок, их закладки на КА и последующего излучения в составе навигационного сигнала.

Формирование ШВС осуществляется с помощью программно-технических средств системы синхронизации соответствующей СНС [2].

В процессе передачи частотно-временной информации от КА к ее потребителям осуществляется вычисление расхождения местной шкалы времени потребителя (ШВП) относительно шкалы времени системы (ШВС). Космический аппарат (КА) СНС периодически (ГЛОНАСС – каждые 2 с, а GPS – каждые 6 с) передает МВ. Момент передачи МВ определяется бортовым хранителем времени (ХВ).

Передача временной информации непосредственно потребителю осуществляется в виде импульса, временное положение которого совпадает с моментом времени, привязанным к шкале времени (ШВ) Государственного эталона времени и частоты (ГЭВЧ) или к UTC в случае СНС GPS. Для этого используется известная разность между ШВ СНС и ШВ ГЭВЧ (или между ШВ СНС и ШВ UTC (SU)). Эта разность передается в составе служебной информации КА.

К числу наземной аппаратуры, получающей частотно-временную информацию от СНС, относятся, например, ПЭИ с приемниками СНС. Функциями этой аппаратуры являются:

- привязка и синхронизация ШВП с ШВ СНС и ШВ ГЭВЧ (т.е. с ШВ UTC (SU));
- сведение частоты опорного генератора аппаратуры (в частности, опорного генератора ПЭИ) с частотой бортового генератора КА;
- формирование и выдача частотно-временной информации на соответствующие интерфейсы.

Состав и характеристики ПЭИ, определяются условиями приема и обработки сигналов, назначением, спецификой установки и используемым методом привязки ШВ. Возможны два варианта работы аппаратуры частотно-временного обеспечения, как при неизвестных координатах её размещения, так и при известных координатах. В первом случае используется навигационная аппаратура, которая в процессе сеанса определяет свои координаты, а также расхождение шкал времени. Во втором случае аппаратура ЧВО работает в режиме только временных определений, как правило, по одному КА, используя координаты потребителя в качестве исходных данных.

Одним из применений аппаратуры ЧВО с приёмниками СНС является использование ее в качестве эталона времени и частоты, что обеспечивает привязку, а при наличии необходимого интерфейса, синхронизацию местной шкалы со шкалой ГЭВЧ. Другими словами, аппаратура ЧВО и, в частности ПЭИ, является источником шкалы ГЭВЧ, высокая точность которого может обеспечиваться привязкой местной шкалы к шкале ГЭВЧ и зависит только от наличия КА в зоне видимости.

Таким образом, аппаратуру ПЭИ, которая работает по сигналам КА СНС, можно квалифицировать как первичный эталон, так как ее периодическая калибровка не требуется в связи с тем, что необходимая калибровка осуществляется автоматически по сигналам КА СНС.

Временной приемник, работающий по сигналам спутниковой навигационной системы (ГЛОНАСС/GPS), для аппаратуры синхронизации цифровых систем передачи синхронной цифровой иерархии (СЦИ) должен обладать следующими возможностями:

- выдавать в сообщении поправку к частоте генератора $\Delta f/f$ с требуемой точностью;
- выдавать импульсный сигнал частоты 1 Гц, фронт которого должен быть синхронизирован с сигналом 1 Гц спутниковой системы радионавигации, и величину расхождения (поправку времени) между этими сигналами с требуемой точностью;
- иметь достаточную для размещения на объекте длину антенного кабеля.

Известно, что ПЭИ и ПЭГ находятся на 1-ом уровне иерархии сетей ТСС операторов связи России, которые построены в соответствии с международными и отечественными нормативными документами [3-5].

При этом ПЭГ – сложный, высоконадежный комплекс аппаратуры, в составе которого несколько ПЭИ, а ПЭИ, устройство существенно более простое, но, тем не менее, формирующее на своих выходах качественные и высокостабильные тактовые синхросигналы.

Следует также отметить, что применяемые, наряду с ПЭГ и ПЭИ, на сети ТСС ВЗГ, находятся на 2-м уровне иерархии и используются для восстановления и размножения синхросигналов. Они сложнее, чем ПЭИ, в частности, вследствие необходимости выполнения указанных выше функций.

Обобщенная схема ПЭИ представлена на рисунке 2.

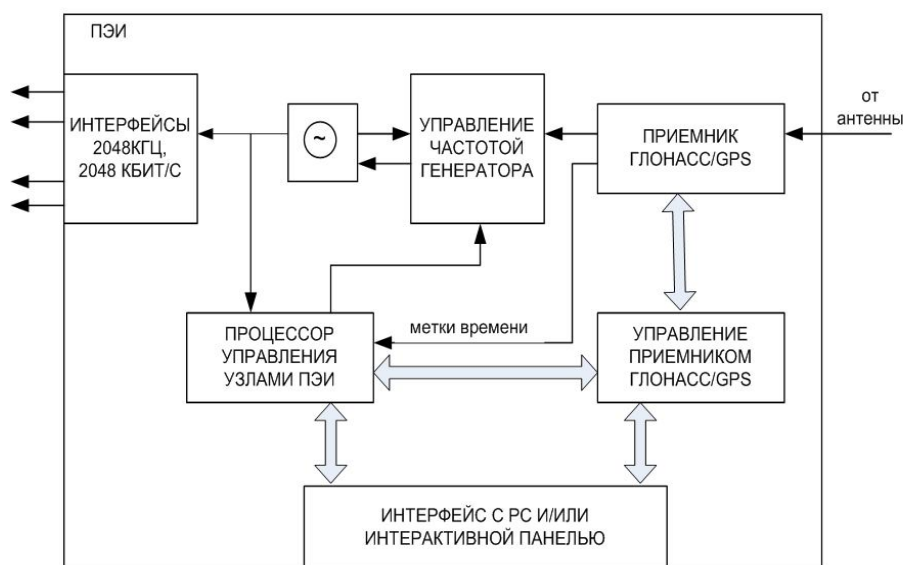


Рис. 2 Обобщенная схема ПЭИ

В условиях, когда в регионах сети ТСС аппаратура, нуждающаяся в синхронизации, синхронизируется от соответствующих ПЭГ регионов, ПЭИ применяются обычно в качестве резервных формирователей синхросигналов высокого качества.

Напротив, в ситуациях, когда синхросигналы к синхронизируемой аппаратуре не могут быть доставлены от ПЭГ региона или когда качество синхросигналов, доставляемых от ПЭГ, не может считаться удовлетворительным, имеется необходимость не в резервном, а в основном ПЭИ.

Следует отметить, что ПЭИ используются операторами связи, на цифровых сетях, как ставших уже традиционными таких, например, как сети СЦИ, так и на сетях следующего поко-

ления с пакетной передачей информации, особенно тогда, когда наряду с доставкой стабильной частоты требуется доставка к сетевым узлам сигналов точного времени.

ПЭИ, сертифицированные в системе сертификации в области связи, представлены в таблице.

Таблица

ПЭИ, сертифицированные в системе сертификации в области связи

№ п/п	Наименование	Изготовитель
1	Приемник синхронизатор VCH-311C**	ЗАО «Время-Ч» (Россия)
2	Резервный источник синхронизации GPS Receiver*	Gillam-Fei (Бельгия)
3	Резервные первичные эталонные источники OSA 4530*, OSA 4531*, OSA 4533*, OSA 5220*, OSA NTP*	Oscilloquartz (Швейцария)
4	Резервный первичный эталонный источник TIME GPS *	Simmetricom (США)
5	Первичные эталонные источники EPSILON CLOCK 1S* EPSILON CLOCK 2S* EPSILON CLOCK 2T** EPSILON CLOCK RTU* EPSILON CLOCK 3S* EPSILON CLOCK NTP*	TEMEX Sync (Швейцария)

Примечание. Звездочкой отмечены ПЭИ, имеющие в своем составе приемник GPS, а двумя звездочками – приемник ГЛОНАСС/GPS.

В таблице представлены ПЭИ с приемниками СНС, при этом ряд, приведенных в таблице ПЭИ, осуществляют прием сигналов СНС ГЛОНАСС и, следовательно, в настоящее время могут рассматриваться не только как ПЭИ резерва, но и, при необходимости, в качестве основных ПЭИ, обеспечивающих синхросигналами оборудования комплекса спутниковой радиосвязи, нуждающуюся в синхронизации и имеющую для этого соответствующие интерфейсы.

Заключение

Синхронизация аппаратуры ЦУС, а также РС-С земного комплекса спутниковой радиосвязи, нуждающаяся в сигналах ТСС и имеющая для этого соответствующие интерфейсы, должна осуществляться от ВЗГ, установленного в ЦУС (РС-С), с доставкой сигнала синхронизации от ПЭГ (ПЭИ) по основному направлению и дополнительно по двум независимым резервным направлениям.

Дополнительный резерв тактовых синхросигналов может быть обеспечен с помощью, аппаратуры, имеющей в своем составе приёмник спутниковой навигационной системы (например, приёмник ГЛОНАСС/GPS). В качестве такой аппаратуры можно использовать, например, те серверы времени, которые имеют выходные интерфейсы тактовых синхросигналов. В настоящее время такие устройства выпускаются как зарубежными, так и отечественными производителями.

Для контроля качества тактовых синхросигналов целесообразно использовать приборы отечественного производства ИВО (измерители временных отклонений) разных модификаций или же аналогичные приборы зарубежного производства. В перспективе постоянный контроль качества синхросигналов целесообразно осуществлять с помощью соответствующей системы мониторинга.

Должен быть обеспечен ряд организационных и технических мероприятий по вводу в действие, разработке документации и обучению персонала, предназначенного для эксплуатации системы ТСС в СНС.

Реализация мероприятий, с учетом технологии построения системы ТСС для системы спутниковой радиосвязи позволит обеспечить высокий уровень устойчивости системы ТСС и ЕТВ, а также системы спутниковой радиосвязи в целом [6, 7, 9].

По вопросу синтеза новых, имеющих повышенную частотную эффективность и помехоустойчивость сигналов, применяемых, в том числе, для позиционирования в устройствах координатно-временного навигационного обеспечения (КВНО) беспилотных аппаратов опубликована статья в [8].

Литература

1. Приказ Госкомсвязи России № 44 от 15.03.99 «Об использовании отечественной глобальной спутниковой радионавигационной системы ГЛОНАСС на сетях связи РФ».
2. Басевич А.Б., Богданов П.П., Белов Л.Я., Дружин В.Е., Новиков Н.Н., Стяжкин А.Д., Тюляков А.Е. (РИРВ) «Система синхронизации ГНСС ГЛОНАСС: современное состояние и перспективы». Труды Института прикладной астрономии РАН, вып. 13, 2005.
3. Рекомендации МСЭ-Т G.803, G.811 – G.813, G.822, G.823.
4. Стандарты ETSI 300 462-1, 2, 3, 4, 5, 6, 7.
5. Рекомендательный документ РСС «Концепция развития и совершенствования сетей синхронизации цифровых сетей связи стран СНГ». М.: ЦНИИС, 2004. Книга 1. 58 с., Книга 2. 49 с., Книга 3. 84 с.
6. Мазуренко Д.К. Аспекты построения системы частотно-временной сетевой синхронизации сигналов // Т-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 8. С. 4-8.
7. Мазуренко Д.К. Разработка прецизионного генератора шкалы времени», журнал «Электросвязь» № 6, 2019, С. 31-35.
8. Мазуренко Д.К. Разработка пакета прикладных программ для математического моделирования и оптимизации процессов передачи и приема сигналов в системах связи // Т-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 8. С. 38-43.
9. Мазуренко Д.К. Измерение качества передачи сигналов единого точного времени в сети связи с пакетной коммутацией // Т-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 7. С. 35-40.

ВОЛОКОННО-ОПТИЧЕСКИЙ ОТВЕТВИТЕЛЬ/ПЕРЕКЛЮЧАТЕЛЬ МОЩНОСТИ ОПТИЧЕСКОГО ИЗЛУЧЕНИЯ

Мансуров Тофиг Магомед оглы,

Азербайджанский Технический Университет, профессор, доктор технических наук, Баку, Азербайджан

Зеневич Андрей Олегович,

Белорусская Государственная Академия Связи, профессор, доктор технических наук, Минск, Белорус

Мамедов Ильтимас Ахмед оглы,

Азербайджанский Технический Университет, доцент, кандидат технических наук, Баку, Азербайджан
tofiq-mansurov@rambler.ru

Аннотация

На основе проведенного анализа определены недостатки существующих волоконно-оптических ответвителей. Указано, что для ответвления оптического излучения волоконный световод разделяется на две части, ответвление оптического излучения осуществляется из одномодового волоконного световода, не обеспечивая изменения коэффициента ответвления в широких пределах, а также не позволяют осуществить переключение оптического излучения из одного волоконного световода в другой с изменением длины волны. С этой целью разработан волоконно-оптический ответвитель мощности источника оптического излучения, позволяющий вести регулировки коэффициента ответвления от 0 до 1 и обеспечить возможность ответвления мощности оптического излучения в другие типы волоконного световода с преобразованием длины волны, а также реализовать функцию переключения оптического излучения из одного оптического волокна в другое и тем самым расширить функциональные возможности.

Ключевые слова

Ответвитель, источник, оптическое излучение, длина волны, волоконный световод, коэффициент ответвления, формирователь микроизгиба, пороговое устройство.

Введение

В последнее время одним из наиболее перспективных и развивающихся направлений построения оптических телекоммуникационных сетей являются широкое применение волоконно-оптических линий связи (ВОЛС). Это объясняется с тем, что они обладают большой пропускной способностью, помехозащищенностью, меньшим коэффициентом затухания, большими длинами регенерационных участков и высокой надежностью работы ВОЛС, что значительно превосходят существующие проводные линии связи.

Волоконно-оптический ответвитель, как пассивный компонент ВОЛС, предназначены для ответвления мощности источника оптического излучения в волоконных световодах локальных сетей, а также они могут применяться при построении разветвленных оптических сетей [1,2] .

По способу передачи мощности оптического излучения волоконно-оптические ответвители делятся на одномодовые и многомодовые, ответвители на различные длины волн, с различной конфигурацией входа и выходов и заданным коэффициентом деления. Волоконно-оптический ответвитель как многополюсное устройство, в котором мощность оптического излучения, поступающая на вход, распределяется между его выходами. Кроме того, волоконно-оптические ответвители делятся на однонаправленные, двунаправленные, чувствительные (частотнозависимые) и нечувствительные к длине волны (частотнонезависимые). В двунаправленном волоконно-оптическом ответвителе вход и каждый выход может работать на прием и на передачу или на прием и передачу одновременно.

Когда в оптических телекоммуникационных системах не используется принцип спектрального уплотнения сигналов, рабочая длина волны оптического излучения занимает узкую поло-

су спектрального диапазона. В этом случае, они предназначаются для ответвления мощности источника оптического излучения между двумя или несколькими выходами.

Волоконно-оптические ответвители должны быть согласованы с входными и выходными участками оптических телекоммуникационных систем, т.е. заканчиваться либо отрезками волоконных световодов, либо разъемными соединителями. К волоконно-оптическим ответвителям предъявляются требования стабильности параметров, надежности и технологичности.

Постановка задачи

В оптических телекоммуникационных системах часто возникает необходимость ответвления части мощности источника оптического излучения из основного канала передачи (например, для проведения мониторинга, измерения или приема сигнала обратной связи, предназначенного для управления уровнем мощности источника оптического излучения), а также разделения или объединения потоков оптического излучения (например, при использовании технологии волнового мультиплексирования (WDM)).

Ответвление можно создать с изменением угла падения оптического излучения на границу раздела «сердцевина-оболочка», если угол падения будет меньше критического угла падения, то оптическое излучение будет ответвляться и выходить в оболочку волоконного световода и от туда в внешнюю среду. Практически эту функцию выполняют волоконно-оптические ответвители.

В связи с этим, проведен анализ существующих волоконно-оптических ответвителей [1-3,5,7,10] и в качестве недостатков указаны [1], что для ответвления мощности источника оптического излучения из волоконного световода необходимо разделение этого волоконного световода на две части, в [2] указано, что ответвление оптического излучения осуществляется из одномодового волоконного световода, когда есть необходимость ответвление оптического излучения из многомодового волоконного световода без его разрыва и в [3] указано, что не обеспечивает изменения коэффициента ответвления оптического излучения, а также не позволяет осуществить переключение оптического излучения из одного волоконного световода в другое с изменением длины волны.

Для устранения перечисленных недостатков возникает необходимость разработки волоконно-оптического ответвителя, позволяющего вести регулировки коэффициента ответвления в широком пределе, обеспечить возможность полного ответвления мощности оптического излучения, а также переключения мощности оптического излучения из входного волоконного световода в различные типы (одно- и многомодовые) волоконного световода с преобразованием длины волны входного оптического излучения, с переключением различных источников оптического излучения с различными длинами волны и тем самым расширить функциональные возможности волоконно-оптического ответвителя.

Целью данной работы является расширение функциональных возможностей волоконно-оптических ответвителей за счет обеспечения регулировки коэффициента ответвления от 0 до 1, выполнение режима полного ответвления оптического излучения из волоконного световода, а также переключения оптического излучения с одного волоконного световода в другой.

Разработка волоконно-оптического ответвителя

Для ответвления мощности оптического излучения из волоконного световода используются волоконно оптические ответвители, которые безразрывно подключаются к данному волоконному световоду с целью идентификации волоконного световода и создания кратковременной служебной линии связи. Они могут быть использованы и для несанкционированного съема информации [3-5].

Разработан волоконно-оптический ответвитель, схема которого представлена на рисунке 1.

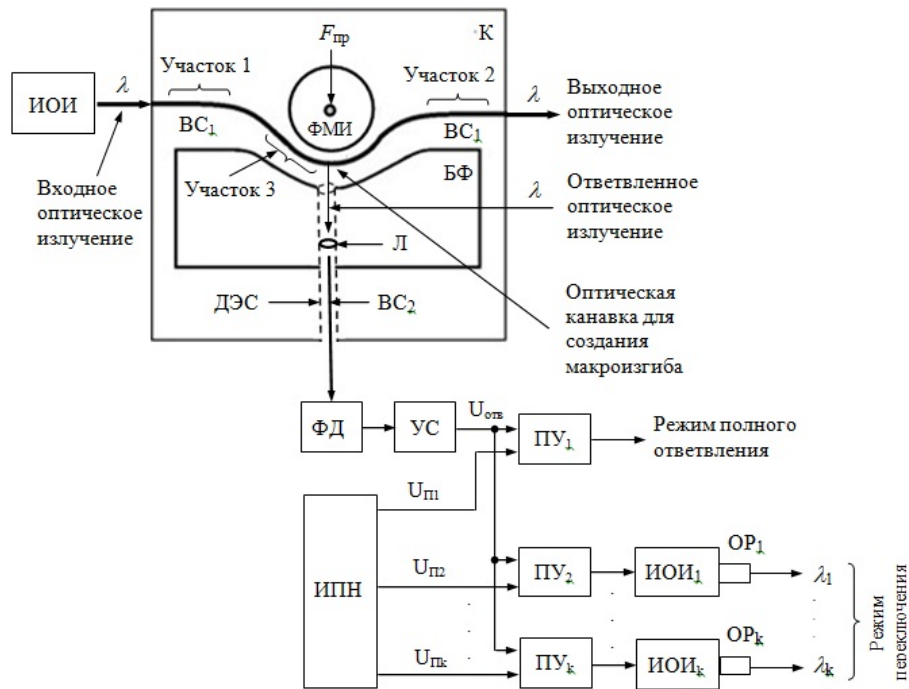


Рис. 1. Схема волоконно-оптического ответвителя

Волоконно-оптический ответвитель состоит из источника оптического излучения (ИОИ) с длиной волны (λ), формирователя макроизгиба (ФМИ), волоконного световода BC_1 с сердцевинной и светоотражающей оболочкой, имеющего два прямолинейных участка (участок 1 и участок 2) и расположенного между ними участка с изгибом (участок 3), блока фокусировки (БФ) с диэлектрической средой (ДЭС), выполненной из прозрачного для этого оптического излучения материала и находящейся в контакте с фокусирующей линзой (Л), волоконного световода (BC_2), соединенного с одной стороны с диэлектрической средой для приема ответвленного оптического излучения и с другой стороны с фотодетектором (ФД) для передачи ответвленного оптического излучения, усилителя (УС), источника пороговых напряжений (ИПН) $U_{п1} > U_{п2} \dots > U_{пk}$, пороговых устройств ($ПУ_1, \dots, ПУ_k$), источников оптического излучения ($ИОИ_1, \dots, ИОИ_k$) с разными длинами волн ($\lambda_1, \dots, \lambda_k$) и с соответствующими выходными оптическими разъемами ($ОР_1, \dots, ОР_k$) и светонепроницаемого кожуха (К). Формирователь макроизгиба, блок фокусировки и часть волоконных световодов BC_1 и BC_2 размещены в светонепроницаемом кожухе.

Источник оптического излучения формирует оптическое излучение с мощностью 1,0 мВт на длинах волн 650, 850, 1300, 1310, 1490, 1550 и 1625 нм, которые применяются для передачи информации и проведения мониторинга, измерения или приема сигнала обратной связи, предназначенного для управления уровнем мощности источника оптического излучения [1,2,6]. Формирователь макроизгиба создает изгибы волоконного световода BC_1 с диаметром d_u в диапазоне от 5,0 мм до 60 мм.

Если выходная мощность источника оптического излучения равна 0 дБм (1,0 мВт) и коэффициент полезного действия $\approx 5\%$ (-13 дБ) волоконно-оптического ответвителя, то потери на макроизгибе волоконного световода BC_1 составляет $\approx 1,0$ дБ. Это означает, что для формирования канала ответвления мощности источника оптического излучения в волоконном световоде BC_1 нужно сформировать макроизгиб с диаметром менее 60 мм.

Изменение диаметра макроизгиба осуществляется с изменением силы прижима $F_{пр}$ на формирователь макроизгиба к оптической канавке призмы. Данный диапазон изменения диаметра макроизгиба выбран исходя из того, что на исследуемых длинах волн при больших зна-

чениях диаметра макроизгиба d_u (больше 60 мм) ответвление оптического излучения в волоконном световоде ВС₁ практически не наблюдается, а при меньших диаметрах макроизгиба (меньше 5 мм) может наступить излом волоконного световода [1,2,4].

Принцип работы волоконно-оптического ответвителя

При запуске к работе волоконно-оптического ответвителя формирователь макроизгиба находится в исходном положении, при котором не создается макроизгиб и не происходит ответвление мощности источника оптического излучения. На волоконном световоде ВС₁ имеется возможность создания и изменения диаметра d_u макроизгиба, которая создается со ступенчатым изменением силы прижима F_{np} на формирователь макроизгиба и формирователя изгиба к V – образной оптической канавке призмы.

Для направления оптического излучения, ответвленного с поверхности волоконного световода ВС₁ в области макроизгиба, в волоконный световод ВС₂, применяется блок фокусировки. Выход блока фокусировки с помощью волоконного световода ВС₂ через фокусирующую линзу соединяется с фотодетектором.

Разработанный волоконно-оптический ответвитель может работать в двух режимах:

- режим полного ответвления мощности источника оптического излучения;
- режим переключения ответвленного оптического излучения с различной мощностью с одного волоконного световода в другой.

Режим полного ответвления

Для полного ответвления оптического излучения с поверхности волоконного световода СВ₁ формирователем макроизгиба формируется участок изгиба волоконного световода СВ₁ с наименьшим диаметром изгиба (участок 3). В этом случае происходит полное ответвление входного оптического излучения с участка изгиба (участка 3) не поступая на второй прямолинейный участок (участок 2) волоконного световода СВ₁. Ответвленное оптическое излучение с поверхности волоконного световода СВ₁ с помощью диэлектрической среды (ДЭС), выполненной из прозрачного для этого оптического излучения материала попадает на фокусирующую линзу (Л). Фокусированное полное ответвленное оптическое излучение подается на вход фотодетектора (ФД), где данное излучение преобразуется в электрический сигнал, который усиливается усилителем (УС) и параллельно поступает на первые входы всех пороговых устройств (ПУ₁,...,ПУ_k), а на вторые входы которых из источника пороговых напряжений подаются соответствующие пороговые напряжения $U_{п1} > U_{п2} \dots > U_{пk}$. Пороговые устройства производят сравнение значения напряжения ответвленного оптического излучения $U_{отв}$ с соответствующими значениями пороговых напряжений $U_{пi}$. При полном ответвлении мощности оптического излучения с поверхности волоконного световода СВ₁ выполняется условия $U_{отв} \geq U_{п1}$ и на выходе первого порогового устройства ПУ₁ появляется сигнал и далее передается по назначению.

Режим переключения

Для переключения входного оптического излучения с поверхности волоконного световода СВ₁ с различной мощностью необходимо изменить силы прижима F_{np} на формирователь макроизгиба к V – образной оптической канавке призмы.

Ответвленное оптическое излучения с помощью линзы фокусируется на фотодетектор и фотодетектором преобразуется в электрический сигнал. Электрический сигнал, усиливаясь усилителем, параллельно передается на первые входы пороговых устройств (ПУ₁,...,ПУ_k), а на вторые входы которых из источника пороговых напряжений подается соответствующие пороговые напряжения $U_{п1} > U_{п2} \dots > U_{пk}$.

Если выполняется условие $U_{П1} > U_{отв} \geq U_{П2}$, то на выходе второго порогового устройства ПУ₂, если выполняется условие $U_{П2} > U_{отв} \geq U_{П3}$, то на выходе третьего порогового устройства ПУ₃ и если выполняется условие $U_{k-1} > U_{отв} \geq U_{Пk}$, то на выходе k -го порогового устройства ПУ_k появляется сигнал. Под воздействием этого сигнала с выхода соответствующего порогового устройства запускается к работе соответствующий источник оптического излучения с соответствующей длиной волны. Выходы всех источников оптического излучения снабжены выходными оптическими разъемами для подключения волоконных световодов различных типов (одно- и многомодовых). Выбор необходимой длины волны оптического излучения позволяет обеспечить минимальный коэффициент затухания ответвленного оптического излучения в волоконном световоде. Ступенчатое изменение силы прижима F_{np} на формирователь макроизгиба к V -образной оптической канавке призмы позволяет изменить коэффициент ответвления и мощности ответвленного оптического излучения в различные типы волоконных световодов.

По сравнению с известными объектами разработанный волоконно-оптический ответвитель имеет следующие преимущества:

1. Введение в предложенный волоконно-оптический ответвитель формирователя макроизгиба с возможностью ступенчатого изменения силы прижима на него и в свою очередь формирователя макроизгиба к V -образной оптической канавке призмы позволяет вести регулировки коэффициента ответвления от 0 до 1.

2. Введение в предложенный волоконно-оптический ответвитель фотодетектора, усилителя, пороговых устройств, источника пороговых напряжений и источников оптического излучения с различными длинами волны и выходными оптическими разъемами, позволяет ответить входное оптическое излучение с изменением мощностью, а также реализовать функции переключения оптического излучения из одного волоконного световода в другой и тем самым расширить функциональные возможности разработанного волоконно-оптического ответвителя.

Параметры волоконно-оптического ответвителя

Волоконно-оптический ответвитель несимметричного Y -образного типа представляет собой обобщение древовидного волоконно-оптического разветвителя, когда мощность источника оптического излучения с длиной волны λ ответвляется в неравной пропорции между выходами i ($i = \overline{2, k}$). Для данного случая упрощенная схема волоконно-оптического ответвителя представлена на рисунке 2, где выходы волоконно-оптического ответвителя пронумерованы в порядке убывания мощности ответвленного оптического излучения [1, 2, 3-6].

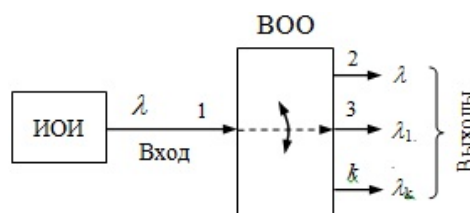


Рис. 2. Упрощенная схема волоконно-оптического ответвителя

Волоконно-оптические ответвители имеют конфигурации 1×2 , 1×3 , 1×4 , ..., $1 \times n$ и обычно меньше 50% мощности источника оптического излучения ответвляется на его выходы, в то время как большая часть мощности источника оптического излучения передается на прямой выход 2 (вход 1 \rightarrow выход 2) без макроизгиба волоконного световода ВС₁.

Волоконно-оптические ответвители характеризуются следующими параметрами, которые играют важную роль при их разработке.

Коэффициент ответвления, показывающий степени ответвления мощности источника оптического излучения на его выходы и определяется по следующей формуле:

$$k_{отв} = P_{вых\ i} / P_{вх\ 1},$$

где $P_{вх\ 1}$ – мощность источника оптического излучения или входная мощность волоконно-оптического ответвителя; $P_{вых\ i}$ – ответвленная мощность оптического излучения на выходе i ($i = \overline{2, k}$) волоконно-оптического ответвителя.

Коэффициент деления определяется отношением мощностей оптического излучения на выходах i ($i = \overline{2, k}$), не изолированных от входа 1 волоконно-оптического ответвителя и определяется следующим образом:

$$k_{дел} = P_{вых\ 1\ i} / P_{вх\ 1},$$

где $P_{вых\ 1}$ – выходная мощность источника оптического излучения или входная мощность волоконно-оптического ответвителя; $P_{вх\ 1\ i}$ – мощность оптического излучения на выходе i ($i = \overline{2, k}$), не изолированных от входа 1 волоконно-оптического ответвителя.

Коэффициент затухания α волоконного световода ВС₁ с макроизгибом определялся по следующей формуле:

$$\alpha = -10 \lg(P_{вх\ 1} / P_{вх}), \quad \text{дБ}$$

где $P_{вх}$ – мощность оптического излучения на входе волоконного световода ВС₁, $P_{вх\ 1}$ – мощность оптического излучения на выходе волоконного световода ВС₁ с макроизгибом.

Изменение значения коэффициента затухания $\Delta\alpha$, вносимого макроизгибом волоконного световода ВС₁ определяется по следующей формуле:

$$\Delta\alpha = \alpha - \alpha_0, \quad \text{дБ}$$

где α – коэффициент затухания волоконного световода ВС₁ с макроизгибом; α_0 – коэффициент затухания волоконного световода ВС₁ без макроизгиба.

Вносимые потери, т.е. потери мощности оптического излучения волоконно-оптическим ответвителем, которая с выхода источника оптического излучения поступает на вход волоконного световода ВС₁ и ответвляется на один из выходов волоконно-оптического ответвителя и определяется по следующей формуле:

$$\alpha_{вн} = -10 \lg(P_i / P_1), \quad \text{дБ}$$

где P_1 – мощность источника оптического излучения, поступающая на вход 1 волоконно-оптического ответвителя; P_i – мощность ответвленного оптического излучения, регистрируемая на одном из выходов i ($i = \overline{2, k}$) при условии поступления оптического излучения из источника оптического излучения на вход 1. Причем вход и выходы волоконно-оптического ответвителя не имеет непосредственной связи друг с другом.

Коэффициенты направленности волоконно-оптического ответвителя являются мерой того, как мощность ответвленного оптического излучения передается в предназначенные выходы. Определяются той же формулой, что и вносимые потери, но в данном случае вход и выходы волоконно-оптического ответвителя изолированы друг от друга:

$$K_{нап} = P_i - P_1, \quad \text{дБ}.$$

Потери на отражение определяются по формуле:

$$A_{\text{отр}} = P_{\text{выхИОН вх\BOO}} - P_1, \text{ дБ.}$$

где P_1 – мощность источника оптического излучения, поступающая на вход 1 волоконно-оптического ответвителя; $P_{\text{выхИОН вх\BOO}}$ – регистрируемая выходная мощность источника оптического излучения на входе 1 волоконно-оптического ответвителя при условии подачи мощности источника оптического излучения на вход 1.

Полные избыточные потери мощности оптического излучения волоконно-оптического ответвителя определяются следующим образом:

$$A_{\text{из}} = -10 \lg \sum P_{li} / P_1, \text{ дБ}$$

где сложение производится только для тех значений $i (i = \overline{2, k})$, при которых вход и выходы волоконно-оптического ответвителя не изолированы друг от друга. Причем мощность источника оптического излучения измеряется в мВт.

Необходимо отметить, что с уменьшением длины волны оптического излучения потери на макроизгибе волоконного световода уменьшается, а с увеличением длины волны траектории распространения оптического излучения отличается от прямолинейного и увеличивается диаметр модового поля и большая часть оптического излучения распространяется в оболочке волоконного световода.

Таким образом, приведенная система параметров позволяет охарактеризовать режимы работы волоконно-оптического ответвителя при ответвлении мощности оптического излучения с различной мощностью на его выходы в зависимости от диаметра создаваемого макроизгиба.

Заключение

1. Разработанный волоконно-оптический ответвитель с возможностью плавного изменения силы прижима на формирователя макроизгиба к V – образной оптической канавке призмы позволяет вести регулировки коэффициента ответвления в пределе от 0 до 1, обеспечить возможность ответвления мощности оптического излучения в одно- и многомодовые волоконные световоды, а также реализует функцию переключения оптического излучения из одного оптического волокна в другой и расширить функциональные возможности волоконно-оптического ответвителя.

2. Экспериментально установлено, что меньше 50% мощности источника оптического излучения передается на выходы волоконно-оптического ответвителя, а основная часть выходной мощности на прямой выход 2.

3. Определено, что для обеспечения нормальной работы волоконно-оптического ответвителя чувствительность фотодетектора должен составлять примерно -20дБм.

4. При значении мощности равной 0 дБм (1,0 мВт) источника оптического излучения, передаваемого по волоконному световоду BC_1 , и коэффициенте полезного действия около 5% (-13 дБ) волоконно-оптического ответвителя, потери на макроизгибе волоконного световода BC_1 составляет примерно 1 дБ. Это означает, что для формирования канала ответвления мощности оптического излучения в волоконном световоде BC_1 нужно сформировать макроизгиб с диаметром от 5 мм до 60 мм.

Литература

1. Горлов Н.И. Оптические линии связи и пассивные компоненты ОСП. Новосибирск: СибГУТИ, 2003. 229 с.
2. Optical communications. Components and Systems: analysis: design: optimization: application / Jurgen Franz, Vi-rander Jain. -Harrow, U.K.: Alpha Science International Ltd, 2000. 717 p.
3. АС СССР № 1318972, МКИ G02 В 27/10, 1987.
4. Волоконно-оптический ответвитель - прищепка. - Режим доступа: <http://www.bnti.ru/dbtexts/ipks/old/ipks/iv180400/tmp/fod5503/manual.pdf>.
5. АС СССР № 1091731, МКИ G 02 В 6/00, 1992.
6. Гришачев В.В. Модель угроз конфиденциальности речевой информации в современном офисе на основе конвергенции функций оптических сетей // Фотоника. М., 2017, №2. С. 90-103.
7. Гришачев В.В. Выявление угроз утечки речевой информации через волоконно-оптические коммуникации // Фотоника. М., 2011. №4. С. 32-39.
8. Гришачев В.В., Халяпин Д.Б., Шевченко Н.А. Анализ угроз утечки конфиденциальной речевой информации через волоконно-оптические коммуникации // Вопросы защиты информации. М., 2008, №5. С.12-17.
9. Хорев А.А. Классификация методов и средств поиска электронных устройств перехвата информации // Специальная техника. М., 2007, № 6. С. 52-60.

СЕРТИФИКАЦИЯ СИСТЕМ РАСПРЕДЕЛЕННОГО РЕЕСТРА КАК ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Панков Константин Николаевич,

МТУСИ, доцент кафедры «Информационная безопасность», к.ф.-м.н., Москва, Россия
pankov_kn@mtuci.ru

Эйнман Анастасия Дмитриевна,

МТУСИ, Москва, Россия

Аннотация

В данной работе исследуется проблема сертификации систем распределенного реестра как способа обеспечения доверия к ним пользователей, что является составной частью информационной безопасности. В статье приводится краткий обзор нормативно-правовой базы государственных организаций, занимающихся сертификацией, анализируются уязвимости субтехнологий систем распределенного реестра и предложен список испытаний, которые должны проводиться в ходе сертификации. Рассмотрен пример информационной системы, успешно прошедшей сертификацию в Российской Федерации.

Ключевые слова

Системы распределенного реестра, блокчейн, информационная безопасность, сертификация, субтехнология, уязвимость, мастерчейн

Введение

В настоящее время в нашей стране действует содержащий перечень из 9 сквозных цифровых технологий [36] паспорт национальной программы «Цифровая экономика Российской Федерации» [41], утвержденный со ссылкой на [55] по итогам заседания президиума Совета при Президенте Российской Федерации (далее – РФ) по стратегическому развитию и национальным проектам 4 июня 2019 года. Одной из этих технологий являются системы распределенного реестра (далее – СРР).

С началом глобальной пандемии COVID-19 в 2020 году возросла потребность в создании информационных систем для удаленного взаимодействия представителей общества и различных государственных и коммерческих структур. Одним из инструментов обеспечения информационной безопасности таких систем является технология СРР вообще, и технология цепной записи данных (блокчейн) [35], как вариант реализации сети распределенных реестров [44] в частности. В силу уже сложившихся представлений в экспертном сообществе, отразившихся в принятой в конце 2019 года Дорожной карте развития СРР [24], можно использовать термины СРР и блокчейн (как это делают ряд западных и отечественных исследователей) в качестве синонимов.

Составляющей частью информационной безопасности существующих систем является доверие [63] к ним пользователей, под которым согласно [19] понимается «выполнение действий или процедур, подтверждающих, что оцениваемый объект соответствует своим целям безопасности». Как справедливо замечено в [26], доверие к информационным системам обеспечивается различными формами сертификации.

Согласно [40] при построении современных СРР активно используются криптографические инструменты, поэтому с точки зрения представителей ФСБ РФ, которая была озвучена на конференции DLTReg 2019, посвященной общим вопросам регулирования технологии, и обоснована в [26], эти системы относятся к средствам криптографической защиты информации (СКЗИ).

В РФ сертификацией различных видов информационных систем и средств защиты информации занимаются ФСБ, ФСТЭК и Банк России [26]. Обзор источников, содержащих нормативно-правовую базу данных государственных организаций в части касающейся сертификации, будет представлен в следующем разделе

Нормативно-правовая база сертификации

В рамках Росстандарта действует технический комитет по стандартизации ТК-159 «Программно-аппаратные средства технологий распределённого реестра и блокчейн», в состав которого с 2017 года входит МТУСИ [27]. К началу 2019 года в рабочей группе № 2 технического комитета «Безопасность, идентификация и конфиденциальность», возглавляемой одним из авторов статьи, был подготовлен отчет [38], в котором была проведена попытка оценить применимость существующей отечественной нормативной базы различного уровня к СРР. Аналогичная попытка была предпринята в отчете [45]. Правовому регулированию таких СРР как криптовалюты посвящена монография [33].

Сразу отметим, что нормативные акты применяются к информационным системам в зависимости от их назначения и характера информации, обрабатываемой в этих системах.

В настоящее время лидирующие позиции в применении информационных систем, основанных на технологии СРР, занимает финансовая отрасль [9], [8], регулятором которой является Банк России. Отметим, что в системах, применяемых в финансовой отрасли, часто обрабатывается охраняемая по законодательству РФ персональная информация. В, [17] и [39] приведены целый ряд нормативных актов Банка России и возглавляемого им ТК-122 «Стандарты финансовых операций», касающихся информационной безопасности, которые обязательны либо рекомендательны для всех финансовых организаций. Кроме того, Банком России в конце 2020 года были утверждены «Условия по защите информации» [56], включающие в себя «Требования к использованию СКЗИ», которые в соответствии с позицией ФСБ России, следовательно, относятся к СРР и отсылают к нормативно-правовым актам этой службы. Согласно внутренней информации ТК-159 сейчас представители Центробанка работают над требованиями к СРР с учетом принятия закона о цифровых финансовых активах [58].

Нормативно-правовая база, касающаяся сертификации средств защиты информации расположена на сайте [23] Федеральной службы по техническому и экспортному контролю (ФСТЭК) России. В работе [50] один из приказов с этого сайта был использован для классификаций мер защиты, которую реализуют современные СРР. Под сертификацией ФСТЭК понимают процедуру получения документа, который подтверждает соответствие средства защиты информации требованиям нормативно-правовой базы. Одной из задач сертификации ФСТЭК позиционируется возможность потребителя выбрать качественное и эффективное программное средство. При этом, в соответствии с приказом ФСТЭК [43], требования этой службы о защите информации не касаются СКЗИ.

Таким образом, в соответствии с законодательством РФ вопросы сертификации СРР при признании его СКЗИ относятся к ведению ФСБ России и регулируются его нормативно-правовой базой, которая в части, касающейся СРР, описана в [26], а для всех СКЗИ подробно разобрана в [31].

Известное специалистам по информационной безопасности Положение ПКЗ-2005 [42], утвержденное приказом службы и являющееся основным документом, регулирующим вопросы проведения оценки соответствия СКЗИ требованиям по информационной безопасности, строго определяет перечень случаев, в которых обязательно его применение к СРР:

- если СРР содержит конфиденциальную информацию [54], защищаемую законодательством РФ;
- если СРР содержит конфиденциальную информацию и используется в органах исполнительной власти РФ и субъектов РФ;
- если СРР содержит конфиденциальную информацию и используется в организациях, выполняющие госзаказы, независимо от организационно-правовой формы и формы собственности этих организаций;

– если обязательность защиты конфиденциальной информации, содержащейся в СРР, возлагается законодательством РФ на лиц, имеющих доступ к ней или уполномоченных распоряжаться содержащимися в ней сведениями;

– если СРР содержит конфиденциальную информацию, принадлежащую госорганам или организациям, которые выполняют госзаказы;

– если СРР содержит конфиденциальную информацию, обладатель которой предпринимает меры к защите ее конфиденциальности с помощью криптографических методов, и используется в госорганах и в организациях, выполняющих госзаказы.

Следовательно, если СРР не попадает под хотя бы один из перечисленных пунктов и при этом не является государственной информационной системой [57], то проведение его сертификации не является обязательным. В противном случае, необходимо перед процедурой сертификации составить техническое задание с указанием проводящей сертификационные испытания организации и класса защиты в соответствии с [48]. Рисунок 1 из [26] иллюстрирует характер взаимодействия при проведении сертификации СРР между заказчиком, разработчиком, организацией, выполняющей исследования по оценке соответствия СРР требованиям ФСБ России, и Центром по лицензированию, сертификации и защите государственной тайны ФСБ России [61], который оценивает полноту и корректность проведенных исследований.

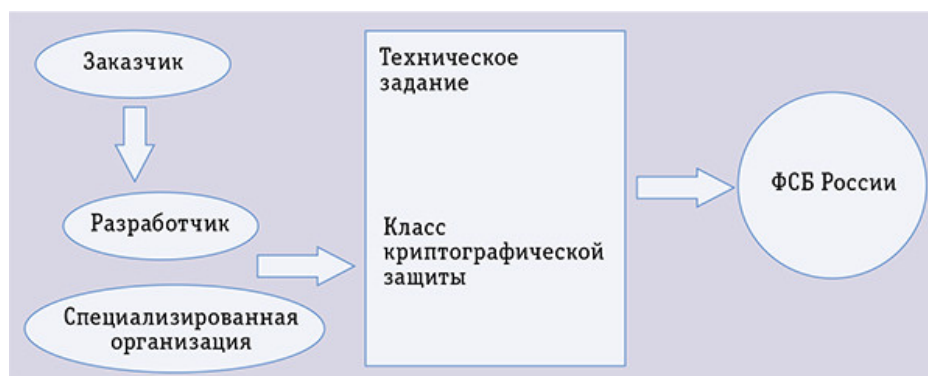


Рис. 1. Порядок взаимодействия сторон при сертификации СРР

Возникает резонный вопрос – какие исследования СРР должна проводить специализированная организация в ходе сертификации, чтобы полнота и корректность проведенных исследований была признана ФСБ России, а в дальнейшем – пользователями СРР?

Уязвимости и ограничения субтехнологий технологии систем распределенных реестров

Прежде, чем переходить к возможному списку исследований, постараемся разобраться с уязвимостями технологии СРР, которые мы будем трактовать в соответствии с [21].

В соответствии с Дорожной картой развития сквозной цифровой технологии (далее – СЦТ) «СРР» [24] «субтехнология» является компонентой СЦТ, благодаря которой возможно выделение продуктов и решений и их отнесение к данной СЦТ; при этом каждая субтехнология является уникальной компонентой для СРР, и субтехнологии не пересекаются и не включают в себя составляющие друг друга; субтехнологии не являются отдельными формами применения СЦТ в качестве составляющих данной технологии. Итогом обсуждения списка субтехнологий с экспертным сообществом в апреле 2019 года, в котором участвовали представители МТУСИ, стал набор [24] из трех пунктов.

1. Технологии организации и синхронизации данных, связанная с определением, организацией и усовершенствованием связей между отдельными частями и различными элементами СРР, обеспечением их согласованности;

2. Технологии обеспечения целостности и непротиворечивости данных (консенсус), которая направлена на приведение в соответствие имеющихся данных в сети к единой логике и структуре согласно изначально заданным правилам. Кроме того данная субтехнология обеспечивает согласования данных и их синхронизацию между узлами сети, чаще всего, децентрализованной;

3. Технологии создания и исполнения децентрализованных приложений и смарт-контрактов (чейнкодов или умных контрактов в терминологии [35]), отвечающая за создание приложений, обеспечивающих взаимодействие участников СРР, и за алгоритмы, которые предназначены для автоматизации контрактов в СРР.

В конце ноября 2019 года в ВШЭ проходило экспертное обсуждение классификаторов СЦТ и связанных с ними цифровых продуктов и услуг [66]. В рамках обсуждения СЦТ СРР было предложено в последнюю субтехнологии добавить токенизацию и назвать эту технологию «технологией управления функциональным процессом СРР» (предложение было выдвинуто вице-президентом российской ассоциации крипто-индустрии и блокчейна – РАКИБ по специальным проектам, главой компании 3D Business Solutions (США) Костенем Д.Г.).

Рассмотрим уязвимости и ограничения для отдельных компонент СРР, которые могут быть основанием для проведения отдельного исследования в рамках сертификации. Ряд атак, которые относятся к разным субтехнологиям, подробно описан в [29].

Для технологии организации и синхронизации данных можно выделить отдельные уровни уязвимостей и ограничений:

- сетевой уровень, на котором возможны такие атаки как широко известная DDoS, а также атака Сивиллы, в результате которой пользователь подключается только к узлам, контролируемым противником.

К этому же уровню относится такое ограничение как пропускная способность. Количество транзакций, обрабатываемых в единицу времени существующими СРР, по сравнению с классическими IT-решениями сравнительно невелико, что ограничивает возможность их сертификации для некоторых областей применения. К примеру, СРР Биткоин работает со скоростью 7 транзакций в секунду (TPS), Эфириум - 15 TPS и т.п. Для сравнения, к примеру еще в 2010 Visa показывала скорость 24000 TPS [10].

- уровень цепной записи данных (блокчейн в его узком понимании). На этом уровне основные ограничения для сертификации будут связаны с используемыми криптографическими алгоритмами (хеш-функций, шифрования, электронной подписи), которые для сертификации СРР в РФ должны соответствовать отечественной нормативно-правовой базе, а в случае независимой сертификации в иных целях должны достаточно стойкими для обеспечения информационной безопасности (стойкости) соответствующей СРР. Кроме самих алгоритмов уязвимости в СРР могут быть связаны с обеспечением защиты соответствующей ключевой системы.

К этому же уровню относятся ограничения, связанные с хранением и обработкой в СРР конфиденциальной информации, к примеру персональной, вопросов защиты которой в СРР касается работа [11].

- уровень пользователя, на котором противник тем или иным путем может осуществлять несанкционированное получение информации пользователя различного характера. Таким образом, на этом уровне должна обеспечиваться защита от несанкционированного доступа [20].

Для технологии обеспечения целостности и непротиворечивости данных (консенсус) можно из уязвимостей выделить актуальную для ряда ныне существующих СРР атаку 51 процента, а также большие энергозатраты при использовании безопасных алгоритмов консенсуса. К примеру, согласно Кембриджскому индексу энергопотребления Биткоина расход электроэнергии для поддержания работы СРР Биткоин за последний год на 29 января 2021 года составляет 111,68 тераватт-часов [4]. Отметим, что наличие данных уязвимостей напрямую зависит от архитектуры, политик и процедур СРР как информационной системы. Таким образом, к этой субтехнологии относятся ограничения, связанные с процедурой прихода к консенсусу и, отчасти, типом СРР в соответствии с [35].

Для технологии создания и исполнения децентрализованных приложений и смарт-контрактов можно отметить такую уязвимость как негибкость и недостаточная безопасность чейнкодов. При использовании смарт-контрактов в ходе его выполнения нельзя изменить его условия или каким-то образом договориться. При нарушении условий чейнкода неминуемо произойдет выполнение соответствующих санкций. Программный код, лежащий в основе умного контракта, может функционировать некорректно из-за допущенных на стадии программирования ошибок, что повлечет неправильное исполнение условий контракта или может создать возможность для мошеннических действий.

Смарт-контракты обычно рассматриваются в качестве инструментов, избавляющий все стороны данного от необходимости подготовки письменных документов и использования небезопасных способов передачи информации. С точки зрения информационной безопасности в настоящее время заключение сложных смарт-контрактов является сомнительным. К слабостям чейнкодов относят в соответствии с [49] уязвимости, которые связаны с ошибками при их составлении и выполнении, с логикой, а также с юридическими аспектами.

Профессиональные посредники на фондовом и финансовом рынках обычно являются специалистами в соответствующих сферах. Их участие приводит к удорожанию классических контрактов, однако отказ от посредников приводит к повышению рисков для всех участников смарт. Согласно [49] использование СРР не приводит к распределению операционного риска между участниками, а концентрирует их на узле, являющимся самым слабым с точки зрения информационной безопасности. В СРР, в которых реализуются смарт-контракты, необходимо находить компромисс между обычной для классических СРР анонимностью и необходимой в соответствии с законодательством для всех финансовых систем идентификацией клиентов. Обеспечение информационной безопасности СРР с реализованными в них смарт-контрактами изучено к настоящему времени недостаточно, поэтому, к примеру в [26] рекомендуют избегать критически важных функций на основе чейнкодов. Отметим, что главный разработчик смарт-контрактов проекта Stratis Джордан Эндрюс уверен [13], что увеличение применения формальных проверок должно сделать смарт-контракты менее уязвимыми [1]. В статье [65] для платформы Эфириум рассматривается подход к проверке функциональных свойств смарт-контрактов методом символьной верификации модели, что позволяет автоматизировать процесс их сертификации на предмет бизнес-логики [64]. К этой же субтехнологии относятся уязвимости связанные с реализованным в СРР языком программирования, на котором пишутся умные контракты. К примеру в «The DAO», основанной на СРР Эфириум, злоумышленникам удалось реализовать в чейнкоде «рекурсивный вызов» – то есть бесконечную операцию, позволяющую бесконечно снимать криптовалюту и переводить ее на нужный счет.

Рассмотренные выше уязвимости и ограничения нельзя относить ко всем сертифицируемым СРР-платформам, поскольку платформы имеют разную архитектуру. Конкретные исследования нужно проводить в зависимости от того, какие конкретно субтехнологии и каким образом реализованы в данной СРР.

Еще можно отметить ограничение, не связанное непосредственно с конкретной субтехнологией. Это интероперабельность СРР, т.е. функциональное взаимодействие различных СРР-платформ. Данной проблемой в ТК-159 занимается рабочая группа № 5, статья руководителя которой о работе технического комитета была недавно размещена на Хабре [25]. Интеграция нескольких СРР-платформ в одну СРР в настоящее время является сложной задачей по ряду причин, к которым относят различия в механизмах консенсуса, наличие или отсутствие в возможности использовать смарт-контракты и т.д. Также стоит отметить имеющееся отсутствие спроса на интеграцию со стороны пользователей в силу малого количества внедрённых СРР-решений и недостаток необходимости их интеграции с централизованными системами.

Современные исследователи [7] выделяют три логические схемы интеграции СРР:

1. Нотариальная схема: использование набора участников, осуществляющих мониторинг сторонней СРР А и “нотариально” заверяющих действия в СРР Б, куда переносятся данные. В этом случае необходимо наличие выделенной СРР В для управления участниками нотариальной схемы (может совпадать с А или Б).

2. Схемы ретрансляции: с использованием смарт-контрактов или мультиподписи. Смарт-контракт или иной механизм CPP А может отслеживать и воздействовать на состояние CPP Б. В этом случае нет необходимости в выделенной CPP, как в предыдущем случае, но одна из CPP (А или Б) назначается ведущей. Сейчас описаны две схемы ретрансляции:

- односторонняя схема ретрансляции, которая реализует связь только в одну сторону [3];
- двухсторонняя схема ретрансляции, которая реализует связь в обе стороны [2];

3. Блокировка с использованием хеш-функций. CPP А и CPP Б отслеживают одну и ту же хеш-функцию. В отличие от схемы ретрансляции здесь нет необходимости в функции ведущего – достаточно только обмена хешами. В этом случае минимизируется объем передаваемой информации, необходимой для интеграции.

Применений механизмов интеграции между несколькими CPP-платформами в промышленных решениях пока не предъявлено, согласно [47], из-за ограничений их масштабируемости и малого опыта эксплуатации технологий. Однако исследования проводятся. Из них можно выделить такие, как

- реализация двухсторонней схемы ретрансляции для двух выделенных CPP-платформ Dogetherium [14];
- реализация протокола Interledger, осуществляющая атомарный обмен (механизм обеспечения гарантированного обмена условными единицами между двумя CPP) [6];
- проекты Cosmos [5] и PolkaDot [15], реализующие нотариальную схему работы для множества CPP-платформ.

Основываясь на этих уязвимостях и ограничениях и можно схематически оценить какие исследования должна проводить специализированная организация в ходе сертификации, и на что нужно обратить внимание разработчикам сертифицируемых CPP-систем.

Рассмотрим единственный на настоящий момент пример сертифицированной CPP-платформы.

Пример сертифицированной системы распределенного реестра

26 ноября 2019 года Ассоциация развития финансовых технологий (ФинТех) получила сертификат ФСБ России на СКЗИ «Мастерчейн» версии 1.0 [34], с которым можно ознакомиться на рисунке 2.



Рис. 2. Сертификат ФСБ России на СКЗИ «Мастерчейн» версии 1.0

Мастерчейн – это российская национальная CPP-платформа для банковских сервисов, целью внедрения которой являлась необходимость разработки решения для финансового рынка,

где участники могли бы реализовывать свои проекты на базе СРР в соответствии с требованиями российского законодательства, с использованием современных решений.

На рисунке 3 из [22] представлено графическое описание взаимодействия организаций, использующих Мастерчейн для своих бизнес-процессов.

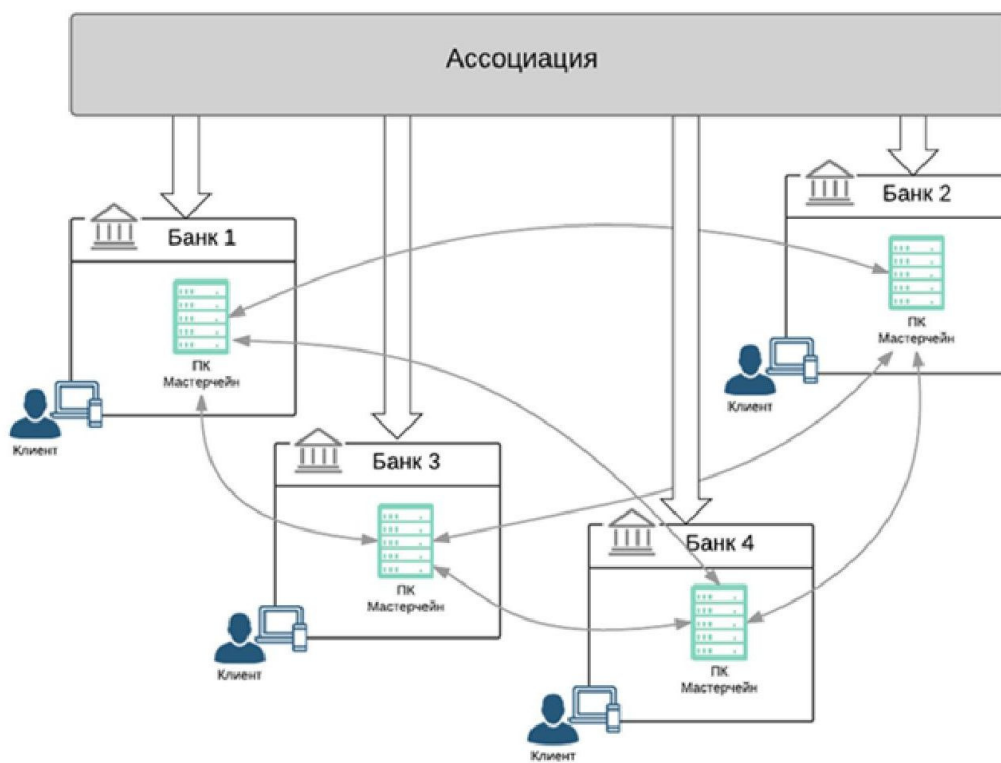


Рис. 3. Схема взаимодействия организаций, использующих Мастерчейн для своих бизнес-процессов

Развитием платформы занимается ассоциация ФинТех, в которую входят ведущие банки и финансовые организации РФ во главе с Банком России.

Использование субтехнологий СРР позволяет платформе создать доверительную среду для участников финансового рынка, в которой информация о транзакциях и данных безопасно хранится и передается, а операционные издержки уменьшены по сравнению с обычными финансовыми информационными системами.

К особенностям «Мастерчейн» можно отнести следующее [22]:

- 1) платформа построена на базе СПП Эфириум, в которой криптографические алгоритмы изменены на соответствующие национальным стандартам;
- 2) процессы идентификации пользователей и масштабирования доработаны с учетом требований законодательства РФ;
- 3) в цепной записи данных СРР-платформы не хранятся информация ограниченного доступа;
- 4) в рамках российской юрисдикции информация, обрабатываемая в «Мастерчейн», обладает юридической значимостью;
- 5) нет технической необходимости в посредниках, которым доверяют пользователи;
- 6) поддержка умных контрактов;
- 7). единая точка отказа на СРР-платформе отсутствует;
- 7) для ресурсов, которые расходуются пользователями на поддержку работы СРР-платформы проводится независимый учет.

Согласно [34] Мастерчейн – это безопасная благодаря конструкции (Secure By Design) система, построенная в соответствии с безопасной архитектурой, в которой присутствуют с несколькими уровнями защиты от сетевого до прикладного уровня. Конфиденциальная информация пользователя хранится за пределами цепной записи или цепочки данных.

Безопасность доступа к этой информации обеспечивается использованием криптографических алгоритмов, удовлетворяющих национальным стандартам. Также Мастерчейн защищен от атаки противника, перехватывающего трафик с целью создать свою цепочку данных, отличную от эталонной. В терминах [44] Мастерчейн является закрытой сетью распределенных реестров с защитой от несанкционированного доступа.

Летом 2019 года Сбербанк сообщил в средствах массовой информации о неудовлетворенности Мастерчейном и желании использовать в дальнейшем такие корпоративные CRR-платформы Hyperledger Fabric или Quorum [32]. Тем не менее, со второго полугодия 2020 года Сбербанк начал в Мастерчейне промышленную эксплуатацию системы учета электронных складных по сделкам с недвижимостью [52].

Весной 2020 года ПАО "Газпром нефть" подтвердила соответствие платформы Мастерчейн требованиям компании по работе с банковскими гарантиями [18] и запланировала его промышленное использование до конца этого года (подтверждений использования на начало 2021 года в открытых источниках не появилось).

CRR Мастерчейн успешно прошел сертификацию, в ходе которой в роли специализированной организации выступила компания КриптоПро, участвовавшая в ее разработке [34].

В 2019 году в средствах массовой информации было объявлено, что ФСБ одобрила еще одного российского CRR-разработчика – компанию «Концерн-Гранит», которая получила сертификат на комплекс программ «Купол-СКЗИ» [60]. Однако в сертификате, который приведен на рисунке 4, указано что он не для СКЗИ (т.е. комплекс не является CRR-платформой и даже просто СКЗИ, несмотря на название), а выдан только средству защиты информации.



Рис. 4. Сертификат ФСБ России на средство защиты информации «Комплекс программ «Купол-СКЗИ»

Вызывает интерес также, что в Москве функционирует автоматизированная блокчейн-платформа [30] или CRR «Активный гражданин», про сертификацию которой, несмотря на явное наличие в ней персональных данных, ничего не известно. Также ничего не известно про сертификацию государственной информационной системы «Семеноводство», в которой также

используется технология СРР [37]. Архитектура данной платформы была сообщена экспертному сообществу разработчиками на конференции DLTReg 2019.

Заключение

Подводя итоги данной статьи, постараемся сформулировать набор исследований, который должен проводиться специализированной организации в ходе сертификационных исследований СРР. Отметим, что еще в конце 2019 года в [34] было объявлено, что специалисты КriptoПро не только проверили реализацию требований по информационной безопасности к СКЗИ Мастерчейн, но и разработали методы анализа информационной безопасности для СРР. В личном разговоре с представителями КriptoПро было выяснено, что готовой методики проведения сертификации именно СРР у них не существует, однако в их выступлениях на конференциях были освещены отдельные аспекты, которые необходимо учитывать в ходе испытаний СРР [16]. При этом проблемы, которые могут возникнуть предлагалось решать исключительно с помощью использования программного обеспечения КriptoПро. Представляет определенный интерес также работа [30], в которой приведены результаты системного анализа и обоснования комплекса организационно-правовых и технологических мероприятий по снижению информационных уязвимостей автоматизированных СРР.

Кроме стандартных сертификационных испытаний СРР как обычного программного обеспечения необходимо:

1. Проводить проверку СРР на устойчивость к известным атакам на блокчейн-системы [29];
2. Проверять достаточность пропускной способности СРР для применения в заявленных разработчиками условиях;
3. Проверять соответствие используемых криптографических алгоритмов (шифрования, хеширования, электронной подписи) национальным стандартам и методическим рекомендациям, используя специально подобранные тестовые последовательности данных;
4. Проверять различные аспекты функционирования ключевой системы (сроки действия, назначение, защиту при эксплуатации и т.п.);
5. Оценивать способы хранения и обработки конфиденциальных данных в СРР в случае, если они обрабатываются системой;
6. Проверять защиту СРР от несанкционированного доступа, процедуры аутентификации при их наличии;
7. Проверять обоснованность выбора процедуры прихода к консенсусу и выбора типа СРР в соответствии с [35] в зависимости от ее назначения;
8. При использовании в СРР субтехнологии создания и исполнения децентрализованных приложений и смарт-контрактов проводить по возможности автоматизированную проверку стандартных смарт-контрактов на предмет бизнес-логики в соответствии с [64];
- 9 В случае если в сертифицируемой СРР предусмотрено функциональное взаимодействие нескольких СРР-платформ, необходимо проводить проверку интероперабельности, процедуру которой еще необходимо разработать.

Отметим, что в связи со вступлением в 2021 году в силу закона о цифровых активах [58], создающего регулируемое правовое поле [46] для использования технологии СРР, задача сертификации СРР-платформ становится еще более актуальной. В конце 2020 года руководство Сбербанка сообщило о планах выпуска собственной криптовалюты [59], а в январе 2021 подало заявку в Центробанк РФ с просьбой зарегистрировать СРР-платформу под названием «сберкоин» [51]. В начале декабря 2020 г. руководство Банка России заявило об эмитировании цифрового рубля без указания сроков эмиссии [28], рассмотрев в докладе для общественных консультаций [62] возможность использования для эмиссии в том числе и технологии СРР.

Таким образом, необходима разработка пошаговой методики сертификации СРР с точки зрения информационной безопасности, которая поможет разработчикам СРР-платформ строить их при необходимости такими, какими они должны быть для успешного прохождения сертификации в соответствии с существующим законодательством.

Интересен факт, что современные исследователи уже задумываются о применении технологии CPP в самом процессе сертификации [53].

Сертификация CPP, как и любого программного обеспечения, вообще является частным случаем экспертизы, которая в свою очередь является одним из методов верификации. На проходившем в 2019 году обсуждении CPP [66] руководителем департамента программной инженерии НИУ ВШЭ Авдошиным С.М. было предложено выделить в CPP еще одну субтехнология – технологии тестирования, верификации и валидации CPP. На настоящий момент данная субтехнология в целом является практически неизученной. Ей как единой субтехнологии посвящена пока только одна статья [12].

Литература

1. April Вопрос на миллиард долларов – устранение ошибок в смарт-контрактах // Электрон. дан. – Заглавие с экрана. Режим доступа: <https://bits.media/vopros-na-milliard-dollarov-ustranenie-oshibok-v-smart-kontraktakh/>
2. Back A., Corallo M., Dashjr L., Friedenbach M., Maxwell G., Miller A., Poelstra A., Timon J., & Wuille P. Enabling Blockchain Innovations with Pegged Sidechains // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.blockstream.com/sidechains.pdf>
3. BTCRelay. a bridge between the Bitcoin blockchain & Ethereum smart contracts // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://btreelay.org>
4. Cambridge Bitcoin Electricity Consumption Index // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://cbeci.org>
5. Cosmos. A Network of Distributed Ledgers. Whitepaper. // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://cosmos.network/cosmos-whitepaper.pdf>
6. Hyperledger Quilt // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.hyperledger.org/projects/quilt>
7. Jin, H., Dai, X., & Xiao, J. Towards a Novel Architecture for Enabling Interoperability amongst Multiple Blockchains // 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS). pp. 1203-1211.
8. Mindsmith. Блокчейн-революция в банках и финансовых институтах: текст отчета, октябрь 2020 года // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://mindsmith.io/map/>
9. Mindsmith. Карта российской корпоративной блокчейн-экосистемы. Текущий статус и перспективы развития в России. Барьеры и возможности для нового бизнеса: текст отчета, октябрь 2019 года // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://mindsmith.io/map/>
10. O'Neal S. Who scales it best? Inside blockchains' ongoing transactions per second race // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://cointelegraph.com/news/who-scales-it-best-inside-blockchains-ongoing-transactions-per-second-race>
11. Pankov K. Enumeration of Boolean Mapping with Given Cryptographic Properties for Personal Data Protection in Blockchain Data Storage // 24th Conference of Open Innovations Association (FRUCT), 2019. С. 300-306.
12. Pankov K.N. Testing, verification and validation of distributed ledger systems // 2020 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia, 2020. С. 1-9.
13. Sedgwick K. The Billion-Dollar Quest to Eliminate Smart Contract Bugs // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://news.bitcoin.com/the-billion-dollar-quest-to-eliminate-smart-contract-bugs/>
14. Teutsch J., Straka M., Boneh D. Retrofitting a two-way peg between blockchains // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://arxiv.org/abs/1908.03999>.
15. Wood G. Polkadot: vision for a heterogeneous multi-chain framework. DRAFT 1 // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://polkadot.network/PolkaDotPaper.pdf>.
16. Багин Д.В. Аспекты безопасности решений на основе распределенного реестра в свете российских требований. Презентация выступления на конференции РусКрипто 2019 // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.ruscrypto.ru/resource/archive/rc2019/files/12_Bagin.pdf.
17. Борисов С. СКЗИ в финансовых организациях // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.securitylab.ru/blog/personal/sborisov/349377.php>
18. "Газпром нефть" подтвердила соответствие платформы Мастерчейн требованиям компании по работе с банковскими гарантиями // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.comnews.ru/content/207319/2020-05-26/2020-w22/gazprom-neft-podtverдила-sootvetstvie-platformy-mastercheyn-trebovaniyam-kompanii-rabote-bankovskimi-garantiyami>

19. ГОСТ 54581-2011 «Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к ИТ» // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://allgosts.ru/35/040/gost_r_54581-2011.pdf.
20. ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://docs.cntd.ru/document/1200075565>.
21. ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://docs.cntd.ru/document/1200123702>.
22. Децентрализованная сеть обмена и хранения информации «МАСТЕРЧЕЙН» Версия 1.1 Whitepaper // Электрон. дан. – Заглавие с экрана. – Режим доступа: http://www.tadviser.ru/images/a/ad/Masterchain_whitepaper_11_08.pdf.
23. Документы по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii#>.
24. Дорожная карта развития «сквозной» цифровой технологии «Системы распределенного реестра» // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://digital.gov.ru/uploaded/files/07102019srr.pdf>.
25. Дружинин И. Тернистый путь стандартизации блокчейн технологий в России. 18 декабря 2020 г. // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://habr.com/ru/post/533682>.
26. Елистратов А., Маршалко Г., Светушкин В. Подводные камни сертификации блокчейн-решений // Открытые системы. СУБД, 2019, № 01 – Режим доступа: <https://www.osp.ru/os/2019/01/13054747>.
27. Ерохин С.Д. Блокчейн – новая организационная парадигма координации деятельности // Электросвязь, 2018, № 03, с. 16-19
28. Касми Э. Цифровой рубль заберет прибыль у банков и отдаст ее россиянам // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.cnews.ru/news/top/2021-01-28_tsifrovoj_rubl_otberet_pribyl.
29. Колесников П., Бекетнова Ю., Крылов Г. Технология блокчейн. Анализ атак, стратегии защиты. Саарбрюккен, LAP LAMBERT Academic Publ., 2017, 76 с.
30. Ловцов Д.А. Информационная безопасность автоматизированных блокчейн систем: угрозы и способы повышения // Трансформация национальной социально-экономической системы России. Материалы II Международной научно-практической конференции. М., Российский государственный университет правосудия, 2020. С. 464-473.
31. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации. М.: Юрайт, 2016. 473 с.
32. Маврина Л. Сбербанк устал от блокчейна // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://expert.ru/2019/07/3/sberbank-ustal-ot-blokchejna/>
33. Максуров А.А. Криптовалюты и правовое регулирование их обращения. М., Дашков и К, 2019, 356 с.
34. Мастерчейн (Masterchain). Российская национальная блокчейн-сеть // Электрон. дан. – Заглавие с экрана. – Режим доступа: [https://www.tadviser.ru/index.php/Продукт:Мастерчейн_\(Masterchain\)_Российская_национальная_блокчейн-сеть](https://www.tadviser.ru/index.php/Продукт:Мастерчейн_(Masterchain)_Российская_национальная_блокчейн-сеть)
35. Методические рекомендации ТК-26 МР 26.4.001-2018 «Термины и определения в области технологий цепной записи данных (блокчейн) и распределенных реестров» // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://tc26.ru/standarts/metodicheskie-rekomendatsii/mr-26-4-001-2018-terminy-i-opredeleniya-v-oblasti-tekhnologiy-tsepnoy-zapisi-dannykh-blokcheyn-i-raspredeleennykh-reestrov.html>.
36. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. «Цифровые технологии» // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://digital.gov.ru/ru/activity/directions/878/#section-docs>.
37. Минсельхоз России разработал прототип системы прослеживаемости семян // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://kvedomosti.ru/news/minselxoz-rossii-razrabotal-prototip-sistemy-proslezhivaemosti-semyan.html>
38. Нормативная база в области технологий распределенного реестра и блокчейн: промежуточный отчет о НИР / Рабочая группа №2 ТК-159 рук. Панков К.Н. М., 2019. – 61 с. // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://yadi.sk/i/fWG5744WAlDcgA>
39. Павлов В. Сертифицированные vs несертифицированные средства защиты информации: требования регулятора или реальная необходимость? // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://habr.com/ru/company/acribia/blog/521162>.

40. Панков К.Н. Использование криптографических средств для сквозных цифровых технологий на примере систем распределенного реестра // Сборник трудов XII Международной научно-технической конференции «Технологии информационного общества». Москва, Московский технический университет связи и информатики (МТУСИ), 14-15 марта 2018 г. В 2-х томах. Том 1. М.: ИД Медиа Паблишер», 2018. С. 365-466.
41. Паспорт национальной программы «Цифровая экономика Российской Федерации» // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://static.government.ru/media/files/urKHm0gTPPnzJlaKw3M5cNLo6gczMkPF.pdf>
42. Приказ ФСБ РФ от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)" // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://base.garant.ru/187947>.
43. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://fstec.ru/component/content/article/110-tehnicheskaya-zashchita-informatsii/dokumenty/prikazy/703-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17>.
44. Развитие технологии распределенных реестров. Доклад для общественных консультаций. Декабрь 2017. ЦБ России // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://cbr.ru/Content/Document/File/36007/reestr_survey.pdf.
45. Разработка методов и средств функционирования и обеспечения информационной безопасности распределенных реестров, предназначенных для архивирования данных: отчет о НИР / Московский технический университет связи и информатики; рук. Саксонов Е. С. М., 2019. 172 с. № ГР АААА-Б20-220020790217-8.
46. Реакция отрасли: закон «О цифровых финансовых активах» сильно запаздывает // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://ict.moscow/news/cryptocurrency-law>.
47. Реализация блокчейн-экосистем в финансовой инфраструктуре рынка: ограничения и возможности. Национальный расчетный депозитарий. Whitepaper. 2019 // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.nsd.ru/common/img/uploaded/WP-blockchain-lab-rus.pdf>.
48. Рекомендации по стандартизации Р 1323565.1.012-2017 «Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации» // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://docs.cntd.ru/document/556323231>.
49. Репин М.М., Пиехотская Е.А. Обеспечение информационной безопасности смарт-контрактов в системах на основе технологии распределенных реестров // Системный администратор, 2019, №05 (198), – Режим доступа: <http://samag.ru/archive/article/3880>.
50. Сазанова Е.В. Технология блокчейн в контексте информационной безопасности // Научно-техническое и экономическое сотрудничество стран атр в XXI веке, 2019, № 01. С. 94-97.
51. Сбербанк подал заявку на регистрацию собственного стейблкоина // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://iz.ru/1114488/2021-01-21/sberbank-podal-zaiavku-na-registraciiu-sobstvennoi-kriptovaliuty>.
52. Сбербанк рассказал о выпуске электронных закладных на базе платформы «Мастерчейн» // Системный администратор, 2019, №05 (198), – Режим доступа: <https://rns.online/finance/Sberbank-rasskazal-o-vipuske-elektronnih-zakladnih-na-baze-platformi-Masterchein-2020-07-28>.
53. Старожук Е.А., Яковлева М.В. Разработка алгоритма сертификационных испытаний технических средств на основе применения блокчейна // Вопросы инновационной экономики. 2019. Т. 9. № 3. С. 1177-1192.
54. Указ Президента Российской Федерации от 06.03.1997 г. N 188 "Об утверждении перечня сведений конфиденциального характера" // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://base.garant.ru/10200083>.
55. Указ Президента Российской Федерации от 07.05.2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» России // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.kremlin.ru/acts/bank/43027>.
56. Условия по защите информации (утв. Банком России 5 октября 2020 г.) России // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.garant.ru/products/ipo/prime/doc/74812340>.
57. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и защите информации» // Электрон. дан. – Заглавие с экрана. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798.

58. Федеральный закон от 31 июля 2020 г. № 259-ФЗ "О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации" // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.garant.ru/products/ipo/prime/doc/74351466>.

59. *Фомин Д.* Сбербанк сообщил о планах запустить сервис для покупки цифровых активов // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.rbc.ru/crypto/news/5fc502b29a794728d3689fe3>.

60. ФСБ одобрила еще одного российского блокчейн-разработчика // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://yandex.ru/turbo/forklog.com/s/fsb-odobrila-eshhe-odnogo-rossijskogo-blokchejn-razrabotchika>.

61. Центр по лицензированию, сертификации и защите государственной тайны ФСБ России. // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://clsz.fsb.ru/common.htm>.

62. Цифровой рубль. Доклад для общественных консультаций. Октябрь 2020. ЦБ России // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://cbr.ru/StaticHtml/File/112957/Consultation_Paper_201013.pdf.

63. *Шиверов П.К., Бондаренко В.В.* Понятие доверия в контексте информационной безопасности // Информационные технологии и нанотехнологии (ИТНТ-2016). Материалы Международной конференции и молодёжной школы. Самарский государственный аэрокосмический университет имени академика С.П. Королёва (национальный исследовательский университет), 2016. С. 414-418.

64. *Шишкин Е.С.* Автоматическая сертификация смарт-контрактов на предмет надежности их бизнес-логики. Презентация выступления на конференции РусКрипто 2019 // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.ruscrypto.ru/resource/archive/rc2019/files/12_Shishkin.pdf.

65. *Шишкин Е.С.* Проверка функциональных свойств смарт-контрактов методом символьной верификации модели // Труды института структурного программирования РАН, 30:5 (2018). С. 265-288.

66. Экспертное обсуждение классификаторов цифровых технологий и связанных с ними цифровых продуктов и услуг // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://issek.hse.ru/announcements/319001229.html>.

РАЗРАБОТКА МОДЕЛИ И АЛГОРИТМОВ ОЦЕНКИ ЭФФЕКТИВНОСТИ ПРОЦЕДУРЫ РАСПРЕДЕЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫХ РЕСУРСОВ В СЕТЯХ 5G

Петров Дмитрий Сергеевич,

*Московский физико-технический институт (национальный исследовательский университет),
магистрант, Москва, Российская Федерация*

petrov.ds@phystech.edu

Аннотация

В данной статье рассматривается проблема распределения ресурсов 5Gсети между различными классами гетерогенного mMTCтрафика, лежащего в основе M2Mкоммуникаций в сетях 5G. Целью исследования является разработка модели процедуры «networkslicing» и алгоритмов оценки ее эффективности. Для успешного решения поставленной задачи были изучены сценарии ранних запусков 5Gсетей, что дало возможность построить математическую модель, которая учитывает особенности архитектуры сетей 5-ого поколения.

Ключевые слова

5G, slicing, mMTC, Erlang, MMPP, resource sharing.

Введение

Еще на этапе стандартизации 5G сетей стало понятно, что к таким сетям предъявляются поистине революционные требования: пиковая скорость передачи – 20Гбит/с, максимальная задержка – 0.5мс, плотность подключения – 1млн/км². Предыдущие стандарты связи следовали парадигме «one size fits all», которая заключается в предоставлении единообразного обслуживания на базе общего ресурса независимо от типа трафика. Ввиду высокой неоднородности обслуживаемого трафика, а также увеличенной плотности подключений, такая парадигма становится неактуальной для стандартов 5G. С целью удовлетворить всем требованиям, в рамках стандартов пятого поколения была разработана концепция 5G «network slicing», позволяющая динамически выделять ресурсы в виде отдельных логических сегментов сети под каждый тип трафика. На настоящий момент слайсинг является очень перспективной технологией, однако математические модели, позволяющие выработать алгоритм оптимального выделения ресурсов в рамках этой технологии, еще не были представлены. Также ни в одной из изученных научных работ не делался упор на соответствие предложенных расчетов реальной архитектуре 5Gсетей, так как на момент их написания сети нового поколения еще не вошли в фазу активного внедрения. Данная статья нацелена на покрытие всех вышеупомянутых пробелов.

Результаты исследований

В рамках технологии «networkslicing» все создаваемые сетевые слайсы опираются на единую физическую инфраструктуру. Это значит, что невозможно создать бесконечное количество слайсов, ведь в определенный момент ресурсы физической сети истощатся и новые слайсы будут не в состоянии обеспечить запрашиваемое качество обслуживания. Это приводит к пониманию того, что в реальной жизни операторы связи выделяют сетевые слайсы не под конкретную заявку, а под группы заявок, которые в общем случае могут быть неоднородными в плане требуемых ресурсов и характеристик обслуживания. Соответственно, перед операторами встает задача оптимального распределения ресурсов сетевого слайса под различные типы заявок (иными словами, типы трафика) – своего рода вторичный слайсинг, при котором уже существ-

вующий слайс делится на слайсы меньшей ресурсной емкости. Конечной целью при этом может являться выравнивание потерь для всех типов заявок, достижение экономической эффективности использования ресурсов и другие.

При составлении модели были учтены, как аналитические метрики, такие как вероятность обрыва сеанса с конкретным потоком заявок, так и сетевые метрики, такие как эффективность утилизации узлов сети. Для этих целей было решено взять два типа трафика и, тем самым, определить два типа заявок. Трафик, идущий от городских камер видеонаблюдения (в дальнейшем будет обозначаться как CCTV), является первым типом трафика, который можно охарактеризовать как обеспечивающий дискретное поступление группы заявок непостоянной интенсивности, требовательных к объему предоставляемого ресурса. Также был задан второй тип трафика – трафик M2X, характерный только для сетей пятого поколения. Этот трафик отличается очень малой потребностью в ресурсах, но очень большим количеством поступающих практически непрерывно заявок. Этот тип трафика используется в тестовых сетях 5G для межмашинного взаимодействия между объектами дорожной инфраструктуры и сетью. А значит, объем поступающих M2X заявок непостоянен и возможны как проседания, так и всплески по количеству заявок в единицу времени. В рамках выбранных типов трафика были рассмотрены возможные стратегии распределения ресурсов [1, 2].

Существует несколько возможных стратегий распределения ресурсов в рамках слайса. Самый простой сценарий распределения – статическое распределение (рис. 1а), при котором вся имеющаяся в распоряжении слайса ресурсная емкость заранее делится в определенных пропорциях для трафика различных типов. Пропорции, в которых ресурсы в рамках такого статического деления распределяются между вторичными слайсами, как правило, рассчитываются еще на этапе планирования сети, в то время как сами вторичные слайсы создаются и резервируются уже на этапе активации виртуальных сетевых функций на сети. Очевидно, что такое фиксированное распределение ресурсов может быть относительно легко (относительно динамических моделей распределения) проанализировано математическими методами, а также для такого распределения может быть составлена относительно несложная математическая модель. Однако, за кажущейся простотой данного сценария скрывается одно из самых нежелательных явлений – неэффективное использование выделенных ресурсов. Действительно, если известно, что в некие критические моменты времени для обслуживания mMTC трафика может потребоваться пиковая пропускная способность в 100 Мбит/с, то оператор связи будет обязан статически закрепить за слайсом, выделенным под межмашинные коммуникации, 100 Мбит/с независимо от средней планируемой нагрузки на сеть. Таким образом, за исключением моментов пиковой нагрузки на сеть, будет наблюдаться простаивание значительной части зарезервированных ресурсов, которые в рамках сценария статического распределения невозможно перераспределить в пользу других слайсов [3].

В противоположность предыдущему сценарию, существует множество сценариев динамического распределения ресурсов слайса. Один из них (рис. 1б) заключается в предоставлении полной емкости слайса для поступающего гетерогенного потока заявок. В таком случае, ресурсы внутри слайса постоянно перераспределяются по вторичным слайсам исходя из требований, содержащихся в поступающих на эти слайсы заявках. Однако, данный подход имеет свои недостатки, так как здесь также возможно неконтролируемое распределение ресурсов в пользу заявок с относительно невысокими требованиями к скорости передачи данных.

Другой подход динамического распределения (рис. 1в) ресурсов заключается в выделении некоторой части ресурсов слайса в общее пользование, в то время как из оставшейся части ресурсов формируются вторичные слайсы, предоставляемые в эксклюзивное пользование каждому определенному типу (группе) заявок. Оба сценария динамического распределения ресурсов требуют более сложного математического исследования, зато обеспечивают высокую эффективность утилизации ресурсов сети.

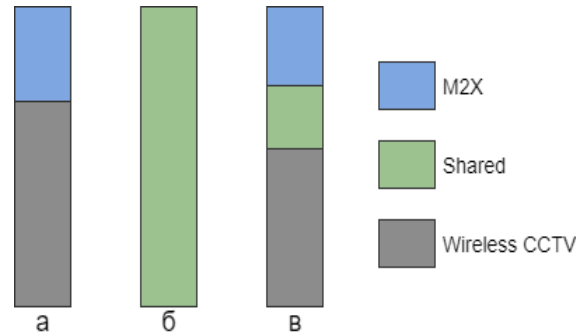


Рис. 1. Три сценария распределения ресурсов сети

Модель сети, использованная в данной работе, состоит из радиointерфейса 5G, расположенного в центре 5G соты, набора виртуальных сетевых функций, осуществляющих установление соединения и управление процессом слайсинга, а также потоков трафика от камер видеонаблюдения и устройств дорожной инфраструктуры. Объем доступных ресурсов радиointерфейса и соответствующих ему сетевых компонентов будет измеряться в ресурсных единицах минимально возможной ресурсоемкости. Очевидно, что M2X трафик предъявляет минимальные требования к ресурсам сети, соответственно, мы измеряем объем ресурсов в ресурсных единицах M2X трафика, но для простоты называем их просто ресурсными единицами или РЕ. Предположим, что суммарное количество доступных РЕ является линейной функцией от количества ресурсных блоков (сокр. РБ) радиointерфейса. Обозначим за ν суммарное количество РЕ, а за c – скорость передачи трафика из расчета на 1 РЕ. Предположим также, что различные камеры предъявляют разные требования к качеству обслуживания. Это означает, что объем передаваемого камерами трафика неодинаков и меняется от камеры к камере в зависимости от ее потребностей в качестве обслуживания. Для учета данной особенности поступающего трафика, в рамках нашей модели будем считать, что в сеть поступает n типов потоков трафика камер видеонаблюдения. Предположим, что заявки на обслуживание k -ого типа трафика камер видеонаблюдения поступают в систему спустя некое случайное время, которое подчиняется экспоненциальному распределению с параметром λ_k . Каждая установленная на основе такой заявки сессия связи требует b_k РЕ для обслуживания и занимает данные ресурсы в течение случайного времени, распределенного экспоненциально с параметром распределения μ_k , где $k = 1, \dots, n$. Также предположим, что заявки на обслуживание M2X трафика поступают в систему спустя некое случайное время, которое подчиняется экспоненциальному распределению с параметром λ_d . Каждая установленная на основе такой заявки сессия связи требует b_d РЕ для получения и обработки файлов, подчиняющихся экспоненциальному распределению со средним F . M2X сессии связи занимают выделенные ресурсы в течение случайного времени, распределенного экспоненциально со средним значением $\frac{F}{b_d}$ и параметром распределения $\frac{b_d}{F}$. Для обоих типов трафика (как от камер видеонаблюдения, так и от систем дорожной инфраструктуры) предполагается, что заблокированные заявки не восстанавливаются и окончательно удаляются из системы [4, 5, 6].

Теперь опишем модели трех сценариев слайсинга. Самый простой из них заключается в статическом распределении всего количества ν РЕ между двумя типами трафика. Для удобства будем обозначать его как **СТАТ**. Обозначим за ν_i количество РЕ, предоставленных в эксклюзивное пользование CCTV трафику, а, соответственно, за $\nu_b = \nu - \nu_i$ – количество РЕ, предоставленных в эксклюзивное пользование M2X трафику. Варьируя параметры ν_i и ν_b , можно предоставлять приоритет по количеству занимаемых ресурсов либо одному, либо дру-

тому типу трафика. Как будет видно далее, такой способ является наиболее простым, но может привести к очень низкому проценту утилизации доступной ресурсоемкости, что будет означать простой значительной доли ресурсов.

Следующий сценарий слайсинга подразумевает, в некотором смысле, контроль доступа. Далее будем обозначать его как **ДИНРЕЗ**, так как в этом сценарии резервируется часть ресурсов под общие нужды, которая будет динамически распределяться между обоими классами трафика исходя из нагрузки, а часть ресурсов статически распределяется между CCTV и M2X трафиком. Обозначим за c_k максимальное количество сессий CCTV трафика k -ого типа, которые могут быть обслужены одновременно. Обозначим за c_d максимальное количество сессий M2X трафика, которые могут быть обслужены одновременно. Далее будет показано, что, варьируя значения v_k , $k = 1, \dots, n$ и v_d , можно обеспечивать приоритетность в обслуживании того или иного трафика, однако суммарная доля утилизируемых ресурсов будет намного выше по сравнению со статическим сценарием. [3, 7]

Последним из сценариев является сценарий полностью динамического распределения ресурсов сети между CCTV и M2X трафиком. Обозначим его как **ДИН** сценарий. В этом случае не производится никакого предварительного статического резервирования, а ресурсы резервируются в процессе поступления заявок исходя из запрашиваемой потребности в количестве ресурсов. Как будет видно далее, такой сценарий позволяет получить самый высокий процент утилизации сетевых ресурсов, но приводит к неконтролируемому росту потерь заявок.

Все три упомянутых сценария могут быть смоделированы заданием v , v_k , $k = 1, \dots, n$ и v_d , поэтому далее будет обсуждаться только **ДИНРЕЗ** сценарий и соответствующая модель.

Обозначим за $i_k(t)$ количество заявок (или, что аналогично в данном контексте, сессий) от камер видеонаблюдения в рамках k -ого потока, которые обслуживаются сетью в момент времени t . Обозначим за $d(t)$ количество заявок (сессий) от объектов дорожной инфраструктуры, которые обслуживаются сетью в момент времени t . Динамику изменения состояний данной модели можно описать марковским процессом $r(t) = (i_1(t), \dots, i_n(t), d(t))$, который определен на конечном наборе S состояний модели. Соответственно, состояние $r(t)$ обозначим как вектор $(i_1(t), \dots, i_n(t), d(t))$, а набор всех возможных состояний $r(t)$ обозначим как S . Вектор $(i_1(t), \dots, i_n(t), d(t))$ принадлежит S , когда для i_k , $k = 1, \dots, n$ и d выполняются следующие соотношения:

$$0 \leq i_k \leq c_k, k = 1, \dots, n$$

$$0 \leq d \leq c_d$$

$$i_1 b_1 + \dots + i_n b_n + d b_d \leq v$$

Обозначим количество занятых РЕ в состоянии $(i_1(t), \dots, i_n(t), d(t)) \in S$ как $i = i_1 b_1 + \dots + i_n b_n + d b_d$. Обозначим за $p(i_1, \dots, i_n, d)$ стационарную вероятность состояния $(i_1, \dots, i_n, d) \in S$. Ее можно интерпретировать как долю времени, в течение которой модель остается в состоянии (i_1, \dots, i_n, d) . Такая интерпретация стационарных вероятностей дает возможность использовать значения $p(i_1, \dots, i_n, d)$ для оценки основных характеристик модели. Определим долю потерянных заявок для k -ого потока CCTV трафика как π_k , а среднее количество занятых РЕ как m_k . Формально эти величины можно задать следующими соотношениями:

$$\pi_k = \sum_{(i_1, \dots, i_n, d) \in U_k} p(i_1, \dots, i_n, d)$$

$$m_k = \sum_{(i_1, \dots, i_n, d) \in S} p(i_1, \dots, i_n, d) i_k b_k$$

где U_k – подмножество S , содержащее $(i_1, \dots, i_n, d) \in U_k$ при условии, что $i_k + 1 > c_k$ или $i + b_k > v$. Похожим образом определяются характеристики обслуживания M2X трафика, где π_d – доля потерянных заявок, а m_d – среднее количество занятых РЕ.

Система уравнений состояний получается посредством приравнивания интенсивности перехода $r(t)$ из произвольного состояния $(i_1, \dots, i_n, d) \in S$ модели к интенсивности перехода $r(t)$ в состояние (i_1, \dots, i_n, d) и для краткости здесь не представлена. Значения $P(i_1, \dots, i_n)$ должны быть нормированы. [3]

Использование предложенной модели делает возможным анализ эффективности рассмотренных сценариев распределения ресурсов. Уровень нагрузки, создаваемой поступающим трафиком, можно охарактеризовать ρ – предложенной нагрузкой из расчета на 1 РЕ. Для того, чтобы найти ρ , необходимо найти предложенную нагрузку каждого потока, рассматриваемого в модели. Обозначим за A_k предложенную нагрузку со стороны k-ого потока CCTV трафика,

причем $A_k = \frac{\lambda_k}{\mu_k} b_k = a_k b_k$, а за A_d – предложенную нагрузку со стороны потока M2X трафика,

причем $A_d = \frac{\lambda_d}{\mu_d} b_d = a_d b_d = \frac{\lambda_d F}{b_d}$. Тогда значение ρ может быть найдено из следующего соотношения:

$$\rho = \frac{A_1 + \dots + A_n + A_d}{v}.$$

Зададим числовые параметры модели. Пусть $v = 200$ РЕ; минимальная характерная скорость передачи, обеспечиваемая 1 РЕ – $c = 1$ Мбит/с; $n = 1$; $b_1 = 10$ РЕ; $b_d = 1$ РЕ; $F = 1$ Мбит; $1/\mu_1 = 1$ с; $1/\mu_d = 0.1$ с. Числовая оценка характеристик модели начинается с оценки π_1 и π_d , графики для которых представлены на рисунке 2, а также с оценки δ_1 – среднего реального значения утилизации ресурса CCTV трафиком, δ_d – среднего реального значения утилизации ресурса M2X трафиком и их суммы $\delta = \delta_1 + \delta_d$ в сравнении с модельным значением предложенной нагрузки из расчета на 1 РЕ – ρ . График для δ_1 , δ_d и их суммы представлен на рисунке 3. Значения показателей эффективности рассчитаны на основе рекурсивного алгоритма и его улучшений.

Предположим, что оба потока трафика (CCTV и M2X) создают одинаковую предложенную нагрузку $A_1 = A_d = \frac{v\rho}{2}$. Это позволит найти интенсивности λ_1 и λ_d потоков заявок для каждого потока трафика, введенного в модели, зная значения ρ . Несмотря на то, что оба класса трафика – CCTV и M2X – создают одинаковую предложенную нагрузку на сеть, графики 2 и 3 показывают, что M2X трафику предоставляется тем больший приоритет в обслуживании, чем выше ρ . Это становится особенно заметно при значениях $\rho > 1$, то есть в условиях перегрузки сети. В данной работе сравниваются три основных сценария распределения ресурсов сети: **СТАТ**, **ДИН** и **ДИНРЕЗ**. Графики характеристик качества обслуживания для этих трех сценариев представлены на рисунках 4 и 5. На рисунке 4 представлена зависимость доли потерянных CCTV заявок от интенсивности поступающих M2X заявок. На рисунке 5 представлена зависимость среднего значения утилизации РЕ от интенсивности поступающих M2X заявок. Здесь использовались такие же входные параметры модели, как и при построении графиков на рисунках 2 и 3, за исключением того, что мы положили $a_1 = 10$ Эрл. В **СТАТ** сценарии приняли $v_1 = v_b = 100$ РЕ, в **ДИНРЕЗ** сценарии приняли $v_1 = 200$ РЕ, $v_d = 100$ РЕ.

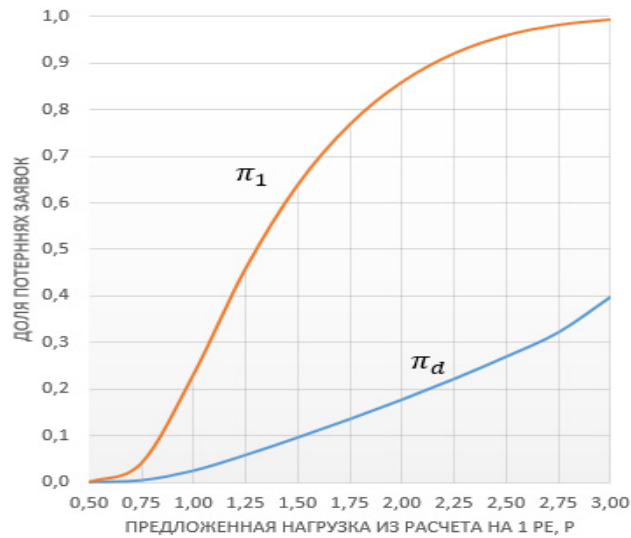


Рис. 2. Доли потерянных заявок для CCTV и M2X трафика

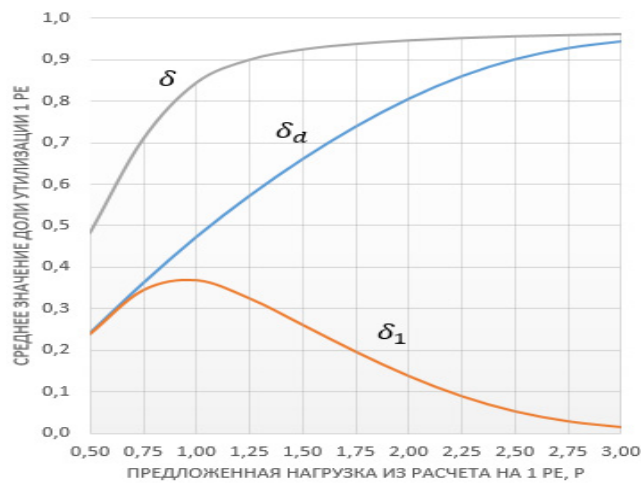


Рис. 3. Значения утилизации 1 РЕ для CCTV и M2X трафика

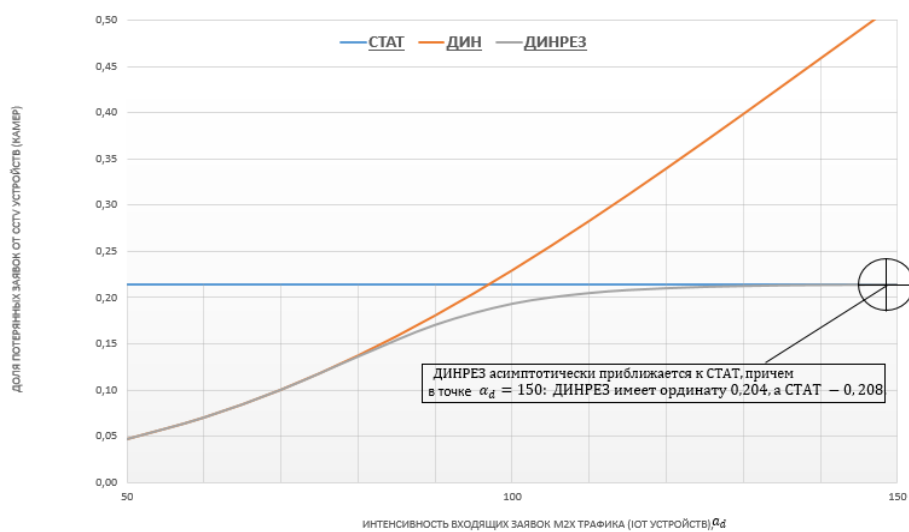


Рис. 4. Зависимость доли потерянных CCTV заявок от интенсивности M2X трафика

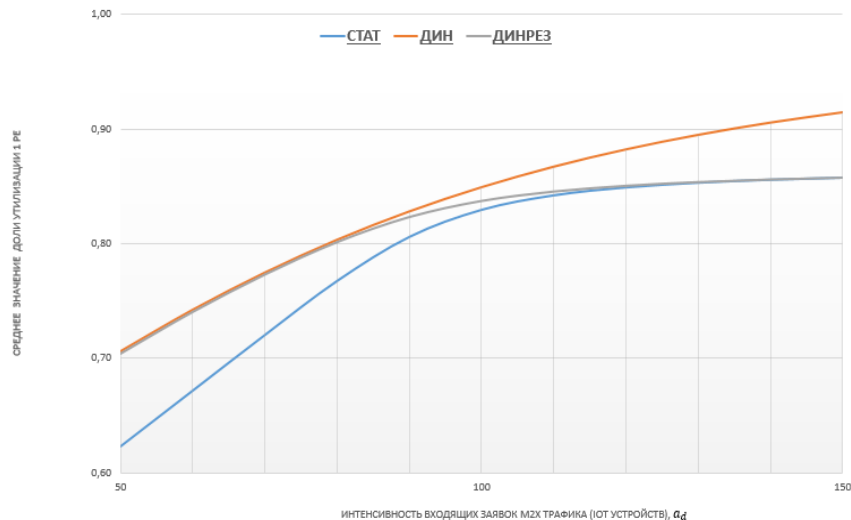


Рис. 5. Зависимость средней доли утилизации ресурсов CCTV трафиком от интенсивности M2X трафика

Заключение

Представленные результаты могут быть обобщены и структурированы следующим образом. Простейший для использования **СТАТ** сценарий слайсинга, в котором ресурсы строго распределяются между устройствами CCTV и потоками M2X трафика устройств IoT, может использоваться для достижения заданных значений показателей производительности, но имеет два недостатка. Во-первых, это высокая степень чувствительности характеристик к величине предлагаемой нагрузки, которая требует априорных знаний об интенсивности поступающего трафика. Во-вторых, это более низкие доли утилизации PE по сравнению с **ДИН** и **ДИНРЕЗ** сценариями.

ДИН сценарий позволяет достичь наиболее высоких показателей утилизации PE, но подвержен неконтролируемому повышению доли потерянных заявок от более требовательного к ресурсам трафика, особенно в случаях перегрузки сети. **ДИНРЕЗ** сценарий превосходит **СТАТ** сценарий, так как оказывается менее чувствительным к величине предлагаемой нагрузки, а также позволяет достичь более приемлемых, по сравнению с **ДИН** сценарием, значений доли потерянных заявок от более требовательного трафика.

Таким образом, **ДИНРЕЗ** сценарий рекомендуется к применению в кейсах ранних запусков 5Gсетей как способный увеличить инертность сетей нового поколения по отношению к возросшей нагрузке на базовые станции и ядро сети, а также уменьшить долю потерянных заявок при обслуживании гетерогенного трафика.

Литература

1. Afolabi I. et al. Network slicing and softwarization: A survey on principles, enabling technologies, and solutions // IEEE Communications Surveys & Tutorials. 2018. Т. 20. № 3. С. 2429-2453.
2. Akyildiz I. F. et al. 5G roadmap: 10 key enabling technologies // Computer Networks. 2016. Т. 106. С. 17-48.
3. Степанов С.Н. Теория телетрафика: концепции, модели, приложения. М: Горячая линия. – Телеком, 2015. 868 с.
4. Bakri S., Frangoudis P. A., Ksentini A. Dynamic slicing of RAN resources for heterogeneous coexisting 5G services // 2019 IEEE Global Communications Conference (GLOBECOM). IEEE, 2019. С. 1-6.
5. Begishev V. et al. Resource allocation and sharing for heterogeneous data collection over conventional 3GPP LTE and emerging NB-IoT technologies // Computer Communications. 2018. Т. 120. С. 93-101.
6. Chen Q., Wang X., Lv Y. An overview of 5G network slicing architecture // AIP Conference Proceedings. – AIP Publishing LLC, 2018. Т. 1967. №. 1. С. 020004.
7. El-Mekawi A., Hesselbach X., Piney J. R. Squatting and kicking model evaluation for prioritized sliced resource management // Computer Networks. 2020. Т. 167. С. 107006.

ИДЕНТИФИКАЦИЯ АНОНИМНЫХ ПОЛЬЗОВАТЕЛЕЙ ВЕБ-РЕСУРСА НА ОСНОВЕ НЕЧЕТКИХ ХЭШ – ФУНКЦИЙ ЦИФРОВЫХ ОТПЕЧАТКОВ УСТРОЙСТВ

Шелухин Олег Иванович,

*Московский Технический Университет Связи и Информатики (МТУСИ),
д.т.н., профессор, заведующий кафедрой «Информационная безопасность», Москва, Россия*
sheluhin@mail.ru

Желнов Максим Сергеевич,

Московский Технический Университет Связи и Информатики (МТУСИ), Москва, Россия
mx306211@yandex.ru

Аннотация

Рассмотрена возможность и целесообразность использования нечеткого хеширования в задачах анализа отпечатков пальцев и идентификации анонимных пользователей. Рассмотрены виды и алгоритмы реализации нечетких хэш-функций в задаче отпечатков пальцев включая кусочное хеширование (Piecewise hashing), контекстно-побуждаемое кусочное хеширование (Context triggered piecewise hashing), выделение статистически маловероятных особенностей (Statistically improbable features) а также алгоритмы блочного перестроения (Block-based rebuilding) и статистические отпечатки. Представлена структура алгоритма извлечения отпечатков на основе нечеткого хеширования. Показано, что алгоритмы нечеткого хеширования sdhash и mvHash имеют наибольшую скорость идентификации анализируемых файлов.

Ключевые слова: идентификация, браузер, отпечаток, нечеткое хеширование, хэш-функции, ssdeep, sdhash, mvHash, анализ данных.

Постановка задачи

Вопрос об идентификации пользователей сети Интернет, владельцев ресурсов в сети Интернет в последнее время становится всё более актуальным. Идентификация пользователей имеет решающее значение для большинства веб-сайтов, с целью предоставления таргетированного контента, либо для отслеживания злоумышленников.

Идентификация анонимных пользователей (деанонимизация) интернет-порталов и идентификация анонимных пользователей веб-ресурса как правило осуществляется на основе цифровых отпечатков устройств. Получил распространение термин «отпечаток» или отпечаток компьютера (браузера) – информация, собранная об удалённом устройстве для дальнейшей идентификации, а под отпечатком понимается сбор этой информации.

Под отпечатком браузера понимается набор информации, относящейся к устройству пользователя, от аппаратного обеспечения до операционной системы, браузера и его конфигурации. Основная концепция, лежащая в основе отпечатка веб браузера заключается в сборе специфичной для устройства информации для таких целей, как идентификация или обеспечение безопасности.

Помимо собственно сбора информации требуется идентифицировать пользователя данного устройства. Для решения этой задачи часто используются хэш-функции цифровых отпечатков устройств. При этом нет необходимости проводить побайтовое сравнение, достаточно посчитать хэш-значение от проверяемого файла, сохранить результат в соответствующей базе данных, имеющей относительно небольшой объем, и сравнить его с исходным. При равенстве хэш-значений с некоторой степенью уверенности можно судить об идентичности файлов, в зависи-

мости от значения уровня коллизий (collision rare) конкретной хэш-функции. Они использовались в основном с целью "идентификации, проверки и аутентификации файловых данных" [10].

Нечеткое хэширование

Результатом сбора информации об устройстве является набор уникальных значений таких как: User Agent; Language; Platform; List of plugin; List of fonts; Canvas; WebGL и т.д.

В качестве примера на рисунке 1 изображен пример списка собранной информации об устройстве. В первой колонке представлены наименования собираемых значений (атрибуты), во второй колонке – источники собираемых значений, в третьей колонке – значения соответствующих атрибутов. С развитием браузеров список уникальных атрибутов может пополняться.

Attribute	Source	Example
User agent	HTTP header	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.119 Safari/537.36
Accept	HTTP header	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Content encoding	HTTP header	gzip, deflate, br
Content language	HTTP header	en-US,en;q=0.9
List of plugins	JavaScript	Plugin 1: Chrome PDF Plugin. Plugin 2: Chrome PDF Viewer. Plugin 3: Native Client. Plugin 4: Shockwave Flash...
Cookies enabled	JavaScript	yes
Use of local/session storage	JavaScript	yes
Timezone	JavaScript	-60 (UTC+1)
Screen resolution and color depth	JavaScript	1920x1200x24
List of fonts	Flash or JS	Abyssinica SIL,Aharoni CLM,AR PL UMing CN,AR PL UMing HK,AR PL UMing TW...
List of HTTP headers	HTTP headers	Referer X-Forwarded-For Connection Accept Cookie Accept-Language Accept-Encoding User-Agent Host
Platform	JavaScript	Linux x86_64
Do Not Track	JavaScript	yes

Рис. 1. Пример извлекаемых параметров устройства

Наиболее часто используемыми криптографическими хэш функциями для обнаружения идентичных известных сигнатур вредоносных программ являются MD5, SHA-1 и SHA-256. Основное различие между этими криптографическими хэш функциями заключается в их длине хэш-значения. Пример идентификации сравниваемых файлов показан на рисунке 2. В качестве хэш функции могут использоваться, например md5.



Рис. 2. Пример использования функции md5

Однако достаточно незначительно изменить некоторый файл для того, чтобы сильно изменить значение хэш-функции, вычисляемой от него. Это следует непосредственно из свойств хэш-функции, в частности, из свойства «лавиного эффекта» [1], согласно которому при незначительном изменении входных данных результат хэш-функции значительно изменяется.

В результате если целью злоумышленника является избежание обнаружения при помощи криптографических хэш-функций, ему достаточно произвести незначительные изменения вредоносного файла. Например в случае фингерпринта изменение версии браузера, когда в результирующей строке меняется 1-2 символа должно приводить к полному изменению значения хэш-функции.

Использование подобных «традиционных» хэш-функций в задачах идентификации пользователей с использованием браузерного фингерпринтинга недопустимо, поскольку они чувствительны к небольшим входным модификациям и могут только определить, являются ли входные данные точно такими же или нет. Нечеткие хэш-функции обладают определенной «терпимостью» к изменениям и могут показать, на сколько различны две последовательности, сравнивая сходство их отпечатков.

Данная задача особенно актуальна в современных условиях, когда злоумышленники активно противостоят эффективному методу обнаружения с использованием статистических сигнатур, используя обфускаторы, позволяющие изменить заранее неизвестную или сложно идентифицируемую аналитиком часть анализируемой последовательности, таким образом, не давая возможности описать эту сигнатуру.

Аналогично традиционным, нечёткие хэш-функции являются инъективным отображением из множества массивов бинарных данных любого размера в строку определенной длины. Однако, если обычные хэш-функции строятся исходя из требований значительно менять своё значение при незначительном изменении, то нечёткая хэш-функция, наоборот незначительно меняет своё значение пропорционально объему изменений в исходных данных. Таким образом, разница между двумя значениями нечётких хэш-функций является метрикой для разницы между соответствующими бинарными данными как это иллюстрируется на рисунке 3.



Рис. 3. Пример использования нечеткой хэш-функции

В зависимости от задач, которые они решают, существуют различные виды нечётких хэш-функций, и различные алгоритмы их реализации. Согласно [6], нечеткое хеширование было разработано в связи с некоторыми ограничениями криптографических хэш-функции и с целью расширения следующих границ:

- **Идентификация встроенных / следовых доказательств.** Учитывая фрагмент данных, такой как JPEG, исследователь должен иметь возможность искать (следы) его существования в другом документе, архиве, образе диска или сетевой трассировке.
- **Идентификация версий кода.** Современное программное обеспечение динамически исправляется и обновляется ежедневно; невозможно вести крипто-хэш-инвентаризацию всех файлов для каждой отдельной версии.
- **Идентификация сопутствующих документов.** Многие документы претерпевают изменения / преобразования по мере их обновления. Часто необходимо иметь возможность идентифицировать и проследить версии по нескольким источникам доказательств.

- **Корреляция источников памяти и дисков.** Исследователь должен уметь соотносить снимки памяти и образы дисков. Макет и содержимое исполняемого файла/документа во время выполнения отличаются от представления на диске, поэтому обычные хэш-функции не работают; однако идентифицируемая общность явно присутствует.

- **Корреляция сетевых и дисковых источников.** Передаваемые файлы фрагментируются и чередуются. В настоящее время корреляция требует трудоемкой реконструкции потока пакетов и анализа протоколов для извлечения передаваемых файлов до применения любой хэш-фильтрации.

Виды и алгоритмы реализации нечётких хэш-функций в задаче фингерпринтинга

Одной из основных классификаций является разделение нечётких хэшей на следующие группы:

- кусочное хэширование (Piecewise hashing);
- контекстно-побуждаемое кусочное хэширование (Context triggered piecewise hashing);
- выделение статистически маловероятных особенностей (Statistically improbable features);
- алгоритмы блочного перестроения (Block-based rebuilding);
- статистические отпечатки.

Скольльзящие Хэши

Скольльзящие хэш-функции генерируют "кусочки" традиционных хэш-строк, "производя псевдослучайное значение, основанное только на контексте входных данных" [2]. Они основаны на алгоритме Рабина-Карпа, который определяется следующим образом: "задается строка Р длины N и строка S длины M, чтобы выяснить все вхождения Р в пределах S." [3]. Они популярны, потому что их легко и быстро вычислить. Они "используются для идентификации похожих строк в блоках данных" [4].

Кусочное Хеширование

Кусочное хеширование генерирует окончательную контрольную сумму для всего документа, как и традиционные хэш-функции. Они преодолевают ограничения и недостатки последних, поскольку кусочные хэш-функции и разделяют весь файл на фиксированные сегменты/части, а затем генерируют хэш-значения для каждого из этих сегментов. Сгенерированные значения сегментов в конце концов формируют окончательную хэш-последовательность. Кроме того, они изначально были созданы для уменьшения потенциальных ошибок при судебно-медицинской визуализации, так что целостность данных будет абсолютной, потому что только один сегмент хэш-значения будет пустым.

Рассмотрим наиболее распространенные алгоритмы нечеткого хеширования.

Ssdeep

Инструмент Context Triggered Piecewise Hash (СТПН) или ssdeep вычисляет сигнатуру (spamsum) для каждого входного файла, которая впоследствии может быть использована для сопоставления этих сигнатур с другими сигнатурами файлов и поиска любых возможных сходств или совпадений. ssdeep – является первым алгоритмом нечеткого хеширования. Реализация алгоритма состоит из трех шагов:

(i) Он использует скольльзящее хеширование для разделения документа "на 6-битные сегменты значений" [5] (блоки переменной длины, которые зависят от алгоритма скольльзящего хеширования);

(ii) Он использует другую хэш-функцию, такую как MD5 или SHA-1, для получения дайджеста (представления) для каждого сегмента;

(iii) Он связывает вместе все сегменты хэш-функции, чтобы сформировать хэш-подпись.

Хотя ssdeep довольно эффективен в поиске сходства между текстовыми файлами, поскольку он изначально был создан для обнаружения спама, его скорость обнаружения изображений и видео невелика.

Sdhash

Основное различие между sdhash (Similarity Digest hash) и ssdeep заключается в том, что sdhash использует фильтры Блума и сравнивает файлы с использованием расстояния Хэмминга. Его результаты основаны на "оценке сходства путем вычисления нормализованной меры эн-

тропии между дайджестами (представлениями), которая колеблется от 0 до 100, где 0-полное несоответствие, а 100 соответствует идеальному совпадению или близком к совпадению” [5]. Согласно [6, 7], преимущество sdhash заключается в том, что вычисление энтропии выполняется для каждой 64-байтовой последовательности (от 0 до 63, затем от 1 до 64 и т. д.). Идентифицированные признаки хэшируются с помощью SHA-1 и вставляются в фильтр Bloom. Это означает, что sdhash может идентифицировать сходство между файлами при условии, что будут идентифицированы общие признаки.

MvHash

Алгоритм mvHash (majority vote hash) – это сохраняющий сходство дайджест (SPD), имеющий *“самое быстрое время вычисления, по сравнению с любым другим алгоритмом SPD, и который почти так же быстр, как SHA-1”* [8]. Алгоритм MvHash использует фильтры Блума, также как sdhash, и *“входные данные подобны, если они имеют сходные базовые последовательности байтов”* [8]. Алгоритм состоит из трех фаз: сначала большинство голосов обрабатывается на битовом уровне, так что любая последовательность будет преобразована в 0 и 1. Вторая фаза – это процедура RLE (Run Length Encoding) которая *применяется для представления этих последовательностей 0 и 1 по их длине (в байтах)”*. Последний этап создание дайджеста подобия.

Mrsh-v2

Алгоритм хеширования сходства с несколькими разрешениями (mrsh) является вариацией ssdeep. Основное различие между ними заключается в том, что ssdeep использует скользящее значение хэш функции, а mrsh – использует полиномиальное представление хэш-djb2. Кроме того, mrsh использует алгоритм MD5 для вычисления хэш-функции.

Структура алгоритма извлечения отпечатков на основе нечеткого хеширования

Рассмотрим вариант алгоритма нечеткого хеширования предназначенный для выбора хэш-значений в качестве функции цифрового отпечатка в текущем окне. Будем считать, что после предварительной обработки входного текста путем устранения шума, такого как вспомогательные слова, знаки препинания и т. д., получена последовательность строк $T[1, \dots, n]$.

Затем сопоставляем длину k из последовательности $T[1, \dots, n]$ с последовательностью хэш-значений с помощью скользящей хэш-функции. Хэш-значения последовательностей (T_1, T_2, \dots, T_k) и $(T_2, \dots, T_k, T_{k+1})$ можно вычислить по формулам:

$$H(T_1, T_2, \dots, T_k) = \text{asc}(T_1)b^{k-1} + \text{asc}(T_2)b^{k-2} + \dots + \text{asc}(T_k) \quad (1)$$

$$H(T_2, \dots, T_k, T_{k+1}) = (H(T_1, T_2, \dots, T_k) - \text{asc}(T_1)b^{k-1})b + \text{asc}(T_{k+1}) \quad (2)$$

где $\text{asc}(c)$ – это ASCII символа c .

Согласно выражениям (1) и (2), скользящая хэш-функция может сопоставить подстроку длины k целому числу $x (0 \leq x \leq b_k)$.

Чтобы выбрать некоторые репрезентативные хэш-значения в качестве цифровых отпечатков пальцев может быть предложена модель принятия решений, включающая для оценки хэш-значений окна три этапа: выбор - валидация - решение.

Функция цифрового отпечатка определяется во время принятия решения.

С этой целью определяется размер окна w и последовательность хэш-значений $H_y = \{H_1, H_2, \dots, H_w\}$.

Каждое полученное значение H_y нужно разделить на несколько частей. Предположим, что значение H_y разбито на n частей которые можно представить в виде $H_{y1}, H_{y2}, \dots, H_{yn}$.

Тогда модель решения может быть описана следующим образом:

а) На этапе принятия решения, среди $H_{y1}, H_{y2}, \dots, H_{yi}$ в качестве опорного значения требуется выбрать минимальное хэш-значение для выбора функции цифрового отпечатка. Эту процедуру можно описать следующим образом:

$$p = \min(H_{y1}, H_{y2}, \dots, H_{yi}) \quad (3)$$

б) На этапе валидации модели принятия решения необходимо проверить эталонное значение v . Минимум последовательности $H_{y(i+1)}, H_{y(i+2)}, \dots, H_{y(k)}$ выражается формулой (4).

$$q = \min(H_{y(i+1)}, H_{y(i+2)}, \dots, H_{y(k)}) \quad (4)$$

Если $p \leq q$ эталонное значение принимается равным $v = p$, в противном случае $v = q$.

с) На этапе принятия решения определяется значение признака цифрового отпечатка p в соответствии с остальными хэш-значениями окна

$$H_{y(k+1)}, H_{y(k+2)}, \dots, H_{y(n)}$$

Для снижения затрат на поиск определяется порог,

$$|H_{y(k+j)} - v| \leq t \quad (1 \leq j \leq w) \quad (5)$$

Если $H_{y(k+j)}$ удовлетворяет уравнению (5) то полученное значение выбирается в качестве значения функции отпечатка и берется в качестве левой границы следующего окна. Таким образом, каждая левая граница следующего окна вычисляется последовательно. Структура алгоритма представлена на рисунке 4.

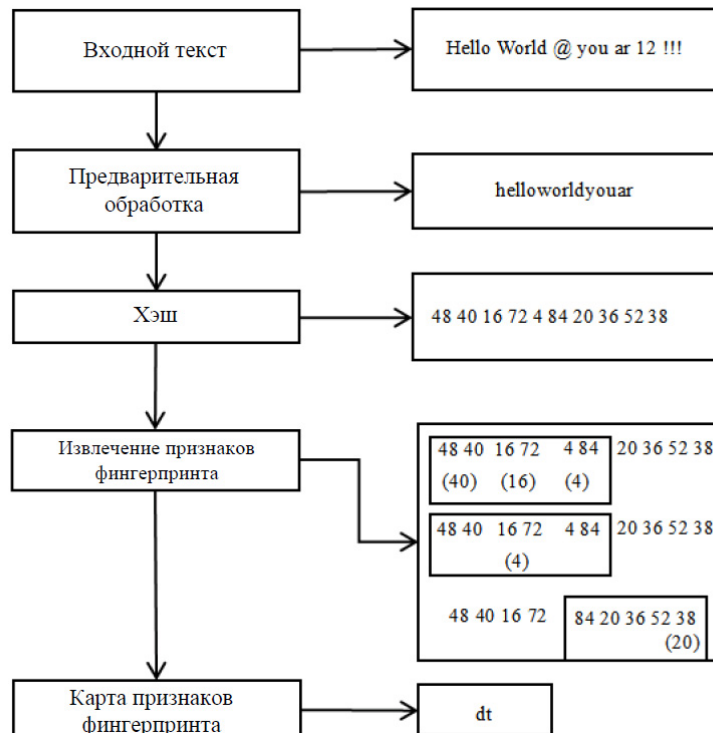


Рис. 4. Выбор цифрового отпечатка

Модель подобного принятия решения ограничивает область выбора объектов цифровых отпечатков в пределах заданного интервала окна. В результате скользящее окно принимает те-

кущий выбранный цифровой отпечаток в качестве отправной точки для следующего положения окна.

Исследования показывают [8,9,10], что алгоритмы нечеткого хеширования *sdhash* и *mvHash* имеют самую высокую скорость идентификации на основе сходства, за ними следуют *mrshv2* и, наконец, *ssdeep*.

Единственным недостатком *sdhash* является его время работы, который однако компенсируется простотой реализации алгоритма и способом представления результатов на основе оценки сходства.

Заключение

Проведенные исследования показали, что задачу анализа отпечатка устройства и последующую идентификацию (деанонимизацию) анонимных пользователей можно свести к задаче извлечения отпечатков на основе нечеткого хеширования и последующего их сравнения с исходной базой данных.

Показана нецелесообразность использования традиционных криптографических хэш-функций в задаче фингепринтинга ввиду их «лавинного эффекта» к незначительным изменениям входных данных.

Рассмотрены основные виды и алгоритмы нечетких хэш-функций. Выявлено, что алгоритмы нечеткого хеширования *sdhash* и *mvHash* имеют самую высокую скорость идентификации на основе сходства.

Недостатком *sdhash* является длительность выполнения вычислений, которая однако компенсируется простотой реализации алгоритма.

Литература

1. Alfred J. Menezes Paul C. van Oorschot and Scott A. Vanstone Handbook of Applied Cryptography. Boca Raton, Florida, CIIA: CRC Press, 2001, 810 стр
2. J. Kornblum, "Identifying almost identical files using context triggered piecewise hashing," Digital investigation, 2006, vol. 3, pp. 91-97.
3. C. Negruseri, "Rolling hash, rabin karp, palindromes, rsync and others," [Online] infoarena.ro. Available at: <http://www.infoarena.ro/blog/rolling-hash> [Accessed: 9 August 2014].
4. K. Candan and M. Sapino, "Data management for multimedia retrieval," 1st ed. Cambridge University Press, 2010.
5. J. Oliver, C. Cheng, and Y. Chen, "Tlsh – a locality sensitive hash," 2013, pp. 7-13.
6. V. Roussev, "An evaluation of forensic similarity hashes," digital investigation, 2011, vol. 8, pp. 34-41.
7. F. Breiting and H. Baier, "Properties of a similarity preserving hash function and their realization in *sdhash*," 2012, pp. 1-8.
8. F. Breiting, K. Astebol, H. Baier, and C. Busch, "mvhash-b - a new approach for similarity preserving hashing," In Proc. of The Seventh International Conference on IT Security Incident Management and IT Forensics, 2013.
9. Liao Mo, Chen Zongji, "Coordinated Target Assignment in Mult-UAV based on Satisfying Decision Theory", Journal of Beijing University of Aeronautics and Astronautics, vol. 33, no. 1, (2007), pp. 81-85.
10. D. L. Lewis, "The hash algorithm dilemma-hash value collisions," [On-line] Available from: <http://www.forensicmag.com/print/235>. [Accessed: 02 August 2014].

РЕАЛИЗАЦИЯ ПЛАТФОРМЫ ТУМАННЫХ ВЫЧИСЛЕНИЙ ДЛЯ ПРЕДОСТАВЛЕНИЯ СЕРВИСОВ IoT

Гадасин Денис Вадимович,

МТУСИ, доцент кафедры СИТус, к.т.н., Москва, Россия
dengadiplom@mail.ru

Шведов Андрей Вячеславович,

МТУСИ, старший преподаватель каф. СИТус, Москва, Россия
a.v.shvedov@mtuci.ru

Клыгина Олеся Григорьевна,

МТУСИ, студентка группы БСТ1702, Москва, Россия
koreeramahan@yandex.ru

Гадасин Даниил Денисович,

ООО Фирма «Телесофт», стажер, Москва, Россия
gadasin115@gmail.com

Аннотация

С продолжающимся интенсивным развитием приложений и сервисов в рамках концепции Интернета вещей (Internet of Things, IoT), а также ожидающимся скором повсеместном распространении устройств, поддерживающих стандарт 5G, классическая парадигма централизованных облачных вычислений сталкивается с рядом проблем, в числе которых можно выделить высокие задержки, низкую емкость и сбои при передаче данных сети. Для решения этих проблем целесообразно применять парадигму туманных вычислений (Fog Computing), в рамках которой возможно обеспечить первоначальную обработку и хранение данных устройств Интернета вещей локально на самих устройствах, без необходимости их обязательной отправки в облачную инфраструктуру. При этом туманные вычисления позволяют предоставлять сервисы с более быстрой реакцией и более высоким качеством. В данной статье представлено современное состояние парадигмы туманных вычислений и способы ее интеграции с IoT, приведена архитектура платформы туманных вычислений и описание ее компонентов, а также рассмотрены вопросы обеспечения корректной маршрутизации и формирования системы управления ею.

Ключевые слова

Туманные вычисления, Интернет Вещей, Облачные вычисления, Облако вещей, маршрутизация, методы маршрутизации, метрика, Fog, Fog Computing, Internet of Things, Cloud Computing, Cloud of Things, routing, IoT, Co, metric.

Введение

Формирование новых технологических концепций информационно-коммуникационных технологий приводит к постоянному возрастанию количества подключаемых устройств и, как следствие, к постоянному возрастанию объемов передаваемой информации по всем типам сетей связи. К числу подобных концепций относится Интернет Вещей (IoT) [1].

Интернет вещей – это концепция информационной вычислительной сети, объекты («вещи») в которой имеют возможность взаимодействовать друг с другом или с внешней средой посредством ИКТ, исключая при этом, по возможности, необходимость участия человека в информационном обмене [2]. Таким образом, происходит синтез физического и цифрового компонентов (материальной и виртуальной реальностей), где для определенной вещи реального физического мира существует виртуальный дублер (цифровой двойник), который будет вступать во взаимодействие с подобными себе устройствами [3,4].

Можно констатировать, что IoT – это одна из ключевых инноваций последних нескольких десятилетий, которая потенциально может принести неограниченную выгоду человеческому обществу. Однако, до сих пор в рамках технологической реализации данной концепции специалисты сталкиваются с рядом проблем, которые не позволяют в полной мере задействовать ее потенциал. К этим проблемам относится ограниченная производительность, выражающаяся в недостаточной вычислительной мощности устройств и ресурсах хранения данных, обеспечение информационной безопасности, конфиденциальности и надежности.

Преодоление большинства из этих проблем возможно путем интеграции концепции Интернета вещей с платформой облачных вычислений и образования таким образом облака вещей (Cloud of Things, CoT). CoT должно упростить процесс сбора и обработки данных на устройствах IoT и обеспечить быструю и недорогую установку, развертывание и интеграцию системы для комплексной обработки, хранения и использования данных.

Однако, устройства и приложения, функционирующие в рамках IoT, генерируют огромные объемы данных [3]. Передача подобных больших данных в облачную инфраструктуру требует чрезмерно высокой пропускной способности каналов передачи данных транспортной сети, а также корректной маршрутизации. Решение такой задачи видится в переходе на технологию туманных вычислений, которая способна обеспечить приемлемое решение для приложений IoT, чувствительных к задержке.

Характеристика туманных вычислений

Понятием туманные вычисления обозначают связанные между собой распределенные вычисления, частично выполняемые на оконечных устройствах, имеющих ограниченные ресурсы и непосредственную связь, как с физическим миром («землей»), так и с облаком. Появление туманных вычислений стало возможным благодаря современной тенденции интеграции сетевых технологий во все большее число бытовых и промышленных устройств, которые обладают, хотя и скромными, но собственными вычислительными ресурсами и системами хранения данных [5]. По сути, туманные вычисления представляют собой расширение облачных вычислений, ресурсы которых расположены ближе к устройствам, которые работают с данными Интернета вещей. Как показано на рисунке 1, туманные вычисления выступают в качестве посредника между облаком и оконечными устройствами, что приближает службы обработки и хранения данных, а также сетевые службы к самим оконечным устройствам. Эти устройства называются узлами туманных вычислений (fog-узлами). Они могут быть развернуты в любом месте, где имеется возможность их сетевого подключения. Узлом туманных вычислений может выступать любое бытовое или промышленное устройство, которое обладает, хотя бы скромными, но собственными вычислительными ресурсами и системами хранения данных [5].

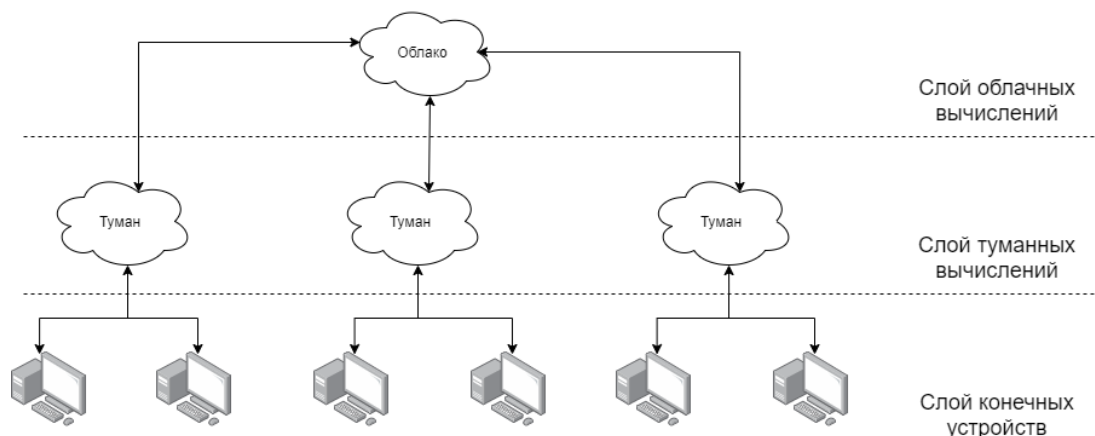


Рис. 1. Схема организации туманных вычислений

Отличительными характеристиками парадигмы туманных вычислений являются:

- Осведомленность о местоположении: туманные вычисления способны обеспечивать осведомленность о местоположении, благодаря чему узлы могут быть развернуты в различных местах;
- Низкая задержка при обработке данных: поскольку инфраструктура туманных вычислений находится ближе к оконечным устройствам, это обеспечивает меньшую задержку при обработке данных на оконечных устройствах;
- Распределенная архитектура вычислений: в отличие от централизованных облачных вычислений, устройства, сервисы и приложения, реализованные и функционирующие в рамках парадигмы туманных вычислений, распределены и могут быть развернуты в любом месте;
- Масштабируемость: для существующих и проектируемых крупномасштабных сенсорных сетей, например, контролирующих состояние окружающей среды, туманные вычисления могут обеспечивать распределенные вычислительные мощности и ресурсы хранения;
- Поддержка мобильности: одним из важных аспектов сервисов и приложений, функционирующих в рамках туманных вычислений, является возможность прямого подключения к мобильным устройствам, что дает возможность использования методов мобильности, например, протокола Locator/ID Separation Protocol (LISP), который обеспечивает новую архитектуру маршрутизации, привносящую новую семантику для IP-адресации. Это также предоставляет возможность доступа мобильным пользователям ко всей информации и приложениям, которые необходимы для подключения к IoT [6];
- Взаимодействие в режиме реального времени: архитектура туманных вычислений обеспечивает взаимодействие между узлами в режиме реального времени, а не в режиме пакетной обработки, используемого в рамках централизованных облачных вычислений;
- Гетерогенность: узлы туманных вычислений могут функционировать в рамках единой вычислительной архитектуры даже если они произведены различными производителями;
- Интероперабельность: узлы туманных вычислений могут взаимодействовать и работать в рамках различных доменов и поставщиками услуг;
- Поддержка онлайн-аналитики и взаимодействие с облаком: платформа туманных вычислений располагается между оконечными устройствами и центрами облачных вычислений, что позволяет играть важную роль в накоплении и обработке данных вблизи самих оконечных устройств.

Концептуальная модель туманных вычислений

Концептуальная модель туманных вычислений в общем случае включает в себя ряд взаимодействующих компонентов – слоев (рис. 2).

Интеграция концепции IoT с платформой облачных вычислений и образование таким образом облака вещей (CoT) может способствовать управлению IoT-ресурсами и обеспечить предоставление более широкого спектра сервисов Интернета вещей.

Стоит отметить, что парадигма CoT вносит новые проблемы в систему IoT, такие как задержка, ограничения пропускной способности, ограниченный ресурс устройств, нестабильность сетевого подключения, обеспечение безопасности, которые не могут быть решены на базе традиционной централизованной архитектуры облачных вычислений.

Кроме того, традиционная архитектура облачных вычислений не удовлетворяет требованиям, предъявляемым к сервисам IoT, например, в части задержки при передаче данных и устойчивости сетевого подключения. В определенных предметных областях, например, в телемедицине или охранной деятельности, даже минимальная задержка может повлечь серьезные последствия. Поэтому для решения задач подобного рода требуется применение новой парадигмы вычислений, которая способна минимизировать влияние ограничений, связанных с пропускной способностью и задержками, путем организации корректной маршрутизации трафика данных, для осуществления которой необходимо произвести корректное проектирование узлов туман-

ных вычислений. В качестве примеров можно указать архитектурные решения Cloudlet, IOx и ParaDrop.

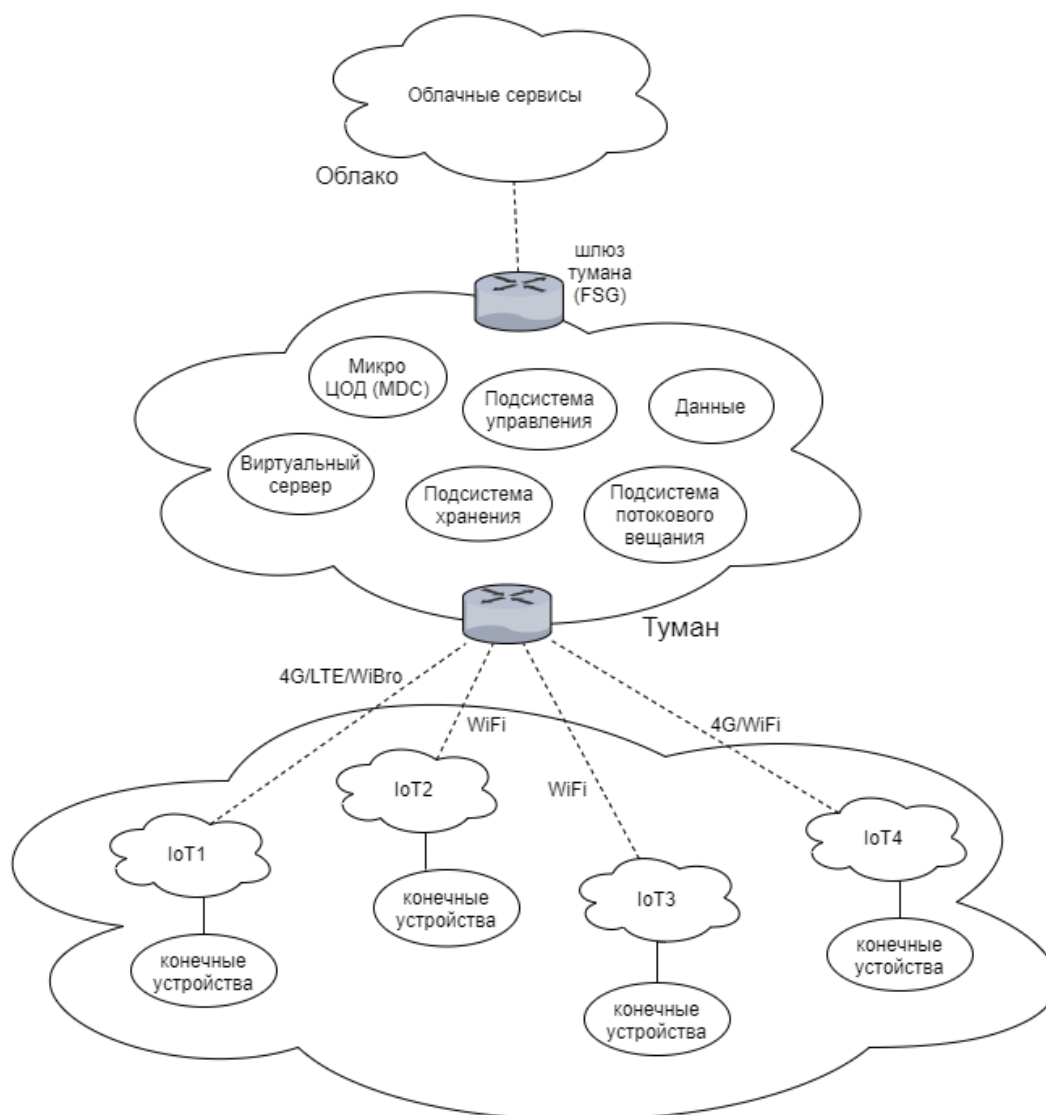


Рис. 2. Архитектурная взаимосвязь компонентов платформы туманных вычислений

На рисунке 3(а) представлена архитектура Cloudlet, которая содержит избыточное количество ресурсов. Она имеет трехслойную конструкцию.

На рисунке 3(б) представлена архитектура Cisco IOx, а именно ее реализация в аппаратно-программном комплексе. Эта платформа не является публичной и в ее основе лежит высокопроизводительное и высоконадежное, а следовательно, и дорогостоящее оборудование.

Решение на базе ParaDrop представляет собой вычислительную платформу с открытым исходным кодом, которая реализуется на базе аппаратного шлюза (Например, точка доступа Wi-Fi или домашняя телеприставка), который является подходящим узлом для туманных вычислений в силу его близости к конечному пользователю. Таким образом, ParaDrop подходит в качестве вспомогательной реализации туманной вычислительной платформы для легких задач.

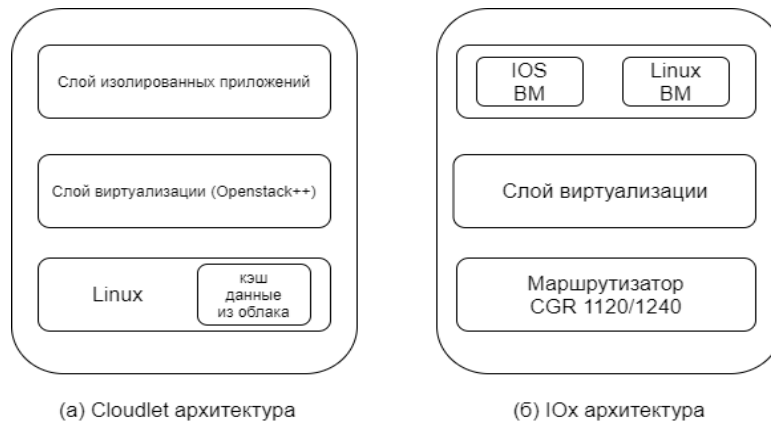


Рис. 3. Архитектура решений Cloudlet (a) и IOx (б)

Первым шагом реализации системы, базирующийся на парадигме туманных вычислений является разработка единой платформы, которая может служить в качестве прототипа. Данная разработка должна помочь в достижении следующих целей:

- Снижение задержек. Для платформы туманных вычислений принципиально важно предлагать конечному пользователю сервисы с гарантированной низкой задержкой.
- Повышение эффективности использования ресурсов и энергии:
 - далеко не все узлы туманных вычислений являются ресурсоемкими. Некоторые из них имеют ограниченную вычислительную мощность и ресурсы хранения данных.
 - большинство узлов туманных вычислений и клиентских устройств имеют автономный источник питания.
- Создание единого интерфейса. Из-за возможной гетерогенности узлов туманных вычислений и клиентских устройств необходимо предоставить одинаковую абстракцию для приложений и сервисов. Должны быть предусмотрены общие интерфейсы прикладного программирования (API) для взаимодействия с существующими протоколами, например, Machine-2-machine, smart vehicle/smart appliance и т.д.

После достижения поставленных целей, необходимо будет решить следующие задачи:

1. Выбор технологии виртуализации. Виртуализация является основным методом обеспечения изолированных сред в туманных вычислениях, а также основным элементом обеспечения приемлемой производительности узла, поэтому необходимо определить тип виртуализации – на основе гипервизора или контейнеров. Например, Cloudlet использует технику виртуализации на основе гипервизора в то время, как ParaDrop использует технологию контейнеров, т.е. виртуализацию на уровне ОС. Одним из недостатков виртуализации на основе контейнеров является потеря гибкости. Например, данный тип не позволяет размещать различные типы гостевых операционных систем на одном узле инфраструктуры. Поэтому более предпочтительным вариантом видится виртуализация на основе гипервизора, а не виртуализация на основе контейнеров.

2. Минимизация задержек. Существует множество факторов, приводящих к возникновению высокой задержки в производительности приложений, сервисов и служб на платформах туманных вычислений. При этом высокая задержка не приемлема, поскольку туманные вычисления нацелены на чувствительные к задержкам приложения, сервисы и службы. Существует несколько возможностей уменьшить задержки:

— Агрегирование данных. Распределенная природа парадигмы туманных вычислений может приводить к возникновению задержек, если процесс агрегирования данных не будет завершено до начала их обработки. Применение методов секционирования и фильтрации данных, а также использование локальности в иерархии для уменьшения объема вычислений позволяет смягчить данную проблему.

— Планирование предоставления ресурсов. При предоставлении ресурсов для решения определенных задач, особенно для узлов туманных вычислений, обладающих ограниченными ресурсами, возникают задержки, которые могут быть уменьшены при более тщательном планировании механизма предоставления ресурсов с использованием модели приоритета и мобильности.

3. Управление сетью. Должно осуществляться с применением технологических концепций SDN и NFV. SDN – это метод администрирования инфокоммуникационных сетей, позволяющий управлять услугами сети, когда функционал управления (control plane) отделен от нижележащего уровня пересылки пакетов (data plane) за счет переноса функций контроля и управления сетевым оборудованием (маршрутизаторами, коммутаторами и т.д.) в приложения, работающие на отдельном сервере (контроллере) [7]. Таким образом, введение новых услуг на сети упрощается и ускоряется. NFV – технология, позволяющая визуализировать физические сетевые элементы телекоммуникационной сети с исполнением сетевых функций программными модулями, работающими на стандартных серверах (чаще всего x86) и виртуальных машинах в них [7]. Однако полноценная интеграция концепций SDN и NFV с платформами туманных вычислений является довольно сложной задачей из-за необходимости редизайна southbound, northbound, eastbound и westbound API, применяемых при включении необходимых примитивов туманных вычислений. Простая интеграция при этом не обеспечивает достижения проектных целей в части снижения задержек и повышения эффективности.

4. Обеспечение безопасности и конфиденциальности. Должно учитываться на каждом этапе проектирования платформы туманных вычислений и является одной из важных проблем, которая должна быть решена в процессе реализации системы, базирующийся на парадигме туманных вычислений. Подходящим решением будет являться применение системы контроля доступа, а также систем обнаружения (IDS) или предотвращения (IPS) вторжений, которые должны использоваться на каждом уровне платформы и, в том числе обеспечивать возможности визуализации обнаружения компьютерных атак [8].

Архитектура платформы туманных вычислений и ее компоненты

На рисунке 4 представлена предлагаемая архитектура платформы туманных вычислений.

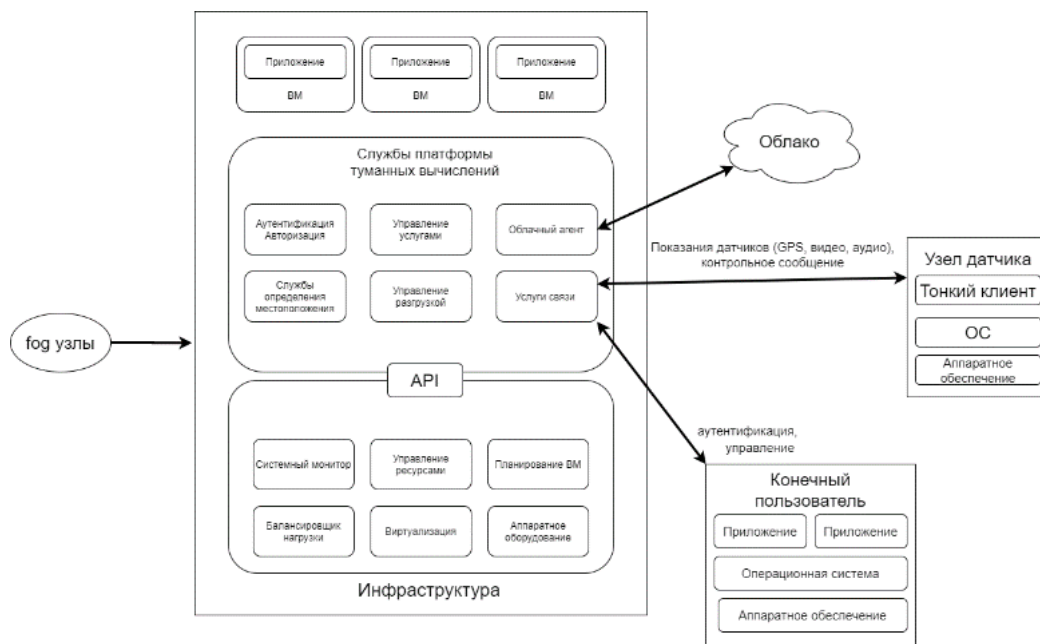


Рис. 4. Компоненты архитектуры платформы туманных вычислений

Она состоит из следующих основных инфраструктурных компонентов:

- службы туманных вычислений;
- платформу виртуализации;
- средства управления сетью;
- приложения.

Инфраструктурные компоненты взаимодействуют с узлами туманных вычислений (fog-узлами), центрами облачных вычислений, пользовательскими устройствами, а также наборами различных датчиков IoT.

К числу наиболее значимых инфраструктурных компонентов относятся следующие:

- Службы аутентификации и авторизации: обеспечивают доступ к ресурсам, услугам и сервисам туманных вычислений. Поскольку они располагаются близко к конечным пользователям, для их идентификации применяются новые схемы аутентификации и авторизации, основанные на шаблонах доступа, шаблонах мобильности и доверенных защищенных устройствах.
- Службы управления разгрузкой: являются важным компонентом, который должен решать следующие задачи:
 - 1) определение видов информации, необходимых для принятия решений о разгрузке;
 - 2) разбиение приложений на разделы для разгрузки;
 - 3) проектирование оптимальной схемы разгрузки.
- Службы определения местоположения: должны поддерживать список местоположений соседних узлов (мобильных и стационарных), отслеживать мобильных пользователей и обеспечивать обмен информацией о местоположении между узлами туманных вычислений.
- Системный монитор: является стандартным компонентом в инфраструктуре центров облачных вычислений, который обеспечить сбор, накопление и анализ данных об основных параметрах и характеристиках узлов, а также осуществлять контроль над производительностью приложений и оборудования, что помогает обеспечивать своевременное принятие необходимых решений и бесперебойное функционирование компонентов инфраструктуры.
- Управление ресурсами: отвечают за большинство задач, связанных с управлением ресурсами и их распределением, а также процессами присоединения и отключения узлов туманных вычислений.

Система туманных вычислений в общем виде реализуется в соответствии с вышеописанной архитектурой и, как правило, состоит как минимум из двух платформ (подсистем). Основой каждой из них является OpenStack в составе четырех основных модулей: Keystone, Glance, Nova и Cinder. Модуль Keystone предназначен для аутентификации и авторизации, модуль Glance – для управления образами виртуальных машин, модуль Nova является вычислительным модулем с простой сетевой функциональностью, а Cinder – это модуль блочного хранилища.

Две платформы туманных вычислений представляют из себя две отдельные подсистемы на базе OpenStack с сетевым соединением между ними. Для обеспечения непрерывности обслуживания необходимо реализовать схему разгрузки виртуальной машины, которая может обеспечивать перенос виртуальной машины из одного кластера платформы в другой.

На рисунке 5 представлен пример системы туманных вычислений, состоящей из двух подсистем, каждая из которых содержит в своем составе граничный маршрутизатор и три сервера.

В данном примере граничные маршрутизаторы подключаются к облаку Amazon EC2 с помощью защищенных каналов передачи данных сети Интернет, а также соединяются друг с другом посредством локальной сети. Для обеспечения подключения мобильных пользователей к системе и облачной инфраструктуре возможно использование маршрутизаторов с функцией беспроводной точки доступа (Wireless AP).

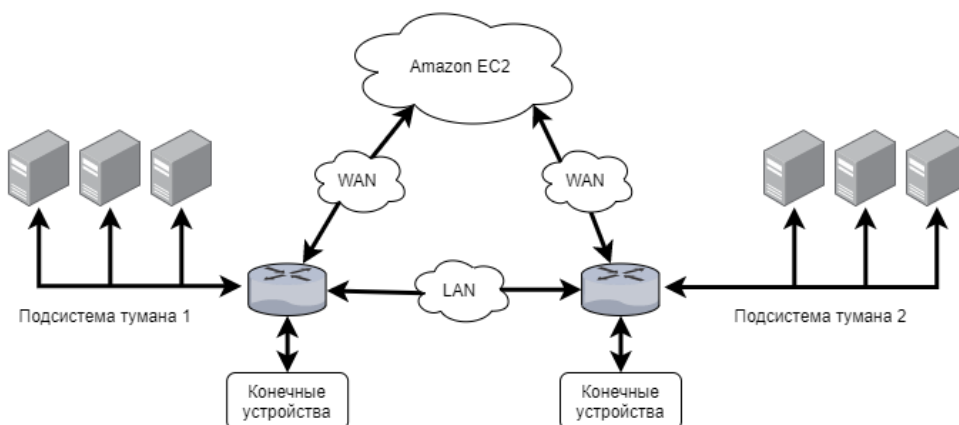


Рис. 5. Подсистемы туманных вычислений

Формирование системы управления маршрутизацией

Обеспечение выбора оптимального и эффективного маршрута доставки сообщений от отправителя к получателю в рамках глобальной сети Интернет называется маршрутизацией и является одной из фундаментальных систем любой сети, обеспечивающей её корректное, бесперебойное, надежное и безопасное функционирование [9-16]. Для правильной маршрутизации, которая способствовала бы достижению целей необходимо выбрать соответствующий метод маршрутизации. В зависимости от технологической платформы построения сети и определенной ситуации в ней может быть эффективен тот или иной метод маршрутизации, за счет применения которого возможно достижение оптимальных значений одного или нескольких показателей эффективности функционирования сети. Предлагается выделить в системе управления сетью подсистему управления маршрутизацией, реализованную в каждом узле туманных вычислений (рис. 6).

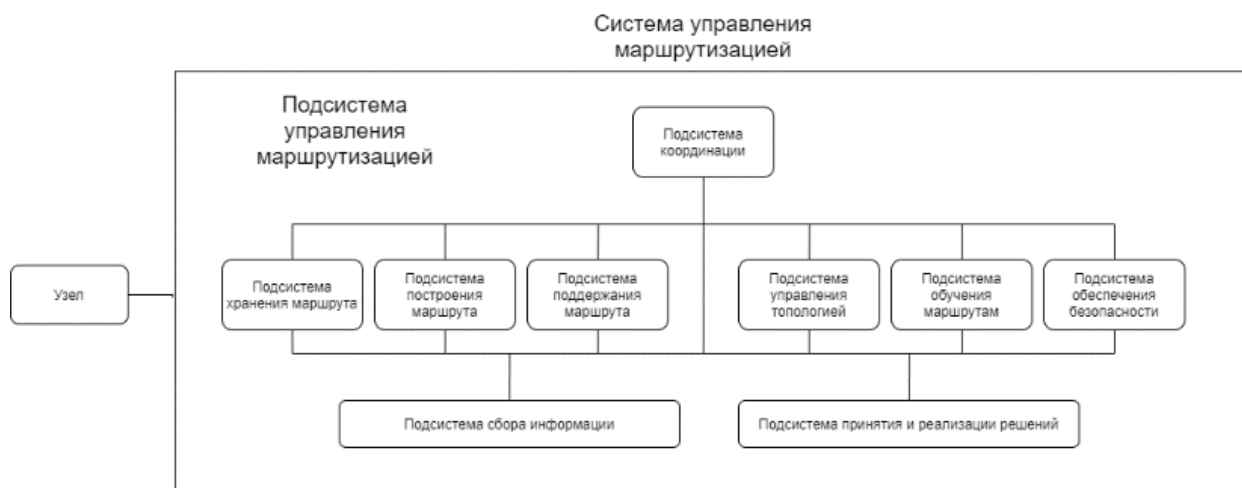


Рис. 6. Функциональная модель системы управления маршрутизацией

Подсистемы сбора информации, построения и хранения маршрутов узла осуществляют рассылку, сбор и хранение информации о сети и ее зонах в соответствии с правилами функционирования соответствующего метода маршрутизации.

Подсистема принятия и реализации решений функционирует на основе анализа собственного состояния, параметров функционирования сети или ее зон (параметры мобильности, нагрузки и другие, которые задаются в виде нечетких переменных) и типа трафика определяет:

- целевую функцию управления,
- метод маршрутизации, при этом количество адресатов определяет выбор однопользовательской, групповой или волновой маршрутизации, а требования к обеспечению надежности и безопасности определяет количество возможных маршрутов (однопутевая или многопутевую);
- функцию маршрутизации;
- формат маршрутной информации.

Подсистема управления топологией перераспределяет мощности передач соседних узлов и/или направленности их антенн исходя из целевой функции управления. Задача управления топологией сведена к задаче ситуационного управления.

Подсистема поддержания маршрута функционирует в пассивном (отправителю посылается сообщение об отказе маршрута) или активном (прогноз состояния маршрутов и, при необходимости, упреждающее перестроение маршрута) режимах.

Подсистема обучения маршрутам использует информацию из проходящих через узел пакетов (служебных и информационных) для пополнения или обновления таблицы маршрутизации.

Подсистема обеспечения безопасности отвечает за идентификацию атак противника на методы маршрутизации, оценку их угроз и обеспечивает меры по их минимизации. При этом стоит помнить, что главная проблема при решении задачи безопасной маршрутизации лежит в распределенном характере сети, при этом зачастую решение проблем, связанных с некорректной маршрутизацией, носит локальный характер в пределах автономных систем или сетей операторов и не является отраслевым стандартом [10].

Подсистема координации осуществляет координацию действий всех подсистем и прогнозирование поведения маршрутов.

Таким образом, получение многопараметрического маршрута сведено к задаче нечеткой многокритериальной оптимизации. Иерархия процесса принятия решения в рамках системы управления маршрутизацией представлена на рисунке 7.

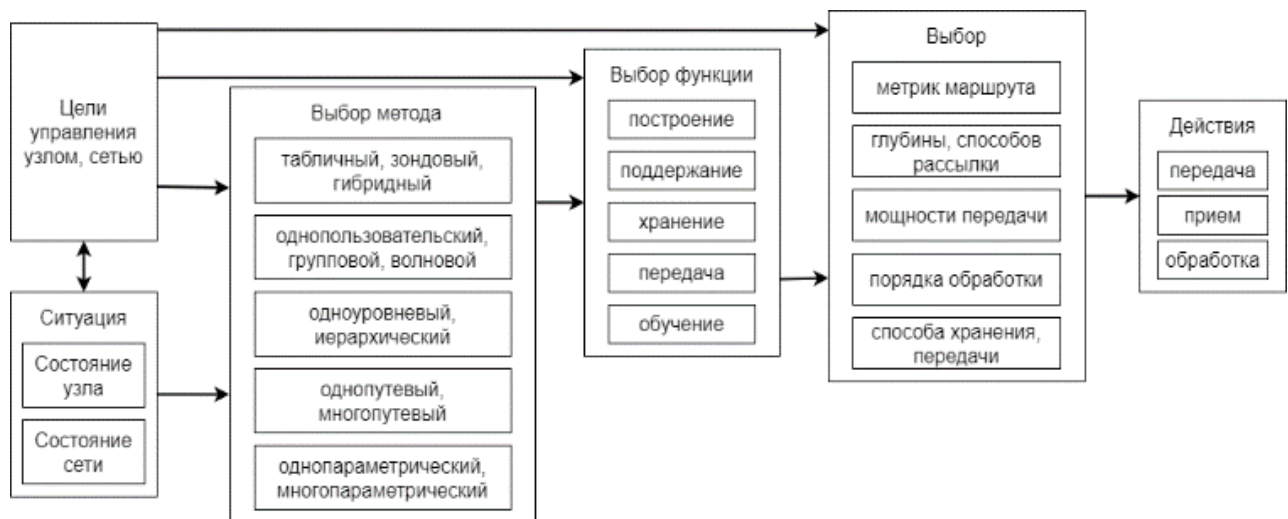


Рис. 7. Иерархия принятия решений по маршрутизации

Заключение

Отправка данных, генерируемых устройствами IoT в инфраструктуру облачных вычислений, требует чрезмерно высокой пропускной способности сети и правильной маршрутизации, что затрудняет и замедляет внедрение инфраструктуры для функционирования сервисов и приложений на базе концепции Интернета Вещей (IoT).

Решением этой проблемы может являться парадигма туманных вычислений. Одной из отличительных особенностей системы туманных вычислений является ее распределенный характер, позволяющий обеспечить обработку, анализ и хранение данных во многих местах системы. Это позволяет считать туманные вычисления одним из оптимальных способов организации предоставления сервисов в рамках концепции IoT,

Литература

1. Докучаев В.А., Ермалович А.В., Шведов А.В. Концепция «Интернет Вещей» как основа развития информационно-коммуникационных технологий (ИКТ) // Актуальные проблемы и перспективы развития экономики. Труды Юбилейной XV международная научно-практической конференции. Симферополь-Гурзуф, 17-19 ноября 2016 год. Саки: ИП Бровко А.А., 2016. С. 298.
2. ITU-T Recommendation Y.2060
3. Гадасин Д.В., Шведов А.В., Ермалович А.В. Концепция "туманные вычисления" – эволюционный этап развития инфокоммуникационных технологий // Технологии информационного общества. Сборник трудов XII Международной отраслевой научно-технической конференции «Технологии информационного общества». (14-15 марта 2018 г. Москва, МТУСИ). М.: ИД Медиа Паблишер, 2018. С. 96-99.
4. Gadasin D.V., Shvedov A.V. and Ermolovich A.V., "The concept "fog computing" – The evolutionary stage of development of infocommunication technologies," 2018 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, 2018, pp. 1-3, doi: 10.1109/SOSG.2018.8350582.
5. Докучаев В.А., Кальфа А.А., Мытенков С.С., Шведов А.В. Анализ технических решений по организации современных центров обработки данных // Т-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 6. С. 16-24.
6. Гадасин Д.В., Шведов А.В. Проблемы интеграции концепции "Интернет вещей" и облачных вычислений // Технологии информационного общества. Сборник трудов XIII Международной отраслевой научно-технической конференции «Технологии информационного общества». (20-21 марта 2019 г. Москва, МТУСИ). М.: ИД Медиа Паблишер, 2019. С. 22-23.
7. Шведов А.В., Назаров М.Д. Зависимость показателей эффективности функционирования корпоративных сетей связи от показателей качества обслуживания (Qos) // Технологии информационного общества. Сборник трудов XIV Международной отраслевой научно-технической конференции «Технологии информационного общества». (18-19 марта 2020 г. Москва, МТУСИ). М.: ИД Медиа Паблишер, 2020. С. 302-304.
8. Свидетельство о государственной регистрации программы для ЭВМ 2018660142 Российская Федерация. Программное приложение "Сигнал-Ф1" для визуализации обнаружения компьютерных атак в СОА «Форпост» / В. А. Докучаев, В. В. Маклачкова, Д. В. Гадасин, А. В. Шведов ; заявитель и правообладатель Общество с ограниченной ответственностью Фирма «ТЕЛЕСОФТ» (ООО Фирма «ТЕЛЕСОФТ») – № 2018617954 ; заявл. 26.07.2018 ; опубл 16.08.2018. – 1 с.
9. Гадасин Д.В., Веденев П.С., Шведов А.В. Уязвимости системы маршрутизации глобальной сети Интернет и возможные пути их преодоления // Перспективные технологии в средствах передачи информации: Материалы 13-ой международной научно-технической конференции / Владим. гос. университет, в 2-х томах; редкол.: А.Г. Самойлов (и др). Владимир: ВлГУ. 2019, том I. С. 94-96.
10. Гадасин Д.В., Шведов А.В., Усачева Д.И. Механизмы обеспечения безопасности маршрутизации в сети Интернет // III научный форум телекоммуникации: теория и технологии ТТТ-2019. Проблемы техники и технологий телекоммуникаций ПТиТТ-2019: материалы XXI Международной научно-технической конференции. Казань, 18-22 ноября 2019 года. Казань: КНИТУ-КАИ, 2019. Т. 1. С. 292-293.
11. Гадасин Д.В., Пак Е.В. Применение модели Бэкмена для распределения потоков в сетях с сегментной маршрутизацией // REDS: Телекоммуникационные устройства и системы. 2020. Т. 10. № 4. С. 18-23.
12. Литвин Я.С., Гадасин Д.В. Семантическая сеть как инструмент обработки визуальной информации // Телекоммуникации и информационные технологии. 2018. Т. 5. № 2. С. 111-118.

13. Докучаев В.А., Ерёменко В.А., Маклачкова В.В., Мытенков С.С., Шевелёв С.В. Профессиональные квалификации специалистов по контролю качества информационно-коммуникационных систем // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 11. С. 62-67.
14. Pavlov S.V., Dokuchaev V.A., Maklachkova V.V., Mytenkov S.S. Features of supporting decision making in modern enterprise infocommunication systems // T-Comm. 2019. Т. 13. № 3. С. 71-74.
15. Dokuchaev V.A., Maklachkova V.V., Statev V.Yu. Classification of personal data security threats in information systems // T-Comm. 2020. Т. 14. № 1. С. 56-60.
16. Pavlov S.V., Dokuchaev V.A., Mytenkov S.S. Model of a fuzzy dynamic decision support system // T-Comm. 2020. Т. 14. № 9. С. 43-47.

АНАЛИЗ РАДИОТЕХНОЛОГИЙ ПРИ РЕАЛИЗАЦИИ ИНТЕЛЛЕКТУАЛЬНЫХ АВТОТРАНСПОРТНЫХ СИСТЕМ

Дрюпина Наталья Сергеевна,
МТУСИ, студент магистратуры, Москва, Россия

Кузьмин Михаил Сергеевич,
МТУСИ, студент бакалавриата, Москва, Россия

Манохина Виктория Игоревна,
МТУСИ, аспирант, Москва, Россия

Нелюбина Александра Евгеньевна,
МТУСИ, студент магистратуры, Москва, Россия

Пшеничников Анатолий Павлович,
МТУСИ, профессор, к.т.н., Москва, Россия
pshenichnikov@mtuci.ru

Аннотация

Рассмотрены определения, архитектура и требования к физической архитектуре интеллектуальных транспортных систем (ИТС) в области автомобильного транспорта крупных городских агломераций. Проведен анализ абонентских терминалов транспортных средств и параметров узкополосных радиотехнологий EC-GSM, NB-IoT, LTE-eMTC для их взаимодействия. Приведены основные параметры радиоканалов стандартов IEEE 802.11p, IEEE 802.11bd и 5G NR. Рассмотрено взаимодействие абонентских терминалов с основными элементами дорожной инфраструктуры ИТС.

Ключевые слова

Скорость передачи данных, интеллектуальная транспортная система, бортовой телематический комплекс, абонентские терминалы, дорожная инфраструктура, диапазон частот.

Введение

Существует множество определений Интеллектуальной транспортной системы – ИТС. Наиболее общее определение дано в Концепции Федерального закона РФ [1]. Более детальное определение ИТС приведено в ГОСТ Р 56829-2015 [2] и в Концепции, утверждённой распоряжением Правительства РФ от 25 марта 2020 года №724-р [3]. Интеллектуальная транспортная система создаётся для автоматизированного управления транспортно-дорожным комплексом региона, конкретным транспортным средством или группой транспортных средств.

Согласно европейской директиве [4], ИТС можно трактовать как систему, которая применяется в сфере автотранспорта с использованием информационных и коммуникационных технологий. ИТС включает инфраструктуру, транспортные средства, участников системы, а также дорожно-транспортное регулирование.

В Решении № 19 Высшего Евразийского экономического совета ИТС определяется как интеграция информационных и коммуникационных технологий с транспортной инфраструктурой, направленная на обеспечение безопасности и эффективности транспортного процесса [5].

Целями создания ИТС являются: достижение максимальных показателей использования дорожной сети; обеспечение комфортности для водителей и пользователей транспорта;

обеспечение заданной мобильности населения; повышение безопасности и эффективности транспортного процесса.

Ниже будут рассматриваться ИТС в области автомобильного транспорта крупной городской агломерации.

1. Требования к физической архитектуре ИТС

Интеллектуальная транспортная система крупной городской агломерации представляет собой большую и сложную систему. В соответствии с системной методологией для адекватного описания таких систем используются различные аспекты описания: функциональное, морфологическое (иногда его называют структурным, физическим, аппаратным), информационное (иногда в него включают программное), организационное.

В ГОСТ Р 56294-2014 [5] приведены требования к функциональной и физической архитектурам ИТС. Так как в данной работе рассматривается применение радиотехнологий при реализации ИТС, то далее рассматривается только физическая архитектура интеллектуальных транспортных систем. Упрощенная физическая архитектура ИТС приведена на рис. 1.

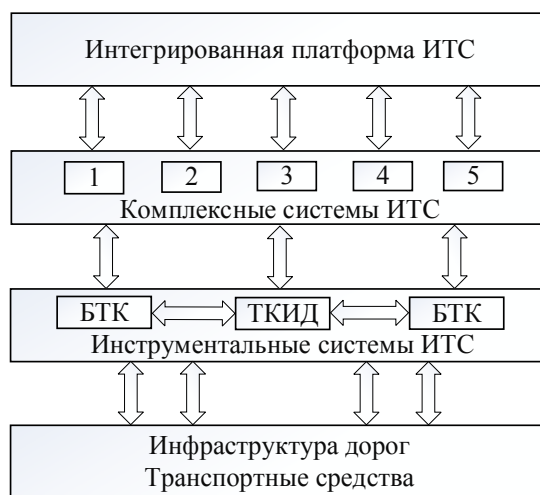


Рис. 1. Физическая архитектура интеллектуальной транспортной системы

На нижнем уровне показаны транспортные средства и инфраструктура дорог. Выше показан уровень инструментальных подсистем ИТС, на котором приведены бортовые телематические комплексы (БТК) и телематические комплексы инфраструктуры дорог (ТКИД). На третьем уровне приведены комплексные подсистемы ИТС. Для компактности рисунка подсистемы ИТС пронумерованы: подсистема управления состоянием дорог (1); система управления дорожным движением (2); подсистема контроля соблюдения ПДД и контроля транспорта (3); подсистема пользовательских сервисов (4); система управления транспортом (5).

На верхнем уровне показана Интегрированная платформа ИТС, которая обеспечивает управление транспортной системой, сбор, агрегирование, обработку и хранение данных от всех подсистем ИТС; визуализацию текущего состояния транспортной системы; корректировку работы подсистем ИТС и режима функционирования транспортной системы.

В ИТС, с использованием радиотехнологий, обмениваются данными элементы транспортных средств, дорожной инфраструктуры, среды коммуникативного взаимодействия, центра обработки данных.

2. Абонентские терминалы транспортных средств

В соответствии с приказом Минтранса РФ № 285 [6], определены требования к средствам навигации, функционирующим с использованием навигационных сигналов системы ГЛОНАСС или ГЛОНАСС/GPS. В документе определён минимальный состав абонентских терминалов:

- навигационный модуль ГЛОНАСС/GPS;
- антенны ГЛОНАСС/GPS и GSM/GPRS;
- тревожная кнопка в кабине водителя;
- соединительные жгуты для присоединения других устройств и датчиков;
- комплект монтажных деталей.

Основными функциями абонентских терминалов являются: прием и обработка сигналов навигационных спутников, передача управляющих сигналов на исполнительные устройства, получение данных с датчиков о состоянии транспортного средства, обеспечение связи с телематическим сервером. Питание абонентских терминалов осуществляется от бортовой сети постоянного тока напряжением 12 или 24 В.

Абонентский терминал обеспечивает возможность подключения дополнительного диспетчерского оборудования:

- голосовой гарнитуры связи водителя с диспетчером;
- датчика уровня топлива транспортного средства;
- датчика пассажиропотока;
- голосового автоинформатора для пассажиров;
- цифрового тахографа для постоянного, автономного и объективного контроля скорости, режима труда, отдыха водителей и членов экипажа;
- маршрутоуказатели для вывода визуальной информации о маршруте движения, а также целый ряд других датчиков.

На первых этапах внедрения ИТС широко использовалась радиотехнология GSM/GPRS по причине повсеместного её применения. Общая тенденция развития радиотехнологий в абонентских устройствах – использование сетей сотовой подвижной связи и беспроводных технологий EC-GSM-IoT/ NB-IoT/ LTE-eMTC. В современном автомобиле передача данных имеет значительные объёмы, так как кроме отслеживания его нормальной работы, обеспечивается и предоставление мультимедийных услуг. Эти технологии дают возможность их использования в абонентских терминалах на базе существующих сетей 2G/3G/4G, обеспечивая максимальную поддержку мобильности транспортных средств. В таблице 1 приведены основные параметры этих технологий [7].

Таблица 1

Основные параметры узкополосных радиотехнологий

Параметры	EC-GSM	NB-IoT	LTE-eMTC
Диапазон частот, МГц	900, 1800	Диапазон LTE	Диапазон LTE
Ширина канала	200 кГц	180 кГц	6 блоков 1,08 МГц в канале от 5 МГц
Скорость передачи данных	70 или 240 кбит/с	158 кбит/с	1 Мбит/с
Задержка	Секунды	Секунды	Миллисекунды

Технология EC-GSM (Extended Coverage GSM) является расширением существующего стандарта GSM. Этот функционал доступен только для абонентских устройств с поддержкой EC-GSM.

Технология NB-IoT (Narrow Band Internet of Things) рекомендуется для Интернета вещей, где требуется максимальная дальность связи, высокая энергоэффективность, малые скорости передачи данных.

Технология LTE-eMTC поддерживает надёжную связь, обеспечивает полную мобильность и высокую скорость передачи данных, но с потерями в максимальном покрытии и в энергетике.

В настоящее время идёт интенсивное развитие абонентских терминалов транспортных средств. Так, компания Cohda Wireless [8] объявила о создании бортового устройства (On-Board Unit) 5-го поколения. Не имея возможности здесь детально рассматривать технические характеристики этого перспективного бортового устройства, отметим лишь некоторые ключевые его особенности.

Устройство основано на автомобильном наборе микросхем RoadLINK, разработанном компанией Cohda в сотрудничестве с NXP Semiconductors. Операционная система – Linux Yocto. Флеш-память – 128 Мб NAND и оперативная память 128 Мб DDR3. Встроенный модуль аппаратных средств безопасности с возможностью создания более 110 подписей в секунду с задержкой подписания менее 9 мс. Спутниковая система навигации – GPS/ГЛОНАСС с чувствительностью: сбор данных -146 дБм; система навигации -158 дБм; система отслеживания -162 дБм. Скорость передачи данных: 3, 4.5, 6, 9, 12, 18, 24, 27 Мбит/с для полосы пропускания 10 МГц.

В бортовом устройстве пятого поколения используется радиосвязь по стандарту IEEE 802.11p. Этот стандарт обеспечивает беспроводную передачу данных между высокоскоростными транспортными средствами со скоростью до 250 км/час и объектами транспортной инфраструктуры. Стандарт используется при создании ИТС, в том числе для подключения автономных транспортных средств.

Дальнейшее развитие стандарта IEEE 802.11p – версия IEEE 802.11bd, основанная на IEEE 802.11ac и обратно совместимая с 802.11p. Стандарт IEEE 802.11bd работает в среде с большой плотностью источников сигнала, увеличивает пропускную способность до более чем 1 Гбит/с, работает со слабыми сигналами с относительной мощностью 3дБм, с увеличением скорости транспортного средства до 500 км/ч. Сравнение основных параметров стандартов IEEE 802.11p, IEEE 802.11bd и 5G NR (New Radio-разработка 3GPP для мобильной сети 5G, Release 15 и 16) приведено в таблице 2 [9,10].

3. Элементы дорожной инфраструктуры

Из анализа определений ИТС, приведенного во введении, следует, что целостность ИТС как системы обеспечивается применением инфокоммуникационных технологий для интеграции средств автоматизации с дорожной инфраструктурой, транспортными средствами и потребностями пользователей транспорта.

Таблица 2

Основные параметры стандартов IEEE 802.11p, IEEE 802.11bd и 5G NR

Параметры	802.11p	802.11bd	5G NR
Диапазон частот, ГГц	5,85 – 5,925	5,85 – 5,925	5,85 – 5,925
Ширина канала, МГц	10/20	10/20	10/20/40/60/80/100
Средняя задержка, мс	< 100	0,5 – 10 (до 300 м) 10 – 100 (от 300 м до 2 км)	0,5 – 10 (до 500 м) 10 – 100 (от 500 м до 2 км)
Дальность связи, км	~ 1	~2	~2
Предельная скорость, км/час	<= 500	<= 500	<= 500
Скорость передачи, Мбит/с	~ 15	~15 – 23	~ 30 - 60
Объём пакета, байт	100-1 500	100-1 500	100-1 500

Дорожная инфраструктура включает следующие сооружения: дорожные знаки и ограждения; устройства для регулирования дорожного движения; технические средства для фиксации нарушений ПДД; остановочные пункты; объекты для освещения автомобильных дорог; дорожки для пешеходов; пункты весового и габаритного контроля транспортных средств; транспон-

деры для взимания платы; парковки транспортных средств; сооружения для охраны автомобильных дорог; тротуары и другие сооружения, за исключением объектов дорожного сервиса. В системах ИТС обязательно функционирует ситуационный центр, который помогает пропускать на вызовы автомобили экстренных служб.

Ниже приведены параметры некоторых элементов дорожной инфраструктуры ИТС [11].

Дорожные видеокamеры высокого разрешения используются в комплексах видеофиксации нарушений ПДД. Промышленные камеры позволяют следить за дорожным потоком, выделять и трассировать движущиеся объекты, выполнять захват кадров с государственными регистрационными знаками транспортных средств, а также распознавать буквенно-символьные изображения на номерах.

Умные светофоры, которыми управляет специальная программа, позволяющая устройству самостоятельно принимать решения на основе поступающей информации о дорожном движении с других аналогичных приборов.

Выделяют три режима работы светофоров.

Локальный. Устройство работает по заложенной схеме, в которой, например, учитываются утренний и вечерний часы пик, а также малая загрузка в течение дня.

Координированный. Предполагает координацию работы нескольких светофоров в одной зоне. Режим используется на «вылетных» магистралях. Светофоры работают синхронно, что способствует поддержанию интенсивного движения на участке.

Адаптивный. Светофор работает самостоятельно и автоматически принимает решения на основе поступающих данных о дорожной ситуации.

Детекторы транспортного потока для фиксации транспортного средства в контролируемой зоне вырабатывают сигнал, который усиливается, обрабатывается и преобразуется в удобный для регистрации вид.

Электронные средства оплаты проезда – транспондеры. Это приемно-передающие устройства, которые позволяют безостановочно двигаться через платные пропускные пункты. Они устанавливаются на лобовое стекло автомобиля, имеют уникальные лицевые счета и идентификационные номера. Чтобы заплатить за проезд, водителю достаточно сбросить скорость до 30 км/ч и деньги автоматически спишутся со счета.

Информационные табло – это основное средство информирования водителей о ситуации на дорогах. На табло может выводиться различная информация: загрузка участков дороги; наличие ДТП на маршруте; состояние дорог и т. д.

Паркоматы – устройства автоматизированной платной парковки. С их помощью автомобилист самостоятельно осуществляет оплату парковки в соответствии с заданными тарифами.

Система автоматизированного управления освещением позволяет полностью автоматизировать уличное и дорожное освещение. Она способна самостоятельно принимать решение о необходимости включения или выключения света в соответствии с ситуацией на дороге, временем суток и других факторов.

Средства автоматической фиксации нарушений -

один из важнейших элементов ИТС, который предназначен не столько для фиксации нарушений ПДД, сколько для предотвращения таких нарушений и дорожно-транспортных происшествий. Камеры способны зафиксировать любое нарушение правил, благодаря чему автомобилисты будут более ответственно соблюдать ПДД.

Интеграция с дорожно-транспортными службами.

Внедрение ИТС предполагает их интеграцию с дорожно-транспортными службами. В случае возникновения любой опасной или аварийной ситуации программное обеспечение сможет быстро провести все уполномоченные спецслужбы до нужного места.

Требования по обеспечению безопасности объектов транспортной инфраструктуры определены в постановлении Правительства РФ №2418 [12]. В этом документе установлены требования по обеспечению транспортной безопасности объектов на 2021-2026 гг. на этапе проектирования и строительства.

Заключение

В результате анализа определений ИТС показано, что основными элементами ИТС являются абонентские терминалы транспортных средств, элементы транспортной инфраструктуры, инструментальные и комплексные подсистемы, информационные и коммуникационные технологии, потребности пользователей в услугах ИТС.

Центральным звеном интеграции абонентских терминалов транспортных средств с элементами транспортной инфраструктуры, с инструментальными и комплексными подсистемами являются информационные и коммуникационные технологии.

При рассмотрении функционирования ИТС в данной работе не рассматривались методы и средства, не связанные или слабо связанные с радиотехнологиями. Поэтому в работе не анализируются информационные технологии искусственного интеллекта и обработки больших данных (Big Data), которые широко применяются в ИТС. В работе детально не рассматривалось подключение к ИТС беспилотных транспортных средств. Приведены лишь краткие сведения о бортовых устройствах пятого поколения. Проблема беспилотных транспортных средств требует отдельного рассмотрения.

Для подтверждения актуальности данной работы нам представляется достаточным следующих сведений. В 2020 году 27 субъектов Российской Федерации прошли отбор в соответствии с методикой, установленной Минтрансом России, и приступили к созданию ИТС. В конце декабря 2020 года распоряжением Правительства Российской Федерации выделено 172,3 млрд рублей на создание ИТС в 27 городских агломерациях.

Литература

1. Концепция Федерального Закона РФ «Интеллектуальная транспортная система Российской Федерации». URL: http://www.tpsa.ru/files/Koncepcia_Intellectualnie_transportnie_sistemy.pdf (дата обращения: 15.01.2021).
2. ГОСТ Р 56829-2015. Интеллектуальные транспортные системы. Термины и определения. Утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 10 декабря 2015 N 2150-ст.
3. Концепция обеспечения безопасности дорожного движения с участием беспилотных транспортных средств на автомобильных дорогах общего пользования. Утверждена распоряжением Правительства РФ от 25 марта 2020 г. № 724-р.
4. Directive 2010/40/eu of the european parliament and of the council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. URL: <https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A02010L0040-20180109> (дата обращения: 20.01.2021).
5. ГОСТ Р 56294-2014. Интеллектуальные транспортные системы. Требования к функциональной и физической архитектурам интеллектуальных транспортных систем. Утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 11 декабря 2014 г. N 1966-ст.
6. «Требования к средствам навигации, функционирующим с использованием навигационных сигналов системы ГЛОНАСС или ГЛОНАСС/GPS и предназначенным для обязательного оснащения транспортных средств категории М, используемых для коммерческих перевозок пассажиров, и категории N, используемых для перевозки опасных грузов». Утверждены приказом Минтранса РФ от 31 июля 2012 г. №285.
7. Концепция построения и развития узкополосных беспроводных сетей связи "Интернета вещей" на территории Российской Федерации. Утверждена приказом Минцифры России от 29 марта 2019 г. № 113.
8. Cohda Wireless' 5th generation On-Board Unit (OBU). URL: www.cohdawireless.com/solutions/hardware/mk5-obu/ (дата обращения: 20.01.2021).
9. Ли П. Архитектура интернета вещей / пер. с англ. М.А. Райтмана. М.: ДМК Пресс, 2020. 454 с.
10. Обзор и сравнение V2X технологий. URL: www.habr.com/ru/post/477826/ (дата обращения: 20.01.2021).
11. Интеллектуальные транспортные системы. URL: <https://center2m.ru/intellektualnye-transportnye-sistemy/> (дата обращения: 26.01.2021).
12. «Требования по обеспечению транспортной безопасности объектов транспортной инфраструктуры по видам транспорта на этапе их проектирования и строительства». Утверждены постановлением Правительства РФ от 31.12.2020 № 2418.