6. Коноплев, В.Г. Реализация микропроцессорных систем на основе суперкристаллов и СБИС пластин / В.Г. Коноплев // Микроэлектроника. – 1988. – Т.17, вып. 5. – С. 432–438.
7. Jerraya, A. Guest Editors' Introduction: Multiprocessor Systems-on-Chips / A. Jerraya, H. Tenhunen, W. Wolf // Computer. – July 2005. – Vol. 38, № 7. – P. 36–40.
8. New Covering Algorithms Implemented in Software System for Input Data Preparation for Single-Beam IC Layout Generator // S. Avakaw [at al.] / Journal of Computational Optimization in Economics and Finance. – 2012. – Vol. 4, Iss. 2-3. – P. 161 – 176.
9. Дудкин, А.А. Методы и алгоритмы перепроектирования интегральных микросхем / А.А. Дудкин // Вестник Брестского государственного технического университета. Физика, математика, информатика. – 2009. – № 5. – С. 62–66.

Материал поступил в редакцию 07.12.14

DOUDKIN A.A. **Algorithm for combining matrix integrated circuit on silicon wafer system**

A description of silicon chips based on Boolean matrices is proposed, that allows to reduce the solution of the task of combining reusable integrated circuit to search the maximum submatrices consisting entirely of good integrated circuits. Using the mathematical apparatus with Boolean matrices allows optimization of combining and obtain better task solutions in comparison of known ones. An algorithm for reconfiguration of the silicon chips is worked out, which is an integral part of modern technology of VLSI non-mask manufacturing.

УДК 004.032.26,004.4

Дудкин А.А., Ганченко В.В., Марушко Е.Е., Чарин С.Н.

КОНТРОЛЬ ТЕЛЕМЕТРИЧЕСКИХ ПАРАМЕТРОВ ЦЕЛЕВОЙ АППАРАТУРЫ КОСМИЧЕСКИХ АППАРАТОВ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ

Введение. Космическая телеметрия – это совокупность технологий, позволяющая производить дистанционный сбор информации о состоянии бортовых подсистем космических аппаратов (КА). В настоящее время в качестве основной физической среды передачи данных телеметрии с КА выступает радиоканал, которому свойственны ограниченные полоса пропускания, длительность сеанса связи и подверженность помехам, что снижает возможности наземных комплексов управления как в отношении мониторинга КА, так и управления им. С другой стороны, своевременное выявление нештатного поведения подсистем КА позволяет в ряде случаев скорректировать их состояние и тем самым, предотвратить развитие на борту аварийной ситуации, что повышает надежность функционирования КА.

В настоящее время телеметрия за редким исключением полностью передается на Землю, где, в случае возникновения на борту нештатных ситуаций (НШС), выполняется ее детальный анализ. Известны четыре метода мониторинга состояния подсистем КА по телеметрическим данным: адаптивный анализ ограничений с использованием относительной векторной регрессии, обнаружение аномалий в телеметрии с использованием метода главных компонент, диагностика и определение аномалий с использованием динамических байесовых сетей (гибридный метод), визуализация телеметрии на основе обнаружения точек перехода.

Надо отметить, что детерминированные алгоритмы не обеспечивают надежной идентификации НШС подсистем КА вследствие утраты той информации, которая содержится в нестационарных и флуктуационных составляющих диагностических сигналов. Нейросетевой подход для решения задач в области контроля, управления и распознавания телеметрической информации благодаря возможности обучения нейронные сети (НС) позволяет учесть не только случайный характер сигналов, но и особенности поведения конкретных подсистем в заданных условиях.

В статье рассматривается задача нейросетевого контроля телеметрической информации (ТМИ) целевой аппаратуры (ЦА) космического белорусского космического аппарата (БКА). Под ЦА понимают аппаратуру, которая обеспечивает выполнение стоящей перед КА, в частности задачу дистанционного зондирования Земли.

Контролируемые параметры ТМИ. Состояние ЦА БКА описывается следующей двухуровневой телеметрической информацией [1]:

- выходное напряжение;
- токопотребление;
- температурный режим.

Мнемосхема блока ЦА и расположение датчиков приведена на рис. 1, где Т38-Т52 –датчики температуры, МСС – многозональная съемочная система, ПСС – панхроматическая съемочная система, ВИП1 и ВИП2 – вторичные источники питания (основной и резервный), логические ядра А и Б – блоки управления.

ВИП обеспечивают токопотребление и входное напряжение бортового записывающего устройства (БЗУ) и контроллера межблочного обмена (КМО), основного контроллера мультиплексного канала обмена (МКО), телеметрии бортовой информационной системы, центрального процессора (ЦП) и запоминающих устройств.

Выходное напряжение включает напряжение ВИП ядра, основного ВИП БЗУ и КМО и резервного ВИП.

Состояние ЦА кодируется сигналами ТМ1-ТМ4 (табл. 1 и 2). Температурные телеметрические параметры приведены в табл. 3.

Таблица 1. Состояния ЦА по сигналам ТМ1, ТМ2

ТМ1	ТМ2	Описание
0	0	Сигналы управления в ЦА не поступали. Процессор и ПЛИС ядра ЦП загружены из основных загрузочных банков.
0	1	В ЦА поступил сигнал управления 1 соответствующего ядра. Произведена перезагрузка процессора из резервного загрузочного банка
1	0	В ЦА поступил сигнал управления 2 соответствующего ядра. Произведена перезагрузка ПЛИС ЯЦП из резервного загрузочного банка
1	1	В ЦА поступил сигнал управления 3 соответствующего ядра. Произведена перезагрузка процессора из основного загрузочного банка. Произведено переключение на резервный источник питания «ВИП ТМ и МКО»

Ганченко Валентин Вячеславович, *кандидат технических наук, научный сотрудник Объединенного института проблем информатики НАН Беларуси.*
Марушко Евгений Евгеньевич, *младший научный сотрудник Объединенного института проблем информатики НАН Беларуси.*
Чарин Сергей Николаевич, *начальник группа ЦУП БКА НИРУП «Геоинформационные системы» НАН Беларуси.*

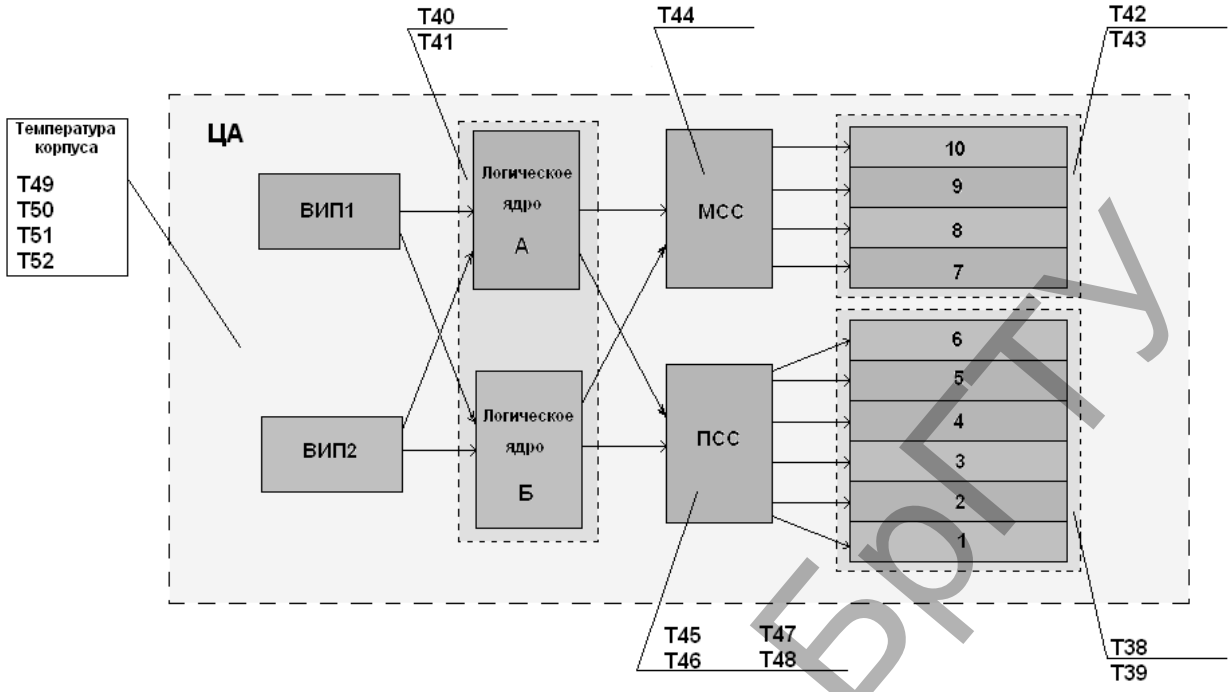

Рис. 1. Мнемосхема ЦА и расположение датчиков

Таблица 2. Состояния ЦА по сигналам ТМ4, ТМ5

Режим	ТМ4	ТМ5	Описание
Включение ЦА	0	0	Инициализация ПО процессора
	1	0	Штатная работа ЦА до маршрута
	0	1	Выполнение операции «Автотест процессора»
	1	1	Выполнение операции «Тестирование ЯМКО»
Работа ЦА	0	0	Штатная работа ЦА вне маршрута
	1	0	Выполняется маршрут со съёмкой в режиме «ЗИ»
	0	1	Выполняется маршрут без съёмки
	1	1	Выполняется маршрут со съёмкой в режиме «НП»

Таблица 3. Температурные телеметрические параметры

Блоки ЦА	Описание
Обеспечения тепловых режимов	Сигналы от 10 датчиков температуры, расположенных в зонах размещения нагревательных элементов ЦА
Электронные	Сигналы от 6 датчиков температуры, расположенных на электронных блоках ЦА (по 2 на каждом из трех блоков)
Источники питания	Сигналы от 9 датчиков температуры

Кроме того, по времени формирования все ТМ параметры подразделяются на массивы двух типов:

- телеметрия включения, которая формируется один раз на каждое включение ЦА;
- текущая телеметрия, которая фиксируется в ЦА в режимах съемки с частотой съемкой кадров, в режимах передачи информации с частотной передачей.

Управление при возникновении неисправностей. При работе КА на орбите возможно возникновение ряда НШС,который можно разделить на две группы:

- аппаратные отказы;
- программные сбои.

К первой группе относятся перегрев оборудования, короткое замыкание в цепях питания, падение напряжения бортовой сети, полный отказ отдельных узлов. К программным сбоям можно отнести недостоверность сформированной приборами информации, программные исключения.

Мониторинг параметров ЦА включает в себя автоматический сбор и диагностирование информации о состоянии КА и выдачу парирующих воздействий: временная приостановка работы КА по целевому назначению, до анализа ситуации. При падении напряжения бортовой сети логичным действием является отключение энергоемких абонентов. При полном отказе какого либо узла производится перевод на дублирующий узел.

Ситуация с отказом оборудования требует еще и точной локализации отказавшего узла. При обнаружении отказа производить работу по его локализации путем перекрестного анализа показаний в течении определенного времени. Если отказ подтверждается по нескольким прямым или косвенным признакам необходимо произвести действия по автоматическому парированию отказа, а в случае если это не удается – перевести КА в энергетически безопасный режим до анализа ситуации.

Управление ЦА при возникновении неисправностей осуществляется следующими видами воздействий:

- передачей с наземного комплекса управления(НКУ) новых установок конфигураций включения ВИП-ов и логических ядер;
- передачей с НКУ в сеансе связи разовых релейных команд управления ЦА или управления питанием ЦА;
- удалением некорректных массивов полетного задания(МПЗ) и передачей с НКУ исправленных МПЗ;
- передачей с НКУ массивов загрузки командно–программной информации(КПИ) ЦА.
- программным управлением ЦА по программам бортовой вычислительной системы(БВС);
- программным управлением ЦА по программам БВС;
- передачей с НКУ массивов загрузки КПИ ЦА.

Модель для идентификация состояний ЦА. Идентификаация состояний подсистем КА основана на нейросетевом подходе ([2], рис. 2).

Входными данными для функционирования предложенной модели являются:

- данные массивов ТМИ соответствующих систем (параметры системы обеспечения тепловых режимов (СОТР), включая СОТР ЦА), параметры системы энергоснабжения (СЭС) (КА и ЦА), параметры корректирующей двигательной установки (КДУ));

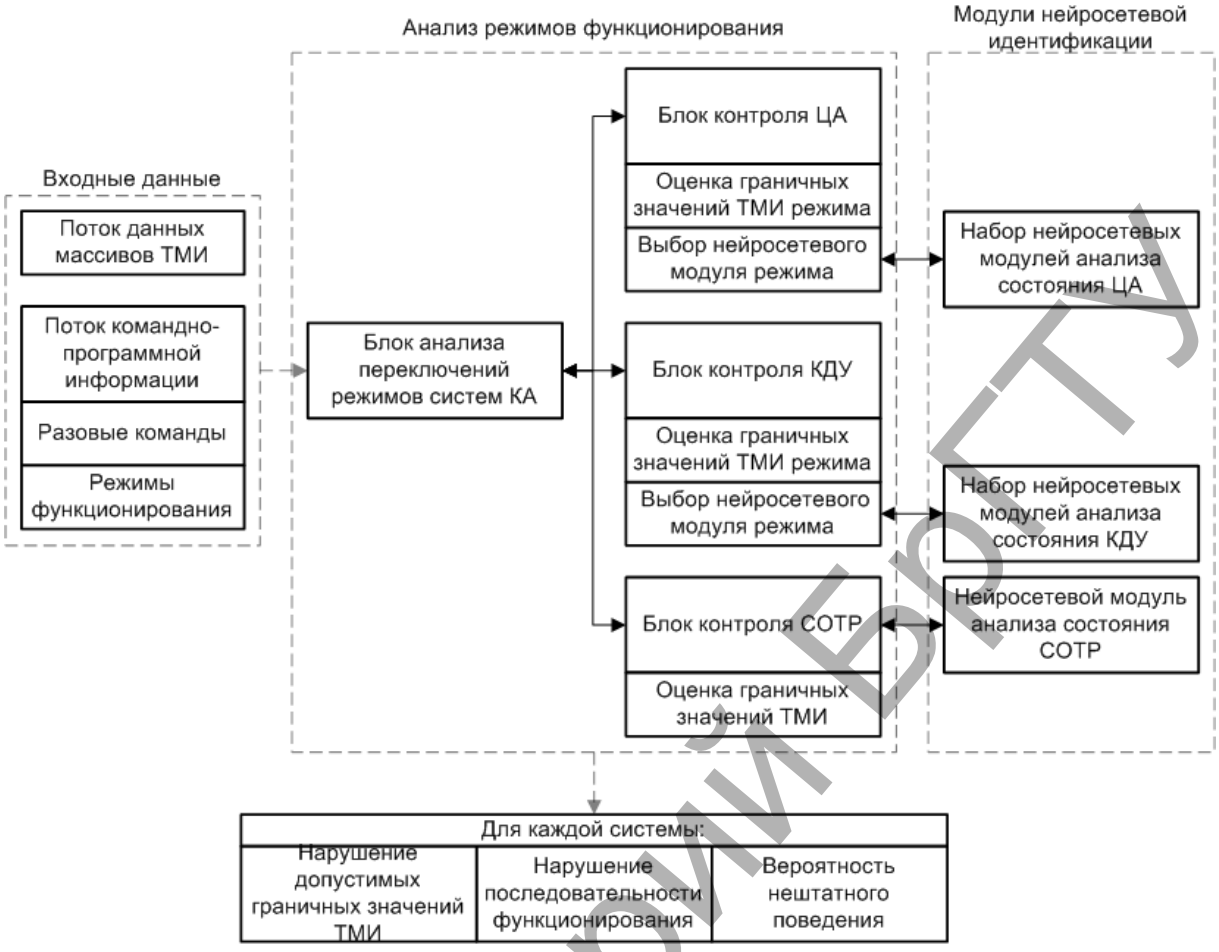

Рис. 2. Схема нейросетевой идентификации состояния подсистем КА

- командно-программная информация (разовые команды, передаваемые с НКУ, предполагаемые режимы функционирования согласно полетному заданию);
- дополнительно могут использоваться данные баллистических траекторных измерений.

Функционирование по данной схеме предполагает наличие этапа обучения. Данный этап включает формирование имитационной модели на основе описания режимов и ограничений функционирования, конструирование нейросетевых модулей для каждого режима функционирования, обучение данных модулей на выборке соответствующей режиму.

Контроль состояния ЦА. Согласно схеме идентификации (рис. 2), анализ режимов функционирования блоков ЦА задействует блок анализа переключений режимов систем КА, блок контроля ЦА, который обращаются к нейросетевым модулям идентификации состояния ЦА.

Блок анализа переключений режимов задействует имитационную модель ЦА функционируют, реализуемую по схеме конечного автомата, в котором множество состояний содержит все допустимые режимы функционирования блоков ЦА, а переходы ограничиваются допустимыми последовательностями функционирования, ограничениями по времени выполнения, ограничениями по управлению. Блок анализа переключений режимов на основе поступающих команд формирует управляющие воздействия для блока контроля ЦА.

В блоке контроля ЦА решаются следующие задачи:

- проверка возможности выполнения текущей команды, и соответствие последовательности выполнения этапов циклограмм;
- анализ нахождения ТМИ в границах допустимых значений;
- при успешном выполнении предыдущих задач, выполняется выбор нейросетевого модуля идентификации, который на основе ТМИ делает прогноз о возможности появления НШС в блоках ЦА (на основе идентификации паттернов нештатных и пред нештатных явлений во временных рядах ТМИ).

Таким образом, формируется решение о нарушении/не нарушении последовательности функционирования (определяет сбой в управлении и поведении ЦА), выходе параметров определенных датчиков за диапазон допустимых значений, заключение о возможности нештатного поведения.

Для осуществления контроля блоков ЦА разработаны следующие алгоритмы:

- общий алгоритм контроля телеметрических параметров ЦА;
- алгоритм анализа последовательности функционирования ЦА;
- алгоритм обучения нейросетевых модулей системы идентификации состояний ЦА;
- алгоритм идентификации НШС ЦА с использованием нейронных сетей;
- алгоритм идентификации этапов функционирования ЦА с использованием НС;
- алгоритм инкрементного дообучения нейросетевых модулей системы идентификации состояний ЦА.

Общий алгоритм контроля телеметрических параметров ЦА предназначен для длительного контроля последовательности функционирования блоков ЦА, контроля внутренних датчиков телеметрии ЦА, прогнозирования нештатного поведения.

Алгоритм состоит из следующих шагов:

1. Инициализация библиотеки имитационных моделей ЦА.
2. Загрузка/обучение нейросетевых модулей анализа состояния ЦА.
3. Прием телеметрических данных и команд.
4. Если подана новая команда (следующая команда МПЗ, команда от НКУ), то производится проверка возможности выполнения команды, и соответствие последовательности команд.

5. Проверка времени выполнения этапов циклограмм режимов функционирования.
6. Анализ нахождения ТМИ в границах допустимых значений для текущего режима ЦА.
7. При успешном выполнении предыдущих операций, выполняется обращение к нейросетевому модуля идентификации, который на основе ТМИ делает заключение о возможности появления НШС ЦА в текущем режиме работы (на основе идентификации паттернов нештатных и преднештатных явлений во временных рядах ТМИ).
8. При успешном выполнении предыдущих операций, анализ точности нейросетевой идентификации, в случае уменьшения – дообучение нейросетевых модулей анализа состояния ЦА.
9. Формирование отчета о состоянии ЦА.
10. Если есть входные данные повторить с п.3.

Шаги 4 и 5 выполняются алгоритмом анализа последовательности функционирования ЦА. На шаге 6 у подсистемы имитационного моделирования ЦА запрашиваются граничные значения для датчиков ТМИ текущего режима функционирования и проверяется нахождение полученных значений в данном диапазоне. Шаг 7 выполняется алгоритмом идентификации НШС ЦА с использованием НС. Шаг 8 реализуется алгоритмом инкрементногодообучения нейросетевых модулей системы идентификации состояний ЦА.

Алгоритм анализа последовательности функционирования ЦА предназначен для проверки корректности последовательности функционирования ЦА, проверки временных интервалов выполнения этапов циклограмм работы. Алгоритм состоит из следующих шагов:

1. Если получена разовая команда (следующая команда МПЗ, команда от НКУ):
   а) Запрос подсистеме имитационного моделирования ЦА на соответствие данной команды возможным состояниям перехода.
   б) Если команда не соответствуют всем возможным состояниям, установить флаг неверно поданной команды.
   в) Если команда соответствуют одному из возможных состояний, перевести конечный автомат подсистемы имитационного моделирования ЦА в найденное.
2. Идентифицировать этап циклограммы функционирования ЦА по полученным массивам ТМИ.
3. Запрос подсистеме имитационного моделирования ЦА на соответствие идентифицированного этапа текущему модельному этапу и предыдущему модельному этапу текущей циклограммы.
4. Если соответствуют предыдущему модельному этапу текущей циклограммы установить флаг нарушения длительности выполнения этапов циклограмм работы и вычислить время превышения выполнения этапа циклограммы.
5. Если этап не соответствуют, установить флаг нарушения последовательности функционирования ЦА.

Обучение нейросетевых модулей системы идентификации состояний ЦА содержит три этапа:

1. Подготовка и отбор релевантных телеметрических данных.
2. Выбор алгоритма обучения (переменной метрики [3], Левенберга-Марквардта [3], эвристический алгоритм обучения многослойного персептрона RPROP [3, 4]).
3. Непосредственно обучение.

Этап подготовки и отбора включает следующие шаги:

1. Формирование набора обучающих данных.
   г) Для задачи идентификации режима/этапа функционирования: каждая запись входного массива Хсодержит значения датчиков в определенный момент времени, выходной массив Y – идентификатор режима/этапа функционирования в соответствующий момент времени.
   д) Для задачи прогнозирования НШС: каждая запись входного массива X содержит значения датчиков в определенном интервале времени, выходной массив Y –сигнал наличия/отсутствия НШС в следующий за интервалом момент времени.
2. Предобработка данных.
3. Выбор поднабора входных данных для обучения. Производится выбор поднабора отдельно для каждого режима функционирования ЦА. Таким образом, сформированный впоследствии нейросетевой модуль будет анализировать ТМИ только одного режима функционирования.

При выборе алгоритма обучения:

1. Выполняется оценка сложности задачи, необходимого объема памяти и вычислительной сложности.
2. Проводится испытательное обучение НС по каждому алгоритму для общего набора данных, оценивается скорость обучения и точность результата.
3. На основании полученных характеристик производится выбор, предпочтение отдается алгоритму с достаточной точностью и высокой скоростью обучения.

На третьем этапе производится синтез и обучение многослойного персептрона на выбранном поднаборе [5]. Обучение подразумевает использование двух тестовых наборов обучающих данных, с финальной оценкой точности на валидационном наборе данных.

Формирование нейросетевых модулей производится для каждого режима ЦА.

Алгоритм идентификации НШС ЦА с использованием НСпредназначен для прогнозирования появления НШСЦА.

Для определения вероятности возникновения НШСна выходе в качестве функции активации используется функция SOFTMAX (1) [3], необходимая для выделения вероятности возникновения неисправности.

$$y(x) = \frac{e^{x}}{\sum_{i} e^{x_i}}. \qquad (1)$$

Вероятности возникновения и не возникновения характеризуют выходной вектор $y = (y_0, y_1)$.

Нейросетевые модули, добавляемые в процессе функционирования на этапе дообучения, для одинаковых режимов организуются в ансамбли.

Ансамбль нейронных сетей (АНС) – представляет собой набор нескольких одиночных НС, независимо решающих задачу. Частные решения одиночных НС поступают на обобщающий модуль (Gatingmodule), который выдает окончательное решение [6, 7]. В качестве обобщающего модуля, согласно алгоритму инкрементного дообучения, используется модуль взвешенного суммирования выходов отдельных НС, веса при этом определяются основываясь на точности каждой НС.

Алгоритм инкрементного дообучения нейросетевых модулей системы идентификации состояний ЦА предназначен для обучения нейросетевых модулей в процессе функционирования, с целью учета изменений ТМИ со временем, вызванных дрейфом целевого значения Понятие дрейф значений относится к изменению значения определения с течением времени, и, следовательно, изменению в распределении данного значения. Среда, из которой эти значения получены, не является стационарной средой. Сдвиг в вероятности может указывать на то, что определения событий также могут изменяться.

Общим знаменателем в алгоритмах детектирования дрейфа выступает ансамбль экспертов, которые постепенно обучаются (без доступа к предыдущим данным) на входных данных, в сочетании с некоторой формой взвешенного голосования для получения финального решения [8]. Правила выбора данных для последующего обучения членов ансамбля, и механизм для определения веса голосования являются отличительными чертами различных алгоритмов. Learn++NSE представляет собой ансамбль, основанный на пакетном обучении, который использует взвешенное голосование большинства, где веса динамически обновляется по отношению к экспертам во время коррекции ошибок на текущих и прошлых данных. Он использует пассивный механизм обнаружения дрейфа, и использует только текущие данные для обучения. Он может обрабатывать различные виды нестационарности: резкое изменение значений, медленный дрейф, циклические изменения, или переменную скорость.

Процедура дообучения повторяется для всех АНС.

Тестирование работы алгоритмов нейросетевой идентификации. Для тестирования взята часть датчиков системы энергообеспечения ЦА БКА.

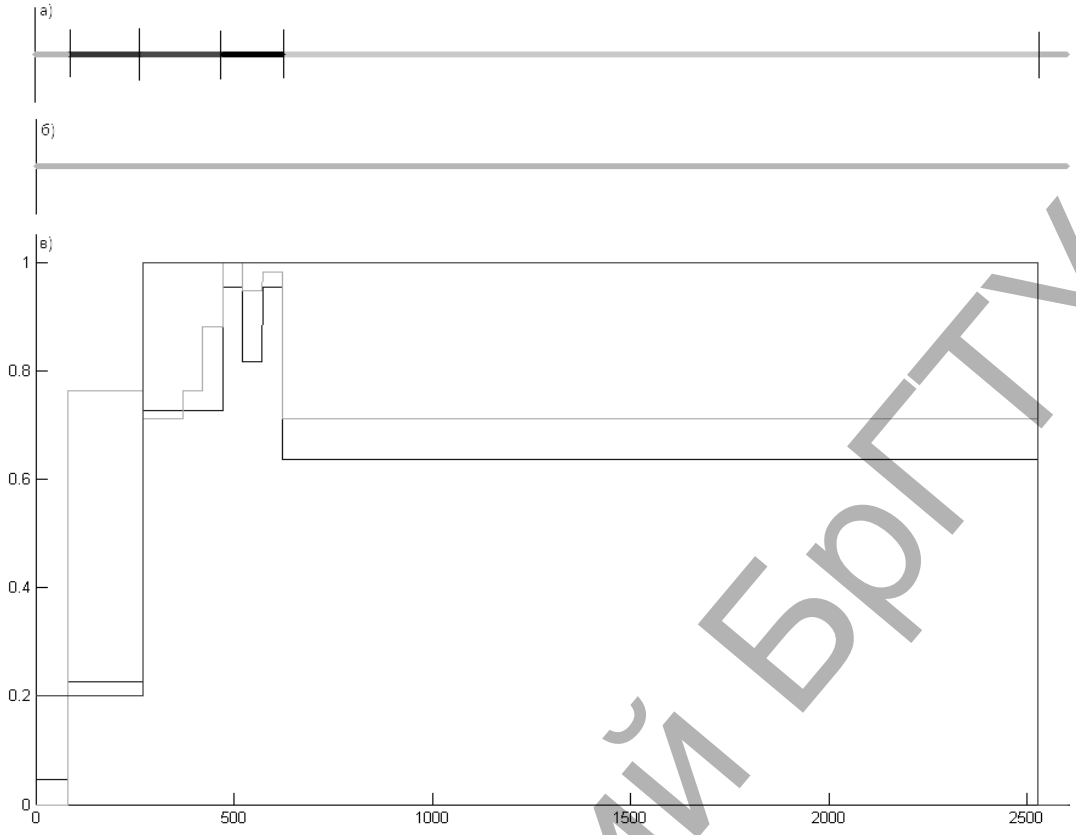

Рис. 3. Идентификация состояний ЦА по многомерным рядам ТМИ:
а) идентифицированные состояние, каждый сегмент соответствует одному этапу циклограммы; б) временная прямая идентификации НШС – НШС не выявлено; в) временные ряды ТМИ датчиков ЦА, нормализованные

Проведено формирование и предобработка обучающей выборки для нейросетевых моделей, включающая нормализацию. Обучены нейросетевые модули идентификации этапов функционирования и НШС. Проведены тестовые проходы по реальным данным ТМИ ЦА.

Результат работы алгоритма идентификации этапов функционирования в графическом виде представлен на рис. 3а.

Результат работы алгоритма идентификации НШС в графическом виде представлен на рисунке 3б. ИдентификацияНШС имеет определенные сложности при обработке на реальных данных, получаемых от работающего космического аппарата. Это низкая вероятность появления сбоя или НШС, что не позволяет сформировать достаточный набор обучающих данных для всех предполагаемых ситуаций. Отсутствие на рисунке 3бвыявленных НШС и проведенное тестирование не позволяет достаточно охарактеризовать алгоритм идентификации НШС ЦА КА и требует дальнейшего изучения.

Заключение. Описанные алгоритмы предоставляют интеллектуальный инструмент решения задач анализа телеметрической информации для разрабатываемого в ОИПИ НАН Беларуси совместно с центром управления полетами БКА экспериментального образца нейросетевой системы мониторинга состояния подсистем космических аппаратов по телеметрическим данным. Положенный в основу мониторинга и диагностики аппарат искусственных нейронных сетей позволяет с высокой точностью обрабатывать телеметрическую информацию, поступающую с КА по радиоканалу, распознавать и классифицировать состояния подсистем и паттерны их поведения даже при неполных и зашумленных входных данных. Открытой задачей для дальнейшей разработки является разработка имитационной модели поведения бортовых объектов и ее взаимодействия с обученными нейросетевыми модулями, что позволит выявлять даже небольшие отклонения динамики поведения от штатно прогнозируемой и принимать соответствующие ситуации решения.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Космический комплекс оперативного мониторинга техногенных и природных чрезвычайных ситуаций «Канопус-В» с космическим аппаратом «Канопус-В» № 1. – М.: ФГУИ «НЛП ВНИИЭМ». 2011. – 110 с.
2. Ганченко, В.В. Нейросетевая модель обработки ТМ-данных для анализа состояния подсистем БКА / В.В. Ганченко и [др.] // VI Белорусский космический конгресс, 28–30 октября 2014 г. – Минск, 2014.
3. Оссовский, С. Нейронные сети для обработки информации / Пер. с пол. И.Д. Рудинского. – М.: Финансыистатистика, 2002. – 344 с.: ил.
4. Riedmiller M., Braun H. A direct adaptive method for faster backpropagation learning: The RPROP algorithm. In Rpoceedings of the IEEE International Conference on Neural Networks (ICNN), pages 586-591, San Francisco, 1993.
5. Царегородцев, В.Г. Конструктивный алгоритм синтеза структуры многослойного персептрона // Вычислительные технологии, 2008. – Т.13 // Вестник КазНУ им. Аль-Фараби, серия "математика, механика, информатика", 2008. №4 (59). (Совм. выпуск). Часть 3. – С. 308–315.
6. Michael I. Jordan, Robert A. Jacobs Hierarchical Mixtures of Experts and the EM Algorithm // Neural Computation. – 1993. – Т. 6. – С. 181–214.
7. Marushko, Y. Using Ensembles of Neural Networks with Different Scales of Input Data for the Analysis of Telemetry Data / Y. Marushko // Proc. of the XV International PhD Workshop OWD 2013, Wisla, 19–22 October 2013. – Gliwice: Silesian University of Technology, 2013. – P. 386–391.
8. Elwell, R. Incremental Learning of Variable Rate Concept Drift / Ryan Elwell and RobiPolikar // MCS, volume 5519 of Lecture Notes in Computer Science. – Springer 2009. – P. 142–151.

Материал поступил в редакцию 08.12.14

DOUDKIN A.A., GANCHENKO V.V., MARUSHKO E.E., CHARIN S.N. **Monitoring telemetry parameters of spacecraft target equipment using neural networks**

Neural network algorithms are proposed for monitoring target equipment on spacecraft telemetry data.

УДК 003.26:51:004(075.8)

Галибус Т.В.

ВЕРИФИКАЦИЯ ПОЛИНОМИАЛЬНОГО МОДУЛЯРНОГО РАЗДЕЛЕНИЯ СЕКРЕТА НАД ДВОИЧНЫМ ПОЛЕМ

В работе предлагается протокол верификации частичных секретов участников полиномиальной пороговой модулярной схемы разделения секрета. Верификация, т.е. проверка корректности разделения секрета, лежит в основе большинства криптографических протоколов в распределенных системах и позволяет исключить обман со стороны участников. В частности, такие схемы применяются для совместных конфиденциальных вычислений (MPC), шифрования на основе атрибутов (ABE) и электронного защищенного голосования (e-voting).

Ранее данную задачу для модулярного подхода решали Ифтене [5], Кайя и Сельджук [8], Кьонг и др.[6], В этих работах внимание уделено исключительно целочисленному разделению секрета [1], [7]. Однако, развивать модулярный подход, в силу его криптографической стойкости как показывает опыт [4], целесообразнее в полиномиальном кольце.

Один из способов верификации параметров полиномиальной схемы основывается на методе Фельдмана [2], и позволяет проверить параметры схем в кольцах $F_p[x]$, таких, что вычисление дискретного логарифма в поле F_p является достаточно трудоемким. Поэтому такое обобщение метода Фельдмана не совсем подходит для кольца $F_2[x]$, на котором построен стандарт разделения секрета СТБ 34.101.60. Для решения указанной задачи предлагается упрощенный протокол, который позволяет участникам при восстановлении исходного значения секрета взаимно верифицировать частичные секреты. Протокол работает при условии, что дилер корректно распределяет данные для проверки и восстановления. Протокол исключает обман со стороны участников схемы. Верификация основывается на опубликованных дилером проверочных значениях и ключах, при помощи которых участники восстановления проверяют частичные секреты друг друга. При этом, получить дополнительную информацию о секрете при помощи проверочных значений доказуемо невозможно, то есть гарантируется безопасность верификации.

Пороговая модулярная схема разделения секрета в кольце $F_p[x]$

Пусть k – число участников схемы и $1 \le t \le k$ – порог. (t, k)-пороговая модулярная полиномиальная схема позволяет раздать участникам частичные секреты таким образом, что секретное значение $s(x) \in F_p[x]$ могут найти лишь t-подмножества участников. Схема позволяет гарантировать защищенность секрета $s(x)$, такого, что $\deg s(x) < n$ при условии, что промежуточный секрет $S(x)$ выбирается так, что $\deg S(x) < tn$:

Распределение частичных секретов:

1) Случайным образом выбирается промежуточное значение секрета $S(x) \in F_p[x]$ с условием
$$\deg S(x) < tn.$$
2) Выбираются попарно различные неприводимые $p_i(x)$, $i = 1,..,k$ и $p(x)$, такие, что $\deg p_i(x) = \deg p(x) = n$.
3) Дилером публикуются $p_i(x)$, $p(x)$, а $s(x) = S(x) \bmod p(x)$ назначается в качестве секрета схемы.
4) Дилером отправляются частичные секреты участников $s_i(x) = S(x) \bmod p_i(x)$ по защищенным каналам связи.

Восстановление секрета:

Участники из подмножества A обмениваются частичными секретами $s_i(x)$, $i \in A$ и находят значение секрета $s(x)$:

$$u_i = s_i P'_{A,i} P_{A\setminus\{i\}}, \forall i \in A,$$
$$S(x) = \sum_{i \in A} u_i \bmod P_A,$$
$$s(x) \equiv S(x) \bmod p(x),$$

где:

$P_A(x) = \prod_{j=i_1}^{i_t} p_j(x)$, где $A = \{i_1,\ldots,i_t\}$ – подмножество t участников;

$$P_{A\setminus\{i\}}(x) = \frac{P_A(x)}{p_i(x)};$$

$$P'_{A,i} = \left(\frac{P_A(x)}{p_i(x)}\right)^{-1} mod\ p_i(x),\ \forall i \in A.$$

Протокол проверки частичных секретов полиномиальной модулярной СРС над двоичным полем. Предлагается протокол проверки частичных секретов участников $s_i(x)$ при восстановлении секрета СРС в кольце $F_2[x]$. Поскольку мультипликативная группа конечного поля является циклической, то для всякого $S(x) \in F_2[x]$ и неприводимого $p(x) \in F_2[x]$, $\deg p(x) = n$, выполняется $(S(x))^d = S(x) mod\ p(x)$, при условии, что $d \equiv 1 mod\ (2^n - 1)$.

Исходными данными протокола являются:

1. Набор неприводимых полиномов в $F_2[x]$:
$$p(x), p_1(x), p_2(x), \ldots, p_k(x), \deg p(x) = \deg p_i(x) = n.$$
При этом $\left(MinDiv\left(2^n - 1\right)\right)^t \ge 2^n - 1$, где $MinDiv(a)$ – наименьший простой делитель натурального числа a.
2. Набор пар $\{e_i, d_i\}$, таких, что $e_i d_i \equiv 1 mod\ (2^n - 1)$, $i = 1,2,\ldots,k$.

Дополнительно к данным, необходимым для восстановления секрета, дилер публикует:

1. $D_1(x) = (S(x))^{d_1} mod\ p_1(x), D_2(x) = \left(S(x)\right)^{d_2} mod\ p_2(x),$
$\ldots, D_k(x) = \left(S(x)\right)^{d_k} mod\ p_k(x),$
которые служат для проверки частичных секретов участников.
2. $E_1 = g^{e_1}, E_2 = g^{e_2}, \ldots, E_k = g^{e_k}$, которые позволяют верифицировать проверочные ключи участников. При этом, $g \in G$ является порождающим элементом циклической группы достаточно большого порядка (а именно, не менее $2^n - 1$), в которой задача дискретного логарифмирования является вычислительно трудной.

Секретными данными участников, которые передаются по закрытым каналам, являются частичные секреты $s_i(x) = S(x) mod\ p_i(x)$ и проверочные ключи e_i.

Галибус Татьяна Васильевна, *доцент кафедры информационных систем управления Белорусского государственного университета. Беларусь, БГУ, 220013, г. Минск, пр. Независимости, 4.*