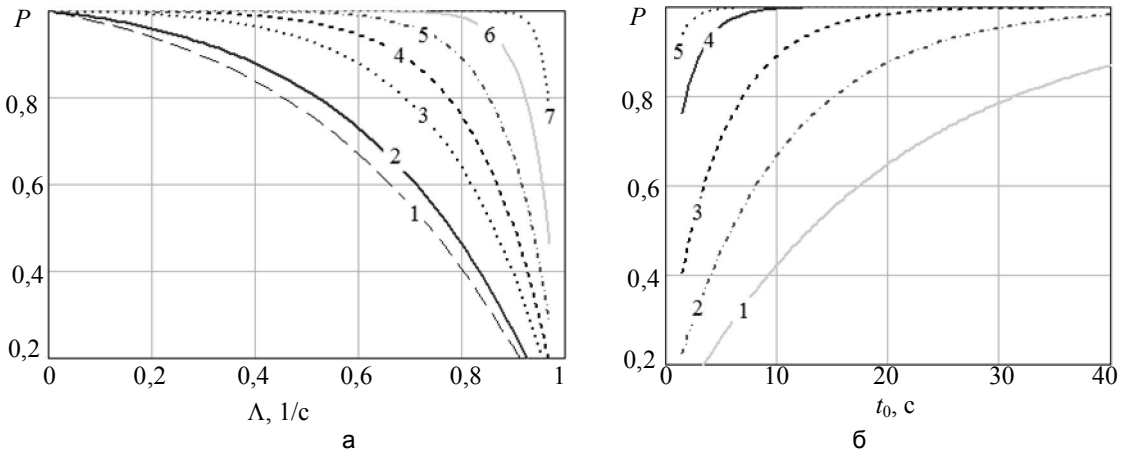
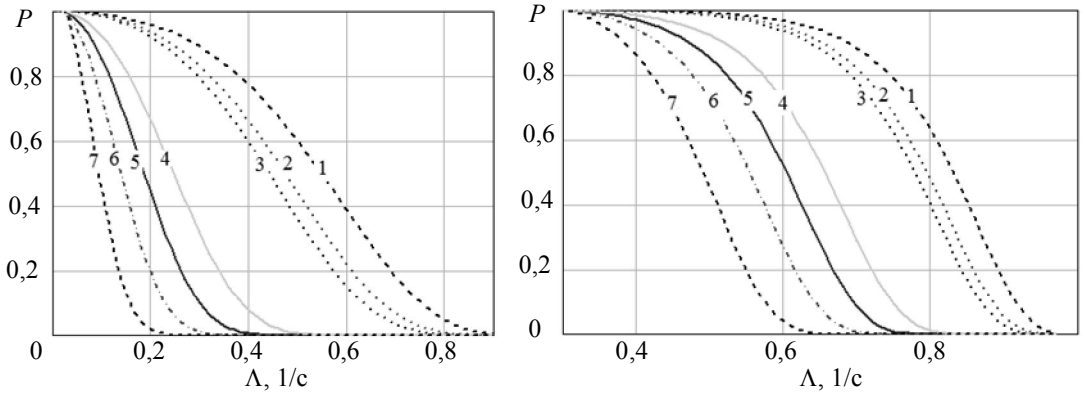


а б

Рис. 1. Вероятности своевременного выполнения критического запроса: от интенсивности их поступления Λ – кривые 1–7 для t_0 = 1,5, 2, 4, 6, 10, 20, 50 с (а); от t_0 – кривые 1–5 для Λ = 0,95, 0,9, 0,8, 0,5, 0,2 1/с



а б

Рис. 2. Вероятность решения критической задачи (кривые 1–7) от интенсивности поступления запросов Λ для времени решения задачи t = 5, 8, 10, 50, 100, 200, 500 с: при t_0 = ≤ 2 с (а) и при t_0 ≤ 10 с (б)

Таким образом, для систем реального времени предложена комплексная оценка надежности, учитывающая готовность вычислительной системы, ее безотказность и вероятность задержек запросов меньших предельно допустимых.

1. Богатырев В.А. Exchange of Duplicated Computing Complexes in Fault tolerant Systems // Automatic Control and Computer Sciences. – 2011. – V. 46. – № 5. – P. 268–276.
2. Богатырев В.А., Богатырев С.В., Богатырев А.В. Оптимизация кластера с ограниченной доступностью кластерных групп // Научно-технический вестник СПбГУ ИТМО. – 2011. – № 1 (71). – С. 63–67.
3. Богатырев В.А., Богатырев С.В., Богатырев А.В. Функциональная надежность вычислительных систем с перераспределением запросов // Изв. вузов. Приборостроение. – 2012. – Т. 55. – № 10. – С. 53–57.

Богатырев Владимир Анатольевич – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, доктор технических наук, профессор, Vladimir.bogatyrev@gmail.com
Богатырев Анатолий Владимирович – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, аспирант, Vladimir.bogatyrev@gmail.com

УДК 004.4'242

ПРИМЕНЕНИЕ МЕТОДОВ РЕШЕНИЯ ЗАДАЧИ О ВЫПОЛНИМОСТИ КВАНТИФИЦИРОВАННОЙ БУЛЕВОЙ ФУНКЦИИ ДЛЯ ПОСТРОЕНИЯ УПРАВЛЯЮЩИХ КОНЕЧНЫХ АВТОМАТОВ ПО СЦЕНАРИЯМ РАБОТЫ И ТЕМПОРАЛЬНЫМ СВОЙСТВАМ

Е.В. Панченко, В.И. Ульянцев

Рассматривается вопрос о применении управляющих автоматов при построении систем со сложным поведением. Предложен метод построения управляющего конечного автомата по заданному множеству сценариев работы и темпоральным свойствам, которые должны выполняться в результирующем автомате. Метод основан на сведении к задаче выполнимости квантифицированной булевой функции. Описан алгоритм построения данной функции и основные составляющие полученной булевой формулы.

Ключевые слова: кванторы, булева функция, управляющие конечные автоматы, верификация.

Парадигма автоматного программирования используется для реализации систем со сложным поведением во многих промышленных отраслях. В настоящее время существуют системы, насчитывающие более тысячи различных состояний, при записи их поведения в виде конечного автомата. Одним из ис-

пользуемых подходов при попытке задать параметры системы на вход сторонним приложениям является передача сценариев работы системы. Как правило, данный метод позволяет эффективно создавать автоматизированные системы по сценариям работы, описываемым, например, в функциональной спецификации продукта. Тем не менее, не все свойства системы можно описать с помощью сценариев работы.

В работе [1] было спроектировано решение, позволяющее решить задачу построения автомата по сценариям работы с помощью сведения ее к задаче о выполнимости булевой формулы (SAT). После этого программный решатель находил набор значений, на котором данная формула истинна, и на основании полученного примера алгоритм строил необходимый автомат.

Полученный автомат удовлетворял заданным сценариям работы, однако зачастую не соответствовал изначальным бизнес-требованиям, поскольку лист сценариев оказывался неполон. Целью настоящей работы является модификация метода построения управляющих автоматов, а именно, добавление возможности использования формул линейной темпоральной логики (LTL) в качестве дополнительного инструмента описания требуемой работы автомата.

На вход разрабатываемой программе подается список сценариев, а также набор темпоральных свойств работы системы. Сценарием работы является последовательность $T_1 \dots T_n$ троек $T_i=<e_i, f_i, A_i>$, где e_i – входное событие; f_i – булева формула от входных переменных, задающая охранное условие; A_i – последовательность выходных воздействий. Автомат, находясь в состоянии S, удовлетворяет элементу сценария T_i, если из S исходит переход, помеченный событием e_i, последовательностью выходных воздействий A_i и охранным условием, тождественно равным f_i как булева формула. Автомат удовлетворяет сценарию работы $T_1 \dots T_n$, если он удовлетворяет каждому элементу данного сценария, находясь при этом в состояниях пути, образованного соответствующими переходами.

На формат входных LTL наложено ограничение в виде невозможности использовать характеристики состояний автомата, поскольку на этапе задания логики состояний еще нет. Однако это позволяет задавать свойства общего формата, что может быть полезно при создании систем с нуля. Было принято решение использовать в качестве переменных LTL-формул входные и выходные воздействия.

Таким образом, синтаксис входных данных включает в себя:

- булевы связки ($!, \wedge, \vee$);
- темпоральные операторы $\mathcal{X}$ (next) и $\mathcal{U}$ (until);
- выведенные темпоральные операторы $\mathcal{F}$ (future), $\mathcal{G}$ (globally in the future), $\mathcal{R}$ (release);
- предикаты:
  - *wasEvent*(*e*) – переход совершен по событию *e*;
  - *wasAction*(*z*) – во время перехода было вызвано выходное воздействие *z*.

Пример входного темпорального свойства, используемого при верификации автомата управления дверьми лифта в работе [2]:

$\mathcal{F}(!(wasEvent(e) \wedge\ !\ wasAction(z))$.

Разработанное программное средство в несколько шагов производит построение искомого конечного автомата, удовлетворящего входным данным.

1. С помощью разработанного в работе [1] алгоритма по заданным сценариям работы создается булева формула, содержащая логические переменные $y_{a,b,e,f}$ (для каждой пары состояний результирующего автомата S_a и S_b, каждого события e, каждой формулы f, встречающейся в заданных сценариях работы), соответствующие наличию перехода из состояния S_a в состояние S_b, помеченного событием e и формулой f в результирующем автомате.
2. С использованием подхода верификации моделей с ограничением на длину вычислений – Bounded Model Checking – входные темпоральные свойста «разворачиваются» в булеву функцию. Для этого используется понятие «обратного цикла» и ограничение его глубины поиска.

   «Обратный цикл» – это цикл, образованный ребром, ведущим из какого-либо состояния пути в состояние, лежащее на данном пути ранее, как показано на рисунке ниже.

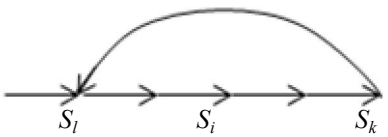


Рисунок. Пример обратного (*k*, *l*)-цикла

Логика линейного времени предполагает, что некоторое утверждение будет выполняться для всех путей. В связи с этим обычно в работах верификации доказательство построено от противного, т.е. проверяется существование пути, на котором выполняется отрицание LTL-формулы. Однако данный подход возможен только при верификации уже построенных автоматов. В нашем случае автомат еще только должен быть построен, поэтому используется квантор всеобщности, позволяя найти такое ре-

шение формулы (значения переменных $y_{a,b,e,f}$), чтобы темпоральные свойства выполнялись на всех путях построенного конечного автомата.

3. Для ограничения времени работы алгоритма устанавливается ограничение на длину цикла k. Таким образом, темпоральные свойства с помощью разложения на композицию темпоральных и булевых предикатов «разворачиваются» по циклу в формулу, размер которой линейно зависит от размера начальной формулы и константы k.
4. Полученные формулы объединяются в одну квантифицированную булеву функцию, проверяющую все бесконечные и конечные пути в радиусе k и содержащую кванторы существования и всеобщности.
5. Для решения полученной формулы используется специализированное программное средство. Полученные значения входных переменных с квантором существования используются для построения искомого управляющего конечного автомата.

Разработан алгоритм автоматизированного построения управляющих автоматов по сценариям работы и темпоральным свойствам, основанный на сведении данных задач к проблеме о разрешимости квантифицированной булевой формулы.

1. Ulyantsev V., Tsarev F. Extended Finite-State Machine Induction using SAT-Solver // Proceedings of the Tenth International Conference on Machine Learning and Applications, ICMLA 2011, Honolulu, HI, USA // IEEE Computer Society, 2011. – V. 2. – P. 346–349.
2. Егоров К.В., Шалыто А.А. Совместное применение генетического программирования и верификация моделей для построения автоматов управления системами со сложным поведением // Научно-технический вестник СПбГУ ИТМО. – 2010. – № 5 (69). – С. 81–89.

Панченко Елена Владиславовна – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, студент, panchenko@rain.ifmo.ru
Ульянцев Владимир Игоревич – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, студент, ulyantsev@rain.ifmo.ru

УДК 004.056

ОБЩАЯ МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОБОТОТЕХНИЧЕСКИХ СИСТЕМ

Е.Н. Коваль, И.С. Лебедев

Предложена модель угроз информационной безопасности робототехнических систем. Ее построение базируется на типовых элементах – программах, ресурсах и структурах.
Ключевые слова: робототехническая система, модель угроз информационной безопасности.

Для широкого применения робототехнических систем (РТС) в различных сферах деятельности необходима формализация технических требований к ним на этапах разработки, внедрения, эксплуатации. Вместе с тем на ранних этапах жизненного цикла разработчики, как правило, уделяют недостаточно внимания вопросам информационной безопасности (ИБ) [1], вследствие чего требуется оценка различных аспектов ИБ, необходимых для выполнения технических и технологических задач.

Анализ ИБ предполагает оценку угроз ИБ от различных факторов, оказывающих влияние на состояние системы [2]. Для описания модели ИБ будем считать, что РТС включает в себя управляющую систему, объект управления и каналы передачи данных. Для каждой составной части РТС, вне зависимости от ее архитектурных и технических особенностей, элементами воздействия угроз могут быть программы, структуры и ресурсы.

На рисунке приведена общая модель ИБ РТС. Совокупность условий и факторов, создающих опасность нарушения ИБ РТС, определяется:

- угрозами, обусловленными воздействием субъектов (персонала или противоборствующей стороны) на систему управления, объекты управления, каналы;
- угрозами, возникающими вследствие особенностей технических характеристик функционирования технических средств (интенсивности сбоев, отказов);
- угрозами, связанными с внешней средой, где применяются РТС.

Реализация угроз может осуществляться посредством уязвимостей, которые в РТС могут иметь:

- программы, обеспечивающие контроль, передачу, прием, анализ команд;
- структуры, определяющие их формы, архитектуры построения и организации действий;
- ресурсы, обеспечивающие выполнение задач.

Представленная общая модель позволяет выделить одинаковые составляющие элементы объектов РТС, что позволяет применять общеизвестные подходы к обеспечению ИБ автоматизированных систем.

Работа выполнена в рамках НИР № 610454 «Разработка интеллектуальных технологий управления, навигации и обработки информации с применением к мобильным робототехническим системам и комплексам».