РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ОТ ВИРУСОВ С ИСПОЛЬЗОВАНИЕМ МОДЕЛИ РАСПРЕДЕЛЕННЫХ ОБЪЕКТНО ОРИЕНТИРОВАННЫХ СТОХАСТИЧЕСКИХ ГИБРИДНЫХ СИСТЕМ

Р. Е. Шарыкин

Белорусский государственный университет, г. Минск;
sharykin@bsu.edu;
науч. рук. – А. Н. Курбацкий, д-р. техн. наук, проф.

Описывается разработка системы стохастической гибридной защиты от вирусов на основе предлагаемой в работе методологии разработки сложных стохастических систем с асинхронной коммуникацией. В соответствии с методологией строится предварительная математическая модель системы защиты в рамках модели Распределенных Объектно-Ориентированных Стохастических Гибридных Систем посредством спецификации модели на языке SHYMaude. Далее следуют этапы апробации и реализации. На каждом из этих этапов проводится статистический анализ модели или имплементации модели для целей апробации и реализации. Результаты анализа используются для доработки исходной модели. В результате применения методологии разработчик получает как программное обеспечение реализующие систему, так и ее математическую модель.

Ключевые слова: математическое моделирование, стохастические гибридные системы, статистический анализ, верификация моделей, разработка программного обеспечения

ВВЕДЕНИЕ

Ввиду растущей важности и сложности современных распределенных систем защиты от вирусов, разработка методологии ориентированной на применение формальных методов на всех этапах разработки, от модели до ее реализации в виде приложения представляется важной задачей.

В данной работе предлагается методология разработки сложных систем с асинхронной коммуникацией с «привязкой» математической модели к разрабатываемому программному обеспечению на всех этапах его разработки, и описывается ее применение к разработке коллаборационной стохастической системы защиты от вирусов.

Такой подход позволяет получить на выходе не только готовое программное обеспечение, но и математическую модель с изученными свойствами, реализацией которой является получаемое программное обеспечение.

МЕТОДОЛОГИЯ РАЗРАБОТКИ

В качестве математической модели предлагается использовать модель РООСГС [1], разработанную для моделирования сложных распределенных стохастических систем с асинхронной коммуникацией. Для спецификации РООСГС предлагается использовать язык SHYMaude [2], который, после трансляции, может выполняться в системе Maude [3]. Для формального задания свойств исследуемой системы предлагается использовать язык QuaTEx [4]. Для статистического анализа системы предлагается использовать инструмент MultiVeStA [5].

Методология разработки описывается следующим образом:

1. Строится модель РООСГС системы посредством ее спецификации на языке SHYMaude.

2. Выбираются и специфицируются на языке QuaTEx метрики, оценки которых представляются важными.

3. С помощью системы MultiVeStA проводится статистическая оценка метрик.

4. В случае обнаружения недочетов в спецификации и/или способов ее «улучшения», спецификация корректируется и переходим к шагу 3. Если результаты удовлетворительны, то переходим к шагу 5.

5. Проводится апробация. Система реализуется на языке, предпочтительно имеющим известное представление в переписывающей логике (например Java). В случае обнаружения аспектов системы, требующих коррекции и/или дополнительного анализа, производится коррекция и/или дополнительный анализ исходной модели и переходим к шагу 3. Если результаты удовлетворительны, переходим к шагу 6.

6. Имеется две возможности усиления полученных результатов: *аналитическое исследование свойств* аналитическими методами и *автоматическое доказательство свойств* с помощью системы автоматического доказательства теорем системы Maude [6].

7. Реализация системы на практике. На данном этапе возможен фоновый статистический анализ для оценки основных метрик системы в реальных условиях.

РАЗРАБОТКА СТОХАСТИЧЕСКОЙ ГРУППОВОЙ СИСТЕМЫ ЗАЩИТЫ ОТ ВИРУСОВ

Первый этап разработки описан в [7], где рассматривается построение предварительной математической модели коллаборационной стохастической системы защиты от вирусов. За основу рассматриваемой

системы защиты взята система, предложенная в [8]. Данная система имела недостаток, который заключался в возможности нахождения «успешной» атаки. В [9] была предложена методика построения атаки [9], следуя которой вирус имел возможность заразить все узлы системы. В [7] данная проблема была решена посредством введения вероятностей в модель. Был проведен статистический анализ метрик, обычно используемых для анализа систем подобного типа и изучено влияние алгоритма выбора групп оповещения на эффективность системы защиты.

Второй этап разработки описан в [10], где описывается апробация полученной системы защиты. Модель системы транслируется в приложение Java, которое разворачивается на виртуальных машинах, имеющих общую сеть, и проводится ее статистический анализ по метрикам, аналогичным использованным на первом этапе разработки с целью выявления аспектов системы, значимость которых проявляется при создании прототипа системы. В процессе апробации было обнаружено преимущество протокола UDP по сравнению с протоколом TCP/IP. Для оценки максимально возможной выгоды от использования UDP был произведен статистический анализ исходной модели РООСГ с соответствующими протоколам значениями параметров. Также было оценено влияние размера групп оповещения и общего количества узлов, и рассмотрен вопрос масштабируемости системы.

В данный момент ведутся работы по реализации системы для целей практического внедрения. Система защиты будет представлять собой сервис, реализованный на языке C и сервисное приложение, которое будет предоставлять информацию о состоянии узлов сети в реальном времени и позволять запускать статистический анализ многократного тестового прогона заражения для оценки функционирования системы на практике.

ЗАКЛЮЧЕНИЕ

В данной работе была предложена методология разработки сложных систем с асинхронной коммуникацией и описана разработка коллаборационной стохастической системы защиты от вирусов в соответствии с предлагаемой методологией. На первом этапе разрабатывается предварительная математическая модель системы, которая дорабатывается на основе результатов проводимого статистического анализа модели. На втором этапе производится апробация модели в условиях, приближенных к реальным, статистический анализ реализации модели и доработка исходной модели

на основе полученных результатов. На третьем этапе ведутся работы по реализации модели для целей практического внедрения системы. Полученная система также будет анализироваться статистическими методами до ее ввода в эксплуатацию.

Библиографические ссылки

1. *Шарыкин Р.Е., Курбацкий А.Н.* Модель распределенных объектно-ориентированных стохастических гибридных систем // Журнал Белорусского государственного университета. Математика. Информатика. – 2019, № 2. – С. 52-61.
2. *Шарыкин Р.Е., Курбацкий А.Н.* Верификация Распределенных Объектно-Ориентированных Стохастических Гибридных Систем // Вестник Гродненского Государственного Университета имени Янки Купалы. Серия 2. Математика. Физика. Информатика, вычислительная техника и управление. – 2019. – Т. 9, № 2. – С. 123-133.
3. *Clavel M. [et al]* Maude: Specification and programming in rewriting logic // Theoretical Computer Science. – 2002. – Vol. 285, iss. 2. – P. 187-243.
4. *Clavel M. [et al]* Building equational proving tools by reflection in rewriting logic // CAFE: An Industrial-Strength Algebraic Formal Method / K. Futatsugi [et al]. – Amsterdam, 2000. – Ch. 1. – P. 1-31.
5. *Sen K., Viswanathan M., Agha G.* On statistical model checking of stochastic systems // Lecture Notes in Computer Science. – 2005. – Vol. 3576. – P. 266-280.
6. *Sebastio S., Vandin A.* MultiVeStA: Statistical model checking for discrete event simulators // Proceedings of the 7th International Conference on Performance Evaluation Methodologies and Tools, Torino, 10-12 December, 2013 ; eds.: A. Horvath [et al]. – Torino, 2013. – P. 310-315.
7. *Шарыкин Р.Е., Курбацкий А.Н.* Применение Формальных Методов при Проектировании Коллаборационной Системы Противовирусной Защиты // Журнал Белорусского государственного университета. Математика. Информатика. – 2020. – Т. 1. – С. 59-69.
8. *Briesmeister L., Porras P.* Microscopic simulation of a group defense strategy // Proceedings of Workshop of Principles of Advanced and Distributed Simulation, Monterey, California, US, 1-3 June, 2005 / Los Alamitos, California, US: IEEE Computer Society ; eds.: D. Nicol [et al]. – 2005. – P. 254-261.
9. *Briesmeister L., Porras P.* Automatically deducing propagation sequences that circumvent a collaborative worm defense // Proceedings of International Performance Computing and Communications Conference, Phoenix, Arizona, US, 10-12 April, 2006 / Los Alamitos, California, US: IEEE Computer Society ; eds.: H. Hassanein [et al]. – Phoenix, 2006. – P. 587-592.
10. *Шарыкин Р.Е.* Апробация модели стохастической коллаборационной защиты от вирусов // Системный анализ и прикладная информатика. – 2021, № 4. – Р. 62-70.