Математические задачи, связанные с верификацией программ и протоколов, обработкой больших данных и машинным обучением

Миронов Андрей Михайлович

Кафедра Математической Теории Интеллектуальных Систем
Механико-математический факультет
Московский Государственный Университет имени М.В.Ломоносова

Москва, 15 апреля 2020 г.

Проблема надежности программного обеспечения

1. Во время запуска ракеты Ariane-5 в июне 1996 года произошел взрыв ракеты спустя 40 сек. после старта (на разработку ракеты было затрачено около $7 млрд.).
   Причина ошибки - неправильная программная реализация преобразований 64- разрядных чисел с плавающей точкой в 16-разрядные целые числа.
2. В феврале 1991 года зенитный комплекс Patriot промахнулся мимо сбиваемой ракеты Scud, ущерб - 28 убитых, более 100 раненых.
   Причина - ошибка в программном обеспечении системы управления (в программе округления дробных чисел).

Проблема надежности программного обеспечения (продолжение)

Другие примеры:

1. ошибки в программе обработки заявлений доноров органов в Великобритании (у 25 человек взяли не те органы)
2. ошибка в антивирусе McAfee (системный файл Windows распознан как вредоносный и удален, что привело к бесконечной перезагрузке операционной системы)
3. 88 критических ошибок в операционной системе Android Froyo (используемой в мобильных устройствах), приводящих к неавторизованному доступу к личным данным пользователей (в том числе - нарушению конфиденциальности электронной переписки, краже денег с банковских счетов, и т.д.).
4. Недавние авиакатастрофы Boeing 737 (сотни погибших).

Это лишь малая часть проблем, связанных с нарушением безопасности компьютерных систем.

Правильность программ

- Нет требований – нет правильности
- Ошибка – несоответствие требованиям
- Ошибки:
  - в формулировке требований,
  - в соблюдении требований.

Ошибки в программах приводят к гибели или травмам людей, крупным финансовым потерям, ущербу окружающей среде, и т.д.
Верификация программы – математическое обоснование утверждения о том, что программа соответствует (или не соответствует) своей спецификации.
Требуется либо найти ошибки, либо формально доказать их отсутствие.

Математические проблемы, связанные с криптографическими протоколами

1. Разработка новых криптографических протоколов аутентификации, электронной подписи, анонимных коммуникаций, распределения криптографических ключей, квантовой передачи, разделения секрета, электронного голосования, электронной коммерции, анонимных аукционов, конфиденциальных вычислений, и др. в новых вычислительных средах (в первую очередь, в облачных вычислениях).
2. Построение математических моделей криптографических протоколов, доказательство стойкости криптографических протоколов на основе этих моделей.
3. Предсказание новых видов атак на криптографические протоколы.

Большие данные и машинное обучение

- Автоматное обучение и процессное обучение, в классах
  - вероятностных автоматов,
  - сетей Петри,
  - распределенных алгоритмов с неограниченным количеством участников
- Анализ естественно-языковых текстов, кластеризация, вероятностно-тематическое моделирование.
- Прогнозирование временных рядов.
- Нечеткая модальная логика.