имитозащиты и защиты данных от случайных сбоев при преобразовании и передаче.

В качестве такой вычислительной модели может выступать клеточный автомат (КЛА) — бесконечная сеть одинаковых автоматов Мура, расположенных в точках пространства с целочисленными координатами, связанных одинаковым образом друг с другом и изменяющих состояние в зависимости от состояний соседей и своего собственного. Динамика состояний однородной пространственно распределенной дискретной системы с локальным взаимодействием элементов может представлять разнообразные варианты поведения (устойчивые конфигурации, циклы, хаос), в том числе не имеющие прямого аналога среди аттракторов непрерывных динамических систем. Такая система в силу однородности и локальности преобразований устойчива к сбоям отдельных элементов.

Алгоритмическая неразрешимость прямой задачи - синтеза функции глобальных (для всех элементарных автоматов) переходов КЛА по локальной функции и обратной задачи - определения структуры и параметров КЛА по множеству его состояний- позволяет использовать такую модель в качестве криптосистемы.

Криптосистемы на клеточных автоматах могут быть как симметричными, так и асимметричными. В случае симметричных криптосистем ключом может служить, например, начальное состояние клеточного автомата, осуществляющего генерацию псевдослучайной последовательности состояний и преобразование открытого текста на основе только локальных правил перехода. Для реализации асимметричных криптосистем могут использоваться обратимые клеточные автоматы. В этом случае в качестве открытого ключа может выступать, например, локальная функция переходов. Для двумерных КЛА отыскание функции, инверсной к заданной локальной функции переходов, относится к числу алгоритмически неразрешимых задач. Поэтому важным направлением исследования является поиск универсальных обратимых КЛА.

Проблему универсальности КЛА можно рассматривать в двух аспектах. В рамках первого универсальность сводится к представлению одних КЛА в других. Клеточный автомат является универсальным, если он моделирует поведение любого другого КЛА той же размерности.

Другой подход к универсальности восходит к универсальной вычислимости. Клеточный автомат является универсальным, если он моделирует универсальную машину Тьюринга. Представляет интерес поиск КЛА с минимальными значениями параметров. Следует отметить, что в общем виде проблема распознавания представимости КЛА также относится к числу алгоритмически неразрешимых.

Кравченко М.В., Лисечко В.П.
(Український державний університет залізничного транспорт, м. Харків)

ДОСЛІДЖЕННЯ МЕТОДІВ НАВЧАННЯ СИСТЕМ УПРАВЛІННЯ МЕРЕЖАМИ КОГНІТИВНОГО РАДІО

Метою роботи є дослідження методів навчання системами управління мережами когнітивного радіо. Це завдання стає все актуальнішим і виходить на передній план, розв'язання якого дало б можливість суттєво підвищити основні характеристики протоколу IEEE 802.22.

В даний час попит на послуги безпроводових телекомунікаційних мереж широкосмугового доступу не забезпечений повною мірою, особливо у приміських і сільських місцевостях, бо постачальники цих послуг найчастіше орієнтовані на густонаселені райони і великі міста. Виходячи з цього, можна стверджувати, що розробка і реалізація безпроводових мережевих рішень регіонального масштабу є актуальною і перспективною.

Стрімкий розвиток безпроводових систем, таких як: системи стільникового та супутникового радіозв'язку, LTE, безпроводові технології Wi-Fi і WiMAX, виявило серйозну проблему. Практично весь частотний діапазон до теперішнього часу розподілений і ліцензований, проте використовується недостатньо ефективно. У результаті, впровадження та використання нових сервісів, для роботи яких необхідна наявність вільних частотних діапазонів, стає важким, а в деяких випадках зовсім неможливим.

Дане завдання стає все актуальнішим і виходить на передній план, розв'язання якого дало б можливість суттєво підвищити основні характеристики протоколу IEEE 802.22.

Косолапов А.А.
(Дніпропетровський національний університет залізничного транспорту імені академіка В. Лазаряна)

ДО ПИТАННЯ ОЦІНКИ ВИМОГ ДО СИСТЕМ ЗАХИСТУ WEB-СЕРВЕРІВ ВІД DDOS-АТАК

Сучасні інформаційні системи будуються на основі інтегрованих корпоративних мереж, що об'єднують величезні інформаційні ресурси з доступом до них великої кількості віддалених користувачів через мережу WWW. Прикладом таких систем є автоматизована система керування вантажними перевезеннями АСК ВП УЗ-Є, інформаційна система українського центру оцінювання якості знань,